Differential Galois groups, specializations and Matzat's conjecture

Ruyong Feng[*] and Michael Wibmer[†]

January 8, 2026

Abstract

We study families of linear differential equations parametrized by an algebraic variety $\mathcal{X}$ and show that the set of all points $x \in \mathcal{X}$, such that the differential Galois group at the generic fibre specializes to the differential Galois group at the fibre over x, is Zariski dense in $\mathcal{X}$. As an application, we prove Matzat's conjecture in full generality: The absolute differential Galois group of a one-variable function field over an algebraically closed field of characteristic zero is a free proalgebraic group.

Contents

1 Introduction

The absolute differential Galois group of a differential field F governs the algebraic properties of solutions of linear differential equations over F. Determining the structure of this group for interesting differential fields is a central problem in differential Galois theory (see e.g., [vdPS03, Section 10]). Matzat's conjecture addresses the case of one-variable function fields.

Matzat's Conjecture. *Let k be an algebraically closed field of characteristic zero and let F be a one-variable function field over k, equipped with a non-trivial k-derivation. Then the absolute differential Galois group of F is the free proalgebraic group on a set of cardinality $|F|$.*

The main goal of this article is to prove Matzat's conjecture (Theorem 5.15) in the form stated above. Several special cases of Matzat's conjecture are already known: The first case, when the differential field F equals $(k(x), \frac{d}{dx})$, with k countable and of infinite transcendence degree (over $\mathbb{Q}$) was established in [BHHW21b]. The case when F is $(k(x), \frac{d}{dx})$, with k of infinite transcendence degree was treated in [BHHW21a]. The

case when k has infinite transcendence degree was established in [Wib23]. Moreover, in [Wib23] it was shown that for an arbitrary algebraically closed field k of characteristic zero, Matzat's conjecture for $(k(x), \frac{d}{dx})$ implies Matzat's conjecture for one-variable function fields over k. On the other hand, thanks to the work in [Wib20] and [BHHW21b], it is known that Matzat's conjecture holds for F countable if and only if every differential embedding problem of finite type over F is solvable. Thus, to prove Matzat's conjecture in full generality, it suffices to prove the following:

Theorem A (Theorem 5.14). *Let k be an algebraically closed field of characteristic zero. Then every differential embedding problem of finite type over $(k(x), \frac{d}{dx})$ is solvable.*

Theorem A was proved in [BHHP21] under the assumption that k has infinite transcendence degree. To remove this unnecessary assumption, we establish a specialization result for Picard-Vessiot rings and differential Galois groups that we deem of independent interest. The most conceptual and useful formulation of our specialization result is in terms of differential torsors (Theorem 4.26). For clarity, we state here a simpler, more concrete, version of our specialization result.

Let $k \subseteq k'$ be an inclusion of algebraically closed fields of characteristic zero. A Picard-Vessiot ring $R/k'(x)$ (the differential analog of the splitting field of a polynomial) for a linear differential equation $\delta(y) = Ay$ with $A \in k'(x)^{n \times n}$, is as a quotient $R = k'(x)[X, \frac{1}{\det(X)}]/\mathfrak{m}$, where X is an $n \times n$ matrix of indeterminates, $\delta(X) = AX$ and $\mathfrak{m}$ is a maximal differential ideal of $k'(x)[X, \frac{1}{\det(X)}]$.

Assume the ideal $\mathfrak{m}$ is generated by $p_1, \ldots, p_m$. Choose a finitely generated k-subalgebra $\mathcal{B}$ of k' and a monic polynomial $f \in \mathcal{B}[x]$ such that $A \in \mathcal{B}[x]_f^{n \times n}$ and $p_1, \ldots, p_m \in \mathcal{B}[x]_f[X, \frac{1}{\det(X)}]$. For $\mathcal{X} = \mathrm{Spec}(\mathcal{B})$, a specialization $c \in \mathcal{X}(k) = \mathrm{Hom}_k(\mathcal{B}, k)$ extends to a map $c \colon \mathcal{B}[x]_f \to k(x)$ by $c(x) = x$. In particular, applying c to the coefficients of A yields a matrix $A^c \in k(x)^{n \times n}$ and applying c to the coefficients of a p_i yields a $p_i^c \in k(x)[X, \frac{1}{\det(X)}]$.

Theorem B (Corollary 5.1). *The set of all $c \in \mathcal{X}(k)$ such that $\mathfrak{m}^c = (p_1^c, \ldots, p_m^c)$ is a maximal differential ideal of $k(x)[X, \frac{1}{\det(X)}]$, i.e., $R^c = k(x)[X, \frac{1}{\det(X)}]/\mathfrak{m}^c$ is a Picard-Vessiot ring for $\delta(y) = A^c y$, is Zariski dense in $\mathcal{X}(k)$.*

So, roughly speaking, Theorem B asserts that, for many specializations, the algebraic relations among the solutions of the specialized equation $\delta(y) = A^c y$ are exactly the specializations of the algebraic relations among the solutions of the generic equation $\delta(y) = Ay$. We note that already the existence of a single "good" specialization in Theorem B is a nontrivial problem.

The behavior of differential Galois groups and Picard-Vessiot rings under specialization has been studied by various authors in various different settings ([Gol57], [Kat90, Section 2.4], [Sin93], [Hru02, Section V], [And04] [BvdP06], [dS09], [Dav16, Section 1.6], [Sei22], [RS23]). Unfortunately, these results are not general or precise enough to be applicable to a proof of Matzat's conjecture.

It is well-known that the set of good specializations in Theorem B may not contain a Zariski open subset, in particular it is in general not Zariski constructible. The easiest example illustrating this point is the differential equation $\delta(y) = \frac{\alpha}{x}y$ with solution x^α, which is transcendental for $\alpha \in k \smallsetminus \mathbb{Q}$ but algebraic for $\alpha \in \mathbb{Q}$.

As in this example, despite the lack of generic behavior with respect to the Zariski topology, the set of good specializations is expected to be "large" and not merely Zariski-dense. To confirm this expectation, we use, following [Hru02], commutative group schemes

3

of finite type over $\mathcal{B}$ to define "open" subsets of $\mathcal{X}(k)$. An ad-open subset (the ad refers to the additive group $\mathbb{G}_a$) of $\mathcal{X}(k)$ is of the form $\{c \in \mathcal{X}(k)|\ c$ is injective on $\Gamma\}$, where Γ is a finitely generated subgroup of $\mathbb{G}_a(\mathcal{B}) = (\mathcal{B}, +)$ and $\mathcal{X}(k)$ is identified with $\mathrm{Hom}_k(\mathcal{B}, k)$. For example, k minus a finitely generated $\mathbb{Q}$-subspace of k, is an ad-open subset of $k = \mathbb{A}^1(k)$. Note that in case Γ is generated by a single element h, the corresponding ad-open subset is the Zariski open subset of $\mathcal{X}(k)$ where h does not vanish. We can thus think of ad-open subsets as a generalization of Zariski open subsets. Ad×Jac-open subsets of $\mathcal{X}(k)$ are defined roughly similar but with the additive group replaced by a product of the additive group with a Jacobian variety. (For a precise formulation see Definition 2.6 below.) For example,

$$\{\alpha \in k|\ 256\alpha^3 - 27 \neq 0 \text{ and } (0,1) \text{ is not torsion on the elliptic curve } y^2 = x^3 - 4\alpha x + 1\} \tag{1}$$

is an ad×Jac-open subset of $k = \mathbb{A}^1(k)$.

A more detailed version of Theorem B, confirming the expectation that the set of good specializations is large, states that the set of good specializations contains an ad×Jac-open subset of $\mathcal{X}(k)$ (Theorem 4.26). Moreover, if the differential Galois group of $\delta(y) = Ay$ (over $k'(x)$) is connected, then the Jacobian variety is not needed, i.e., the set of good specializations contains an ad-open subset (Corollary 4.27).

We note that a result similar to Theorem B but for finite difference equations, i.e., for the operator $k(x) \to k(x)$, $h(x) \mapsto h(x+1)$ instead of the derivation $\frac{d}{dx}$, was established in [Fen21]. There Jacobian varieties are not needed, essentially because $k(x)$ does not have nontrivial finite difference field extensions. (In our context, the Jacobian varieties arise via Jacobians of curves associated to finite field extensions of $k(x)$, which are of course differential fields.) However, in [Fen21] one also requires subsets that are "open" with respect to the multiplicative group. These occur in the step when one has to determine the multiplicative independence of rational functions. In our context, this step is replaced by determining the logarithmic independence of algebraic functions which leads to ad×Jac-open subsets.

Our proof of Theorem B owes a lot to [Hru02]. In particular, it relies on the ideas underlying Hrushovski's algorithm for computing the differential Galois group of a linear differential equation. Compared to the specialization results in [Hru02, Section V], our result is more general and more precise: In [Hru02] open subsets with respect to arbitrary commutative algebraic groups are required, whereas for us, the algebraic group can be chosen to be a direct product of the additive group with a Jacobian variety. If the generic differential Galois group is connected, even the additive group alone is sufficient for us. Moreover, many of the statements in [Hru02, Section V.A] are restricted to the case that $\mathcal{B}$ has Krull dimension one and $k = \overline{\mathbb{Q}}$.

Historically, a prime force for the development of differential algebra and differential Galois theory, was the desire to understand when an indefinite integral or differential equation can be solved "by quadratures". Of course, making the notion of "solving" rigorous was part of the problem. As explained in the beautiful survey [Zan14a], when studied in families, this somewhat old-fashioned topic of solving, is closely connected to some modern problems in the realm of unlikely intersections.

Given an indefinite integral of an algebraic function depending on a parameter, or a linear differential equation depending on a parameter, an important question (asked in [Zan14a, p. 550]) is the following:

For which values of the parameter can the solutions be expressed within some prescribed class, assuming this can't be done for the generic solution?

The expectation is that this set of "exceptional" parameter values is small (albeit not necessarily finite). For example, in [MZ20], it was shown that for a parametric family of differentials on an algebraic curve, which cannot be integrated in elementary terms at the generic fibre, the set of specializations such that the specialized differential can be integrated in elementary terms is small, in fact, finite in many circumstances.

Based on our specialization result (Theorem 4.26) we can answer the above question for classes of functions that are amenable to differential Galois theory in the sense that solvability of a linear differential equation in the class of functions can be characterized through a property of the differential Galois group. For example, for the widely used class of Liouvillian functions we obtain:

Corollary B1 (Corollary 5.6)**.** *Assume that the differential equation $\delta(y) = Ay$ (over $k'(x)$) does not have a basis of solutions consisting of Liouvillian functions, then the set of specializations $c \in \mathcal{X}(k)$ such that the differential equation $\delta(y) = A^c y$ (over $k(x)$) has a basis of solutions consisting of Liouvillian functions, is contained in an ad×Jac-closed subset of $\mathcal{X}(k)$.*

Moreover, if the differential Galois group of $\delta(y) = Ay$ (over $k'(x)$) is connected, then already an ad-closed subset suffices. Here a subset of $\mathcal{X}(k)$ is called ad×Jac-closed (or ad-closed) if its complement is ad×Jac-open (or ad-open). For example, a finitely generated $\mathbb{Q}$-subspace of k is an ad-closed subset of $k = \mathbb{A}^1(k)$.

As an illustration of Corollary B1, consider Bessel's differential equation

$$\delta^2(y) + \tfrac{1}{x}\delta(y) + (1 - (\tfrac{\alpha}{x})^2)y = 0.$$

It has a basis of solutions consisting of Liouvillian functions if and only if $\alpha \notin \frac{1}{2} + \mathbb{Z}$. The exceptional set $\frac{1}{2} + \mathbb{Z}$ is contained in $\mathbb{Q}$, an ad-closed subset of k. As predicted by the general theory, in this case, the Jacobian variety is not needed because the differential Galois group at the generic fibre (i.e., the differential Galois group of Bessel's equation over $k'(x)$, where k' is the algebraic closure of the rational function field $k(\alpha)$) is SL_2, which is connected.

If we choose as class of functions, the class of all algebraic functions, we obtain an equicharacteristic zero version of the Grothendieck-Katz conjecture (cf. [Hru02, Cor. to Prop. 5.1] and [And04, Prop. 7.1.1]):

Corollary B2 (Corollary 5.8)**.** *Assume that the differential equation $\delta(y) = Ay$ (over $k'(x)$) does not have a basis of solutions consisting of algebraic functions, then the set of all specializations $c \in \mathcal{X}(k)$ such that the differential equation $\delta(y) = A^c y$ (over $k(x)$) has a basis of solutions consisting of algebraic functions, is contained in an ad×Jac-closed subset of $\mathcal{X}(k)$.*

Again, if the differential Galois group of $\delta(y) = Ay$ (over $k'(x)$) is connected, then already an ad-closed subset suffices. As the intersection of two ad×Jac-open subsets of $\mathcal{X}(k)$ is nonempty (Remark 2.25), Corollary B2 can also be reformulated in the maybe more familiar spirit of a local to global principle: If the set of all $c \in \mathcal{X}(k)$ such that $\delta(y) = A^c y$ has a basis of solutions consisting of algebraic functions, contains an ad×Jac-open subset (e.g., a nonempty Zariski open subset), then $\delta(y) = Ay$ has a basis of solutions consisting of algebraic functions.

Theorem B (and its more detailed variant Theorem 4.26) can be used to transfer results from a single algebraically closed field of constants (e.g., the field $\mathbb{C}$ of complex numbers) to an arbitrary algebraically closed field of constants. Our prime illustration of this fact is of course our proof of Theorem A. However, we also show how one can deduce a new and very short proof of the *solution of the inverse problem* in differential Galois theory from Theorem 4.26. Recall that the solution of the inverse problem states that every linear algebraic group over k is a differential Galois group over $k(x)$. Using analytic methods, namely Plemelj's (weak) solution of the Riemann-Hilbert problem, this was proved for $k = \mathbb{C}$ already in 1979 ([TT79]). However, it took more than 25 years and contributions of many authors to finally solve the inverse problem for an arbitrary algebraically closed field k of characteristic zero ([Har05]). Using Theorem 4.26, we can deduce the solution of the inverse problem from the solution over $\mathbb{C}$ rather directly. To the best of our knowledge, so far only two types of proofs of the solution of the inverse problem were known. Firstly, the proof from [Har05], secondly proofs that rely on patching. Of course, also Matzat's conjecture and Theorem A imply the solution of the inverse problem. However, these results ultimately rely on patching.

We conclude the introduction with a more detailed outline of the paper. The larger part of the article (Sections 3 and 4) is concerned with the proof of the specialization theorem, which states that the set of "good" specializations contains an ad×Jac-open subset. This result would be vacuous if we do not know that ad×Jac-open subsets are nonempty. While the Zariski denseness of ad-open subsets is readily available in the literature, the Zariski denseness of ad×Jac-open subsets does not seem to be available in the generality required for the proof of Matzat's conjecture. In Section 2 we therefore provide a proof of the Zariski denseness of ad×Jac-open subsets based on a variant of Néron's specialization theorem and a geometric version of abstract Hilbert sets.

In Section 3 we collect various constructions and results from differential Galois theory that are required for the proof of the specialization theorem, including the concept of differential torsors. Differential torsors provide a convenient framework to simultaneously study Picard-Vessiot rings and differential Galois groups under specialization in a compatible fashion. This compatibility is vital for the proof of Theorem A, where, in effect, we consider differential embedding problems under specialization. Roughly, a differential torsor is obtained by spreading out a Picard-Vessiot ring R for $\delta(y) = Ay$ (over $k'(x)$) with the action of the differential Galois group G, into a nice family $\mathcal{R}$ with an action of an affine group scheme $\mathcal{G}$. Our main specialization result, proved at the end of Section 4, then states that there exists an ad×Jac-open subset $\mathcal{U}$ of the parameter space $\mathcal{X}(k)$ such that $\mathcal{R}_c$ is a Picard-Vessiot ring with differential Galois group $\mathcal{G}_c$ for every $c \in \mathcal{U}$.

In the earlier parts of Section 4 the various constructions and criteria from Section 3 are shown to be well-behaved under specialization. Roughly, the proof of the main specialization theorem relies on two intermediate specialization results corresponding to the two main steps of Hrushovski's algorithm. In the first main step of Hrushovski's algorithm one computes the $k'(x)$-algebraic relations among the entries of a fundamental solution matrix for $\delta(y) = Ay$, $A \in k'(x)^{n \times n}$ up to a fixed predetermined degree $d = d(n)$. The corresponding specialization result (Theorem 4.24) is that, if $p_1, \ldots, p_m$ is a basis of the $k'(x)$-vector space of all algebraic relations of degree at most d among the entries of a generic solution matrix, then there exists an ad-open subset $\mathcal{U}$ of $\mathcal{X}(k)$ such that $p_1^c, \ldots, p_m^c$ is a $k(x)$-basis of the vector space of all $k(x)$-algebraic relations of degree at most d among the entries of a fundamental solution matrix for the specialized equation $\delta(y) = A^c y$ for all $c \in \mathcal{U}$.

Roughly, the first step in Hrushovski's algorithm allows one to compute the differential

Galois group up to a torus (and a finite group, which is however irrelevant for our purpose). In the second main step of Hrushovski's algorithm ("the toric part") the central question is to decide the logarithmic independence of algebraic functions. Here, elements $f_1, \ldots, f_m \in F$ belonging to a finite field extension F of $k'(x)$ are called *logarithmically independent* over F if a relation of the form

$$d_1 f_1 + \ldots + d_m f_m = \frac{\delta(f)}{f} \quad \text{with } d_1, \ldots, d_m \in \mathbb{Z} \text{ and } f \in F^\times$$

implies $d_1, \ldots, d_m = 0$.

For $F = k'(x)$ this question can be settled as follows. An element of $k'(x)$ is a logarithmic derivative of an element of $k'(x)$ if and only if all its poles are simple with integer residues. Thus an inspection of the poles and residues of $f_1, \ldots, f_m$ will yield all possible values of $d_1, \ldots, d_m$. For $F/k'(x)$ finite, there exists a similar criterion, however, in this case, it involves the degree zero divisor class group of F/k'. This is exactly how the Jacobian varieties enter into the picture. The degree zero divisor class group of F/k' can be identified with the group $J(k')$, where J is the Jacobian of a smooth projective curve with function field F/k'. The criterion for the logarithmic independence, thus relates the computation of the differential Galois group to the question if certain elements $\gamma_1, \ldots, \gamma_\ell \in J(K)$ are $\mathbb{Z}$-linearly independent. For example, if $a = \frac{x^2}{x^4+x+\alpha}$, the differential Galois group G_α of

$$\delta^2(y) - \left(2a + \frac{\delta(a)}{2a}\right)\delta(y) + \left(a^2 - a - \frac{\delta(a)}{2}\right)y = 0$$

is a subgroup of the group G of 2×2 monomial matrices. A sufficient criterion for $G_\alpha = G$, derived from the criterion for logarithmic independence, is that the point $(0, 1)$ is not a torsion point on the elliptic curve $y^2 = x^3 - 4\alpha x + 1$. This leads to the ad$\times$Jac-open subset in (1). The specialization result corresponding to the second step of Hrushovski's algorithm (Theorem 4.10) states that logarithmic independence of algebraic functions is preserved on an ad$\times$Jac-open subset.

Finally, in Section 5, with the specialization theorem in hand, we prove all the results outlined in the introduction above, including Matzat's conjecture.

Notation and conventions: All rings are assumed to be commutative and unital. All fields are assumed to be of characteristic zero. The group of multiplicative units of a ring $\mathcal{B}$ is denoted by $\mathcal{B}^\times$.

If $\mathcal{X}$ is a scheme over $\mathcal{B}$ and $\mathcal{B} \to \mathcal{B}'$ is a morphism of rings, then $\mathcal{X}_{\mathcal{B}'}$ denotes the scheme over $\mathcal{B}'$ obtained by base change via $\mathcal{B} \to \mathcal{B}'$. A similar notation applies to morphisms of schemes. For an affine scheme $\mathcal{X}$ over $\mathcal{B}$ we write $\mathcal{B}[\mathcal{X}]$ for the ring of global sections of $\mathcal{X}$ so that $\mathcal{X} = \mathrm{Spec}(\mathcal{B}[\mathcal{X}])$. We sometimes abbreviate $\mathcal{B}'[\mathcal{X}_{\mathcal{B}'}]$ to $\mathcal{B}'[\mathcal{X}]$.

For a ring $\mathcal{B}$, the polynomial ring $\mathcal{B}[x]$ over $\mathcal{B}$ in the variable x is always considered as a differential ring with respect to the derivation $\frac{d}{dx}$. Similarly, the field of rational functions in x (over some field of constants) is always considered as a differential field with respect to $\frac{d}{dx}$. We use $R^\delta = \{r \in R \mid \delta(r) = 0\}$ to denote the constants of a differential ring (R, δ). With $X = (X_{ij})_{1 \le i,j \le n}$ we always denote an $n \times n$ matrix of indeterminates (over practically any ring that is around). It is the matrix of coordinate functions on GL_n.

For an algebra $\mathcal{B}$ over a field k and a prime ideal $\mathfrak{p}$ of $\mathcal{B}$ we denote the residue field at $\mathfrak{p}$ with $k(\mathfrak{p})$. If $\mathcal{B}$ is an integral domain, we write $k(\mathcal{B})$ for the field of fractions of $\mathcal{B}$.

If $\mathcal{X}$ is an integral scheme over k, we write $k(\mathcal{X})$ for the function field of $\mathcal{X}$. With $\overline{K}$ we denote the algebraic closure of a field K. As a general rule, we use calligraphic letters (like $\mathcal{A}, \mathcal{B}, \mathcal{E}, \mathcal{X}, \ldots$) when thinking about objects that vary in a family.

Throughout this article k is an algebraically closed field of characteristic zero. By "algebraic group over k" we mean a (not necessarily linear) group scheme of finite type over k. Algebraic groups, or more generally group schemes, are often identified with their functor of points. By a "closed subgroup" of a group scheme we mean a closed subgroup scheme. A "variety" is a geometrically integral separated scheme of finite type over a field.

2   Ad×Jac-open sets

As explained in the introduction, our main goal is to show that, for a linear differential equation depending on parameters, the set of parameter values under which the algebraic properties of the solutions are preserved is "large". In this section, we make precise the meaning of "large" by introducing ad×Jac-open sets following [Hru02] and [Fen21]. Our main specialization theorem (Theorem 4.26) states that the set of good specializations contains an ad×Jac-open subset. This result would of course be useless if it is not known that an ad×Jac-open subset is nonempty.

The main result of this section is that an ad×Jac-open subset is not only nonempty but in fact Zariski dense (Theorem 2.24). It was already shown in [Fen21] that the intersection of an ad-open set with an open set with respect to the multiplicative group is Zariski dense. So most of our work here is focused on the case of abelian varieties. For related but weaker results see [Hru02, Section V.A].

Throughout Section 2 we assume that

- k is an algebraically closed field of characteristic zero;

- $\mathcal{B}$ is a finitely generated k-algebra that is an integral domain and

- $\mathcal{X} = \mathrm{Spec}(\mathcal{B})$.

2.1   Open sets defined by commutative group schemes

Let $\mathcal{E}$ be a commutative group scheme of finite type over $\mathcal{B}$. For every $c \in \mathcal{X}(k)$ we have a specialization morphism
$$\sigma_c \colon \mathcal{E}(\mathcal{B}) \to \mathcal{E}(k),$$
given by applying $\mathcal{E}$, considered as a functor on the category of $\mathcal{B}$-algebras, to the morphism $c \colon \mathcal{B} \to k$. For a finitely generated subgroup Γ of $\mathcal{E}(\mathcal{B})$ we set

$$W_{\mathcal{X}}(\mathcal{E}, \Gamma) = \{c \in \mathcal{X}(k) |\ \sigma_c \text{ is injective on } \Gamma\}.$$

The subsets of $\mathcal{X}(k)$ of the form $W_{\mathcal{X}}(\mathcal{E}, \Gamma)$ satisfy the axioms for a basis of a topology: $\mathcal{X}(k) = W_{\mathcal{X}}(\mathcal{E}, 1)$ and

$$W_{\mathcal{X}}(\mathcal{E}_1, \Gamma_1) \cap W_{\mathcal{X}}(\mathcal{E}_2, \Gamma_2) = W_{\mathcal{X}}(\mathcal{E}_1 \times \mathcal{E}_2, \Gamma_1 \times \Gamma_2). \tag{2}$$

This statement remains true if we restrict the $\mathcal{E}$'s to belong to a class of group schemes that is closed under taking products, such as the class of all abelian schemes.

We can thus consider the topology of $\mathcal{X}(k)$ generated by such a basis. The point of this construction is that, while families of linear differential equations parametrized by $\mathcal{X}$ do not exhibit generic behaviour with respect to the Zariski topology, they may exhibit generic behaviour with respect to such a finer topology. If we allow more $\mathcal{E}$'s in our class, the corresponding topology gets finer and so the genericity statement we hope to prove gets weaker. It is therefore vital to restrict the shape of the allowed $\mathcal{E}$'s as much as possible. In this context, it is then irrelevant whether or not the sets of the form $W_{\mathcal{X}}(\mathcal{E}, \Gamma)$ with $\mathcal{E}$ an allowed group scheme still form a basis of a topology. We note however, that already a genericity result with respect to the discrete topology is not easily obtained, i.e., in the context of Theorem B from the introduction, it is nontrivial to prove the existence of a single good specialization. In fact, we are not aware of a proof of the existence of a single good specialization that does not go through Theorem 2.24.

We next discuss the shape that we will allow for the possible $\mathcal{E}$'s.

Definition 2.1. *A subset $\mathcal{U}$ of $\mathcal{X}(k)$ is* ad-open *if it is of the form $\mathcal{U} = W_{\mathcal{X}}(\mathbb{G}_a, \Gamma)$, for some finitely generated subgroup Γ of $\mathbb{G}_a(\mathcal{B}) = (\mathcal{B}, +)$.*

In other words, a subset $\mathcal{U}$ of $\mathcal{X}(k)$ is ad-open if it is open with respect to the additive group scheme $\mathbb{G}_a$ over $\mathcal{B}$. As we are in characteristic zero, the group $\Gamma \leq (\mathcal{B}, +)$ is torsion free and thus a finite free $\mathbb{Z}$-module. If follows that the ad-open subsets of $\mathcal{X}(k)$ consist of exactly those specializations that preserve the $\mathbb{Z}$-linear independence of a finite family of elements of $\mathcal{B}$.

Note that if Γ is generated by a single nonzero element $b \in \mathcal{B}$, then

$$W_{\mathcal{X}}(\mathbb{G}_a, \Gamma) = \{c \in \mathcal{X}(k) | \ c(b) \neq 0\}$$

is the basic Zariski open subset of $\mathcal{X}(k)$ where b does not vanish. In this sense, the "topology" generated by the ad-open sets is finer than the Zariski topology.

Example 2.2. Let $\mathcal{B} = k[\alpha]$ be a univariate polynomial ring over k so that $\mathcal{X} = \mathbb{A}_k^1$ and $\mathcal{X}(k) = k$. For $\mathbb{Q}$-linearly independent elements $\lambda_1, \ldots, \lambda_n \in k$, let Γ be the subgroup of $(\mathcal{B}, +)$ generated by $\lambda_1, \ldots, \lambda_n$ and α. Then $W_{\mathcal{X}}(\mathbb{G}_a, \Gamma) = k \smallsetminus V$ consists of all elements of k that are not contained in the $\mathbb{Q}$-vector space V generated by $\lambda_1, \ldots, \lambda_n$.

Remark 2.3. *If $\Gamma_1, \ldots, \Gamma_n$ are finitely generated subgroups of $(\mathcal{B}, +)$ and Γ is the subgroup generated by $\Gamma_1, \ldots, \Gamma_n$, then $W_{\mathcal{X}}(\mathbb{G}_a, \Gamma) \subseteq W_{\mathcal{X}}(\mathbb{G}_a, \Gamma_1) \cap \ldots \cap W_{\mathcal{X}}(\mathbb{G}_a, \Gamma_n)$. Thus a finite intersection of ad-open subsets of $\mathcal{X}(k)$ contains an ad-open subset.*

For the specialization arguments to be carried out in Section 4, it is often important to be able to enlarge the k-algebra $\mathcal{B}$ by adjoining finitely many elements from $\overline{k(\mathcal{B})}$, because certain properties of the differential equation at the generic fibre may only manifest themselves over the algebraic closure $\overline{k(\mathcal{B})}$ of the field of fractions of $\mathcal{B}$. We therefore also need to consider subsets of $\mathcal{X}(k)$ that are the form $\phi(W_{\mathcal{X}'}(\mathcal{E}, \Gamma))$, where $\mathcal{X}' = \mathrm{Spec}(\mathcal{B}')$ with $\mathcal{B} \subseteq \mathcal{B}' \subseteq \overline{k(\mathcal{B})}$ and $\mathcal{B}'$ is finitely generated over $\mathcal{B}$, $\mathcal{E}$ is a commutative group scheme of finite type over $\mathcal{B}'$, Γ is a finitely generated subgroup of $\mathcal{E}(\mathcal{B}')$ and $\phi \colon \mathcal{X}'(k) \to \mathcal{X}(k)$ is the morphism induced by the inclusion $\mathcal{B} \subseteq \mathcal{B}'$.

We call an inclusion of integral domains $\mathcal{B} \subseteq \mathcal{B}'$ *algebraic* if the field extension $k(\mathcal{B}')/k(\mathcal{B})$ is algebraic.

The following lemma is a slight variation of [Hru02, Lemma 5A.1]. It shows that for ad-open subsets it is not necessary to consider these more general subsets.

Lemma 2.4. *Let $\mathcal{B} \subseteq \mathcal{B}'$ be an inclusion of integral domains such that $\mathcal{B}'$ is finitely generated and algebraic over $\mathcal{B}$. Set $\mathcal{X}' = \mathrm{Spec}(\mathcal{B}')$ and let $\phi \colon \mathcal{X}'(k) \to \mathcal{X}(k)$ be the morphism induced by the inclusion $\mathcal{B} \subseteq \mathcal{B}'$. If $\mathcal{U}'$ is an ad-open subset $\mathcal{X}'(k)$, then there exists an ad-open subset $\mathcal{U}$ of $\mathcal{X}(k)$ such that $\mathcal{U} \subseteq \phi(\mathcal{U}')$ and $\phi^{-1}(\mathcal{U}) \subseteq \mathcal{U}'$.*

Proof. Let $\mathcal{U}' = W_{\mathcal{X}'}(\mathbb{G}_a, \Gamma')$, where $\Gamma' \leq (\mathcal{B}', +)$ is generated by $\gamma_1', \ldots, \gamma_n'$. Let M be the Galois closure of $k(\mathcal{B}')/k(\mathcal{B})$ and let $T, y_1, \ldots, y_n$ be indeterminates. Set

$$p(T, y_1, \ldots, y_n) = \prod_{g \in \mathrm{Gal}(M/k(\mathcal{B}))} \left(T - \sum_{i=1}^{n} g(\gamma_i') y_i \right) = \sum_{i=0}^{|\mathrm{Gal}(M/k(\mathcal{B}))|} \left(\sum_{j=1}^{\ell_i} b_{i,j} \mathbf{m}_{i,j} \right) T^i,$$

where $\mathbf{m}_{i,1}, \ldots, \mathbf{m}_{i,\ell_i}$ are all monomials in $y_1, \ldots, y_n$ of degree $|\mathrm{Gal}(M/k(\mathcal{B}))| - i$. Since $g(p) = p$ for every $g \in \mathrm{Gal}(M/k(\mathcal{B}))$, all $b_{i,j}$ are in $k(\mathcal{B})$. Write $b_{i,j} = \gamma_{i,j}/a$ where $\gamma_{i,j}, a \in \mathcal{B}$ and $a \neq 0$. Let b be a nonzero element of $\mathcal{B}$ such that any $c \in \mathcal{X}(k)$ with $c(b) \neq 0$ can be lifted to a $c' \in \mathcal{X}'(k)$. (Such a b exists by Chevalley's theorem.) Set $\mathcal{U} = W_{\mathcal{X}}(\mathbb{G}_a, \Gamma)$, where Γ is the subgroup of $\mathcal{B}$ generated by b and all $\gamma_{i,j}$'s.

Assume that $c \in \mathcal{U}$, $c' \in \mathcal{X}'(k)$ and $\phi(c') = c$. We claim that $c' \in \mathcal{U}'$. For a contradiction, suppose $c' \notin \mathcal{U}'$. Then there exists a $\gamma' \in \Gamma' \setminus \{0\}$ such that $c'(\gamma') = 0$. Write $\gamma' = \sum_{i=1}^{n} d_i \gamma_i'$ with $d_1, \ldots, d_n \in \mathbb{Z}$. Since $\gamma' \neq 0$,

$$ap(0, d_1, \ldots, d_n) = a(-1)^{|\mathrm{Gal}(M/k(\mathcal{B}))|} \prod_{g \in \mathrm{Gal}(M/k(\mathcal{B}))} g(\gamma') \neq 0.$$

Furthermore, $ap(\gamma', d_1, \ldots, d_n) = 0$ and

$$ap(0, d_1, \ldots, d_n) = a \sum_{j=1}^{\ell_0} b_{0,j} \mathbf{m}_{0,j}(d_1, \ldots, d_n) = \sum_{j=1}^{\ell_0} \gamma_{0,j} \mathbf{m}_{0,j}(d_1, \ldots, d_n) \in \Gamma.$$

On the other hand, since $c'(\gamma') = 0$, one has that

$$0 = c'\left(ap(\gamma', d_1, \ldots, d_n) \right) = \sum_{i=0}^{|\mathrm{Gal}(M/k(\mathcal{B}))|} c'\left(\sum_{j=1}^{\ell_i} \gamma_{i,j} \mathbf{m}_{i,j}(d_1, \ldots, d_n) \right) c'(\gamma')^i$$

$$= c'\left(\sum_{j=1}^{\ell_0} \gamma_{0,j} \mathbf{m}_{0,j}(d_1, \ldots, d_n) \right) = c'(ap(0, d_1, \ldots, d_n)) = c(ap(0, d_1, \ldots, d_n)).$$

This implies that c is not injective on Γ, because $0 \neq ap(0, d_1, \ldots, d_n) \in \Gamma$, a contradiction. Therefore $\phi^{-1}(\mathcal{U}) \subseteq \mathcal{U}'$.

To see that $\mathcal{U} \subseteq \phi(\mathcal{U}')$, it suffices to note that every $c \in \mathcal{U}$ lifts to a $c' \in \mathcal{X}'(k)$ because $c(b) \neq 0$ as $b \in \Gamma$. $\qquad \square$

For group schemes, other than the additive group $\mathbb{G}_a$, we do not have a statement analogous to Lemma 2.4 at hand. Therefore, in this case, we need to consider algebraic extensions $\mathcal{B}' \supseteq \mathcal{B}$.

For simplicity, we call a group scheme $\mathcal{E}$ over some integral domain $\mathcal{B}_0$ of *abelian type* (or of *Jacobian type*) if it is commutative, separated and of finite type over $\mathcal{B}_0$ such that the generic fibre $\mathcal{E} \times_{\mathrm{Spec}(\mathcal{B}_0)} \mathrm{Spec}(K_0)$ is an abelian variety (or a Jacobian variety) over K_0, where K_0 is the field of fractions of $\mathcal{B}_0$.

Lemma 2.5. *Consider the following three kinds of subsets of $\mathcal{X}(k)$:*

(i) *subsets of the form $\phi(W_{\mathcal{X}'}(\mathbb{G}_a \times \mathcal{J}, \Gamma))$ with $\mathcal{J}$ of Jacobian type;*

(ii) *subsets of the form $\phi(W_{\mathcal{X}'}(\mathbb{G}_a, \Gamma_1) \cap W_{\mathcal{X}'}(\mathcal{J}, \Gamma_2))$ with $\mathcal{J}$ of Jacobian type;*

(iii) *subsets of the form $W_{\mathcal{X}}(\mathbb{G}_a, \Gamma_1) \cap \phi(W_{\mathcal{X}'}(\mathcal{J}, \Gamma_2))$ with $\mathcal{J}$ of Jacobian type.*

Then a subset of one kind contains a subset of any other kind. Here, in all of the above cases, $\mathcal{X}' = \mathrm{Spec}(\mathcal{B}')$, with $\mathcal{B}'$ finitely generated and algebraic over $\mathcal{B}$ and $\phi \colon \mathcal{X}'(k) \to \mathcal{X}(k)$ is induced by the inclusion $\mathcal{B} \subseteq \mathcal{B}'$.

Proof. As $W_{\mathcal{X}'}(\mathbb{G}_a, \Gamma_1) \cap W_{\mathcal{X}'}(\mathcal{J}, \Gamma_2) = W_{\mathcal{X}'}(\mathbb{G}_a \times \mathcal{J}, \Gamma_1 \times \Gamma_2)$, a set of the second kind is in fact a set of the first kind. Conversely, given $\Gamma \le \mathbb{G}_a(\mathcal{B}') \times \mathcal{J}(\mathcal{B}')$ let $\Gamma_1 \le \mathbb{G}_a(\mathcal{B}')$ denote the image of Γ under $\mathbb{G}_a(\mathcal{B}') \times \mathcal{J}(\mathcal{B}') \to \mathbb{G}_a(\mathcal{B}')$ and $\Gamma_2 \le \mathcal{J}(\mathcal{B}')$ the image of Γ under $\mathbb{G}_a(\mathcal{B}') \times \mathcal{J}(\mathcal{B}') \to \mathcal{J}(\mathcal{B}')$. Then $\Gamma \le \Gamma_1 \times \Gamma_2$ and so

$$W_{\mathcal{X}'}(\mathbb{G}_a, \Gamma_1) \cap W_{\mathcal{X}'}(\mathcal{J}, \Gamma_2) = W_{\mathcal{X}'}(\mathbb{G}_a \times \mathcal{J}, \Gamma_1 \times \Gamma_2) \subseteq W_{\mathcal{X}'}(\mathbb{G}_a \times \mathcal{J}, \Gamma).$$

Thus a subset of the first kind contains a subset of the second kind.

If $W_{\mathcal{X}}(\mathbb{G}_a, \Gamma_1) \cap \phi(W_{\mathcal{X}'}(\mathcal{J}, \Gamma_2))$ is a subset of the third kind, we may consider Γ_1 as a subgroup of $(\mathcal{B}', +)$ and then $W_{\mathcal{X}}(\mathbb{G}_a, \Gamma_1) \cap \phi(W_{\mathcal{X}'}(\mathcal{J}, \Gamma_2)) = \phi(W_{\mathcal{X}'}(\mathbb{G}_a, \Gamma_1) \cap W_{\mathcal{X}'}(\mathcal{J}, \Gamma_2))$. Thus a subset of the third kind is in fact a subset of the second kind.

Finally, given a subset $\phi(W_{\mathcal{X}'}(\mathbb{G}_a, \Gamma_1) \cap W_{\mathcal{X}'}(\mathcal{J}, \Gamma_2))$ of the second kind, there exists, by Lemma 2.4, a finitely generated subgroup Γ_0 of $(\mathcal{B}, +)$ such that $W_{\mathcal{X}}(\mathbb{G}_a, \Gamma_0) \subseteq \phi(W_{\mathcal{X}'}(\mathbb{G}_a, \Gamma_1))$ and $\phi^{-1}(W_{\mathcal{X}}(\mathbb{G}_a, \Gamma_0)) \subseteq (W_{\mathcal{X}'}(\mathbb{G}_a, \Gamma_1)$. We then have

$$W_{\mathcal{X}}(\mathbb{G}_a, \Gamma_0) \cap \phi(W_{\mathcal{X}'}(\mathcal{J}, \Gamma_2)) \subseteq \phi(W_{\mathcal{X}'}(\mathbb{G}_a, \Gamma_1) \cap W_{\mathcal{X}'}(\mathcal{J}, \Gamma_2)).$$

So a subset of the second kind contains a subset of the third kind. $\square$

We now define the "open" subsets of $\mathcal{X}(k)$ that are the most relevant for us.

Definition 2.6. *A subset $\mathcal{U}$ of $\mathcal{X}(k)$ is ab-open (or Jac-open) if it is of the form $\mathcal{U} = \phi(W_{\mathcal{X}'}(\mathcal{E}, \Gamma))$, where $\mathcal{X}' = \mathrm{Spec}(\mathcal{B}')$ with $\mathcal{B}'$ containing $\mathcal{B}$ an integral domain finitely generated and algebraic over $\mathcal{B}$, $\mathcal{E}$ is a group scheme over $\mathcal{B}'$ of abelian (or of Jacobian) type, Γ is a finitely generated subgroup of $\mathcal{E}(\mathcal{B}')$ and $\phi \colon \mathcal{X}'(k) \to \mathcal{X}(k)$ is the morphism induced by the inclusion $\mathcal{B} \subseteq \mathcal{B}'$.*

A subset of $\mathcal{X}(k)$ is $\mathrm{ad} \times \mathrm{Jac}$-open if it is the intersection of an ad-open subset with a Jac-open subset of $\mathcal{X}(k)$.

A subset of $\mathcal{X}(k)$ is $\mathrm{ad} \times \mathrm{Jac}$-closed (or ad-closed) if its complement is $\mathrm{ad} \times \mathrm{Jac}$-open (or ad-open).

In particular, a Jac-open subset is ab-open. We have used the third kind of subsets from Lemma 2.5 to define $\mathrm{ad} \times \mathrm{Jac}$-open subset. The lemma shows that we could have, more or less equivalently, also used the first or second kind of subsets in the definition.

Lemma 2.7. *Let $\mathcal{B}'$ be an integral domain containing $\mathcal{B}$ such that $\mathcal{B}'$ is finitely generated and algebraic over $\mathcal{B}$. Let $\phi \colon \mathcal{X}'(k) \to \mathcal{X}(k)$ denote the morphism induced by the inclusion $\mathcal{B} \subseteq \mathcal{B}'$ and let $\mathcal{U}'$ be a subset of $\mathcal{X}'(k)$ that is either ad-open, ab-open, Jac-open or $\mathrm{ad} \times \mathrm{Jac}$-open, then $\phi(\mathcal{U}')$ contains a subset $\mathcal{U}$ of $\mathcal{X}(k)$ that is of the same type as $\mathcal{U}'$.*

Proof. The case of ad-open subsets follows from Lemma 2.4. For the case of ab-open and Jac-open subsets it suffices to note that if $\mathcal{B} \subseteq \mathcal{B}' \subseteq \mathcal{B}''$ are such that $\mathcal{B}'$ is finitely generated and algebraic over $\mathcal{B}$ and $\mathcal{B}''$ is finitely generated and algebraic over $\mathcal{B}'$, then $\mathcal{B}''$ is finitely generated and algebraic over $\mathcal{B}$. The case of $\mathrm{ad} \times \mathrm{Jac}$-open subsets is similar but also uses Lemma 2.5. $\square$

2.2 Hilbert sets

To show that ad×Jac-open subsets are Zarisiki dense we will use Hilbert sets. We therefore, in this section, recall their definition and discuss the properties that are relevant for our proof.

Throughout Section 2.2 let k_0 be a field of characteristic zero and let $\mathcal{B}_0$ be a finitely generated k_0-algebra that is an integral domain.

We begin by recalling the abstract definition of *Hilbert sets* from [Lan83, Chapter 9, Section 5]. This is closely related to the notion of *thin sets* (see e.g., [FJ08, Section 13.5]) but restricted to the affine setting.

For an inclusion $\mathcal{B}_0 \subseteq \mathcal{B}_0'$ of integral domains, an element $b' \in \mathcal{B}_0'$ is called *algebraic* over $\mathcal{B}_0$ if b' (considered as an element of the field of fractions of $\mathcal{B}_0'$) is algebraic over the field of fractions of $\mathcal{B}_0$, i.e., b' satisfies a nonzero (not necessarily monic) univariate polynomial over $\mathcal{B}_0$. Moreover, $\mathcal{B}_0'$ is *algebraic* over $\mathcal{B}_0$ if every element of $\mathcal{B}'$ is algebraic over $\mathcal{B}$, i.e., the field extension $k_0(\mathcal{B}_0')/k_0(\mathcal{B}_0)$ of the corresponding fields of fractions is algebraic.

Let $\mathcal{B}_0'$ be an integral domain containing $\mathcal{B}_0$ such that $\mathcal{B}_0'$ is algebraic over $\mathcal{B}_0$ and a finitely generated $\mathcal{B}_0$-algebra. The corresponding fields of fractions then form a finite field extension $k_0(\mathcal{B}_0')/k_0(\mathcal{B}_0)$.

Let $H(\mathcal{B}_0'/\mathcal{B}_0)$ denote the subset of $\mathrm{Spec}(\mathcal{B}_0)$ consisting of all $\mathfrak{p} \in \mathrm{Spec}(\mathcal{B}_0)$ such that there exists a unique $\mathfrak{p}' \in \mathrm{Spec}(\mathcal{B}_0')$ lying above $\mathfrak{p}$ and for this $\mathfrak{p}'$ one has $[k_0(\mathfrak{p}') : k_0(\mathfrak{p})] = [k_0(\mathcal{B}_0') : k_0(\mathcal{B}_0)]$. A subset of $\mathrm{Spec}(\mathcal{B}_0)$ of the form $H(\mathcal{B}_0'/\mathcal{B}_0)$ is called a *basic Hilbert set*.

Recall that a basic Zariski open subset of $\mathrm{Spec}(\mathcal{B}_0)$ has the form $D(b) = \{\mathfrak{p} \in \mathrm{Spec}(\mathcal{B}_0)| \ b \notin \mathfrak{p}\}$ for some nonzero $b \in \mathcal{B}_0$. A *Hilbert subset* of $\mathrm{Spec}(\mathcal{B}_0)$ is a finite intersection of basic Hilbert sets with a basic Zariski open set.

Example 2.8. Let $p \in \mathcal{B}_0[y]$ be a univariate polynomial of positive degree such that $(p) \subseteq \mathcal{B}_0[y]$ is a prime ideal. Set $\mathcal{B}_0' = \mathcal{B}_0[y]/(p)$. Then $H(\mathcal{B}_0'/\mathcal{B}_0)$ consists of all $\mathfrak{p} \in \mathrm{Spec}(\mathcal{B}_0)$ such that the leading coefficient of p does not lie in $\mathfrak{p}$ and the image $\bar{p}$ of p in $k_0(\mathfrak{p})[y]$ is an irreducible polynomial. To see this, note that the set of primes of $\mathcal{B}_0'$ lying above $\mathfrak{p}$ can be identified with the spectrum of $\mathcal{B}_0' \otimes_{\mathcal{B}_0} k_0(\mathfrak{p}) = k_0(\mathfrak{p})[y]/(\bar{p})$.

For k_0 algebraically closed, the above notion of Hilbert subset is not really useful: If $\mathfrak{p}$ is a closed point of $\mathrm{Spec}(\mathcal{B}_0)$ (i.e., a maximal ideal) then $k_0(\mathfrak{p}) = k_0$ has no finite extensions. Thus, if $\mathfrak{p}$ belongs to some basic Hilbert set $H(\mathcal{B}_0'/\mathcal{B}_0)$, we must have $[k_0(\mathcal{B}_0') : k_0(\mathcal{B}_0)] = 1$. So $k_0(\mathcal{B}_0') = k_0(\mathcal{B}_0)$ and $\mathcal{B}_0'$ is contained in a localization of $\mathcal{B}_0$.

The following definition introduces a notion of Hilbert set that is useful when working over an algebraically closed field. Recall that (throughout Section 2) k is an algebraically closed field of characteristic zero, $\mathcal{B}$ is a finitely generated k-algebra that is an integral domain and $\mathcal{X} = \mathrm{Spec}(\mathcal{B})$.

Definition 2.9. *A subset $\mathcal{H}$ of $\mathcal{X}(k)$ is a* geometric Hilbert set *if there exists a subfield k_0 of k finitely generated over $\mathbb{Q}$, a finitely generated k_0-subalgebra $\mathcal{B}_0$ of $\mathcal{B}$ such that the canonical map $\mathcal{B}_0 \otimes_{k_0} k \to \mathcal{B}$ is an isomorphism and a Hilbert subset H of $\mathcal{X}_0 = \mathrm{Spec}(\mathcal{B}_0)$ such that $\mathcal{H}$ is the inverse image of H under $\mathcal{X}(k) \to \mathcal{X} \to \mathcal{X}_0$. In case we need to be more specific, we call such an $\mathcal{H}$ a* geometric $\mathcal{B}_0/k_0$-Hilbert set.

We will see below that geometric Hilbert sets are always Zariski dense in $\mathcal{X}(k)$. The following two lemmas will be needed to establish further good behavior of (geometric) Hilbert sets.

Lemma 2.10. *Let $\mathcal{B}'_0$ be an integral domain containing $\mathcal{B}_0$ such that $\mathcal{B}'_0$ is algebraic over $\mathcal{B}_0$ and a finitely generated $\mathcal{B}_0$-algebra. Then there exists a nonzero $b \in \mathcal{B}_0$ such that for every $\mathfrak{p} \in D(b)$*

- *there exists a $\mathfrak{p}' \in \operatorname{Spec}(\mathcal{B}'_0)$ lying above $\mathfrak{p}$;*

- *the fibre $\mathcal{B}'_0 \otimes_{\mathcal{B}_0} k_0(\mathfrak{p})$ is a $k_0(\mathfrak{p})$-vector space of dimension $[k_0(\mathcal{B}'_0) : k_0(\mathcal{B}_0)]$;*

- *for every prime $\mathfrak{p}' \in \operatorname{Spec}(\mathcal{B}'_0)$ lying above $\mathfrak{p}$ one has $[k_0(\mathfrak{p}') : k_0(\mathfrak{p})] \leq [k_0(\mathcal{B}'_0) : k_0(\mathcal{B}_0)]$.*

Proof. As $\mathcal{B}'_0$ is finitely generated algebraic over $\mathcal{B}_0$, there exists a nonzero $b_1 \in \mathcal{B}_0$ such that $(\mathcal{B}'_0)_{b_1}$ is integral over $(\mathcal{B}_0)_{b_1}$. Since $(\mathcal{B}'_0)_{b_1}$ is finitely generated over $(\mathcal{B}_0)_{b_1}$, in fact $(\mathcal{B}'_0)_{b_1}$ is finite over $(\mathcal{B}_0)_{b_1}$. By generic freeness (see e.g., [Sta24, Tag 051S]) there exists a nonzero $b_2 \in \mathcal{B}_0$ such that $(\mathcal{B}'_0)_{b_1 b_2}$ is not only finite over $(\mathcal{B}_0)_{b_1 b_2}$ but even free. The rank d of $(\mathcal{B}'_0)_{b_1 b_2}$ as a $(\mathcal{B}_0)_{b_1 b_2}$-module is then necessarily equal to $[k_0(\mathcal{B}'_0) : k_0(\mathcal{B}_0)]$.

We claim that $b = b_1 b_2$ has the required property. First note that because $(\mathcal{B}'_0)_b$ is integral over $(\mathcal{B}_0)_b$, for every $\mathfrak{p} \in D(b)$ there exists a $\mathfrak{p}' \in \operatorname{Spec}(\mathcal{B}'_0)$ lying above $\mathfrak{p}$.

Regarding the second point, note that for $\mathfrak{p} \in D(b)$ the fibre

$$\mathcal{B}'_0 \otimes_{\mathcal{B}_0} k_0(\mathfrak{p}) = (\mathcal{B}'_0)_b \otimes_{(\mathcal{B}_0)_b} k_0(\mathfrak{p})$$

is a $k_0(\mathfrak{p})$-vector space of dimension d. Thirdly, a prime $\mathfrak{p}' \in \operatorname{Spec}(\mathcal{B}'_0)$ lying above $\mathfrak{p}$ corresponds to a prime $\tilde{\mathfrak{p}}'$ in $\operatorname{Spec}(\mathcal{B}'_0 \otimes_{\mathcal{B}_0} k_0(\mathfrak{p}))$. The residue field of $\mathfrak{p}'$ can be identified with the residue field of $\tilde{\mathfrak{p}}'$, which is an extension of degree at most d of $k_0(\mathfrak{p})$. □

Lemma 2.11. *Let $\mathcal{B}'_0$ be an integral domain containing $\mathcal{B}_0$ such that $\mathcal{B}'_0$ is algebraic and finitely generated over $\mathcal{B}_0$. Let $\pi \colon \operatorname{Spec}(\mathcal{B}'_0) \to \operatorname{Spec}(\mathcal{B}_0)$ denote the morphism corresponding to the inclusion $\mathcal{B}_0 \subseteq \mathcal{B}'_0$ and let $H' \subseteq \operatorname{Spec}(\mathcal{B}'_0)$ be a Hilbert set. Then there exists a Hilbert set H in $\operatorname{Spec}(\mathcal{B}_0)$ satisfying the following two conditions:*

- $H \subseteq \pi(H')$ *and*

- *for every $\mathfrak{p} \in H$ there exists a unique $\mathfrak{p}' \in \operatorname{Spec}(\mathcal{B}'_0)$ lying above $\mathfrak{p}$. (Of course then $\mathfrak{p}' \in H'$.)*

Proof. Write $H' = H(\mathcal{B}''_1/\mathcal{B}'_0) \cap \ldots \cap H(\mathcal{B}''_n/\mathcal{B}'_0) \cap D(b')$. By Lemma 2.10 there exists a nonzero $b'_1 \in \mathcal{B}'_0$ such that, for $i = 1, \ldots, n$, every prime in $D(b'_1)$ lifts to a prime in $\mathcal{B}''_i$ and for every prime $\mathfrak{p}''_i \in \operatorname{Spec}(\mathcal{B}''_i)$ lying above $\mathfrak{p}' \in D(b'_1)$ one has $[k_0(\mathfrak{p}''_i) : k_0(\mathfrak{p}')] \leq [k_0(\mathcal{B}''_i) : k_0(\mathcal{B}'_0)]$. By Chevalley's theorem there exists a nonzero $b_1 \in \mathcal{B}_0$ such that $D(b_1) \subseteq \pi(D(b'_1 b'))$.

By Lemma 2.10 again, there exists a nonzero $b_2 \in \mathcal{B}_0$ such that for every $\mathfrak{p} \in D(b_2)$ the $k_0(\mathfrak{p})$-vector space $\mathcal{B}'_0 \otimes_{\mathcal{B}_0} k_0(\mathfrak{p})$ has dimension $[k_0(\mathcal{B}'_0) : k_0(\mathcal{B}_0)]$ and for every prime $\mathfrak{p}'$ of $\mathcal{B}'_0$ lying above $\mathfrak{p}$ one has $[k_0(\mathfrak{p}') : k_0(\mathfrak{p})] \leq [k_0(\mathcal{B}'_0) : k_0(\mathcal{B}_0)]$.

We claim that $H = H(\mathcal{B}''_1/\mathcal{B}_0) \cap \ldots \cap H(\mathcal{B}''_n/\mathcal{B}_0) \cap D(b_1 b_2)$ has the required property. Let $\mathfrak{p} \in H$. As $\mathfrak{p} \in D(b_1) \subseteq \pi(D(b'_1 b'))$, there exists a prime $\mathfrak{p}' \in D(b'_1 b')$ lying above $\mathfrak{p}$. Since $\mathfrak{p} \in D(b_2)$ we have $[k_0(\mathfrak{p}') : k_0(\mathfrak{p})] \leq [k_0(\mathcal{B}'_0) : k_0(\mathcal{B}_0)]$.

Because $\mathfrak{p}' \in D(b'_1)$ there exists, for every $i = 1, \ldots, n$, a prime $\mathfrak{p}''_i \in \operatorname{Spec}(\mathcal{B}''_i)$ lying above $\mathfrak{p}'$ and satisfying $[k_0(\mathfrak{p}''_i) : k_0(\mathfrak{p}')] \leq [k_0(\mathcal{B}''_i) : k_0(\mathcal{B}'_0)]$. As $\mathfrak{p}''_i \in \operatorname{Spec}(B''_i)$ is a prime above $\mathfrak{p}$ and $\mathfrak{p} \in H(\mathcal{B}''_i/\mathcal{B}_0)$, we see that $\mathfrak{p}''_i$ is the unique prime of $\mathcal{B}''_i$ above $\mathfrak{p}$ and that $[k_0(\mathfrak{p}''_i) : k_0(\mathfrak{p})] = [k_0(\mathcal{B}''_i) : k_0(\mathcal{B}_0)]$. Therefore

13

$$[k_0(\mathcal{B}_i'') : k_0(\mathcal{B}_0)] = [k_0(\mathcal{B}_i'') : k_0(\mathcal{B}_0')] \cdot [k_0(\mathcal{B}') : k_0(\mathcal{B}_0)] \geq [k_0(\mathfrak{p}_i'') : k_0(\mathfrak{p}')] \cdot [k_0(\mathfrak{p}') : k_0(\mathfrak{p})] =$$
$$= [k_0(\mathfrak{p}_i'') : k_0(\mathfrak{p})] = [k_0(\mathcal{B}_i'') : k_0(\mathcal{B}_0)]$$

and it follows that

$$[k_0(\mathfrak{p}') : k_0(\mathfrak{p})] = [k_0(\mathcal{B}') : k_0(\mathcal{B}_0)] \quad \text{and} \quad [k_0(\mathfrak{p}_i'') : k_0(\mathfrak{p}')] = [k_0(\mathcal{B}_i'') : k_0(\mathcal{B}_0')]. \qquad (3)$$

We next show that $\mathfrak{p}' \in H'$. As $\mathfrak{p}' \in D(b')$ we only have to show that $\mathfrak{p}' \in H(\mathcal{B}_i''/\mathcal{B}')$ for $i = 1, \ldots, n$. If there was a prime of $\mathcal{B}_i''$ other than $\mathfrak{p}_i''$ lying above $\mathfrak{p}'$, this would also be a prime other than $\mathfrak{p}_i''$ lying above $\mathfrak{p}$ which is impossible. Thus $\mathfrak{p}_i''$ is the unique prime of $\mathcal{B}_i''$ lying above $\mathfrak{p}'$. By (3) we see that $\mathfrak{p}' \in H(\mathcal{B}_i''/\mathcal{B}')$. So $\mathfrak{p}' \in H'$ and $\mathfrak{p} \in \pi(H')$, i.e., $H \subseteq \pi(H')$.

Regarding the second item, note that by the choice of b_2, the fibre $\mathcal{B}_0' \otimes_{\mathcal{B}_0} k_0(\mathfrak{p})$ is a $k_0(\mathfrak{p})$-vector space of dimension $[k_0(\mathcal{B}') : k_0(\mathcal{B}_0)]$. On the other hand, there exists a prime in $\mathcal{B}_0' \otimes_{\mathcal{B}_0} k_0(\mathfrak{p})$ whose residue field is an extension of $k_0(\mathfrak{p})$ of degree $[k_0(\mathcal{B}') : k_0(\mathcal{B}_0)]$. Thus $\mathcal{B}_0' \otimes_{\mathcal{B}_0} k_0(\mathfrak{p})$ is a field and there is only one prime in $\mathrm{Spec}(\mathcal{B}_0')$ lying above $\mathfrak{p}$. $\qquad \square$

We next relate the abstract notion of Hilbert set with the more classical notion concerned with polynomials that remain irreducible under specialization (see [FJ08, Chapter 12]).

Let $p_1, \ldots, p_n \in \mathcal{B}_0[y]$ be monic univariate polynomials that are irreducible as elements of $k_0(\mathcal{B}_0)[y]$. For a prime ideal $\mathfrak{p}$ of $\mathcal{B}_0$ let $\overline{p_i}$ denote the image of p_i in $k_0(\mathfrak{p})[y]$, i.e., the coefficients of p_i are reduced modulo $\mathfrak{p}$. We set

$$H_{\mathcal{B}_0}(p_1, \ldots, p_n) = \{\mathfrak{p} \in \mathrm{Spec}(\mathcal{B}_0)|\ \overline{p_1}, \ldots, \overline{p_n} \in k_0(\mathfrak{p})[y] \text{ are irreducible }\}.$$

Lemma 2.12. *Let $\mathcal{B}_0'$ be an integral domain containing $\mathcal{B}_0$, finitely generated and algebraic over $\mathcal{B}_0$. Then there exists a monic polynomial $p \in \mathcal{B}_0[y]$ such that p is irreducible in $k_0(\mathcal{B}_0)[y]$ and a nonzero $b \in \mathcal{B}_0$ such that*

$$H_{\mathcal{B}_0}(p) \cap D(b) \subseteq H(\mathcal{B}_0'/\mathcal{B}_0).$$

Proof. As $k_0(\mathcal{B}_0')/k_0(\mathcal{B}_0)$ is a finite field extension, there exists, by the primitive element theorem, a $b' \in \mathcal{B}_0'$ such that $k_0(\mathcal{B}') = k_0(\mathcal{B}_0)[b']$. Replacing b' with a $\mathcal{B}_0$-multiple of b' if necessary, we can assume that the minimal polynomial p of b' over $k_0(\mathcal{B}_0)$ has coefficients in $\mathcal{B}_0$. Write $\mathcal{B}_0' = \mathcal{B}_0[b_1', \ldots, b_n']$ and $b_i' = p_i(b')$ with $p_i \in k_0(\mathcal{B}_0)[y]$ ($1 \leq i \leq n$). Let $b \in \mathcal{B}_0 \smallsetminus \{0\}$ be such that bp_i has coefficients in $\mathcal{B}_0$ for $i = 1, \ldots, n$. Then $b_i' \in (\mathcal{B}_0)_b[b']$ and therefore $(\mathcal{B}_0')_b = (\mathcal{B}_0)_b[b'] = (\mathcal{B}_0)_b[y]/(p)$.

Let $\mathfrak{p} \in H_{\mathcal{B}_0}(p) \cap D(b)$. Then $\mathfrak{p}_b$ is a prime ideal of $(\mathcal{B}_0)_b$ and for the fibre of $\mathcal{B}_0'/\mathcal{B}_0$ over $\mathfrak{p}$ we have

$$\mathcal{B}_0' \otimes_{\mathcal{B}_0} k_0(\mathfrak{p}) = (\mathcal{B}_0')_b \otimes_{(\mathcal{B}_0)_b} k_0(\mathfrak{p}_b) = (\mathcal{B}_0)_b[y]/(p) \otimes_{(\mathcal{B}_0)_b} k_0(\mathfrak{p}_b) = k_0(\mathfrak{p})[y]/(\overline{p}).$$

As $\mathfrak{p} \in H_{\mathcal{B}_0}(p)$, we see that $\mathcal{B}_0' \otimes_{\mathcal{B}_0} k_0(\mathfrak{p})$ is a field extension of $k_0(\mathfrak{p})$ of degree $\deg(p) = [k_0(\mathcal{B}_0') : k_0(\mathcal{B}_0)]$. Thus $\mathfrak{p} \in H(\mathcal{B}_0'/\mathcal{B}_0)$ as desired. $\qquad \square$

As an immediate corollary to Lemma 2.12 we obtain:

Corollary 2.13. *Let H be a Hilbert subset of $\operatorname{Spec}(\mathcal{B}_0)$. Then there exist $p_1 \ldots, p_n \in \mathcal{B}_0[y]$ monic and irreducible in $k_0(\mathcal{B}_0)[y]$ and $b \in \mathcal{B}_0 \smallsetminus \{0\}$ such that*

$$H_{\mathcal{B}_0}(p_1, \ldots, p_n) \cap D(b) \subseteq H.$$

□

A different, less intrinsic, notion of geometric Hilbert set was used in [Fen21]. In order to be able to use the results from [Fen21], we have to relate the two notions. Let us first recall the definition from [Fen21, Notation 2.6].

Recall that $\mathcal{B}$ is a finitely generated k-algebra that is an integral domain. By Noether's normalization lemma, we can find $\eta_1, \ldots, \eta_\ell, \ldots, \eta_m \in \mathcal{B}$ such that $\mathcal{B} = k[\eta_1, \ldots, \eta_m]$, $\eta_1, \ldots, \eta_\ell$ are algebraically independent over k and $\eta_{\ell+1}, \ldots, \ldots, \eta_m$ are integral over $k[\eta_1, \ldots, \eta_\ell]$. We abbreviate $\boldsymbol{\eta} = (\eta_1, \ldots, \eta_m)$ and $\boldsymbol{\eta}_\ell = (\eta_1, \ldots, \eta_l)$.

Note that for $i = 1, \ldots, m-\ell$, the minimal polynomial of $\eta_{\ell+i}$ over $k(\boldsymbol{\eta}_l)$ has coefficients in $k[\boldsymbol{\eta}_\ell]$ since $k[\boldsymbol{\eta}_\ell]$ is integrally closed ([AM69, Prop. 5.15]). We can thus find a subfield k_0 of k finitely generated over $\mathbb{Q}$ such that, for $i = 1, \ldots, m - \ell$, the minimal polynomial of $\eta_{\ell+i}$ over $k(\boldsymbol{\eta}_l)$ has coefficients in $k_0[\boldsymbol{\eta}_\ell]$.

Let $\boldsymbol{p}$ be a finite tuple of monic elements of $k_0[\boldsymbol{\eta}][y]$ that are irreducible in $k_0(\boldsymbol{\eta})[y]$. Furthermore, let $b \in k_0[\boldsymbol{\eta}] \smallsetminus \{0\}$ and let $\boldsymbol{d} = (d_1, \ldots, d_\ell) \in \mathbb{Z}^\ell$ be an ℓ-tuple of positive integers. Identifying $\mathcal{X}(k)$ with $\operatorname{Hom}_k(\mathcal{B}, k)$ we define

$$\mathcal{H}^{\boldsymbol{\eta}}_{k_0, \mathcal{X}(k)}(\boldsymbol{d}, \boldsymbol{p}, b)$$

as the set of all $c \in \mathcal{X}(k)$ such that

- $[k_0(c(\eta_1), \ldots, c(\eta_i)) : k_0(c(\eta_1), \ldots, c(\eta_{i-1}))] \geq d_i$ for $i = 1, \ldots, \ell$;

- for every entry p of $\boldsymbol{p}$ the polynomial p^c obtained from p by applying c to the coefficients is irreducible in $k_0(c(\boldsymbol{\eta}))[y]$;

- $c(b) \neq 0$.

The following lemma shows that every geometric Hilbert set contains a set of the form $\mathcal{H}^{\boldsymbol{\eta}}_{k_0, \mathcal{X}(k)}(\boldsymbol{d}, \boldsymbol{p}, b)$.

Lemma 2.14. *Let $k_0 \subseteq k$ be a finitely generated field extension of $\mathbb{Q}$ and $\mathcal{B}_0 \subseteq \mathcal{B}$ a finitely generated k_0-algebra such that $\mathcal{B}_0 \otimes_{k_0} k \to \mathcal{B}$ is an isomorphism. Furthermore, let H be a Hilbert subset of $\mathcal{X}_0 = \operatorname{Spec}(\mathcal{B}_0)$ and let $\mathcal{H} \subseteq \mathcal{X}(k)$ be the corresponding geometric Hilbert set.*

Then there exists $\boldsymbol{\eta} \in \mathcal{B}_0^m$ with $\mathcal{B}_0 = k_0[\boldsymbol{\eta}]$ and appropriate $\boldsymbol{p}, b$ such that

$$\mathcal{H}^{\boldsymbol{\eta}}_{k_0, \mathcal{X}(k)}((1, \ldots, 1), \boldsymbol{p}, b) \subseteq \mathcal{H}.$$

Proof. Applying Noether's normalization lemma to $\mathcal{B}_0$, we find $\boldsymbol{\eta} = (\eta_1, \ldots, \eta_\ell, \ldots, \eta_m) \in \mathcal{B}_0^m$ with $\mathcal{B}_0 = k_0[\boldsymbol{\eta}]$ such that $\eta_1, \ldots, \eta_\ell$ are algebraically independent over k_0 and $\eta_{\ell+1}, \ldots, \eta_m$ are integral over $k_0[\eta_1, \ldots, \eta_\ell]$. Note that $\eta_1, \ldots, \eta_\ell$ are also algebraically independent over k and $\eta_{\ell+1}, \ldots, \eta_m$ are integral over $k[\eta_1, \ldots, \eta_\ell]$. Moreover, for $i = 1, \ldots, m - \ell$, the minimal polynomial of $\eta_{\ell+i}$ over $k(\eta_1, \ldots, \eta_\ell)$ has coefficients in $k_0[\eta_1, \ldots, \eta_\ell]$.

By Corollary 2.13, there exist monic polynomials $p_1, \ldots, p_n \in \mathcal{B}_0[y]$ irreducible in $k_0(\mathcal{B}_0)[y]$ and a $b \in \mathcal{B}_0 \smallsetminus \{0\}$ such that $H_{\mathcal{B}_0}(p_1, \ldots, p_n) \cap D(b) \subseteq H$. With $\boldsymbol{p} = (p_1, \ldots, p_n)$ we thus have $\mathcal{H}^{\boldsymbol{\eta}}_{k_0, \mathcal{X}(k)}((1, \ldots, 1), \boldsymbol{p}, b) \subseteq \mathcal{H}$. □

The following proposition, going back to [Hru02], explains why the sets of the form $\mathcal{H}_{k_0,\mathcal{X}(k)}^{\boldsymbol{\eta}}(\boldsymbol{d},\boldsymbol{p},b)$ are useful for us. We assume that k_0 and $\boldsymbol{\eta}$ are as described after Corollary 2.13.

Proposition 2.15. *Let Γ be a finitely generated subgroup of $(k_0[\boldsymbol{\eta}],+)$. Then there exists a $\boldsymbol{d}$ such that $\mathcal{H}_{k_0,\mathcal{X}(k)}^{\boldsymbol{\eta}}(\boldsymbol{d},\emptyset,1) \subseteq W_{\mathcal{X}}(\mathbb{G}_a,\Gamma)$.*

Proof. This is really just a restatement of [Fen21, Prop. 2.10]. □

2.3 Néron's specialization theorem

Néron's specialization theorem is a crucial ingredient in our proof that ad×Jac-open sets are Zariski dense (Theorem 2.24). Roughly speaking, Néron's specialization theorem states that in an algebraic family of abelian varieties, the specialization map defined by a point of the parameter space is injective for all points in a Hilbert subset of the parameter space. This theorem can be used to construct abelian varieties with groups of rational points of large rank. Several versions of Néron's specialization theorem are available in the literature. The original reference is [Nér52]. Other presentations are in [Ser97b, Section 11.1], [Lan83, Chapter 9, Section 6] and [Pet06, Section 3]. Unfortunately, none of these versions seems to directly yield the result we need. We therefore include a self-contained proof of our variant of Néron's specialization theorem, mostly following [Ser97b] in the argument (cf. [Fen21, Section 2]).

Throughout Section 2.3 we make the following assumptions:

- k_0 is a field of characteristic zero;

- $\mathcal{X}_0 = \mathrm{Spec}(\mathcal{B}_0)$ is an affine variety over k_0 (i.e., a geometrically integral affine scheme of finite type over k_0);

- $K_0 = k_0(\mathcal{B}_0)$ is the function field of $\mathcal{X}_0$, i.e., the field of fractions of $\mathcal{B}_0$;

- $\mathcal{B}_0' \subseteq \overline{K_0}$ is a finitely generated $\mathcal{B}_0$-algebra;

- $\mathcal{X}_0' = \mathrm{Spec}(\mathcal{B}_0')$;

- $\mathcal{E}_0$ is a commutative separated group scheme of finite type over $\mathcal{B}_0$ such that $\mathcal{E}_0 \times_{\mathcal{X}_0} \mathrm{Spec}(K_0)$ is connected.

We also make the following assumption on $\mathcal{E}_0$.

(A) For every finitely generated subgroup Γ of $\mathcal{E}_0(K_0)$, the group

$$\{\varepsilon \in \mathcal{E}_0(K_0) \mid \varepsilon^n \in \Gamma \text{ for some } n \geq 1\}$$

is also finitely generated.

We will need a few lemmas of a preparatory nature.

Lemma 2.16. *Let G be a connected commutative algebraic group over k_0 and let $n \geq 1$ be an integer. Then the morphism $[n]\colon G \to G$, $g \mapsto g^n$ has finite kernel and $[n]\colon G(\overline{k_0}) \to G(\overline{k_0})$ is surjective.*

Proof. Note that $[n]$ is a morphism of algebraic groups because G is commutative. The induced morphism $\mathrm{Lie}([n])\colon \mathrm{Lie}(G) \to \mathrm{Lie}(G)$ on the Lie algebra of G is multiplication by n. As we are in characteristic zero, this implies that $\mathrm{Lie}([n])$ is an isomorphism. In particular, $\mathrm{Lie}(\ker([n])) = \ker(\mathrm{Lie}([n])) = 0$. Thus $\ker([n])$ is finite. Then, for dimension reasons, the image of $[n]\colon G(\overline{k_0}) \to G(\overline{k_0})$ must have the same dimension as G. As the image is closed and G is connected, it follows that $[n]\colon G(\overline{k_0}) \to G(\overline{k_0})$ is surjective. $\square$

For every $x' \in \mathcal{X}_0'$ we have a specialization morphism

$$\sigma_{x'}\colon \mathcal{E}_0(\mathcal{B}_0') \to \mathcal{E}_0(k_0(x')),$$

obtained by applying $\mathcal{E}_0$, considered as a functor on the category of $\mathcal{B}_0$-algebras, to the morphism $\mathcal{B}_0' \to k_0(x')$.

Lemma 2.17. *Let $\gamma \in \mathcal{E}_0(\mathcal{B}_0')$ and $n \geq 1$. Then the set $\{\varepsilon \in \mathcal{E}_0(\overline{K_0}) \mid \varepsilon^n = \gamma\}$ is finite and nonempty and there exist a nonempty Zariski open subset $\mathcal{U}'$ of $\mathcal{X}_0'$ such that*

$$|\{\varepsilon \in \mathcal{E}_0(\overline{k_0(x')}) \mid \varepsilon^n = \sigma_{x'}(\gamma)\}| = |\{\varepsilon \in \mathcal{E}_0(\overline{K_0}) \mid \varepsilon^n = \gamma\}|$$

for every $x' \in \mathcal{U}'$.

Proof. The set $\{\varepsilon \in \mathcal{E}_0(\overline{K_0}) \mid \varepsilon^n = \gamma\}$ is finite and nonempty by Lemma 2.16. Set $\mathcal{E}_0' = \mathcal{E}_{0,\mathcal{B}_0'}$ and consider the morphism $[n]\colon \mathcal{E}_0' \to \mathcal{E}_0'$, $g \mapsto g^n$ and its kernel $\ker([n]) \leq \mathcal{E}_0'$. Then $\ker([n])_{x'}$ is the kernel of the n-th power map on $\mathcal{E}_{0,x'}'$ for every $x' \in \mathcal{X}_0'$.

It follows from Lemma 2.16 that $\ker([n])_{\xi'}$ is finite, where ξ' is the generic point of $\mathcal{X}_0'$. Being finite spreads out from the generic fibre and also the number of geometric points is constant over a nonempty Zariski open subset ([Gro66, Cor. 9.7.9]). Thus, there exists a nonempty Zariski open subset $\mathcal{U}'$ of $\mathcal{X}_0'$ such that

$$|\{\varepsilon \in \mathcal{E}_{0,x'}'(\overline{k_0(x')}) \mid \varepsilon^n = 1\}| = |\{\varepsilon \in \mathcal{E}_{0,\xi'}'(\overline{K_0}) \mid \varepsilon^n = 1\}|$$

for all $x' \in \mathcal{U}'$. Shrinking $\mathcal{U}'$ if necessary, we can also assume that $\mathcal{E}_{0,x'}'$ is connected for all $x' \in \mathcal{U}'$. (Recall that an algebraic group is connected if and only if it is geometrically connected). Using Lemma 2.16 we then find

$$|\{\varepsilon \in \mathcal{E}_0(\overline{k_0(x')}) \mid \varepsilon^n = \sigma_{x'}(\gamma)\}| = |\{\varepsilon \in \mathcal{E}_{0,x'}'(\overline{k_0(x')}) \mid \varepsilon^n = \sigma_{x'}(\gamma)\}| =$$
$$= |\{\varepsilon \in \mathcal{E}_{0,x'}'(\overline{k_0(x')}) \mid \varepsilon^n = 1\}| = |\{\varepsilon \in \mathcal{E}_{0,\xi'}'(\overline{K_0}) \mid \varepsilon^n = 1\}| =$$
$$= |\{\varepsilon \in \mathcal{E}_0(\overline{K_0}) \mid \varepsilon^n = \gamma\}|$$

for all $x' \in \mathcal{U}'$. $\square$

Lemma 2.18. *Let $\mathcal{S}$ be a scheme of finite type over $\mathcal{B}_0$ and let $s \in \mathcal{S}(\mathcal{B}_0')$ be such that $k_0(s(\xi')) \to k_0(\xi') = k_0(\mathcal{B}_0')$ is an isomorphism, where ξ' is the generic point of $\mathcal{X}_0'$ and we think of s as a morphism $s\colon \mathcal{X}_0' \to \mathcal{S}$. Then there exists a nonempty Zariski open subset $\mathcal{U}'$ of $\mathcal{X}_0'$ such that the morphism $k_0(s(x')) \to k_0(x')$ induced by s is an isomorphism for every $x' \in \mathcal{U}'$.*

Proof. Let $\mathcal{U}$ be an affine open subset of $\mathcal{S}$ containing $s(\xi')$ and let $D(b')$ be a basic Zariski open subset of $\mathcal{X}_0'$ contained in $s^{-1}(\mathcal{U})$. Then the restriction $\tilde{s}\colon D(b') \to \mathcal{U}$ of $s\colon \mathcal{X}_0' \to \mathcal{S}$ satisfies the assumption of the lemma, i.e., the induced map $k_0(\tilde{s}(\xi')) \to k_0(\xi')$ is an isomorphism. We can thus assume without loss of generality that $\mathcal{S}$ is affine.

17

So we can identify $\mathcal{S}$ with the spectrum of a finitely generated $\mathcal{B}_0$-algebra $\mathcal{R}$. The point $s \in \mathcal{S}(\mathcal{B}'_0)$ corresponds to a morphism $\psi \colon \mathcal{R} \to \mathcal{B}'_0$ of $\mathcal{B}_0$-algebras. The assumption that $k_0(s(\xi')) \to k_0(\xi')$ is an isomorphism, means that the field of fractions of $\psi(\mathcal{R})$ (formed inside $k_0(\mathcal{B}'_0)$) equals all of $k_0(\mathcal{B}'_0)$.

Fix $b'_1, \ldots, b'_n \in \mathcal{B}'_0$ such that $\mathcal{B}'_0 = \mathcal{B}_0[b'_1, \ldots, b'_n]$. For $i = 1, \ldots, n$ we can then write $b'_i = \frac{\psi(r_i)}{\psi(\widetilde{r_i})}$ with $r_1, \ldots, r_n, \widetilde{r_1}, \ldots, \widetilde{r_n} \in \mathcal{R}$ and $\psi(\widetilde{r_1}), \ldots, \psi(\widetilde{r_m}) \in \mathcal{B}'_0$ nonzero. We claim that $\mathcal{U}' = D(\psi(\widetilde{r_1}) \ldots \psi(\widetilde{r_n})) \subseteq \mathcal{X}'_0$ has the desired property.

Let $x' \in \mathcal{U}'$ correspond to the prime ideal $\mathfrak{p}'$ of $\mathcal{B}'_0$. For $b' \in \mathcal{B}'_0$ let $\overline{b'} \in \mathcal{B}'_0/\mathfrak{p}' \subseteq k_0(\mathcal{B}'_0/\mathfrak{p}') = k_0(x')$ denote the image of b' in $\mathcal{B}'_0/\mathfrak{p}'$. As $\psi(\widetilde{r_i})b'_i = \psi(r_i)$ in $\mathcal{B}'_0$, we have $\overline{\psi(\widetilde{r_i})b'_i} = \overline{\psi(r_i)}$ for $i = 1, \ldots, n$. As $x' \in \mathcal{U}'$, we can divide by $\overline{\psi(\widetilde{r_i})}$ in $k_0(x')$ to obtain $\overline{b'_i} = \frac{\overline{\psi(r_i)}}{\overline{\psi(\widetilde{r_i})}}$ in $k_0(x')$. Note that the morphism $k_0(s(x')) \to k_0(x')$ is obtained from the injection $\mathcal{R}/\psi^{-1}(\mathfrak{p}') \to \mathcal{B}'_0/\mathfrak{p}'$ by passing to the field of fractions. In particular, $k_0(s(x')) \to k_0(x')$ is an isomorphism if and only if the field of fractions of $\overline{\psi(\mathcal{R})} \subseteq \mathcal{B}'_0/\mathfrak{p}' \subseteq k_0(\mathcal{B}'_0/\mathfrak{p}')$ equals all of $k_0(\mathcal{B}'_0/\mathfrak{p}')$. As $k_0(\mathcal{B}'_0/\mathfrak{p}') = k_0(\mathcal{B}_0)(\overline{b'_1}, \ldots, \overline{b'_n})$, the latter follows from $\overline{b'_i} = \frac{\overline{\psi(r_i)}}{\overline{\psi(\widetilde{r_i})}}$. $\qquad\square$

Lemma 2.19. *Let S be a finite subset of $\mathcal{E}_0(\mathcal{B}'_0)$. Then there exists a nonempty Zariski open subset $\mathcal{U}'$ of $\mathcal{X}'_0$ such that $\sigma_{x'}$ is injective on S for every $x' \in \mathcal{U}'$.*

Proof. It suffices to treat the case when S consists of two distinct elements s_1, s_2. As $\mathcal{E}_0 \to \mathcal{X}_0$ is separated, the equalizer $\mathcal{Z} \to \mathcal{X}'_0$ of $s_1, s_2 \colon \mathcal{X}'_0 \to \mathcal{E}_0$ (in the category of schemes over $\mathcal{X}_0$) is a closed subscheme of $\mathcal{X}'_0$ ([Sta24, Tag 01KM]). In particular, for a morphism $\phi \colon \widetilde{\mathcal{Z}} \to \mathcal{X}'_0$ of $\mathcal{X}_0$-schemes one has $s_1\phi = s_2\phi$ if and only if ϕ factors through the closed immersion $\mathcal{Z} \hookrightarrow \mathcal{X}'_0$.

We will show that $\mathcal{Z}$ defines a proper closed subset of $\mathcal{X}'_0$. Suppose, for a contradiction, that the underlying set of $\mathcal{Z}$ is all of $\mathcal{X}'_0$. Since $\mathcal{X}'_0$ is reduced, the only closed subscheme supported on all of $\mathcal{X}'_0$ is $\mathcal{X}'_0$ itself. So $\mathcal{Z} = \mathcal{X}'_0$ (as schemes). But then $s_1 = s_2$; a contradiction.

Thus $\mathcal{Z}$ defines a proper closed subset of $\mathcal{X}'_0$ and its complement $\mathcal{U}' \subseteq \mathcal{X}'_0$ is a nonempty Zariski open subset. For $x' \in \mathcal{U}'$, the morphism $\phi_{x'} \colon \mathrm{Spec}(k_0(x')) \to \mathcal{X}'_0$ does not factor through $\mathcal{Z} \to \mathcal{X}'_0$ and so $s\phi_{x'} \neq s'\phi_{x'}$, i.e., $\sigma_{x'}(s_1) \neq \sigma_{x'}(s_2)$. $\qquad\square$

The following lemma explains how Hilbert subsets enter into Néron's specialization theorem.

Lemma 2.20. *Let $n \geq 1$, $\tilde{\mathcal{B}} \subseteq K_0$ a finitely generated $\mathcal{B}_0$-algebra and $\gamma \in \mathcal{E}_0(\tilde{\mathcal{B}})$ such that $\{\varepsilon \in \mathcal{E}_0(K_0) \mid \varepsilon^n = \gamma\} \subseteq \mathcal{E}_0(\tilde{\mathcal{B}})$. Then there exists a Hilbert subset $\tilde{H}$ of $\tilde{\mathcal{X}} = \mathrm{Spec}(\tilde{\mathcal{B}})$ such that*

$$\{\varepsilon \in \mathcal{E}_0(k_0(\tilde{x})) \mid \varepsilon^n = \sigma_{\tilde{x}}(\gamma)\} = \sigma_{\tilde{x}}(\{\varepsilon \in \mathcal{E}_0(K_0) \mid \varepsilon^n = \gamma\}). \tag{4}$$

for all $\tilde{x} \in \tilde{H}$.

Proof. Note that the inclusion "$\supseteq$" in (4) is trivial. Set $S = \{\varepsilon \in \mathcal{E}_0(\overline{K_0}) \mid \varepsilon^n = \gamma\}$. Let $\mathcal{B}'_0 \subseteq \overline{K_0}$ be a finitely generated $\tilde{\mathcal{B}}$-algebra such that $S \subseteq \mathcal{E}_0(\mathcal{B}'_0)$. By Lemma 2.19 there exists a nonempty Zariski open subset $\mathcal{U}'$ of $\mathcal{X}'_0 = \mathrm{Spec}(\mathcal{B}'_0)$ such that $\sigma_{x'}$ is injective on S for all $x' \in \mathcal{U}'$. By Lemma 2.17, there exists a nonempty Zariski open subset $\mathcal{V}'$ of $\mathcal{X}'_0$ such that

$$|\{\varepsilon \in \mathcal{E}_0(\overline{k_0(x')}) \mid \varepsilon^n = \sigma_{x'}(\gamma)\}| = |S| \tag{5}$$

for all $x' \in \mathcal{V}'$. Let $\phi \colon \mathcal{X}'_0 \to \tilde{\mathcal{X}}$ be the morphism corresponding to the inclusion $\tilde{\mathcal{B}} \subseteq \mathcal{B}'_0$. Since $\mathcal{B}'_0$ is algebraic over $\tilde{\mathcal{B}}$, there exists a nonempty Zariski open subset $\mathcal{W}'$ of $\mathcal{X}'_0$ such

18

that $k_0(x')$ is algebraic over $k_0(\phi(x'))$ for all $x' \in \mathcal{W}'$. (This follows, for example, from Lemma 2.10.) By Chevalley's theorem, there exists a nonempty basic Zariski open subset $\tilde{\mathcal{U}}$ of $\tilde{\mathcal{X}}$ contained in $\phi(\mathcal{U}' \cap \mathcal{V}' \cap \mathcal{W}')$.

Let $\tilde{x} \in \tilde{\mathcal{U}}$. Then there exists an $x' \in \mathcal{U}' \cap \mathcal{V}' \cap \mathcal{W}'$ with $\phi(x') = \tilde{x}$. We claim that

$$\{\varepsilon \in \mathcal{E}_0(\overline{k_0(\tilde{x})}) \mid \varepsilon^n = \sigma_{\tilde{x}}(\gamma)\} = \sigma_{x'}(S). \tag{6}$$

As $\sigma_{x'}$ is injective on S, we find

$$|S| = |\sigma_{x'}(S)| \leq |\{\varepsilon \in \mathcal{E}_0(k_0(x')) \mid \varepsilon^n = \sigma_{x'}(\gamma)\}| \leq |\{\varepsilon \in \mathcal{E}_0(\overline{k_0(x')}) \mid \varepsilon^n = \sigma_{x'}(\gamma)\}|.$$

From (5), we thus deduce that $\sigma_{x'}(S) = \{\varepsilon \in \mathcal{E}_0(\overline{k_0(x')}) \mid \varepsilon^n = \sigma_{x'}(\gamma)\}$. This implies (6) because $\overline{k_0(x')} = \overline{k_0(\tilde{x})}$ since $k_0(x')$ is algebraic over $k_0(\tilde{x}) = k_0(\phi(x'))$.

We first assume that $S \subseteq \mathcal{E}_0(K_0)$. Then $S = \{\varepsilon \in \mathcal{E}_0(K_0) \mid \varepsilon^n = \gamma\} \subseteq \mathcal{E}_0(\tilde{\mathcal{B}})$ by assumption. The commutativity of

$$
\begin{array}{ccc}
\mathcal{E}_0(\tilde{\mathcal{B}}) & \lhook\joinrel\longrightarrow & \mathcal{E}_0(\mathcal{B}'_0) \\
\sigma_{\tilde{x}} \downarrow & & \downarrow \sigma_{x'} \\
\mathcal{E}_0(k_0(\tilde{x})) & \lhook\joinrel\longrightarrow & \mathcal{E}_0(k_0(x'))
\end{array}
$$

paired with (6) then yields $\sigma_{\tilde{x}}(S) = \{\varepsilon \in \mathcal{E}_0(\overline{k_0(\tilde{x})}) \mid \varepsilon^n = \sigma_{\tilde{x}}(\gamma)\}$. In particular, $\{\varepsilon \in \mathcal{E}_0(k_0(\tilde{x})) \mid \varepsilon^n = \sigma_{\tilde{x}}(\gamma)\} = \sigma_{\tilde{x}}(S)$ as desired. So, in case $S \subseteq \mathcal{E}_0(K_0)$, we can choose as $\tilde{H} = \tilde{\mathcal{U}}$.

Now assume that $S \setminus \mathcal{E}_0(K_0) \neq \emptyset$ and let $\varepsilon \in S \setminus \mathcal{E}_0(K_0)$. Then $k_0(\varepsilon(\bar{\xi})) \hookrightarrow \overline{K_0}$ is a finite extension of K_0 with $[k_0(\varepsilon(\bar{\xi})) : K_0] > 1$, where we think of ε as a morphism $\varepsilon \colon \mathrm{Spec}(\overline{K_0}) \to \mathcal{E}_0$ and $\bar{\xi}$ is the unique point of $\mathrm{Spec}(\overline{K_0})$. Let $\mathcal{B}_\varepsilon \subseteq k_0(\varepsilon(\bar{\xi}))$ be a finitely generated $\tilde{\mathcal{B}}$-algebra with $k_0(\varepsilon(\bar{\xi}))$ as field of fractions and such that $\varepsilon \in \mathcal{E}_0(\mathcal{B}_\varepsilon)$. Furthermore, we may assume $\mathcal{B}_\varepsilon \subseteq \mathcal{B}'_0$.

Then Lemma 2.18, applied with $\mathcal{S} = \mathcal{E}_0$, $\mathcal{B}'_0 = \mathcal{B}_\varepsilon$ and $s = \varepsilon \in \mathcal{E}_0(\mathcal{B}_\varepsilon)$, yields a nonempty Zariski open subset $\mathcal{V}_\varepsilon$ of $\mathrm{Spec}(\mathcal{B}_\varepsilon)$ such that $k_0(\varepsilon(x)) \to k_0(x)$ is an isomorphism for every $x \in \mathcal{V}_\varepsilon$. By Chevalley's theorem, there exists a nonempty basic Zariski open subset $\mathcal{U}_\varepsilon$ of $\tilde{\mathcal{X}} = \mathrm{Spec}(\tilde{\mathcal{B}})$ such that $\mathcal{U}_\varepsilon$ lies in the image of $\mathcal{V}_\varepsilon$ under $\mathrm{Spec}(\mathcal{B}_\varepsilon) \to \mathrm{Spec}(\tilde{\mathcal{B}})$.

Set $\tilde{H}_\varepsilon = \mathcal{U}_\varepsilon \cap H(\mathcal{B}_\varepsilon/\tilde{\mathcal{B}})$ and let $\tilde{x} \in \tilde{H}_\varepsilon$. Then $[k_0(x_\varepsilon) : k_0(\tilde{x})] = [k_0(\varepsilon(\bar{\xi})) : K_0] > 1$, where x_ε is the unique element of $\mathrm{Spec}(\mathcal{B}_\varepsilon)$ lying above $\tilde{x}$. As $x_\varepsilon \in \mathcal{V}_\varepsilon$, the field extensions $k_0(\varepsilon(x_\varepsilon))$ and $k_0(x_\varepsilon)$ of $k_0(\tilde{x})$ are isomorphic. Therefore, $k_0(\varepsilon(x_\varepsilon))$ is a non-trivial field extension of $k_0(\tilde{x})$.

We will show that $\tilde{H} = \tilde{\mathcal{U}} \cap (\cap_{\varepsilon \in S \setminus \mathcal{E}_0(K_0)} \tilde{H}_\varepsilon)$ has the desired property. Let $\tilde{x} \in \tilde{H}$. Then there exist an $x' \in \mathcal{U}' \cap \mathcal{V}' \cap \mathcal{W}' \subseteq \mathcal{X}'_0$ with $\phi(x') = \tilde{x}$. Given (6), to verify (4), it suffices to show that $\sigma_{x'}(\varepsilon) \notin \mathcal{E}_0(k_0(\tilde{x}))$ for every $\varepsilon \in S \setminus \mathcal{E}_0(K_0)$. Note that $\sigma_{x'}(\varepsilon) \notin \mathcal{E}_0(k_0(\tilde{x}))$ if and only if $k_0(\varepsilon(x'))$ is a non-trivial extension of $k_0(\tilde{x})$.

For $\varepsilon \in S \setminus \mathcal{E}_0(K_0)$, since x_ε is the unique element of $\mathrm{Spec}(\mathcal{B}_\varepsilon)$ lying above $\tilde{x}$ and $\mathcal{B}_\varepsilon \subseteq \mathcal{B}'_0$, we see that x_ε is the image of x' under $\mathrm{Spec}(\mathcal{B}'_0) \to \mathrm{Spec}(\mathcal{B}_\varepsilon)$. So $\varepsilon(x') = \varepsilon(x_\varepsilon)$ and $k_0(\varepsilon(x')) = k_0(\varepsilon(x_\varepsilon))$ is a non-trivial extension of $k_0(\tilde{x})$ as desired. □

We are now prepared to prove our variant of Néron's specialization theorem.

Theorem 2.21. *Let Γ be a finitely generated subgroup of $\mathcal{E}_0(\mathcal{B}_0)$. Then there exists a Hilbert subset H_0 of $\mathcal{X}_0$ such that $\sigma_{x_0} \colon \mathcal{E}_0(\mathcal{B}_0) \to \mathcal{E}_0(k_0(x_0))$ is injective on Γ for every $x_0 \in H_0$.*

Proof. Set $\tilde{\Gamma} = \{\varepsilon \in \mathcal{E}_0(K_0) \mid \varepsilon^n \in \Gamma \text{ for some } n \geq 1\}$. Then $\tilde{\Gamma}$ is a subgroup of $\mathcal{E}_0(K_0)$ and by assumption (A) it is finitely generated. Let $\tilde{\mathcal{B}} \subseteq K_0$ be a finitely generated $\mathcal{B}_0$-algebra such that $\tilde{\Gamma} \subseteq \mathcal{E}_0(\tilde{\mathcal{B}})$. We shall show that there exists a Hilbert subset $\tilde{H}$ of $\tilde{\mathcal{X}} = \mathrm{Spec}(\tilde{\mathcal{B}})$ such that the specialization map $\sigma_{\tilde{x}} \colon \mathcal{E}_0(\tilde{\mathcal{B}}) \to \mathcal{E}(k_0(\tilde{x}))$ is injective on $\tilde{\Gamma}$ for every $\tilde{x} \in \tilde{H}$. Note that this implies the theorem since, by Lemma 2.11, there exists a Hilbert subset H_0 of $\mathcal{X}_0$ contained in the image of $\tilde{H}$ under $\tilde{\mathcal{X}} \to \mathcal{X}_0$ and if $\tilde{x} \in \tilde{H}$ maps to $x_0 \in H_0$, then the diagram

$$
\begin{array}{ccc}
\mathcal{E}_0(\mathcal{B}) & \hookrightarrow & \mathcal{E}_0(\tilde{\mathcal{B}}) \\
\sigma_{x_0} \downarrow & & \downarrow \sigma_{\tilde{x}} \\
\mathcal{E}_0(k_0(x_0)) & \hookrightarrow & \mathcal{E}_0(k_0(\tilde{x}))
\end{array}
$$

commutes.

Let $n > 1$ be an integer such that the order of the torsion subgroup of $\tilde{\Gamma}$ divides n. Let $\{\gamma_1, \ldots, \gamma_m\}$ be a set of representatives of $\tilde{\Gamma}/\tilde{\Gamma}^n$. Without loss of generality we may assume that $\gamma_1 = 1$. For $i = 1, \ldots, m$ set $\Delta_i = \{\varepsilon \in \tilde{\Gamma} \mid \varepsilon^n = \gamma_i\}$. Note that $\Delta_i = \{\varepsilon \in \mathcal{E}_0(K_0) \mid \varepsilon^n = \gamma_i\}$ by construction of $\tilde{\Gamma}$.

Lemma 2.20 applied with $\gamma = \gamma_i$, yields a Hilbert subset $\tilde{H}_i$ of $\tilde{\mathcal{X}}$ such that

$$
\{\varepsilon \in \mathcal{E}_0(k_0(\tilde{x})) \mid \varepsilon^n = \sigma_{\tilde{x}}(\gamma_i)\} = \sigma_{\tilde{x}}(\Delta_i)
$$

for every $\tilde{x} \in \tilde{H}_i$. Set $\tilde{H} = \cap_{i=1}^m \tilde{H}_i$ and let $\tilde{x} \in \tilde{H}$. We will show that $\sigma_{\tilde{x}}$ is injective on $\tilde{\Gamma}$. It suffices to show that $\Gamma_0 = \ker(\sigma_{\tilde{x}}) \cap \tilde{\Gamma}$ is trivial. Note that Γ_0 is a finitely generated group because it is a subgroup of the finitely generated group $\tilde{\Gamma}$.

We claim that $\Gamma_0 = \Gamma_0^n$. Let $\gamma \in \Gamma_0$ and write $\gamma = \gamma_i \tilde{\gamma}^n$ for some i and $\tilde{\gamma} \in \tilde{\Gamma}$. Then $1 = \sigma_{\tilde{x}}(\gamma) = \sigma_{\tilde{x}}(\gamma_i)\sigma_{\tilde{x}}(\tilde{\gamma})^n$ and so $\sigma_{\tilde{x}}(\tilde{\gamma}^{-1})^n = \sigma_{\tilde{x}}(\gamma_i)$. Because $\tilde{x} \in \tilde{H}_i$, we have $\sigma_{\tilde{x}}(\tilde{\gamma}^{-1}) = \sigma_{\tilde{x}}(\varepsilon)$ for some $\varepsilon \in \Delta_i$, i.e., $\varepsilon^n = \gamma_i$. This implies that $\gamma_i = 1$, i.e., $i = 1$.

Hence $\sigma_{\tilde{x}}(\tilde{\gamma}^{-1}) = \sigma_{\tilde{x}}(\varepsilon)$ for $\varepsilon \in \tilde{\Gamma}$ and $\varepsilon^n = 1$. So $\sigma_{\tilde{x}}(\varepsilon\tilde{\gamma}) = 1$ and $\varepsilon\tilde{\gamma} \in \Gamma_0$. Moreover,

$$
\gamma = \gamma_i \tilde{\gamma}^n = \tilde{\gamma}^n = \varepsilon^n \tilde{\gamma}^n = (\varepsilon\tilde{\gamma})^n \in \Gamma_0^n.
$$

Thus $\Gamma_0 = \Gamma_0^n$ as claimed. As the order of the torsion subgroup of $\tilde{\Gamma}$ divides n, the group $\tilde{\Gamma}^n$ is torsion free. Therefore, also $\Gamma_0 = \Gamma_0^n \subseteq \tilde{\Gamma}^n$ is torsion free. But a finitely generated torsion-free group is a free $\mathbb{Z}$-module and so can satisfy $\Gamma_0^n = \Gamma_0$ only if $\Gamma_0 = 1$ is trivial. Thus $\Gamma_0 = 1$ and $\sigma_{\tilde{x}}$ is injective on $\tilde{\Gamma}$ for every $\tilde{x} \in \tilde{\Gamma}$ as desired. $\qquad\square$

The following corollary contains the special case of Theorem 2.21 relevant for our purpose.

Corollary 2.22. *Let k_0 be a finitely generated field extension of $\mathbb{Q}$, $\mathcal{X}_0 = \mathrm{Spec}(\mathcal{B}_0)$ an affine variety over k_0 and $\mathcal{E}_0$ a group scheme over $\mathcal{B}_0$ of abelian type. Then there exists a Hilbert subset H_0 of $\mathcal{X}_0$ such that the specialization morphism $\sigma_{x_0} \colon \mathcal{E}_0(\mathcal{B}_0) \to \mathcal{E}_0(k_0(x_0))$ is injective for every $x_0 \in H_0$.*

Proof. Since K_0 is finitely generated over $\mathbb{Q}$, by the generalized Mordell-Weil theorem ([Lan83, Chapter 6, Thm. 1]) the group $\mathcal{E}_0(K_0)$ is finitely generated. Therefore, assumption (A) is satisfied and also $\Gamma = \mathcal{E}_0(\mathcal{B}_0) \leq \mathcal{E}_0(K_0)$ is finitely generated. Thus Theorem 2.21 applies. $\qquad\square$

In addition to the case of group schemes of abelian type explained in the above corollary, Theorem 2.21 also applies in the case where k_0 is a finitely generated field extension

of $\mathbb{Q}$ and $\mathcal{E}_0 = \mathbb{G}_{m,\mathcal{B}_0}$ is the multiplicative group scheme over $\mathcal{B}_0$. In this case assumption assumption (A) is verified by [Fen21, Prop. 2.12].

Theorem 2.21 does not apply to the additive group scheme $\mathbb{G}_{a,\mathcal{B}_0}$ over $\mathcal{B}_0$ because assumption (A) is violated. For example, for $\Gamma = (\mathbb{Z}, +)$, the group in (A) equals $(\mathbb{Q}, +)$.

2.4 Denseness of ad×Jac-open sets

In this section we combine the results of the previous sections to show that ad×Jac-open subsets are Zariski dense. The following proposition is an important step in this direction. It can be seen as a "geometric" version of Corollary 2.22.

Proposition 2.23. *Let $\mathcal{U}$ be an ab-open subset of $\mathcal{X}(k)$ and $S \subseteq \mathcal{B}$ a finite subset. Then there exists a geometric $\mathcal{B}_0/k_0$-Hilbert set $\mathcal{H} \subseteq \mathcal{X}(k)$ such that $S \subseteq \mathcal{B}_0$ and $\mathcal{H} \subseteq \mathcal{U}$. In particular, every ab-open subset of $\mathcal{X}(k)$ contains a geometric Hilbert set.*

Proof. The ab-open set $\mathcal{U}$ is of the form $\mathcal{U} = \phi(W_{\mathcal{X}'}(\mathcal{E}, \Gamma))$, where $\mathcal{X}' = \mathrm{Spec}(\mathcal{B}')$ with $\mathcal{B}'$ an integral domain containing $\mathcal{B}$, finitely generated and algebraic over $\mathcal{B}$, $\mathcal{E}$ is a group scheme of abelian type over $\mathcal{B}'$, Γ is a finitely generated subgroup of $\mathcal{E}(\mathcal{B}')$ and $\phi \colon \mathcal{X}'(k) \to \mathcal{X}(k)$ is the morphism induced by the inclusion $\mathcal{B} \subseteq \mathcal{B}'$. The idea of the proof is to descend the whole situation from k to a finitely generated field extension of $\mathbb{Q}$ so that we can apply Néron's specialization theorem. We claim that we can find

- a nonzero $b \in \mathcal{B}$ such that every $\mathfrak{p} \in D(b)$ lifts to a prime ideal of $\mathcal{B}'$;

- a subfield k_0 of k that is finitely generated over $\mathbb{Q}$;

- a finitely generated k_0-subalgebra $\mathcal{B}_0$ of $\mathcal{B}$ containing b and S such that the canonical map $\mathcal{B}_0 \otimes_{k_0} k \to \mathcal{B}$ is an isomorphism;

- a finitely generated k_0-subalgebra $\mathcal{B}_0'$ of $\mathcal{B}'$ containing $\mathcal{B}_0$ such that the canonical map $\mathcal{B}_0' \otimes_{k_0} k \to \mathcal{B}'$ is an isomorphism and such that $\mathcal{B}_0'$ is algebraic over $\mathcal{B}_0$;

- a group scheme $\mathcal{E}_0$ over $\mathcal{B}_0'$ of abelian type such that the base change from k_0 to k of $\mathcal{E}_0/\mathcal{B}_0'$ equals $\mathcal{E}/\mathcal{B}'$ and $\Gamma \subseteq \mathcal{E}_0(\mathcal{B}_0')$ (where we identify $\mathcal{E}_0(\mathcal{B}_0')$ with a subset of $\mathcal{E}(\mathcal{B}')$).

To see that we can find the above items we argue as follows. First, by Chevalley's theorem, we can find an appropriate $b \in \mathcal{B}$. Let $\gamma_1, \ldots, \gamma_n$ be a finite generating set of Γ. Writing $\mathcal{B}'$ as the directed union of all of its finitely generated $\mathbb{Z}$-algebras and considering the morphisms $\gamma_1 \colon \mathrm{Spec}(\mathcal{B}') \to \mathcal{E}, \ldots, \gamma_n \colon \mathrm{Spec}(\mathcal{B}') \to \mathcal{E}$ and the separated commutative group scheme $\mathcal{E}$ over $\mathcal{B}'$, we can combine Theorem 8.8.2 and Theorem 8.10.5 (v) of [Gro66], to obtain a finitely generated $\mathbb{Z}$-subalgebra $\tilde{\mathcal{B}}$ of $\mathcal{B}'$, a commutative separated group scheme $\tilde{\mathcal{E}}$ of finite type over $\tilde{\mathcal{B}}$ and morphisms $\tilde{\gamma}_i \colon \mathrm{Spec}(\tilde{\mathcal{B}}) \to \tilde{\mathcal{E}}$ ($i = 1, \ldots, n$) such that the base change of $\tilde{\mathcal{E}}$ from $\tilde{\mathcal{B}}$ to $\mathcal{B}'$ is $\mathcal{E}$ and the base change of $\tilde{\gamma}_i$ from $\tilde{\mathcal{B}}$ to $\mathcal{B}'$ is γ_i for $i = 1, \ldots, n$. So, if we identify $\tilde{\mathcal{E}}(\tilde{\mathcal{B}})$ with a subset of $\mathcal{E}(\mathcal{B}')$, then $\Gamma \subseteq \tilde{\mathcal{E}}(\tilde{\mathcal{B}})$.

Next, choose a finite generating set S' of $\mathcal{B}'$ as a k-algebra such that S' contains a finite generating set of $\tilde{\mathcal{B}}$ as a $\mathbb{Z}$-algebra. Then choose a finite generating set T of $\mathcal{B}$ as a k-algebra such that $b \in T$, $S \subseteq T$ and all elements of S' satisfy a nonzero univariate (not necessarily monic) polynomial over $\mathbb{Z}[T]$. Set $T' = S' \cup T$. Then $T \subseteq T'$, T generates $\mathcal{B}$ as a k-algebra, T' generates $\mathcal{B}'$ as a k-algebra and every element of T' is algebraic over $\mathbb{Z}[T]$. Next, let $k_0 \subseteq k$ be a finitely generated field extension of $\mathbb{Q}$ such that the ideal of

all k-algebraic relations among the elements of T as well as the ideal of all k-algebraic relations among the elements of T' is generated by polynomials with coefficients in k_0. Set $\mathcal{B}_0 = k_0[T]$ and $\mathcal{B}'_0 = k_0[T']$. Then $\mathcal{B}_0 \subseteq \mathcal{B}'_0$ and $\mathcal{B}'_0$ is finitely generated and algebraic over $\mathcal{B}_0$. Moreover, $b \in \mathcal{B}_0$, $S \subseteq \mathcal{B}_0$, $\tilde{\mathcal{B}} \subseteq \mathcal{B}'_0$ and the morphisms $\mathcal{B}_0 \otimes_{k_0} k \to \mathcal{B}$ and $\mathcal{B}'_0 \otimes_{k_0} k \to \mathcal{B}'$ are isomorphism.

Let $\mathcal{E}_0$ be the base change of $\tilde{\mathcal{E}}$ from $\tilde{\mathcal{B}}$ to $\mathcal{B}'_0$. Then $\mathcal{E}_0$ is a commutative separated group scheme of finite type over $\mathcal{B}'_0$ with $\Gamma \subseteq \mathcal{E}_0(\mathcal{B}'_0)$ and the base change of $\mathcal{E}_0$ from $\mathcal{B}'_0$ to $\mathcal{B}'$ is $\mathcal{E}$. It follows that the base change of $\mathcal{E}_0 \times_{\mathrm{Spec}(\mathcal{B}'_0)} \mathrm{Spec}(k_0(\mathcal{B}'_0))$ from $k_0(\mathcal{B}'_0))$ to $k(\mathcal{B}')$ is $\mathcal{E} \times_{\mathrm{Spec}(\mathcal{B}')} k(\mathcal{B}')$. Since the latter is an abelian variety, also $\mathcal{E}_0 \times_{\mathrm{Spec}(\mathcal{B}'_0)} \mathrm{Spec}(k_0(\mathcal{B}'_0))$ must be an abelian variety. So $\mathcal{E}_0$ is of abelian type. In summary, we have successfully descended everything to k_0: The base change of $\mathcal{B}'_0/\mathcal{B}_0$ from k_0 to k is $\mathcal{B}'/\mathcal{B}$ and the base change of $\mathcal{E}_0/\mathcal{B}'_0$ from k_0 to k is $\mathcal{E}/\mathcal{B}'$.

Set $\mathcal{X}_0 = \mathrm{Spec}(\mathcal{B}_0)$ and $\mathcal{X}'_0 = \mathrm{Spec}(\mathcal{B}'_0)$ so that $\mathcal{E} \to \mathcal{X}' \to \mathcal{X}$ is the base change from k_0 to k of $\mathcal{E}_0 \to \mathcal{X}'_0 \to \mathcal{X}_0$.

By Neron's specialization theorem (Corollary 2.22), there exists a Hilbert subset H'_0 of $\mathcal{X}'_0$ such that the specialization map $\sigma_{x'_0} \colon \mathcal{E}_0(\mathcal{B}'_0) \to \mathcal{E}_0(k_0(x'_0))$ is injective for every $x'_0 \in H'_0$. By Lemma 2.11 there exists a Hilbert subset H_0 of $\mathcal{X}_0$ such that the image of H'_0 in $\mathcal{X}_0$ contains H_0 and every element of H_0 has a unique lift to an element of $\mathcal{X}'_0$. Let $\mathcal{H}$ be the inverse image of $H_0 \cap D(b)$ under $\mathcal{X}(k) \to \mathcal{X} \to \mathcal{X}_0$. Then $\mathcal{H}$ is a geometric $\mathcal{B}_0/k_0$-Hilbert set.

We claim that the geometric Hilbert set $\mathcal{H}$ is contained in $\mathcal{U}$. Let $c \in \mathcal{H}$ and let x, x_0 denote the image of c in $\mathcal{X}, \mathcal{X}_0$ respectively. By construction of H_0, there exists an $x'_0 \in H'_0$ mapping to x_0. On the other hand, if $\mathfrak{p}$ is the prime ideal of $\mathcal{B}$ corresponding to x, then $b \notin \mathfrak{p}$ and so x lifts to a point x' of $\mathcal{X}'$ by the choice of b. The commutative diagram

$$\begin{array}{ccc} \mathcal{X}' & \longrightarrow & \mathcal{X} \\ \downarrow & & \downarrow \\ \mathcal{X}'_0 & \longrightarrow & \mathcal{X}_0 \end{array}$$

then shows that the image of x' in $\mathcal{X}'_0$ equals x'_0 because x'_0 is the unique lift of x_0 to an element of $\mathcal{X}'_0$. We then have a commutative diagram

$$\begin{array}{ccc} \mathcal{E}_0(\mathcal{B}'_0) & \longrightarrow & \mathcal{E}(\mathcal{B}') \\ \sigma_{x'_0} \downarrow & & \downarrow \sigma_{x'} \\ \mathcal{E}_0(k_0(x'_0)) & \longrightarrow & \mathcal{E}(k(x')) \end{array}$$

where the horizontal maps are injections. As $\sigma_{x'_0}$ is injective, it is in particular injective on Γ. Thus also $\sigma_{x'} = \sigma_c$ is injective on Γ. So $c \in W_{\mathcal{X}'}(\mathcal{E}, \Gamma) = \mathcal{U}$ as desired. $\qquad\square$

We are now prepared to prove the main theorem of Section 2.

Theorem 2.24. *The intersection of an ad-open and an ab-open subset of $\mathcal{X}(k)$ is Zariski dense in $\mathcal{X}(k)$. In particular, an ad×Jac-open subset of $\mathcal{X}(k)$ is Zariski dense in $\mathcal{X}(k)$.*

Proof. Let $\mathcal{U} = W_{\mathcal{X}}(\mathbb{G}_a, \Gamma)$ be an ad-open subset of $\mathcal{X}(k)$ and let $\mathcal{V}$ be an ab-open subset of $\mathcal{X}(k)$. We first show that $\mathcal{U} \cap \mathcal{V}$ is nonempty.

Choose a finite generating set $S \subseteq \mathcal{B}$ of the finitely generated subgroup Γ of $(\mathcal{B}, +)$. By Proposition 2.23 there exists a geometric $\mathcal{B}_0/k_0$-Hilbert set $\mathcal{H}$ of $\mathcal{X}(k)$ with $S \subseteq \mathcal{B}_0$

22

and $\mathcal{H} \subseteq \mathcal{V}$. Now Lemma 2.14 yields an $\boldsymbol{\eta} \in \mathcal{B}_0^m$ with $\mathcal{B}_0 = k_0[\boldsymbol{\eta}]$ and appropriate $\boldsymbol{p}$, b such that $\mathcal{H}_{k_0,\mathcal{X}(k)}^{\boldsymbol{\eta}}((1,\ldots,1),\boldsymbol{p},b) \subseteq \mathcal{H}$. In particular, $\mathcal{H}_{k_0,\mathcal{X}(k)}^{\boldsymbol{\eta}}((1,\ldots,1),\boldsymbol{p},b) \subseteq \mathcal{V}$.

On the other hand, $\Gamma \subseteq \mathcal{B}_0$ as $S \subseteq \mathcal{B}_0$ and so by Proposition 2.15, there exists a $\boldsymbol{d}$ such that $\mathcal{H}_{k_0,\mathcal{X}(k)}^{\boldsymbol{\eta}}(\boldsymbol{d},\emptyset,1) \subseteq \mathcal{U}$. Thus

$$\mathcal{H}_{k_0,\mathcal{X}(k)}^{\boldsymbol{\eta}}(\boldsymbol{d},\boldsymbol{p},b) = \mathcal{H}_{k_0,\mathcal{X}(k)}^{\boldsymbol{\eta}}(\boldsymbol{d},\emptyset,1) \cap \mathcal{H}_{k_0,\mathcal{X}(k)}^{\boldsymbol{\eta}}((1,\ldots,1),\boldsymbol{p},b) \subseteq \mathcal{U} \cap \mathcal{V}.$$

Since $\mathcal{H}_{k_0,\mathcal{X}(k)}^{\boldsymbol{\eta}}(\boldsymbol{d},\boldsymbol{p},b) \neq \emptyset$ by [Fen21, Prop. 2.8], we can conclude that $\mathcal{U} \cap \mathcal{V} \neq \emptyset$.

We next show that $\mathcal{U} \cap \mathcal{V}$ is Zariski dense in $\mathcal{X}(k)$. Suppose, for a contradiction, that $\mathcal{U} \cap \mathcal{V}$ is not Zariski dense. Then there exists a nonempty Zariski open subset $\mathcal{U}'$ of $\mathcal{X}(k)$ such that $\mathcal{U}' \cap \mathcal{U} \cap \mathcal{V} = \emptyset$. So, if $\mathcal{U}''$ is any ad-open subset of $\mathcal{X}(k)$ contained in $\mathcal{U}' \cap \mathcal{U}$, then $\mathcal{U}'' \cap \mathcal{V} = \emptyset$. This contradicts the first part of the proof. $\square$

We can do slightly better:

Remark 2.25. *The intersection of finitely many ad-open and finitely many ab-open subsets of $\mathcal{X}(k)$ is Zariski dense in $\mathcal{X}(k)$.*

Proof. The intersection of finitely many ad-open subsets contains an ad-open subset (Remark 2.3) and the intersection of finitely many ab-open subsets is an ab-open subset (argue as in (2)). Thus the remark follows from Theorem 2.24. $\square$

3 Some topics in differential Galois theory

This section is a collection of definitions, results and constructions from differential Galois theory, mostly related to the computation of the differential Galois group via Hrushovski's algorithm. In Section 4, in the course of the proof of our main specialization theorem (Theorem 4.26), we will then show that many of the properties and constructions discussed here are preserved on an ad×Jac-open subset of the parameter space.

Throughout Section 3 we assume that

- (F,δ) is a differential field with field of constants

- $k = F^\delta$ algebraically closed and of characteristic zero.

In the later subsections we will specialize to the case $(F,\delta) = (k(x),\frac{d}{dx})$ or F a finite field extension of $k(x)$. The reader is invited to recall our notational conventions from the end of the introduction.

3.1 Basics of differential Galois theory

We begin by recalling the basic definitions and results from the Galois theory of linear differential equations. Proofs and more background can be found in any of the introductory textbooks [Mag94], [vdPS03], [CH11], [Sau16].

Recall that a differential ring R is *δ-simple* if it is not the zero ring and the only δ-ideals of R are R and the zero ideal.

Definition 3.1. *A* Picard-Vessiot ring *for $\delta(y) = Ay$, $(A \in F^{n \times n})$ is a δ-simple F-δ-algebra R such that there exists a $Y \in \mathrm{GL}_n(R)$ with $\delta(Y) = AY$ and $R = F[Y, \frac{1}{\det(Y)}]$.*

For any given $A \in F^{n \times n}$, there exist a Picard-Vessiot ring R/F for $\delta(y) = Ay$ and it is unique up to an F-δ-isomorphism. Moreover, $R^\delta = k$. The *differential Galois group* $G = G(R/F)$ of R/F (or of $\delta(y) = Ay$) is the functor from the category of k-algebras to the category of groups given by $G(T) = \mathrm{Aut}(R \otimes_k T/F \otimes_k T)$, where T is considered as a constant differential ring. It is a linear algebraic group (over k). Its coordinate ring $k[G]$ can explicitly be described as $k[G] = (R \otimes_F R)^\delta = k[Z, \frac{1}{\det(Z)}]$, with $Z = Y^{-1} \otimes Y \in$ $\mathrm{GL}_n((R \otimes_K R)^\delta)$ and Y as in Definition 3.1. The canonical map

$$R \otimes_k k[G] \to R \otimes_F R$$

is an isomorphism and so we may make the identification $R \otimes_F R = R \otimes_k k[G]$. For a k-algebra T, any $g \in G(T)$, i.e., any $K \otimes_k T$-δ-isomorphism $g \colon R \otimes_k T \to R \otimes_k T$, is determined by $g(Y \otimes 1)$. Moreover, $g(Y \otimes 1) = Y \otimes [g]$ for a unique $[g] \in \mathrm{GL}_n(T)$. The assignment $g \mapsto [g]$ determines a morphism $G \to \mathrm{GL}_{n,k}$ of algebraic groups over k which is a closed embedding. The dual of this morphism is the map $k[\mathrm{GL}_n] = k[X, \frac{1}{\det(X)}] \to k[G]$, $X \mapsto Z$.

The (functorial) action of G on R/F is determined by the map $\rho \colon R \to R \otimes_k k[G]$, which, under the identification $R \otimes_F R = R \otimes_k k[G]$ corresponds to the inclusion into the second factor. Explicitly, we have $\rho(Y) = Y \otimes Z$. For $g \in G(T) = \mathrm{Hom}(k[G], T)$, the corresponding automorphism $g \colon R \otimes_k T \to R \otimes_k T$ is the T-linear extension of $R \xrightarrow{\rho} R \otimes_k k[G] \to R \otimes_k T$.

The following lemma shows that Picard-Vessiot rings and differential Galois group are well-behaved under extension of the constants. For a proof see, e.g. [BHHW21a, Lemma 5.2].

Lemma 3.2. *Let $k \subseteq k'$ be an inclusion of algebraically closed fields and let $R/k(x)$ be a Picard-Vessiot ring with differential Galois group G. Then $R \otimes_{k(x)} k'(x)/k'(x)$ is a Picard-Vessiot ring with differential Galois group $G_{k'}$.* $\qquad\square$

3.2 Differential torsors

Differential torsors were introduced in [BHHW18] for the purpose of solving differential embedding problems. To study the behaviour of Picard-Vessiot rings and differential embedding problems under specialization, we will need a version of differential torsors that works over an arbitrary base and not just a differential field, as in [BHHW18].

As in the introduction, consider an inclusion $k \subseteq k'$ of algebraically closed fields of characteristic zero and a differential equation $\delta(y) = Ay$ over $k'(x)$ with differential Galois group G and Picard-Vessiot ring $R/k'(x)$. To discuss specializations of G and R down to k one first needs to spread out G and R into families, i.e., we would like to have a finitely generated k-subalgebra $\mathcal{B}$ of k', an affine group scheme $\mathcal{G}$ and a differential ring $\mathcal{R}$ over $\mathcal{B}$ such that the base change from $\mathcal{B}$ to k' yields G and R. It is then natural to also ask for an action of $\mathcal{G}$ on $\mathcal{R}$ compatible with the action of G on R. Moreover, since R defines a G-torsor, also $\mathcal{R}$ should define a $\mathcal{G}$-torsor. This idea is formalized through the notion of differential torsor.

Let $\mathcal{B}$ be a k-algebra (considered as a constant δ-ring) and let $\mathcal{Q}$ be a $\mathcal{B}$-δ-algebra. The two most relevant cases for us are, firstly $\mathcal{B} = k$ and $\mathcal{Q} = k(x)$ and, secondly $\mathcal{Q} = \mathcal{B}[x]_f$, where $f \in \mathcal{B}[x]$ is a monic polynomial.

For a $\mathcal{Q}$-δ-algebra $\mathcal{R}$, we define $\underline{\mathrm{Aut}}(\mathcal{R}/\mathcal{Q})$ to be the functor from the category of $\mathcal{B}$-algebras to the category of groups given by $\underline{\mathrm{Aut}}(\mathcal{R}/\mathcal{Q})(\mathcal{T}) = \mathrm{Aut}(\mathcal{R} \otimes_{\mathcal{B}} \mathcal{T}/\mathcal{Q} \otimes_{\mathcal{B}} \mathcal{T})$ for

any $\mathcal{B}$-algebra $\mathcal{T}$. Here $\mathcal{T}$ is considered as a constant δ-ring and the automorphisms are understood to be differential automorphisms. An element g of $\underline{\mathrm{Aut}}(\mathcal{R}/\mathcal{Q})(\mathcal{T})$ is thus a $\mathcal{Q} \otimes_{\mathcal{B}} \mathcal{T}$-$\delta$-isomorphism $g \colon \mathcal{R} \otimes_{\mathcal{B}} \mathcal{T} \to \mathcal{R} \otimes_{\mathcal{B}} \mathcal{T}$. On morphisms $\underline{\mathrm{Aut}}(\mathcal{R}/\mathcal{Q})$ is given by base change.

Let $\mathcal{G}$ be an affine group scheme over $\mathcal{B}$. An *action of $\mathcal{G}$ on $\mathcal{R}/\mathcal{Q}$* is a morphism $\mathcal{G} \to \underline{\mathrm{Aut}}(\mathcal{R}/\mathcal{Q})$ of group functors. In particular, for a $\mathcal{B}$-algebra $\mathcal{T}$, every $g \in \mathcal{G}(\mathcal{T})$ defines a $\mathcal{Q} \otimes_{\mathcal{B}} \mathcal{T}$-$\delta$-automorphism $g \colon \mathcal{R} \otimes_{\mathcal{B}} \mathcal{T} \to \mathcal{R} \otimes_{\mathcal{B}} \mathcal{T}$.

Lemma 3.3. *To specify an action of $\mathcal{G}$ on $\mathcal{R}/\mathcal{Q}$ is equivalent to specifying a morphism $\rho \colon \mathcal{R} \to \mathcal{R} \otimes_{\mathcal{B}} \mathcal{B}[\mathcal{G}]$ of $\mathcal{Q}$-δ-algebras such that the diagrams*

$$
\begin{array}{ccc}
\mathcal{R} & \xrightarrow{\;\;\rho\;\;} & \mathcal{R} \otimes_{\mathcal{B}} \mathcal{B}[\mathcal{G}] \\
{\scriptstyle \rho}\downarrow & & \downarrow{\scriptstyle \rho \otimes \mathcal{B}[\mathcal{G}]} \\
\mathcal{R} \otimes_{\mathcal{B}} \mathcal{B}[\mathcal{G}] & \xrightarrow{\;\mathcal{R} \otimes \Delta\;} & \mathcal{R} \otimes_{\mathcal{B}} \mathcal{B}[\mathcal{G}] \otimes_{\mathcal{B}} \mathcal{B}[\mathcal{G}]
\end{array}
$$

and

$$
\begin{array}{ccc}
\mathcal{R} & \xrightarrow{\;\;\rho\;\;} & \mathcal{R} \otimes_{\mathcal{B}} \mathcal{B}[\mathcal{G}] \\
& {\scriptstyle \mathrm{id}}\searrow & \downarrow{\scriptstyle \mathrm{id} \cdot \varepsilon} \\
& & \mathcal{R}
\end{array}
$$

commute, where $\Delta \colon \mathcal{B}[\mathcal{G}] \to \mathcal{B}[\mathcal{G}] \otimes_{\mathcal{B}} \mathcal{B}[\mathcal{G}]$ is the comultiplication and $\varepsilon \colon \mathcal{B}[\mathcal{G}] \to \mathcal{B}$ the counit of the Hopf algebra $\mathcal{B}[\mathcal{G}]$ over $\mathcal{B}$.

Proof. As this is a fairly standard argument, we only sketch the proof. First assume that an action of $\mathcal{G}$ on $\mathcal{R}/\mathcal{Q}$ is given. For $\mathcal{T} = \mathcal{B}[\mathcal{G}]$ and $g = \mathrm{id} \in \mathcal{G}(\mathcal{T}) = \mathrm{Hom}(\mathcal{B}[\mathcal{G}], \mathcal{B}[\mathcal{G}])$ we thus have a $\mathcal{Q} \otimes_{\mathcal{B}} \mathcal{B}[\mathcal{G}]$-$\delta$-automorphism $g \colon \mathcal{R} \otimes_{\mathcal{B}} \mathcal{B}[\mathcal{G}] \to \mathcal{R} \otimes_{\mathcal{B}} \mathcal{B}[\mathcal{G}]$. Then we can define ρ as the composition $\rho \colon \mathcal{R} \to \mathcal{R} \otimes_{\mathcal{B}} \mathcal{B}[\mathcal{G}] \xrightarrow{g} \mathcal{R} \otimes_{\mathcal{B}} \mathcal{B}[\mathcal{G}]$.

Conversely, given ρ, we define an action of $\mathcal{G}$ on $\mathcal{R}/\mathcal{Q}$ as follows. For a $\mathcal{B}$-algebra $\mathcal{T}$ and $g \in \mathcal{G}(\mathcal{T}) = \mathrm{Hom}(\mathcal{B}[\mathcal{G}], \mathcal{T})$ we define $g \colon \mathcal{R} \otimes_{\mathcal{B}} \mathcal{T} \to \mathcal{R} \otimes_{\mathcal{B}} \mathcal{T}$ as the $\mathcal{T}$-linear extension of $\mathcal{R} \xrightarrow{\rho} \mathcal{R} \otimes_{\mathcal{B}} \mathcal{B}[\mathcal{G}] \xrightarrow{\mathcal{R} \otimes g} \mathcal{R} \otimes_{\mathcal{B}} \mathcal{T}$. The first diagram corresponds to the associativity of this action while the second diagram shows that the identity acts trivial. $\qquad\square$

As above, let $\mathcal{G}$ act on $\mathcal{R}/\mathcal{Q}$ and let $\rho \colon \mathcal{R} \to \mathcal{R} \otimes_{\mathcal{B}} \mathcal{B}[\mathcal{G}]$ denote the *coaction* (as in Lemma 3.3). We call $\mathcal{R}/\mathcal{Q}$ a *differential $\mathcal{G}$-torsor* if $\mathcal{R}$ is not the zero ring and the map $\mathcal{R} \otimes_{\mathcal{Q}} \mathcal{R} \to \mathcal{R} \otimes_{\mathcal{B}} \mathcal{B}[\mathcal{G}]$, $a \otimes b \mapsto (a \otimes 1) \cdot \rho(b)$ is an isomorphism. The geometric interpretation of this condition is the usual torsor condition, i.e., for $\mathcal{Z} = \mathrm{Spec}(\mathcal{R})$, the morphism

$$
\mathcal{Z} \times_{\mathcal{Q}} \mathcal{G}_{\mathcal{Q}} \to \mathcal{Z} \times_{\mathcal{Q}} \mathcal{Z}, \;\; (z, g) \mapsto (z, zg)
$$

of affine schemes over $\mathcal{Q}$ is an isomorphism.

Definition 3.4. *Let $\mathcal{A} \in \mathcal{Q}^{n \times n}$. A differential $\mathcal{G}$-torsor $\mathcal{R}/\mathcal{Q}$ is a* differential $\mathcal{G}$-torsor for $\delta(y) = \mathcal{A}y$ *if there exists a $\mathcal{Y} \in \mathrm{GL}_n(\mathcal{R})$ such that*

(i) $\delta(\mathcal{Y}) = \mathcal{A}\mathcal{Y}$,

(ii) $\mathcal{R} = \mathcal{Q}[\mathcal{Y}, \frac{1}{\det(\mathcal{Y})}]$ *and*

(iii) *for every $\mathcal{B}$-algebra $\mathcal{T}$ and every $g \in \mathcal{G}(\mathcal{T})$ there exists a $[g] \in \mathrm{GL}_n(\mathcal{T})$ such that $g(\mathcal{Y} \otimes 1) = (\mathcal{Y} \otimes 1)(1 \otimes [g])$.*

A matrix $\mathcal{Y} \in \mathrm{GL}_n(\mathcal{R})$ such that the above three conditions are satisfied is called a funda-mental matrix.

Assuming Definition 3.4, the assignment $g \mapsto [g]$ defines a morphism $\mathcal{G} \to \mathrm{GL}_{n,\mathcal{B}}$ of group schemes over $\mathcal{B}$.

Example 3.5. The most basic example of the above definitions is when $\mathcal{B} = k$, $\mathcal{Q} = F$ is a differential field with $F^\delta = k$ and $\mathcal{R} = R$ is a Picard-Vessiot ring over F for $\delta(y) = Ay$ $(A \in F^{n \times n})$ with differential Galois group $\mathcal{G} = G$. As explained in Section 3.1, G acts on R/F and R/F is a differential G-torsor for $\delta(y) = Ay$. Note that if $\mathcal{Y} = Y \in \mathrm{GL}_n(R)$ is such that $\delta(Y) = AY$ and $R = K[Y, \frac{1}{\det Y}]$, then condition (iii) of Definition 3.4 is automatically satisfied (because $(R \otimes_k T)^\delta = T$ for any k-algebra T).

In the following example we construct a differential torsor for the group scheme of 2×2 monomial matrices.

Example 3.6. Let $\mathcal{B} \subseteq \mathcal{Q} \subseteq \mathcal{Q}[\eta]$ be an inclusion of differential k-algebras such that $\mathcal{B}$ is constant and $\mathcal{Q}[\eta]$ is an integral domain. We assume that η has minimal polynomial $y^2 - a$ over the field of fractions of $\mathcal{Q}$, where a is some element of $\mathcal{Q}^\times$. We also fix $b \in \mathcal{Q}$. Let y_1, y_2 be indeterminates over $\mathcal{Q}[\eta]$ and define a derivation δ on $\mathcal{R} = \mathcal{Q}[\eta][y_1, y_2, y_1^{-1}, y_2^{-1}]$ by $\delta(y_1) = (b + \eta)y_1$, $\delta(y_2) = (b - \eta)y_2$. Set

$$\mathcal{Y} = \begin{pmatrix} y_1 & y_2 \\ \delta(y_1) & \delta(y_2) \end{pmatrix} = \begin{pmatrix} y_1 & y_2 \\ (b+\eta)y_1 & (b-\eta)y_2 \end{pmatrix}.$$

Then $\det(\mathcal{Y}) = -2\eta y_1 y_2$. Therefore $\mathcal{R} = \mathcal{Q}[\mathcal{Y}, \frac{1}{\det(\mathcal{Y})}]$. A direct computation shows that $\delta(\mathcal{Y}) = A\mathcal{Y}$, where

$$A = \begin{pmatrix} 0 & 1 \\ a + \delta(b) - b^2 - \frac{\delta(a)b}{2a} & 2b + \frac{\delta(a)}{2a} \end{pmatrix} \in \mathcal{Q}^{2 \times 2}.$$

We would like to describe $\mathcal{Z} = \mathrm{Spec}(\mathcal{R})$ explicitly as a closed subscheme of $\mathrm{GL}_{2,\mathcal{Q}}$. To this end, let $\mathcal{I}$ denote the kernel of the morphism $\mathcal{Q}[X, \frac{1}{\det(X)}] \to \mathcal{R}$, $X \mapsto \mathcal{Y}$. As $\mathcal{R}$ is an integral domain, $\mathcal{I}$ is a prime differential ideal of $\mathcal{Q}[X, \frac{1}{\det(X)}]$, where $\delta(X) = AX$. We have

$$(b + \eta)y_1 \cdot (b - \eta)y_2 = (b^2 - a)y_1 y_2 \quad \text{and} \quad (b + \eta)y_1 \cdot y_2 + (b - \eta)y_2 \cdot y_1 = 2by_1 y_2.$$

Therefore, the polynomials

$$p_1 = X_{21}X_{22} - (b^2 - a)X_{11}X_{12} \quad \text{and} \quad p_2 = X_{21}X_{12} + X_{22}X_{11} - 2bX_{11}X_{12}$$

lie in $\mathcal{I}$. We will show that $\mathcal{I} = (p_1, p_2)$. For this, it suffices to show that the induced map $\mathcal{Q}[X, \frac{1}{\det(X)}]/(p_1, p_2) \to \mathcal{R}$ is injective. Let z_1, z_2, z_1', z_2' denote the image in $\mathcal{Q}[X, \frac{1}{\det(X)}]/(p_1, p_2)$ of $X_{11}, X_{12}, X_{21}, X_{22}$ respectively. Then

$$z_1' z_2' = (b^2 - a)z_1 z_2, \tag{7}$$

and

$$z_1' z_2 + z_2' z_1 = 2bz_1 z_2. \tag{8}$$

Subtracting $2z_1'z_2$ from (8) yields $z_1z_2' - z_1'z_2 = 2z_2(bz_1 - z_1')$. Since $z_1z_2' - z_1'z_2$ is invertible, we see that also z_2 is invertible. Similarly, subtracting $2z_2'z_1$ from (8), we see that z_1 is invertible. So (8) can be rewritten as

$$\frac{z_1'}{z_1} + \frac{z_2'}{z_2} = 2b \tag{9}$$

whereas (7) becomes $\frac{z_1'}{z_1} \cdot \frac{z_2'}{z_2} = b^2 - a$. Plugging $\frac{z_2'}{z_2} = 2b - \frac{z_1'}{z_1}$ into the latter equation yields $(\frac{z_1'}{z_1} - b)^2 = a$. Set $\eta' = \frac{z_1'}{z_1} - b$. Then $\eta'^2 = a$, $z_1' = (b + \eta')z_1$ and from (9) we obtain $z_2' = (b - \eta')z_2$.

Set $\mathcal{S} = \mathcal{Q}[\eta', z_1, z_2, z_1^{-1}, z_2^{-1}]$. We claim that $\mathcal{S} = \mathcal{Q}[X, \frac{1}{\det(X)}]/(p_1, p_2)$. It suffices to show that z_1', z_2' and $\frac{1}{z_1z_2' - z_1'z_2}$ lie in $\mathcal{S}$. But $z_1' = (b + \eta')z_1 \in \mathcal{S}$, $z_2' = (b - \eta')z_2 \in \mathcal{S}$ and $z_1z_2' - z_1'z_2 = 2\eta'z_1z_2$. So $\frac{1}{z_1z_2' - z_1'z_2} \in \mathcal{S}$ and $\mathcal{S} = \mathcal{Q}[X, \frac{1}{\det(X)}]/(p_1, p_2)$ as claimed.

The map

$$\mathcal{Q}[\eta'][z_1, z_2, z_1^{-1}, z_2^{-1}] = \mathcal{Q}[X, \tfrac{1}{\det(X)}]/(p_1, p_2) \longrightarrow \mathcal{R} = \mathcal{Q}[\eta][y_1, y_2, y_1^{-1}, y_2^{-1}] \tag{10}$$

sends η' to η, z_1 to y_1 and z_2 to y_2. As $\eta'^2 = a$, the restriction $\mathcal{Q}[\eta'] \to \mathcal{Q}[\eta]$ is injective. But then, since y_1 and y_2 are algebraically independent over $\mathcal{Q}[\eta]$, the map (10) is injective. Thus $\mathcal{I} = (p_1, p_2)$ as claimed. In other words, $\mathcal{Z}$ is the closed subscheme of $\mathrm{GL}_{2, \mathcal{Q}}$ defined by p_1 and p_2.

Let $\mathcal{G}$ be the group scheme of monomial 2×2 matrices over $\mathcal{B}$, i.e.,

$$\mathcal{G}(\mathcal{T}) = \left\{ \begin{pmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{pmatrix} \in \mathrm{GL}_2(\mathcal{T}) \mid g_{11}g_{12} = g_{21}g_{22} = g_{11}g_{21} = g_{12}g_{22} = 0 \right\} \leq \mathrm{GL}_2(\mathcal{T}) \tag{11}$$

for any $\mathcal{B}$-algebra $\mathcal{T}$. In particular, if $\mathcal{T}$ is an integral domain then

$$\mathcal{G}(\mathcal{T}) = \left\{ \begin{pmatrix} s & 0 \\ 0 & t \end{pmatrix} \mid s, t \in \mathcal{T}^\times \right\} \cup \left\{ \begin{pmatrix} 0 & s \\ t & 0 \end{pmatrix} \mid s, t \in \mathcal{T}^\times \right\} \leq \mathrm{GL}_2(\mathcal{T}).$$

Note that the equations in (11) are redundant, in fact,

$$\mathcal{G}(\mathcal{T}) = \left\{ \begin{pmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{pmatrix} \in \mathrm{GL}_2(\mathcal{T}) \mid g_{11}g_{12} = g_{21}g_{22} = 0 \right\}$$

for any $\mathcal{B}$-algebra $\mathcal{T}$. For example, if $g_{11}g_{12} = g_{21}g_{22} = 0$, then $(g_{11}g_{22} - g_{12}g_{21})g_{11}g_{21} = 0$ and so also $g_{11}g_{21} = 0$ since $g_{11}g_{22} - g_{12}g_{21}$ is invertible.

We will define an action of $\mathcal{G}$ on $\mathcal{R}/\mathcal{Q}$. Roughly, the idea is that a diagonal matrix $\begin{pmatrix} s & 0 \\ 0 & t \end{pmatrix}$ acts by $y_1 \mapsto sy_1$, $y_2 \mapsto ty_2$ and fixing η, whereas the permutation matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ acts by interchanging y_1 with y_2 and η with $-\eta$. In general, for $\mathcal{T}$ a $\mathcal{B}$-algebra, $g = \begin{pmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{pmatrix} \in \mathcal{G}(\mathcal{T})$ acts on $\mathcal{R} \otimes_{\mathcal{B}} \mathcal{T}$ by $g(\mathcal{Y}) = \mathcal{Y} \otimes g$. To make sure that this is well-defined, we check that for any $\mathcal{Q}$-algebra $\mathcal{S}$, $Z = \begin{pmatrix} Z_{11} & Z_{12} \\ Z_{21} & Z_{22} \end{pmatrix} \in \mathcal{Z}(\mathcal{S})$ and $g = \begin{pmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{pmatrix} \in \mathcal{G}(\mathcal{S})$, we have $Zg = \begin{pmatrix} Z_{11}g_{11} + Z_{12}g_{21} & Z_{11}g_{12} + Z_{12}g_{22} \\ Z_{21}g_{11} + Z_{22}g_{21} & Z_{21}g_{12} + Z_{22}g_{22} \end{pmatrix} \in \mathcal{Z}(\mathcal{S})$. Using (11), we find

$$p_1(Zg) = (Z_{21}g_{11} + Z_{22}g_{21})(Z_{21}g_{12} + Z_{22}g_{22}) - (b^2 - a)(Z_{11}g_{11} + Z_{12}g_{21})(Z_{11}g_{12} + Z_{12}g_{22})$$

$$= Z_{21}Z_{22}g_{11}g_{22} + Z_{22}Z_{21}g_{21}g_{12} - (b^2 - a)(Z_{11}Z_{12}g_{11}g_{22} + Z_{12}Z_{11}g_{21}g_{12})$$

$$= p_1(Z)g_{11}g_{22} + p_1(Z)g_{21}g_{12} = 0$$

and

$$p_2(Zg) = (Z_{21}g_{11} + Z_{22}g_{21})(Z_{11}g_{12} + Z_{12}g_{22}) + (Z_{21}g_{12} + Z_{22}g_{22})(Z_{11}g_{11} + Z_{12}g_{21}) -$$
$$2b(Z_{11}g_{11} + Z_{12}g_{21})(Z_{11}g_{12} + Z_{12}g_{22})$$
$$= Z_{21}Z_{12}g_{11}g_{22} + Z_{22}Z_{11}g_{21}g_{12} + Z_{21}Z_{12}g_{12}g_{21} + Z_{22}Z_{11}g_{11}g_{22} -$$
$$2b(Z_{11}Z_{12}g_{11}g_{22} + Z_{12}Z_{11}g_{21}g_{12})$$
$$= p_2(Z)g_{11}g_{22} + p_2(Z)g_{21}g_{12} = 0.$$

To see that $\mathcal{R}/\mathcal{Q}$ is indeed a differential $\mathcal{G}$-torsor, it suffices to check that for $Z, Z' \in \mathcal{Z}(\mathcal{S})$, the matrix $Z^{-1}Z'$ lies in $\mathcal{G}(\mathcal{S})$. As

$$Z^{-1}Z' = \frac{1}{\det(Z)} \begin{pmatrix} Z_{22} & -Z_{12} \\ -Z_{21} & Z_{11} \end{pmatrix} \begin{pmatrix} Z'_{11} & Z'_{12} \\ Z'_{21} & Z'_{22} \end{pmatrix} = \frac{1}{\det(Z)} \begin{pmatrix} Z_{22}Z'_{11} - Z_{12}Z'_{21} & Z_{22}Z'_{12} - Z_{12}Z'_{22} \\ Z_{11}Z'_{21} - Z_{21}Z'_{11} & Z_{11}Z'_{22} - Z_{21}Z'_{12} \end{pmatrix},$$

it suffices to show that

$$(Z_{22}Z'_{11} - Z_{12}Z'_{21})(Z_{22}Z'_{12} - Z_{12}Z'_{22}) = 0 \tag{12}$$

and

$$(Z_{11}Z'_{21} - Z_{21}Z'_{11})(Z_{11}Z'_{22} - Z_{21}Z'_{12}) = 0. \tag{13}$$

To verify these identities, it is helpful to rewrite $p_1(Z) = 0$ and $p_2(Z) = 0$ as

$$\frac{Z_{21}}{Z_{11}} \cdot \frac{Z_{22}}{Z_{12}} = b^2 - a \quad \text{and} \quad \frac{Z_{21}}{Z_{11}} + \frac{Z_{22}}{Z_{12}} = 2b. \tag{14}$$

(Note that subtracting $2Z_{21}Z_{12}$ from $p_2(Z) = 0$ and using the invertibility of $\det(Z)$ shows that Z_{12} is invertible. By a similar argument, Z_{11} is invertible.) From (14) we deduce $(\frac{Z_{22}}{Z_{12}} - b)^2 = a$, which leads to

$$0 = (\tfrac{Z_{22}}{Z_{12}})^2 - 2b\tfrac{Z_{22}}{Z_{12}} + (b^2 - a) = (\tfrac{Z_{22}}{Z_{12}})^2 - \left(\tfrac{Z'_{21}}{Z'_{11}} + \tfrac{Z'_{22}}{Z'_{12}}\right)\tfrac{Z_{22}}{Z_{12}} - \tfrac{Z'_{21}}{Z'_{11}} \cdot \tfrac{Z'_{22}}{Z'_{12}} =$$
$$= \left(\tfrac{Z_{22}}{Z_{12}} - \tfrac{Z'_{21}}{Z'_{11}}\right)\left(\tfrac{Z_{22}}{Z_{12}} - \tfrac{Z'_{22}}{Z'_{12}}\right).$$

Clearing denominators, we find (12). A similar computation verifies (13). In summary, we see that $\mathcal{R}/\mathcal{Q}$ is a differential $\mathcal{G}$-torsor for $\delta(y) = \mathcal{A}y$ with fundamental matrix $\mathcal{Y}$.

In the next lemma we collect three basic observations that will be used repeatedly in what follows.

Lemma 3.7. *Let $\mathcal{G}$ act on $\mathcal{R}/\mathcal{Q}$.*

(i) *If $\mathcal{B} \to \mathcal{B}'$ is a morphism of k-algebras, then $\mathcal{G}_{\mathcal{B}'}$ acts on $\mathcal{R} \otimes_{\mathcal{B}} \mathcal{B}'/\mathcal{Q} \otimes_{\mathcal{B}} \mathcal{B}'$.*

(ii) *If $\mathcal{S}$ is a multiplicatively closed subset of $\mathcal{Q}$, then the action of $\mathcal{G}$ on $\mathcal{R}/\mathcal{Q}$ extends canonically to an action of $\mathcal{G}$ on $\mathcal{S}^{-1}\mathcal{R}/\mathcal{S}^{-1}\mathcal{Q}$.*

(iii) *If $\mathcal{Q} \to \mathcal{Q}'$ is a morphism of δ-rings, then $\mathcal{G}$ acts on $\mathcal{R} \otimes_{\mathcal{Q}} \mathcal{Q}'/\mathcal{Q}'$.*

Moreover, if $\mathcal{R}/\mathcal{Q}$ is a differential $\mathcal{G}$-torsor, then also the actions in (i), (ii) *and* (iii) *define differential torsors, provided that $\mathcal{R} \otimes_{\mathcal{B}} \mathcal{B}'$, $\mathcal{S}^{-1}\mathcal{R}$ and $\mathcal{R} \otimes_{\mathcal{Q}} \mathcal{Q}'$ respectively is not the zero ring.* $\square$

For later use we record a lemma on differential torsors in the case $\mathcal{B} = k$ and $\mathcal{Q} = k(x)$.

Lemma 3.8. *Let G be a linear algebraic group over k and let $R/k(x)$ be a differential G-torsor. Then the intersection of all maximal δ-ideals of R is zero.*

Proof. Let $\mathfrak{m}$ be a maximal δ-ideal of R. For every $g \in G(k)$, also $g(\mathfrak{m})$ is a maximal δ-ideal of R. It thus suffices to show that the ideal $I = \bigcap_{g \in G(k)} g(\mathfrak{m})$ of R is zero. Clearly $g(I) \subseteq I$ for every $g \in G(k)$. In terms of the coaction $\rho\colon R \to R \otimes_k k[G]$ (as in Lemma 3.3) this property translates to $\rho(I) \subseteq I \otimes_k k[G]$. But then the closed subscheme W of $\mathrm{Spec}(R)$ defined by I is stable under the action of $G_{k(x)}$. Since $\mathrm{Spec}(R)$ is a $G_{k(x)}$-torsor, this is only possible if $W = \mathrm{Spec}(R)$, i.e, $I = 0$. $\qquad\square$

To explain how differential torsors are obtained by "spreading out" a Picard-Vessiot ring into a family of differential rings we will need a basic lemma on linear algebraic groups.

Lemma 3.9. *Let G be a linear algebraic group over k and let k'/k be a field extension. If $\phi'\colon G_{k'} \to \mathrm{GL}_{n,k'}$ is a closed embedding of algebraic groups over k', then there exists a finitely generated k-subalgebra $\mathcal{B}$ of k' and a closed embedding $\phi\colon G_{\mathcal{B}} \to \mathrm{GL}_{n,\mathcal{B}}$ of group schemes over $\mathcal{B}$ such that $\phi_{k'} = \phi'$.*

Proof. Writing k' as the directed union of its finitely generated k-subalgebras, this follows from Theorem 8.8.2 and Theorem 8.10.5 (iv) in [Gro66]. $\qquad\square$

The following simple example illustrates Lemma 3.9.

Example 3.10. Let k'/k be a field extension and $b \in k' \smallsetminus \{0\}$. Consider the closed embedding $\phi'\colon \mathbb{G}_{a,k'} \to \mathrm{GL}_{2,k'}$ of algebraic groups over k' (where $\mathbb{G}_{a,k'}$ denotes the additive group over k') given by

$$g \mapsto \begin{pmatrix} 1 & bg \\ 0 & 1 \end{pmatrix}. \tag{15}$$

For $\mathcal{B} = k[b] \subseteq k'$, formula (15) defines a morphism $\mathbb{G}_{a,\mathcal{B}} \to \mathrm{GL}_{2,\mathcal{B}}$ of group schemes over $\mathcal{B}$ that need not be a closed embedding, e.g., if b is transcendental over k, the fibre over $b = 0$ is not a closed embedding. However, for $\mathcal{B} = k[b, b^{-1}] \subseteq k'$, formula (15) defines a closed embedding $\mathbb{G}_{a,\mathcal{B}} \to \mathrm{GL}_{2,\mathcal{B}}$ of group schemes over $\mathcal{B}$.

One can think of differential torsors as the kind of objects one obtains when "spreading out" a Picard-Vessiot ring into a nice family. This is formalized in the following lemma.

Lemma 3.11. *Let $k \subseteq k'$ be an inclusion of algebraically closed fields and let $R/k'(x)$ be a Picard-Vessiot ring for $\delta(y) = Ay$ with $A \in k'(x)^{n\times n}$ and $Y \in \mathrm{GL}_n(R)$ such that $\delta(Y) = AY$. Then there exist*

- *a finitely generated k-subalgebra $\mathcal{B}$ of k',*

- *a monic polynomial $f \in \mathcal{B}[x]$,*

- *an affine group scheme $\mathcal{G}$ of finite type over $\mathcal{B}$ and*

- *a differential $\mathcal{G}$-torsor $\mathcal{R}/\mathcal{B}[x]_f$*

such that

- *$A \in \mathcal{B}[x]_f^{n\times n}$,*

29

- $\mathcal{R}$ is flat over $\mathcal{B}[x]_f$ and $\mathcal{R}/\mathcal{B}[x]_f$ is a differential $\mathcal{G}$-torsor for $\delta(y) = Ay$ with fundamental solution matrix $\mathcal{Y} \in \mathrm{GL}_n(\mathcal{R})$ and $R^{\mathrm{gen}} = \mathcal{R} \otimes_{\mathcal{B}[x]_f} K(x)$ is δ-simple, where $K \subseteq k'$ is the algebraic closure of the field of fractions of $\mathcal{B}$ and

- $R^{\mathrm{gen}} \otimes_{K(x)} k'(x) \simeq R$ via an isomorphism that identifies $\mathcal{Y}$ with Y.

Moreover, if $\mathcal{B}_0$ is a finitely generated k-subalgebra of k' and $f_0 \in \mathcal{B}_0[x]$ is monic, then $\mathcal{B}$ can be chosen such that $\mathcal{B}_0 \subseteq \mathcal{B}$ and f can be chosen such that f_0 divides f in $\mathcal{B}[x]$. If, in addition, $f_0 \in \mathcal{B}_0[x]$ is such that $A \in \mathcal{B}_0[x]_{f_0}^{n \times n}$, then $\mathcal{B}$ can, in addition, be chosen such that $\mathcal{B}$ is contained in the algebraic closure of the field of fractions of $\mathcal{B}_0$.

Furthermore, if the differential Galois group G of $R/k'(x)$ is of the form $G = G_{0,k'}$ for some algebraic group G_0 over k, then $\mathcal{G}$ can be chosen to be equal to $G_{0,\mathcal{B}}$.

Proof. We consider the differential Galois group G of $R/k'(x)$ as a closed subgroup of $\mathrm{GL}_{n,k'}$ via the choice of Y. The contributions to $\mathcal{B}$ and f came from three different sources. We go through them one by one:

(a) Let $\mathcal{B}_1$ be a finitely generated k-subalgebra of k' and $f_1 \in \mathcal{B}[x]$ a monic polynomial such that $A \in \mathcal{B}_1[x]_{f_1}^{n \times n}$. Then $\mathcal{B}_1[x]_{f_1}[Y, \frac{1}{\det(Y)}]$ is a δ-subring of R.

(b) Consider the ideal I of $k'(x)[X, \frac{1}{\det(X)}]$ given by $I = \{p \in k'(x)[X, \frac{1}{\det(X)}] | \, p(Y) = 0\}$. Choose $p_1, \ldots, p_r \in I$ such that $I = (p_1, \ldots, p_r)$. Let $\mathcal{B}_2$ be a finitely generated k-subalgebra of k' and let $f_2 \in \mathcal{B}_2[x]$ be monic such that $p_1, \ldots, p_r \in \mathcal{B}_2[x]_{f_2}[X, \frac{1}{\det(X)}] \subseteq k'(x)[X, \frac{1}{\det(X)}]$.

(c) Let $\mathcal{B}_3$ be a finitely generated k-subalgebra of k' and $\mathcal{G}_3$ a closed subgroup scheme of $\mathrm{GL}_{n,\mathcal{B}_3}$ such that $\mathcal{G}_{3,k'} = G$ as closed subgroups of $\mathrm{GL}_{n,k'}$. By generic flatness ([Eis04, Theorem 14.4]), we may assume that $\mathcal{G}$ is flat over $\mathcal{B}_3$.

Let $\mathcal{B}_4$ be the k-subalgebra of k' generated by $\mathcal{B}_1, \mathcal{B}_2$ and $\mathcal{B}_3$. Furthermore, set $f_4 = f_1 f_2$ and consider the finitely generated $\mathcal{B}_4[x]_{f_4}$-algebra $\mathcal{B}_4[x]_{f_4}[Y, \frac{1}{\det(Y)}] \subseteq R$. By generic flatness ([Eis04, Theorem 14.4]), there exists a nonzero (not necessarily monic) $h \in \mathcal{B}_4[x]_{f_4}$ such that $(\mathcal{B}_4[x]_{f_4})_h[Y, \frac{1}{\det(Y)}]$ is flat over $(\mathcal{B}_4[x]_{f_4})_h$. Write $h = \frac{h_1}{f_4^m}$ with $h_1 \in \mathcal{B}_4[x]$ and $m \geq 1$. With $h' = f_4 h_1 \in \mathcal{B}_4[x]$ we then have $(\mathcal{B}_4[x]_{f_4})_h = \mathcal{B}_4[x]_{h'}$.

Let $\mathcal{B}$ be the k-subalgebra of k' generated by $\mathcal{B}_4$ and the inverse (in k') of the leading coefficient b of h'. In general, if $R \to S$ is a flat ring map and $f \in R$, then $S_f = S \otimes_R R_f$ is a flat R_f-module ([Sta24, Tag 00HI]). Therefore, since $\mathcal{B}_4[x]_{h'}[Y, \frac{1}{\det(Y)}]$ is a flat $\mathcal{B}_4[x]_{h'}$-module, $(\mathcal{B}_4[x]_{h'})_b[Y, \frac{1}{\det(Y)}]$ is a flat $(\mathcal{B}_4[x]_{h'})_b$-module. For the monic polynomial $f = \frac{1}{b} h' \in \mathcal{B}[x]$ we have $(\mathcal{B}_4[x]_{h'})_b = \mathcal{B}[x]_f$ and so $\mathcal{B}[x]_f[Y, \frac{1}{\det(Y)}]$ is a flat $\mathcal{B}[x]_f$-module.

We set $\mathcal{R} = \mathcal{B}[x]_f[Y, \frac{1}{\det(Y)}]$ and $\mathcal{G} = \mathcal{G}_{3,\mathcal{B}}$. Then $\mathcal{R}$ is a $\mathcal{B}[x]_f$-δ-algebra and flat over $\mathcal{B}[x]_f$. Moreover, the canonical surjection $\mathcal{R} \otimes_{\mathcal{B}[x]_f} k'(x) \to R$ is an isomorphism by item (b) above. Since $\mathcal{G}_3$ is flat over $\mathcal{B}_3$, we see that $\mathcal{G}$ is flat over $\mathcal{B}$. Furthermore, $\mathcal{G}_{k'} = (\mathcal{G}_{3,\mathcal{B}})_{k'} = \mathcal{G}_{3,k'} = G$. In particular, $k'(x) \otimes_{\mathcal{B}} \mathcal{B}[\mathcal{G}] = k'(x) \otimes_{k'} k'[G]$.

The above flatness properties allow us to identify $\mathcal{R} \otimes_{\mathcal{B}} \mathcal{B}[\mathcal{G}]$ with a δ-subring of $R \otimes_{k'} k'[\mathcal{G}]$. In detail, since $\mathcal{B}[\mathcal{G}]$ is a flat $\mathcal{B}$-algebra, $\mathcal{B}[x]_f \otimes_{\mathcal{B}} \mathcal{B}[\mathcal{G}]$ is a flat $\mathcal{B}[x]_f$-algebra and therefore $\mathcal{R} \otimes_{\mathcal{B}} \mathcal{B}[\mathcal{G}] = \mathcal{R} \otimes_{\mathcal{B}[x]_f} (\mathcal{B}[x]_f \otimes_{\mathcal{B}} \mathcal{B}[\mathcal{G}])$ is a flat $\mathcal{B}[x]_f$-algebra. This entails that the map $\mathcal{R} \otimes_{\mathcal{B}} \mathcal{B}[\mathcal{G}] \to (\mathcal{R} \otimes_{\mathcal{B}} \mathcal{B}[\mathcal{G}]) \otimes_{\mathcal{B}[x]_f} k'(x)$ is injective. But

$$(\mathcal{R} \otimes_{\mathcal{B}} \mathcal{B}[\mathcal{G}]) \otimes_{\mathcal{B}[x]_f} k'(x) = (\mathcal{R} \otimes_{\mathcal{B}[x]_f} k'(x)) \otimes_{k'(x)} (k'(x) \otimes_{\mathcal{B}} \mathcal{B}[\mathcal{G}]) =$$
$$= R \otimes_{k'(x)} (k'(x) \otimes_{k'} k'[G]) = R \otimes_{k'} k'[G].$$

So we can consider $\mathcal{R} \otimes_{\mathcal{B}} \mathcal{B}[\mathcal{G}]$ as a subring of $R \otimes_{k'} k'[G]$.

As explained in Section 3.1, the closed embedding $G \to \mathrm{GL}_{n,k'}$ corresponds to the morphism $k'[X, \frac{1}{\det(X)}] \to k'[G] = (R \otimes_{k'(x)} R)^{\delta}$, $X \mapsto Z = Y^{-1} \otimes Y$. Moreover, the coaction $R \to R \otimes_{k'} k'[G]$ is determined by $Y \mapsto Y \otimes Z$. In summary, we see that the coaction $R \to R \otimes_{k'} k'[G]$ restricts to a map $\mathcal{R} \to \mathcal{R} \otimes_{\mathcal{B}} \mathcal{B}[\mathcal{G}]$. It is then clear that $\mathcal{G}$ acts on $\mathcal{R}/\mathcal{B}[x]_f$. Indeed, for a $\mathcal{B}$-algebra $\mathcal{T}$, every $g \in \mathcal{G}(\mathcal{T}) \leq \mathrm{GL}_n(\mathcal{T})$ acts on $\mathcal{R} \otimes_{\mathcal{B}} \mathcal{T}$ by $Y \otimes 1 \mapsto Y \otimes g$.

To see that $\mathcal{R}/\mathcal{B}[x]_f$ is a differential $\mathcal{G}$-torsor, let us first show that $\mathcal{R} \otimes_{\mathcal{B}[x]_f} \mathcal{R} \to R \otimes_{k'(x)} R$ is injective. Note that

$$(\mathcal{R} \otimes_{\mathcal{B}[x]_f} \mathcal{R}) \otimes_{\mathcal{B}[x]_f} k'(x) = (\mathcal{R} \otimes_{\mathcal{B}[x]_f} k'(x)) \otimes_{k'(x)} (\mathcal{R} \otimes_{\mathcal{B}[x]_f} k'(x)) = R \otimes_{k'(x)} R.$$

It thus suffices to show that the map $\mathcal{R} \otimes_{\mathcal{B}[x]_f} \mathcal{R} \to (\mathcal{R} \otimes_{\mathcal{B}[x]_f} \mathcal{R}) \otimes_{\mathcal{B}[x]_f} k'(x)$ is injective. But this follows from the flatness of $\mathcal{B}[x]_f \to \mathcal{R} \otimes_{\mathcal{B}[x]_f} \mathcal{R}$, which in turn follows from the flatness of $\mathcal{B}[x]_f \to \mathcal{R}$.

We claim that the isomorphism $R \otimes_{k'(x)} R \to R \otimes_{k'} k'[G]$ restricts to an isomorphism $\mathcal{R} \otimes_{\mathcal{B}[x]_f} \mathcal{R} \to \mathcal{R} \otimes_{\mathcal{B}} \mathcal{B}[\mathcal{G}]$. Injectivity being obvious, the surjectivity of $\mathcal{R} \otimes_{\mathcal{B}[x]_f} \mathcal{R} \to \mathcal{R} \otimes_{\mathcal{B}} \mathcal{B}[\mathcal{G}]$ follows from $\mathcal{B}[\mathcal{G}] = \mathcal{B}[Z, \frac{1}{\det(Z)}]$, where $Z = Y^{-1} \otimes Y \in \mathrm{GL}_n(R \otimes_{k'(x)} R)$, and $\mathcal{R} \otimes_{\mathcal{B}[x]_f} \mathcal{R} \to \mathcal{R} \otimes_{\mathcal{B}} \mathcal{B}[\mathcal{G}]$ maps $Y^{-1} \otimes Y$ to $1 \otimes Z$. Thus $\mathcal{R}/\mathcal{B}[x]_f$ is a differential $\mathcal{G}$-torsor. As $\delta(Y) = AY$ and $\mathcal{R} = \mathcal{B}[x]_f[Y, \frac{1}{\det(\mathcal{Y})}]$, we see that, in fact, $\mathcal{R}/\mathcal{B}[x]_f$ is a differential $\mathcal{G}$-torsor for $\delta(y) = Ay$ with fundamental matrix $\mathcal{Y} = Y$.

As $(\mathcal{R} \otimes_{\mathcal{B}[x]_f} K(x)) \otimes_{K(x)} k'(x) = \mathcal{R} \otimes_{\mathcal{B}[x]_f} k'(x) = R$ is δ-simple, we see that also $R^{\mathrm{gen}} = \mathcal{R} \otimes_{\mathcal{B}[x]_f} K(x)$ must be δ-simple. We have thus established the first claim of the lemma.

To address the second claim, let $K_0 \subseteq k'$ be the algebraic closure of the field of fractions of $\mathcal{B}_0$. Note that there is no difficulty in arranging $\mathcal{B}$ such that $\mathcal{B}_0 \subseteq \mathcal{B}$. For example, in the above construction of $\mathcal{B}$, we could choose $\mathcal{B}_1$ such that $\mathcal{B}_0 \subseteq \mathcal{B}_1$. Similarly, we can choose f_1 so that f_0 divides f_1.

Assume that $A \in \mathcal{B}_0[x]_{f_0}^{n \times n}$. As $A \in K_0(x)^{n \times n}$, we may consider a Picard-Vessiot ring $R_0/K_0(x)$ for $\delta(y) = Ay$. It then follows from Lemma 3.2 that $R_0 \otimes_{K_0(x)} k'(x)$ is a Picard-Vessiot ring for $\delta(y) = Ay$ over $k'(x)$. By the uniqueness of Picard-Vessiot rings, we thus have $R \simeq R_0 \otimes_{K_0(x)} k'(x)$. We can now apply the first claim of the lemma to the inclusion $k \subseteq K_0$ and the Picard-Vessiot ring $R_0/K_0(x)$. Then automatically $\mathcal{B} \subseteq K_0$.

Concerning the last claim of the lemma, note that, according to Lemma 3.9, the closed embedding $G = G_{k'} \to \mathrm{GL}_{n,k'}$ determined by Y spreads out to a closed embedding $G_{\mathcal{B}'} \to \mathrm{GL}_{n,\mathcal{B}'}$, where $\mathcal{B}'$ is a finitely generated k-subalgebra of k'. In point (c) above, we can thus choose $\mathcal{B}_3 = \mathcal{B}'$ and $\mathcal{G}_3 = G_{\mathcal{B}_3}$, so that $\mathcal{G} = G_{0,\mathcal{B}}$.

$\qquad\square$

3.3 Proto-Picard-Vessiot rings

For a linear algebraic group G, let G^t denote the intersection of all kernels of all characters of G°, the identity component of G. The algebraic group G^t plays a fundamental role in the study of moduli of linear differential equations ([Sin93]) and in Hrushovski's algorithm ([Hru02]). In regards to Hrushovski's algorithm, the key point concerning G^t is the following. While the degree of defining equations of a closed subgroup of GL_n cannot be bounded uniformly in n (consider, e.g., the groups μ_m of m-th roots of unity in GL_1), there exists a function $\mathbf{d}$ of n such that for every closed subgroup H of GL_n there exists

a closed subgroup G of GL_n defined by equations of degree at most $\mathbf{d}(n)$ satisfying

$$G^t \leq H \leq G. \tag{16}$$

Given H, an algebraic group G satisfying (16) is called a *proto-Galois group* for H ([AMP22, Def. 4.1]). In the first main step of Hrushovski's algorithm a proto-Galois group for the differential Galois group is computed.

For our purpose, the mere existence of the function $\mathbf{d}(n)$ is sufficient. To make Hrushovski's algorithm practical (a goal that seems rather far out of reach), it is important to find small bounds. In [AMP22] it is shown that one can take $\mathbf{d}(n) = (4n)^{3n^2}$.

One can think of G as an "approximation" of H. This approximation is good in the sense that G/G^t is small. Indeed, G^t is normal in G and the identity component of G/G^t is a torus. An alternative description of G^t is, as the closed subgroup of G generated by all unipotent elements of G. In this section we introduce an analog of this notion for differential torsors: Proto-Picard-Vessiot ring. We think of them as "approximations" of Picard-Vessiot rings. We also establish a criterion that enables us to decide whether or not a proto-Picard-Vessiot ring is a Picard-Vessiot ring.

In addition to the standing assumption of Section 3 that F is a differential field with field of constants $k = F^\delta$ algebraically closed and of characteristic zero, throughout Section 3.3 we make the following assumptions:

- G is a linear algebraic group over k;

- $A \in F^{n \times n}$;

- R/F is a differential G-torsor for $\delta(y) = Ay$ with fundamental matrix $Y \in \mathrm{GL}_n(R)$ such that R is an integral domain;

- F' is the integral closure of F in R;

- E is the field compositum of $\overline{F}$ and the field of fractions of R (inside the algebraic closure of the field of fractions of R).

Note that if $\mathfrak{m}$ is a maximal δ-ideal of R, then $R/\mathfrak{m}$ is a Picard-Vessiot ring for $\delta(y) = Ay$. As we will now explain, the differential Galois group H of $R/\mathfrak{m}$ is canonically a closed subgroup of G (cf. the proof of Proposition 1.15 in [BHHW18]). The composition

$$R \otimes_k k[G] \xrightarrow{\simeq} R \otimes_F R \rightarrow R/\mathfrak{m} \otimes_F R/\mathfrak{m} \xrightarrow{\simeq} R/\mathfrak{m} \otimes_k k[H] \tag{17}$$

maps $k[G]$ into $k[H]$, because the elements of $k[G]$ are constant and the constants of $R/\mathfrak{m} \otimes_k k[H]$ are just $k[H]$. Thus the surjection (17) is of the form $\pi \otimes \psi$, where $\pi \colon R \rightarrow R/\mathfrak{m}$ is the canonical map and $\psi \colon k[G] \rightarrow k[H]$ is a surjective map of k-algebras. So ψ defines a closed embedding $H \rightarrow G$ and we may identify H with a closed subscheme of G. We claim that

$$H(T) = \{g \in G(T) \mid g(\mathfrak{m} \otimes_k T) = \mathfrak{m} \otimes_k T\} \tag{18}$$

for every k-algebra T. In particular, H is a closed subgroup of G.

The commutative diagram

$$
\begin{array}{ccc}
R & \xrightarrow{\rho} & R \otimes_k k[G] \\
\pi \downarrow & & \downarrow \pi \otimes \psi \\
R/\mathfrak{m} & \longrightarrow & R/\mathfrak{m} \otimes_k k[H]
\end{array}
$$

shows that $\rho(\mathfrak{m}) \subseteq \mathfrak{m} \otimes_k k[G] + R \otimes_k \mathbb{I}(H)$, where $\mathbb{I}(H) = \ker(\psi) \subseteq k[G]$ is the defining ideal of H. Therefore $g(\mathfrak{m} \otimes_k T) \subseteq \mathfrak{m} \otimes_k T$ for $g \in H(T)$. Since also $g^{-1} \in H(T)$, we deduce that indeed $g(\mathfrak{m} \otimes_k T) = \mathfrak{m} \otimes_k T$.

Conversely, if $g \in G(T)$ satisfies $g(\mathfrak{m} \otimes_k T) = \mathfrak{m} \otimes_k T$, then g induces a differential automorphism of $(R \otimes_k T)/(\mathfrak{m} \otimes_k T) = R/\mathfrak{m} \otimes_k T$ and thus belongs to $H(T)$, by definition of H. This proves (18).

Now let $\mathfrak{m}'$ be another maximal δ-ideal of R. Then $R/\mathfrak{m}'$ is a Picard-Vessiot ring over F with differential Galois group H' canonically contained in G. We will show that $G^t \leq H$ if and only if $G^t \leq H'$.

As a first step, let us show that there exists a $g \in G(k)$ such that $\mathfrak{m}' = g(\mathfrak{m})$. Consider the morphism

$$k[G] \to R \otimes_k k[G] \xrightarrow{\simeq} R \otimes_F R \to R/\mathfrak{m}' \otimes_F R/\mathfrak{m} \to S, \qquad (19)$$

where S is a quotient of $R/\mathfrak{m}' \otimes_F R/\mathfrak{m}$ by a maximal δ-ideal. As S is δ-simple and finitely generated over F, we have $S^\delta = k$ ([vdPS03, Lemma 1.17]). Thus (19) maps $k[G]$ into k and therefore defines a point $g \in G(k)$. By construction, $g(\mathfrak{m}) \subseteq \mathfrak{m}'$. Since $g(\mathfrak{m})$ is a maximal δ-ideal of R, we obtain $g(\mathfrak{m}) = \mathfrak{m}'$ as claimed.

From (18), we thus deduce that $H' = gHg^{-1}$. As G^t is normal G, we see that $G^t \leq H$ if and only if $G^t \leq H'$.

In summary, if $\mathfrak{m}$ and $\mathfrak{m}'$ are maximal δ-ideals in R, yielding differential Galois groups $H \leq G$ and $H' \leq G$ respectively, then $G^t \leq H$ if and only if $G^t \leq H'$. So we can use this property to define proto-Picard-Vessiot rings.

Definition 3.12. *The differential torsor R/F is* proto-Picard-Vessiot *if for one (equivalently every) maximal δ-ideal $\mathfrak{m}$ of R we have $G^t \leq H$, where H is the differential Galois group of $R/\mathfrak{m}$.*

Clearly, R/F is proto-Picard-Vessiot if R/F is Picard-Vessiot. Our next goal is to find a criterion to test if a differential torsor is proto-Picard-Vessiot. In the next defintion and lemma k' is a field of characteristic zero. Following [Fen15] and [AMP22, Def. 2.3] we make the below definition.

Definition 3.13. *A geometrically reduced closed subscheme Z of $\mathrm{GL}_{n,k'}$ is* bounded *by a positive integer d, if there exist polynomials $p_1, \ldots, p_m \in k'[X]$ of degree at most d such that*

$$Z(\overline{k'}) = \{g \in \mathrm{GL}_n(\overline{k'}) \mid p_1(g) = \ldots = p_m(g) = 0\}. \qquad (20)$$

Note that, by Hilbert's Nullstellensatz, (20) is equivalent to $\mathbb{I}(Z) = \sqrt{(p_1, \ldots, p_m)}$, where $\mathbb{I}(Z) \subseteq k'[X, \frac{1}{\det X}]$ is the defining ideal of Z and $(p_1, \ldots, p_m)$ is the ideal of $k'[X, \frac{1}{\det X}]$ generated by $p_1, \ldots, p_m$.

Lemma 3.14. *Let G be a closed subgroup of $\mathrm{GL}_{n,k'}$ and Z a geometrically reduced closed subscheme of $\mathrm{GL}_{n,k'}$ such that Z is a G-torsor under right multiplication. If G is bounded by d, then also Z is bounded by d.*

Proof. A point $z \in Z(\overline{k'})$ defines an isomorphism $G_{\overline{k'}} \to Z_{\overline{k'}}$, $g \mapsto zg$ of schemes over $\overline{k'}$. If $p_1, \ldots, p_m \in k'[X]$ are such that

$$G(\overline{k'}) = \{g \in \mathrm{GL}_n(\overline{k'}) \mid p_1(g) = \ldots = p_m(g) = 0\},$$

then

$$Z(\overline{k'}) = \{g \in \mathrm{GL}_n(\overline{k'})| \ p_1(z^{-1}g) = \ldots = p_m(z^{-1}g) = 0\}.$$

So $\mathbb{I}(Z_{\overline{k'}}) = \sqrt{(p_1(z^{-1}X), \ldots, p_m(z^{-1}X))} \subseteq \overline{k'}[X, \frac{1}{\det(X)}]$.

We have $\mathbb{I}(Z_{\overline{k'}}) = \mathbb{I}(Z) \otimes_{k'} \overline{k'}$ and so, if $p_i(z^{-1}X) \in \overline{k'}[X]$ has degree at most d, i.e, p_i has degree at most d, then $p_i(z^{-1}X)$ can be written as a $\overline{k'}$-linear combination of polynomials $q_{i,j} \in k'[X] \cap \mathbb{I}(Z)$ of degree at most d. The set of solutions of all q_{ij}'s in $\mathrm{GL}_n(\overline{k'})$ is $Z(\overline{k'})$. Therefore Z is bounded by d. $\qquad\square$

As above, set $\mathbf{d}(n) = (4n)^{3n^2}$. The following lemma allows us to test if a differential torsor is proto-Picard-Vesssiot. Roughly speaking, it shows that R/F is proto-Picard-Vessiot if R encodes the algebraic relations among the entries of a fundamental solution matrix up to degree $\mathbf{d}(n)$.

Lemma 3.15. *Let $\mathfrak{m}$ be a maximal δ-ideal of R. If $p(Y) = 0$ for every $p \in F[X]$ with $\deg(p) \leq \mathbf{d}(n)$ and $p(Y) \in \mathfrak{m}$, then R/F is proto-Picard-Vessiot.*

Proof. Let $H \leq G$ be the differential Galois group of $R/\mathfrak{m}$ and consider H as a closed subgroup of $\mathrm{GL}_{n,k}$ via the fundamental solution matrix $\overline{Y} \in \mathrm{GL}_n(R/\mathfrak{m})$, the image of Y in $R/\mathfrak{m}$. Due to Corollary 4.1 of [AMP22], there exists a closed subgroup $\tilde{G}$ of $\mathrm{GL}_{n,k}$ bounded by $\mathbf{d}(n)$ such that $\tilde{G}^t \leq H \leq \tilde{G}$.

Let $\mathfrak{m}'$ be the maximal δ-ideal of $F[X, \frac{1}{\det(X)}]$ whose image in R is $\mathfrak{m}$ and let Z' be the closed subscheme of $\mathrm{GL}_{n,F}$ defined by $\mathfrak{m}'$. The image $\tilde{Z}$ of $Z' \times \tilde{G}_F \to \mathrm{GL}_{n,F}, (z, g) \mapsto zg$ is a $\tilde{G}_F$-torsor. Indeed, for a point $z \in Z'(\overline{F})$ we have

$$\tilde{Z}(\overline{F}) = Z'(\overline{F})\tilde{G}(\overline{F}) = zH(\overline{F})\tilde{G}(\overline{F}) = z\tilde{G}(\overline{F}).$$

We know from Lemma 3.14 that $\tilde{Z}$ is bounded by $\mathbf{d}(n)$. Let $p_1, \ldots, p_m \in F[X]$ be polynomials of degree at most $\mathbf{d}(n)$ such that $\mathbb{I}(\tilde{Z}) = \sqrt{(p_1, \ldots, p_m)}$. As $Z' \subseteq \tilde{Z}$, we have $\mathbb{I}(\tilde{Z}) \subseteq \mathfrak{m}'$. Therefore $p_1(Y), \ldots, p_m(Y) \in \mathfrak{m}$. By assumption, the image of $p_1, \ldots, p_m$ in R is zero. Since R is reduced, we see that in fact the image of $\mathbb{I}(\tilde{Z})$ in R is zero. Geometrically, this means that $Z \subseteq \tilde{Z}$, where $Z \subseteq \mathrm{GL}_{n,F}$ is the closed subscheme defined by $\mathbb{I}(Z) = \{p \in F[X, \frac{1}{\det(X)}]| \ p(Y) = 0\}$. As Z is a G_F-torsor and $\tilde{Z}$ is a $\tilde{G}_F$-torsor (both under right multiplication), we must have $G \leq \tilde{G}$. Therefore, $G^t \leq \tilde{G}^t \leq H$ and R/F is proto-Picard-Vessiot. $\qquad\square$

We now work towards a criterion to decided if a proto-Picard-Vessiot ring is Picard-Vessiot. Recall that G° denotes the identity component of the algebraic group G and that F' is the integral closure of F in R.

Lemma 3.16. *The F'-δ-algebra R/F' is a differential G°-torsor for $\delta(y) = Ay$.*

Proof. As in [Wat79, Section 6.5], for a k'-algebra S over a field k', let $\pi_0(S/k')$ denote the union of all étale k'-subalgebras of S. In particular, $\pi_0(R/F) = F'$ and $\pi_0(k[G]/k) = k[G/G^\circ]$. In fact, the defining ideal $\mathbb{I}(G^\circ) \subseteq k[G]$ of G° is the ideal of $k[G]$ generated by $\ker(\varepsilon) \cap \pi_0(k[G]/k)$, where $\varepsilon \colon k[G] \to k$ is the counit ([Wat79, Section 6.7]).

In the diagram

$$\begin{array}{ccc} R \otimes_F R & \xrightarrow{\ \simeq\ } & R \otimes_k k[G] \\ \downarrow & & \downarrow \\ R \otimes_{F'} R & & R \otimes_k k[G^\circ] \end{array} \qquad\qquad (21)$$

34

the kernel of the left vertical map is $(f \otimes 1 - 1 \otimes f \mid f \in F') \subseteq R \otimes_F R$. The kernel of the right vertical map is $R \otimes_k \mathbb{I}(G^\circ)$, the ideal of $R \otimes_k k[G]$ generated by $\ker(\varepsilon) \cap \pi_0(k[G]/k)$. We claim that these two kernels correspond to each other under the isomorphism.

The diagram

$$
\begin{array}{ccc}
F' \otimes_F F' & \xrightarrow{\;\simeq\;} & F' \otimes_k \pi_0(k[G]/k) \\
& \searrow \qquad \swarrow {\scriptstyle \mathrm{id} \,\cdot\, \varepsilon} & \\
& F' &
\end{array}
$$

where the top isomorphism is obtained by applying π_0 to $R \otimes_F R \simeq R \otimes_k k[G]$, commutes. The kernel of the left map is $(f \otimes 1 - 1 \otimes f \mid f \in F') \subseteq F' \otimes_F F'$. The kernel of the right map is $F' \otimes_k (\pi_0(k[G]/k) \cap \ker(\varepsilon))$. This shows that the two kernels in (21) correspond to each other. We thus have an induced isomorphism $R \otimes_{F'} R \simeq R \otimes_k k[G^\circ]$, showing that R/F' is a differential G°-torsor. $\qquad \square$

Let $\overline{F}R$ denote the ring compositum of $\overline{F}$ and R (inside the algebraic closure of the field of fractions of R). In other words, $\overline{F}R$ is the $\overline{F}$-algebra generated by R.

Corollary 3.17. *We have $\overline{F}R = R \otimes_{F'} \overline{F}$ and $\overline{F}R/\overline{F}$ is a differential G°-torsor.*

Proof. Since R/F' is a differential G°-torsor (Lemma 3.16), it follows from Lemma 3.7 that $R \otimes_{F'} \overline{F}/\overline{F}$ is a differential G°-torsor. As G° is connected, this implies that $R \otimes_{F'} \overline{F}$ is an integral domain, i.e., R is a regular F'-algebra. This implies ([Bou90, Chapter V, §17, Sections 4 and 5] that F' is relatively algebraically closed in the field of fractions $F'(R)$ of R and that $F'(R) \otimes_F \overline{F}$ is a field. Thus the canonical map $F'(R) \otimes_{F'} \overline{F} \to E$ is injective (in fact bijective) and so also $R \otimes_{F'} \overline{F} \to \overline{F}R$ is injective. $\qquad \square$

Following [Gro67, Def. 4.5.2], for a field k' and a k'-algebra R', the number of irreducible components of $\mathrm{Spec}(R' \otimes_{k'} \overline{k'})$ is called the *geometric number of irreducible components of R'/k'.*

Corollary 3.18. *The geometric number of irreducible components of R/F is $[F' : F]$.*

Proof. Because R/F is a differential G-torsor, $R \otimes_F \overline{F}$ is isomorphic to $\overline{F}[G_{\overline{F}}]$ (as an $\overline{F}$-algebra). The number of irreducible components of $G_{\overline{F}}$ is the same as the number of connected components of $G_{\overline{F}}$ and this is the same as the number of connected components of G. The latter is the same as the dimension $\dim_k \pi_0(k[G]/k)$ of $\pi_0(k[G]/k)$ as a k-vector space. As observed in the proof of Lemma 3.16, we have $F' \otimes_F F' = F' \otimes_k \pi_0(k[G]/k)$. So $\dim_k \pi_0(k[G]/k)$ must equal $[F' : F]$. $\qquad \square$

Recall that E denotes the field compositum of $\overline{F}$ and the field of fractions of R (inside the algebraic closure of the field of fractions of R). The idea for the criterion to decide if a proto-Picard-Vessiot ring R/F is Picard-Vessiot is to first Gauge transform the equation $\delta(y) = Ay$ with fundamental solution matrix Y to an equation $\delta(y) = A'y$ (where $A' = BAB^{-1} + \delta(B)B^{-1}$) with fundamental matrix BY via a matrix $B \in \mathrm{GL}_n(\overline{F})$ such that $BY \in G^\circ(E)$ and then apply characters of G° to BY. The following corollary shows that we can always find such a transformation matrix B.

Corollary 3.19. *For $\vartheta \in \mathrm{Hom}_{F'}(R, \overline{F})$ and $B = \vartheta(Y)^{-1} \in \mathrm{GL}_n(\overline{F})$ we have $BY \in G^\circ(E)$.*

35

Proof. Set $Z = \operatorname{Spec}(R)$, considered as a scheme over F'. As R/F' is a G°-torsor by Lemma 3.16, the morphism

$$Z \times_{F'} G^\circ_{F'} \to Z \times_{F'} Z, \ (z,g) \mapsto (z, zg) \tag{22}$$

is an isomorphism. If we consider Z and $G^\circ_{F'}$ as closed subschemes of $\operatorname{GL}_{n,F'}$ via Y, the inverse of (22) is given by $(z_1, z_2) \mapsto (z_1, z_1^{-1} z_2)$. In particular, for any field extension $\widetilde{F}$ of F' and $z_1, z_2 \in Z(\widetilde{F})$, we have $z_1^{-1} z_2 \in G^\circ(\widetilde{F})$. With $\widetilde{F} = E$, $z_1 = \vartheta(Y)$ and $z_2 = Y$, this implies the claim. $\square$

We note that there is a fixed embedding of F' into $\overline{F}$ derived from forming the algebraic closure of F inside the the algebraic closure of the field of fractions of R and $\operatorname{Hom}_{F'}(R, \overline{F})$ has to be interpreted accordingly.

We denote with I_n the $n \times n$-identity matrix.

Lemma 3.20. *Let χ be a character of G°, $\vartheta \in \operatorname{Hom}_{F'}(R, \overline{F})$ and $B = \vartheta(Y)^{-1} \in \operatorname{GL}_n(\overline{F})$. Then*

$$\delta(\chi(BY)) = \left(\sum_{i,j=1}^{n} \frac{\partial \chi}{\partial X_{ij}}(I_n)(BAB^{-1} + \delta(B)B^{-1})_{ij} \right) \chi(BY).$$

Proof. We will work with the ring $E[\varepsilon]$ of dual numbers, i.e., $\varepsilon^2 = 0$. For $p \in F[X, \frac{1}{\det(X)}]$, $C \in \operatorname{GL}_n(E)$ and $D \in E^{n \times n}$ (i.e., $C + \varepsilon D \in \operatorname{GL}_n(E[\varepsilon])$), we then have $p(C + \varepsilon D) = p(C) + \varepsilon \sum_{i,j=1}^{n} \frac{\partial p}{\partial X_{ij}}(C) D_{ij}$. Therefore

$$p(C + \varepsilon \delta(C)) = p(C) + \varepsilon \sum_{i,j=1}^{n} \frac{\partial p}{\partial X_{ij}}(C) \delta(C_{ij}) = p(C) + \varepsilon(\delta(p(C))). \tag{23}$$

For $Y' = BY \in \operatorname{GL}_n(E)$ and $A' = BAB^{-1} + \delta(B)B^{-1} \in \overline{F}^{n \times n}$ we have $\delta(Y') = A'Y'$. As $Y' \in G^\circ(E)$ (Corollary 3.19) it follows from (23) that $Y' + \varepsilon \delta(Y') \in G^\circ(E[\varepsilon])$. We have

$$\chi(Y' + \varepsilon \delta(Y'))\chi(Y'^{-1}) = (\chi(Y') + \varepsilon \delta(\chi(Y')))\chi(Y'^{-1}) = 1 + \varepsilon \delta(\chi(Y'))\chi(Y')^{-1}.$$

On the other hand,

$$\chi(Y' + \varepsilon \delta(Y'))\chi(Y'^{-1}) = \chi((Y' + \varepsilon \delta(Y'))Y'^{-1}) = \chi(I_n + \varepsilon A') = 1 + \varepsilon \sum_{i,j=1}^{n} \frac{\partial \chi}{\partial X_{ij}}(I_n) A'_{ij}.$$

Thus

$$\delta(\chi(Y')) = \left(\sum_{i,j=1}^{n} \frac{\partial \chi}{\partial X_{ij}}(I_n) A'_{ij} \right) \chi(Y')$$

as claimed. $\square$

The proof of Lemma 3.20 shows that $\sum_{i,j=1}^{n} \frac{\partial \chi}{\partial X_{ij}}(I_n)(BAB^{-1} + \delta(B)B^{-1})_{ij} \in \overline{F}$ does not depend on the lift of $\chi \in k[G^\circ]$ to an element of $k[X, \frac{1}{\det(X)}]$.

Our criterion that characterizes Picard-Vessiot rings among proto-Picard-Vessiot rings is based on the concept of *logarithmic independence* that we now define.

36

Definition 3.21. *Elements $f_1, \ldots, f_m$ of a differential field F are* logarithmically in-dependent *(over F) if $\sum_{i=1}^{m} d_i f_i = \delta(f)/f$ for $d_1, \ldots, d_m \in \mathbb{Z}$ and $f \in F^{\times}$ implies $d_1 = \cdots = d_m = 0$.*

The significance of the above definition is the following. Let $h_1, \ldots, h_m$ be nonzero elements of some δ-field extension of F with no new constants such that $\delta(h_i) = f_i h_i$ for $i = 1, \ldots, m$. By the Kolchin-Ostrowski theorem ([Kol68]), if $h_1, \ldots, h_m$ are alge-braically dependent over F, then there exist $d_1, \ldots, d_m \in \mathbb{Z}$ not all equal to zero such that $h_1^{d_1} \ldots h_m^{d_m} = f \in F$. Applying the logarithmic derivative $h \mapsto \frac{\delta(h)}{h}$ to this equation yields $\sum_{i=1}^{m} d_i f_i = \delta(f)/f$.

On the other hand, if $\sum_{i=1}^{m} d_i f_i = \delta(f)/f$ holds, the logarithmic derivative of $\frac{h_1^{d_1} \ldots h_m^{d_m}}{f}$ is zero. So $\frac{h_1^{d_1} \ldots h_m^{d_m}}{f}$ is a constant λ and $h_1^{d_1} \ldots h_m^{d_m} = f\lambda \in F$. In summary, we see that $h_1, \ldots, h_m$ are algebraically independent over F if and only if $f_1, \ldots, f_m$ are logarithmically independent.

Note that if $F \subseteq \widetilde{F}$ is an inclusion of differential fields, then $f_1, \ldots, f_m \in F$ may be logarithmically independent over F but logarithmically dependent over $\widetilde{F}$. However, from the above discussion we deduce the following.

Remark 3.22. *If $\widetilde{F}/F$ is an algebraic extension of differential fields and $f_1, \ldots, f_m \in F$, then $f_1, \ldots, f_m$ are logarithmically independent over F if and only if $f_1, \ldots, f_m$ are logarithmically independent over $\widetilde{F}$.*

The following lemma provides a criterion to test if a proto-Picard-Vessiot ring is Picard-Vessiot. We denote with $X(G^{\circ})$ the group of characters of G°.

Lemma 3.23. *Assume that R/F is proto-Picard-Vessiot and let $\chi_1, \ldots, \chi_m$ be a basis of $X(G^{\circ})$ (as a $\mathbb{Z}$-module). Choose $\vartheta \in \mathrm{Hom}_{F'}(R, \overline{F})$ and set $B = \vartheta(Y)^{-1}$ and*

$$
f_\ell = \sum_{i,j=1}^{n} \frac{\partial \chi_\ell}{\partial X_{ij}}(I_n)(BAB^{-1} + \delta(B)B^{-1})_{ij} \in \overline{F}.
$$

for $\ell = 1, \ldots, m$. Then R/F is Picard-Vessiot if and only if $f_1, \ldots, f_m$ are logarithmically independent over $\overline{F}$.

Proof. Suppose R/F is not Picard-Vessiot, i.e., R is not δ-simple. We will show that $f_1, \ldots, f_m$ are logarithmically dependent. As a non-trivial δ-ideal of R, gives rise to a non-trivial δ-ideal of $R \otimes_{F'} \overline{F}$, this implies that also $R \otimes_{F'} \overline{F}$ is not δ-simple.

From Corollary 3.17 we know that $\overline{F}R = R \otimes_{F'} \overline{F}$ is a differential G°-torsor over $\overline{F}$. Let $\overline{\mathfrak{m}}$ be a maximal δ-ideal of $\overline{F}R = R \otimes_{F'} \overline{F}$ and set $\mathfrak{m} = \overline{\mathfrak{m}} \cap R$. Then $(\overline{F}R)/\overline{\mathfrak{m}}$ is a Picard-Vessiot ring for $\delta(y) = Ay$ over $\overline{F}$ and $R/\mathfrak{m}$ embeds into $(\overline{F}R)/\overline{\mathfrak{m}}$. This implies that the field of fractions of $R/\mathfrak{m}$ does not have new constants. So $R/\mathfrak{m}$ is a Picard-Vessiot ring (over F) for $\delta(y) = Ay$ and $\mathfrak{m}$ is a maximal δ-ideal of R. Let H be the differential Galois group of $R/\mathfrak{m}$. As R/F is proto-Picard-Vessiot, we have $G^t \leq H \leq G$.

The ring compositum $\overline{F}(R/\mathfrak{m})$ of $\overline{F}$ and $R/\mathfrak{m}$ (inside the algebraic closure of the field of fractions of $R/\mathfrak{m}$) can be identified with $(\overline{F}R)/\overline{\mathfrak{m}}$. In fact, using Corollary 3.17 (applied to $R/\mathfrak{m}$), we get a map $\overline{F}(R/\mathfrak{m}) \to (\overline{F}R)/\overline{\mathfrak{m}}$ which then necessarily is an isomorphism. By Corollary 3.17, the differential Galois group of $\overline{F}(R/\mathfrak{m}) = (\overline{F}R)/\overline{\mathfrak{m}}$ is H°.

As $\mathfrak{m}$ is a nonzero prime ideal of R and R is an integral domain, we see that

$$
\dim(H) = \dim(R/\mathfrak{m}) < \dim(R) = \dim(G).
$$

Therefore H° is a proper subgroup of G°. As the identity component G°/G^t of G/G^t is a torus and H°/G^t is a proper subgroup of G°/G^t, there exists a non-trivial character of G°/G^t that is trivial on H°/G^t, i.e., there exists a non-trivial character χ of G° such that $H^\circ \subseteq \ker(\chi)$.

Let $\overline{Y} \in \mathrm{GL}_n(R/\mathfrak{m}) \subseteq \mathrm{GL}_n((\overline{F}R)/\overline{\mathfrak{m}})$ denote the image of $Y \in \mathrm{GL}_n(R)$ and set $Y' = B\overline{Y} \in \mathrm{GL}_n(\overline{F}(R/\mathfrak{m})) = \mathrm{GL}_n((\overline{F}R)/\overline{\mathfrak{m}})$. As $BY \in G^\circ(\overline{F}R)$ (Corollary 3.19), we have $Y' \in G^\circ((\overline{F}R)/\overline{\mathfrak{m}})$. For every $h \in H^\circ(k)$ we can write $h(Y') = Y'[h]$ with $[h] \in \mathrm{GL}_n(k)$. Indeed, as explained in Section 3.1, we may identify H° with a closed subgroup of $\mathrm{GL}_{n,k}$. Then

$$h(\chi(Y')) = \chi(Y'[h]) = \chi(Y')\chi([h]) = \chi(Y')$$

for every $h \in H^\circ(k)$.

Thus $\chi(Y') = f \in \overline{F} \setminus \{0\}$ by the differential Galois correspondence. Write $\chi = \prod_{i=1}^m \chi_i^{d_i}$ with $d_i \in \mathbb{Z}$. Then not all d_i are zero, because χ is non-trivial. By Lemma 3.20, we have $\delta(\chi_i(BY)) = f_i\chi_i(BY)$ for $i = 1, \ldots, m$. This is an identity in $\overline{F}R$. Taking the quotient mod $\overline{\mathfrak{m}}$ yields $\delta(\chi_i(Y')) = f_i\chi_i(Y')$ in $(\overline{F}R)/\overline{\mathfrak{m}} = \overline{F}(R/\mathfrak{m})$. So

$$\frac{\delta(f)}{f} = \frac{\delta(\chi(Y'))}{\chi(Y')} = \sum_{i=1}^m d_i \frac{\delta(\chi_i(Y'))}{\chi_i(Y')} = \sum_{i=1}^m d_i f_i.$$

Thus $f_1, \ldots, f_m$ are logarithmically dependent over $\overline{F}$.

Conversely, assume that R/F is Picard-Vessiot. Then G is the differential Galois group of R/F and $E/\overline{F}$ is a Picard-Vessiot extension with differential Galois group G°. Suppose $f_1, \ldots, f_m$ are logarithmically dependent, i.e., there are $d_1, \ldots, d_m \in \mathbb{Z}$ not all zero and $f \in \overline{F} \setminus \{0\}$ such that $\sum_{i=1}^m d_i f_i = \delta(f)/f$. Write $\chi = \prod_{i=1}^m \chi_i^{d_i}$. Then χ is a non-trivial character of G°. For $Y' = BY$, using Lemma 3.20, we obtain

$$\frac{\delta(\chi(Y'))}{\chi(Y')} = \sum_{i=1}^m d_i \frac{\delta(\chi_i(Y'))}{\chi_i(Y')} = \sum_{i=1}^m d_i f_i = \frac{\delta(f)}{f}.$$

Thus $\delta(\frac{\chi(Y')}{f}) = 0$, i.e., $\frac{\chi(Y')}{f} = \lambda \in k$. So $\chi(Y') = \lambda f \in \overline{F}$.

For every $g \in G^\circ(k)$ we can write $g(Y') = Y'[g]$ for some $[g] \in \mathrm{GL}_n(k)$, thereby identifying G° with a closed subgroup of $\mathrm{GL}_{n,k}$. Then

$$\chi(Y') = g(\chi(Y')) = \chi(g(Y')) = \chi(Y'[g]) = \chi(Y')\chi([g]),$$

for all $g \in G^\circ(k)$. This implies that χ is trivial; a contradiction. Therefore, $f_1, \ldots, f_m$ are logarithmically independent over $\overline{F}$. $\qquad\square$

Note that in case $X(G^\circ)$ is trivial, Lemma 3.23 asserts that a proto-Picard-Vessiot ring is automatically Picard-Vessiot.

Remark 3.24. *If $F = k(x)$ and R/F is Picard-Vessiot with connected differential Galois group G, then the $\vartheta \in \mathrm{Hom}_{F'}(R, \overline{F})$ in Lemma 3.23 can be chosen such that $B = \vartheta(Y)^{-1} \in \mathrm{GL}_n(F)$ and therefore also $f_1, \ldots, f_m \in F$.*

Proof. By Tsen's theorem the field $F = k(x)$ is a C_1-field and so by Steinberg's theorem every torsor for a connected linear algebraic group over F is trivial ([Ser97a, Chapter III, Section 2.3]). As R defines a torsor for G_F, we see that there exists a morphisms $\vartheta \in \mathrm{Hom}_F(R, F)$. Because G is connected, the differential Galois correspondence implies that the integral closure F' of F in R is equal to F. So $\vartheta \in \mathrm{Hom}_{F'}(R, \overline{F})$ and $\vartheta(Y)^{-1} \in \mathrm{GL}_n(F)$ as desired. $\qquad\square$

The following example illustrates Lemma 3.23

Example 3.25. Let $a, b \in F$ such that $a \in F^\times$ is not a square in F. Then $F(\eta) = F[y]/(y^2 - a)$ is a differential field extension of F. As in Example 3.6 we set

$$R = F(\eta)[y_1, y_2, y_1^{-1}, y_2^{-1}] = F[X, \tfrac{1}{\det(X)}]/(p_1, p_2) = F[Y, \tfrac{1}{\det(Y)}],$$

where $\delta(y_1) = (b + \eta)y_1$, $\delta(y_2) = (b - \eta)y_2$,

$$p_1 = X_{21}X_{22} - (b^2 - a)X_{11}X_{12}, \qquad p_2 = X_{21}X_{12} + X_{22}X_{11} - 2bX_{11}X_{12},$$

$$A = \begin{pmatrix} 0 & 1 \\ a + \delta(b) - b^2 - \frac{\delta(a)b}{2a} & 2b + \frac{\delta(a)}{2a} \end{pmatrix} \in F^{2 \times 2},$$

and $\delta(X) = AX$. Then R is an integral domain and R/F is a differential G-torsor for $\delta(y) = Ay$, where $G \leq \mathrm{GL}_{2,k}$ is the group of 2×2 monomial matrices (as seen in Example 3.6). As $G^t = 1$, it is clear that R/F is proto-Picard Vessiot.

The algebraic group G° is the diagonal torus in $\mathrm{GL}_{2,k}$ and so a basis χ_1, χ_2 of $X(G^\circ)$ is represented by X_{11} and X_{22}. The integral closure F' of F in R equals $F' = F(\eta)$. Define $\vartheta \in \mathrm{Hom}_{F'}(R, \overline{F})$ by $\vartheta(y_1) = \vartheta(y_2) = 1$. Then

$$\vartheta(Y) = \begin{pmatrix} 1 & 1 \\ b + \eta & b - \eta \end{pmatrix} \in \mathrm{GL}_2(\overline{F}) \quad \text{and} \quad \vartheta(Y) \begin{pmatrix} y_1 & 0 \\ 0 & y_2 \end{pmatrix} = Y.$$

We have

$$\delta \begin{pmatrix} y_1 & 0 \\ 0 & y_2 \end{pmatrix} = \begin{pmatrix} b + \eta & 0 \\ 0 & b - \eta \end{pmatrix} \begin{pmatrix} y_1 & 0 \\ 0 & y_2 \end{pmatrix} \text{ and } \delta(Y) = AY. \qquad (24)$$

Because $\begin{pmatrix} y_1 & 0 \\ 0 & y_2 \end{pmatrix} = BY$ for $B = \vartheta(Y)^{-1}$, the matrices defining the differential equations in (24) are related via the Gauge transformation defined by B, i.e., $BAB^{-1} + \delta(B)B^{-1} = \begin{pmatrix} b + \eta & 0 \\ 0 & b - \eta \end{pmatrix}$. Therefore,

$$f_1 = \sum_{i,j=1}^{2} \frac{\partial \chi_1}{\partial X_{ij}}(I_2)(BAB^{-1} + \delta(B)B^{-1})_{ij} = b + \eta \quad \text{and}$$

$$f_2 = \sum_{i,j=1}^{2} \frac{\partial \chi_2}{\partial X_{ij}}(I_2)(BAB^{-1} + \delta(B)B^{-1})_{ij} = b - \eta.$$

So Lemma 3.23 shows that R/F is Picard-Vessiot if and only if $b + \eta$ and $b - \eta$ are logarithmically independent over $F(\eta)$.

3.4 Logarithmic independence via residues

In the previous section (Lemma 3.23), we have seen that whether or not a proto-Picard-Vessiot ring is Picard-Vessiot, depends on the logarithmic (in)dependence of certain algebraic functions. The point of this short section is to present a criterion from [CS99] for the logarithmic independence of algebraic functions via differential forms and their residues.

In Section 4 we will then show that this criterion is preserved under many specializations.

Let F be a finite field extension of $k(x)$, i.e., F/k is a function field of one variable. Recall ([Sti09, Def. 4.2.10]) that the *residue* $\operatorname{res}_P(\omega)$ of a differential form ω of F/k at a place P of F/k is defined as $\operatorname{res}_P(\omega) = \lambda_{-1} \in k$, where $\omega = f\,dt$ with $t \in F$ a uniformizing variable at P and $f = \sum_{i=\ell}^{\infty} \lambda_i t^i$ the P-adic expansion of $f \in F$. In other words, $\operatorname{res}_P(\omega) = \operatorname{res}_{P,t}(f)$.

Let $f_1, \ldots, f_m \in F$ and set $\mathbf{f} = (f_1, \ldots, f_m)$. Let $\mathcal{P}$ be the (finite) set of places of F/k consisting of all poles of the differential forms $f_1 dx, \ldots, f_m dx$. Define

$$Z_1(\mathbf{f}, \mathcal{P}) = \left\{ (d_1, \ldots, d_m) \in \mathbb{Z}^m \,\middle|\, \sum_{i=1}^{m} d_i \operatorname{res}_P(f_i dx) \in \mathbb{Z} \; \forall P \in \mathcal{P} \text{ and } \sum_{P \in \mathcal{P}} \sum_{i=1}^{m} d_i \operatorname{res}_P(f_i dx) = 0 \right\},$$

$$Z_2(\mathbf{f}, \mathcal{P}) = \left\{ (d_1, \ldots, d_m) \in Z_1(\mathbf{f}, \mathcal{P}) \,\middle|\, \sum_{P \in \mathcal{P}} \left(\sum_{i=1}^{m} d_i \operatorname{res}_P(f_i dx) \right) P \text{ is a principal divisor of } F/k \right\}.$$

Note that $Z_1(\mathbf{f}, \mathcal{P})$ and $Z_2(\mathbf{f}, \mathcal{P})$ are submodules of $\mathbb{Z}^m$ and thus are free $\mathbb{Z}$-modules. Let $\{(e_{1,\ell}, \ldots, e_{m,\ell}) \mid \ell = 1, \ldots, n\}$ be a basis of $Z_2(\mathbf{f}, \mathcal{P})$ and for $\ell = 1, \ldots, n$ write

$$\sum_{P \in \mathcal{P}} \left(\sum_{i=1}^{m} e_{i,\ell} \operatorname{res}_P(f_i dx) \right) P = (h_\ell) \quad \text{with} \quad h_\ell \in F^{\times}.$$

For $\ell = 1, \ldots, n$, set $\omega_\ell = \left(\frac{\delta(h_\ell)}{h_\ell} - \sum_{i=1}^{m} e_{i,\ell} f_i \right) dx$.

Lemma 3.26. *The elements $f_1, \ldots, f_m$ are logarithmically independent over F if and only if $\omega_1, \ldots, \omega_n$ are $\mathbb{Z}$-linearly independent. In particular, if $Z_2(\mathbf{f}, \mathcal{P}) = 0$, then $f_1, \ldots, f_m$ are logarithmically independent over F.*

Proof. The proof of this lemma is contained in the proof of [CS99, Prop. 2.4]. For the convenience of the reader we include the details.

First assume that $f_1, \ldots, f_m$ are logarithmically independent over F. Let $d_1, \ldots, d_n \in \mathbb{Z}$ be such that $\sum_{\ell=1}^{n} d_\ell \omega_\ell = 0$. By definition of ω_ℓ, this implies $\sum_{\ell=1}^{n} d_\ell \frac{\delta(h_\ell)}{h_\ell} = \sum_{\ell=1}^{n} \sum_{i=1}^{m} d_\ell e_{i,\ell} f_i$. For $h = \prod_{\ell=1}^{n} h_\ell^{d_\ell} \in F^{\times}$, we thus have

$$\frac{\delta(h)}{h} = \sum_{\ell=1}^{n} d_\ell \frac{\delta(h_\ell)}{h_\ell} = \sum_{i=1}^{m} \left(\sum_{\ell=1}^{n} d_\ell e_{i,\ell} \right) f_i.$$

The logarithmic independence of $f_1, \ldots, f_m$ implies that $\sum_{\ell=1}^{n} d_\ell e_{i,\ell} = 0$ for $i = 1, \ldots, m$. The $\mathbb{Z}$-linear independence of the $(e_{1,\ell}, \ldots, e_{m,\ell})$'s thus yields $d_1 = \ldots = d_n = 0$ as desired.

Conversely, assume that $\omega_1, \ldots, \omega_n$ are $\mathbb{Z}$-linearly independent. Let $d_1, \ldots, d_m \in \mathbb{Z}$ and $h \in F^{\times}$ be such that $\frac{\delta(h)}{h} = \sum_{i=1}^{m} d_i f_i$. We will show that $(d_1, \ldots, d_m) \in Z_2(\mathbf{f}, \mathcal{P})$. First note that the differential form $\frac{\delta(h)}{h} dx = \frac{dh}{h}$ has only simple poles and the residues are all integers. In fact, the residue at a place P of F/K is the P-valuation of h. (This can, for example, be deduced from [Sti09, Prop. 4.2.7].) So $\sum_{i=1}^{m} d_i \operatorname{res}_P(f_i dx) = \operatorname{res}_P(\sum_{i=1}^{m} d_i f_i dx) = \operatorname{res}_P(\frac{dh}{h}) \in \mathbb{Z}$ for every place P of F/K and

$$(h) = \sum_{P} \operatorname{res}_P(\tfrac{dh}{h}) P = \sum_{P} \sum_{i=1}^{m} d_i \operatorname{res}_P(f_i dx) P,$$

where the sum is taken over all places of F/K. However, since $\mathrm{res}_P(\sum_{i=1}^m d_i f_i dx) = 0$, unless P is a pole of one of the forms $f_i dx$, the sum can be restricted to $P \in \mathcal{P}$. As principal divisors have degree zero ([Sti09, Theorem 1.4.11]), we see that $(d_1, \ldots, d_m) \in Z_1(\mathbf{f}, \mathcal{P})$ and also $(d_1, \ldots, d_m) \in Z_2(\mathbf{f}, \mathcal{P})$. Therefore, there exist $c_1, \ldots, c_n \in \mathbb{Z}$ such that $d_i = \sum_{\ell=1}^n c_\ell e_{i,\ell}$ for $i = 1, \ldots, m$. Then

$$
\begin{aligned}
\sum_{\ell=1}^n c_\ell \omega_\ell &= \sum_{\ell=1}^n c_\ell \omega_\ell - \left(\tfrac{\delta(h)}{h} - \sum_{i=1}^m d_i f_i \right) dx = \\
&= \sum_{\ell=1}^n c_\ell \left(\tfrac{\delta(h_\ell)}{h_\ell} - \sum_{i=1}^m e_{i,\ell} f_i \right) dx - \tfrac{\delta(h)}{h} dx + \sum_{i=1}^m \sum_{\ell=1}^n c_\ell e_{i,\ell} f_i dx = \\
&= \frac{\delta(h^{-1} \prod_{\ell=1}^n h_\ell^{c_\ell})}{h^{-1} \prod_{\ell=1}^n h_\ell^{c_\ell}} dx = \frac{d(h^{-1} \prod_{\ell=1}^n h_\ell^{c_\ell})}{h^{-1} \prod_{\ell=1}^n h_\ell^{c_\ell}}.
\end{aligned}
$$

By construction, the differential forms ω_ℓ have no simple poles; so $\sum_{\ell=1}^n c_\ell \omega_\ell$ has no simple pole. On the other hand, $\frac{d(h^{-1} \prod_{\ell=1}^n h_\ell^{c_\ell})}{h^{-1} \prod_{\ell=1}^n h_\ell^{c_\ell}}$ has only simple poles. This is only possible if $\sum_{\ell=1}^n c_\ell \omega_\ell = 0$.

Now the $\mathbb{Z}$-linear independence of the ω_ℓ's yields that all c_ℓ's are zero. Hence also all d_i's are zero and the f_i's are logarithmically independent as desired. $\qquad\square$

The following example illustrates Lemma 3.26

Example 3.27. Let $F = k(x, z)$ with $z^2 = x^4 + x + \alpha$ and $\alpha \in k$. We assume that the discriminant $256\alpha^3 - 27$ of $x^4 + x + \alpha$ is nonzero so that $x^4 + x + \alpha$ has four distinct roots $\alpha_3, \alpha_4, \alpha_5, \alpha_6$ in k. Let $\beta \in k$ with $\beta^4 + \beta + \alpha \neq 0$. Set $b = \frac{(x-\beta)^2}{x^4+x+\alpha} = (\frac{x-\beta}{z})^2$ and $\eta = \frac{x-\beta}{z}$. We will investigate the logarithmic independence of $f_1 = b + \eta$ and $f_2 = b - \eta$. (This choice of f_1, f_2 is motivated by Example 3.25.)

We first need to find the set $\mathcal{P}$ of poles of $f_1 dx$ and $f_2 dx$. Note that the projective curve $C' \subseteq \mathbb{P}_k^2$ defined by the affine equation $z^2 = x^4 + x + \alpha$ has a singularity at infinity.

The transformation

$$ x = -\tfrac{v+1}{2u}, \quad z = (\tfrac{v+1}{2u})^2 - \tfrac{u}{2} $$

yields a smooth model $C \subseteq \mathbb{P}_k^2$ defined by the affine equation $v^2 = u^3 - 4\alpha u + 1$. The inverse transformation is given by

$$ u = 2(x^2 - z), \quad v = -4(x^2 - z)x - 1. $$

These transformations yield an isomorphism between $C \setminus \{(0 : 1 : 1), (0 : 1 : 0)\}$ and $C' \setminus \{(0 : 1 : 0)\}$. The singular point $(0 : 1 : 0)$ of C' has two preimages in C, namely $(0 : 1 : 1)$ and $(0 : 1 : 0)$. The places of F/k are in one-to-one correspondence with $C(k)$. The inclusion $k(x) \subseteq F$ of function fields corresponds to the morphism

$$ C \to \mathbb{P}_k^1, \quad (u : v : w) \mapsto (v + w : -2u). $$

By the Hurwitz genus formula ([Sti09, Cor. 3.5.6]), this morphism has exactly four ramification points. They are $\alpha_3, \alpha_4, \alpha_5, \alpha_6 \in \mathbb{A}^1(k) \subseteq \mathbb{P}^1(k)$. Let P_3, P_4, P_5, P_6 denote the (unique) places of F/k extending the places of $k(x)$ corresponding to $\alpha_3, \alpha_4, \alpha_5, \alpha_6$. The point of $C(k)$ corresponding to P_i is $(2\alpha_i^2 : -4\alpha_i^3 - 1 : 1)$ for $i = 3, \ldots, 6$.

For a place P of F/k let ν_P denote the corresponding valuation on F. Similarly, every $\lambda \in k \cup \{\infty\}$ defines a valuation ν_λ on $k(x)$. For $a \in k(x)$ we have $\nu_{P_i}(a) = 2\nu_{\alpha_i}(a)$ for $i =$

$3, \ldots, 6$. For any other place P of F/k (i.e., $P \notin \{P_3, P_4, P_5, P_6\}$) we have $\nu_P(a) = \nu_\lambda(a)$, where λ corresponds to the restriction of P. With this preparation, one sees immediately that the poles of $b = \frac{(x-\beta)^2}{x^4+x+\alpha}$ are P_3, P_4, P_5, P_6 and $\nu_{P_i}(b) = -2$ for $i = 3, \ldots, 6$. Because $b = \eta^2$, it follows that the poles of η are P_3, P_4, P_5, P_6 and $\nu_{P_i}(\eta) = -1$ for $i = 3, \ldots, 6$.

There are two places P_1, P_2 of F/k that restrict to the infinite place of $k(x)$. They correspond to the points $(0 : 1 : 0)$ and $(0 : 1 : 1)$ of $C(k)$. Then the poles of x are P_1, P_2 and $\nu_{P_i}(x) = -1$ for $i = 1, 2$.

Set $\mathcal{P} = \{P_1, \ldots, P_6\}$. Then the poles of bdx and ηdx belong to $\mathcal{P}$, because outside of $\mathcal{P}$ neither b, η or x has a singularity. As $\nu_{P_i}(\frac{1}{x}) = 1$ for $i = 1, 2$ we can use x^{-1} as a uniformizer at P_1, P_2. Then $bdx = -bx^2 d(x^{-1})$ and so $\nu_{P_i}(bdx) = \nu_{P_i}(-bx^2) = \nu_\infty(-bx^2) = 0$. Hence P_1, P_2 are not poles of bdx.

As
$$\nu_{P_i}(z^2) = \nu_{P_i}(x^4 + x + \alpha) = 2\nu_{\alpha_i}(x^4 + x + \alpha) = 2,$$
for $i = 3, \ldots, 6$, we see that z is a uniformizer at P_3, P_4, P_5, P_6. From $z^2 = x^4 + x + \alpha$ it follows that $\delta(z) = \frac{4x^3+1}{2z}$ and so

$$bdx = \frac{(x-\beta)^2 2z}{z^2(4x^3+1)}dz = \frac{2(x-\beta)^2}{(4x^3+1)z}dz.$$

Therefore $\nu_{P_i}(bdx) = -1$ for $i = 3, \ldots, 6$. Thus the poles of bdx are P_3, P_4, P_5, P_6.

For $i = 1, 2$ we have $\nu_{P_i}(b) = 2$ and so $\nu_{P_i}(\eta) = 1$. It follows that

$$\nu_{P_i}(\eta dx) = \nu_{P_i}(-\eta x^2 d(x^{-1})) = \nu_{P_i}(-\eta x^2) = -1$$

for $i = 1, 2$. So P_1, P_2 are poles of ηdx. On the other hand, $\eta dx = \frac{2\eta z}{4x^3+1}dz$ and so $\nu_{P_i}(\eta dx) = 0$ for $i = 3, \ldots, 6$. So the poles of ηdx are P_1, P_2.

In summary, we see that the poles of $f_1 dx$ as well as of $f_2 dx$ are exactly $\mathcal{P}$.

We next compute the residues. As $\nu_{P_i}(x - \alpha_i) = 2$ for $i = 3, \ldots, 6$, the P_i-adic expansion of $x - \alpha_i$ is of the form $c_i z^2 + \ldots$ with $c_i \in k^\times$. Substituting $x = \alpha_i + c_i z^2 + \ldots$ we find

$$bdx = \frac{2(x-\beta)^2}{(4x^3+1)z}dz = \frac{2(\alpha_i - \beta + c_i z^2 + \ldots)^2}{4(\alpha_i + c_i z^2 + \ldots)^3 + 1}\frac{1}{z}dz = \left(\frac{2(\alpha_i-\beta)^2}{4\alpha_i^3 + 1}\frac{1}{z} + \ldots\right)dz.$$

Therefore $\operatorname{res}_{P_i}(bdx) = \frac{2(\alpha_i-\beta)^2}{4\alpha_i^3+1}$ for $i = 3, \ldots, 6$. We next compute $\operatorname{res}_{P_i}(\eta dx)$ for $i = 1, 2$.

As $\nu_{P_i}(z^2) = \nu_{P_i}(x^4 + x + \alpha) = -4$, we see that $\nu_{P_i}(z) = -2$ for $i = 1, 2$. So the P_i-adic expansion of z is of the form $z = c_i(x^{-1})^{-2} + \ldots$ with $c_i \in K^\times$ for $i = 1, 2$. We have

$$\eta dx = -\eta x^2 d(x^{-1}) = \frac{-(x-\beta)x^2}{z}d(x^{-1}) = \frac{-(x^{-1})^{-3} + \beta(x^{-1})^{-2}}{c_i(x^{-1})^{-2} + \ldots}d(x^{-1})$$

and so $\operatorname{res}_{P_i}(\eta dx) = -1/c_i$.

Plugging $z = c_i(x^{-1})^{-2} + \ldots$ into $z^2 = x^4 + x + \alpha$ we find $(c_i(x^{-1})^{-2} + \ldots)^2 = (x^{-1})^{-4} + \ldots$ and so $c_i \in \{1, -1\}$ for $i = 1, 2$. Suppose $c_1 = c_2$. Then $\frac{z}{x^2}$ and $\frac{1}{x}$ are rational functions on C that take the same value in k on P_1 and P_2 and $F = k(\frac{z}{x^2}, \frac{1}{x})$. Thus $P_1 = P_2$; a contradiction. So $c_1 \neq c_2$. To find the exact value of c_i we can evaluate $\frac{z}{x^2} = 1 - \frac{2u^3}{(v+1)^2}$ at the point $(0 : 1 : 1)$ corresponding to P_2. This yields $c_2 = 1$ and so $c_1 = -1$. Thus $\operatorname{res}_{P_1}(\eta dx) = 1$ and $\operatorname{res}_{P_2}(\eta dx) = -1$.

With this information at hand we can now calculate

$$Z_1((f_1, f_2), \mathcal{P}) = \left\{(d_1, d_2) \in \mathbb{Z}^2 \;\middle|\; \sum_{i=1}^2 d_i \operatorname{res}_P(f_i dx) \in \mathbb{Z} \; \forall P \in \mathcal{P} \text{ and } \sum_{P \in \mathcal{P}} \sum_{i=1}^2 d_i \operatorname{res}_P(f_i dx) = 0\right\}.$$

Note that for P_i ($i = 3, \ldots, 6$), the first condition is $(d_1 + d_2)\frac{2(\alpha_i - \beta)^2}{4\alpha_i^3 + 1} \in \mathbb{Z}$, whereas for P_1, P_2 the first condition is vacuous, because $\mathrm{res}_{P_i}(f_j) \in \mathbb{Z}$ for $i = 1, 2$. There indeed exist $\alpha, \beta \in k$ such that $\frac{2(\alpha_i - \beta)^2}{4\alpha_i^3 + 1} \in \mathbb{Q}$ for $i = 3, \ldots, 6$, for example, $\alpha = 0$ and $\beta = \frac{1}{2}$.

Set $r = \prod_{i=3}^{6} \frac{(\alpha_i - \beta)^2}{4\alpha_i^3 + 1}$. A direct calculation shows that $r = \frac{(\beta^4 + \beta + \alpha)^2}{256\alpha^3 - 27}$. Thus, the first condition mentioned above, implies that $r \in \mathbb{Q}$ if $d_1 + d_2 \neq 0$.

Assume that $r \notin \mathbb{Q}$. Then

$$Z_1((f_1, f_2), \mathcal{P}) = \{(-d, d) \in \mathbb{Z}^2 \mid d \in \mathbb{Z}\}$$

and for $(-d, d) \in Z_1((f_1, f_2), \mathcal{P})$ we have

$$\sum_{P \in \mathcal{P}} \left(\sum_{i=1}^{2} d_i \, \mathrm{res}_P(f_i dx) \right) P = -2dP_1 + 2dP_2 = 2d(P_2 - P_1)$$

and so

$$Z_2((f_1, f_2), \mathcal{P}) = \{(-d, d) \in \mathbb{Z}^2 \mid 2d(P_2 - P_1) \text{ is a principal divisor of } F/k\}.$$

Recall (see e.g., [Sti09, Prop. 6.1.6]) that the choice of a point of $C(k)$ defines a bijection between the degree zero divisor class group $\mathrm{Cl}^0(F/k)$ and $C(k)$. As usual, we choose the point to be $(0 : 1 : 0) \in C(k)$. Thus the point $(0 : 1 : 0)$ corresponding to P_1 is the neutral element of the group $C(k)$. Then $2d(P_2 - P_1)$ is principal, i.e., equal to zero in $\mathrm{Cl}^0(F/k)$, if and only if $2d(0 : 1 : 1) = 0$ in $C(k)$. Therefore $Z_2((f_1, f_2), \mathcal{P})$ is trivial if and only if the point $(0, 1)$ is not a torsion point of the elliptic curve $v^2 = u^3 - 4\alpha u + 1$. In this case f_1, f_2 are logarithmically independent over F by Lemma 3.26. It is not easy to exactly determine the values of α for which $(0, 1)$ is a torsion point, but this question will be further discussed in Example 4.28.

If $(0, 1)$ is a torsion point, then a basis of $Z_2((f_1, f_2), \mathcal{P})$ is given by $e_1 = (-e, e)$, where $2e$ is the order of $(0, 1)$ in $C(k)$. One can then write $2e(P_2 - P_1) = (h_1)$ with $h_1 \in F^\times$. In this case, f_1, f_2 are logarithmically independent if and only if

$$\frac{\delta(h_1)}{h_1} - (-e)f_1 - ef_2 = \frac{\delta(h_1)}{h_1} + 2e\eta$$

is nonzero. The latter questions will also be further discussed in Example 4.28.

3.5 Exponential bounds for linear differential operators

A solution h of a homogeneous scalar linear differential equation over $k(x)$ is an *exponential solution* if its logarithmic derivative $\delta(h)/h$ lies in $k(x)$, i.e., h satisfies $\delta(h) = ah$, with $a \in k(x)$. The goal of this section is to describe a fairly explicit bound on the degrees of the logarithmic derivatives of the exponential solutions.

We will work with the (non-commutative) ring $k(x)[\delta]$ of linear differential operators with coefficients in $k(x)$ (as defined in [vdPS03, Section 2.1]). Thus a (scalar) linear differential equation

$$\delta^n(y) + a_{n-1}\delta^{n-1}(y) + \ldots + a_0 y = 0$$

with $a_0, \ldots, a_n \in k(x)$, can be written more succinctly as $Ly = 0$, where

$$L = \delta^n + a_{n-1}\delta^{n-1} + \ldots + a_0 \in k(x)[\delta]$$

is the corresponding linear differential operator.

A nonzero solution h of $Ly = 0$ (in some Picard-Vessiot extension of $k(x)$) is called an *exponential solution* of $Ly = 0$ if $\delta(h)/h \in k(x)$. The reader is referred to Section 4.1 of [vdPS03] for more background on exponential solutions and their computation.

Recall that the *degree* of a nonzero rational function $a = \frac{a_1}{a_2} \in k(x)$ with $a_1, a_2, \in k[x]$ relatively prime, is defined as $\deg(a) = \max\{\deg(a_1), \deg(a_2)\}$. By convention, $\deg(0) = -\infty$.

Definition 3.28. *An integer N is an* exponential bound *for $Ly = 0$, if $\deg(\delta(h)/h) \leq N$ for any exponential solution h of $Ly = 0$ (belonging to some Picard-Vessiot extension of $k(x)$).*

The main point of this section is to describe an exponential bound $N(L)$ for $Ly = 0$ that is well-behaved under specialization. This bound is also described in the second paragraph on page 109 of [vdPS03].

The elements $u \in k(x)$ of the form $u = \delta(h)/h$ for some exponential solution h of $Ly = 0$ are exactly the solutions of the Riccati equation associated with $Ly = 0$ ([vdPS03, Def. 4.6]). Another description of these u's is, as the set of elements of $k(x)$ such that $\delta - u \in k(x)[\delta]$ is a right-hand factor of L.

To describe the bound $N(L)$ we need to introduce some notation from [vH97b] and [vH97a]. Set $\bar{\delta} = x\delta$. Then $k(x)[\delta] = k(x)[\bar{\delta}]$, i.e., every operator in δ can be rewritten as an operator in $\bar{\delta}$. Set

$$\mathbb{E} = \bigcup_{r \in \mathbb{Z}_{>0}} k[x^{-1/r}]$$

and let $e \in \mathbb{E}$. The *ramification index* $\mathrm{ram}(e)$ of e is the minimal r such that $e \in k[x^{-1/r}]$. For $L \in k(x)[\bar{\delta}]$, or more generally, for $L \in k((x))[\bar{\delta}]$ we set $S_e(L) = L(\bar{\delta} + e) \in k((x^{-1/r}))[\bar{\delta}]$ and write

$$S_e(L) = \sum_{i \geq \ell} x^{i/r} N_{i,e,L}(\bar{\delta}),$$

where $N_{i,e,L} \in k[T]$ (with T a new variable) and $N_{\ell,e,L} \neq 0$. Following [vH97b, Section 3.4] $N_{\ell,e,L}$ is called the *Newton polynomial* of $S_e(L)$ at 0 for slope 0. Let $m_{e,0}(L)$ be the multiplicity of 0 in $N_{\ell,e,L}(T)$. Following [vH97a, Def. 3.1], we define the generalized exponents of L:

Definition 3.29. *An element $e \in \mathbb{E}$ is a* generalized exponent *of L at 0 if $m_{e,0}(L) > 0$.*

The number $m_{e,0}(L)$ is called the *multiplicity* of e in L. By (3.3) on page 542 of [vH97a], we have

$$\sum_{e \in \mathbb{E}} m_{e,0}(L) = \mathrm{ord}(L)(= n). \tag{25}$$

In particular, L only has finitely many generalized exponents at 0.

Example 3.30. Let us determine the generalized exponents for the linear differential operator $L = \delta^2 + \frac{1}{x}\delta + 1 - (\frac{\alpha}{x})^2 \in k(x)[\delta]$ corresponding to Bessel's differential equation, where α is an arbitrary element of k. Rewriting L in terms of $\bar{\delta}$, we have $L = \frac{1}{x^2}\bar{\delta}^2 + 1 - (\frac{\alpha}{x})^2$. So, after normalizing (which does not effect the generalized exponents), the relevant operator is $L' = \bar{\delta}^2 + x^2 - \alpha^2$. For $e \in \mathbb{E}$ we have

$$L'(\bar{\delta} - e) = (\bar{\delta} - e)^2 + x^2 - \alpha^2 = \bar{\delta}^2 - 2e\bar{\delta} - x\delta(e) + e^2 + x^2 - \alpha^2.$$

Thus, choosing $e \in \{\alpha, -\alpha\}$, we have $L'(\bar{\delta} - e) = \bar{\delta}^2 - 2e\bar{\delta} + x^2$, which has Newton polynomial $T^2 - 2eT$. By (25), the generalized exponents of L are α and $-\alpha$. In case $\alpha = 0$, the generalized exponent $e = 0$ has multiplicity two.

Remark 3.31. *Due to Lemma 3.4 of [vH97a], if $\bar{\delta} - u \in k((x))[\bar{\delta}]$ is a right-hand factor of $L \in k(x)[\bar{\delta}] \subseteq k((x))[\bar{\delta}]$, then $u = e + u'$, where $e \in k[x^{-1}]$ is a generalized exponent of L at 0 with $\mathrm{ram}(e) = 1$ and $u' \in xk[[x]]$. However, this can also be seen directly: If $L = L_1 \cdot (\bar{\delta} - u)$ is a factorization in $k((x))[\bar{\delta}]$, and u is written as $u = e + u'$ with $e \in k[x^{-1}]$ and $u' \in xk[[x]]$, then $S_e(L) = S_e(L_1) \cdot (\bar{\delta} - u')$, which has a Newton polynomial vanishing at zero, because for every power of x occurring in $S_e(L_1)u'$, there is a smaller power of x occurring in $S_e(L_1)\bar{\delta}$.*

In order to define the generalized exponents at a point $\lambda \in \mathbb{P}^1(k) = k \cup \{\infty\}$ different from 0, we introduce (following [vH97a, Section 3.4]) the k-algebra automorphism

$$l_\lambda : k(x)[\delta] \to k(x)[\delta]$$

as follows: if $\lambda \in k$, then $l_\lambda(x) = x + \lambda$ and $l_\lambda(\delta) = \delta$, otherwise $l_\infty(x) = 1/x$ and $l_\infty(\delta) = -x^2\delta$. For $e \in \mathbb{E}$ set $m_{e,\lambda}(L) = m_{e,0}(l_\lambda(L))$.

Definition 3.32. *If $m_{e,\lambda}(L) > 0$, then e is called a generalized exponent of L at λ and $m_{e,\lambda}(L)$ is called the multiplicity of e in L at λ.*

Since we are only interested in the factors of $L \in k(x)[\delta]$ that are of the form $\delta - u$ with $u \in k(x)$, we only need to consider the generalized exponents e of L with $\mathrm{ram}(e) = 1$. However, generalized exponents with ramification index larger than 1 are necessary for (25) to hold and this formula is crucial for showing that our exponential bound is preserved under many specializations (Proposition 4.3). We will next explain how Remark 3.31 can be used to obtain the possible principal parts of an exponential solution of L.

Before proceeding, let us recall some terminology for rational function. The *principal part* of an element $u \in k(x)$ at $\lambda \in k$ is $\sum_{i=\ell}^{-1} u_i(x - \lambda)^i$, when $u = \sum_{i=\ell}^{\infty} u_i(x - \lambda_i)^i$ is written as an element of $k((x - \lambda))$. The *residue* $\mathrm{res}_\lambda(u)$ of u at λ is $\mathrm{res}_\lambda(u) = u_{-1}$. The *order* $\mathrm{ord}_\lambda(u)$ of u at λ is $\mathrm{ord}_\lambda(u) = -\ell$, where $u_\ell \neq 0$. By convention, $\mathrm{ord}_\lambda(0) = 0$.

The residue at infinity is defined as $\mathrm{res}_\infty(u) = \mathrm{res}_0(-\frac{1}{x^2}u(\frac{1}{x}))$, while the order at infinity is $\mathrm{ord}_\infty(u) = \mathrm{ord}_0(u(\frac{1}{x}))$. These definitions are such that the sum of all residues of u is zero (see e.g. [Sti09, Cor. 4.3.3]).

The principal part of u at ∞ is $\sum_{i=\ell}^{1} u_i x^{-i}$, when $u = \sum_{i=\ell}^{\infty} u_i x^{-i}$ is written as an element of $k((x^{-1}))$. This definition is such that $\mathrm{res}_\infty(u)$ can be determined (as $-u_1$) from the principal part at infinity.

Assume that $e \in \mathbb{E}$ is a generalized exponent of L at λ with $\mathrm{ram}(e) = 1$. We set

$$\mathrm{pp}(e, \lambda) = \begin{cases} \frac{l_{-\lambda}(e)}{x - \lambda} & \text{if } \lambda \in k \\ -\frac{l_\infty(e)}{x} & \text{if } \lambda = \infty. \end{cases}$$

Lemma 3.33. *Let $u \in k(x)$ be such that $\delta - u$ is a right-hand factor of L. Then, for every $\lambda \in \mathbb{P}^1(k)$, the principal part of u at λ is of the form $\mathrm{pp}(e, \lambda)$ for some generalized exponent e of L at λ with $\mathrm{ram}(e) = 1$.*

Proof. We write $L = L_1 \cdot (\delta - u)$, with $L_1 \in k(x)[\delta]$. First assume that $\lambda \in k$. Applying l_λ yields $l_\lambda(L) = l_\lambda(L_1) \cdot (\delta - l_\lambda(u)) = L_2 \cdot (\bar{\delta} - xl_\lambda(u))$ for some $L_2 \in k(x)[\bar{\delta}]$. By Remark 3.31, $xl_\lambda(u) = e + u'$, where $e \in \mathbb{E}$ is a generalized exponent of L at λ with $\mathrm{ram}(e) = 1$ and

45

$u' \in xk[[x]]$. Applying $l_{-\lambda}$ to $xl_{\lambda}(u) = e + u'$, we find $u = \frac{l_{-\lambda}(e)}{x-\lambda} + \frac{l_{-\lambda}(u')}{x-\lambda}$. Thus $\frac{l_{-\lambda}(e)}{x-\lambda}$ is the principal part of u at λ.

Now let us consider the case $\lambda = \infty$. We have

$$l_{\infty}(L) = l_{\infty}(L_1) \cdot (-x^2\delta - l_{\infty}(u)) = l_{\infty}(L_1) \cdot (-x\bar{\delta} - l_{\infty}(u)) = L_2 \cdot \left(\bar{\delta} - \frac{-l_{\infty}(u)}{x}\right).$$

Therefore, as above, by Remark 3.31, we have $\frac{-l_{\infty}(u)}{x} = e + u'$, where e is a generalized exponent of L at ∞ with $\mathrm{ram}(e) = 1$ and $u' \in xk[[x]]$. Applying $(l_{\infty})^{-1} = l_{\infty}$, we obtain $u = -\frac{l_{\infty}(e) + l_{\infty}(u')}{x}$. This implies the claim. $\qquad\square$

For $\lambda \in \mathbb{P}^1(k) = k \cup \{\infty\}$ we set

$$\mathrm{PP}(L, \lambda) = \{\mathrm{pp}(e, \lambda) \mid e \in \mathbb{E} \text{ is a generalized exponent of } L \text{ at } \lambda \text{ with } \mathrm{ram}(e) = 1\}.$$

With $\mathrm{Sing}(L) \subseteq k$ we denote the set of all singular points of L, i.e., the elements of k that are poles of one of the coefficients a_i of L. Write $\mathrm{Sing}(L) \cup \{\infty\} = \{\lambda_1, \dots, \lambda_m\}$ and define

$$
\begin{aligned}
\Phi_L : \mathrm{PP}(L, \lambda_1) \times \cdots \times \mathrm{PP}(L, \lambda_m) &\longrightarrow & k \\
(f_1, \dots, f_m) &\longmapsto & -\sum_{i=1}^{m} \mathrm{res}_{\lambda_i}(f_i)
\end{aligned}
$$

and

$$N(L) = \max\{\{0\} \cup (\mathrm{Im}(\Phi_L) \cap \mathbb{Z})\} + \sum_{\lambda \in \mathrm{Sing}(L) \cup \{\infty\}} \max_{f \in \mathrm{PP}(L,\lambda)} \mathrm{ord}_{\lambda}(f).$$

Lemma 3.34. *The number $N(L)$ is an exponential bound for $Ly = 0$.*

Proof. Let h be an exponential solution of $Ly = 0$ and set $u = \delta(h)/h \in k(x)$. We have to show that $\deg(u) \le N(L)$. As u is a solution of the Riccati equation associated with $Ly = 0$, it follows from (4.3) on page 107 of [vdPS03], that u is of the form

$$u = \frac{\delta(p_1)}{p_1} + q_1 + \frac{p_2}{q_2}, \tag{26}$$

where $p_i, q_i \in k[x]$, $\deg(p_2) < \deg(q_2)$, the zeros of q_2 are in $\mathrm{Sing}(L)$ and the zeros of p_1 are not in $\mathrm{Sing}(L)$.

Note that the partial fraction decomposition of $\frac{\delta(p_1)}{p_1}$ is of the form $\sum_{i=1}^{d} \frac{n_i}{x - \lambda'_i}$, with $n_i \in \mathbb{N}$, $n_1 + \dots + n_d = \deg(p_1)$ and $\lambda'_i \in k \setminus \mathrm{Sing}(L)$. The partial fraction decomposition of $\frac{p_2}{q_2}$ is a sum of terms of the form $\sum_{i=1}^{d} \frac{\lambda'_i}{(x-\lambda)^i}$ with $\lambda'_i \in k$ and $\lambda \in \mathrm{Sing}(L)$. The polynomial q_1 can be thought of as the contribution at ∞.

By Lemma 3.33 we have

$$\mathrm{ord}_{\lambda}(u) \le \max_{f \in \mathrm{PP}(L,\lambda)} \{\mathrm{ord}_{\lambda}(f)\}$$

for any $\lambda \in \mathbb{P}^1(k)$. As $\mathrm{ord}_{\lambda}(q_1 + \frac{p_2}{q_2}) \le \mathrm{ord}_{\lambda}(u)$ for $\lambda \in \mathrm{Sing}(L) \cup \{\infty\}$, this yields $\mathrm{ord}_{\lambda}(q_1 + \frac{p_2}{q_2}) \le \max_{f \in \mathrm{PP}(L,\lambda)} \{\mathrm{ord}_{\lambda}(f)\}$ for $\lambda \in \mathrm{Sing}(L) \cup \{\infty\}$. Thus

$$\deg(q_1 + \tfrac{p_2}{q_2}) \le \sum_{\lambda \in \mathrm{Sing}(L) \cup \{\infty\}} \mathrm{ord}_{\lambda}(q_1 + \tfrac{p_2}{q_2}) \le \sum_{\lambda \in \mathrm{Sing}(L) \cup \{\infty\}} \max_{f \in \mathrm{PP}(L,\lambda)} \mathrm{ord}_{\lambda}(f). \tag{27}$$

To also bound $\deg(p_1)$, let $B \subseteq k$ be the set of poles of u that are not in $\mathrm{Sing}(L)$. Then B is the set of zeros of p_1. Moreover, q_1 and $\frac{p_2}{q_2}$ have residue zero at any point of B. Therefore

$$\sum_{\lambda \in B} \mathrm{res}_\lambda(u) = \sum_{\lambda \in B} \mathrm{res}_\lambda\left(\frac{\delta(p_1)}{p_1}\right) = \deg(p_1).$$

As $\mathrm{Sing}(L) \cup B \cup \{\infty\}$ contains all poles of u, we have

$$0 = \sum_{\lambda \in \mathrm{Sing}(L) \cup B \cup \{\infty\}} \mathrm{res}_\lambda(u) = \deg(p_1) + \sum_{\lambda \in \mathrm{Sing}(L) \cup \{\infty\}} \mathrm{res}_\lambda(u).$$

On the other hand, $\mathrm{res}_\lambda(u) = \mathrm{res}_\lambda(f)$ for some $f \in \mathrm{PP}(L, \lambda)$. Therefore $\deg(p_1) \in \mathrm{Im}(\Phi_L) \cap \mathbb{Z}$. So $\deg(p_1) \leq \max\{\{0\} \cup (\mathrm{Im}(\Phi_L) \cap \mathbb{Z})\}$. Combing this with (26) and (27) yields the claim of the lemma. $\qquad\square$

Example 3.35. Let us determine the exponential bound $N(L)$ from Lemma 3.34 for the linear differential operator $L = \delta^2 + \frac{1}{x}\delta + 1 - \left(\frac{\alpha}{x}\right)^2 \in k(x)[\delta]$ corresponding to Bessel's differential equation. Note that $\mathrm{Sing}(L) = \{0\}$. We already determined the generalized exponents of L at 0 in Example 3.30. They are α and $-\alpha$. Thus $\mathrm{PP}(L, 0) = \{\frac{\alpha}{x}, \frac{-\alpha}{x}\}$.

To compute $N(L)$, we also need to determine the generalized exponents at ∞. We have $l_\infty(L) = (-x^2\delta)^2 - x^3\delta + 1 - (\alpha x)^2 = x^2\bar\delta^2 + 1 - (\alpha x)^2$. So, after normalizing, the relevant operator is $L' = \bar\delta^2 + \frac{1}{x^2} - \alpha^2$. For $e \in \mathbb{E}$, we have $L'(\bar\delta - e) = \bar\delta^2 - 2e\bar\delta - x\delta(e) + e^2 + \frac{1}{x^2} - \alpha^2$. Let i and $-i$ denote the roots of the polynomial $T^2 + 1$ in k. For $e = \frac{i}{x} - \frac{1}{2}$ we find $L'(\bar\delta - e) = \bar\delta^2 - \left(\frac{2i}{x} - 1\right)\bar\delta + \frac{1}{4} - \alpha^2$, which has Newton polynomial $2iT$. Similarly, for $e = \frac{-i}{x} - \frac{1}{2}$, one finds the Newton polynomial $-2iT$. Thus, by (25), the generalized exponents of L at $p = \infty$ are $\frac{i}{x} - \frac{1}{2}$ and $\frac{-i}{x} - \frac{1}{2}$. Therefore $\mathrm{PP}(L, \infty) = \{i + \frac{1}{2x}, -i + \frac{1}{2x}\}$. The image of $\Phi_L \colon \mathrm{PP}(L, 0) \times \mathrm{PP}(L, \infty) \to k$ is $\{-\alpha - \frac{1}{2}, \alpha - \frac{1}{2}\}$.

Let us first assume that $\alpha - \frac{1}{2}$ is not an integer. Then $\mathrm{Im}(\Phi_L) \cap \mathbb{Z} = \emptyset$ and it follows that $N(L) = 1$. More precisely, if $u \in k(x)$ is a solution of the Riccati equation associated with $Ly = 0$ and $u = \frac{\delta(p_1)}{p_1} + q_1 + \frac{p_2}{q_2}$ is written as in (26), then the proof of Lemma 3.34 shows that $\deg(p_1) = 0$, i.e., $\frac{\delta(P_1)}{P_1} = 0$. Moreover, the only possibilities for $q_1 + \frac{p_2}{q_2}$ are $i + \frac{\alpha}{x}$, $-i + \frac{\alpha}{x}$, $i - \frac{\alpha}{x}$, $-i - \frac{\alpha}{x}$. These are not solutions of the Riccati equation

$$\delta(u) + u^2 + \frac{1}{x}u + 1 - \left(\frac{\alpha}{x}\right)^2 = 0$$

associated with $Ly = 0$. Thus, there are no exponential solutions in this case.

Now assume that $\alpha - \frac{1}{2} \in \mathbb{Z}$. Then $\max\{\{0\} \cup (\mathrm{Im}(\Phi_L) \cap \mathbb{Z})\} = |\alpha| - \frac{1}{2}$. Therefore $N(L) = |\alpha| + \frac{1}{2}$. In this case there are indeed exponential solutions. The interested reader can find their explicit form in the Appendix of [Kol68].

3.6 Linear relations

Let F be a differential field and R/F a Picard-Vessiot ring. For a vector $v \in R^\ell$ satisfying $\delta(v) = A'v$ for some $A' \in F^{\ell \times \ell}$ we set

$$\mathrm{LinRel}(v, F) = \{p \in F[y_1, \ldots, y_\ell] \mid p \text{ is linear homogeneous and } p(v) = 0\}.$$

Then $\mathrm{LinRel}(v, F)$ is an F-vector space of dimension at most ℓ; the vector space of linear relations among the entries of v. The main goal of this section is to describe, in the case $F = k(x)$, with the help of Section 3.5, a bound N such that $\mathrm{LinRel}(v, F)$ has a basis

consisting of elements of the form $a_1 y_1 + \ldots + a_\ell y_\ell$, with $a_1, \ldots, a_\ell \in k(x)$ and $\deg(a_i) \leq N$ for $i = 1, \ldots, \ell$.

By the cyclic vector lemma, any linear differential system $\delta(y) = Ay$, with $A \in k(x)^{n \times n}$ is equivalent to a scalar linear differential equation $Ly = 0$ with $L = \delta^n + a_{n-1}\delta^{n-1} + \ldots + a_0 \in k(x)[\delta]$, i.e., there exists a matrix $T \in \mathrm{GL}_n(k(x))$ such that $T^{-1}AT + \delta(T^{-1})T$ is of the form

$$\begin{pmatrix} 0 & 1 & 0 & & & \\ & \ddots & \ddots & \ddots & & \\ & & 0 & 1 & 0 \\ & & & 0 & 1 \\ -a_0 & -a_1 & \ldots & \ldots & -a_{n-1} \end{pmatrix} \in k(x)^{n \times n}.$$

We call such a T a *transformation matrix* from $\delta(y) = Ay$ to $Ly = 0$. Furthermore, $\deg(T)$ is defined as the maximum of all degrees of entries of T.

To a linear differential system $\delta(y) = Ay$, with $A \in k(x)^{n \times n}$, one can associate, for every $i = 1, \ldots, n$, a new linear differential system $\delta(y) = (\bigwedge^i A)y$ with $\bigwedge^i A \in k(x)^{\binom{n}{i} \times \binom{n}{i}}$. If one works with differential modules (as in [vdPS03, Section 2.2]) and M is the differential module associated with $\delta(y) = Ay$, then $\bigwedge^i M$ is the differential module associated with $\delta(y) = (\bigwedge^i A)y$.

Lemma 3.36. *Let $v \in R^\ell$ be a solution of $\delta(y) = A'y$, where $A' \in k(x)^{\ell \times \ell}$ and $R/k(x)$ is a Picard-Vessiot ring (not necessarily for $\delta(y) = A'y$). Let d be the dimension of the $k(x)$-vector space generated by the entries of v and let $T \in k(x)^{m \times m}$ ($m = \binom{\ell}{d}$) be a transformation matrix from $\delta(y) = (\bigwedge^d A')y$ to $Ly = 0$, where $L \in k(x)[\delta]$. Furthermore, let N be an exponential bound for L.*

Then $\mathrm{LinRel}(v, k(x))$ has a $k(x)$-basis consisting of elements of the form $a_1 y_1 + \ldots + a_\ell y_\ell$, with $a_1, \ldots, a_\ell \in k(x)$ and $\deg(a_i) \leq 2m\deg(T) + m(m-1)N$ for $i = 1, \ldots, \ell$.

Proof. Write $v = (v_1, \ldots, v_\ell)^t \in R^\ell$. Without loss of generality, we may assume that $v_1, \ldots, v_d$ are linearly independent over $k(x)$. For $i = d+1, \ldots, \ell$, write

$$v_i = \sum_{j=1}^d a_{i,j} v_j, \quad a_{i,j} \in k(x). \tag{28}$$

Then $\left(y_i - \sum_{j=1}^d a_{i,j} y_j\right)_{i=d+1,\ldots,\ell}$ is a $k(x)$-basis of $\mathrm{LinRel}(v, k(x))$ and our goal is to bound $\deg(a_{i,j})$. Let V be the k-subspace of R^ℓ generated by $\{g(v)|\ g \in G(k)\}$, where G is the differential Galois group of $R/k(x)$. We claim that $\dim_k V = d$. Set

$$\mathrm{Rel}(V) = \{(a_1, \ldots, a_\ell)^t \in k(x)^\ell|\ a_1 u_1 + \ldots + a_\ell u_\ell = 0 \ \forall\ u = (u_1, \ldots, u_\ell)^t \in V\}.$$

From (28) it follows that $u_i = \sum_{j=1}^d a_{i,j} u_i$ for every $(u_1, \ldots, u_\ell)^t \in V$ and $i = d+1, \ldots, \ell$. On the other hand, $v_1, \ldots, v_d$ are $k(x)$-linearly independent. Thus $\mathrm{Rel}(V)$ is a $k(x)$-vector space of dimension $\ell - d$.

We will show (cf. [BBH88, Prop. 1.5]) that also $\dim_{k(x)} \mathrm{Rel}(V) = \ell - \dim_k V$. Let $b_1, \ldots, b_r$ be a basis of V and let $B \in R^{\ell \times r}$ be the matrix with columns $b_1, \ldots, b_r$. As $b_1, \ldots, b_r$ are solutions of $\delta(y) = A'y$, their k-linear independence, implies their E-linear independence, where E is the field of fractions of R ([vdPS03, Lemma 1.7]). Thus there exists an $r \times r$-submatrix $C \in \mathrm{GL}_r(E)$ of B. As $g \in G(k)$ acts on B and C via right

48

multiplication with a matrix in $\mathrm{GL}_r(k)$, we see that BC^{-1} is fixed by g. So $BC^{-1} \in k(x)^{\ell \times r}$ by the differential Galois correspondence. We have

$$\mathrm{Rel}(V) = \{a \in k(x)^\ell \mid aB = 0\} = \{a \in k(x)^\ell \mid aBC^{-1} = 0\}.$$

Since $BC^{-1} \in k(x)^{\ell \times r}$ has linearly independent columns, we see that $\dim_{k(x)} \mathrm{Rel}(V) = \ell - r = \ell - \dim_k(V)$. Therefore $\dim_k V = d$ as claimed.

Let $b_1, \ldots, b_d$ be a k-basis of V. For a vector or a matrix w, denote by $w^{(i)}$ the i-th row of w. For $I = (n_1, \ldots, n_d)$ with $1 \leq n_1 < n_2 < \cdots < n_d \leq \ell$, set $b_I = \det((b_j^{(n_i)})_{1 \leq i,j \leq d}) \in R$. A calculation, that is probably best understood by using the exterior power of the associated differential module ([vdPS03, Lemma 2.27]), shows that

$$\delta(b_I) = \sum_{\substack{J=(m_1,\ldots,m_d) \\ 1 \leq m_1 < m_2 < \cdots < m_d \leq \ell}} a_{I,J} b_J, \tag{29}$$

where $a_{I,J} \in k(x)$ and $\bigwedge^d A' = (a_{I,J}) \in k(x)^{m \times m}$. That is, the vector $(b_I)_I \in R^m$ is a solution of $\delta(y) = (\bigwedge^d A')y$. We extend the definition of the $a_{i,j}$'s from (28) to all values of $i \in \{1, \ldots, \ell\}$ by

$$a_{i,j} = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise} \end{cases}$$

for $i = 1, \ldots, d$ and $j = 1, \ldots, d$. Then (28) is true for all values of $i \in \{1, \ldots, \ell\}$ and so $b_n^{(i)} = \sum_{j=1}^d a_{i,j} b_n^{(j)}$ for $i = 1, \ldots, \ell$ and $n = 1, \ldots, d$, or in matrix form

$$\left(b_j^{(i)}\right)_{\substack{1 \leq i \leq \ell \\ 1 \leq j \leq d}} = \left(a_{i,j}\right)_{\substack{1 \leq i \leq \ell \\ 1 \leq j \leq d}} \left(b_j^{(i)}\right)_{\substack{1 \leq i \leq d \\ 1 \leq j \leq d}}.$$

For $I = (n_1, \ldots, n_d)$ with $1 \leq n_1 < n_2 < \cdots < n_d \leq \ell$, we thus have

$$b_I = c_I b_{(1,2,\ldots,d)}, \tag{30}$$

with $c_I = \det((a_{n_i,j})_{1 \leq i,j \leq d}) \in k(x)$. In particular,

$$c_I = \begin{cases} 1 & \text{for } I = (1, 2, \ldots, d), \\ (-1)^{d-j} a_{i,j} & \text{for } I = (1, \ldots, j-1, j+1, \ldots, d, i), \end{cases} \tag{31}$$

where $1 \leq j \leq d$ and $d < i \leq \ell$. From (29) and (30) it follows that $b_{(1,2,\ldots,d)} \in R$ is exponential over $k(x)$, i.e., $\delta(b_{(1,2,\ldots,d)})/b_{(1,2,\ldots,d)} \in k(x)$.

As T transforms $\delta(y) = (\bigwedge^d A')y$ into $Ly = 0$, the solution $(b_I)_I \in R^m$ of $\delta(y) = (\bigwedge^d A')y$ is transformed to a vector $T^{-1}(b_I)_I = (h, \delta(h), \ldots, \delta^{\ell-1}(h))^t \in R^\ell$ with $L(h) = 0$. Using (30), we see that $h = b_{(1,2,\ldots,d)} c$ with $c \in k(x)$. It follows that h is an exponential solution of $L(y) = 0$. Write $\delta(h) = a_1 h$ with $a_1 \in k(x)$. Then also $\delta^i(h) = a_i h$ with $a_i \in k(x)$ for $i = 1, \ldots, m-1$. So

$$T^{-1}(b_I)_I = h \begin{pmatrix} 1 \\ a_1 \\ \vdots \\ a_{m-1} \end{pmatrix} \quad \text{or} \quad (b_I)_I = hT \begin{pmatrix} 1 \\ a_1 \\ \vdots \\ a_{m-1} \end{pmatrix}.$$

The last equation implies $b_I = hT^{(I)}(1, a_1, \ldots, a_{m-1})^t$, where $T^{(I)}$ denotes the I-th row of T. Combining this with (30) and (31) yields

$$(-1)^{d-j}a_{i,j} = \frac{T^{(I)}\begin{pmatrix} 1 \\ \vdots \\ a_{m-1} \end{pmatrix}}{T^{((1,2,\ldots,d))}\begin{pmatrix} 1 \\ \vdots \\ a_{m-1} \end{pmatrix}}, \tag{32}$$

where $I = (1, \ldots, j-1, j+1, \ldots, d, i)$.

We claim that $\deg(a_i) \leq i\deg(a_1)$ for $i = 1, \ldots, m-1$. Indeed, writing $a_1 = \frac{p_1}{q}$ with $p_1, q \in k[x]$ relatively prime, we will show by induction on i, that $a_i = \frac{p_i}{q^i}$ with $p_i \in k[x]$ and $\deg(p_i) \leq i\deg(a_1)$. We have

$$a_{i+1} = \delta(a_i) + a_i a_1 = \frac{\delta(p_i)q^i - ip_i q^{i-1}\delta(q)}{q^{2i}} + \frac{p_i p_1}{q^{i+1}} = \frac{\delta(p_i)q - ip_i\delta(q) + p_i p_1}{q^{i+1}}.$$

So $\deg(p_{i+1}) = \deg(\delta(p_i)q - ip_i\delta(q) + p_i p_1) \leq (i+1)\deg(a_1)$.

Recall that the degree of a rational function satisfies $\deg(ab) \leq \deg(a) + \deg(b)$ and $\deg(a+b) \leq \deg(a) + \deg(b)$ for $a, b \in k(x)$. From $\deg(a_i) \leq i\deg(a_1)$, we obtain

$$\deg(T^{(I)}(1, a_1, \ldots, a_{m-1})^t) \leq \sum_{i=0}^{m-1}(\deg(T) + i\deg(a_1)) \leq m\deg(T) + \tfrac{m(m-1)}{2}\deg(a_1).$$

Using (32), we find

$$\deg(a_{i,j}) \leq 2m\deg(T) + m(m-1)\deg(a_1). \tag{33}$$

As $a_1 = \delta(h)/h$, with h an exponential solution of $Ly = 0$, this implies the claim of the lemma. $\qquad\square$

4 Specializations

In this section we prove our main specialization result (Theorem 4.26). To this end, we first show that various criteria and properties discussed in Section 3 are preserved under many specializations. Throughout Section 4 we make the following assumptions:

- k is an algebraically closed field of characteristic zero;

- $\mathcal{B}$ is a finitely generated k-algebra that is an integral domain;

- $\mathcal{X} = \mathrm{Spec}(\mathcal{B})$;

- K is the algebraic closure of the field of fractions of $\mathcal{B}$.

We usually identify a $c \in \mathcal{X}(k)$ with the corresponding k-algebra morphism $c : \mathcal{B} \to k$. We denote with b^c the image of $b \in \mathcal{B}$ under c. For a polynomial or Laurent polynomial p with coefficients in $\mathcal{B}$, we denote with p^c the polynomial obtained from p by applying c

to its coefficients. A similar notation applies to fractions of polynomials with coefficients in $\mathcal{B}$ (assuming that the denominator does not specialize to zero under c). Moreover, $M^c = \{p^c \mid p \in M\}$ for any set M such that p^c makes sense for any $p \in M$. In a similar spirit, if v is a tuple or matrix such that the specialization c can be applied to the entries of v, then v^c is the tuple or matrix obtained from v by applying c to the entries of v.

We now provide an outline of the proof of the main specialization result (respectively Theorem B from the introduction). Starting from an inclusion of algebraically closed fields $k \subseteq k'$ and a differential equation $\delta(y) = Ay$, $A \in k'(x)^{n \times n}$ with differential Galois group G and Picard-Vessiot ring $R/k'(x)$, we first spread out (using Lemma 3.11) R and G into nice families $\mathcal{R}$ and $\mathcal{G}$ over a parameter space $\mathcal{X}$. Our goal then is to show that the fibre $\mathcal{R}^c$ over c is Picard-Vessiot for all c in an ad×Jac-open subset of $\mathcal{X}(k)$. This is achieved via two main steps, corresponding to the two main steps of Hrushovski's algorithm. The first main step is to show, using the criterion of Lemma 3.15, that $\mathcal{R}^c/k(x)$ is proto-Picard-Vessiot for all c in an ad-open subset of $\mathcal{X}(k)$. The key ingredient for this is Theorem 4.24, which, roughly speaking, states that for a fixed degree d, a basis of the space of algebraic relations of degree at most d among the entries of a solution matrix for $\delta(y) = Ay$ specializes to a basis of the space of algebraic relations of degree at most d among the entries of a solution matrix for $\delta(y) = A^c y$ for all c in an ad-open subset of $\mathcal{X}(k)$. Theorem 4.24 is proved in Section 4.5, using Section 3.6 (via a reduction to the study of linear relations) and Section 4.1, where it is shown that the exponential bound from Section 3.5 is preserved under specialization on an ad-open subset of $\mathcal{X}(k)$.

The second main step of the proof is to find, inside the ad-open subset of $\mathcal{X}(k)$ over which $\mathcal{R}^c/k(x)$ is proto-Picard-Vessiot, an ad×Jac-open subset over which $\mathcal{R}^c/k(x)$ is Picard-Vessiot. The criterion of Lemma 3.23 allows us to decide if a proto-Picard-Vessiot ring is Picard-Vessiot by testing if certain algebraic functions are logarithmically independent. To apply this criterion, we thus need to show that logarithmic independence of algebraic functions is preserved on an ad×Jac-open subset of the parameter space (Theorem 4.10. This is proved in Section 4.3, where it is shown, building on specialization results for divisors from Section 4.2, that the criterion of Section 3.4 to test the logarithmic independence of algebraic functions is well-behaved under specialization.

4.1 The exponential bound under specialization

In this section we show that the exponential bound from Lemma 3.34 is preserved on an ad-open subset of the parameter space.

We first note a remark regarding the possibility of extending $\mathcal{B}$ if necessary that will be used repeatedly in what follows.

Remark 4.1. *Assume we are given a family $\mathcal{F}$ over $\mathcal{X}$ and we would like to show that a certain property holds of the fibre $\mathcal{F}_c$ for all c in a*

- *Zariski open,*

- *ad-open,*

- *Jac-open or*

- *ad×Jac-open*

subset of $\mathcal{X}(k)$. Then we can, without loss of generality, replace $\mathcal{B}$ with a finitely generated $\mathcal{B}$-subalgebra of K.

Proof. In the applications below it will always be clear what the family $\mathcal{F}$ is. Let $\mathcal{B}'$ be a finitely generated $\mathcal{B}$-subalgebra of K. We assume here that we can base change the family $\mathcal{F}$ over $\mathcal{X}$ to a family $\mathcal{F}'$ over $\mathcal{X}' = \mathrm{Spec}(\mathcal{B}')$ such that $\mathcal{F}'_{c'} = \mathcal{F}_{\phi(c')}$ for all $c' \in \mathcal{X}'(k)$, where $\phi \colon \mathcal{X}'(k) \to \mathcal{X}(k)$ is the morphism corresponding to the inclusion $\mathcal{B} \subseteq \mathcal{B}'$. By Chevalley's theorem, if $\mathcal{U}'$ is a nonempty Zariski open subset of $\mathcal{X}'(k)$, then $\phi(\mathcal{U}')$ contains a nonempty Zariski open subset of $\mathcal{X}(k)$. By Lemma 2.7, a similar statement holds for ad-open, Jac-open, and ad$\times$Jac-open subsets of $\mathcal{X}(k)$. $\qquad\square$

Let $f \in \mathcal{B}[x]$ be a monic polynomial and let

$$\mathcal{L} = \delta^n + a_{n-1}\delta^{n-1} + \ldots + a_0$$

be a linear differential operator with $a_0, \ldots, a_{n-1} \in \mathcal{B}[x]_f \subseteq K(x)$. So $\mathcal{L} \in K(x)[\delta]$ and for any $c \in \mathcal{X}(k)$ we have a linear differential operator

$$\mathcal{L}^c = \delta^n + a_{n-1}^c\delta^{n-1} + \ldots + a_0^c \in k(x)[\delta].$$

Example 4.2. Let $\mathcal{B} = k[\alpha]$ (with α transcendental over k), $f = x$ and $\mathcal{L} = \delta^2 + \frac{1}{x}\delta + 1 - (\frac{\alpha}{x})^2 \in \mathcal{B}[x]_f[\delta]$. From Example 3.35 we know that $N(\mathcal{L}) = 1$ and $N(\mathcal{L}^c) = 1$ for any $c \in \mathcal{X}(k) = k$ with $c - \frac{1}{2} \notin \mathbb{Z}$. On the other hand, $N(\mathcal{L}^c) = |c| + \frac{1}{2}$ in case $c - \frac{1}{2} \in \mathbb{Z}$. So $N(\mathcal{L})$ specializes well only on an ad-open subset of $\mathcal{X}(k)$.

Proposition 4.3. *There exists an ad-open subset $\mathcal{U}$ of $\mathcal{X}(k)$ such that $N(\mathcal{L}^c) = N(\mathcal{L})$ for all $c \in \mathcal{U}$. In particular, $N(\mathcal{L})$ is an exponential bound for $\mathcal{L}^c$ for all $c \in \mathcal{U}$.*

Proof. Enlarging $\mathcal{B}$ if necessary (Remark 4.1), we may assume that $\mathrm{Sing}(\mathcal{L}) \subseteq \mathcal{B}$ and that all coefficients of all generalized exponents at points in $\mathrm{Sing}(\mathcal{L}) \cup \{\infty\}$ belong to $\mathcal{B}$. There exists a nonempty Zariski open subset $\mathcal{U}_1$ of $\mathcal{X}(k)$ such that for any $c \in \mathcal{U}_1$,

(i) $\mathrm{Sing}(\mathcal{L})^c = \mathrm{Sing}(\mathcal{L}^c)$ and $\lambda_1^c \neq \lambda_2^c$ for $\lambda_1, \lambda_2 \in \mathrm{Sing}(\mathcal{L})$ (one can use resultants for this step);

(ii) $\mathrm{ram}(e^c) = \mathrm{ram}(e)$ and $\mathrm{ord}_0(e^c) = \mathrm{ord}_0(e)$ for every generalized exponent e of $\mathcal{L}$ at every point of $\mathrm{Sing}(\mathcal{L}) \cup \{\infty\}$;

(iii) $m_{e^c, \lambda^c}(\mathcal{L}^c) = m_{e, \lambda}(\mathcal{L})$ for every $\lambda \in \mathrm{Sing}(\mathcal{L}) \cup \{\infty\}$ and every generalized exponent e of $\mathcal{L}$ at λ.

For (iii), note that the units of the ring $\mathcal{B}((x))$ of formal Laurent series over $\mathcal{B}$, are exactly those Laurent series whose lowest nonzero coefficient is a unit in $\mathcal{B}$. So f may not be a unit in $\mathcal{B}((x))$. However, if $b \in \mathcal{B}$ is the lowest nonzero coefficient of f, then f is a unit in $\mathcal{B}_b((x))$ and therefore $\mathcal{B}[x]_f \subseteq \mathcal{B}_b((x))$. It follows that for $\lambda \in \mathrm{Sing}(\mathcal{L}) \cup \{\infty\}$ and $e \in \mathcal{B}[x^{-1/r}]$, the operator $S_e(l_\lambda(\mathcal{L})) \in K((x^{1/r}))[\bar{\delta}]$ has coefficients in $\mathcal{B}_b((x^{1/r}))$. Thus, all that is required to guarantee (iii), is that c does not specialize b or any coefficient of the Newton polynomial of $S_e(l_\lambda(\mathcal{L}))$ for slope 0 to zero.

Assume that $c \in \mathcal{U}_1$. By (iii), e^c is a generalized exponent of $\mathcal{L}^c$ at λ^c with multiplicity $m_{e, \lambda}(\mathcal{L})$, for every generalized exponent e of $\mathcal{L}$ at $\lambda \in \mathrm{Sing}(\mathcal{L}) \cup \{\infty\}$. From formula (25), it follows that every generalized exponent of $\mathcal{L}^c$ at p^c is equal to e^c for some generalized exponent e of $\mathcal{L}$ at λ. Hence $\mathrm{PP}(\mathcal{L}^c, \lambda^c) = \mathrm{PP}(\mathcal{L}, \lambda)^c$ for every $\lambda \in \mathrm{Sing}(\mathcal{L}) \cup \{\infty\}$. Furthermore, $\mathrm{Im}(\Phi_{\mathcal{L}^c}) = \mathrm{Im}(\Phi_\mathcal{L})^c$.

In general, $\mathrm{Im}(\Phi_\mathcal{L})^c \cap \mathbb{Z}$ can be larger than $\mathrm{Im}(\Phi_\mathcal{L}) \cap \mathbb{Z}$. However, if Γ is the subgroup of $\mathbb{G}_a(\mathcal{B})$ generated by $\{1\} \cup \mathrm{Im}(\Phi_\mathcal{L})$, then $\mathrm{Im}(\Phi_\mathcal{L})^c \cap \mathbb{Z} = \mathrm{Im}(\Phi_\mathcal{L}) \cap \mathbb{Z}$ for $c \in W_\mathcal{X}(\mathbb{G}_a, \Gamma)$. Therefore, for $\mathcal{U}$ an ad-open subset of $\mathcal{U}_1 \cap W_\mathcal{X}(\mathbb{G}_a, \Gamma)$ and $c \in \mathcal{U}$, we have $\mathrm{Im}(\Phi_{\mathcal{L}^c}) \cap \mathbb{Z} = \mathrm{Im}(\Phi_\mathcal{L}) \cap \mathbb{Z}$ and consequently $N(\mathcal{L}^c) = N(\mathcal{L})$. $\qquad\square$

4.2 Divisors under specialization

Our next goal is to show that logarithmic independence of algebraic functions is preserved under many specializations. To show that the criterion for the logarithmic independence from Lemma 3.26 is preserved under many specializations, we first need to know that principal divisors and residues are preserved under many specializations.

Let F/K be a function field of one variable, i.e., a finitely generated field extension of transcendence degree one. Let C be a smooth projective model of the function field F/K, i.e., C is a smooth projective (irreducible) curve over K with function field F. We fix a closed embedding of C into $\mathbb{P}^n_K = \mathrm{Proj}(K[y_0, \dots, y_n])$. So C is defined by a homogeneous prime ideal I of $K[y_0, \dots, y_n]$. Enlarging $\mathcal{B}$ if necessary, we can assume that I is generated by homogeneous polynomials with coefficients in $\mathcal{B}$, and so $\mathcal{I} = I \cap \mathcal{B}[y_0, \dots, y_n]$ is a homogeneous prime ideal of $\mathcal{B}[y_0, \dots, y_n]$ such that $\mathcal{I} \otimes_{\mathcal{B}} K = I$ in $\mathcal{B}[y_0, \dots, y_n] \otimes_{\mathcal{B}} K = K[y_0, \dots, y_n]$.

Set $\mathcal{C} = \mathrm{Proj}(\mathcal{B}[y_0, \dots, y_n]/\mathcal{I})$, i.e., $\mathcal{C}$ is the closed subscheme of $\mathbb{P}^n_{\mathcal{B}}$ defined by $\mathcal{I}$. Then $\mathcal{C}$ is an integral scheme of finite type over k, projective over $\mathcal{X}$. Since $(\mathcal{B}[y_0, \dots, y_n]/\mathcal{I}) \otimes_{\mathcal{B}} K = K[y_0, \dots, y_n]/I$, we have $\mathcal{C} \times_{\mathcal{X}} \mathrm{Spec}(K) = C$. Thus the generic fibre of $\mathcal{C} \to \mathcal{X}$ is smooth, geometrically irreducible and of dimension one. These three properties are generic properties. (For geometric irreducibly see [Sta24, Tag 0559], for fibre dimension see [Sta24, Tag 05F7] and for smoothness see [Gro67, Prop. 17.7.11].) Thus there exists a nonempty Zariski open subset $\mathcal{U}$ of $\mathcal{X}$ such that for every $u \in \mathcal{U}$, the fibre $\mathcal{C}_u$ over u is a smooth geometrically irreducible curve (over the residue field at u). Hence, replacing $\mathcal{B}$ with a localization of $\mathcal{B}$ if necessary, we may (and henceforth do) assume that $\mathcal{C}_u$ is a smooth geometrically irreducible curve for all $u \in \mathcal{X}$. In line with our notation for specializations we set $C^c = \mathcal{C}_c$ for $c \in \mathcal{X}(k) \subseteq \mathcal{X}$. Note that, concretely, $C^c \subseteq \mathbb{P}^n_k$ is the closed subscheme defined by the homogeneous polynomials obtained by applying c to a set of homogeneous generators of $\mathcal{I}$.

Throughout Section 4.2 we assume that $\mathcal{C}$ is as described above. In particular, $\mathcal{C} \subseteq \mathbb{P}^n_{\mathcal{B}}$ is an integral scheme of finite type over k, projective over $\mathcal{X}$ and all fibres $C^c \subseteq \mathbb{P}^n_k$ are smooth, irreducible curves.

In the sequel, we will usually identify the places of F/K with $C(K)$ (and similarly for $k(C^c)/k$ and $C^c(k)$). The discrete valuation on F/K (or $k(C^c)/k$) corresponding to a point (respectively place) P is denoted ν_P.

For every $c \in \mathcal{X}(k)$ we have a specialization map

$$\mathcal{C}(\mathcal{B}) \to C^c(k), \ P \mapsto P^c,$$

where $P^c \colon \mathrm{Spec}(k) \to \mathcal{C} \times_{\mathcal{X}} \mathrm{Spec}(k)$ is such that the composition of P^c with the projection to $\mathcal{C}$ is the composition of $\mathrm{Spec}(k) \xrightarrow{c} \mathcal{X}$ with $P \colon \mathcal{X} \to \mathcal{C}$.

A rational function h on $\mathcal{C}$ yields a rational function h^{gen} on C via the projection $C = \mathcal{C} \times_{\mathcal{X}} \mathrm{Spec}(K) \to \mathcal{C}$. Note that h^{gen} is well-defined because for a nonempty Zariski open subset $\mathcal{U}$ of $\mathcal{C}$, the inverse image $\mathcal{U} \times_{\mathcal{X}} \mathrm{Spec}(K)$ of $\mathcal{U}$ under the projection $\mathcal{C} \times_{\mathcal{X}} \mathrm{Spec}(K) \to \mathcal{C}$ is nonempty, since the generic point of $\mathcal{U}$ and the point of $\mathrm{Spec}(K)$ map to the generic point of $\mathcal{X}$.

Roughly speaking, the following lemma shows that principal divisors are preserved under specialization on a nonempty Zariski open subset. We think this lemma is well-known to the experts, but we were not able to locate a suitable reference.

Lemma 4.4. *Let h be a nonzero rational function on $\mathcal{C}$ and let $Z_1, \ldots, Z_r$ and $P_1, \ldots, P_s$ be the zeros and poles of h^{gen} in $C(K)$. Assume that $Z_1, \ldots, Z_r, P_1, \ldots, P_s \in \mathcal{C}(\mathcal{B}) \subseteq \mathcal{C}(K) = C(K)$. Then there exists a nonempty Zariski open subset $\mathcal{U}$ of $\mathcal{X}(k)$ such that for every $c \in \mathcal{U}$*

- *h yields a rational function h^c on C^c via the projection $C^c = \mathcal{C} \times_{\mathcal{X}} \mathrm{Spec}(k) \to \mathcal{C}$;*

- *$Z_1^c, \ldots, Z_r^c, P_1^c, \ldots, P_s^c$ are all distinct;*

- *$Z_1^c, \ldots, Z_r^c$ is the set of zeros of h^c and $P_1^c, \ldots, P_s^c$ is the set of poles of h^c;*

- *$\nu_{Z_i^c}(h^c) = \nu_{Z_i}(h^{\mathrm{gen}})$ and $\nu_{P_i^c}(h^c) = \nu_{P_i}(h^{\mathrm{gen}})$ for all i.*

In particular, if $(h^{\mathrm{gen}}) = \sum_{i=1}^r d_i Z_i + \sum_{j=1}^s e_j P_j$, then $(h^c) = \sum_{i=1}^r d_i Z_i^c + \sum_{j=1}^s e_j P_j^c$.

Proof. Assume that h is given by a regular function on a nonempty Zariski open subset $\mathcal{V}$ of $\mathcal{C}$. For h^c to be well-defined, we need to know that $\mathcal{V} \times_{\mathcal{X}} \mathrm{Spec}(k) \subseteq \mathcal{C} \times_{\mathcal{X}} \mathrm{Spec}(k) = C^c$ is nonempty. Since $\mathcal{V} \to \mathcal{X}$ is a dominant morphism of schemes of finite type over k, the image contains a nonempty Zariski open subset $\mathcal{U}_1$ by Chevalley's theorem. Then $\mathcal{V} \times_{\mathcal{X}} \mathrm{Spec}(k)$ is nonempty for every $c \in \mathcal{U}_1(k)$ because there is an element of $\mathcal{V}$ mapping to $c \in \mathcal{X}$. This takes care of the first item in the lemma.

For the remaining three items, we choose a linear form $\ell = a_0 y_0 + \ldots + a_n y_n \in K[y_0, \ldots, y_n]$ such that the hyperplane $H \subseteq \mathbb{P}_K^n$ defined by $\ell = 0$ does not contain any of the Z_i's or P_i's. Enlarging $\mathcal{B}$ if necessary, we may assume that $\ell \in \mathcal{B}[y_0, \ldots, y_n]$. In fact, after localizing $\mathcal{B}$ if necessary, we can assume that $(a_0, \ldots, a_n) \in \mathcal{B}^{n+1}$ is a column of an invertible matrix in $\mathcal{B}^{(n+1) \times (n+1)}$. Thus, after a linear change of coordinates on $\mathbb{P}_{\mathcal{B}}^n$, we can assume that ℓ is given by $\ell = y_0$.

Let $\mathcal{U}_0$ be the open subscheme of $\mathbb{P}_{\mathcal{B}}^n$ where x_0 does not vanish. So $\mathcal{U}_0$ can be identified with $\mathbb{A}_{\mathcal{B}}^n = \mathrm{Spec}(\mathcal{B}[y_1, \ldots, y_n])$. Recall (see [Mil17, Chapter 7, Section d] or [Str99, Prop. 3.4]) that a point $P \in \mathbb{P}_{\mathcal{B}}^n(\mathcal{B})$, i.e., a morphism $\mathcal{X} \to \mathbb{P}_{\mathcal{B}}^n$ (over $\mathcal{B}$) can be identified with a submodule L of $\mathcal{B}^{n+1}$ such that L is a direct summand (i.e., there exists a submodule M of $\mathcal{B}^{n+1}$ such that $\mathcal{B}^{n+1} = L \oplus M$) and L is locally free of rank 1. The point P lies in $\mathcal{U}_0(\mathcal{B}) \subseteq \mathbb{P}_{\mathcal{B}}^n$ (i.e., $\mathcal{X} \to \mathbb{P}_{\mathcal{B}}^n$ factors through $\mathcal{U}_0 \hookrightarrow \mathbb{P}_{\mathcal{B}}^n$) if and only if L has a basis vector of the form $(b_0, \ldots, b_n) \in \mathcal{B}^n$ with $b_0 = 1$. As the Z_i's and P_i's (considered as elements of $\mathbb{P}_K^n(K)$) do not lie in $H(K)$, we see that, after replacing $\mathcal{B}$ with a localization of $\mathcal{B}$, we may assume that all the Z_i's and P_i's (considered as elements of $\mathbb{P}_{\mathcal{B}}^n(\mathcal{B})$) lie in $\mathcal{U}_0(\mathcal{B})$.

Consider the open subscheme $\mathcal{C}_0 = \mathcal{C} \cap \mathcal{U}_0$ of $\mathcal{C}$. Then $\mathcal{C}_0$ identifies with a closed subscheme of $\mathcal{U}_0 = \mathbb{A}_{\mathcal{B}}^n$ and the Z_i's and P_i's identify with elements of $\mathbb{A}_{\mathcal{B}}^n(\mathcal{B}) = \mathcal{B}^n$. On the Zariski open subset of $\mathcal{X}(k)$ where the product of suitable differences of coordinates of the Z_i's and P_i's does not vanish, the elements $Z_1^c, \ldots, Z_r^c, P_1^c, \ldots, P_s^c$ are all distinct.

Let $Z = (z_1, \ldots, z_n) \in \mathcal{B}^n \subseteq K^n$ be one of the Z_i's. Assume that h^{gen} has a zero of multiplicity $m \geq 1$ at Z, i.e., $m = \nu_Z(h^{\mathrm{gen}})$. So h^{gen} is contained in the m-th power $\mathfrak{m}_{C,Z}^m$ of the maximal ideal $\mathfrak{m}_{C,Z}$ of the local ring $\mathcal{O}_{C,Z}$.

Let C_0 be the open subscheme of C where y_0 does not vanish, in other words, $C_0 = \mathcal{C}_0 \times_{\mathcal{X}} \mathrm{Spec}(K)$. Then $K(C) = K(C_0)$ and $\mathcal{O}_{C,Z} = \mathcal{O}_{C_0,Z}$. As the maximal ideal $\mathfrak{m}_{C_0,Z}$ of $\mathcal{O}_{C_0,Z}$ is generated by the images of $y_1 - z_1, \ldots, y_n - z_n$, we see that $\mathfrak{m}_{C_0,Z}^m$ is generated by the set M consisting of the images of m-fold products of elements from $\{y_1 - z_1, \ldots, y_n - z_n\}$. So we can write $h^{\mathrm{gen}} = f_1 m_1 + \ldots + f_d m_d$ with $f_1, \ldots, f_d \in \mathcal{O}_{C_0,Z} \subseteq K(C_0)$ and $m_1, \ldots, m_d \in M$. Enlarging $\mathcal{B}$ if necessary, we may assume that $f_1, \ldots, f_d$ come from rational functions on $\mathcal{C}$, i.e., $f_i = h_i^{\mathrm{gen}}$ for some rational function h_i on $\mathcal{C}$ for $i = 1, \ldots, d$.

Recall that $k(\mathcal{B})$ denotes the field of fractions of $\mathcal{B}$. Note that the function field $k(\mathcal{C})$ of $\mathcal{C}$ (considered as a scheme over k) agrees with the function field $k(\mathcal{B})(\mathcal{C}_{k(\mathcal{B})})$ of $\mathcal{C}_{k(\mathcal{B})} = \mathcal{C} \times_{\mathcal{X}} \mathrm{Spec}(k(\mathcal{B}))$ (considered as a scheme over $k(\mathcal{B})$) and the latter is contained in the function field $K(C)$ (considered as a scheme over K). In fact, $K(C) = k(\mathcal{B})(\mathcal{C}_{k(\mathcal{B})}) \otimes_{k(\mathcal{B})} K$. So the identity $h^{\mathrm{gen}} = f_1 m_1 + \ldots + f_d m_d$ that holds in $K(C)$, can be interpreted as an identity

$$h = h_1 m_1 + \ldots + h_d m_d \tag{34}$$

that holds in $k(\mathcal{C})$.

We already observed in the beginning of the proof that a rational function h on $\mathcal{C}$ can be specialized to a rational function h^c on C^c for all c in some nonempty Zariski open subset of $\mathcal{X}(k)$. To specialize (34), we would like to know that if $h^{\mathrm{gen}} \in \mathcal{O}_{C_0,\mathfrak{z}}$, then $h^c \in \mathcal{O}_{C_0^c,Z^c}$, where C_0^c is the open subscheme of C^c where y_0 does not vanish, i.e., $C_0^c = \mathcal{C}_0 \times_{\mathcal{X}} \mathrm{Spec}(k)$.

But $h^{\mathrm{gen}} \in \mathcal{O}_{C_0,Z}$ means that h can locally be described by a fraction $\frac{p}{q}$ of two polynomials $p, q \in \mathcal{B}[y_1, \ldots, y_n]$ such that q does not vanish at Z. Thus, on the Zariski open subset of $\mathcal{X}(k)$, where $q(Z) \in \mathcal{B}$ does not vanish, the rational function h^c is locally described by the fraction $\frac{p^c}{q^c}$ and so $h^c \in \mathcal{O}_{C_0^c,Z^c}$.

Since the maximal ideal $\mathfrak{m}_{C_0^c,Z^c}$ of $\mathcal{O}_{C_0^c,Z^c}$ is generated by the images of $y_1 - c(z_1), \ldots, y_n - c(z_n)$, the specialization $h^c = h_1^c m_1^c + \ldots + h_d^c m_d^c$ of (34) shows that $h^c \in \mathfrak{m}_{C_0^c,Z^c}^m$. Therefore $\nu_{Z^c}(h^c) \geq m = \nu_Z(h^{\mathrm{gen}})$ for all c in a nonempty Zariski open subset of $\mathcal{X}(k)$.

From this inequality for the zeros, we can immediately derive a similar inequality for the poles, because a point is a pole of multiplicity m of a rational function if and only if it is a zero of multiplicity m of the inverse of the rational function. So there exists a nonempty Zariski open subset $\mathcal{U}_2$ of $\mathcal{X}(k)$ such that for all $c \in \mathcal{U}_2$

- h^c is well-defined;

- $Z_1^c, \ldots, Z_r^c, P_1^c, \ldots, P_s^c$ are all distinct;

- $\nu_{Z_i^c}(h^c) \geq \nu_{Z_i}(h^{\mathrm{gen}})$ for $i = 1, \ldots, r$; in particular, $Z_1^c, \ldots, Z_r^c$ are zeros of h^c;

- $\nu_{P_i^c}(h^c) \leq \nu_{P_i}(h^{\mathrm{gen}})$ for all $i = 1, \ldots, s$; in particular, $P_1^c, \ldots, P_s^c$ are poles of h^c.

Note that the statement of the lemma is trivial in case h is constant (i.e., h lies in K) since in that case there are no zeros or poles. We may thus assume that h is not constant. Under this assumption we will now show that

$$[K(C) : K(h^{\mathrm{gen}})] = [k(C^c) : k(h^c)] \tag{35}$$

for all c in a nonempty Zariski open subset of $\mathcal{X}(k)$. Since h^{gen} is transcendental over K, the field extension $K(C)/K(h^{\mathrm{gen}})$ is finite and we can choose $\eta \in K(C)$ such that $K(C) = K(h^{\mathrm{gen}}, \eta)$. Let $q \in K(h^{\mathrm{gen}})[y]$ be the minimal polynomial of η over $K(h^{\mathrm{gen}})$. Replacing η with a $K(h^{\mathrm{gen}})$-multiple of η if necessary, we can assume that $q \in K[h^{\mathrm{gen}}][y]$. Enlarging $\mathcal{B}$ if necessary, we can indeed assume that $q \in \mathcal{B}[h^{\mathrm{gen}}][y]$. Let $p \in \mathcal{B}[x, y]$ be such that $p(h^{\mathrm{gen}}, y) = q$. By Gauss's lemma, $p \in K[x, y]$ is irreducible. In fact, since p is monic as a polynomial in y, we see that p is a prime element of $\mathcal{B}[x, y]$. So $\mathcal{D} = \mathrm{Spec}(\mathcal{B}[x, y]/(p))$ is an integral scheme and $\mathcal{D}_K = \mathcal{D} \times_{\mathcal{X}} \mathrm{Spec}(K) = \mathrm{Spec}(K[x, y]/(p))$ has function field $K(h^{\mathrm{gen}}, \eta) = K(C)$.

Let $\mathcal{V} = \mathrm{Spec}(\mathcal{B}[a_1, \ldots, a_m])$ be an open affine subscheme of $\mathcal{C}$. Then

$$\mathcal{V}_K = \mathcal{V} \times_{\mathcal{X}} \mathrm{Spec}(K) = \mathrm{Spec}(\mathcal{B}[a_1, \ldots, a_m] \otimes_{\mathcal{B}} K)$$

is a nonempty affine open subscheme of $C = \mathcal{C} \times_{\mathcal{X}} \mathrm{Spec}(K)$. Moreover $\mathcal{D}_K$ and $\mathcal{V}_K$ are birationally equivalent (over K). In other words, the fields of fractions of $\mathcal{B}[\overline{x}, \overline{y}] \otimes_{\mathcal{B}} K$ and $\mathcal{B}[a_1, \ldots, a_m] \otimes_{\mathcal{B}} K$ are isomorphic as field extensions of K, where $\overline{x}$ and $\overline{y}$ stand for the images of x and y in $\mathcal{B}[x, y]/(p)$ respectively. Such an isomorphism and its inverse is given by fractions of polynomials with coefficients in K. Enlarging $\mathcal{B}$ if necessary, we may assume that all coefficients belong to $\mathcal{B}$. Then there exist nonzero elements $b \in \mathcal{B}[\overline{x}, \overline{y}]$ and $a \in \mathcal{B}[a_1, \ldots, a_m]$ such that $\mathcal{B}[\overline{x}, \overline{y}]_b$ and $\mathcal{B}[a_1, \ldots, a_n]_a$ are isomorphic over $\mathcal{B}$. In other words, there exist an open subscheme $\mathcal{D}'$ of $\mathcal{D}$ and an open subscheme $\mathcal{V}'$ of $\mathcal{C}$ such that $\mathcal{D}'$ and $\mathcal{V}'$ are isomorphic over $\mathcal{B}$. Note that under this isomorphism, the rational function h^{gen} on $\mathcal{V}'$ corresponds to $\overline{x}$.

By Chevalley's theorem, there exists a nonempty Zariski open subset $\mathcal{U}_3$ of $\mathcal{X}(k)$ such that $\mathcal{U}_3$ is contained in the image of the vertical maps in the commutative diagram

$$
\begin{array}{ccc}
\mathcal{D}' & \overset{\simeq}{\longrightarrow} & \mathcal{V}'. \\
{\scriptstyle \pi_1} \searrow & & \swarrow {\scriptstyle \pi_2} \\
& \mathcal{X} &
\end{array}
$$

For $c \in \mathcal{U}_3 \subseteq \mathcal{X}(k) \subseteq \mathcal{X}$, the fibre $\pi_2^{-1}(c)$ is a nonempty open subscheme of C^c and therefore has function field $k(C^c)$. On the other hand, the fibre $\pi_2^{-1}(c)$ is an open subscheme of the spectrum of $(\mathcal{B}[x, y]/(p)) \otimes_{\mathcal{B}} k = k[x, y]/(p^c)$. The isomorphism $\mathcal{D}' \simeq \mathcal{V}'$ induces an isomorphism $\pi_1^{-1}(c) \simeq \pi_2^{-1}(c)$. Under the corresponding isomorphism of functions fields, $h^c \in k(C^c)$ corresponds to the image of x in the field of fractions of $k[x, y]/(p^c)$. The degree of the field of fractions of $k[x, y]/(p^c)$ over the image of x is the degree of p as a polynomial in y, which equals $[K(C) : K(h^{\mathrm{gen}})]$. Thus (35) holds for all $c \in \mathcal{U}_3$.

Set $\mathcal{U} = \mathcal{U}_2 \cap \mathcal{U}_3$. By [Sti09, Theorem 1.4.11], the degree of the zero divisor and the degree of the pole divisor of h^{gen} is equal to $[K(C) : K(h^{\mathrm{gen}})]$ and similarly for h^c in place of h^{gen}. Thus

$$
[K(C) : K(h^{\mathrm{gen}})] = \sum_{i=1}^{r} \nu_{Z_i}(h^{\mathrm{gen}}) \leq \sum_{i=1}^{r} \nu_{Z_i^c}(h^c) \leq [k(C^c) : k(h^c)] = [K(C) : K(h^{\mathrm{gen}})]
$$

for all $c \in \mathcal{U}$. This implies that $\nu_{Z_i^c}(h^c) = \nu_{Z_i}(h^{\mathrm{gen}})$ for $i = 1, \ldots, r$ and that h^c has no zeros other than $Z_1^c, \ldots, Z_r^c$. A similar argument applies for the poles instead of the zeros. We conclude that $\mathcal{U}$ has the desired properties. $\qquad \square$

Roughly speaking, the following lemma shows that residues are preserved under specialization on a nonempty Zariski open subset.

Lemma 4.5. *Let h and t be rational functions on $\mathcal{C}$ such that t^{gen} is a uniformizer at $P \in \mathcal{C}(\mathcal{B}) \subseteq \mathcal{C}(K) = C(K)$. Then there exists a nonempty Zariski open subset $\mathcal{U}$ of $\mathcal{X}(k)$ such that for all $c \in \mathcal{U}$*

- *h^c, t^c and $\mathrm{res}_{P, t^{\mathrm{gen}}}(h^{\mathrm{gen}})^c$ are well-defined;*

- *t^c is a uniformizer at P^c and*

- *$\mathrm{res}_{P^c, t^c}(h^c) = \mathrm{res}_{P, t^{\mathrm{gen}}}(h^{\mathrm{gen}})^c$.*

Proof. Note that uniformizers are characterized by the property that their valutation is one. It thus follows from Lemma 4.4 that there exists a nonempty Zariski open subset $\mathcal{U}_1$ of $\mathcal{X}$ such that h^c and t^c are well-defined and that t^c is a uniformizer at P^c for all $c \in \mathcal{U}_1$.

If $\nu_P(h^{\mathrm{gen}}) \geq 0$, then $\mathrm{res}_{P,t^{\mathrm{gen}}}(h^{\mathrm{gen}}) = 0$ and the claim follows from Lemma 4.4. We may thus assume that $\nu_P(h^{\mathrm{gen}}) = -m$, with $m \geq 1$.

From the uniqueness of the P-adic representation, it follows that there exist uniquely determined elements $a_{-m}, \ldots, a_{-1} \in K$ such that $\nu_P(h^{\mathrm{gen}} - \sum_{i=1}^{m} a_{-i}(t^{\mathrm{gen}})^{-i}) \geq 0$ and that in this situation $a_{-1} = \mathrm{res}_{P,t^{\mathrm{gen}}}(h^{\mathrm{gen}})$. Enlarging $\mathcal{B}$ if necessary, we may assume that $a_{-m}, \ldots, a_{-1} \in \mathcal{B}$. By Lemma 4.4, there exists a nonempty Zariski open subset $\mathcal{U}$ of $\mathcal{X}(k)$ such that for every $c \in \mathcal{U}$ the rational function $f = h - \sum_{i=1}^{m} a_{-i}t^{-i}$ on $\mathcal{C}$ has a well-defined specialization $f^c = h^c - \sum_{i=1}^{m} a_{-i}^c (t^c)^{-i}$ with $\nu_{P^c}(f^c) \geq 0$. It follows that $a_{-1}^c = \mathrm{res}_{P^c,t^c}(h^c)$. $\qquad\square$

The following lemma explains the origin of the Jac-open subset that occurs in our main specialization result (Theorem 4.26). We denote with $\mathrm{Div}^0(-)$ the group of divisors of degree zero.

Lemma 4.6. *Let $P_1, \ldots, P_r \in \mathcal{C}(\mathcal{B}) \subseteq \mathcal{C}(K) = C(K)$. Then there exists an $\mathrm{ad} \times \mathrm{Jac}$-open subset $\mathcal{U}$ of $\mathcal{X}(k)$ such that for all $c \in \mathcal{U}$ and all $d_1, \ldots, d_r \in \mathbb{Z}$, if $d_1 P_1 + \ldots + d_r P_r \in \mathrm{Div}^0(C)$ is not principal, then $d_1 P_1^c + \ldots + d_r P_r^c \in \mathrm{Div}^0(C^c)$ is not principal.*

Proof. Let J be the Jacobian of C and let $\varphi \colon C \to J$ be a canonical embedding. For more background on Jacobian varieties see e.g., [Mil86] or [BLR90, Chapter 9]. Enlarging $\mathcal{B}$ if necessary (Remark 4.1), there exists a commutative separated group scheme $\mathcal{J}$ of finite type over $\mathcal{B}$ and a closed embedding $\phi \colon \mathcal{C} \to \mathcal{J}$ over $\mathcal{X}$ such that

- $\phi_K = \varphi$ (in particular, $\mathcal{J}$ is of Jacobian type) and

- there exists a nonempty Zariski open subset $\mathcal{U}_1$ of $\mathcal{X}(k)$ such that the base change $\phi^c \colon C^c \to \mathcal{J}^c$ of ϕ via $c \colon \mathrm{Spec}(k) \to \mathcal{X}$ is a canonical embedding of C^c into its Jacobian $\mathcal{J}^c$ for every $c \in \mathcal{U}_1$.

For every $c \in \mathcal{U}_1$ we have a commutative diagram

$$
\begin{array}{ccc}
\mathcal{C}(\mathcal{B}) & \lhook\joinrel\longrightarrow & \mathcal{J}(\mathcal{B}) \\
\downarrow & & \downarrow \\
C^c(k) & \lhook\joinrel\longrightarrow & \mathcal{J}^c(k)
\end{array}
$$

where the vertical maps are the specialization maps. Let Γ be the subgroup of $\mathcal{J}(\mathcal{B})$ generated by $P_1, \ldots, P_r \in \mathcal{C}(\mathcal{B}) \subseteq \mathcal{J}(\mathcal{B})$ and set $\mathcal{V} = W_{\mathcal{X}}(\mathcal{J}, \Gamma)$ (notation as in Section 2.1).

Then $\mathcal{U} = \mathcal{U}_1 \cap \mathcal{V}$ is an $\mathrm{ad} \times \mathrm{Jac}$-open subset of $\mathcal{X}(k)$. Let $c \in \mathcal{U}$ and assume that $d_1 P_1 + \ldots + d_r P_r \in \mathrm{Div}^0(C)$ is not principal. Then $d_1 P_1 + \ldots + d_r P_r \in \mathcal{J}(\mathcal{B}) \subseteq \mathcal{J}(K) = J(K)$ is nonzero because $\mathrm{Div}^0(C) \to J(K)$ is surjective with kernel the subgroup of principal divisors. Since the specialization map $\mathcal{J}(\mathcal{B}) \to \mathcal{J}^c(k)$ is injective on Γ, we see that $d_1 P_1^c + \ldots + d_r P_r^c \in \mathcal{J}^c(k)$ is nonzero. Therefore $d_1 P_1^c + \ldots + d_r P_r^c \in \mathrm{Div}^0(C^c)$ is not principal. $\qquad\square$

4.3 Logarithmic independence under specialization

In this section we show that logarithmic independence is preserved on an $\mathrm{Ad} \times \mathrm{Jac}$-open subset of the parameter space.

Let F be a finite field extension of $K(x)$. So F/K is a function field of one variable, considered as a differential field via $\delta = \frac{d}{dx}$. Let $\eta \in F$ be such that $F = K(x, \eta)$ and

the minimal polynomial of η over $K(x)$ has coefficients in $\mathcal{B}[x]$. Let $f \in \mathcal{B}[x]$ be a monic polynomial such that $\mathcal{B}[x]_f[\eta]$ is a differential subring of F.

Let $p \in \mathcal{B}[x, y] \subseteq K(x)[y]$ be the minimal polynomial of η over $K(x)$. By Gauss's lemma $p \in K[x, y]$ is irreducible and by the Bertini-Noether theorem ([FJ08, Prop. 9.4.3]) there exists a nonempty Zariski open subset $\mathcal{U}$ of $\mathcal{X}(k)$ such that $p^c \in k[x, y]$ is irreducible for all $c \in \mathcal{U}$. Then

$$\mathcal{B}[x]_f[\eta] \otimes_{\mathcal{B}[x]_f} k(x) = (\mathcal{B}[x]_f[y]/(p)) \otimes_{\mathcal{B}[x]_f} k(x) = k(x)[y]/(p^c)$$

is a finite field extension of $k(x)$ for all $c \in \mathcal{U}$. Replacing $\mathcal{B}$ with a localization of $\mathcal{B}$, we mays assume that $\mathcal{U} = \mathcal{X}(k)$. For $c \in \mathcal{X}(k)$ we set

$$F^c = \mathcal{B}[x]_f[\eta] \otimes_{\mathcal{B}[x]_f} k(x)$$

and for $h \in \mathcal{B}[x]_f[\eta]$ we set $h^c = h \otimes 1 \in F^c$. The following lemma explains that this notation is consistent with the notation from Section 4.2. Let C be a smooth projective model of F/K and let $\mathcal{C}$ and C^c be as described in Section 4.2.

Lemma 4.7. *After enlarging $\mathcal{B}$ if necessary, there exists a nonzero element $b \in \mathcal{B}[x]_f[\eta]$ such that $\mathrm{Spec}((\mathcal{B}[x]_f[\eta])_b)$ is isomorphic (over $\mathcal{B}$) to an open subscheme of $\mathcal{C}$. Moreover, there exists a nonempty Zariski open subset $\mathcal{U}$ of $\mathcal{X}(k)$ such that for all $c \in \mathcal{U}$ we have $F^c \simeq k(C^c)$ and for $h \in \mathcal{B}[x]_f[\eta]$ the rational function $h^c \in k(C^c)$ as defined in Lemma 4.4 corresponds to $h^c = h \otimes 1$ as defined above.*

Proof. The argument is quite similar to the argument used towards the end of the proof of Lemma 4.4. We therefore only replicate the main points.

Let $\mathcal{D} = \mathrm{Spec}(\mathcal{B}[x, y]/(p))$ be the closed subscheme of $\mathbb{A}_{\mathcal{B}}^2$ defined by p. Then $\mathcal{D}$ is an integral scheme of finite type over k such that the geometric generic fibre $\mathcal{D}_K = \mathcal{D} \times_{\mathcal{X}} \mathrm{Spec}(K) = \mathrm{Spec}(K[x, y]/(p))$ of $\mathcal{D} \to \mathcal{X}$ is birationally equivalent (over K) to C.

Let $\mathcal{V} = \mathrm{Spec}(\mathcal{B}[a_1, \ldots, a_m])$ be an open affine subscheme of $\mathcal{C}$. Then

$$\mathcal{V}_K = \mathcal{V} \times_{\mathcal{X}} \mathrm{Spec}(K) = \mathrm{Spec}(\mathcal{B}[a_1, \ldots, a_m] \otimes_{\mathcal{B}} K)$$

is a nonempty affine open subscheme of $C = \mathcal{C} \times_{\mathcal{X}} \mathrm{Spec}(K)$ and $\mathcal{D}_K$ and $\mathcal{V}_K$ are birationally equivalent (over K). In other words, the fields of fractions of $\mathcal{B}[\overline{x}, \overline{y}] \otimes_{\mathcal{B}} K$ and $\mathcal{B}[a_1, \ldots, a_m] \otimes_{\mathcal{B}} K$ are isomorphic as field extensions of K, where $\overline{x}$ and $\overline{y}$ stand for the images of x and y in $\mathcal{B}[x, y]/(p)$ respectively. Enlarging $\mathcal{B}$ if necessary, we can find elements $b \in \mathcal{B}[\overline{x}, \overline{y}]$ and $a \in \mathcal{B}[a_1, \ldots, a_m]$ such that $\mathcal{B}[\overline{x}, \overline{y}]_b$ and $\mathcal{B}[a_1, \ldots, a_n]_a$ are isomorphic over $\mathcal{B}$.

Localizing both sides one more time, we get an isomorphism between $\mathcal{B}[\overline{x}, \overline{y}]_{bf}$ and $\mathcal{B}[a_1, \ldots, a_m]_{a'}$ for some $a' \in \mathcal{B}[a_1, \ldots, a_m]$. This establishes the first claim of the lemma since $\mathcal{V}' = \mathrm{Spec}(\mathcal{B}[a_1, \ldots, a_m]_{a'})$ is an open subscheme of $\mathcal{C}$ and

$$\mathcal{B}[\overline{x}, \overline{y}]_{bf} = (\mathcal{B}[x, y]/(p))_{bf} = (\mathcal{B}[x][\eta])_{bf} = (\mathcal{B}[x]_f[\eta])_b.$$

By Chevalley's theorem, there exists a nonempty Zariski open subset $\mathcal{U}$ of $\mathcal{X}(k)$ such that $\mathcal{U}$ is contained in the image of the vertical maps in the commutative diagram

$$
\mathrm{Spec}((\mathcal{B}[x]_f[\eta])_b) \xrightarrow{\;\simeq\;} \mathcal{V}'.
$$
$$
\pi_1 \searrow \qquad \swarrow \pi_2
$$
$$
\mathcal{X}
$$

For $c \in \mathcal{U} \subseteq \mathcal{X}(k) \subseteq \mathcal{X}$ the fibre $\pi_1^{-1}(c)$ is the spectrum of $(\mathcal{B}[x]_f[\eta])_b \otimes_\mathcal{B} k = (k[x,y]/(p^c))_{(bf)^c}$; a ring with field of fractions $F^c = k(x)[y]/(p^c) = \mathcal{B}[x]_f[\eta] \otimes_{\mathcal{B}[x]_f} k(x)$. On the other hand, the fibre $\pi_2^{-1}(c) = \mathcal{V}' \times_\mathcal{X} \mathrm{Spec}(k)$ is an open subscheme of $\mathcal{C} \times_\mathcal{X} \mathrm{Spec}(k) = C^c$ and therefore has function field $k(C^c)$. Thus the function fields F^c and $k(C^c)$ of the fibres are isomorphic. On each fibre, h^c is the interpretation of h as a rational function on the fibre. $\qquad \square$

In the sequel, we will consider elements of $\mathcal{B}[x]_f[\eta]$ as rational functions on $\mathcal{C}$ as explained in Lemma 4.7. Note that if $h \in \mathcal{B}[x]_f[\eta]$ is interpreted as a rational function on $\mathcal{C}$, then h^{gen} is simply h, considered as an element of F. In this situation, we will therefore usually write h instead of h^{gen}.

Lemma 4.8. *Let $h \in \mathcal{B}[x]_f[\eta]$ and $P \in \mathcal{C}(\mathcal{B}) \subseteq C(K)$. Then there exists a nonempty Zariski open subset $\mathcal{U}$ of $\mathcal{X}(k)$ such that $\mathrm{res}_P(hdx)^c = \mathrm{res}_{P^c}(h^c dx)$ for all $c \in \mathcal{U}$.*

Proof. After enlarging $\mathcal{B}$ and replacing f with a multiple of f if necessary, we can write $hdx = h_1 dt$, where $h_1, t \in \mathcal{B}[x]_f[\eta]$ and t is a uniformizer at P. We then have $h = h_1 \delta(t)$ and so $h^c = h_1^c \delta(t^c)$, i.e., $h^c dx = h_1^c dt^c$ for all $c \in \mathcal{X}(k)$.

By Lemma 4.5, there exists a nonempty Zariski open subset $\mathcal{U}$ of $\mathcal{X}(k)$ such that t^c is a uniformizer at P^c and $\mathrm{res}_{P^c, t^c}(h_1^c) = \mathrm{res}_{P,t}(h_1)^c$ for all $c \in \mathcal{U}$. Therefore,

$$\mathrm{res}_P(hdx)^c = \mathrm{res}_P(h_1 dt)^c = \mathrm{res}_{P,t}(h_1)^c = \mathrm{res}_{P^c, t^c}(h_1^c) = \mathrm{res}_{P^c}(h_1^c dt^c) = \mathrm{res}_{P^c}(h^c dx).$$

$\qquad \square$

We next show that the $\mathbb{Z}$-modules Z_1 and Z_2 (as defined in Section 3.4) are preserved under many specializations.

Lemma 4.9. *Let $\mathbf{f} = (f_1, \ldots, f_m)$ be a tuple of elements of $\mathcal{B}[x]_f[\eta]$ and let $\mathcal{P}$ be the set of poles of the differential forms $f_1 dx, \ldots, f_m dx$ on C. Assume that $\mathcal{P} \subseteq \mathcal{C}(\mathcal{B}) \subseteq C(K) = C(K)$. Then there exists an ad-open subset $\mathcal{U}$ of $\mathcal{X}(k)$ such that for all $c \in \mathcal{U}$*

- *$\mathcal{P}^c$ is the set of poles of the differential forms $f_1^c dx, \ldots, f_m^c dx$ on C^c and*

- *$Z_1(\mathbf{f}^c, \mathcal{P}^c) = Z_1(\mathbf{f}, \mathcal{P})$.*

Moreover, there exists an ad×Jac-open subset $\mathcal{V}$ of $\mathcal{X}(k)$ such that, in addition to the above two properties, we also have $Z_2(\mathbf{f}^c, \mathcal{P}^c) = Z_2(\mathbf{f}, \mathcal{P})$ for all $c \in \mathcal{V}$.

Proof. To resolve the first item, let us first discuss how the poles of a differential form $\omega = hdx$ are determined by h and x. To see if ω has a pole at a place P, one can write $\omega = h_1 dt$ with $t = t_P$ a uniformizer at P and then see if $\nu_P(\omega) = \nu_P(h_1)$ is negative. But $hdx = h_1 dt$ entails $h_1 = h\delta_t(x)$, where δ_t is the derivation determined by $\delta_t(t) = 1$. So $\nu_P(h_1) = \nu_P(h) + \nu_P(\delta_t(x))$. Using [Sti09, Prop. 4.2.7], we see that

$$\nu_P(\delta_t(x)) = \begin{cases} \nu_P(x) - 1 & \text{if } \nu_P(x) \neq 0, \\ \nu_P(x - a_P) - 1 & \text{if } \nu_P(x) = 0, \end{cases}$$

where a_P denotes the value of x at P, i.e., the image of x in the residue field $\mathcal{O}_P/\mathfrak{m}_P$. Thus $\omega = hdx$ has a pole at P if and only if ($\nu_P(x) \neq 0$ and $\nu_P(h) + \nu_P(x) - 1 \leq -1$) or ($\nu_P(x) = 0$ and $\nu_P(h) + \nu_P(x - a_P) - 1 \leq -1$).

Now let h be one of the f_i's. After enlarging $\mathcal{B}$ if necessary (Remark 4.1), we may assume that all zeros and poles of x and h lie in $\mathcal{C}(\mathcal{B})$. Then, by Lemma 4.4, there exists

a nonempty Zariski open subset $\mathcal{U}_1$ of $\mathcal{X}(k)$ such that the principal divisors defined by x and h are preserved under all specializations belonging to $\mathcal{U}_1$. Similarly, by the same lemma, and after enlarging $\mathcal{B}$ if necessary, we can also assume that for every $c \in \mathcal{U}_1$ and every pole P of h we have $\nu_P(x - a_P) = \nu_{P^c}((x - a_P)^c) = \nu_{P^c}(x^c - a_{P^c})$.

In particular, for $c \in \mathcal{U}_1$, every zero or pole of $x^c \in k(C^c)$ is the specialization of a zero or pole of $x \in F/K$. For a place Q of $k(C^c)/k$ that is not the specialization of a zero or pole of x or of a pole of h, we then have $\nu_Q(x^c) = 0$ and $\nu_Q(h^c) + \nu_Q(x^c - a_Q) - 1 \geq 0 + 0 = 0$. So, by the above consideration, Q is not a pole $h^c dx$.

By construction, for those places Q of $k(C^c)/k$ that come from zeros or poles of x or from poles of h, all the relevant valuations are preserved under specialization and so we see that for $c \in \mathcal{U}_1$ the poles of $h^c dx$ are exactly the specializations of the poles of hdx. Thus we can find a nonempty Zariski open subset $\mathcal{U}_2$ of $\mathcal{X}(k)$ such that the first item of the lemma is satisfied for all $c \in \mathcal{U}_2$.

By Lemma 4.8, there exists a nonempty Zariski open subset $\mathcal{U}_3$ of $\mathcal{X}(k)$ such that $\mathrm{res}_P(f_i dx)^c = \mathrm{res}_{P^c}(f_i^c dx)$ for all $P \in \mathcal{P}$ and $i = 1, \ldots, m$. Thus $Z_1(\mathbf{f}, \mathcal{P}) \subseteq Z_1(\mathbf{f}^c, \mathcal{P}^c)$ for all $c \in \mathcal{U}_2 \cap \mathcal{U}_3$. For the reverse inclusion, let Γ be the finitely generated subgroup of $(\mathcal{B}, +)$ generated by 1 and $\mathrm{res}_P(f_i dx)$ ($P \in \mathcal{P}$, $i \in \{1, \ldots, m\}$). Let $\mathcal{U}$ be a nonempty ad-open subset contained in $\mathcal{U}_2 \cap \mathcal{U}_3 \cap W_{\mathcal{X}}(\mathbb{G}_a, \Gamma)$.

Let $c \in \mathcal{U}$ and $(d_1, \ldots, d_m) \in Z_1(\mathbf{f}^c, \mathcal{P}^c)$, i.e., $d_{P,c} = \sum_{i=1}^m d_i \, \mathrm{res}_{P^c}(f_i^c dx) \in \mathbb{Z}$ for all $P \in \mathcal{P}$ and $\sum_{P \in \mathcal{P}} d_{P,c} = 0$. Then

$$\left(\sum_{i=1}^m d_i \, \mathrm{res}_P(f_i dx) - d_{P,c} \right)^c = \sum_{i=1}^m d_i \, \mathrm{res}_P(f_i dx)^c - d_{P,c} = \sum_{i=1}^m d_i \, \mathrm{res}_{P^c}(f_i^c dx) - d_{P,c} = 0$$

for all $P \in \mathcal{P}$. As $c \in W_{\mathcal{X}}(\mathbb{G}_a, \Gamma)$, we can conclude that $\sum_{i=1}^m d_i \, \mathrm{res}_P(f_i dx) - d_{P,c} = 0$. In particular, $\sum_{i=1}^m d_i \, \mathrm{res}_P(f_i dx) \in \mathbb{Z}$. Moreover, $\sum_{P \in \mathcal{P}} \sum_{i=1}^m d_i \, \mathrm{res}_P(f_i dx) = \sum_{P \in \mathcal{P}} d_{P,c} = 0$. Thus $(d_1, \ldots, d_m) \in Z_1(\mathbf{f}, \mathcal{P})$ and so $Z_1(\mathbf{f}, \mathcal{P}) = Z_1(\mathbf{f}^c, \mathcal{P}^c)$ for all $c \in \mathcal{U}$.

Our next goal is to find a nonempty Zariski open subset $\mathcal{U}_4$ of $\mathcal{X}(k)$ such that $Z_2(\mathbf{f}, \mathcal{P}) \subseteq Z_2(\mathbf{f}^c, \mathcal{P}^c)$ for all $c \in \mathcal{U}_2 \cap \mathcal{U}_3 \cap W_{\mathcal{X}}(\mathbb{G}_a, \Gamma) \cap \mathcal{U}_4$.

Let $(e_{1,\ell}, \ldots, e_{m,\ell})_{1 \leq \ell \leq n}$ be a basis of the $\mathbb{Z}$-module $Z_2(\mathbf{f}, \mathcal{P})$ and for $\ell = 1, \ldots, n$ write $\sum_{P \in \mathcal{P}} e_{\ell, P} P = (h_\ell)$, with $h_\ell \in F^\times$ and $e_{\ell, P} = \sum_{i=1}^m e_{i,\ell} \, \mathrm{res}_P(f_i dx) \in \mathbb{Z}$. Replacing f with a mulitple and enlarging $\mathcal{B}$ if necessary, we may assume that $h_1, \ldots, h_n, h_1^{-1}, \ldots, h_n^{-1} \in \mathcal{B}[x]_f[\eta]$. By Lemma 4.4, there exists a nonempty Zariski open subset $\mathcal{U}_4$ of $\mathcal{X}(k)$ such that $(h_\ell^c) = \sum_{P \in \mathcal{P}} e_{\ell, P} P^c$ for $\ell = 1, \ldots, n$ and all $c \in \mathcal{U}_4$.

Let $c \in \mathcal{U}_2 \cap \mathcal{U}_3 \cap W_{\mathcal{X}}(\mathbb{G}_a, \Gamma) \cap \mathcal{U}_4$ and $(d_1, \ldots, d_m) \in Z_2(\mathbf{f}, \mathcal{P})$. Then there exist $a_1, \ldots, a_n \in \mathbb{Z}$ such that $d_i = \sum_{\ell=1}^n a_\ell e_{i,\ell}$ for $i = 1, \ldots, m$. Moreover, since $\sum_{i=1}^m d_i \, \mathrm{res}_P(f_i dx) \in \mathbb{Z}$, we have

$$\sum_{i=1}^m d_i \, \mathrm{res}_P(f_i dx) = \left(\sum_{i=1}^m d_i \, \mathrm{res}_P(f_i dx) \right)^c = \sum_{i=1}^m d_i \, \mathrm{res}_P(f_i dx)^c = \sum_{i=1}^m d_i \, \mathrm{res}_{P^c}(f_i^c dx)$$

for all $P \in \mathcal{P}$. Therefore

$$((h_1^{a_1} \ldots h_n^{a_n})^c) = ((h_1^c)^{a_1} \ldots ((h_n)^c)^{a_n}) = \sum_{\ell=1}^{n} a_\ell(h_\ell^c) = \sum_{\ell=1}^{n} \sum_{P \in \mathcal{P}} a_\ell e_{\ell,P} P^c =$$

$$= \sum_{\ell=1}^{n} \sum_{P \in \mathcal{P}} \sum_{i=1}^{m} a_\ell e_{i,\ell} \operatorname{res}_P(f_i dx) P^c = \sum_{P \in \mathcal{P}} \sum_{i=1}^{m} d_i \operatorname{res}_P(f_i dx) P^c =$$

$$= \sum_{P \in \mathcal{P}} \sum_{i=1}^{m} d_i \operatorname{res}_{P^c}(f_i^c dx) P^c.$$

This shows that $(d_1, \ldots, d_m) \in Z_2(\mathbf{f}^c, \mathcal{P}^c)$. So $Z_2(\mathbf{f}, \mathcal{P}) \subseteq Z_2(\mathbf{f}^c, \mathcal{P}^c)$ for all $c \in \mathcal{U}_2 \cap \mathcal{U}_3 \cap W_{\mathcal{X}}(\mathbb{G}_a, \Gamma) \cap \mathcal{U}_4$.

For the reverse inclusion, we can use Lemma 4.6 to find an ad×Jac-open subset $\mathcal{V}_1$ of $\mathcal{X}(k)$ such that for all $c \in \mathcal{V}_1$ and all $d_P \in \mathbb{Z}$, $(P \in \mathcal{P})$, if $\sum_{P \in \mathcal{P}} d_P P \in \operatorname{Div}^0(C)$ is not principal, then $\sum_{P \in \mathcal{P}} d_P P^c \in \operatorname{Div}^0(C^c)$ is not principal. For all $c \in \mathcal{U}_2 \cap \mathcal{U}_3 \cap W_{\mathcal{X}}(\mathbb{G}_a, \Gamma) \cap \mathcal{U}_4 \cap \mathcal{V}_1$ we then have $Z_2(\mathbf{f}, \mathcal{P}) = Z_2(\mathbf{f}^c, \mathcal{P}^c)$. $\square$

We are now prepared to show that logarithmic independence is preserved on an Ad×Jac-open subset.

Theorem 4.10. *Let $f_1, \ldots, f_m \in \mathcal{B}[x]_f[\eta]$ be logarithmically independent over F. Then there exists an ad×Jac-open subset $\mathcal{U}$ of $\mathcal{X}(k)$ such that $f_1^c, \ldots, f_m^c$ are logarithmically independent over F^c for all $c \in \mathcal{U}$.*

Proof. Set $\mathbf{f} = (f_1, \ldots, f_m)$ and let $\mathcal{P}$ be the set of poles of $f_1, \ldots, f_m \in F$. Fix a basis $\{(e_{1,\ell}, \ldots, e_{m,\ell}) | \ell = 1, \ldots, n\}$ of $Z_2(\mathbf{f}, \mathcal{P})$ and for $\ell = 1, \ldots, n$ write

$$\sum_{P \in \mathcal{P}} \left(\sum_{i=1}^{m} e_{i,\ell} \operatorname{res}_P(f_i dx) \right) P = (h_\ell) \quad \text{with} \quad h_\ell \in F^\times. \tag{36}$$

After enlarging $\mathcal{B}$ and replacing f with a multiple if necessary, we can assume that

- the set $\mathcal{P}$ belongs to $\mathcal{C}(\mathcal{B}) \subseteq \mathcal{C}(K) = C(K)$ and

- $h_1, \ldots, h_n, h_1^{-1}, \ldots, h_n^{-1} \in \mathcal{B}[x]_f[\eta]$.

Let d be the degree of η over $K(x)$. As $a_\ell = \frac{\delta(h_\ell)}{h_\ell} - \sum_{i=1}^{m} e_{i,\ell} f_i \in \mathcal{B}[x]_f[\eta]$ for $\ell = 1, \ldots, n$, we can find $r, s \in \mathbb{N}$ and $b_{i,j,\ell} \in \mathcal{B}$ such that

$$a_\ell = \frac{1}{f^r} \left(\sum_{i=1}^{s} \sum_{j=1}^{d} b_{i,j,\ell} x^i \eta^j \right)$$

for $\ell = 1, \ldots, n$. Since $f_1, \ldots, f_m$ are logarithmically independent over F, it follows from Lemma 3.26 that the differential forms $a_1 dx, \ldots, a_n dx$ are $\mathbb{Z}$-linearly independent. Note that the latter condition is equivalent to: If $d_1, \ldots, d_n \in \mathbb{Z}$ such that $d_1 b_{i,j,1} + \ldots + d_n b_{i,j,n} = 0$ for all $1 \leq i \leq s$, $1 \leq j \leq d$, then $d_1 = \ldots = d_n = 0$.

Let Γ be the subgroup of $\mathbb{G}_a(\mathcal{B}) = (\mathcal{B}, +)$ generated by all $b_{i,j,\ell}$'s and let $\mathcal{U}_1 = W_{\mathcal{X}}(\mathbb{G}_a, \Gamma)$ be the ad-open subset of $\mathcal{X}(k)$ defined by Γ. By Lemma 4.9 there exists an ad×Jac-open subset $\mathcal{U}_2$ of of $\mathcal{X}(k)$ such that $\mathcal{P}^c$ is the set of poles of $\mathbf{f}^c$ and $Z_2(\mathbf{f}^c, \mathcal{P}^c) = Z_2(\mathbf{f}, \mathcal{P})$ for all $c \in \mathcal{U}_2$. Moreover, by Lemmas 4.4 and 4.8, we can find a nonempty Zariski

61

open subset $\mathcal{U}_3$ of $\mathcal{X}(k)$ such that the principal divisors defined by h_ℓ, $(\ell = 1, \ldots, n)$ are preserved under specialization and $\mathrm{res}_P(f_i dx)^c = \mathrm{res}_{P^c}(f_i^c dx)$ $(i = 1, \ldots, m,\ P \in \mathcal{P})$ for all $c \in \mathcal{U}_3$.

Let $\mathcal{U}$ be an ad×Jac-open subset of $\mathcal{X}(k)$ contained in $\mathcal{U}_1 \cap \mathcal{U}_2 \cap \mathcal{U}_3$. We claim that $f_1^c, \ldots, f_m^c$ are logarithmically independent over F^c for all $c \in \mathcal{U}$.

Let $c \in \mathcal{U}$. Using that $c \in \mathcal{U}_3$, we can specialize (36) to

$$\sum_{P \in \mathcal{P}} \left(\sum_{i=1}^{m} e_{i,\ell} \, \mathrm{res}_{P^c}(f_i^c dx) \right) = (h_\ell^c)$$

for $\ell = 1, \ldots, n$. Furthermore, $a_\ell^c = \left(\frac{\delta(h_\ell)}{h_\ell} - \sum_{i=1}^{m} e_{i,\ell} f_i \right)^c = \frac{\delta(h_\ell^c)}{h_\ell^c} - \sum_{i=1}^{m} e_{i,\ell} f_i^c$. Using that $Z_2(\mathbf{f}^c, \mathcal{P}^c) = Z_2(\mathbf{f}, \mathcal{P})$, the criterion of Lemma 3.26 states that $f_1^c, \ldots, f_m^c$ are logarithmically independent over F^c if and only if $a_1^c, \ldots, a_n^c$ are $\mathbb{Z}$-linearly independent. Note that the degree of η^c over $k(x)$ equals d, the degree of η over $K(x)$ (cf. the discussion before Lemma 4.7). As

$$a_\ell^c = \frac{1}{(f^c)^r} \left(\sum_{i=1}^{s} \sum_{j=1}^{d} b_{i,j,\ell}^c x^i (\eta^c)^j \right),$$

we see that $a_1^c, \ldots, a_n^c$ are $\mathbb{Z}$-linearly independent if and only if $d_1 b_{i,j,1}^c + \ldots + d_n b_{i,j,n}^c = 0$ for $d_1, \ldots, d_n \in \mathbb{Z}$, $1 \leq i \leq s$, $1 \leq j \leq d$ implies $d_1 = \ldots = d_n = 0$. But $d_1 b_{i,j,1}^c + \ldots + d_n b_{i,j,m}^c = 0$ implies, by the injectivity of $\Gamma \to k$, $\gamma \mapsto \gamma^c$, that $d_1 b_{i,j,1} + \ldots + d_n b_{i,j,n} = 0$. Thus $a_1^c, \ldots, a_n^c$ are $\mathbb{Z}$-linearly independent and $f_1^c, \ldots, f_m^c$ are logarithmically independent as desired. $\qquad \square$

Remark 4.11. *In case $\eta = 1$, i.e., $F = K(x)$, the Jac-open subset is not needed, i.e., the set $\mathcal{U}$ in Theorem 4.10 can be chosen to be ad-open.*

Proof. In this case we can choose $\mathcal{C} = \mathbb{P}^1_{\mathcal{B}}$ and so $C^c = \mathbb{P}^1_k$ for all $c \in \mathcal{X}(k)$. In this case Lemma 4.6 is trivial because all degree zero divisors are principal. Thus Lemma 4.6 does not create a Jac-open set and also the subsequent results (Lemma 4.9 and Theorem 4.10) can make do without the Jac-open set. $\qquad \square$

4.4 The setup for specializing Picard-Vessiot rings

Let $k \subseteq k'$ be an inclusion of algebraically closed fields. In Lemma 3.11 we have seen how a Picard-Vessiot ring $R/k'(x)$ can be spread out to a differential torsor $\mathcal{R}/\mathcal{B}[x]_f$. In this section we discuss some first properties of $\mathcal{R}$ and its specializations R^c. We now describe our framework for specializing Picard-Vessiot rings.

Notation 4.12.

- k is an algebraically closed field of characteristic zero;

- $\mathcal{B}$ is a finitely generated k-algebra and an integral domain;

- $\mathcal{X} = \mathrm{Spec}(\mathcal{B})$;

- K is the algebraic closure of the field of fractions $k(\mathcal{B})$ of $\mathcal{B}$;

- $\mathcal{G}$ is an affine group scheme of finite type over $\mathcal{B}$;

- $f \in \mathcal{B}[x]$ is a monic polynomial and $\mathcal{B}[x]_f$ is a differential ring with respect to $\delta = \frac{d}{dx}$;

- $\mathcal{A} \in \mathcal{B}[x]_f^{n \times n}$;

- $\mathcal{R}/\mathcal{B}[x]_f$ is a differential $\mathcal{G}$-torsor for $\delta(y) = \mathcal{A}y$ with fundamental matrix $\mathcal{Y} \in \mathrm{GL}_n(\mathcal{R})$ such that $\mathcal{R}$ is flat over $\mathcal{B}[x]_f$;

- $R^c = \mathcal{R} \otimes_{\mathcal{B}[x]_f} k(x)$, where $c \in \mathcal{X}(k) = \mathrm{Hom}_k(\mathcal{B}, k)$ and the tensor product is formed using the extension of $c \colon \mathcal{B} \to k$ to $c \colon \mathcal{B}[x]_f \to k(x)$ determined by $c(x) = x$;

- $Y^c = \mathcal{Y} \otimes 1 \in \mathrm{GL}_n(R^c)$ is the image of $\mathcal{Y}$ in R^c;

- $A^c \in k(x)^{n \times n}$ is obtained from $\mathcal{A}$ by applying $c \colon \mathcal{B}[x]_f \to k(x)$ to the coefficients of $\mathcal{A}$;

- $G^c = \mathcal{G}_c$ is the algebraic group over k obtained from $\mathcal{G}$ by base change via $c \colon \mathcal{B} \to k$;

- $R^{\mathrm{gen}} = \mathcal{R} \otimes_{\mathcal{B}[x]_f} K(x)$ is δ-simple;

- $Y^{\mathrm{gen}} = \mathcal{Y} \otimes 1 \in \mathrm{GL}_n(R^{\mathrm{gen}})$ is the image of $\mathcal{Y}$ in R^{gen};

- $G^{\mathrm{gen}} = \mathcal{G}_K$ is the algebraic group over K obtained from $\mathcal{G}$ by base change via $\mathcal{B} \to K$.

Furthermore, for $h \in \mathcal{R}$, denote with $h^c = h \otimes 1 \in R^c$ the image of h in R^c. Similarly, $h^{\mathrm{gen}} = h \otimes 1 \in R^{\mathrm{gen}}$ denotes the image of h in R^{gen}.

For the remainder of Section 4 we assume Notation 4.12.

Notation 4.12 gives a precise meaning to the idea of a family of potential Picard-Vessiot rings for a family of linear differential equations with prescribed potential differential Galois groups. (Lemmas 4.14 and 4.15 below elaborate this point.) We think of $\mathcal{R}$ as defining the family $(R^c)_{c \in \mathcal{X}(k)}$ and we would like to compare the individual R^c's with the ring R^{gen} at the generic fibre.

We now explore some first consequences of Notation 4.12.

Lemma 4.13. *The ring $\mathcal{R}$ is an integral domain and the morphisms $\mathcal{B}[x]_f \to \mathcal{R}$, $\mathcal{B} \to \mathcal{B}[\mathcal{G}]$ and $\mathcal{R} \to R^{\mathrm{gen}}$ are injective.*

Proof. Suppose that $h \in \mathcal{B}[x]_f$ is a nonzero element of the kernel of $\mathcal{B}[x]_f \to \mathcal{R}$. Then the image h^{gen} of h in R^{gen} is zero but also a unit. Thus R^{gen} must be the zero ring. This contradicts the assumption that R^{gen} is δ-simple.

Assume that $b \in \mathcal{B}$ lies in the kernel of $\mathcal{B} \to \mathcal{B}[\mathcal{G}]$. Then the image of b in $\mathcal{R} \otimes_{\mathcal{B}} \mathcal{B}[\mathcal{G}]$ is zero. But then the second diagram of Lemma 3.3 implies that $b = 0$.

As $\mathcal{R}$ is flat over $\mathcal{B}[x]_f$ it is clear that $\mathcal{R} \to R^{\mathrm{gen}}$ is injective. From this it follows that $\mathcal{R}$ is an integral domain because differentially simple rings are integral domains. $\square$

Because $\mathcal{R} \to R^{\mathrm{gen}}$ is injective, it is not really necessary to distinguish between an element $h \in \mathcal{R}$ and its image h^{gen} in R^{gen}. However, we will sometimes use the notation h^{gen} to emphasize that we are considering h as an element of R^{gen}.

At the generic fibre we have a Picard-Vessiot ring:

Lemma 4.14. *The $K(x)$-δ-algebra R^{gen} is a Picard-Vessiot ring for $\delta(y) = \mathcal{A}y$ with fundamental matrix Y^{gen} and differential Galois group G^{gen}.*

Proof. As $\mathcal{R}/\mathcal{B}[x]_f$ is a differential $\mathcal{G}$-torsor, $\mathcal{R}\otimes_\mathcal{B}K/\mathcal{B}[x]_f\otimes_\mathcal{B}K$ is a differential G^{gen}-torsor by Lemma 3.7 (i). But $\mathcal{R}\otimes_\mathcal{B}K = \mathcal{R}\otimes_{\mathcal{B}[x]_f}K[x]_f$ and $\mathcal{B}[x]_f\otimes_\mathcal{B}K = K[x]_f$. Thus $R^{\text{gen}}/K(x)$ is a differential G^{gen}-torsor by Lemma 3.7 (ii).

As $\mathcal{R} = \mathcal{B}[x]_f[\mathcal{Y}, \frac{1}{\det(\mathcal{Y})}]$ and $\delta(\mathcal{Y}) = \mathcal{A}\mathcal{Y}$, we have $R^{\text{gen}} = K(x)[Y^{\text{gen}}, \frac{1}{\det(Y^{\text{gen}})}]$ and $\delta(Y^{\text{gen}}) = AY^{\text{gen}}$. Because R^{gen} is assumed to be δ-simple, we see that $R^{\text{gen}}/K(x)$ is a Picard-Vessiot ring for $\delta(y) = Ay$.

It follows from [BHHW18, Prop. 1.12] that the differential Galois group of $R^{\text{gen}}/K(x)$ is G^{gen}. $\square$

So, reversing the idea of Lemma 3.11, we can think of $\mathcal{R}/\mathcal{B}[x]_f$ as having been obtained by "spreading out" the Picard-Vessiot ring $R^{\text{gen}}/K(x)$. At the special fibres we either have nothing or a ring that "looks like" a Picard-Vessiot ring:

Lemma 4.15. *If $c \in \mathcal{X}(k)$ is such that R^c is not the zero ring, then $R^c/k(x)$ is a differential G^c-torsor for $\delta(y) = A^cy$ with fundamental matrix Y^c. Moreover, there exists a nonempty Zariski open subset $\mathcal{U}$ of $\mathcal{X}(k)$ such that R^c is not the zero ring for every $c \in \mathcal{U}$.*

Proof. Assume that R^c is not the zero ring. As in Lemma 4.14, using Lemma 3.7, one sees that $R^c/k(x)$ is a differential G^c-torsor. Furthermore, $R^c = k(x)[Y^c, \frac{1}{\det(Y^c)}]$ and $\delta(Y^c) = A^cY^c$. Let T be a k-algebra and $g \in G^c(T)$. When interpreted as an element of $\mathcal{G}(T)$, g acts on $\mathcal{Y} \otimes 1 \in \text{GL}_n(\mathcal{R} \otimes_\mathcal{B} T)$ by multiplication with a matrix $[g] \in \text{GL}_n(T)$. Thus g also acts on $Y^c \otimes 1 \in \text{GL}_n(R^c \otimes_k T)$ by multiplication with $[g]$. This proves the first claim of the lemma.

For the second claim, note that $\mathcal{B}[x]_f \subseteq \mathcal{R}$ by Lemma 4.13 and that $\mathcal{R}$ is a finitely generated $\mathcal{B}[x]_f$-algebra. By [Bou72, Cor. 3, Chapter V, §3.1] (applied with $b = 1$) there exists a nonzero $h \in \mathcal{B}[x]_f$ such that any morphism ψ (of rings) from $\mathcal{B}[x]_f$ into an algebraically closed field with $\psi(h) \neq 0$, extends to a morphism on $\mathcal{R}$. Without loss of generality we may assume $h \in \mathcal{B}[x]$. Let $a \in \mathcal{B}$ be the leading coefficient of h and let $\mathcal{U}$ be the Zariski open subset of $\mathcal{X}(k)$ defined by a, i.e., $\mathcal{U}$ is the complement of the vanishing locus of a.

Let $c \in \mathcal{U}$. We will show that R^c is not the zero ring. Taking ψ as $\psi\colon \mathcal{B}[x]_f \xrightarrow{c} k(x) \to \overline{k(x)}$, we see that $\psi(h) \neq 0$ and so ψ extends to a morphism $\psi\colon \mathcal{R} \to \overline{k(x)}$. Then $\mathcal{R} \otimes_{\mathcal{B}[x]_f} k(x) \to \overline{k(x)}$, $r \otimes s \mapsto \psi(r)s$ is a morphism of rings. Thus $\mathcal{R} \otimes_{\mathcal{B}[x]_f} k(x)$ cannot be the zero ring. $\square$

We can do slightly better:

Lemma 4.16. *There exists a nonempty Zariski open subset $\mathcal{U}$ of $\mathcal{X}(k)$ such that R^c is an integral domain for all $c \in \mathcal{U}$.*

Proof. The key fact from algebraic geometry that we will use is that being geometrically integral "spreads out" from the generic fibre ([Poo17, Theorem 3.2.1 (ii)]). More concretely, if $\mathcal{B} \subseteq \mathcal{R}$ is an inclusion of finitely generated k-algebras, such that $\mathcal{R} \otimes_\mathcal{B} K$ is an integral domain (where, as usual, K is the algebraic closure of the field of fractions $k(\mathcal{B})$ of $\mathcal{B}$), then there exists a nonempty Zariski open subset $\mathcal{U}$ of $\text{Spec}(\mathcal{B})$ such that $\mathcal{R} \otimes_\mathcal{B} \overline{k(\mathfrak{p})}$ is an integral domain for every $\mathfrak{p} \in \mathcal{U}$.

To apply this to our situation, note that $\mathcal{R}\otimes_\mathcal{B}K$ is an integral domain because $\mathcal{R}\otimes_\mathcal{B}K = \mathcal{R} \otimes_{\mathcal{B}[x]_f} K[x]_f \subseteq \mathcal{R} \otimes_{\mathcal{B}[x]_f} K(x) = R^{\text{gen}}$ and the latter is an integral domain.

By the first paragraph, there exists a nonempty Zariski open subset $\mathcal{U}$ of $\mathcal{X}(k)$ such that $\mathcal{R} \otimes_{\mathcal{B}} k$ is an integral domain for all $c \in \mathcal{U}$. As

$$R^c = \mathcal{R} \otimes_{\mathcal{B}[x]_f} k(x) = (\mathcal{R} \otimes_{\mathcal{B}[x]_f} k[x]_{f^c}) \otimes_{k[x]_{f^c}} k(x) = (\mathcal{R} \otimes_{\mathcal{B}} k) \otimes_{k[x]_{f^c}} k(x),$$

we see that R^c is a localization of the integral domain $R \otimes_{\mathcal{B}} k$ for all $c \in \mathcal{U}$. So R^c is either the zero ring or an integral domain. Thus the claim follows from Lemma 4.15. $\qquad\square$

The following example illustrates Lemma 4.16.

Example 4.17. Let a be a unit of $\mathcal{B}[x]_f$ such that a is not a square in $k(\mathcal{B})(x)$. Then $\mathcal{B}[x]_f[y]/(y^2 - a) = \mathcal{B}[x]_f[\eta]$ is an integral domain and naturally a differential ring (with $\delta(\eta) = \frac{\delta(a)}{2a}\eta$). Let $b \in \mathcal{B}[x]_f$. As in Example 3.6 set

$$\mathcal{R} = \mathcal{B}[x]_f[\eta][y_1, y_2, y_1^{-1}, y_2^{-1}] = \mathcal{B}[x]_f[X, \tfrac{1}{\det(X)}]/(p_1, p_2) = \mathcal{B}[x]_f[\mathcal{Y}, \tfrac{1}{\det(\mathcal{Y})}],$$

where $\delta(y_1) = (b + \eta)y_1$, $\delta(y_2) = (b - \eta)y_2$,

$$p_1 = X_{21}X_{22} - (b^2 - a)X_{11}X_{12}, \qquad p_2 = X_{21}X_{12} + X_{22}X_{11} - 2bX_{11}X_{12},$$

$$\mathcal{A} = \begin{pmatrix} 0 & 1 \\ a + \delta(b) - b^2 - \frac{\delta(a)b}{2a} & 2b + \frac{\delta(a)}{2a} \end{pmatrix} \in \mathcal{B}[x]_f^{2\times 2},$$

and $\delta(X) = \mathcal{A}X$. Then $\mathcal{R}$ is an integral domain and $\mathcal{R}/\mathcal{B}[x]_f$ is a differential $\mathcal{G}$-torsor for $\delta(y) = \mathcal{A}y$, where $\mathcal{G}$ is the group scheme of 2×2 monomial matrices over $\mathcal{B}$ (as seen in Example 3.6).

We claim that for $c \in \mathcal{X}(k)$ the $k(x)$-δ-algebra $R^c = \mathcal{R} \otimes_{\mathcal{B}[x]_f} k(x)$ is an integral domain if and only if a^c is not a square in $k(x)$. Note that $\mathcal{R}$ is a Laurent-polynomial ring in y_1, y_2 over $\mathcal{B}[x]_f[\eta]$. Therefore, $\mathcal{R} \otimes_{\mathcal{B}[x]_f} k(x)$ is a Laurent polynomial ring over $\mathcal{B}[x]_f[\eta] \otimes_{\mathcal{B}[x]_f} k(x)$. The latter is an integral domain, if and only if $\mathcal{B}[x]_f[\eta] \otimes_{\mathcal{B}[x]_f} k(x) = k(x)[y]/(y^2 - a^c)$ is an integral domain and this is the case if and only if a^c is not a square in $k(x)$.

Thus, for example, for $\mathcal{B} = k[\alpha, \beta]$, with α, β algebraically independent over k and $a = x^2 + \alpha x + \beta$, we see that R^c is an integral domain if and only if $c \in \mathcal{U}$, where $\mathcal{U} \subseteq \mathcal{X}(k)$ is the Zariski open subset where the discriminant $\alpha^2 - 4\beta$ does not vanish.

By Lemma 4.15 the R^c's "look like" Picard-Vessiot rings for $\delta(y) = A^c y$ with differential Galois group G^c. The only missing piece of information is whether or not R^c is δ-simple. If R^c is δ-simple, then $R^c/k(x)$ is a Picard-Vessiot ring with differential Galois group G^c.

The main question is: Are there "many" c's in $\mathcal{X}(k)$ such that $R^c/k(x)$ is Picard-Vessiot? (In Theorem 4.26 we will see that the answer is yes.)

The following example illustrates that the set of all $c \in \mathcal{X}(k)$ such that R^c is Picard-Vessiot is in general not constructible.

Example 4.18. Let $\mathcal{B} = k[\alpha]$, with α a variable over k and set $f = x$. Let

$$\mathcal{A} = \begin{pmatrix} 0 & 1 \\ (\frac{\alpha}{x})^2 - 1 & -\frac{1}{x} \end{pmatrix} \in \mathcal{B}[x]_f^{2\times 2} = k[\alpha, x]_x^{2\times 2}$$

be the companion matrix of Bessel's differential equation $\delta^2(y) + \frac{1}{x}\delta(y) + (1 - (\frac{\alpha}{x})^2)y = 0$. Let X be a 2×2 matrix of indeterminates over $\mathcal{B}[x]_f$. Consider $\mathcal{B}[x]_f[X, \frac{1}{\det(X)}]$ as a $\mathcal{B}[x]_f$-δ-algebra via $\delta(X) = \mathcal{A}X$. Then

$$\delta(\det(X) - \tfrac{1}{x}) = \delta(\det(X)) + \tfrac{1}{x^2} = -\tfrac{1}{x}\det(X) + \tfrac{1}{x^2} = -\tfrac{1}{x}(\det(X) - \tfrac{1}{x})$$

and so $(\det(X) - \frac{1}{x})$ is a δ-ideal of $\mathcal{B}[x]_f[X, \frac{1}{\det(X)}]$ and $\mathcal{R} = \mathcal{B}[x]_f[X, \frac{1}{\det(X)}]/(\det(X) - \frac{1}{x})$ is a $\mathcal{B}[x]_f$-δ-algebra. Let $\mathcal{Y} \in \mathrm{GL}_n(\mathcal{R})$ denote the image of X in $\mathcal{R}$. Let $\mathcal{G} = \mathrm{SL}_2 = \mathrm{SL}_{2,\mathcal{B}}$ be the group scheme SL_2 over $\mathcal{B}$. Then $\mathcal{G}$ acts on $\mathcal{R}/\mathcal{B}[x]_f$: For a $\mathcal{B}$-algebra $\mathcal{T}$, a $g \in \mathrm{SL}_2(\mathcal{T})$ defines a $\mathcal{B}[x]_f \otimes_\mathcal{B} \mathcal{T}$-$\delta$-automorphism $g : \mathcal{R} \otimes_\mathcal{B} \mathcal{T} \to \mathcal{R} \otimes_\mathcal{B} \mathcal{T}$ by $g(\mathcal{Y} \otimes 1) = (\mathcal{Y} \otimes 1)(1 \otimes g)$. The corresponding morphism $\rho : \mathcal{R} \to \mathcal{R} \otimes_\mathcal{B} \mathcal{B}[\mathrm{SL}_2]$ of $\mathcal{B}[x]_f$-δ-algebras (as in Lemma 3.3) is given by $\rho(\mathcal{Y}) = (\mathcal{Y} \otimes 1)(1 \otimes T)$, where $T \in \mathcal{B}[\mathrm{SL}_2]^{2 \times 2}$ is the matrix of coordinate functions on SL_2. The morphism $\mathcal{R} \otimes_{\mathcal{B}[x]_f} \mathcal{R} \to \mathcal{R} \otimes_\mathcal{B} \mathcal{B}[\mathcal{G}]$, $a \otimes b \mapsto (a \otimes 1) \cdot \rho(b)$ is an isomorphism, its inverse is determined by $1 \otimes T \mapsto (\mathcal{Y} \otimes 1)^{-1}(1 \otimes \mathcal{Y})$. So $\mathcal{R}/\mathcal{B}[x]_f$ is a differential $\mathcal{G}$-torsor for $\delta(y) = \mathcal{A}y$.

From a more geometric perspective, if $\mathcal{Q}$ is any ring (e.g., $\mathcal{B}[x]_f$) and $a \in \mathcal{Q}^\times$, it is clear that the closed subscheme $\mathcal{Z}$ of $\mathrm{GL}_{2,\mathcal{Q}}$ defined by $\det(X) - a$ is an $\mathrm{SL}_{2,\mathcal{Q}}$-torsor: For any $\mathcal{Q}$-algebra $\mathcal{Q}'$, the map $\mathcal{Z}(\mathcal{Q}') \times \mathrm{SL}_2(\mathcal{Q}') \to \mathcal{Z}(\mathcal{Q}') \times \mathcal{Z}(\mathcal{Q}')$, $(z, g) \mapsto (z, zg)$ is bijective with inverse $(z_1, z_2) \mapsto (z_1, z_1^{-1}z_2)$.

The differential Galois group of Bessel's equation is SL_2 if $\alpha - \frac{1}{2} \notin \mathbb{Z}$ and the multiplicative group otherwise (Appendix of [Kol68]). The significance of the condition $\alpha - \frac{1}{2} \notin \mathbb{Z}$ is also explained in Example 3.35. It follows that $R^{\mathrm{gen}} = \mathcal{R} \otimes_{\mathcal{B}[x]_f} K(x)/K(x)$ is Picard-Vessiot. Moreover, R^c is Picard-Vessiot if and only if $c \in k \smallsetminus \{\frac{1}{2} + m \mid m \in \mathbb{Z}\}$.

The following three lemmas will be useful later on.

Lemma 4.19. *Let $h \in \mathcal{R}$ be nonzero. Then there exists a nonempty Zariski open subset $\mathcal{U}$ of $\mathcal{X}(k)$ such that $h^c \in R^c$ is nonzero for every $c \in \mathcal{U}$.*

Proof. Applying [Bou72, Cor. 3, Chapter V, §3.1] to the inclusion $\mathcal{B}[x]_f \subseteq \mathcal{R}$, we find a nonzero element $h' \in \mathcal{B}[x]_f$ such that every morphism ψ (of rings) from $\mathcal{B}[x]_f$ into an algebraically closed field with $\psi(h') \neq 0$, extends to a morphism ψ on $\mathcal{R}$ with $\psi(h) \neq 0$. Without loss of generality we may assume that $h' \in \mathcal{B}[x]$. Let $a \in \mathcal{B}$ be the leading coefficient of h' and let $\mathcal{U}$ be the Zariski open subset of $\mathcal{X}(k)$ defined by a.

For $c \in \mathcal{U}$ let ψ be defined by $\psi : \mathcal{B}[x]_f \xrightarrow{c} k(x) \to \overline{k(x)}$. Then $\psi(h') \neq 0$ and ψ extends to $\mathcal{R}$ with $\psi(h) \neq 0$. We can thus define a morphism $\psi' : R^c = \mathcal{R} \otimes_{\mathcal{B}[x]_f} k(x) \to \overline{k(x)}$, $r \otimes s \mapsto \psi(r)s$. Then $\psi'(h^c) = \psi(h) \neq 0$. Thus $h^c \neq 0$. $\square$

Recall (Definition 3.4) that the fundamental matrix $\mathcal{Y} \in \mathrm{GL}_n(\mathcal{R})$ defines a morphism $\mathcal{G} \to \mathrm{GL}_{n,\mathcal{B}}$ of group schemes over $\mathcal{B}$.

Lemma 4.20. *There exists a nonzero element $b \in \mathcal{B}$ such that the base change of $\mathcal{G} \to \mathrm{GL}_{n,\mathcal{B}}$ via $\mathcal{B} \to \mathcal{B}_b$ is a closed embedding.*

Proof. Set $\mathcal{R}' = \mathcal{R} \otimes_{\mathcal{B}[x]_f} k(\mathcal{B})(x)$. As in the proof of Lemma 4.14 we see that $\mathcal{R}'/k(\mathcal{B})(x)$ is a differential $\mathcal{G}_{k(\mathcal{B})}$-torsor for $\delta(y) = \mathcal{A}y$ with fundamental matrix $\mathcal{Y} \otimes 1 \in \mathrm{GL}_n(\mathcal{R}')$. From this we deduce that the morphism $\mathcal{G}_{k(\mathcal{B})} \to \mathrm{GL}_{n,k(\mathcal{B})}$ determined by $\mathcal{Y} \otimes 1$ is a closed embedding as follows: Assume $\mathcal{T}$ is a $k(\mathcal{B})$-algebra and $g \in \mathcal{G}_{k(\mathcal{B})}(\mathcal{T}) = \mathrm{Hom}_{k(\mathcal{B})}(k(\mathcal{B})[\mathcal{G}], \mathcal{T})$ is in the kernel of $\mathcal{G}_{k(\mathcal{B})}(\mathcal{T}) \to \mathrm{GL}_n(\mathcal{T})$, i.e., g acts trivially on $\mathcal{R}' \otimes_{k(\mathcal{B})} \mathcal{T}$. Let $\rho' : \mathcal{R}' \to$

66

$\mathcal{R}' \otimes_{k(\mathcal{B})} k(\mathcal{B})[\mathcal{G}]$ denote the coaction and $e \in \operatorname{Hom}(k(\mathcal{B})[\mathcal{G}], \mathcal{T}) = \mathcal{G}(\mathcal{T})$ the identity element. As g acts trivially, the maps

$$\mathcal{R}' \xrightarrow{\rho'} \mathcal{R}' \otimes_{k(\mathcal{B})} k(\mathcal{B})[\mathcal{G}] \xrightarrow{\mathcal{R}' \otimes g} \mathcal{R}' \otimes_{k(\mathcal{B})} \mathcal{T}$$

and

$$\mathcal{R}' \xrightarrow{\rho'} \mathcal{R}' \otimes_{k(\mathcal{B})} k(\mathcal{B})[\mathcal{G}] \xrightarrow{\mathcal{R}' \otimes e} \mathcal{R}' \otimes_{k(\mathcal{B})} \mathcal{T}$$

agree (with $a \mapsto a \otimes 1$). As the $\mathcal{R}'$-linear extension of ρ' is an isomorphism, it follows that $\mathcal{R}' \otimes g = \mathcal{R}' \otimes e$ and therefore $g = e$. This shows that $\mathcal{G}_{k(\mathcal{B})}(\mathcal{T}) \to \operatorname{GL}_n(\mathcal{T})$ is injective for every $k(\mathcal{B})$-algebra $\mathcal{T}$. Therefore $\mathcal{G}_{k(\mathcal{B})} \to \operatorname{GL}_{n,k(\mathcal{B})}$ is a closed embedding ([Wat79, Section 15.3]).

The morphism $\mathcal{G} \to \operatorname{GL}_{n,\mathcal{B}}$ determined by $\mathcal{Y}$, after base change via $\mathcal{B} \to k(\mathcal{B})$, yields the morphism $\mathcal{G}_{k(\mathcal{B})} \to \operatorname{GL}_{n,k(\mathcal{B})}$ determined by $\mathcal{Y} \otimes 1$ (and, as we have just seen, the latter is a closed embedding). So the map $\psi \colon \mathcal{B}[X, \frac{1}{\det(X)}] \to \mathcal{B}[\mathcal{G}]$, dual to the morphism $\mathcal{G} \to \operatorname{GL}_{n,\mathcal{B}}$, becomes surjective after the base change $\mathcal{B} \to k(\mathcal{B})$. In other words, the map $S^{-1}\psi \colon S^{-1}\mathcal{B}[X, \frac{1}{\det(X)}] \to S^{-1}\mathcal{B}[\mathcal{G}]$ is surjective, where S is the multiplicatively closed subset of all nonzero elements of $\mathcal{B}$.

Let $a_1, \ldots, a_m \in \mathcal{B}[\mathcal{G}]$ be generators of $\mathcal{B}[\mathcal{G}]$ as a $\mathcal{B}$-algebra and let $\frac{f_1}{s_1}, \ldots, \frac{f_m}{s_m} \in S^{-1}\mathcal{B}[X, \frac{1}{\det(X)}]$ be such that $(S^{-1}\psi)(\frac{f_i}{s_i}) = \frac{a_i}{1}$ for $i = 1, \ldots, m$. Then there exist $s'_1, \ldots, s'_m \in S$ such that $s'_i(\psi(f_i) - s_i a_i) = 0$ for $i = 1, \ldots, m$. Thus $b = s_1 \ldots s_m s'_1 \ldots s'_m$ has the desired property. $\qquad\square$

Lemma 4.21. *Let $\mathcal{B}[x]'_f$ denote the integral closure of $\mathcal{B}[x]_f$ in $\mathcal{R}$ and for $c \in \mathcal{X}(k)$ let $k(x)'$ denote the integral closure of $k(x)$ in R^c. Then there exists a nonempty Zariski open subset $\mathcal{U}$ of $\mathcal{X}(k)$ such that $\mathcal{B}[x]'_f \otimes_{\mathcal{B}[x]_f} k(x) \to k(x)' \subseteq R^c = \mathcal{R} \otimes_{\mathcal{B}[x]_f} k(x)$ is an isomorphism for every $c \in \mathcal{U}$.*

Proof. Let m denote the geometric number of irreducible components of $R^{\mathrm{gen}}/K(x)$. As $\overline{k(\mathcal{B})(x)} = \overline{K(x)}$, it is clear that the geometric number of irreducible components of $\mathcal{R} \otimes_{\mathcal{B}[x]_f} k(\mathcal{B})(x)/k(\mathcal{B})(x)$ is also m.

We claim that the (vector space) dimension $\dim_{k(\mathcal{B})(x)} \mathcal{B}[x]'_f \otimes_{\mathcal{B}[x]_f} k(\mathcal{B})(x)$ equals m. The inclusion $k(\mathcal{B})(x) = \mathcal{B}[x]_f \otimes_{\mathcal{B}[x]_f} k(\mathcal{B})(x) \subseteq \mathcal{R} \otimes_{\mathcal{B}[x]_f} k(\mathcal{B})(x)$ can be identified with the localization of the inclusion $\mathcal{B}[x]_f \subseteq \mathcal{R}$ at the multiplicatively closed subset of all nonzero elements of $\mathcal{B}[x]_f$. As integral closure commutes with localization ([Sta24, Tag 0307]), the integral closure $k(\mathcal{B})(x)'$ of $k(\mathcal{B})(x)$ in $\mathcal{R} \otimes_{\mathcal{B}[x]_f} k(\mathcal{B})(x)$ is $k(\mathcal{B})(x)' = \mathcal{B}[x]'_f \otimes_{\mathcal{B}[x]_f} k(\mathcal{B})(x)$. As integral closure commutes with separable algebraic base change ([Sta24, Tag 0CBF]), it follows that the integral closure $K(x)'$ of $K(x)$ in

$$(\mathcal{R} \otimes_{\mathcal{B}[x]_f} k(\mathcal{B})(x)) \otimes_{k(\mathcal{B})(x)} K(x) = \mathcal{R} \otimes_{\mathcal{B}[x]_f} K(x) = R^{\mathrm{gen}}$$

is $K(x)' = (\mathcal{B}[x]'_f \otimes_{\mathcal{B}[x]_f} k(\mathcal{B})(x)) \otimes_{k(\mathcal{B})(x)} K(x)$. As $[K(x)' : K(x)] = m$ by Corollary 3.18, it follows that $\dim_{k(\mathcal{B})(x)} \mathcal{B}[x]'_f \otimes_{\mathcal{B}[x]_f} k(\mathcal{B})(x) = m$ as claimed.

It is known that $\mathcal{B}[x]'_f$ is a finitely generated $\mathcal{B}[x]_f$-module ([Eis04, Cor. 13.13]). Thus, there exists a nonempty Zariski open subset $\mathcal{V}_1$ of $\operatorname{Spec}(\mathcal{B}[x]_f)$ such that $\dim_{k(\mathfrak{p})} \mathcal{B}[x]'_f \otimes_{\mathcal{B}[x]_f} k(\mathfrak{p})$ is constant on $\mathcal{V}_1$ (e.g., using [Eis04, Theorem 14.4]). As $\dim_{k(\mathcal{B})(x)} \mathcal{B}[x]'_f \otimes_{\mathcal{B}[x]_f} k(\mathcal{B})(x) = m$, we must have $\dim_{k(\mathfrak{p})} \mathcal{B}[x]'_f \otimes_{\mathcal{B}[x]_f} k(\mathfrak{p}) = m$ for all $\mathfrak{p} \in \mathcal{V}_1$.

For a morphism of schemes of finite type the number of geometrically irreducible components of the fibres is constant on a nonempty Zariski open subset ([Sta24, Tag

055A]). Applying this to the dual of the inclusion $\mathcal{B}[x]_f \subseteq \mathcal{R}$ shows that there exists a non-empty Zariski open subset $\mathcal{V}_2$ of $\mathrm{Spec}(\mathcal{B}[x]_f)$ such that the number of geometrically irreducible components of $\mathcal{R} \otimes_{\mathcal{B}[x]_f} k(\mathfrak{p})$ is constant on $\mathcal{V}_2$. As the number of geometrically irreducible components of $\mathcal{R} \otimes_{\mathcal{B}[x]_f} k(\mathcal{B})(x)$ is m, we see that the number of geometrically irreducible components of $\mathcal{R} \otimes_{\mathcal{B}[x]_f} k(\mathfrak{p})$ is m for all $\mathfrak{p}$ in $\mathcal{V}_2$.

The inclusion $\mathcal{B} \subseteq K$, being a composition of a localization with a field extension, makes K a flat $\mathcal{B}$-module. Thus the map $\mathcal{B}[x]'_f \otimes_{\mathcal{B}} K \to \mathcal{R} \otimes_{\mathcal{B}} K$ is injective. We already noted in the proof of Lemma 4.16 that $\mathcal{R} \otimes_{\mathcal{B}} K$ is an integral domain and so $\mathcal{B}[x]'_f \otimes_{\mathcal{B}} K$ is an integral domain. As in loc. cit. it follows that there exists a nonempty Zariski open subset $\mathcal{U}_1$ of $\mathcal{X}(k)$ such that $\mathcal{B}[x]'_f \otimes_{\mathcal{B}[x]_f} k(x)$ is an integral domain for all $c \in \mathcal{U}_1$.

Let $h \in \mathcal{B}[x]$ be a nonzero polynomial such that $D(h) \subseteq \mathcal{V}_1 \cap \mathcal{V}_2$ and let $\mathcal{U}$ be the Zariski open subset of $\mathcal{U}_1$ where the leading coefficient of h does not vanish. We will show that $\mathcal{B}[x]'_f \otimes_{\mathcal{B}[x]_f} k(x) \to k(x)'$ is an isomorphism for every $c \in \mathcal{U}$. Let $c \in \mathcal{U}$ and let $\mathfrak{p}$ be the kernel of $c \colon \mathcal{B}[x]_f \to k(x)$. Then $\mathcal{B}[x]'_f \otimes_{\mathcal{B}[x]_f} k(\mathfrak{p}) = \mathcal{B}[x]'_f \otimes_{\mathcal{B}[x]_f} k(x)$ and $\mathcal{R} \otimes_{\mathcal{B}[x]_f} k(\mathfrak{p}) = \mathcal{R} \otimes_{\mathcal{B}[x]_f} k(x) = R^c$. As c does not vanish on the leading coefficient of h we have $\mathfrak{p} \in \mathcal{V}_1 \cap \mathcal{V}_2$. So $\dim_{k(x)} \mathcal{B}[x]'_f \otimes_{\mathcal{B}[x]_f} k(x) = m$ and the geometric number of connected components of R^c is m. It thus follows from Corollary 3.18 that $[k(x)' : k(x)] = m$. Therefore, $\mathcal{B}[x]'_f \otimes_{\mathcal{B}[x]_f} k(x)$ and $k(x)'$ have the same degree m over $k(x)$. It thus suffices to show that $\mathcal{B}[x]'_f \otimes_{\mathcal{B}[x]_f} k(x) \to k(x)'$ is injective. But as $c \in \mathcal{U}_1$, the ring $\mathcal{B}[x]'_f \otimes_{\mathcal{B}[x]_f} k(x)$ is an integral domain and therefore a field, since it is integral over $k(x)$. $\qquad\square$

The following remark, which is important from a technical perspective and will be used repeatedly in what follows, specializes Remark 4.1 to the context of Notation 4.12.

Remark 4.22. *Assume that in the setup of Notation 4.12 we would like to show that there exists*

- *an ad-open,*

- *a Jac-open or*

- *an ad×Jac-open*

subset $\mathcal{U}$ of $\mathcal{X}(k)$ such that

- *the differential $k(x)$-algebra R^c has a certain property for every $c \in \mathcal{U}$ or*

- *that for given $f_1, \ldots, f_m \in \mathcal{R}$, the elements $f_1^c, \ldots, f_m^c \in R^c$ have a certain property,*

then we can, without loss of generality, replace $\mathcal{B}$ with an integral domain $\mathcal{B}'$ such that $\mathcal{B} \subseteq \mathcal{B}'$ and $\mathcal{B}'$ is finitely generated and algebraic over $\mathcal{B}$.

Proof. Note that $k(\mathcal{B}) \subseteq k(\mathcal{B}') \subseteq \overline{k(\mathcal{B})} = K$. Set

$$\mathcal{R}' = \mathcal{R} \otimes_{\mathcal{B}} \mathcal{B}' = \mathcal{R} \otimes_{\mathcal{B}[x]_f} \mathcal{B}'[x]_f \subseteq \mathcal{R} \otimes_{\mathcal{B}[x]_f} K(x) = R^{\mathrm{gen}}.$$

Then $\mathcal{R}'$ is not the zero ring and so $\mathcal{R}'$ is a differential $\mathcal{G}' = \mathcal{G}_{\mathcal{B}'}$-torsor over $\mathcal{B}[x]_f \otimes_{\mathcal{B}} \mathcal{B}' = \mathcal{B}'[x]_f$ by Lemma 3.7. We next verify that $\mathcal{R}'/\mathcal{B}'[x]_f$ has all the properties listed in Notation 4.12. The matrix $\mathcal{Y}' = \mathcal{Y} \otimes 1 \in \mathrm{GL}_n(\mathcal{R}')$ is such that $\delta(\mathcal{Y}') = \mathcal{A}\mathcal{Y}'$ and $\mathcal{R}' = \mathcal{B}'[x]_f[\mathcal{Y}', \frac{1}{\det(\mathcal{Y}')}]$. Since $\mathcal{G}$ acts on $\mathcal{Y}$ through matrix multiplication, also $\mathcal{G}'$ acts on $\mathcal{Y}'$ through matrix multiplication. Thus $\mathcal{R}'/\mathcal{B}'[x]_f$ is a differential $\mathcal{G}'$-torsor for $\delta(y) = \mathcal{A}y$

with fundamental matrix $\mathcal{Y}'$. As $\mathcal{R}$ is a flat over $\mathcal{B}[x]_f$, we see that $\mathcal{R}' = \mathcal{R} \otimes_{\mathcal{B}[x]_f} \mathcal{B}'[x]_f$ is flat over $\mathcal{B}'[x]_f$. Moreover,

$$R'^{\text{gen}} = \mathcal{R}' \otimes_{\mathcal{B}'[x]_f} K(x) = (\mathcal{R} \otimes_{\mathcal{B}[x]_f} \mathcal{B}'[x]_f) \otimes_{\mathcal{B}'[x]_f} K(x) = \mathcal{R} \otimes_{\mathcal{B}[x]_f} K(x) = R^{\text{gen}}$$

is δ-simple.

Similarly, if $\phi \colon \mathcal{X}'(k) \to \mathcal{X}(k)$ is the morphism induced by the inclusion $\mathcal{B} \subseteq \mathcal{B}'$ and $c' \in \mathcal{X}(k)$ is such that $\phi(c') = c$, then

$$R'^{c'} = \mathcal{R}' \otimes_{\mathcal{B}'[x]_f} k(x) = (\mathcal{R} \otimes_{\mathcal{B}[x]_f} \mathcal{B}'[x]_f) \otimes_{\mathcal{B}'[x]_f} k(x) = \mathcal{R} \otimes_{\mathcal{B}[x]_f} k(x) = R^c.$$

Furthermore, for $i = 1, \ldots, m$, the image $f_i^{c'}$ of f_i in $R'^{c'}$ agrees with the image f_i^c of f_i in R^c.

Thus, if there exists a subset $\mathcal{U}'$ of $\mathcal{X}'(k)$ of one of the three kinds listed in the remark such that one of the two properties of the remark is true for all $c' \in \mathcal{U}'$, then Lemma 2.7 yields a subset $\mathcal{U}$ of $\mathcal{X}(k)$ of the corresponding kind such that $\mathcal{U} \subseteq \phi(\mathcal{U}')$ and the corresponding property holds for all $c \in \mathcal{U}$. $\qquad\square$

4.5 Algebraic relations under specialization

Recall that we assume Notation 4.12 for the remainder of Section 4. The main result of this section (Theorem 4.24) is that a basis of the vector space of algebraic relations of degree at most d among the entries of a fundamental solution matrix for $\delta(y) = \mathcal{A}y$ specializes to a basis of the vector space of algebraic relations of degree at most d among the entries of a fundamental solution matrix for $\delta(y) = A^c y$ for all c in an ad-open subset of the parameter space. This is in spirit similar to Theorem B from the introduction. However, the present result is weaker because we have to fix the degree of the algebraic relations.

By considering the vector of all monomials of degree at most d in the entries of a fundamental solution matrix, the study of the algebraic relations of degree at most d among the entries of a fundamental solution matrix can be reduced to the study of the linear relations satisfied by the entries of one solution vector. We therefore, first study the behavior of linear relations under specialization. Combining the main result of Section 3.6 with the main result of Section 4.1 we obtain:

Proposition 4.23. *Let $v \in \mathcal{R}^\ell$ be such that $v^{\text{gen}} \in (R^{\text{gen}})^\ell$ is a solution of $\delta(y) = \mathcal{A}'y$, with $\mathcal{A}' \in K(x)^{\ell \times \ell}$. Then there exists a positive integer N and an ad-open subset $\mathcal{U}$ of $\mathcal{X}(k)$ such that for every $c \in \mathcal{U}$ the following holds: If $\mathfrak{m}_c$ is a maximal δ-ideal of R^c and $\overline{v^c} \in (R^c/\mathfrak{m}_c)^\ell$ is the image of v^c in $R^c/\mathfrak{m}_c$, then the $k(x)$-vector space $\mathrm{LinRel}(\overline{v^c}, k(x))$ has a basis consisting of elements of the form $a_1 y_1 + \ldots + a_\ell y_\ell$, with $a_1, \ldots, a_\ell \in k(x)$ and $\deg(a_i) \le N$ for $i = 1, \ldots, \ell$.*

Proof. For $i = 1, \ldots, \ell$, let $\mathcal{L}_i \in K(x)[\delta]$ be a monic differential operator, equivalent to $\delta(y) = (\bigwedge^i \mathcal{A}')y$ and let $T_i \in \mathrm{GL}_{\binom{\ell}{i}}(K(x))$ be a corresponding transformation matrix. (See Section 3.6.) Enlarging $\mathcal{B}$ if necessary (Remark 4.22), we can assume that $\mathcal{A}'$, T_i and $\mathcal{L}_i$ $(1 \le i \le \ell)$ have coefficients in $\mathcal{B}[x]_{ff_1}$, where $f_1 \in \mathcal{B}[x]$ is a monic polynomial. So, for a nonempty Zariski open subset $\mathcal{U}'$ of $\mathcal{X}(k)$, the matrix T_i^c lies in $\mathrm{GL}_{\binom{\ell}{i}}(k(x))$ and is a transformation matrix from $\delta(y) = (\bigwedge^i \mathcal{A}')^c y = (\bigwedge^i \mathcal{A}'^c)y$ to $\mathcal{L}_i^c y = 0$. Note that v^c is a solution of $\delta(y) = \mathcal{A}'^c y$ for every $c \in \mathcal{X}(k)$.

69

By Proposition 4.3, for each $i = 1, \ldots, \ell$, there exists an ad-open subset $\mathcal{U}_i$ of $\mathcal{X}(k)$ such that $N(\mathcal{L}_i)$ is an exponential bound for $\mathcal{L}_i^c y = 0$ for any $c \in \mathcal{U}_i$. Note that $\dim_{k(x)} \mathrm{LinRel}(\overline{v^c}, k(x))$ lies between 1 and ℓ for any $c \in \mathcal{X}(k)$. It thus follows from Lemma 3.36 that

$$N = \max_{1 \leq i \leq \ell} \left\{ 2\binom{\ell}{i} \deg(T_i) + \binom{\ell}{i}\left(\binom{\ell}{i} - 1\right) N(\mathcal{L}_i) \right\}$$

and $\mathcal{U}$ any ad-open subset of $\mathcal{U}' \cap \mathcal{U}_1 \cap \ldots \cap \mathcal{U}_\ell$ have the required property. $\qquad \square$

Let F be a differential field, $A \in F^{n \times n}$ and R/F a Picard-Vessiot ring for $\delta(y) = Ay$ with fundamental matrix $Y \in \mathrm{GL}_n(R)$. For a fixed positive integer d, we set

$$\mathrm{AlgRel}(Y, d, F) = \{ p \in F[X] \mid p(Y) = 0, \ \deg(p) \leq d \}.$$

Then $\mathrm{AlgRel}(Y, d, F)$ is a finite dimensional F-vector space; the vector space of algebraic relations of degree at most d among the entries of Y.

The following theorem shows that a basis of the vector space of algebraic relations of degree at most d among the entries of a fundamental solution matrix is preserved on an ad-open subset of the parameter space.

Theorem 4.24. *For any $c \in \mathcal{X}(k)$, let $\mathfrak{m}_c$ be a maximal δ-ideal of R^c and let $\overline{Y^c} \in \mathrm{GL}_n(R^c/\mathfrak{m}_c)$ denote the image of Y^c in $R^c/\mathfrak{m}_c$. Let $p_1, \ldots, p_m \in \mathcal{B}[x][X]$ be a $K(x)$-basis of $\mathrm{AlgRel}(Y^{\mathrm{gen}}, d, K(x))$. Then there exists an ad-open subset $\mathcal{U}$ of $\mathcal{X}(k)$ such that $p_1^c, \ldots, p_m^c$ is a $k(x)$-basis of $\mathrm{AlgRel}(\overline{Y^c}, d, k(x))$ for any $c \in \mathcal{U}$.*

Proof. The main step of the proof is to show that there exists an ad-open subset $\mathcal{U}_1$ of $\mathcal{X}(k)$ such that

$$\dim_{k(x)} \mathrm{AlgRel}(\overline{Y^c}, d, k(x)) \leq \dim_{K(x)} \mathrm{AlgRel}(Y^{\mathrm{gen}}, d, K(x)) \tag{37}$$

for every $c \in \mathcal{U}_1$.

Let $\mathbf{m}_1, \ldots, \mathbf{m}_r$ denote all monomials in X of degree at most d (so $r = \binom{n^2+d}{d}$) and let ℓ be the dimension of the $K(x)$-vector space generated by $\mathbf{m}_1(Y^{\mathrm{gen}}), \ldots, \mathbf{m}_r(Y^{\mathrm{gen}})$ (inside R^{gen}). We may assume, without loss of generality, that $\mathbf{m}_1(Y^{\mathrm{gen}}), \ldots, \mathbf{m}_\ell(Y^{\mathrm{gen}})$ are $K(x)$-linearly independent. We see that $m = \dim_{K(x)} \mathrm{AlgRel}(Y^{\mathrm{gen}}, d, K(x)) = r - \ell$.

As $\delta(Y^{\mathrm{gen}}) = \mathcal{A}Y^{\mathrm{gen}}$, the vector $(\mathbf{m}_1(Y^{\mathrm{gen}}), \ldots, \mathbf{m}_r(Y^{\mathrm{gen}}))^t \in (R^{\mathrm{gen}})^r$ is a solution of $\delta(y) = \mathcal{A}_1 y$ for some $\mathcal{A}_1 \in K(x)^{r \times r}$. Since $\mathbf{m}_i(Y^{\mathrm{gen}})$ ($\ell + 1 \leq i \leq r$) can be expressed as a $K(x)$-linear combination of $\mathbf{m}_1(Y^{\mathrm{gen}}), \ldots, \mathbf{m}_\ell(Y^{\mathrm{gen}})$, it follows that the vector $(\mathbf{m}_1(Y^{\mathrm{gen}}), \ldots, \mathbf{m}_\ell(Y^{\mathrm{gen}}))^t$ is a solution of $\delta(y) = \mathcal{A}'y$ for some $\mathcal{A}' \in K(x)^{\ell \times \ell}$. Set $v = (\mathbf{m}_1(\mathcal{Y}), \ldots, \mathbf{m}_\ell(\mathcal{Y}))^t \in \mathcal{R}^\ell$.

By Proposition 4.23, there exists a positive integer N and an ad-open subset $\mathcal{U}'$ of $\mathcal{X}(k)$ such that for every $c \in \mathcal{U}'$ the following holds: If $\widetilde{\mathfrak{m}_c}$ is a maximal δ-ideal of R^c and $\widetilde{v^c} \in (R^c/\widetilde{\mathfrak{m}_c})^\ell$ is the image of v^c in $R^c/\widetilde{\mathfrak{m}_c}$, then $\mathrm{LinRel}(\widetilde{v^c}, k(x))$ has a $k(x)$-basis of the form $a_1 y_1 + \ldots + a_\ell y_\ell$ with $a_i \in k(x)$ and $\deg(a_i) \leq N$ for $i = 1, \ldots, \ell$.

Recall that the *wronskian* $\mathrm{wr}(h_1, \ldots, h_s)$ of elements $h_1, \ldots, h_s$ of some differential ring R, is defined as the determinant of the wronskian matrix

$$\begin{pmatrix} h_1 & \ldots & h_s \\ \delta(h_1) & \ldots & \delta(h_s) \\ \vdots & & \vdots \\ \delta^{s-1}(h_1) & \ldots & \delta^{s-1}(h_s) \end{pmatrix}.$$

The crucial property of the wronskian is that, if R is a field, then $h_1, \ldots, h_s$ are R^δ-linearly independent if and only if $\mathrm{wr}(h_1, \ldots, h_s)$ is nonzero ([vdPS03, Lemma 1.12]).

Because $\mathbf{m}_1(Y^{\mathrm{gen}}), \ldots, \mathbf{m}_\ell(Y^{\mathrm{gen}}) \in R^{\mathrm{gen}}$ are $K(x)$-linearly independent, the elements $x^j \mathbf{m}_i(Y^{\mathrm{gen}})$ $(0 \le j \le \ell N, \ 1 \le i \le \ell)$ of R^{gen} are K-linearly independent. Thus their wronskian is nonzero. Let $w \in \mathcal{R}$ be the wronskian of $x^j \mathbf{m}_i(\mathcal{Y})$ $(0 \le j \le \ell N, \ 1 \le i \le \ell)$. By Lemma 4.19, there exists a nonempty Zariski open subset $\mathcal{U}''$ of $\mathcal{X}(k)$ such that $w^c \in R^c$ is nonzero for every $c \in \mathcal{U}'$. Therefore, by Lemma 3.8, there exists, for every $c \in \mathcal{U}''$, a maximal δ-ideal $\widetilde{\mathfrak{m}_c}$ of R^c such that $w^c \notin \widetilde{\mathfrak{m}_c}$. Let $\widetilde{Y^c} \in \mathrm{GL}_n(R^c/\widetilde{\mathfrak{m}_c})$ denote the image of Y^c in $R^c/\widetilde{\mathfrak{m}_c}$. As the image of w in $R^c/\widetilde{\mathfrak{m}_c}$ is nonzero for every $c \in \mathcal{U}''$, the family $x^j \mathbf{m}_i(\widetilde{Y^c})$ $(0 \le j \le \ell N, \ 1 \le i \le \ell)$ is k-linearly independent.

We claim that $\mathbf{m}_1(\widetilde{Y^c}), \ldots, \mathbf{m}_\ell(\widetilde{Y^c})$ are $k(x)$-linearly independent for every $c \in \mathcal{U}' \cap \mathcal{U}''$. Suppose this is not the case. Then $\mathrm{LinRel}(\widetilde{v^c}, k(x))$ is nonzero for some $c \in \mathcal{U}' \cap \mathcal{U}''$. By the choice of N and $\mathcal{U}'$ above, there exist $a_1, \ldots, a_\ell \in k(x)$ with $\deg(a_i) \le N$ and $a_1 \mathbf{m}_1(\widetilde{Y^c}) + \ldots + a_\ell \mathbf{m}_\ell(\widetilde{Y^c}) = 0$. Clearing denominators, we find that the family $x^j \mathbf{m}_i(\widetilde{Y^c})$ $(0 \le j \le \ell N, \ 1 \le i \le \ell)$ is k-linearly dependent; a contradiction.

Thus $\mathbf{m}_1(\widetilde{Y^c}), \ldots, \mathbf{m}_\ell(\widetilde{Y^c}) \in R^c/\widetilde{\mathfrak{m}_c}$ are $k(x)$-linearly independent. This implies that

$$\dim_{k(x)} \mathrm{AlgRel}(\widetilde{Y^c}, d, k(x)) \le r - \ell = \dim_{K(x)} \mathrm{AlgRel}(Y^{\mathrm{gen}}, d, K(x)).$$

Since $\dim_{k(x)} \mathrm{AlgRel}(\overline{Y^c}, d, k(x))$ does not depend on the choice of the maximal δ-ideal $\mathfrak{m}_c$ of R^c, we obtain (37) with $\mathcal{U}_1$ an ad-open subset of $\mathcal{U}' \cap \mathcal{U}''$.

As $p_i(Y^{\mathrm{gen}}) = 0$, also $p_i^c(Y^c) = (p_i(\mathcal{Y}))^c = 0$ for $i = 1, \ldots, m$ and $c \in \mathcal{X}(k)$. So $p_1^c, \ldots, p_m^c \in \mathrm{AlgRel}(\overline{Y^c}, d, k(x))$ for any $c \in \mathcal{X}(k)$.

The $K(x)$-linear independence of $p_1, \ldots, p_m \in \mathcal{B}[x][X]$ can be expressed through the non-vanishing of determinants. Thus, there exists a nonempty Zariski open $\mathcal{U}_2$ of $\mathcal{X}(k)$ such that $p_1^c, \ldots, p_m^c \in k(x)[X]$ are $k(x)$-linearly independent for any $c \in \mathcal{U}_2$. Combining this with (37), we see that, for $c \in \mathcal{U}_1 \cap \mathcal{U}_2$, equality holds in (37) and that $p_1^c, \ldots, p_m^c$ is a $k(x)$-basis of $\mathrm{AlgRel}(\overline{Y^c}, d, k(x))$. We can thus choose $\mathcal{U}$ as any ad-open subset of $\mathcal{U}_1 \cap \mathcal{U}_2$. $\qquad\square$

4.6 Picard-Vessiot rings under specialization

Recall that we assume Notation 4.12 for the remainder of Section 4. In this section we prove our main specialization result, namely, that $R^c/k(x)$ is Picard-Vessiot for all c in an ad$\times$Jac-open subset of $\mathcal{X}(k)$.

Combining the criterion of Lemma 3.15 with Theorem 4.24, we first show that $R^c/k(x)$ is proto-Picard-Vessiot for all c in an ad-open subset of $\mathcal{X}(k)$.

Proposition 4.25. *There exists an ad-open subset $\mathcal{U}$ of $\mathcal{X}(k)$ such that $R^c/k(x)$ is proto-Picard-Vessiot for all $c \in \mathcal{X}(k)$.*

Proof. By Lemma 4.16, there exists a nonempty Zariski open subset $\mathcal{U}_1$ of $\mathcal{X}(k)$ such that R^c is an integral domain for every $c \in \mathcal{U}_1$.

Let $p_1, \ldots, p_m \in K[x][X]$ be a $K(x)$-basis of $\mathrm{AlgRel}(Y^{\mathrm{gen}}, \mathbf{d}(n), K(x))$. Extending $\mathcal{B}$ if necessary (Remark 4.22), we may assume that $p_1, \ldots, p_m \in \mathcal{B}[x][X]$. As $p_i(\mathcal{Y}) = 0$, also $p_i^c(Y^c) = (p_i(\mathcal{Y}))^c = 0$ for $i = 1, \ldots, m$ and all $c \in \mathcal{X}(k)$.

For $c \in \mathcal{X}(k)$ let $\mathfrak{m}_c$ be a maximal δ-ideal of R^c and let $\overline{Y^c} \in \mathrm{GL}_n(R^c/\mathfrak{m}_c)$ denote the image of Y^c in $R^c/\mathfrak{m}_c$. By Theorem 4.24, there exists an ad-open subset $\mathcal{U}_2$ of $\mathcal{X}(k)$ such that $p_1^c, \ldots, p_m^c$ is a $k(x)$-basis of $\mathrm{AlgRel}(\overline{Y^c}, \mathbf{d}(n), k(x))$ for any $c \in \mathcal{U}_2$.

We will show that $R^c/k(x)$ is proto-Picard-Vessiot for any $c \in \mathcal{U}_1 \cap \mathcal{U}_2$. Let $p \in k(x)[X]$ with $\deg(p) \leq \mathbf{d}(n)$ and $p(Y^c) \in \mathfrak{m}_c$. According to Lemma 3.15, it suffices to show that $p(Y^c) = 0$.

As $p(\overline{Y^c}) = 0$, i.e., $p \in \mathrm{AlgRel}(\overline{Y^c}, \mathbf{d}(n), k(x))$, we have $p = \sum_{i=1}^m a_i p_i^c$ for appropriate $a_1, \ldots, a_m \in k(x)$. Therefore, $p(Y^c) = \sum_{i=1}^m a_i p_i^c(Y^c) = 0$. Thus, we can choose $\mathcal{U}$ as any ad-open subset of $\mathcal{U}_1 \cap \mathcal{U}_2$. $\qquad \square$

We next make the step from proto-Picard-Vessiot to Picard-Vessiot. Roughly, this corresponds to the second main step of Hrushovski's algorithm, which is more or less the Compoint-Singer algorithm from [CS99, Section 2.5]. Besides Proposition 4.25, key ingredients for the proof are the characterization of Picard-Vessiot rings among proto-Picard-Vessiot rings from Lemma 3.23 and the preservation of logarithmic independence under specialization from Theorem 4.10. The following theorem is our main specialization result. We assume the setup of Notation 4.12.

Theorem 4.26. *There exists an ad$\times$Jac-open subset $\mathcal{U}$ of $\mathcal{X}(k)$ such that $R^c/k(x)$ is Picard-Vessiot for all $c \in \mathcal{U}$. In particular, the set of all $c \in \mathcal{X}(k)$ such that $R^c/k(x)$ is Picard-Vessiot, is Zariski dense in $\mathcal{X}(k)$.*

Proof. Extending $\mathcal{B}$ if necessary (Remark 4.22), we can assume that the morphism $\mathcal{G} \to \mathrm{GL}_{n,\mathcal{B}}$ defined by $\mathcal{Y}$ is a closed embedding (Lemma 4.20). We can thus consider $\mathcal{G}$ as a closed subgroup of $\mathrm{GL}_{n,\mathcal{B}}$. Note that the equations defining $\mathcal{G}$ as a closed subgroup of $\mathrm{GL}_{n,\mathcal{B}}$, also define G^{gen} as a closed subgroup of $\mathrm{GL}_{n,K}$. Let $\{\chi_1, \ldots, \chi_m\}$ be a basis of $X((G^{\mathrm{gen}})^\circ)$ and let $q_1, \ldots, q_m \in K[X, \frac{1}{\det(X)}]$ be such that the image of q_i in $K[(G^{\mathrm{gen}})^\circ]$ agrees with χ_i for $i = 1, \ldots, m$. Let $K(x)'$ denote the integral closure of $K(x)$ in R^{gen} and let $\vartheta \in \mathrm{Hom}_{K(x)'}(R^{\mathrm{gen}}, \overline{K(x)})$. Note that $K(x)'$ is canonically embedded into $\overline{K(x)}$ by forming $\overline{K(x)}$ inside the algebraic closure of the field of fractions of R^{gen}. As $\vartheta(R^{\mathrm{gen}})$ is a finite field extension of $K(x)$, there exists an $\eta \in \overline{K(x)}$ such that $\vartheta(R^{\mathrm{gen}}) = K(x)[\eta] = K(x, \eta)$. In particular, $B = \vartheta(Y^{\mathrm{gen}})^{-1} \in \mathrm{GL}_n(\overline{K(x)})$ has coefficients in $K(x)[\eta]$. Replacing η with a $K(x)$-multiple of η if necessary, we can assume that the minimal polynomial $p \in K(x)[y]$ of η over $K(x)$ has coefficients in $K[x]$.

Extending $\mathcal{B}$ and replacing f by a multiple of f if necessary (Remark 4.22), we may assume that

- the coefficients of $p, q_1, \ldots, q_m$ are all in $\mathcal{B}$,

- $\delta(\eta) \in \mathcal{B}[x]_f[\eta]$, so that $\mathcal{B}[x]_f[\eta]$ is a differential subring of $K(x, \eta)$ and

- $B, B^{-1} \in \mathcal{B}[x]_f[\eta]^{n \times n}$.

By [Fen21, Prop. 3.5], there exists a nonempty Zariski open subset $\mathcal{U}_1$ of $\mathcal{X}(k)$ such that the images $\chi_1^c, \ldots, \chi_m^c$ of $q_1^c, \ldots, q_m^c$ in $k[(G^c)^\circ]$ are a basis of $X((G^c)^\circ)$ for every $c \in \mathcal{U}_1$.

As $p \in \mathcal{B}[x, y]$ is irreducible in $K(x)[y]$ and monic in y, it follows from Gauss's lemma that p is irreducible in $K[x, y]$. By the Bertini-Noether theorem ([FJ08, Prop. 9.4.3]), there exits a nonempty Zariski open subset $\mathcal{U}_2$ of $\mathcal{U}_1$ such that $p^c(x, y)$ is irreducible in $k[x, y]$, and hence also irreducible in $k(x)[y]$, for any $c \in \mathcal{U}_2$. So, for $c \in \mathcal{U}_2$, the ring $\mathcal{B}[x]_f[\eta] \otimes_{\mathcal{B}[x]_f} k(x) = k(x)[y]/(p^c)$ is a field, in fact, a finite field extension of $k(x)$.

For $c \in \mathcal{X}(k)$, let $k(x)'$ denote the integral closure of $k(x)$ in R^c. Our next goal is to construct, using ϑ, elements $\vartheta^c \in \mathrm{Hom}_{k(x)'}(R^c, \overline{k(x)})$. Recall (Lemma 4.13) that we may

regard $\mathcal{R}$ as a δ-subring of R^{gen}. So the morphism $\vartheta\colon R^{\mathrm{gen}} \to K(x,\eta)$ of $K(x)'$-algebras restricts to a morphism $\vartheta\colon \mathcal{R} \to \mathcal{B}[x]_f[\eta]$ of $\mathcal{B}[x]_f'$-algebras. Thus for $c \in \mathcal{U}_2$ we can base change $\vartheta\colon \mathcal{R} \to \mathcal{B}[x]_f[\eta]$ via $c\colon \mathcal{B}[x]_f \to k(x)$ to a morphism $\theta^c\colon R^c = \mathcal{R} \otimes_{\mathcal{B}[x]_f} k(x) \to \mathcal{B}[x]_f[\eta] \otimes_{\mathcal{B}[x]_f} k(x)$ of $\mathcal{B}[x]_f' \otimes_{\mathcal{B}[x]_f} k(x)$-algebras. By Lemma 4.21, there exists a nonempty Zariski open subset $\mathcal{U}_3$ of $\mathcal{U}_2$ such that the map $\mathcal{B}[x]_f' \otimes_{\mathcal{B}[x]_f} k(x) \to k(x)' \subseteq R^c$ is an isomorphism. So composing θ^c with a $\mathcal{B}[x]_f' \otimes_{\mathcal{B}[x]_f} k(x) = k(x)'$ embedding of $\mathcal{B}[x]_f[\eta] \otimes_{\mathcal{B}[x]_f} k(x)$ into $\overline{k(x)}$, we obtain a morphism $\vartheta^c\colon R^c \to \overline{k(x)}$ of $k(x)'$-algebras. Note that $B^c = \vartheta^c(Y^c)^{-1} \in \mathrm{GL}_n(\overline{k(x)})$ agrees with the image of B under $\mathcal{B}[x]_f[\eta] \to \mathcal{B}[x]_f[\eta] \otimes_{\mathcal{B}[x]_f} k(x) \to \overline{k(x)}$ for all $c \in \mathcal{U}_3$.

For $\ell = 1, \ldots, m$ we set

$$f_\ell = \sum_{i,j=1}^n \frac{\partial q_\ell}{\partial X_{ij}}(I_n)(B\mathcal{A}B^{-1} + \delta(B)B^{-1})_{ij} \in \mathcal{B}[x]_f[\eta] \subseteq K(x,\eta) \subseteq \overline{K(x)}.$$

As $R^{\mathrm{gen}}/K(x)$ is Picard-Vessiot, it follows from Lemma 3.23 and Remark 3.22 that $f_1, \ldots, f_m$ are logarithmically independent over $K(x,\eta)$.

For an element a of $\mathcal{B}[x]_f[\eta]$ and $c \in \mathcal{U}_3$, let us write $a^c = a \otimes 1 \in \mathcal{B}[x]_f[\eta] \otimes_{\mathcal{B}[x]} k(x)$ for the image of a in $\mathcal{B}[x]_f[\eta] \otimes_{\mathcal{B}[x]} k(x) \hookrightarrow \overline{k(x)}$. For $\ell = 1, \ldots, m$, we then have

$$f_\ell^c = \sum_{i,j=1}^n \frac{\partial q_\ell^c}{\partial X_{ij}}(I_n)(B^c A^c (B^c)^{-1} + \delta(B^c)(B^c)^{-1})_{ij} \in \mathcal{B}[x]_f[\eta] \otimes_{\mathcal{B}[x]_f} k(x) \hookrightarrow \overline{k(x)}.$$

By Theorem 4.10, there exists an ad×Jac-open subset $\mathcal{U}'$ of $\mathcal{X}(k)$ contained in $\mathcal{U}_3$ such that $f_1^c, \ldots, f_m^c$ are logarithmically independent over $\mathcal{B}[x]_f[\eta] \otimes_{\mathcal{B}[x]_f} k(x)$ for all $c \in \mathcal{U}'$. Then $\mathcal{U}'$ is of the form $\mathcal{U}' = \mathcal{U}_4 \cap \mathcal{V}$ with $\mathcal{U}_4$ ad-open and $\mathcal{V}$ Jac-open.

By Proposition 4.25, there exists an ad-open subset $\mathcal{U}_5$ of $\mathcal{X}(k)$ such that $R^c/k(x)$ is proto-Picard-Vessiot for any $c \in \mathcal{U}_5$. Let $\mathcal{U}_6$ be an ad-open subset of $\mathcal{U}_4 \cap \mathcal{U}_5$. Then $\mathcal{U} = \mathcal{U}_6 \cap \mathcal{V}$ is ad×Jac-open. Now Lemma 3.23 implies that $R^c/k(x)$ is Picard-Vessiot for any $c \in \mathcal{U}$.

The last statement of the theorem follows from Theorem 2.24. $\qquad\square$

The proof of Theorem 4.26 shows that if the algebraic group G^{gen} over K is such that $(G^{\mathrm{gen}})^t = G^{\mathrm{gen}}$ (e.g., G^{gen} is semisimple or unipotent), then the Jac-open subset is not needed, i.e., the set of good specializations contains an ad-open subset. However, we can do much better than that:

Corollary 4.27. *Assume that in the setup of Notation 4.12 the generic differential Galois group G^{gen} is connected. Then there exists an ad-open subset $\mathcal{U}$ of $\mathcal{X}(k)$ such that $R^c/k(x)$ is Picard-Vessiot for every $c \in \mathcal{U}$.*

Proof. If G^{gen} is connected, then the $\vartheta \in \mathrm{Hom}_{K(x)}(R^{\mathrm{gen}}, \overline{K(x)})$ in the proof of Theorem 4.26 can be chosen such that $B = \vartheta(Y^{\mathrm{gen}})^{-1} \in \mathrm{GL}_n(K(x))$ by Remark 3.24. We can therefore choose $\eta = 1$ and so $f_1, \ldots, f_m \in \mathcal{B}[x]_f \subseteq K(x)$. By Remark 4.11, the Jac-open subset $\mathcal{V}$ is then not needed so that $\mathcal{U}' = \mathcal{U}_5$ is ad-open and therefore also $\mathcal{U}$ is ad-open. $\quad\square$

While Jac-open subsets do not occur when the generic differential Galois is connected, they do indeed occur in the non-connected case. This is illustrated in the following example.

Example 4.28. Let α and β be variables over k and set $\mathcal{B} = k[\alpha, \beta]$. In line with Notation 4.12 we also set $K = \overline{k(\alpha, \beta)}$.

Let $a = \frac{(x-\beta)^2}{x^4+x+\alpha}$, $f = (x^4 + x + \alpha)(x - \beta)$ and consider the differential equation

$$\delta^2(y) - \left(2a + \tfrac{\delta(a)}{2a}\right)\delta(y) + \left(a^2 - a - \tfrac{\delta(a)}{2}\right)y = 0 \tag{38}$$

over $\mathcal{B}[x]_f$. Note that the companion matrix $\mathcal{A} \in \mathcal{B}[x]_f^{2\times 2}$ of (38) is of the form described in Examples 3.6 and 4.17 with $b = a$.

As a is not a square in $k(\alpha, \beta)(x)$, we see that $\mathcal{B}[x]_f[y]/(y^2 - a) = \mathcal{B}[x]_f[\eta]$ is an integral domain and a differential ring. As in the previous examples we set

$$\mathcal{R} = \mathcal{B}[x]_f[\eta][y_1, y_2, y_1^{-1}, y_2^{-1}] = \mathcal{B}[x]_f[X, \tfrac{1}{\det(X)}]/(p_1, p_2) = \mathcal{B}[x]_f[\mathcal{Y}, \tfrac{1}{\det(\mathcal{Y})}],$$

where

$$p_1 = X_{21}X_{22} - (a^2 - a)X_{11}X_{12} \qquad p_2 = X_{21}X_{12} + X_{22}X_{11} - 2aX_{11}X_{12},$$

$\delta(y_1) = (a + \eta)y_1$, $\delta(y_2) = (a + \eta)y_2$ and $\delta(\mathcal{Y}) = \mathcal{A}\mathcal{Y}$.

We know from Example 3.6 that $\mathcal{R}/\mathcal{B}[x]_f$ is a differential $\mathcal{G}$-torsor for $\delta(y) = \mathcal{A}y$ where $\mathcal{G}$ is the group scheme of 2×2 monomial matrices over $\mathcal{B}$. Therefore,

$$R^{\mathrm{gen}} = \mathcal{R} \otimes_{\mathcal{B}[x]_f} K(x) = K(x, \eta)[y_1, y_2, y_1^{-1}, y_2^{-1}] = K(x)[Y^{\mathrm{gen}}, \tfrac{1}{Y^{\mathrm{gen}}}]$$

is a differential $G^{\mathrm{gen}} = \mathcal{G}_K$-torsor. Example 3.25 shows that $R^{\mathrm{gen}}/K(x)$ is Picard-Vessiot if and only if $f_1 = a + \eta$ and $f_2 = a - \eta$ are logarithmically independent over $K(x, \eta)$. From Example 3.27 we know that f_1, f_2 are logarithmically independent over $K(x, \eta)$ if the point $(0, 1)$ is not a torsion point on the elliptic curve (over K) defined by $v^2 = u^3 - 4\alpha u + 1$.

Combining Example 2.4 (i) of [Zan14a] and Proposition 12.1 of [Zan14b] we see that the latter is the case and so $R^{\mathrm{gen}}/K(x)$ is Picard-Vessiot. (Note that in the notation of these references $\infty_+ = (0, 1)$ and ∞_- is the neutral element.)

Set $\mathcal{X} = \mathrm{Spec}(\mathcal{B}) = \mathbb{A}_k^2$. We would like to determine an ad$\times$Jac-open subset $\mathcal{U}$ of $\mathcal{X}(k) = k^2$ such that $R^c = \mathcal{R} \otimes_{\mathcal{B}[x]_f} k(x)$ is Picard-Vessiot for every $c \in \mathcal{U}$. To this end, we follow the same strategy as at the generic point. Example 4.17 shows that R^c is an integral domain provided that $256(\alpha^c)^3 - 27 \neq 0$. For these c's, Example 3.25 shows that R^c is Picard-Vessiot if and only if $f_1^c = a^c + \eta^c$ and $f_2^c = a^c - \eta^c$ are logarithmically independent over $F^c = k(x, \eta^c) = k(x)[y]/(y^2 - a^c)$. With $z^c = \frac{x - \beta^c}{\eta^c}$, we have $F^c = k(x, z^c)$ and $(z^c)^2 = x^4 + x + \alpha^c$.

Set $\mathcal{U} = W_{\mathcal{X}}(\mathbb{G}_a, \Gamma) \cap \mathcal{V}$, where Γ is the subgroup of $(\mathcal{B}, +)$ generated by $(\beta^4 + \beta + \alpha)^2$ and $256\alpha^3 - 27$ and $\mathcal{V}$ is the set of all $c = (\alpha^c, \beta^c) \in \mathcal{X}(k)$ such that $256(\alpha^c)^3 - 27 \neq 0$ and $(0 : 1 : 1)$ is not a torsion point of the elliptic curve $\mathcal{E}^c$ with affine equation: $u^2 = v^3 - 4\alpha^c v + 1$. So $\mathcal{U}$ is an ad$\times$Jac-open subset of $\mathcal{X}(k)$. We will show that $R^c/k(x)$ is Picard-Vessiot for every $c \in \mathcal{U}$.

Let $c \in \mathcal{U}$. Because $c \in W_{\mathcal{X}}(\mathbb{G}_a, \Gamma)$, we have

$$(\beta^c)^4 + \beta^c + \alpha^c \neq 0, \;\; 256(\alpha^c)^3 - 27 \neq 0, \;\; \text{and} \;\; \frac{((\beta^c)^4 + \beta^c + \alpha^c)^2}{256(\alpha^c)^3 - 27} \notin \mathbb{Q}.$$

From Example 3.27 with α, β being replaced by α^c, β^c respectively, we see that $Z_1((f_1^c, f_2^c), \mathcal{P}) = \{(d, -d) \mid d \in \mathbb{Z}\}$, where $\mathcal{P} = \{P_1, P_2, \ldots, P_6\}$ are all poles of $f_1^c dx$ and $f_2^c dx$. In particular, P_1, P_2 are places of the function field $F^c = k(x, z^c)$ with $(z^c)^2 = x^4 + x + \alpha^c$ and P_1

is the place corresponding to the neutral element $(0 : 1 : 0) \in E^c(k)$, while P_2 corresponds to the point $(0 : 1 : 1) \in E^c(k)$. For each $(d, -d) \in Z_1((f_1^c, f_2^c), \mathcal{P})$,

$$\sum_{P \in \mathcal{P}} \left(\sum_{i=1}^{2} d \operatorname{res}_P(f_i^c dx) \right) P = 2d(P_2 - P_1)$$

Furthermore, as $c \in \mathcal{V}$, $2d(P_2 - P_1)$ is not a torsion point of $\mathcal{E}^c(k)$ if $d \neq 0$. Thus $Z_2((f_1^c, f_2^c), \mathcal{P})$ is trivial and therefore f_1^c, f_2^c are logarithmically independent (see Example 3.27 for details). So $R^c/k(x)$ is Picard-Vessiot for every $c \in \mathcal{U}$.

In the following, we also show that there are infinitely many $c = (\alpha^c, \beta^c) \in k^2 = \mathcal{X}(k)$ with $256(\alpha^c)^3 - 27 \neq 0$ such that R^c is not Picard-Vessiot, i.e., f_1^c, f_2^c are logarithmically dependent. By Example 2.4 (i) of [Zan14a], there exist infinitely many $\alpha^c \in k$ with $256(\alpha^c)^3 - 27 \neq 0$ such that $(0, 1)$ is a torsion point on the elliptic curve $\mathcal{E}^c$. For every such $\alpha^c \in k$, let $m_c \geq 2$ denote the order of $(0, 1)$. Now $m_c(0, 1)$ is the neutral element of $\mathcal{E}^c$, if and only if the divisor $m_c(P_2 - P_1)$ is principal. Thus, there exist an $h_c \in F^c$ such that $(h_c) = m_c(P_2 - P_1)$. Note that $\frac{dx}{z^c}$ is a regular differential of F^c. The only poles of $\frac{dh^c}{h_c} = \frac{\delta(h_c)}{h_c} dx$ are P_1 and P_2. Moreover, these poles are simple with residues $-m_c$ and m_c respectively. On the other hand, $\frac{m_c x}{z^c} dx = \frac{m_c x^2}{z^c} d(x^{-1})$ and the P_i-adic expansion of z^c is $z^c = c_i(x^{-1})^{-1} + \ldots$ for $i = 1, 2$ with $c_1 = -1$ and $c_2 = 1$ (Example 3.27). It follows that also the differential $\frac{m_c x}{z^c} dx - \frac{\delta(h_c)}{h_c} dx$ is regular. As F^c/k has genus one, the space of regular differentials is one dimensional. Therefore, there exists an $s \in k$ such that $\frac{m_c x}{z^c} - \frac{\delta(h_c)}{h_c} = \frac{s}{z^c}$. If we set $\beta^c = \frac{s}{m_c} \in k$, then

$$m_c(f_1^c - f_2^c) = m_c \eta^c = \frac{m_c(x - \beta^c)}{z^c} = \frac{\delta(h_c)}{h_c},$$

so that indeed f_1^c, f_2^c are logarithmically dependent for $c = (\alpha^c, \beta^c) \in \mathcal{X}(k)$.

As the above c's are not really given explicitly, let us present at least one explicit $c \in W_{\mathcal{X}}(\mathbb{G}_a, \Gamma)$ such that $R^c/k(x)$ is not Picard-Vessiot. (In this sense the set $\mathcal{V}$ is necessary.)

Set $c = (\alpha^c, \beta^c) = (-\frac{1 + \sqrt{-3}}{4}, -\frac{1 + \sqrt{-3}}{8})$. Then

$$256\alpha^c - 27 = 5, \quad ((\beta^c)^4 + \beta^c + \alpha^c)^2 = \frac{37249(\sqrt{-3} + 1)^2}{262144}.$$

So $c = (\alpha^c, \beta^c) \in W_{\mathcal{X}}(\mathbb{G}_a, \Gamma)$ but f_1^c, f_2^c are logarithmically dependent. In fact, one has that

$$2(f_1^c - f_2^c)dx = 4\frac{(x - \frac{1 + \sqrt{-3}}{8})dx}{\sqrt{x^4 + x - \frac{1 + \sqrt{-3}}{4}}} = \frac{\delta(h)}{h},$$

where $h = p + q\sqrt{x^4 + x - \frac{1 + \sqrt{-3}}{4}}$ with

$$p = (2x^4 - x^2 + x)\sqrt{3} + \sqrt{-1}(2x^4 + 4x^3 + x^2 + x + 1),$$
$$q = (2x^2 - 1)\sqrt{3} + \sqrt{-1}(2x^2 + 4x + 1).$$

5 Applications of the specialization theorem

In this section, we present some applications of our specialization theorem (Theorem 4.26). The main application, which in fact motivated this entire paper, is the proof of Matzat's conjecture. Besides Matzat's conjecture, we also present the proofs for the results announced in the introduction and a very short proof of the solution of the inverse problem.

5.1 Exceptional parameter values

In this section we deduce the results announced in the introduction from Theorem 4.26.

5.1.1 Exceptional parameter values for the algebraic relations among the solutions in a family of linear differential equations

Let $k \subseteq k'$ be an inclusion of algebraically closed fields of characteristic zero and let $R/k'(x)$ be a Picard-Vessiot ring for $\delta(y) = Ay$ with $A \in k'(x)^{n \times n}$. Then R is of the form $R = k'(x)[X, \frac{1}{\det(X)}]/\mathfrak{m}$ for some maximal differential ideal $\mathfrak{m}$ of $k'(x)[X, \frac{1}{\det(X)}]$, where $\delta(X) = AX$. Let $p_1, \ldots, p_m$ be a generating set of the ideal $\mathfrak{m}$. Fix a finitely generated k-subalgebra $\mathcal{B}_0$ of k' and $f_0 \in \mathcal{B}_0[x]$ a monic polynomial such that $A \in \mathcal{B}_0[x]_{f_0}^{n \times n}$ and $p_1, \ldots, p_m \in \mathcal{B}_0[x]_{f_0}[X, \frac{1}{\det(X)}]$. Set $\mathcal{X}_0 = \mathrm{Spec}(\mathcal{B}_0)$ and for $c_0 \in \mathcal{X}_0(k)$ let $\mathfrak{m}^{c_0}$ denote the ideal of $k(x)[X, \frac{1}{\det(X)}]$ generated by $p_1^{c_0}, \ldots, p_m^{c_0}$.

Corollary 5.1. *There exists an $\mathrm{ad} \times \mathrm{Jac}$-open subset $\mathcal{U}_0$ of $\mathcal{X}_0(k)$ such that $\mathfrak{m}^{c_0}$ is a maximal differential ideal of $k(x)[X, \frac{1}{\det(X)}]$ for every $c_0 \in \mathcal{U}_0$, where $k(x)[X, \frac{1}{\det(X)}]$ as a differential ring with respect to the derivation determined by $\delta(X) = A^{c_0} X$.*

Proof. By Lemma 3.11, there exists

- a finitely generated k-subalgebra $\mathcal{B}$ of k' containing $\mathcal{B}_0$ and contained in the algebraic closure of the field of fractions of $\mathcal{B}_0$;

- a monic polynomial $f \in \mathcal{B}[x]$ such that f_0 divides f in $\mathcal{B}[x]$;

- an affine group scheme $\mathcal{G}$ of finite type over $\mathcal{B}$;

- a differential $\mathcal{G}$-torsor $\mathcal{R}/\mathcal{B}[x]_f$ for $\delta(y) = Ay$ such that $\mathcal{R}$ is a flat $\mathcal{B}[x]_f$-module, $\mathcal{R} \otimes_{\mathcal{B}[x]_f} K(x)$ is δ-simple, where $K \subseteq k'$ is the algebraic closure of the field of fractions of $\mathcal{B}$ and $\mathcal{R} \otimes_{\mathcal{B}[x]_f} k'(x) \simeq R$.

Let Y denote the image of X in $R = k'(x)[X, \frac{1}{\det(X)}]/\mathfrak{m}$ and let $\mathcal{Y} \in \mathrm{GL}_n(\mathcal{R})$ be the fundamental matrix corresponding to Y under the isomorphism $\mathcal{R} \otimes_{\mathcal{B}[x]_f} k'(x) \simeq R$. Then

$$\mathfrak{m} = \left\{ p \in k'(x)[X, \tfrac{1}{\det(X)}] \mid p(Y) = 0 \right\}$$

and for

$$\mathcal{I} = \{ p \in \mathcal{B}[x]_f[X, \tfrac{1}{\det(X)}] \mid p(\mathcal{Y}) = 0 \}$$

we have $\mathcal{I} \otimes_{\mathcal{B}[x]_f} k'(x) = \mathfrak{m} = (p_1, \ldots, p_m) \subseteq k'(x)[X, \frac{1}{\det(X)}]$.

Set $\mathcal{X} = \mathrm{Spec}(\mathcal{B})$ and let $\phi \colon \mathcal{X}(k) \to \mathcal{X}_0(k)$ be the map induced by the inclusion $\mathcal{B}_0 \subseteq \mathcal{B}$.

We claim that there exists a nonempty Zariski open subset $\mathcal{U}$ of $\mathcal{X}(k)$ such that $\mathcal{I} \otimes_{\mathcal{B}[x]_f} k(x) = \mathfrak{m}^{\phi(c)} \subseteq k(x)[X, \frac{1}{\det(X)}]$ for all $c \in \mathcal{U}$, where the tensor product $\mathcal{I} \otimes_{\mathcal{B}[x]_f} k(x)$ is formed using $c \colon \mathcal{B}[x]_f \to k(x)$. As $p_1, \ldots, p_m \in \mathcal{I}$, we have $\mathfrak{m}^{\phi(c)} \subseteq \mathcal{I} \otimes_{\mathcal{B}[x]_f} k(x)$ for all $c \in \mathcal{X}(k)$.

Set

$$\mathcal{I}' = \{ p \in k(\mathcal{B})(x)[X, \tfrac{1}{\det(X)}] \mid p(\mathcal{Y}) = 0 \}.$$

As $\mathcal{I}' \otimes_{k(\mathcal{B})(x)} k'(x) = \mathfrak{m} = (p_1, \ldots, p_m) \subseteq k'(x)[X, \frac{1}{\det(X)}]$, we must have $\mathcal{I}' = (p_1, \ldots, p_m) \subseteq k(\mathcal{B})(x)[X, \frac{1}{\det(X)}]$.

Let $q_1, \ldots, q_d \in \mathcal{B}[x]_f[X, \frac{1}{\det(X)}]$ be such that $\mathcal{I} = (q_1, \ldots, q_d)$. As $q_i \in \mathcal{I} \subseteq \mathcal{I}' = (p_1, \ldots, p_m)$, we can find a nonzero $b \in \mathcal{B}$ and a monic $f' \in \mathcal{B}[x]$ such that $bf'q_i \in (p_1, \ldots, p_m) \subseteq \mathcal{B}[x][X, \frac{1}{\det(X)}]$ for $i = 1, \ldots, d$. Let $\mathcal{U}$ be the Zariski open subset of $\mathcal{X}(k)$ where b does not vanish. Then $q_i^c \in (p_1^c, \ldots, p_m^c) \subseteq k(x)[X, \frac{1}{\det(X)}]$ for $i = 1, \ldots, d$ for every $c \in \mathcal{U}$. Therefore

$$\mathcal{I} \otimes_{\mathcal{B}[x]_f} k(x) = (q_1, \ldots, q_d) \otimes_{\mathcal{B}[x]_f} k(x) = (q_1^c, \ldots, q_d^c) \subseteq (p_1^c, \ldots, p_m^c) = \mathfrak{m}^{\phi(c)}$$

and so $\mathcal{I} \otimes_{\mathcal{B}[x]_f} k(x) = \mathfrak{m}^{\phi(c)}$ for all $c \in \mathcal{U}$ as claimed. In particular, since $\mathcal{I}$ is a differential ideal, also $\mathfrak{m}^{\phi(c)}$ is a differential ideal for all $c \in \mathcal{U}$.

Theorem 4.26 applied to the differential torsor $\mathcal{R}/\mathcal{B}[x]_f$ yields an ad$\times$Jac-open subset $\mathcal{V}$ of $\mathcal{X}(k)$ such that $\mathcal{R} \otimes_{\mathcal{B}[x]_f} k(x)$ is δ-simple for every $c \in \mathcal{V}$. For $c \in \mathcal{U} \cap \mathcal{V}$ we then have that

$$\mathcal{R} \otimes_{\mathcal{B}[x]_f} k(x) = (\mathcal{B}[x]_f[X, \tfrac{1}{\det(X)}]/\mathcal{I}) \otimes_{\mathcal{B}[x]_f} k(x) = k(x)[X, \tfrac{1}{\det(X)}]/\mathcal{I} \otimes_{\mathcal{B}[x]_f} k(x) =$$
$$= k(x)[X, \tfrac{1}{\det(X)}]/\mathfrak{m}^{\phi(c)}$$

is δ-simple, i.e., $\mathfrak{m}^{\phi(c)}$ is a maximal δ-ideal. By Lemma 2.7, there exists an ad$\times$Jac-open subset $\mathcal{U}_0$ of $\mathcal{X}_0(k)$ such that $\mathcal{U}_0 \subseteq \phi(\mathcal{U} \cap \mathcal{V})$. Then $\mathfrak{m}^{c_0}$ is a maximal δ-ideal for all $c_0 \in \mathcal{U}_0$. $\qquad\square$

Remark 5.2. *If, in the context of Corollary 5.1, the differential Galois group of $\delta(y) = Ay$ (over $k'(x)$) is connected, then the set $\mathcal{U}_0$ can be chosen to be ad-open.*

Proof. If the differential Galois group G of $\delta(y) = Ay$ is connected, also the differential Galois group G^{gen} of $\mathcal{R}^{\text{gen}} = \mathcal{R} \otimes_{\mathcal{B}[x]_f} K(x)$ is connected because $G = (G^{\text{gen}})_{k'}$ by Lemma 3.2. Thus, by Corollary 4.27, the ad$\times$Jac-open subset $\mathcal{V}$ of $\mathcal{X}(k)$ in the proof of Corollary 5.1 can be chosen to be ad-open. Then by Lemma 2.7 also $\mathcal{U}_0$ can be chosen to be ad-open. $\qquad\square$

5.1.2 Families of not solvable algebraic groups

We next work towards a proof of Corollary B1 from the introduction. A linear differential equation is solvable by Liouvillian functions if and only if the identity component of the differential Galois group is solvable ([vdPS03, Theorem 1.43]). For the proof of Corollary B1 we need to know that the contrapositive of this property spreads out from the generic fibre to an open subset of the parameter space.

Throughout Section 5.1.2 we make the following assumptions:

- k is an algebraically closed field of characteristic zero;

- $\mathcal{B}$ is a finitely generated k-algebra that is an integral domain;

- $K = \overline{k(\mathcal{B})}$ is the algebraic closure of the field of fractions $k(\mathcal{B})$ of $\mathcal{B}$;

- $\mathcal{X} = \operatorname{Spec}(\mathcal{B})$;

- $\mathcal{G}$ is an affine group scheme of finite type over $\mathcal{X}$ such that $\mathcal{G} \to \mathcal{X}$ is dominant, i.e., the dual map $\mathcal{B} \to \mathcal{B}[\mathcal{G}]$ is injective.

- ξ is the generic point of $\mathcal{X}$ and $\mathcal{G}_\xi = \mathcal{G} \times_{\mathcal{X}} \operatorname{Spec}(k(\xi))$ is the generic fibre (an algebraic group over $k(\xi) = k(\mathcal{B})$) whereas $\mathcal{G}_{\bar\xi} = \mathcal{G} \times_{\mathcal{X}} \operatorname{Spec}(K)$ is the geometric generic fibre (an algebraic group over K). Moreover, $\mathcal{G}_c$ is the fibre over $c \in \mathcal{X}$ (an algebraic group over the residue field of c).

The main goal of this subsection is to prove the following:

Proposition 5.3. *If $(\mathcal{G}_{\bar\xi})^\circ$ is not solvable, then there exists a nonempty Zariski open subset $\mathcal{U}$ of $\mathcal{X}(k)$ such that $(\mathcal{G}_c)^\circ$ is not solvable for every $c \in \mathcal{U}$.*

The proof of Proposition 5.3 is given at the end of Section 5.1.2. We will need some properties of the derived subgroup of an algebraic group. For more background see [Mil17, Section 6 d] or [Wat79, Section 10.1]. Let k' be a field of characteristic zero and let G be an algebraic group over k'. The *derived group* $\mathcal{D}(G)$ of G can be defined as the smallest closed normal subgroup of G such that $G/\mathcal{D}(G)$ is abelian. Alternatively, it can also be described as the closed subgroup of G generated by the commutator map $G \times G \to G$, $(g, h) \mapsto ghg^{-1}h^{-1}$ ([Mil17, Prop. 6.18]). More generally, for every $n \geq 1$, consider the map

$$\phi_n \colon G^{2n} \to G, \ (g_1, h_1, \ldots, g_n, h_n) \mapsto g_1 h_1 g_1^{-1} h_1^{-1} \ldots g_n h_n g_n^{-1} h_n^{-1}$$

and its dual $\phi_n^* \colon k'[G] \to \otimes^{2n} k'[G]$. So $\ker(\phi_n^*)$ is the defining ideal of the closure of the image of ϕ_n. One has $\ker(\phi_1^*) \supseteq \ker(\phi_2^*) \supseteq \ldots$ and the defining ideal $\mathbb{I}(\mathcal{D}(G)) \subseteq k'[G]$ of $\mathcal{D}(G)$ is $\mathbb{I}(\mathcal{D}(G)) = \bigcap_{n \geq 1} \ker(\phi_n^*)$. In fact, $\mathbb{I}(\mathcal{D}(G)) = \ker(\phi_n^*)$ for some n ([Mil17, Prop. 6.20]).

The algebraic group G is *perfect* if $\mathcal{D}(G) = G$. Thus G is perfect if and only of ϕ_n^* is injective for some $n \geq 1$. In other words, G is perfect if and only if ϕ_n is dominant for some $n \geq 1$.

The higher derived groups $\mathcal{D}^i(G)$ are defined recursively by $\mathcal{D}^i(G) = \mathcal{D}(\mathcal{D}^{i-1}(G))$. Then $G \supseteq \mathcal{D}(G) \supseteq \mathcal{D}^2(G) \supseteq \ldots$ is a descending sequence of closed subgroups (the derived series) that must eventually terminate, say at $\mathcal{D}^n(G)$. If $\mathcal{D}^n(G) = 1$ is the trivial group, then G is called *solvable*. Otherwise, $\mathcal{D}^n(G)$ is a nontrivial perfect closed subgroup of G.

Lemma 5.4. *If $\mathcal{G}_\xi$ is perfect and nontrivial, then there exists a nonempty Zariski open subset $\mathcal{U}$ of $\mathcal{X}$ such that $\mathcal{G}_c$ is perfect and nontrivial for every $c \in \mathcal{U}$.*

Proof. As above, for $n \geq 1$ consider the scheme morphism

$$\phi_n \colon \mathcal{G}^{2n} \to \mathcal{G}, \ (g_1, h_1, \ldots, g_n, h_n) \mapsto g_1 h_1 g_1^{-1} h_1^{-1} \ldots g_n h_n g_n^{-1} h_n^{-1}.$$

Since $\mathcal{G}_\xi$ is perfect $(\phi_n)_\xi \colon \mathcal{G}_\xi^n \to \mathcal{G}_\xi$ is dominant for some $n \geq 1$. By [Gro66, Theorem 9.6.1 (ii)], the set of all $c \in \mathcal{X}$ such that $(\phi_n)_c \colon \mathcal{G}_c^n \to \mathcal{G}_c$ is dominant is constructible. As it contains the generic point ξ, this set thus contains a nonempty Zariski open subset $\mathcal{U}'$ of $\mathcal{X}$. So for every $c \in \mathcal{U}'$, the algebraic group $\mathcal{G}_c$ is perfect.

By generic freeness ([Sta24, Tag 051S]), there exists nonzero $b \in \mathcal{B}$ such that $\mathcal{B}[\mathcal{G}]_b$ is a free $\mathcal{B}_b$-module, say of rank κ. Then, $\mathcal{B}[\mathcal{G}] \otimes_{\mathcal{B}} k(\mathfrak{p})$ is a $k(\mathfrak{p})$-vector space of dimension κ for every prime ideal $\mathfrak{p} \in D(b)$. The assumption that $\mathcal{G}_\xi$ is nontrivial means that $\mathcal{B}[\mathcal{G}] \otimes_{\mathcal{B}} k(\mathcal{B})$ is not reduced to $k(\mathcal{B})$. So $\kappa > 1$ and $\mathcal{B}[\mathcal{G}] \otimes_{\mathcal{B}} k(\mathfrak{p})$ is not reduced to $k(\mathfrak{p})$ for any $\mathfrak{p} \in D(b)$, i.e., $\mathcal{G}_c$ is nontrivial for $c \in D(b)$. Thus $\mathcal{U} = \mathcal{U}' \cap D(b)$ has the required property. $\qquad\square$

Lemma 5.5. *If $\mathcal{G}_\xi$ is not solvable, there exists a nonempty Zariski open subset $\mathcal{U}$ of $\mathcal{X}$ such that $\mathcal{G}_c$ is not solvable for every $c \in \mathcal{U}$.*

Proof. Since $\mathcal{G}_\xi$ is not solvable, there exists an $n \geq 1$ such that $H = \mathcal{D}^n(\mathcal{G}_\xi)$ is nontrivial and perfect. The closed subgroup H of $\mathcal{G}_\xi$ spreads out to a closed subgroup $\mathcal{H}$ over a nonempty Zariski open subset of $\mathcal{X}$. In detail, there exists a nonempty affine Zariski open $\mathcal{U}'$ of $\mathcal{X}$ and a closed subgroup scheme $\mathcal{H}$ of $\mathcal{G}_{\mathcal{U}'} = \mathcal{G} \times_{\mathcal{X}} \mathcal{U}'$ such that $\mathcal{H}_\xi = H$. This follows, for example, from [Gro66, Theorems 8.8.2 and 8.10.5].

Lemma 5.4 applied to $\mathcal{H}$, yields a nonempty Zariski open subset $\mathcal{U}$ of $\mathcal{U}'$ such that $\mathcal{H}_c$ is nontrivial and perfect for every $c \in \mathcal{U}$. Thus, for every $c \in \mathcal{U}$, the algebraic group $\mathcal{G}_c$ contains the closed nontrivial perfect subgroup $\mathcal{H}_c$ and can therefore not be solvable. $\quad\square$

We are now prepared to prove the main result of this subsection.

Proof of Proposition 5.3. Because solvability ([Mil17, Cor. 6.31]) and the formation of the identity component ([Mil17, Prop. 1.34]) is compatible with base change, we see that $(\mathcal{G}_\xi)^\circ$ is not solvable. As in the proof of Lemma 5.5, the closed subgroup $H = (\mathcal{G}_\xi)^\circ$ of $\mathcal{G}_\xi$ spreads out to a closed subgroup scheme over a nonempty Zariski open subset of $\mathcal{X}$, i.e., there exists a nonempty Zariski open subset $\mathcal{U}_1$ of $\mathcal{X}$ and a closed subgroup $\mathcal{H}$ of $\mathcal{G}_{\mathcal{U}_1} = \mathcal{G} \times_{\mathcal{X}} \mathcal{U}_1$ such that $\mathcal{H}_\xi = (\mathcal{G}_\xi)^\circ$. Because $\mathcal{H}_c$ is (geometrically) connected, there exists a nonempty Zariski open subset $\mathcal{U}_2$ of $\mathcal{U}_1$ such that $\mathcal{H}_c$ is (geometrically) connected for every $c \in \mathcal{U}_2$ ([Gro66, Theorem 9.7.7]). Moreover, there exists a nonempty Zariski open subset $\mathcal{U}_3$ of $\mathcal{U}_1$ such that $\dim(\mathcal{G}_c) = \dim(\mathcal{G}_\xi)$ and $\dim(\mathcal{H}_c) = \dim(H_\xi)(= \dim(\mathcal{G}_\xi))$ for all $c \in \mathcal{U}_3$ ([Sta24, Tag 05F7]). In summary, this shows that we can find a nonempty Zariski open subset $\mathcal{U}'$ of $\mathcal{U}_1$ such that $\mathcal{H}_c = (\mathcal{G}_c)^\circ$ for all $c \in \mathcal{U}'$.

Applying Lemma 5.5 to the affine group scheme $\mathcal{H}_{\mathcal{U}'} = \mathcal{H} \times_{\mathcal{U}_1} \mathcal{U}'$ over $\mathcal{U}'$ yields a nonempty Zariski open susbset $\mathcal{U}''$ of $\mathcal{U}'$ such that $\mathcal{H}_c = (\mathcal{G}_c)^\circ$ is not solvable for all $c \in \mathcal{U}''$. In particular, $(\mathcal{G}_c)^\circ$ is not solvable for every $c \in \mathcal{U} = \mathcal{U}'' \cap \mathcal{X}(k)$. $\quad\square$

5.1.3 Exceptional parameter values for solving in a family of linear differential equations

Throughout Subsection 5.1.3 we make the following assumptions:

- $k \subseteq k'$ is an inclusion of algebraically closed fields of characteristic zero;

- $\delta(y) = Ay$ is a linear differential equation over $k'(x)$, i.e., $A \in k'(x)^{n \times n}$;

- $\mathcal{B}_0 \subseteq k'$ is a finitely generated k-algebra and $f_0 \in \mathcal{B}_0[x]$ is a monic polynomial such that $A \in \mathcal{B}_0[x]_{f_0}^{n \times n}$;

- $\mathcal{X}_0 = \mathrm{Spec}(\mathcal{B}_0)$;

- for $c_0 \in \mathcal{X}_0(k)$ we denote with $A^{c_0} \in k(x)^{n \times n}$ the matrix obtained from A by applying $c_0 \colon \mathcal{B}_0 \to k$ to the coefficients of the entries of A.

We first treat the case of solving in Liouvillian extensions. Recall that a subset of $\mathcal{X}_0(k)$ is called ad$\times$Jac-closed (or ad-closed) if its complement is ad$\times$Jac-open (or ad-open).

Corollary 5.6. *Assume that the differential equation $\delta(y) = Ay$ (over $k'(x)$) does not have a basis of solutions consisting of Liouvillian functions, then the set of all $c_0 \in \mathcal{X}_0(k)$ such that the differential equation $\delta(y) = A^{c_0}y$ (over $k(x)$) has a basis of solutions consisting of Liouvillian functions, is contained in an ad$\times$Jac-closed subset of $\mathcal{X}_0(k)$.*

Proof. Let $R/k'(x)$ be a Picard-Vessiot ring for $\delta(y) = Ay$. By Lemma 3.11, there exists

- a finitely generated k-subalgebra $\mathcal{B}$ of k' containing $\mathcal{B}_0$ and contained in the algebraic closure of the field of fractions of $\mathcal{B}_0$;

- a monic polynomial $f \in \mathcal{B}[x]$ such that f_0 divides f in $\mathcal{B}[x]$;

- an affine group scheme $\mathcal{G}$ of finite type over $\mathcal{B}$;

- a differential $\mathcal{G}$-torsor $\mathcal{R}/\mathcal{B}[x]_f$ for $\delta(y) = Ay$ such that $\mathcal{R}$ is a flat $\mathcal{B}[x]_f$-module, $\mathcal{R} \otimes_{\mathcal{B}[x]_f} K(x)$ is δ-simple, where K is the algebraic closure of the field of fractions of $\mathcal{B}$ and $\mathcal{R} \otimes_{\mathcal{B}[x]_f} k'(x) \simeq R$.

Note that $\mathcal{R} \otimes_{\mathcal{B}[x]_f} K(x)$ is a Picard-Vessiot ring over $K(x)$ with differential Galois group $\mathcal{G}_K$ (Lemma 4.14). So it follows from Lemma 3.2 that $\mathcal{R} \otimes_{\mathcal{B}[x]_f} k'(x) \simeq R$ is a Picard-Vessiot ring over $k'(x)$ with differential Galois group $\mathcal{G}_{k'}$. Because $\delta(y) = Ay$ (over $k'(x)$) does not have a basis consisting of Liouvillian functions, we know that $(\mathcal{G}_{k'})^\circ$ is not solvable ([vdPS03, Theorem 1.43]). As the formation of the identity component ([Mil17, Prop. 1.34]) and solvability ([Mil17, Cor. 6.31]) is compatible with base change, this implies that $(\mathcal{G}_K)^\circ$ is not solvable.

Set $\mathcal{X} = \mathrm{Spec}(\mathcal{B})$. By Proposition 5.3, there exists a nonempty Zariski open subset $\mathcal{U}_1$ of $\mathcal{X}(k)$ such that $(\mathcal{G}_c)^\circ$ is not solvable for every $c \in \mathcal{U}_1$.

Theorem 4.26 applied to the differential torsor $\mathcal{R}/\mathcal{B}[x]_f$ for $\delta(y) = Ay$ yields an ad$\times$Jac-open subset $\mathcal{U}_2$ of $\mathcal{X}(k)$ such that $R^c = \mathcal{R} \otimes_{\mathcal{B}[x]_f} k(x)$ is Picard-Vessiot for all $c \in \mathcal{U}_2$. By Lemma 2.7, there exists an ad$\times$Jac-open subset $\mathcal{U}_0$ of $\mathcal{X}_0(k)$ such that $\mathcal{U}_0$ is contained in the image $\mathcal{U}_1 \cap \mathcal{U}_2$ under $\mathcal{X}(k) \to \mathcal{X}_0(k)$. For any $c_0 \in \mathcal{U}_0$, there thus exists a $c \in \mathcal{U}_1 \cap \mathcal{U}_2$ mapping to c_0. We then have $A^{c_0} = A^c$ and $R^c/k(x)$ is a Picard-Vessiot ring for $\delta(y) = A^c y$ with differential Galois group $G^c = \mathcal{G}_c$. As $(\mathcal{G}_c)^\circ$ is not solvable, we see that $\delta(y) = A^{c_0} y$ does not have a basis of solutions consisting of Liouvillian functions for every $c_0 \in \mathcal{U}_0$. Thus the set of all $c_0 \in \mathcal{X}_0(k)$ such that $\delta(y) = A^{c_0} y$ has a basis of solutions consisting of Liouvillian functions, is contained in the complement of $\mathcal{U}_0$. $\square$

Remark 5.7. *If, in the context of Corollary 5.6, the differential Galois group of $\delta(y) = Ay$ (over $k'(x)$) is connected, we can make do with an ad-closed subset of $\mathcal{X}_0(k)$.*

Proof. As in Remark 5.2, we see that the differential Galois group G^{gen} of $\mathcal{R}^{\mathrm{gen}}$ is connected and so $\mathcal{U}_2$ can be chosen to be ad-open by Corollary 4.27. $\square$

We next treat the case of solving in algebraic extensions.

Corollary 5.8. *Assume that the differential equation $\delta(y) = Ay$ (over $k'(x)$) does not have a basis of solutions consisting of algebraic functions, then the set of all $c_0 \in \mathcal{X}_0(k)$ such that the differential equation $\delta(y) = A^{c_0} y$ (over $k(x)$) has a basis consisting of algebraic functions, is contained in an ad$\times$Jac-closed subset of $\mathcal{X}_0(k)$.*

Proof. This could be deduced directly from Corollary 5.1. Alternatively, noting that a differential equation has a basis of algebraic solutions if and only if its differential Galois group is finite, this can be proved exactly like Corollary 5.6 but replacing Proposition 5.3 with the following statement: With the notation of Subsection 5.1.2, if $\mathcal{G}_{\bar{\xi}}$ is finite, then there exists a nonempty Zariski open subset $\mathcal{U}$ of $\mathcal{X}(k)$ such that $\mathcal{G}_c$ is finite for every $c \in \mathcal{U}$. $\square$

Remark 5.9. *Again, if in the context of Corollary 5.8, the differential Galois group of $\delta(y) = Ay$ (over $K(x)$) is connected, then we can make do with an ad-closed subset of $\mathcal{X}_0(k)$.*

5.2 A short solution of the inverse problem

The *solution of the inverse problem* states that every linear algebraic group over k is a differential Galois group over $k(x)$. Using the Riemann-Hilbert correspondence, this was proved for $k = \mathbb{C}$ already in 1979 ([TT79]) but it took more than 25 years and contributions of many authors to finally solve the inverse problem for an arbitrary algebraically closed field k of characteristic zero ([Har05]).

In this short section, we explain how Theorem 4.26 can be used to deduce the solution of the inverse problem over k, from the solution of the inverse problem over $\mathbb{C}$. Of course, our solution is only short if one accepts Theorem 4.26 and the solution of the inverse problem over $\mathbb{C}$, as given.

Theorem 5.10. *Let k be an algebraically closed field of characteristic zero. Then every linear algebraic group over k is a differential Galois group over $k(x)$.*

Proof. Let G be a linear algebraic group over k. Then G descends to a finitely generated field, i.e., there exists a subfield k_0 of k finitely generated over $\mathbb{Q}$ and a linear algebraic group G_0 over k_0 such that $(G_0)_k = G$. Passing to the algebraic closure $k_1 \subseteq k$ of k_0, we obtain a countable algebraically closed field k_1 and a linear algebraic group G_1 over k_1 such that $(G_1)_k = G$.

By Lemma 3.2, it suffices to show that G_1 is a differential Galois group over $k_1(x)$. Since k_1 is countable, there exists an embedding of k_1 into $\mathbb{C}$ that we now fix.

By [TT79], there exists a Picard-Vessiot ring $R/\mathbb{C}(x)$ for some equation $\delta(y) = Ay$, $(A \in \mathbb{C}(x)^{n \times n})$ with differential Galois group $(G_1)_{\mathbb{C}}$. The Picard-Vessiot ring $R/\mathbb{C}(x)$ can now be spread out by Lemma 3.11, i.e., there exists

- a finitely generated k_1-subalgebra $\mathcal{B}$ of $\mathbb{C}$,

- a monic polynomial $f \in \mathcal{B}[x]$ with $A \in \mathcal{B}[x]_f^{n \times n}$

- and a differential $(G_1)_{\mathcal{B}}$-torsor $\mathcal{R}/\mathcal{B}[x]_f$ for $\delta(y) = Ay$ such that $\mathcal{R}$ is flat over $\mathcal{B}[x]_f$ and $\mathcal{R} \otimes_{\mathcal{B}[x]_f} K(x)$ is δ-simple, where K is the algebraic closure of the field of fractions of $\mathcal{B}$.

Set $\mathcal{X} = \mathrm{Spec}(\mathcal{B})$. By the specialization theorem (Theorem 4.26), there exists a $c \in \mathcal{X}(k_1)$ such that $R^c = \mathcal{R} \otimes_{\mathcal{B}[x]_f} k_1(x)$ is Picard-Vessiot. So $R^c/k_1(x)$ is a Picard-Vessiot ring for $\delta(y) = A^c y$ with differential Galois group $((G_1)_{\mathcal{B}})^c = ((G_1)_{\mathcal{B}})_{k_1} = G_1$. In particular, G_1 is a differential Galois group over $k_1(x)$ as desired. $\square$

5.3 Proof of Matzat's conjecture

In this section we show that every differential embedding problem of finite type over $(k(x), \frac{d}{dx})$ has a solution (Theorem 5.14) and deduce Matzat's conjecture from this. The idea for the proof is to first solve the differential embedding problem over a sufficiently large field of constants $k' \supseteq k$ and then to go back down to k using Theorem 4.26.

Throughout Section 5.3 we assume that k is an algebraically closed field of characteristic zero. Let us recall some background on differential embedding problems. Let F be a differential field with $F^\delta = k$. If $R \subseteq S$ is an inclusion of Picard-Vessiot rings over F, then there is a restriction map $G(S/F) \twoheadrightarrow G(R/F)$ on the differential Galois groups which is a quotient map, i.e., the dual map is injective.

Definition 5.11. *A* differential embedding problem *of finite type over F is a pair* $(\phi\colon G \twoheadrightarrow H, R)$, *consisting of a quotient map $\phi\colon G \twoheadrightarrow H$ of linear algebraic groups over k and a Picard-Vessiot ring R/F with differential Galois group H. A* solution *is a Picard-Vessiot ring S/F containing R together with an isomorphism $G \simeq G(S/F)$ such that*

$$
\begin{array}{ccc}
G & \xrightarrow{\;\;\simeq\;\;} & G(S/F) \\
& \searrow \qquad \swarrow & \\
& H = G(R/F) &
\end{array}
\tag{39}
$$

commutes. In other words, the restriction map $G(S/F) \twoheadrightarrow G(R/F)$ realizes the given morphism $\phi\colon G \twoheadrightarrow H$.

The attribute "of finite type" in Definition 5.11 refers to the assumption that G (and hence H) is a group scheme of finite type (over k). In general, to deal with Matzat's conjecture, it is important to allow more general differential embedding problems (not necessarily of finite type). See [BHHW21b]. However, for our purpose differential embedding problems of finite type are sufficient. On the ring side, the commutativity of (39) is expressed by the commutativity of

$$
\begin{array}{ccc}
S & \longrightarrow & S \otimes_k k[G] \\
\uparrow & & \uparrow \\
R & \longrightarrow & R \otimes_k k[H]
\end{array}
$$

where $R \otimes_k k[H] \to S \otimes_k k[G]$, $r \otimes a \mapsto r \otimes \phi^*(a)$ with $\phi^*\colon k[H] \to k[G]$ the dual of ϕ.

As detailed in the following remark, a differential embedding problem over $k(x)$ can always be extended to a differential embedding problem over $k'(x)$.

Remark 5.12. *Let $(\phi\colon G \twoheadrightarrow H, R)$ be a differential embedding problem of finite type over $k(x)$ and let k' be an algebraically closed field extension of k. Then $R' = R \otimes_{k(x)} k'(x)$ is a Picard-Vessiot ring over $k'(x)$ with differential Galois group $H_{k'}$ (Lemma 3.2). Therefore, $(\phi_{k'}\colon G_{k'} \twoheadrightarrow H_{k'}, R')$ is a differential embedding problem of finite type over $k'(x)$.*

To apply Theorem 4.26 we first need to "spread out" a solution of the extended differential embedding problem into a family with nice properties. This is achieved in the following lemma. Recall that actions of affine group schemes on differential algebras were defined in Section 3.2.

Lemma 5.13. *Let $(\phi\colon G \twoheadrightarrow H, R)$ be a differential embedding problem of finite type over $k(x)$. Let k' be an algebraically closed field extension of k and let $S'/k'(x)$ be a solution of the induced differential embedding problem $(\phi_{k'}\colon G_{k'} \twoheadrightarrow H_{k'}, R')$ over $k'(x)$, where $R' = R \otimes_{k(x)} k'(x)$. Then there exist*

(i) *a monic polynomial $h \in k[x]$, and a $k[x]_h$-δ-subalgebra R_0 of R with an action of H on $R_0/k[x]_h$ such that $R_0 \otimes_{k[x]_h} k(x) = R$ (equivalently, $U^{-1}R_0 = R$, where $U = k[x]_h \smallsetminus \{0\}$) and the induced action of H on $U^{-1}R_0/U^{-1}k[x]_h$ is the natural action of H on $R/k(x)$,*

(ii) *a finitely generated k-subalgebra $\mathcal{B}$ of k' and a monic polynomial $f \in \mathcal{B}[x]$ such that $h \in k[x] \subseteq \mathcal{B}[x]$ divides f in $\mathcal{B}[x]$,*

(iii) *a matrix $\mathcal{A} \in \mathcal{B}[x]_f^{n \times n}$ and a differential $G_{\mathcal{B}}$-torsor $\mathcal{S}/\mathcal{B}[x]_f$ for $\delta(y) = \mathcal{A}y$ such that $\mathcal{S}$ is flat over $\mathcal{B}[x]_f$ and $S^{\mathrm{gen}} = \mathcal{S} \otimes_{\mathcal{B}[x]_f} K(x)$ is δ-simple, where $K = \overline{k(\mathcal{B})} \subseteq k'$ is the algebraic closure of the field of fractions of $\mathcal{B}$,*

(iv) *a morphism $\mathcal{R} \to \mathcal{S}$ of $\mathcal{B}[x]_f$-δ-algebras that is equivariant with respect to the morphism $\phi_{\mathcal{B}}\colon G_{\mathcal{B}} \to H_{\mathcal{B}}$, where $\mathcal{R} = R_0 \otimes_{k[x]_h} \mathcal{B}[x]_f = (R_0 \otimes_k \mathcal{B})_f$ and $\mathcal{R}/\mathcal{B}[x]_f$ has an $H_{\mathcal{B}}$-action induced from* (i) *above. (The equivariance means that for every $\mathcal{B}$-algebra $\mathcal{T}$ and $g \in G_{\mathcal{B}}(\mathcal{T})$ the diagram*

$$
\begin{array}{ccc}
\mathcal{S} \otimes_{\mathcal{B}} \mathcal{T} & \xrightarrow{\;g\;} & \mathcal{S} \otimes_{\mathcal{B}} \mathcal{T} \\
\uparrow & & \uparrow \\
\mathcal{R} \otimes_{\mathcal{B}} \mathcal{T} & \xrightarrow{\;\phi(g)\;} & \mathcal{R} \otimes_{\mathcal{B}} \mathcal{T}
\end{array}
$$

commutes.)

Proof. We begin with (i). Choose $A \in k(x)^{m \times m}$ such that $R/k(x)$ is a Picard-Vessiot ring for $\delta(y) = Ay$. Let $h \in k[x]$ be a monic polynomial such that $A \in k[x]_h^{m \times m}$ and let $Y \in \mathrm{GL}_m(R)$ satisfy $\delta(Y) = AY$. Then $R_0 = k[x]_h[Y, \frac{1}{\det(Y)}]$ is a δ-subring of R because $\delta(Y) = AY \in R_0^{m \times m}$. For a k-algebra T an element $g \in H(T)$ acts on $R \otimes_k T$ by $Y \otimes 1 \mapsto Y \otimes [g]$ for some matrix $[g] \in \mathrm{GL}_m(T)$. Thus $g\colon R \otimes_k T \to R \otimes_k T$ restricts to a $k[x]_h \otimes_k T$-δ-automorphism of $R_0 \otimes_k T$. This defines an action of H on $R_0/k[x]_h$ that clearly induces the given action on $R/k(x)$.

To address the remaining points, fix $A' \in k'(x)^{n \times n}$ and $Y' \in \mathrm{GL}_n(S')$ such that $S'/k'(x)$ is a Picard-Vessiot ring for $\delta(y) = A'y$ and $\delta(Y') = A'Y'$. As $R \subseteq R' \subseteq S' = k'(x)[Y', \frac{1}{\det(Y')}]$, there exists a finitely generated k-subalgebra $\mathcal{B}_0$ of k' and a monic polynomial $f_0' \in \mathcal{B}_0[x]$ such that all entries of Y and $\frac{1}{\det(Y)}$ lie in $\mathcal{B}_0[x]_{f_0'}[Y', \frac{1}{\det(Y')}] \subseteq S'$. Set $f_0 = hf_0' \in \mathcal{B}_0[x]$. Then $R_0 = k[x]_h[Y, \frac{1}{\det(Y)}] \subseteq \mathcal{B}_0[x]_{f_0}[Y', \frac{1}{\det(Y')}] \subseteq S'$.

Now Lemma 3.11 yields a finitely generated k-subalgebra $\mathcal{B}$ of k' with $\mathcal{B}_0 \subseteq \mathcal{B}$, a monic polynomial $f \in \mathcal{B}[x]$ such that f_0 divides f in $\mathcal{B}[x]$, a differential $G_{\mathcal{B}}$-torsor $\mathcal{S}/\mathcal{B}[x]_f$ for $\delta(y) = A'y$ with fundamental solution matrix $\mathcal{Y}$ such that $\mathcal{S}$ is flat over $\mathcal{B}[x]_f$, $S^{\mathrm{gen}} = \mathcal{S} \otimes_{\mathcal{B}[x]_f} K(x)$ is δ-simple and $\mathcal{S} \otimes_{\mathcal{B}[x]_f} k'(x) \simeq S'$ via $\mathcal{Y} \mapsto Y'$. So, $\mathcal{S}$ can be identified with $\mathcal{B}[x]_f[Y', \frac{1}{\det(Y')}] \subseteq S'$ and $R_0 \subseteq \mathcal{S}$.

By now we have established (i), (ii) and (iii) of the lemma. Let us move on to (iv). Setting $\mathcal{R} = R_0 \otimes_{k[x]_h} \mathcal{B}[x]_f$, the inclusion $R_0 \subseteq \mathcal{S}$ yields a morphism $\mathcal{R} \to \mathcal{S}$ of $\mathcal{B}[x]_f$-δ-algebras. Since $S'/k'(x)$ is a solution of the differential embedding problem ($\phi_{k'}\colon G_{k'} \twoheadrightarrow H_{k'}$, R') the diagram

$$
\begin{array}{ccc}
S' & \longrightarrow & S' \otimes_{k'} k'[G_{k'}] \\
\uparrow & & \uparrow \\
R' & \longrightarrow & R' \otimes_{k'} k'[H_{k'}]
\end{array}
$$

commutes. Therefore also

$$
\begin{array}{ccccccc}
\mathcal{S} & \longrightarrow & \mathcal{S} \otimes_{\mathcal{B}} \mathcal{B}[G_{\mathcal{B}}] & = & \mathcal{S} \otimes_k k[G] & \hookrightarrow & S' \otimes_k k[G] = S' \otimes_{k'} k'[G_{k'}] \\
\uparrow & & & & \uparrow & & \uparrow \\
R_0 & & \longrightarrow & & R_0 \otimes_k k[H] & \hookrightarrow & R' \otimes_k k[H] = R' \otimes_{k'} k'[H_{k'}]
\end{array}
$$

and

$$\begin{array}{ccc}
\mathcal{S} & \longrightarrow & \mathcal{S} \otimes_{\mathcal{B}} \mathcal{B}[G_{\mathcal{B}}] \\
\uparrow & & \uparrow \\
\mathcal{R} & \longrightarrow & \mathcal{R} \otimes_{\mathcal{B}} \mathcal{B}[H_{\mathcal{B}}]
\end{array}$$

commutes. This establishes (iv). $\qquad\square$

The following theorem was proved in [BHHP21] under the assumption that k has infinite transcendence degree over $\mathbb{Q}$. Thanks to Theorem 4.26 we are able to remove this unnecessary assumption.

Theorem 5.14. *Let k be an algebraically closed field of characteristic zero. Then every differential embedding problem of finite type over $(k(x), \frac{d}{dx})$ is solvable.*

Proof. Let $(\phi\colon G \twoheadrightarrow H, \ R)$ be a differential embedding problem of finite typer over $k(x)$. Let k' be an algebraically closed field extension of k such that k' has infinite transcendence degree over $\mathbb{Q}$. Consider the induced differential embedding problem $(\phi_{k'}\colon G_{k'} \twoheadrightarrow H_{k'}, \ R')$, where $R' = R \otimes_{k(x)} k'(x)$. According to [BHHP21, Cor. 4.6] it has a solution $S'/k'(x)$. Let $h, R_0, \mathcal{B}, f, \mathcal{A}, \mathcal{R}$ and $\mathcal{S}$ be as in Lemma 5.13 and set $\mathcal{X} = \mathrm{Spec}(\mathcal{B})$. Then $\mathcal{S}/\mathcal{B}[x]_f$ satisfies all the assumptions of Notation 4.12 and it follows from Theorem 4.26 that there exists a $c \in \mathcal{X}(k)$ such that $S^c = \mathcal{S} \otimes_{\mathcal{B}[x]_f} k(x)$ is a Picard-Vessiot ring. In fact, $S^c/k(x)$ is a Picard-Vessiot ring with differential Galois group $G^c = (G_{\mathcal{B}})_c = G$.

The morphism $\mathcal{R} \to \mathcal{S}$ of $\mathcal{B}[x]_f$-δ-algebras yields a morphism $\mathcal{R} \otimes_{\mathcal{B}[x]_f} k(x) \to \mathcal{S} \otimes_{\mathcal{B}[x]_f} k(x)$ of $k(x)$-δ-algebras. But

$$\mathcal{R} \otimes_{\mathcal{B}[x]_f} k(x) = (R_0 \otimes_{k[x]_h} \mathcal{B}[x]_f) \otimes_{\mathcal{B}[x]_f} k(x) = R_0 \otimes_{k[x]_h} k(x) = R$$

and $\mathcal{S} \otimes_{\mathcal{B}[x]_f} k(x) = S^c$. We thus obtain an embedding $R \to S^c$ of Picard-Vessiot rings over $k(x)$. By (iv) of Lemma 5.13 the diagram

$$\begin{array}{ccc}
\mathcal{S} & \longrightarrow & \mathcal{S} \otimes_{\mathcal{B}} \mathcal{B}[G_{\mathcal{B}}] \\
\uparrow & & \uparrow \\
\mathcal{R} & \longrightarrow & \mathcal{R} \otimes_{\mathcal{B}} \mathcal{B}[H_{\mathcal{B}}]
\end{array}$$

commutes. Therefore also its base change

$$\begin{array}{ccc}
S^c & \longrightarrow & S^c \otimes_k k[G] \\
\uparrow & & \uparrow \\
R & \longrightarrow & R \otimes_k k[H]
\end{array}$$

via $\mathcal{B}[x]_f \to k(x)$ commutes. Thus $S^c/k(x)$ is a solution of $(\phi\colon G \twoheadrightarrow H, \ R)$. $\qquad\square$

We are now prepared to prove Matzat's conjecture in full generality.

Theorem 5.15. *Let k be an algebraically closed field of characteristic zero and let F be a one-variable function field over k, equipped with a non-trivial k-derivation. Then the absolute differential Galois group of F is the free proalgebraic group on a set of cardinality $|F|$.*

Proof. The case when k has infinite transcendence degree (over $\mathbb{Q}$) is proved in [Wib23, Theorem 2.9]. So we can assume that k has finite transcendence degree. In particular, k is countable. In [Wib23, Prop. 2.8] it is shown that if Matzat's conjecture is true for $(k(x), \frac{d}{dx})$, then it is true for F. So we have reduced to proving the theorem for $(k(x), \frac{d}{dx})$ with k countable. According to [BHHW21b, Cor. 3.9], the absolute differential Galois group of a countable differential field F is free on a countably infinite set if and only if every differential embedding problem over F of finite type is solvable. It therefore suffices to show that every differential embedding problem of finite type over $(k(x), \frac{d}{dx})$ is solvable. This is exactly Theorem 5.14. $\square$

References

[AM69]   M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra.* Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[AMP22]   Eli Amzallag, Andrei Minchenko, and Gleb Pogudin. Degree bound for toric envelope of a linear algebraic group. *Math. Comp.*, 91(335):1501–1519, 2022.

[And04]   Yves André. Sur la conjecture des p-courbures de Grothendieck-Katz et un problème de Dwork. In *Geometric aspects of Dwork theory. Vol. I, II*, pages 55–112. Walter de Gruyter, Berlin, 2004.

[BBH88]   Frits Beukers, W. Dale Brownawell, and Gert Heckman. Siegel normality. *Ann. of Math. (2)*, 127(2):279–308, 1988.

[BHHP21]   Annette Bachmayr, David Harbater, Julia Hartmann, and Florian Pop. Large fields in differential Galois theory. *J. Inst. Math. Jussieu*, 20(6):1931–1946, 2021.

[BHHW18]   Annette Bachmayr, David Harbater, Julia Hartmann, and Michael Wibmer. Differential embedding problems over complex function fields. *Doc. Math.*, 23:241–291, 2018.

[BHHW21a] Annette Bachmayr, David Harbater, Julia Hartmann, and Michael Wibmer. The differential Galois group of the rational function field. *Adv. Math.*, 381, 2021.

[BHHW21b] Annette Bachmayr, David Harbater, Julia Hartmann, and Michael Wibmer. Free differential Galois groups. *Trans. Amer. Math. Soc.*, 374(6):4293–4308, 2021.

[BLR90]   Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron models*, volume 21 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1990.

[Bou72]   Nicolas Bourbaki. *Elements of mathematics. Commutative algebra.* Hermann, Paris, 1972. Translated from the French.

[Bou90]   N. Bourbaki. *Algebra. II. Chapters 4–7.* Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 1990. Translated from the French by P. M. Cohn and J. Howie.

[BvdP06]   Maint Berkenbosch and Marius van der Put. Families of linear differential equations on the projective line. In *Groupes de Galois arithmétiques et différentiels*, volume 13 of *Sémin. Congr.*, pages 39–68. Soc. Math. France, Paris, 2006.

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

[CS99]   Élie Compoint and Michael F. Singer. Computing Galois groups of completely reducible differential equations. *J. Symbolic Comput.*, 28(4-5):473–494, 1999.

[Dav16]   Damien Davy. *Spécialisation du pseudo-groupe de Malgrange et irréductibilité*. Theses, Université Rennes 1, December 2016.

[dS09]   João Pedro P. dos Santos. The behaviour of the differential Galois group on the generic and special fibres: a Tannakian approach. *J. Reine Angew. Math.*, 637:63–98, 2009.

[Eis04]   David Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*. Number 150 in GTM. Springer, 2004.

[Fen15]   Ruyong Feng. Hrushovski's algorithm for computing the Galois group of a linear differential equation. *Adv. in Appl. Math.*, 65:1–37, 2015.

[Fen21]   Ruyong Feng. Difference Galois groups under specialization. *Trans. Amer. Math. Soc.*, 374(1):61–96, 2021.

[FJ08]   Michael D. Fried and Moshe Jarden. *Field arithmetic*, volume 11 of *Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics*. Springer-Verlag, Berlin, third edition, 2008. Revised by Jarden.

[Gol57]   Lawrence Goldman. Specialization and Picard-Vessiot theory. *Trans. Amer. Math. Soc.*, 85:327–356, 1957.

[Gro66]   A. Grothendieck. Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. III. *Inst. Hautes Études Sci. Publ. Math.*, (28):255, 1966.

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

[Har05]   Julia Hartmann. On the inverse problem in differential Galois theory. *J. Reine Angew. Math.*, 586:21–44, 2005.

[Hru02]   Ehud Hrushovski. Computing the Galois group of a linear differential equation. In *Differential Galois theory (Bedlewo, 2001)*, volume 58 of *Banach Center Publ.*, pages 97–138. Polish Acad. Sci., Warsaw, 2002.

[Kat90]   Nicholas M. Katz. *Exponential sums and differential equations*, volume 124 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1990.

[Kol68]   E. R. Kolchin. Algebraic groups and algebraic dependence. *Amer. J. Math.*, 90:1151–1164, 1968.

[Lan83]   Serge Lang. *Fundamentals of Diophantine geometry*. Springer-Verlag, New York, 1983.

[Mag94]   Andy R. Magid. *Lectures on differential Galois theory*, volume 7 of *University Lecture Series*. American Mathematical Society, Providence, RI, 1994.

[Mil86]   J. S. Milne. Abelian varieties. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 103–150. Springer, New York, 1986.

[Mil17]   J. S. Milne. *Algebraic groups*, volume 170 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2017. The theory of group schemes of finite type over a field.

[MZ20]   David Masser and Umberto Zannier. Torsion points, Pell's equation, and integration in elementary terms. *Acta Math.*, 225(2):227–313, 2020.

[Nér52]   André Néron. Problèmes arithmétiques et géométriques rattachés à la notion de rang d'une courbe algébrique dans un corps. *Bull. Soc. Math. France*, 80:101–166, 1952.

[Pet06]   Sebastian Petersen. On a question of Frey and Jarden about the rank of abelian varieties. *J. Number Theory*, 120(2):287–302, 2006.

[Poo17]   Bjorn Poonen. *Rational points on varieties*, volume 186 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2017.

[RS23]   Daniel Robertz and Matthias Seiß. Normal forms in differential Galois theory for the classical groups. *Comm. Algebra*, 51(4):1492–1516, 2023.

[Sau16]   Jacques Sauloy. *Differential Galois theory through Riemann-Hilbert correspondence*, volume 177 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2016. An elementary introduction, With a foreword by Jean-Pierre Ramis.

[Sei22]   Matthias Seiß. Root parametrized differential equations for the classical groups. 2022. arXiv:1609.05535.

[Ser97a]   Jean-Pierre Serre. *Galois cohomology*. Springer-Verlag, Berlin, 1997. Translated from the French by Patrick Ion and revised by the author.

[Ser97b]   Jean-Pierre Serre. *Lectures on the Mordell-Weil theorem*. Aspects of Mathematics. Friedr. Vieweg & Sohn, Braunschweig, third edition, 1997. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt, With a foreword by Brown and Serre.

[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.

[Sta24]   The Stacks Project Authors. Stacks Project. `http://stacks.math.columbia.edu`, 2024.

[Sti09]   Henning Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.

[Str99]   Neil P. Strickland. Formal schemes and formal groups. In *Homotopy invariant algebraic structures (Baltimore, MD, 1998)*, volume 239 of *Contemp. Math.*, pages 263–352. Amer. Math. Soc., Providence, RI, 1999.

[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.

[vdPS03]   Marius van der Put and Michael F. Singer. *Galois theory of linear differential equations*, volume 328 of *Fundamental Principles of Mathematical Sciences*. Springer-Verlag, Berlin, 2003.

[vH97a]   Mark van Hoeij. Factorization of differential operators with rational functions coefficients. *J. Symbolic Comput.*, 24(5):537–561, 1997.

[vH97b]   Mark van Hoeij. Formal solutions and factorization of differential operators with power series coefficients. *J. Symbolic Comput.*, 24(1):1–30, 1997.

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

[Wib20]   Michael Wibmer. Free proalgebraic groups. *Épijournal Géom. Algébrique*, 4:Art. 1, 36, 2020.

[Wib23]   Michael Wibmer. Subgroups of free proalgebraic groups and Matzat's conjecture for function fields. *Israel J. Math.*, 253(2):841–863, 2023.

[Zan14a]   Umberto Zannier. Elementary integration of differentials in families and conjectures of Pink. In *Proceedings of the International Congress of Mathematicians—Seoul 2014. Vol. II*, pages 531–555. Kyung Moon Sa, Seoul, 2014.

[Zan14b]   Umberto Zannier. Unlikely intersections and Pell's equations in polynomials. In *Trends in contemporary mathematics*, volume 8 of *Springer INdAM Ser.*, pages 151–169. Springer, Cham, 2014.

Ruyong Feng, KLMM, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, and School of Mathematics, University of Chinese Academy of Sciences, No.55 Zhongguancun East Road, 100190, Beijing, China, `ryfeng@amss.ac.cn`

Michael Wibmer, School of Mathematics, University of Leeds, LS2 9JT, Leeds, United Kingdom, `m.wibmer@leeds.ac.uk`