Difference Galois Groups under Specialization

Ruyong Feng

KLMM, Academy of Mathematics and Systems Science,
School of Mathematics, University of Chinese Academy of Sciences,
Chinese Academy of Sciences, Beijing 100190, China
ryfeng@amss.ac.cn

Abstract

We present a difference analogue of a result on specializations of differential Galois groups given by Hrushovski. Let k be a field of characteristic zero and let D be a finitely generated domain over k. Consider the linear difference equation

$$\sigma(Y) = AY$$

where A is an invertible matrix with entries in the field of fractions of $D[x]$ and σ is a shift operator $\sigma(x) = x + 1$. We prove that the set of k-homomorphisms φ from D to $\bar{k}$ under which the Galois group of $\sigma(Y) = AY$ specializes to the Galois group of $\sigma(Y) = \varphi(A)Y$ over $\bar{k}(x)$ is not empty, and if D is transcendental over k then this set is infinite.

We apply our result to van der Put-Singer conjecture which asserts that an algebraic subgroup G of $\mathrm{GL}_n(\bar{k})$ is the Galois group of a linear difference equation over $\bar{k}(x)$ if and only if the quotient G/G° by the identity component is cyclic. We show that if van der Put-Singer conjecture is true for $\bar{k} = \mathbb{C}$ then it will be true for $\bar{k}$ to be any algebraically closed field of characteristic zero.

Keywords: Linear difference equations, Difference Galois groups, Specializations, Inverse problem.

1 Introduction

Let K be a function field of one variable over $\mathbb{Q}$ and let L be a linear differential operator with coefficients in the differential field $(K(t), \mathrm{d}/\mathrm{d}t)$. In [7], Hrushovski proved that for many places $\mathfrak{p}$ in K, the Galois group of $L = 0$ specializes precisely to the Galois group of $L_{\mathfrak{p}} = 0$, where $L_{\mathfrak{p}}$ denotes the operator obtained by applying $\mathfrak{p}$ to the coefficients of L. As a corollary, he proved a function field analogue of Grothendieck-Katz conjecture. Besides Hrushovski's result, Goldman in [5] proved a weaker result that under an analytic specialization, the Galois group of $L = 0$ specializes to a group which contains the Galois group of the specialization of $L = 0$. It is natural to ask whether a similar phenomenon occurs for linear difference equations. The goal of this paper is to provide an affirmative answer of this question. Let us start with an example.

2010 Mathematics Subject Classification. Primary 12H10; Secondary 13B05

Example 1.1 *Consider*

$$\sigma(Y) = \mathrm{diag}(t, x, x+t)Y$$

where t is an indeterminate and σ is a shift operator $\sigma(x) = x+1$. Denote $A(t) = \mathrm{diag}(t, x, x+t)$. Due to van der Put-Singer's method (see Section 2.2 of [13]), $\mathbb{G}_m^3(\overline{\mathbb{C}(t)})$ is the Galois group of the above equation over $\overline{\mathbb{C}(t)}(x)$, where $\mathbb{G}_m$ stands for the multiplicative group. Now let t specialize to $c \in \mathbb{C} \setminus \{0\}$, i.e. consider the $\mathbb{C}$-homomorphism from $\mathbb{C}[t]$ to $\mathbb{C}$ which sends t to c. By van der Put-Singer's method again, one sees that the Galois group of $\sigma(Y) = A(c)Y$ over $\mathbb{C}(x)$ equals $\mathbb{G}_m^3(\mathbb{C})$ if and only if c is neither a root of unity nor an integer. On the other hand, under every specialization, $\mathbb{G}_m^3(\overline{\mathbb{C}(t)})$ specializes to $\mathbb{G}_m^3(\mathbb{C})$ (note that the defining polynomials of $\mathbb{G}_m^3(\overline{\mathbb{C}(t)})$ do not vary under specializations).

This example implies that on the one hand there are infinitely many "good" $c \in \mathbb{C}$ such that the Galois group of $\sigma(Y) = A(c)Y$ over $\mathbb{C}(x)$ is equal to $\mathbb{G}_m^3(\mathbb{C})$, on the other hand the set of these good c is not an open subset of $\mathbb{A}(\mathbb{C})$ in the sense of Zariski topology. Thus we need to introduce other algebraic structures rather than Zariski open sets to describe these good c.

To state our result precisely, let us first recall some notations and basic concepts in difference Galois theory. Throughout this paper, Ω stands for an algebraically closed field of characteristic zero and k denotes a subfield of Ω. $\Omega(x)$ stands for the field of rational functions in x with coefficients in Ω. Over $\Omega(x)$, we can define a shift operator σ as the following: $\sigma(x) = x+1$ and $\sigma(\omega) = \omega$ for all $\omega \in \Omega$. Consider the linear difference equation

$$\sigma(Y) = AY \tag{1}$$

where Y is an n-vector of indeterminates and $A \in \mathrm{GL}_n(\Omega(x))$. Let $X = (X_{i,j})$ be an $n \times n$ matrix of indeterminates and $\Omega(x)[X, 1/\det(X)]$ (resp. $\Omega[X, 1/\det(X)]$) denote the ring over $\Omega(x)$ (resp. Ω) generated by entries of X and $1/\det(X)$. Over $\Omega(x)[X, 1/\det(X)]$, one can extend the automorphism σ by setting $\sigma(X) = AX$ so that $\Omega(x)[X, 1/\det(X)]$ becomes a σ-extension ring of $\Omega(x)$. Let $\mathfrak{m}$ be a maximal σ-ideal of $\Omega(x)[X, 1/\det(X)]$ and let

$$\mathcal{R} = \Omega(x)[X, 1/\det(X)]/\mathfrak{m}.$$

Then $\mathcal{R}$ is the Picard-Vessiot extension ring of $\Omega(x)$ for (1). The Galois group $\mathcal{G}$ of (1) over $\Omega(x)$ is defined to be the set of $\Omega(x)$-automorphisms of $\mathcal{R}$ which commute with σ. Set $\bar{X} = X \mod \mathfrak{m}$. Then $\bar{X}$ is a fundamental matrix of (1), which induces a group homomorphism from $\mathcal{G}$ to $\mathrm{GL}_n(\Omega)$ given by sending $\phi \in \mathcal{G}$ to $\bar{X}^{-1}\phi(\bar{X})$. The image of this homomorphism is an algebraic subgroup of $\mathrm{GL}_n(\Omega)$. Throughout this paper, Galois groups always mean the images of $\mathcal{G}$ under homomorphisms induced by fundamental matrices. One can find more details on difference Galois theory from the standard reference [13].

Let $D \subset \Omega$ be a finitely generated k-algebra. We denote by $\mathrm{Hom}_k(D, \bar{k})$ the set of k-homomorphisms from D to $\bar{k}$, which are what specializations mean in this paper. In Example 1.1, let Γ_1 be the subgroup of $\mathbb{G}_a(\mathbb{C}(t))$ generated by t and 1 where $\mathbb{G}_a$ denotes the additive group, and let Γ_2 be the subgroup of $\mathbb{G}_m(\mathbb{C}(t))$ generated by t. Then the set

$$\{\varphi \in \mathrm{Hom}_{\mathbb{C}}(\mathbb{C}[t, 1/t], \mathbb{C}) \mid \varphi \text{ is injective on } \Gamma_1 \cup \Gamma_2\}$$

consists of good specializations. This motivates the following.

Definition 1.2 *Let Γ be a finitely generated subgroup of $\mathbb{G}_a(\Omega)$ or $\mathbb{G}_m(\Omega)$. Denote*

$$\mathcal{B}(D,\Gamma) = \{\varphi|_D \mid \varphi \in \mathrm{Hom}_k(D[\Gamma], \bar{k}) \text{ that is injective on } \Gamma\}$$

where $D[\Gamma] \subset \Omega$ denotes the D-algebra generated by Γ. A basic open subset of $\mathrm{Hom}_k(D, \bar{k})$ is defined to be the intersection of finitely many subsets of $\mathrm{Hom}_k(D, \bar{k})$ of the form $\mathcal{B}(D,\Gamma)$. When Γ is the subgroup of $\mathbb{G}_a(\Omega)$ generated by a single element $c \in \Omega$, we will abbreviate $\mathcal{B}(D,\Gamma)$ to $\mathcal{B}(D, c)$.

We prove in Corollary 2.18 that basic open subsets of $\mathrm{Hom}_k(D, \bar{k})$ are not empty and moreover they are infinite if D is transcendental over k. We should remark that the set $\mathcal{B}(D,\Gamma)$ given in Definition 1.2 can be seen as a special case of the notion of basic gr-open subsets of $\mathrm{Spec}(D)$ introduced by Hrushovski in [7]. Let G be a commutative algebraic group scheme over D and let Γ be a finitely generated subgroup of $G(D)$. The set of primes $\mathfrak{p} \in \mathrm{Spec}(D)$ satisfying that the canonical map $D \to D/\mathfrak{p}$ is injective on Γ is called a basic gr-open subset of $\mathrm{Spec}(D)$, denoted by $\mathrm{W}(G,\Gamma)$. When $G = \mathbb{G}_a$ or $G = \mathbb{G}_m$, one has that

$$\{\ker(\varphi) \mid \varphi \in \mathcal{B}(D,\Gamma)\} = \mathrm{W}(G,\Gamma) \cap \max(D)$$

where $\max(D)$ denotes the set of maximal ideals of D. In Lemma 5A.10 of [7], Hrushovski proved that if k is a number field and $\mathrm{tr.deg}(F/k) = 1$ where F is the field of fractions of D then $\mathrm{W}(G,\Gamma)$ is infinite. The key idea of his proof is reducing G to the cases that G is an Abelian variety or $\mathbb{G}_m$ or $\mathbb{G}_a$. The case that G is an Abelian variety is due to Néron (see for example Section 6 in Chapter 9 of [8] or Section 11.1 of [11]). The case when $G = \mathbb{G}_a$ was proved in Lemma 5A.4 of [7]. For the case when $G = \mathbb{G}_m$, Hrushovski claimed that one can use an entirely similar argument as that in the proof of Néron's Theorem. Note that in Section 11.1 of [11], Serre also made a similar claim for the case when k is a number field and F is a purely transcendental extension of k. Here to be complete, we shall present a more elementary proof for the case when $G = \mathbb{G}_a$ and provide a detailed proof for the case when $G = \mathbb{G}_m$. Moreover we remove the restrictions on k and D.

We also need the following notations to present our main result. Suppose that $\varphi \in \mathrm{Hom}_k(D, \bar{k})$ and $p \in D[X, 1/\det(X)]$. $\varphi(p)$ stands for the element in $\bar{k}[X, 1/\det(X)]$ obtained by applying φ to the coefficients of p. Let K be a subfield of Ω and $I \subset \Omega[X, 1/\det(X)]$. We use $\mathbb{V}_K(I)$ to denote the set of zeroes of I in $\mathrm{GL}_n(K)$. The main result of this paper is the following theorem.

Theorem 1.3 *Suppose that $S \subset \Omega[X, 1/\det(X)]$ is a finite set satisfying that $\mathbb{V}_\Omega(S)$ is the Galois group of $\sigma(Y) = AY$ over $\Omega(x)$. Let $D \subset \Omega$ be a finitely generated k-algebra with F as field of fractions such that $A \in \mathrm{GL}_n(F(x))$ and $S \subset D[X, 1/\det(X)]$. Then there is a basic open subset U of $\mathrm{Hom}_k(D, \bar{k})$ such that for any $\varphi \in U$, $\mathbb{V}_{\bar{k}}(\varphi(S))$ is the Galois group of $\sigma(Y) = \varphi(A)Y$ over $\bar{k}(x)$.*

This theorem together with Corollary 2.18 answers the question posed at the beginning of this paper affirmatively. Similar to the proof of Proposition 5.1 of [7], the proof of the theorem relies on algorithmic aspects of linear difference equations. The algorithm for computing proto-Galois groups (see Section 3.1 of [3]) and the criterion (see Proposition 5.5) for a proto-Galois group to be a difference Galois group enable us to construct a required basic open subset of $\mathrm{Hom}_k(D, \bar{k})$.

Theorem 1.3 can be applied to van der Put-Singer conjecture concerning the inverse problem in difference Galois theory. Let G be an algebraic subgroup of $\mathrm{GL}_n(\bar{k})$ defined over k. Theorem 1.3 implies that if $G(\Omega)$ is the Galois group of a linear difference equation over $\Omega(x)$ then G is the Galois group of a linear difference equation with coefficients in $\tilde{k}(x)$ where $\tilde{k}$ is a finite field extension of k. This enables us to reduce van der Put-Singer conjecture to the case where the field of constants is the field of complex numbers. Additionally, we want to remind that the specialization technique also plays an important role in realizing a semisimple, simply-connected linear algebraic group defined over $\mathbb{F}_q$ as a Galois group of a Frobenuis difference equation (see [9]).

The rest of this paper is organized as follows. In Section 2, we show that basic open subsets of $\mathrm{Hom}_k(D, \bar{k})$ are not empty, and moreover if D is transcendental over k then they are infinite. In Section 3, we investigate algebraic subgroups of $\mathrm{GL}_n(\Omega)$ under specializations. We prove that the group of characters of a connected algebraic subgroup does not vary under specializations in some basic open subset of $\mathrm{Hom}_k(D, \bar{k})$. In Section 4, we consider σ-ideals in $\Omega(x)[X, 1/\det(X)]$ under specializations. We show that given a ν-maximal σ-ideal I_ν of $\Omega(x)[X, 1/\det(X)]$ (see Definition 4.1), there is a basic open subset of $\mathrm{Hom}_k(D, \bar{k})$ such that each specialization in this set sends I_ν to a ν-maximal σ-ideal of $\bar{k}(x)[X, 1/\det(X)]$. In Section 5, we prove the main result of this paper, i.e. Theorem 1.3. In Section 6, we apply Theorem 1.3 to the inverse problem in difference Galois theory.

Acknowledges: The author would like to thank Michael F. Singer for many valuable conversations. Especially, he suggested considering the arguments in the proof of Theorem 4.4 of [12].

For convenience, let us list frequently used notations below.

Ω	an algebraically closed field of characteristic zero
k, K	subfields of Ω
$\bar{k}$	the algebraic closure of k
$D, \tilde{D}$	finitely generated k-algebras in Ω
$\mathrm{Hom}_k(D, \bar{k})$	the set of k-homomorphisms from D to $\bar{k}$
$\Gamma, \tilde{\Gamma}$	finitely generated subgroups of $\mathbb{G}_a(\Omega)$ or $\mathbb{G}_m(\Omega)$
$\tilde{U}, U, U_1, U_2, \cdots$	basic open subsets of $\mathrm{Hom}_k(D, \bar{k})$ or $\mathrm{Hom}_k(\tilde{D}, \bar{k})$
G	an algebraic subgroup of $\mathrm{GL}_n(\Omega)$
G°	the identity component of G
$X(G)$	the group of characters of G
$G(\Omega(x))$	the set of $\Omega(x)$-points of G
$\mathbf{Z}(f)$	the set of integer zeroes of f
X	$(X_{i,j})$, $n \times n$ matrix with indeterminate entries $X_{i,j}$
S	a finite subset of $\Omega[X, 1/\det(X)]$
$\mathbb{V}_K(S)$	the set of zeroes of S in $\mathrm{GL}_n(K)$
$\langle P \rangle_E$	the ideal in $E[X, 1/\det(X)]$ generated by P, where E is a subfield of $\Omega(x)$

2 Basic open subsets of $\mathrm{Hom}_k(D, \bar{k})$

In this section, we shall show that basic open subsets of $\mathrm{Hom}_k(D, \bar{k})$ are not empty. We start with two properties of basic open sets.

Lemma 2.1 (1) *If D is transcendental over k and every basic open subset of $\mathrm{Hom}_k(D, \bar{k})$ is not empty, then every basic open subset of $\mathrm{Hom}_k(D, \bar{k})$ is infinite.*

(2) *Assume that $\tilde{D}$ is a finitely generated D-algebra in Ω and $\tilde{U}$ is a basic open subset of $\mathrm{Hom}_k(\tilde{D}, \bar{k})$. Then $\{\varphi|_D \mid \varphi \in \tilde{U}\}$ includes a basic open subset of $\mathrm{Hom}_k(D, \bar{k})$.*

Proof. (1) Let U be a basic open subset of $\mathrm{Hom}_k(D, \bar{k})$. Suppose on the contrary that U is finite, say $U = \{\varphi_1, \cdots, \varphi_m\}$. Let $t \in D$ be transcendental over k. Let $f_i(y) \in k[y]$ be the minimal polynomial of $\varphi_i(t)$ over k for all $1 \le i \le m$ and let Γ be the subgroup of $\mathbb{G}_a(D)$ generated by

$$c = f_1(t) f_2(t) \cdots f_m(t) \in D.$$

For all $1 \le i \le m$, $\varphi_i(c) = 0$ and thus $\varphi_i \notin \mathcal{B}(D, \Gamma)$. This implies that $U \cap \mathcal{B}(D, \Gamma) = \emptyset$, which is impossible.

(2) It suffices to show the assertion with $\tilde{U} = \mathcal{B}(\tilde{D}, \Gamma)$, where Γ is a finitely generated subgroup of $\mathbb{G}_a(\Omega)$ or $\mathbb{G}_m(\Omega)$. Assume that $\tilde{D}$ is generated by a finite subset T of $\Omega \setminus \{0\}$ as a D-algebra. Let $\tilde{\Gamma}$ be generated by $\Gamma \cup T$ as a group having the same type as Γ. Then $\tilde{D}[\Gamma] \subset D[\tilde{\Gamma}]$. From the definition, one has that

$$\begin{aligned} &\mathcal{B}(D, \tilde{\Gamma}) = \{\varphi|_D \mid \varphi \in \mathcal{B}(D[\tilde{\Gamma}], \tilde{\Gamma})\}, \\ &\mathcal{B}(\tilde{D}, \Gamma) = \{\varphi|_{\tilde{D}} \mid \varphi \in \mathcal{B}(\tilde{D}[\Gamma], \Gamma)\} \supset \{\varphi|_{\tilde{D}} \mid \varphi \in \mathcal{B}(D[\tilde{\Gamma}], \tilde{\Gamma})\}. \end{aligned}$$

Hence

$$\{\varphi|_D \mid \varphi \in \mathcal{B}(\tilde{D}, \Gamma)\} \supset \{\varphi|_D \mid \varphi \in \mathcal{B}(D[\tilde{\Gamma}], \tilde{\Gamma})\} = \mathcal{B}(D, \tilde{\Gamma}).$$

□

Remark 2.2 *(a) Suppose that $\mathcal{B}(D, \Gamma) \neq \emptyset$. Given a $\varphi \in \mathcal{B}(D, \Gamma)$, there may be more than one elements of $\mathrm{Hom}_k(D[\Gamma], \bar{k})$ which extend φ. The following example shows that there may exist extended homomorphisms which are not injective on Γ. Set $D = k$ and $\Gamma = \mathbb{Z}u$ where u is transcendental over k. Then $\mathcal{B}(k, \Gamma) = \{\mathbf{1}_k\}$ and all elements of $\mathrm{Hom}_k(k[u], \bar{k})$ extend $\mathbf{1}_k$. Let $\psi \in \mathrm{Hom}_k(k[u], \bar{k})$ satisfy that $\psi(u) = 0$. Then ψ is not injective on Γ. On the other hand, one sees that all elements of $\mathrm{Hom}_k(k[u], \bar{k})$ except for ψ are injective on Γ.*

(b) In many cases, we construct a required basic open subset of $\mathrm{Hom}_k(D, \bar{k})$ as follows. First, we construct a basic open subset $\tilde{U}$ in $\mathrm{Hom}_k(\tilde{D}, \bar{k})$ for some finitely generated D-algebra $\tilde{D}$. Second, restrict homomorphisms in $\tilde{U}$ to D, and construct a require basic open subset of $\mathrm{Hom}_k(D, \bar{k})$ inside these restriction homomorphisms. Assume that $\tilde{\Gamma}$ is a finitely generated subgroup of $\mathbb{G}_a(\tilde{D})$. Hrushovski showed in Lemma 5A.1 of [7] that there is a finitely generated subgroup Γ of $\mathbb{G}_a(D)$ satisfying that

$$\mathcal{B}(D, \Gamma) \subset \{\varphi|_D \mid \varphi \in \mathcal{B}(\tilde{D}, \tilde{\Gamma})\}.$$

For a finitely generated subgroup $\tilde{\Gamma}$ of $\mathbb{G}_m(\tilde{D})$, we do not know whether a similar assertion holds. This is why we do not require Γ to be a subset of D in Definition 1.2.

Before proving that each basic open subset of $\mathrm{Hom}_k(D,\bar{k})$ is not empty, let us first prove that $\mathcal{B}(D,\Gamma)\neq\emptyset$. Observe that if $\tilde{D}\subset\Omega$ is a D-algebra then

$$\{\varphi|_D\,|\,\varphi\in\mathcal{B}(\tilde{D},\Gamma)\}\subset\mathcal{B}(D,\Gamma).$$

In particular, $\{\varphi|_D\,|\,\varphi\in\mathcal{B}(D[\Gamma],\Gamma)\}\subset\mathcal{B}(D,\Gamma)$. Hence it suffices to show that $\mathcal{B}(\tilde{D},\Gamma)\neq\emptyset$ for a suitable $\tilde{D}$ with $\Gamma\subset\tilde{D}$. Let F be the field of fractions of D. The case when $\mathrm{tr.deg}(F/k)=0$ is trivial. We suppose that $\mathrm{tr.deg}(F/k)=m>0$ and assume that $\{z_1,\cdots,z_m\}$ is a transcendental basis of F over k. Then $F=k(z_1,\cdots,z_m,\eta)$ where $\eta\in F$ is algebraic over $k(z_1,\cdots,z_m)$. Denote $\mathbf{z}=(z_1,\cdots,z_m)$. There is a nonzero $l(\mathbf{z})\in k[\mathbf{z}]$ such that $D\subset k[\mathbf{z},1/l(\mathbf{z}),\eta]$ and η is integral over $k[\mathbf{z},1/l(\mathbf{z})]$. The above observation implies that we only need to prove that $\mathcal{B}(k[\mathbf{z},1/l(\mathbf{z}),\eta],\Gamma)\neq\emptyset$ with $\Gamma\subset k[\mathbf{z},1/l(\mathbf{z}),\eta]$. Therefore, in this section, D is always supposed to have the form $k[\mathbf{z},1/l(\mathbf{z}),\eta]$ and contain Γ.

We first deal with the case that $k\subset\Omega$ is finitely generated over $\mathbb{Q}$. In this case, k is a hilbertian field (see the page 141 of [4] or Section 1.1 of [14] for the definition).

Notation 2.3 *Let $\mathbf{f}$ be a finite set of irreducible polynomials in $k[\mathbf{z},y]\setminus k[\mathbf{z}]$ and let g be a nonzero element in $k[\mathbf{z}]$. Let d be a positive integer. $\mathcal{H}_D(d,\mathbf{f},g)$ stands for the set of elements in $\mathrm{Hom}_k(D,\bar{k})$ satisfying that*

(1) *$\varphi(g)\neq 0$;*

(2) *for $1\le i\le m$, $[k(\varphi(z_1),\cdots,\varphi(z_i)):k]=d^i$;*

(3) *for every $f\in\mathbf{f}$, $\varphi(f(\mathbf{z},y))$ is not in $k(\varphi(\mathbf{z}))$ and is irreducible over $k(\varphi(\mathbf{z}))$.*

We first show that $\mathcal{H}_D(d,\mathbf{f},g)$ is not empty.

Lemma 2.4 *Assume that $\tilde{k}$ is a finite extension of k. For any positive integer d, there is $\alpha\in\bar{k}$ with $[k(\alpha):k]=[\tilde{k}(\alpha):\tilde{k}]=d$.*

Proof. Consider the polynomial $y^d-t\in k[y,t]$ which is irreducible over $\tilde{k}$. Since k is hilbertian, there is $c\in k$ such that y^d-c is irreducible in $\tilde{k}[y]$ by Corollary 1.8 of [14]. Let $\alpha\in\bar{k}$ satisfy that $\alpha^d-c=0$. □

Proposition 2.5 *$\mathcal{H}_D(d,\mathbf{f},g)\neq\emptyset$.*

Proof. Let $\tilde{k}\subset\bar{k}$ be a finite extension of k such that for every $f\in\mathbf{f}$, all irreducible factors of f in $\tilde{k}[\mathbf{z},y]$ are absolutely irreducible. By Lemma 2.4, there are $a_1,\cdots,a_m\in\bar{k}$ such that for $1\le i\le m$,

$$[k(a_1,\cdots,a_i):k(a_1,\cdots,a_{i-1})]=[\tilde{k}(a_1,\cdots,a_i):\tilde{k}(a_1,\cdots,a_{i-1})]=d.$$

It is easy to verify that $[k(a_1,\cdots,a_i):k]=d^i$ for all $1\le i\le m$ and $k(\mathbf{a})\cap\tilde{k}=k$ where $\mathbf{a}=(a_1,\cdots,a_m)$. We claim that every element of $\mathbf{f}$ is irreducible over $k(\mathbf{a})$. Otherwise, let $f\in\mathbf{f}$ be reducible over $k(\mathbf{a})$. Suppose that $\bar{f}$ is an irreducible factor of f in $k(\mathbf{a})[\mathbf{z},y]$. Then there is $\lambda\in\bar{k}$ such that $\lambda\bar{f}\in\tilde{k}[\mathbf{z},y]$ by the assumption on $\tilde{k}$. Since f is irreducible over k, there are two nonzero coefficients of $\bar{f}$, say a,b, satisfying that $a/b\notin k$. While $a/b\in k(\mathbf{a})\cap\tilde{k}$. This implies that $k(\mathbf{a})\cap\tilde{k}\neq k$, a contradiction. This proves our claim. The claim implies that for each $f \in \mathbf{f}$, $f(\mathbf{z}+\mathbf{a}, y)$ is irreducible over $k(\mathbf{a})$. Due to Lemma 11.6 in the page 144 of [4], the set of $\mathbf{c} \in k^m$ such that $f(\mathbf{c}+\mathbf{a}, y)$ is irreducible in $k(\mathbf{a})[y]$ for all $f \in \mathbf{f}$ contains a hilbertian subset of k^m and thus it is Zariski dense in k^m. Therefore there is $\bar{\mathbf{c}} \in k^m$ such that $f(\bar{\mathbf{c}}+\mathbf{a}, y)$ is irreducible in $k(\mathbf{a})[y]$ for all $f \in \mathbf{f}$ and $l(\bar{\mathbf{c}}+\mathbf{a})g(\bar{\mathbf{c}}+\mathbf{a})\bar{g}(\bar{\mathbf{c}}+\mathbf{a}) \neq 0$, where $\bar{g}(\mathbf{z})$ is the product of the leading coefficients of all $f \in \mathbf{f}$ viewed as polynomials in y. Let $\varphi \in \mathrm{Hom}_k(k[\mathbf{z}], \bar{k})$ be such that $\varphi(\mathbf{z}) = \bar{\mathbf{c}}+\mathbf{a}$. Then φ can be extended to an element in $\mathrm{Hom}_k(D, \bar{k})$ and this element belongs to $\mathcal{H}_D(d, \mathbf{f}, g)$. $\square$

Remark 2.6 (1) *When $d=1$ and $D=k[\mathbf{z}]$, $\mathcal{H}_D(d,\mathbf{f},g)$ is a usual hilbertian subset of k^m. Here we identity k^m with $\mathrm{Hom}_k(k[\mathbf{z}],k)$.*

(2) *By the above proposition and an argument similar to that in the proof of Lemma 2.1, one sees that when D is transcendental over k, $\mathcal{H}_D(d,\mathbf{f},g)$ is infinite.*

(3) *One sees that $\mathcal{H}_D(d_1,\mathbf{f}_1,g_1) \cap \mathcal{H}_D(d_2,\mathbf{f}_2,g_2) \neq \emptyset$ if and only if $d_1 = d_2$.*

Lemma 2.7 *Let $f \in F[y]$ be irreducible over F where F is the field of fractions of D and let $b \in D$ be nonzero. Then there is an irreducible polynomial $h(\mathbf{z},y) \in k[\mathbf{z},y]$ and a nonzero $g \in k[\mathbf{z}]$ such that for any positive integer d and any $\varphi \in \mathcal{H}_D(d,h,g)$, one has that*

(1) *$\varphi(f)$ is well-defined and is irreducible over the field of fractions of $\varphi(D)$;*

(2) *$\deg_y(f) = \deg_y(\varphi(f))$;*

(3) *$\varphi(b) \neq 0$.*

Proof. Recall that D is of the form $k[\mathbf{z}, 1/l(\mathbf{z}), \eta]$. Let α be a zero of $f(y)$ in $\overline{k(\mathbf{z})}$ and let $w \in \overline{k(\mathbf{z})}$ be such that $k(\mathbf{z},w) = k(\mathbf{z},\eta,\alpha)$. There are nonzero $q_1, q_2 \in k[\mathbf{z}]$ such that

$$D[\alpha] \subset k[\mathbf{z}, 1/q_1, w] \text{ and } w \in k[\mathbf{z}, 1/q_2, \eta, \alpha].$$

Let $h \in k[\mathbf{z},y]$ be an irreducible polynomial satisfying that $h(\mathbf{z},w)=0$. Let q_3 be the leading coefficient of h viewed as a polynomial in y and let q_4 be an element in $k[\mathbf{z}]$ such that $f \in k[\mathbf{z}, 1/q_4, \eta, y]$. Write the norm of $b\tilde{g}$ (down to $k(\mathbf{z})$) in the form $g_1(\mathbf{z})/g_2(\mathbf{z})$ where $\tilde{g}$ is the leading coefficient of f and $g_1, g_2 \in k[\mathbf{z}]$. Set $g = q_1q_2q_3q_4g_1g_2$. Assume that d is a positive integer and $\varphi \in \mathcal{H}_D(d,h,g)$. Then φ can be extended to an element $\psi \in \mathrm{Hom}_k(k[\mathbf{z},1/g,w], \bar{k})$, because w is integral over $k[\mathbf{z},1/g]$. Obviously, $\varphi(b) = \psi(b) \neq 0$. We shall show that $\psi(f)$ is irreducible over $k(\psi(\mathbf{z}),\psi(\eta))$, the field of fractions of $\psi(D)$ and $\deg_y(f) = \deg_y(\psi(f))$. One sees that $k(\psi(\mathbf{z}),\psi(w)) \subset k(\psi(\mathbf{z}),\psi(\eta),\psi(\alpha))$ and

$$\begin{aligned}\deg_y(\psi(h)) &= [k(\psi(\mathbf{z}),\psi(w)) : k(\psi(\mathbf{z}))] \leq [k(\psi(\mathbf{z}),\psi(\eta),\psi(\alpha)) : k(\psi(\mathbf{z}))]\\ &= [k(\psi(\mathbf{z}),\psi(\eta),\psi(\alpha)) : k(\psi(\mathbf{z}),\psi(\eta))][k(\psi(\mathbf{z}),\psi(\eta)) : k(\psi(\mathbf{z}))]\\ &\leq [k(\mathbf{z},\eta,\alpha) : k(\mathbf{z},\eta)][k(\mathbf{z},\eta) : k(\mathbf{z})] = \deg_y(h).\end{aligned}$$

The nonvanishing of $\psi(q_3)$ implies that $\deg_y(\psi(h)) = \deg_y(h)$. Hence

$$[k(\psi(\mathbf{z}),\psi(\eta),\psi(\alpha)) : k(\psi(\mathbf{z}),\psi(\eta))] = [k(\mathbf{z},\eta,\alpha) : k(\mathbf{z},\eta)].$$

This implies that $\psi(f)$ is irreducible over the field of fractions of $\psi(D)$ and $\deg_y(f) = \deg_y(\psi(f))$. Now the lemma follows from the fact that $\psi(f) = \varphi(f)$ and $\psi(D) = \varphi(D)$. $\square$

Corollary 2.8 *Let f be a polynomial in $F[y]$ where F is the field of fractions of D. Then there is a finite set $\mathbf{h}$ of irreducible polynomials in $k[\mathbf{z}, y]$ and a nonzero $g \in k[\mathbf{z}]$ such that for any $d > 0$ and any $\varphi \in \mathcal{H}_D(d, \mathbf{h}, g)$, $\varphi(f) = 0$ has a root in the field of fractions of $\varphi(D)$ if and only if $f = 0$ has a root in F.*

Proof. Decompose f into irreducible polynomials in $F[y]$, say $f_1, f_2, \cdots, f_m$. By Lemma 2.7, there is a finite set $\mathbf{h}$ of irreducible polynomials in $k[\mathbf{z}, y]$ and a nonzero $g \in k[\mathbf{z}]$ such that for any $d > 0$ and any $\varphi \in \mathcal{H}_D(d, \mathbf{h}, g)$, $\varphi(f_i)$ is irreducible over the field of fractions of $\varphi(D)$ and $\deg_y(f_i) = \deg_y(\varphi(f_i))$ for all $1 \leq i \leq m$. Let $\varphi \in \mathcal{H}_D(d, \mathbf{h}, g)$. Corollary then follows from the fact that $\varphi(f) = 0$ (resp. $f = 0$) has a root in the field of fractions of $\varphi(D)$ (resp. F) if and only if some of $\{\varphi(f_1), \cdots, \varphi(f_m)\}$ (resp. $\{f_1, \cdots, f_m\}$) are of degree one. $\square$

Proposition 2.9 *Suppose that Γ is a finitely generated subgroup of $\mathbb{G}_a(D)$. Then there is an irreducible polynomial $f \in k[\mathbf{z}, y]$, a nonzero $g \in k[\mathbf{z}]$ and $e > 0$ such that for any $d > e$, $\mathcal{H}_D(d, f, g) \subset \mathcal{B}(D, \Gamma)$.*

Proof. If $\Gamma = \{0\}$ then there is nothing to prove. Assume that $\Gamma \neq \{0\}$. Recall that D is of the form $k[\mathbf{z}, 1/l(\mathbf{z}), \eta]$. Let f be an irreducible polynomial in $k[\mathbf{z}, y]$ such that $f(\mathbf{z}, \eta) = 0$. Note that Γ is torsion-free. Thus Γ is free. Assume that $\{w_1, w_2, \cdots, w_N\}$ is a basis of Γ. Denote $\ell = \deg_y(f)$. Then there are $p_{i,j}(\mathbf{z}) \in k[\mathbf{z}]$ with $1 \leq i \leq N, 0 \leq j \leq \ell - 1$ and a nonnegative integer ν such that for all $1 \leq i \leq N$,

$$w_i = \frac{\sum_{j=0}^{\ell-1} p_{i,j}(\mathbf{z})\eta^j}{l(\mathbf{z})^\nu}. \tag{2}$$

Now set

$$e = \max_{1 \leq i \leq N, 0 \leq j \leq \ell-1}\{\deg(p_{i,j}(\mathbf{z}))\}.$$

Let $d \in \mathbb{Z}$ with $d > e$ and $g = \mathrm{lc}(f)l$ where $\mathrm{lc}(f)$ is the leading coefficient of f in y. Suppose that $\varphi \in \mathcal{H}_D(d, f, g)$. We shall prove that $\varphi(w_1), \cdots, \varphi(w_N)$ are linearly independent over $\mathbb{Z}$. Assume that there are $c_1, \cdots, c_N \in \mathbb{Z}$ such that

$$c_1\varphi(w_1) + \cdots + c_N\varphi(w_N) = 0.$$

Substituting (2) to the above equality and multiplying both sides by $l(\varphi(\mathbf{z}))^\nu$, one obtains that

$$\sum_{j=0}^{\ell-l}\left(\sum_{i=1}^{N} c_i p_{i,j}(\varphi(\mathbf{z}))\right)\varphi(\eta)^j = 0.$$

Note that $\varphi(\mathrm{lc}(f)) \neq 0$, which implies that

$$[k(\varphi(\mathbf{z}), \varphi(\eta)) : k(\varphi(\mathbf{z}))] = \deg_y(f(\varphi(\mathbf{z}), y)) = \ell.$$

One then has that for all $0 \leq j \leq \ell - 1$,

$$\sum_{i=1}^{N} c_i p_{i,j}(\varphi(\mathbf{z})) = 0.$$

From the definition of $\mathcal{H}_D(d, f, g)$, one sees that

$$\varphi(z_1)^{i_1}\varphi(z_2)^{i_2}\cdots\varphi(z_m)^{i_m}, 0 \leq i_1, \cdots, i_m \leq d-1$$

are linearly independent over k. Hence for all $0 \leq j \leq \ell - 1$,

$$\sum_{i=1}^{N} c_i p_{i,j}(\mathbf{z}) = 0.$$

Equivalently, $\sum_{i=1}^{N} c_i w_i = 0$. Since $w_1, \cdots, w_N$ are linearly independent over $\mathbb{Z}$, $c_i = 0$ for all $1 \leq i \leq N$, Hence $\varphi(w_1), \cdots, \varphi(w_N)$ are linearly independent over $\mathbb{Z}$. This implies that $\varphi \in \mathcal{B}(D, \Gamma)$. $\square$

Remark 2.10 (1) *One sees that Proposition 2.9 remains true if we take $\Gamma \subset D$ to be a k-vector space of finite dimension.*

(2) *In Lemma 5A.4 of [7], Hrushovski proved that when k is neither real closed nor algebraically closed, there is $\varphi \in \mathrm{Hom}_k(D, \bar{k})$ such that φ is injective on V where $V \subset D^l$ is a finite dimensional k-vector space. His proof applied Artin-Schreier theory. Our proof of Proposition 2.9 seems elementary.*

Next, we are going to deal with the case that Γ is a finitely generated subgroup of $\mathbb{G}_m(D)$. It has been claimed in the page 154 of [11] and in Discussion 5A.8 (4) of [7] that the proof of Néron's theorem can be applied to proving that $\mathcal{B}(D, \Gamma) \neq \emptyset$. The readers are referred to Section 6 in Chapter 9 of [8] or Section 11.1 of [11] for the proof of Néron's theorem. Following that proof, we present a detailed proof of the claim made by Hrushovski and Serre. Let $K \subset \Omega$ be a subfield.

Definition 2.11 *Suppose Γ is a subgroup of $\mathbb{G}_m(K)$. The radical of Γ in K, denoted by $\mathrm{rad}_K(\Gamma)$, is defined to be*

$$\{\alpha \in \mathbb{G}_m(K) \mid \exists\, l > 0 \ s.t.\ \alpha^l \in \Gamma\}.$$

We say Γ is radical in K if $\Gamma = \mathrm{rad}_K(\Gamma)$.

It is easy to see that $\mathrm{rad}_K(\Gamma)$ is also a subgroup of $\mathbb{G}_m(K)$. We shall show that if K is a field finitely generated over $\mathbb{Q}$ and Γ is finitely generated then $\mathrm{rad}_K(\Gamma)$ is also finitely generated. We first prove the case where K is a number field.

Lemma 2.12 *Let K be a number field and Γ be a finitely generated subgroup of $\mathbb{G}_m(K)$. Then $\mathrm{rad}_K(\Gamma)$ is also finitely generated.*

Proof. Assume that $a_1, \cdots, a_m$ are generators of Γ. Let $\mathfrak{p}_1, \cdots, \mathfrak{p}_\ell$ be all prime ideals of $\mathcal{O}_K$ satisfying that for each $1 \leq i \leq \ell$, $\mathrm{ord}_{\mathfrak{p}_i}(a_j) \neq 0$ for some $1 \leq j \leq m$, where $\mathrm{ord}_{\mathfrak{p}_i}(a_j)$ denotes the order of a_j at $\mathfrak{p}_i$. Consider the group homomorphism $\varphi : \mathrm{rad}_K(\Gamma) \to \mathbb{Z}^\ell$ defined by

$$\varphi(\alpha) = (\mathrm{ord}_{\mathfrak{p}_1}(\alpha), \cdots, \mathrm{ord}_{\mathfrak{p}_\ell}(\alpha)).$$

One can easily verify that $\ker(\varphi) = \mathrm{rad}_K(\Gamma) \cap \mathcal{O}_K^\times$. So it is finitely generated, because $\mathcal{O}_K^\times$ is finitely generated. The image of φ is also finitely generated, as it is a subgroup of $\mathbb{Z}^\ell$. Hence $\mathrm{rad}_K(\Gamma)$ is finitely generated. $\square$

Using an argument similar to the above, one can show the following proposition.

Proposition 2.13 *Let K be a field finitely generated over $\mathbb{Q}$ and Γ be a finitely generated subgroup of $\mathbb{G}_m(K)$. Then $\mathrm{rad}_K(\Gamma)$ is also finitely generated.*

Proof. Assume that $a_1, \cdots, a_m$ are generators of Γ. By Lemma 2.12, we only need to prove the case that K is transcendental over $\mathbb{Q}$. Due to the results in the page 99 of [15], there is a set $S^\star$ of prime divisors of $K/\mathbb{Q}$ such that for any $b \in K$ if $\mathrm{ord}_{\mathfrak{p}}(b) \geq 0$ for all $\mathfrak{p} \in S^\star$ then b is algebraic over $\mathbb{Q}$. Let $\mathfrak{p}_1, \cdots, \mathfrak{p}_\ell$ be all elements in $S^\star$ satisfying that for each $1 \leq i \leq \ell$, $\mathrm{ord}_{\mathfrak{p}_i}(a_j) \neq 0$ for some $1 \leq j \leq m$, where $\mathrm{ord}_{\mathfrak{p}_i}(a_j)$ denotes the order of a_j at $\mathfrak{p}_i$. Consider the group homomorphism $\varphi : \mathrm{rad}_K(\Gamma) \to \mathbb{Z}^\ell$ defined by

$$\varphi(\alpha) = (\mathrm{ord}_{\mathfrak{p}_1}(\alpha), \cdots, \mathrm{ord}_{\mathfrak{p}_\ell}(\alpha)).$$

One can verify that $\ker(\varphi) = \tilde{\mathbb{Q}} \cap \mathrm{rad}_K(\Gamma)$ where $\tilde{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$ in K. The image of φ is a subgroup of $\mathbb{Z}^\ell$ and so it is finitely generated. Therefore to show that $\mathrm{rad}_K(\Gamma)$ is finitely generated, if suffices to show that $\ker(\varphi)$ is finitely generated. Let $R = \tilde{\mathbb{Q}}[a_1, 1/a_1, \cdots, a_m, 1/a_m]$ and let $\phi \in \mathrm{Hom}_{\tilde{\mathbb{Q}}}(R, \bar{\mathbb{Q}})$. Then $\phi(a_i) \neq 0$ for all $1 \leq i \leq m$. Let $\tilde{\Gamma}$ be the subgroup of $\mathbb{G}_m(\bar{\mathbb{Q}})$ generated by $\phi(a_1), \cdots, \phi(a_m)$ and let $E = \tilde{\mathbb{Q}}(\phi(a_1), \cdots, \phi(a_m))$. Then $\tilde{\Gamma} = \phi(\Gamma)$ and E is a number field. Suppose that $\gamma \in \ker(\varphi)$, i.e.$\gamma \in \tilde{\mathbb{Q}}$ and $\gamma^d \in \Gamma$ for some $d > 0$. Applying ϕ to γ yields that

$$\gamma^d = \phi(\gamma)^d \in \tilde{\Gamma}.$$

This implies that $\gamma \in \mathrm{rad}_E(\tilde{\Gamma})$ and thus $\ker(\varphi) \subset \mathrm{rad}_E(\tilde{\Gamma})$. Lemma 2.12 implies that $\mathrm{rad}_E(\tilde{\Gamma})$ is finitely generated. So $\ker(\varphi)$ is finitely generated. $\Box$

The example below shows that if K is not finitely generated over $\mathbb{Q}$ then $\mathrm{rad}_K(\Gamma)$ may not be finitely generated.

Example 2.14 *Let $K = \mathbb{Q}(\eta_2, \eta_3, \cdots)$ where η_i is a primitive i-th root of unity, and let $\Gamma = \{1\}$. Then $\mathrm{rad}_K(\Gamma)$ contains all η_i, and thus it is not finitely generated.*

Suppose that ℓ is a positive integer and Γ is a subgroup of $\mathbb{G}_m(D)$. Denote

$$\Gamma_\ell = \{\gamma \in \Gamma | \gamma^\ell = 1\}.$$

Lemma 2.15 *Suppose that Γ is a finitely generated subgroup of $\mathbb{G}_m(D)$ and Γ is radical in F where F is the field of fractions of D. Let ℓ be a positive integer. Then there exists a finite set $\mathbf{f}$ of irreducible polynomials in $k[\mathbf{z}, y]$ and a nonzero $g \in k[\mathbf{z}]$ such that for any $d > 0$ and $\varphi \in \mathcal{H}_D(d, \mathbf{f}, g)$, $\varphi(\Gamma)$ is a finitely generated subgroup of $\mathbb{G}_m(\varphi(D))$ and $\varphi(\Gamma_\ell) = \varphi(\Gamma)_\ell$.*

Proof. Let h be a monic polynomial in $F[y]$ such that

$$h \prod_{c \in \Gamma_\ell} (y - c) = y^\ell - 1.$$

Then $h = 0$ has no roots in F, because Γ is radical in F. By Corollary 2.8, there exists a finite set $\mathbf{f}$ of irreducible polynomials in $k[\mathbf{z}, y]$ and a nonzero

$\bar{g} \in k[\mathbf{z}]$ such that for any $d > 0$ and $\varphi \in \mathcal{H}_D(d, \mathbf{f}, \bar{g})$, $\varphi(h) = 0$ has no roots in the field of fractions of $\varphi(D)$. Suppose that $a_1, \cdots, a_N$ are generators of Γ. For each $i = 1, \cdots, N$, denote by s_i/r the norm of a_i (down to $k(\mathbf{z})$), where $r, s_i \in k[\mathbf{z}]$. Set $g = \bar{g} r s_1 \cdots s_N$. Suppose that $\varphi \in \mathcal{H}_D(d, \mathbf{f}, g)$. Then $\varphi(a_i) \neq 0$ for all $1 \leq i \leq N$ and $\varphi(h) = 0$ has no roots in the field of fractions of $\varphi(D)$. Hence $\varphi(\Gamma)$ is a finitely generated subgroup of $\mathbb{G}_m(\varphi(D))$, and furthermore since $y^\ell - 1 = \varphi(h) \prod_{c \in \Gamma_\ell}(y - \varphi(c))$, one has that $\varphi(\Gamma)_\ell = \{\varphi(c) | c \in \Gamma_\ell\}$. □

Proposition 2.16 *Suppose that Γ is a finitely generated subgroup of $\mathbb{G}_m(D)$. There exists a set $\mathbf{f}$ of irreducible polynomials in $k[\mathbf{z}, y]$ and a nonzero $g \in k[\mathbf{z}]$ such that for any $d > 0$, $\mathcal{H}_D(d, \mathbf{f}, g) \subset \mathcal{B}(D, \Gamma)$.*

Proof. Denote by F the field of fractions of D. Set $\tilde{\Gamma} = \mathrm{rad}_F(\Gamma)$. Then by Proposition 2.13, $\tilde{\Gamma}$ is finitely generated. Assume that $a_1, \cdots, a_N$ are generators of $\tilde{\Gamma}$. Let $\tilde{D} = D[a_1, 1/a_1, \cdots, a_N, 1/a_N]$. We first show that there is a set $\mathbf{f}$ of irreducible polynomials in $k[\mathbf{z}, y]$ and a nonzero $g \in k[\mathbf{z}]$ such that for any $d > 0$, $\mathcal{H}_{\tilde{D}}(d, \mathbf{f}, g) \subset \mathcal{B}(\tilde{D}, \tilde{\Gamma})$.

Let T be the torsion group of $\tilde{\Gamma}$ and $\ell = |T|$. By Lemma 2.15, there exists a finite set $\mathbf{f}_1$ of irreducible polynomials in $k[\mathbf{z}, y]$ and a nonzero $g_1 \in k[\mathbf{z}]$ such that for any $d > 0$ and $\varphi \in \mathcal{H}_{\tilde{D}}(d, \mathbf{f}_1, g)$, $\varphi(\tilde{\Gamma})$ is a finitely generated subgroup of $\mathbb{G}_m(\varphi(\tilde{D}))$ and $\varphi(\tilde{\Gamma}_\ell) = \varphi(\tilde{\Gamma})_\ell$. Suppose that $\{b_1 = 1, b_2, \cdots, b_\nu\}$ is a set of representatives of $\tilde{\Gamma}/\tilde{\Gamma}^\ell$. Note that F is the field of fractions of $\tilde{D}$. Corollary 2.8 implies that there exist a finite set $\mathbf{f}_2$ of irreducible polynomials in $k[\mathbf{z}, y]$ and a nonzero $g_2 \in k[\mathbf{z}]$ such that for any $d > 0$ and any $\varphi \in \mathcal{H}_{\tilde{D}}(d, \mathbf{f}_2, g_2)$, $y^\ell - \varphi(b_i) = 0$ has a root in the field of fractions of $\varphi(\tilde{D})$ if and only if $y^\ell - b_i = 0$ has a root in F. Since $\tilde{\Gamma}$ is radical in F, all roots of $y^\ell - b_i = 0$ in F are in $\tilde{\Gamma}$. Thus for each $\varphi \in \mathcal{H}_{\tilde{D}}(d, \mathbf{f}_2, g_2)$, $y^\ell - \varphi(b_i) = 0$ has a root in the field of fractions of $\varphi(\tilde{D})$ only if $i = 1$. Now set $\mathbf{f} = \mathbf{f}_1 \cup \mathbf{f}_2$ and $g = g_1 g_2$. We claim that for any $d > 0$, $\mathcal{H}_{\tilde{D}}(d, \mathbf{f}, g) \subset \mathcal{B}(\tilde{D}, \tilde{\Gamma})$. Suppose that $\varphi \in \mathcal{H}_{\tilde{D}}(d, \mathbf{f}, g)$. Let $I = \varphi^{-1}(1) \cap \tilde{\Gamma}$. Then I is a finitely generated subgroup of $\tilde{\Gamma}$. We shall show that $I = I^\ell$ and I is free. This will imply $I = 1$ and then $\varphi \in \mathcal{B}(\tilde{D}, \tilde{\Gamma})$. Since $\ell = |T|$, it follows from $I = I^\ell$ that I is torsion-free and then it is free. So we only need to prove that $I = I^\ell$. Suppose $w \in I$. Write $w = b_i \bar{w}^\ell$ for some i and some $\bar{w} \in \tilde{\Gamma}$. Then $\varphi(\bar{w}^{-1})^\ell = \varphi(b_i)$. The assumption on φ indicates that $b_i = 1$. This implies $w = \bar{w}^\ell$ and then $\varphi(\bar{w})^\ell = 1$, i.e. $\varphi(\bar{w}) \in \varphi(\tilde{\Gamma})_\ell$. As $\varphi(\tilde{\Gamma}_\ell) = \varphi(\tilde{\Gamma})_\ell$, there is $v \in \tilde{\Gamma}_\ell$ such that $\varphi(\bar{w}) = \varphi(v)$. In other words, $\bar{w} v^{-1} \in I$. While $v^\ell = 1$, $w = \bar{w}^\ell = (\bar{w} v^{-1})^\ell \in I^\ell$. Therefore $I = I^\ell$. This proves our claim.

One sees that $\tilde{D}$ is integral over D, because $a_i^l \in \Gamma \subset D$ for some $l > 0$. Hence every $\varphi \in \mathrm{Hom}_k(D, \bar{k})$ can be extended to an element in $\mathrm{Hom}_k(\tilde{D}, \bar{k})$. It follows that any $\varphi \in \mathcal{H}_D(d, \mathbf{f}, g)$ can be extended to an element in $\mathcal{H}_{\tilde{D}}(d, \mathbf{f}, g)$. Therefore for any $d > 0$,

$$\mathcal{H}_D(d, \mathbf{f}, g) = \{\tilde{\varphi}|_D \mid \tilde{\varphi} \in \mathcal{H}_{\tilde{D}}(d, \mathbf{f}, g)\} \subset \{\tilde{\varphi}|_D \mid \tilde{\varphi} \in \mathcal{B}(\tilde{D}, \tilde{\Gamma})\} \subset \mathcal{B}(D, \Gamma).$$

□

Theorem 2.17 *Assume that $k \subset \Omega$ is a field finitely generated over $\mathbb{Q}$ and $D \subset \Omega$ is a finitely generated k-algebra. Then any basic open subset of $\mathrm{Hom}_k(D, \bar{k})$ is nonempty. In particular, when D is transcendental over k, any basic open subset of $\mathrm{Hom}_k(D, \bar{k})$ is infinite.*

Proof. Suppose that U is a basic open subset of $\mathrm{Hom}_k(D,\bar{k})$. Write $U=\cap_{i=1}^m \mathcal{B}(D,\Gamma_i)$. Without loss of generality, we may assume that $\Gamma_1,\cdots,\Gamma_l$ are finitely generated subgroups of $\mathbb{G}_a(D)$ and $\Gamma_{l+1},\cdots,\Gamma_m$ are finitely generated subgroups of $\mathbb{G}_m(D)$. Due to Proposition 2.9, for each $i=1,\cdots,l$, there is an irreducible polynomial f_i in $k[\mathbf{z},y]$, a nonzero $g_i\in k[\mathbf{z}]$ and $e_i>0$ such that for any $d>e_i$, $\mathcal{H}_D(d,f_i,g_i)\subset\mathcal{B}(D,\Gamma_i)$. By Proposition 2.16, for each $j=1,\cdots,m-l$, there is a finite set $\mathbf{h}_j$ of irreducible polynomials in $k[\mathbf{z},y]$ and a nonzero $g_{j+l}\in k[\mathbf{z}]$ such that for any $d>0$, $\mathcal{H}_D(d,\mathbf{h}_j,g_{j+l})\subset\mathcal{B}(D,\Gamma_{j+l})$. Set

$$\mathbf{f}=\{f_1,\cdots,f_l\}\cup\mathbf{h}_1\cup\cdots\cup\mathbf{h}_{m-l}\text{ and }g=g_1g_2\cdots g_m.$$

Then for any $d>\max\{e_1,\cdots,e_l\}$, $\mathcal{H}_D(d,\mathbf{f},g)\subset U$. This proves the first assertion. The second assertion follows from Lemma 2.1. □

Corollary 2.18 *Suppose that $k\subset\Omega$ is a field and $D\subset\Omega$ is a finitely generated k-algebra. Then any basic open subset of $\mathrm{Hom}_k(D,\bar{k})$ is nonempty. In particular, when D is transcendental over k, any basic open subset of $\mathrm{Hom}_k(D,\bar{k})$ is infinite.*

Proof. Suppose that U is a basic open subset of $\mathrm{Hom}_k(D,\bar{k})$. Write $U=\cap_{i=1}^m\mathcal{B}(D,\Gamma_i)$. Note that D is of the form $k[\mathbf{z},1/l(\mathbf{z}),\eta]$. Let f be an irreducible polynomial in $k[\mathbf{z},y]$ such that $f(\mathbf{z},\eta)=0$. Let $\tilde{k}\subset k$ be a field finitely generated over $\mathbb{Q}$ such that $f,l(\mathbf{z})\in\tilde{k}[\mathbf{z},y]$ and $\Gamma_i\subset\tilde{k}[\mathbf{z},1/l(\mathbf{z}),\eta]$ for all $1\le i\le m$. One sees that every $\varphi\in\mathrm{Hom}_{\tilde{k}}(\tilde{k}[\mathbf{z},1/l(\mathbf{z}),\eta],\bar{k})$ can be extended to an element of $\mathrm{Hom}_k(D,\bar{k})$. The corollary then follows from Theorem 2.17. □

The following two lemmas will be used later.

Lemma 2.19 *Suppose that $f\in D[y]$. There is a finitely generated subgroup Γ of $\mathbb{G}_a(\Omega)$ such that for any $\varphi\in\mathcal{B}(D,\Gamma)$, one has that $\mathbf{Z}(f)=\mathbf{Z}(\varphi(f))$.*

Proof. Let $\alpha_1,\cdots,\alpha_\ell$ be all zeroes of f in $\Omega\backslash\mathbb{Z}$ and a be the leading coefficient of f. Set Γ to be the subgroup of $\mathbb{G}_a(\Omega)$ generated by $1,a,\alpha_1,\cdots,\alpha_\ell$ and set $\tilde{D}$ to be the extension of D generated by $\alpha_1,\cdots,\alpha_\ell$. Suppose that $\varphi\in\mathcal{B}(D,\Gamma)$. By the definition of basic open subsets, φ can be extended to an element $\psi\in\mathrm{Hom}_k(\tilde{D},\bar{k})$ such that ψ is injective on Γ. One sees that $\psi(\alpha_i)\notin\mathbb{Z}$ for all $1\le i\le\ell$ and then $\mathbf{Z}(f)=\mathbf{Z}(\psi(f))=\mathbf{Z}(\varphi(f))$. □

Lemma 2.20 *Assume that M is a matrix in $D^{l\times m}$. Then there is a nonzero $c\in D$ such that for any $\varphi\in\mathcal{B}(D,c)$, $\mathrm{rank}(M)=\mathrm{rank}(\varphi(M))$.*

Proof. Clearly, $\mathrm{rank}(\varphi(M))\le\mathrm{rank}(M)$ for all $\varphi\in\mathrm{Hom}_k(D,\bar{k})$. Let $r=\mathrm{rank}(M)$. If $r=0$, there is nothing to prove. Suppose that $r>0$ and c is a nonzero $r\times r$ minors of M. Suppose $\varphi\in\mathcal{B}(D,c)$. It is easy to see that $\varphi(c)$ is a $r\times r$ minor of $\varphi(M)$. So $\mathrm{rank}(\varphi(M))\ge r$. This implies that $r=\mathrm{rank}(\varphi(M))$. □

3 Algebraic groups under specialization

Throughout this section, G denotes an algebraic subgroup of $\mathrm{GL}_n(\Omega)$ and $S\subset\Omega[X,1/\det(X)]$ stands for a finite set such that $\mathbb{V}_\Omega(S)=G$. Recall that $\mathbb{V}_\Omega(S)$

denotes the set of zeroes of S in $\mathrm{GL}_n(\Omega)$. Let $D \subset \Omega$ be a finitely generated k-algebra such that $S \subset D[X, 1/\det(X)]$. We shall investigate $\mathbb{V}_{\bar{k}}(\varphi(S))$ for φ in a basic open subset of $\mathrm{Hom}_k(D, \bar{k})$.

Lemma 3.1 *Let F be the field of fractions of D. Assume that S_1 and S_2 are two finite subsets of $F(x)[X, 1/\det(X)]$ (resp. $F[X, 1/\det(X)]$) such that $S_1 \subset \langle S_2 \rangle_{\Omega(x)}$ (resp. $S_1 \subset \langle S_2 \rangle_{\Omega}$). Then there is a nonzero $c \in D$ such that for any $\varphi \in \mathcal{B}(D, c)$,*

$$\varphi(S_1) \subset \langle \varphi(S_2) \rangle_{\bar{k}(x)} \text{ (resp. } \varphi(S_1) \subset \langle \varphi(S_2) \rangle_{\bar{k}}).$$

PROOF. One only need to prove the case that $S_1, S_2 \subset F(x)[X, 1/\det(X)]$. The other case can be proved similarly. For each $p \in S_1$, write

$$p = \sum_{q \in S_2} a_{p,q} q,$$

with $a_{p,q} \in F(x)[X, 1/\det(X)]$. Let c be a nonzero element in D such that for any $\varphi \in \mathcal{B}(D, c)$, $\varphi(p), \varphi(q), \varphi(a_{p,q})$ are well-defined for all $p \in S_1, q \in S_2$. Then one sees that for any $\varphi \in \mathcal{B}(D, c)$, $\varphi(S_1)$ is a subset of the ideal in $\bar{k}(x)[X, 1/\det(X)]$ generated by $\varphi(S_2)$. $\square$

Let $\mathcal{X}$ be a finite subset of $X(G)$, the group of characters of G, whose elements are represented by polynomials in $\Omega[X, 1/\det(X)]$. Let $D \subset \Omega$ be a finitely generated k-algebra such that $S, \mathcal{X} \subset D[X, 1/\det(X)]$.

Lemma 3.2 *There is a basic open subset U of $\mathrm{Hom}_k(D, \bar{k})$ such that for any $\varphi \in U$, one has that*

(a) *$\mathbb{V}_{\bar{k}}(\varphi(S))$ is an algebraic subgroup of $\mathrm{GL}_n(\bar{k})$;*

(b) *$[G : G^\circ] = [\mathbb{V}_{\bar{k}}(\varphi(S)) : \mathbb{V}_{\bar{k}}(\varphi(S))^\circ]$ and $\dim(\mathbb{V}_{\bar{k}}(\varphi(S))) = \dim(G)$;*

(c) *$\varphi(\mathcal{X}) \subset X(\mathbb{V}_{\bar{k}}(\varphi(S)))$.*

PROOF. Note that to show that a variety V in $\mathrm{GL}_n(\bar{k})$ is an algebraic group, it suffices to show that $1 \in V$ and if $g_1, g_2 \in V$ then $g_1 g_2 \in V$. Let F be the field of fractions of D. Let $Z = (Z_{i,j})$ denote an $n \times n$ matrix with indeterminate entries. Set I to be the ideal in $F[X, Z, 1/\det(X), 1/\det(Z)]$ generated by

$$S \cup \{p(Z) | p \in S\}.$$

Then for each $p \in S$, $p^{\mu_p}(XZ) \in I$ for some $\mu_p > 0$ and for each $\chi \in \mathcal{X}$, $(\chi(XZ) - \chi(X)\chi(Z))^{\nu_\chi} \in I$ for some $\nu_\chi > 0$. Write

$$\begin{aligned} p^{\mu_p}(XZ) &= \sum_{q \in S} a_{p,q} q(X) + \sum_{q \in S} b_{p,q} q(Z), \\ (\chi(XZ) - \chi(X)\chi(Z))^{\nu_\chi} &= \sum_{q \in S} \alpha_{\chi,q} q(X) + \sum_{q \in S} \beta_{\chi,q} q(Z) \end{aligned}$$

where $a_{p,q}, b_{p,q}, \alpha_{\chi,q}, \beta_{\chi,q} \in F[X, Z, 1/\det(X), 1/\det(Z)]$. It is easy to see that there is a nonzero $c_1 \in D$ such that

$$a_{p,q}, b_{p,q}, \alpha_{\chi,q}, \beta_{\chi,q} \in D[1/c_1][X, Z, 1/\det(X), 1/\det(Z)]$$

for all $p, q \in S$ and $\chi \in \mathcal{X}$, because all p, q, χ are defined over D. Then for any $\psi \in \mathcal{B}(D, c_1)$, $\mathbb{V}_{\bar{k}}(\psi(S))$ is an algebraic subgroup of $\mathrm{GL}_n(\bar{k})$ and $\psi(\mathcal{X}) \subset X(\mathbb{V}_{\bar{k}}(\psi(S)))$.

Let $G = \cup_{i=1}^{\ell} G_i$ be the minimal irreducible decomposition. Suppose that $S_i \subset \Omega[X, 1/\det(X)]$ is a finite set that defines G_i. Since $G_i \cap G_j = \emptyset$ if $i \neq j$, there is $q_i \in \langle S_i \rangle_\Omega$ such that $q_i + q_j = 1$ if $i \neq j$. Without loss of generality, we may assume that $q_i \in S_i$. Let $\tilde{D} \subset \Omega$ be a finitely generated D-algebra such that $S_i \subset \tilde{D}[X, 1/\det(X)]$ for all $i = 1, \cdots, \ell$. Due to a result of Bertini-Neother (Proposition 9.29 in the page 120 of [4]), there is a nonzero $c_2 \in \tilde{D}$ such that if $\psi \in \mathcal{B}(\tilde{D}, c_2)$ then $\mathbb{V}_{\bar{k}}(\psi(S_i))$ is irreducible and $\dim(G_i) = \dim(\mathbb{V}_{\bar{k}}(\psi(S_i))$ for all $1 \leq i \leq \ell$. Since $\psi(q_i) + \psi(q_j) = 1$ if $i \neq j$, one has that $\mathbb{V}_{\bar{k}}(\psi(S_i)) \cap \mathbb{V}_{\bar{k}}(\psi(S_j)) = \emptyset$ if $i \neq j$. Denote $\tilde{S} = \{p_1 \cdots p_\ell | p_i \in S_i\}$. Then

$$\mathbb{V}_\Omega(\tilde{S}) = \cup_{i=1}^{\ell} \mathbb{V}_\Omega(S_i) = G.$$

Thus the ideals $\langle S \rangle_\Omega$ and $\langle \tilde{S} \rangle_\Omega$ have the same radical. Lemma 3.1 implies that there is a nonzero $c_3 \in \tilde{D}$ such that for any $\psi \in \mathcal{B}(\tilde{D}, c_3)$, $\langle \psi(S) \rangle_{\bar{k}}$ and $\langle \psi(\tilde{S}) \rangle_{\bar{k}}$ have the same radical.

Now set $c = c_1 c_2 c_3 \in \tilde{D}$. Suppose that $\psi \in \mathcal{B}(\tilde{D}, c)$. Then $\mathbb{V}_{\bar{k}}(\psi(S))$ is an algebraic group in $\mathrm{GL}_n(\bar{k})$, $\psi(\mathcal{X}) \subset X(\mathbb{V}_{\bar{k}}(\psi(S)))$ and

$$\mathbb{V}_{\bar{k}}(\psi(S)) = \mathbb{V}_{\bar{k}}(\psi(\tilde{S})) = \cup_{i=1}^{\ell} \mathbb{V}_{\bar{k}}(\psi(S_i)).$$

For all $1 \leq i \leq \ell$, $\mathbb{V}_{\bar{k}}(\psi(S_i))$ is irreducible. Moreover if $1 \leq i \neq j \leq \ell$, $\mathbb{V}_{\bar{k}}(\psi(S_i)) \cap \mathbb{V}_{\bar{k}}(\psi(S_j)) = \emptyset$. This implies that

$$[\mathbb{V}_{\bar{k}}(\psi(S)) : \mathbb{V}_{\bar{k}}(\psi(S))^\circ] = \ell.$$

Finally, since $\dim(\mathbb{V}_{\bar{k}}(\psi(S_i))) = \dim(G_i)$ for all $1 \leq i \leq \ell$, $\dim(\mathbb{V}_{\bar{k}}(\psi(S))) = \dim(G)$.

Due to Lemma 2.1, there is a basic open subset U of $\mathrm{Hom}_k(D, \bar{k})$ such that

$$U \subset \{\psi|_D \mid \psi \in \mathcal{B}(\tilde{D}, c)\}.$$

For $\varphi \in U$, let $\psi \in \mathcal{B}(\tilde{D}, c)$ be such that $\psi|_D = \varphi$. Then $\mathbb{V}_{\bar{k}}(\varphi(S)) = \mathbb{V}_{\bar{k}}(\psi(S))$, which satisfies (a)-(c). □

Lemma 3.3 *Suppose that G is generated by unipotent elements of $\mathrm{GL}_n(\Omega)$. Then there is a basic open subset U of $\mathrm{Hom}_k(D, \bar{k})$ such that for any $\varphi \in U$, $\mathbb{V}_{\bar{k}}(\varphi(S))$ is an algebraic subgroup of $\mathrm{GL}_n(\bar{k})$ generated by unipotent elements.*

Proof. Due to Proposition in the page 55 of [6], there is a matrix

$$\mathcal{P}(t_1, \cdots, t_\ell) = \prod_{i=1}^{\ell} \left(\sum_{j=0}^{n-1} \frac{\mathbf{m}_i^j t_i^j}{j!} \right) \in \mathrm{GL}_n(\Omega[t_1, \cdots, t_\ell])$$

where $\ell \leq 2\dim(G)$ and $\mathbf{m}_1, \cdots, \mathbf{m}_\ell$ are nilpotent matrices in $\mathrm{Mat}_n(\Omega)$ such that

$$G = \{ \mathcal{P}(c_1, \cdots, c_\ell) | \; c_1, \cdots, c_\ell \in \Omega \}.$$

By Lemma B.8 of [2], there is an integer $s(n)$ depending on n such that any algebraic subgroup of $\mathrm{GL}_n(\Omega)$ (resp. $\mathrm{GL}_n(\bar{k})$) generated by unipotent elements is defined by a finite set of polynomials in $\Omega[X]$ (resp. $\bar{k}[X]$) with degree not greater than $s(n)$. Set

$$I_1 = \mathbb{I}(G) \cap \Omega[X]_{\leq s(n)}$$

where $\mathbb{I}(G)$ denotes the vanishing ideal of G. Then I_1 is an Ω-vector space of finite dimension and $\mathbb{V}_\Omega(I_1) = G$. Denote by $M_1, \cdots, M_\mu$ all monomials in X with degree not greater than $s(n)$. For each $1 \leq i \leq \mu$, write

$$M_i|_{X=\mathcal{P}(t_1,\cdots,t_\ell)} = \sum_{|\mathbf{d}| \leq (n-1)s(n)} a_{i,\mathbf{d}} \mathbf{t}^{\mathbf{d}}$$

where $\mathbf{d} = (d_1, \cdots, d_\ell) \in \mathbb{Z}_{\geq 0}^\ell$, $\mathbf{t}^{\mathbf{d}} = t_1^{d_1} \cdots t_\ell^{d_\ell}$ and $a_{i,\mathbf{d}} \in \Omega$. Let B be the $\binom{(n-1)s(n)+\ell}{\ell} \times \mu$ matrix formed by the vectors $(a_{1,\mathbf{d}}, \cdots, a_{\mu,\mathbf{d}})$ with $|\mathbf{d}| \leq (n-1)s(n)$. Suppose that $p \in \Omega[X]_{\leq s(n)}$. Write $p = \sum_{i=1}^\mu c_i M_i$ and denote

$$\mathbf{c}(p) = (c_1, \cdots, c_\mu)^T.$$

Then $p \in I_1$ if and only if $B\mathbf{c}(p) = 0$. Assume that $p_1, \cdots, p_l$ is a basis of I_1. Then $\{\mathbf{c}(p_1), \cdots, \mathbf{c}(p_l)\}$ is a basis of the right kernel of B. Additionally, one has that $\sqrt{\langle p_1, \cdots, p_l \rangle_\Omega} = \sqrt{\langle S \rangle_\Omega}$, since $\mathbb{V}_\Omega(I_1) = \mathbb{V}_\Omega(S) = G$.

Now let $\tilde{D} \subset \Omega$ be a finitely generated D-algebra such that $\mathbf{m}_i \in \mathrm{Mat}_n(\tilde{D})$ for all $i = 1, \cdots, \ell$ and $p_j \in \tilde{D}[X]$ for all $j = 1, \cdots, l$. One easily sees that there is a nonzero $b \in \tilde{D}$ such that for any $\varphi \in \mathcal{B}(\tilde{D}, b)$, $\{\mathbf{c}(\varphi(p_1)), \cdots, \mathbf{c}(\varphi(p_l))\}$ is a basis of the right kernel of $\varphi(B)$. Lemmas 3.1 and 3.2 imply that there is a basic open subset U_1 of $\mathrm{Hom}_k(\tilde{D}, \bar{k})$ such that for any $\varphi \in U_1$,

(1) $\mathbb{V}_{\bar{k}}(\{\varphi(p_1), \cdots, \varphi(p_l)\})$ is a connected algebraic subgroup of $\mathrm{GL}_n(\bar{k})$ and

$$\dim(\mathbb{V}_{\bar{k}}(\{\varphi(p_1), \cdots, \varphi(p_l)\})) = \dim(G);$$

(2) $\sqrt{\langle \varphi(p_1), \cdots, \varphi(p_l) \rangle_{\bar{k}}} = \sqrt{\langle \varphi(S) \rangle_{\bar{k}}}$.

Let $U_2 = \mathcal{B}(\tilde{D}, b) \cap U_1$ and let $\varphi \in U_2$. Denote

$$H = \{\varphi(\mathcal{P})(c_1, \cdots, c_\ell) | c_1, \cdots, c_\ell \in \bar{k}\}$$

and set

$$I_2 = \mathbb{I}(H) \cap \bar{k}[X]_{\leq s(n)}.$$

Then for any $q \in \bar{k}[X]_{\leq s(n)}$, $q \in I_2$ if and only if $\mathbf{c}(q)$ is in the right kernel of $\varphi(B)$. This implies that $\{\varphi(p_1), \cdots, \varphi(p_l)\}$ is a basis of I_2. Let $\bar{H}$ be the algebraic subgroup of $\mathrm{GL}_n(\bar{k})$ generated by H. Then $\bar{H} \subset \mathbb{V}_{\bar{k}}(\{\varphi(p_1), \cdots, \varphi(p_l)\})$, since $\mathbb{V}_{\bar{k}}(\{\varphi(p_1), \cdots, \varphi(p_l)\})$ is an algebraic group containing H. On the other hand, note that H consists of unipotent elements, $\bar{H}$ is defined by some polynomials in $\bar{k}[X, 1/\det(X)]$ with degree not greater than $s(n)$ and thus it is defined by $\mathbb{I}(\bar{H}) \cap \bar{k}[X]_{\leq s(n)}$ which is a subset of I_2. Hence

$$\bar{H} \supset \mathbb{V}_{\bar{k}}(I_2) = \mathbb{V}_{\bar{k}}(\{\varphi(p_1), \cdots, \varphi(p_l)\}).$$

So $\mathbb{V}_{\bar{k}}(\{\varphi(p_1), \cdots, \varphi(p_l)\}) = \bar{H}$ that is generated by unipotent elements.

Finally, by (3), $\mathbb{V}_{\bar{k}}(\varphi(S)) = \mathbb{V}_{\bar{k}}(\{\varphi(p_1), \cdots, \varphi(p_l)\})$. The lemma then follows from Lemma 2.1. $\square$

Let $K \subset \Omega$ be algebraically closed. Let H be a connected algebraic subgroup of $\mathrm{GL}_n(K)$. The following lemma gives a criterion for a finite subset $\mathcal{X} \subset X(H)$ to be a basis of $X(H)$. We say $\mathcal{X}$ is multiplicatively independent if the equality $\prod_{\chi\in\mathcal{X}} \chi^{d_\chi} = 1$ with $d_\chi \in \mathbb{Z}$ implies that $d_\chi = 0$ for all $\chi \in \mathcal{X}$

Lemma 3.4 *Let $\mathcal{X} \subset X(H)$ be a finite set. Then $\mathcal{X}$ is a basis of $X(H)$ if and only if $\mathcal{X}$ is multiplicatively independent and $\cap_{\chi\in\mathcal{X}} \ker(\chi)$ is generated by unipotent elements.*

Proof. The necessary part follows from Lemma B.10 of [2]. For the sufficient part, it suffices to show that $\mathcal{X}$ generates $X(H)$. Assume that $\mathcal{X} = \{\chi_1, \cdots, \chi_l\}$ and $\chi' \in X(H)$. By Lemma B.10 of [2], any unipotent element of H is contained in $\ker(\chi')$. Thus $\cap_{i=1}^l \ker(\chi_i) \subset \ker(\chi')$. Consider the following morphisms of algebraic groups

$$\begin{array}{ccccc} H/\cap_{i=1}^l \ker(\chi_i) & \xrightarrow{\Phi} & \mathbb{G}_m(K)^{l+1} & \xrightarrow{\pi} & \mathbb{G}_m(K)^l \\ \bar{\mathbf{c}} & \longrightarrow & \begin{pmatrix} \chi_1(\bar{\mathbf{c}}) \\ \vdots \\ \chi_l(\bar{\mathbf{c}}) \\ \chi'(\bar{\mathbf{c}}) \end{pmatrix} & \longrightarrow & \begin{pmatrix} \chi_1(\bar{\mathbf{c}}) \\ \vdots \\ \chi_l(\bar{\mathbf{c}}) \end{pmatrix}. \end{array}$$

Note that $\pi \circ \Phi$ is an isomorphism of algebraic groups, since $\ker(\pi \circ \Phi) = \cap_{i=1}^l \ker(\chi_i)$. This implies that $\pi|_{\mathrm{img}(\Phi)}$ is an isomorphism of algebraic groups and then χ' is equal to a product of powers of $\chi_1, \cdots, \chi_l$. Therefore $\mathcal{X}$ generates $X(H)$. $\square$

Now we are ready to prove the main result of this section.

Proposition 3.5 *Let $G \subset \mathrm{GL}_n(\Omega)$ be a connected algebraic group defined by a finite set $S \subset \Omega[X, 1/\det(X)]$ and let $\mathcal{X} \subset \Omega[X, 1/\det(X)]$ be a basis of $X(G)$. Let D be a finitely generated k-algebra such that $S, \mathcal{X} \subset D[X, 1/\det(X)]$. Then there is a basic open subset U of $\mathrm{Hom}_k(D, \bar{k})$ such that for any $\varphi \in U$,*

(a) *$\mathbb{V}_{\bar{k}}(\varphi(S))$ is a connected algebraic group and $\dim(\mathbb{V}_{\bar{k}}(\varphi(S))) = \dim(G)$;*

(b) *$\varphi(\mathcal{X})$ is a basis of $X(\mathbb{V}_{\bar{k}}(\varphi(S)))$.*

Proof. Let $\{p_\chi | \chi \in \mathcal{X}\}$ be a set of distinct prime numbers. By Lemma C in the page 104 of [6], there is $\mathbf{c} \in G$ such that $\chi(\mathbf{c}) = p_\chi$ for all $\chi \in \mathcal{X}$. Let $\tilde{D}$ be a finitely generated D-algebra such that $\mathbf{c} \in \mathrm{Mat}_n(\tilde{D})$. Set

$$T = S \cup \{\chi - 1 | \chi \in \mathcal{X}\}.$$

Then $\mathbb{V}_{\bar{k}}(T) = \cap_{\chi\in\mathcal{X}} \ker(\chi)$ and by Lemma B.10 of [2] it is generated by all unipotent elements of G. Let U_1 be a basic open subset of $\mathrm{Hom}_k(\tilde{D}, \bar{k})$ such that for any $\varphi \in U_1$, one has that

(1) $\mathbb{V}_{\bar{k}}(\varphi(S))$ is a connected algebraic group and its dimension equals $\dim(G)$;

(2) $\mathbb{V}_{\bar{k}}(\varphi(T))$ is an algebraic subgroup of $\mathbb{V}_{\bar{k}}(\varphi(S))$ generated by unipotent elements;

(3) $\varphi(\mathcal{X}) \subset X(\mathbb{V}_{\bar{k}}(\varphi(S)))$.

Due to Lemmas 3.2 and 3.3, such U_1 exists. Now set $U_2 = U_1 \cap \mathcal{B}(\tilde{D}, \det(\mathbf{c}))$. Suppose that $\varphi \in U_2$. We first show that $\{\varphi(\chi) | \chi \in \mathcal{X}\}$ is multiplicatively independent. Assume that $\prod_{\chi \in \mathcal{X}} \varphi(\chi)^{\nu_\chi} = 1$ with $\nu_\chi \in \mathbb{Z}$. Since $\varphi(\det(\mathbf{c})) \neq 0$, $\varphi(\mathbf{c}) \in \mathbb{V}_{\bar{k}}(\varphi(S))$. Then

$$1 = \prod_{\chi \in \mathcal{X}} \varphi(\chi)^{\nu_\chi}|_{X=\varphi(\mathbf{c})} = \prod_{\chi \in \mathcal{X}} \varphi(\chi(\mathbf{c}))^{\nu_\chi} = \prod_{\chi \in \mathcal{X}} p_\chi^{\nu_\chi},$$

which implies that $\nu_\chi = 0$ for all $\chi \in \mathcal{X}$. Hence $\varphi(\mathcal{X})$ is multiplicatively independent. On the other hand, from (2), $\cap_{\chi \in \mathcal{X}} \ker(\varphi(\chi)) = \mathbb{V}_{\bar{k}}(\varphi(T))$ which is generated by unipotent elements. Lemma 3.4 implies that $\varphi(\mathcal{X})$ is a basis of $X(\mathbb{V}_{\bar{k}}(\varphi(S)))$. Finially, Lemma 2.1 completes the proof. $\square$

4 Difference equations under specialization

Let K be a subfield of Ω and $B \in \mathrm{GL}_n(K(x))$. The automorphism σ of $K(x)$ can be extended to an automorphism of $K(x)[X, 1/\det(X)]$ by setting $\sigma(X) = BX$. As we shall deal with a family of automorphisms, to void confusion, the automorphism of $K(x)[X, 1/\det(X)]$ induced by $\sigma(X) = BX$ will be denoted by σ_B. An ideal I of $K(x)[X, 1/\det(X)]$ is called a σ_B-ideal if $\sigma_B(I) = I$.

Let A be given as in (1) and D be a finitely generated k-algebra with F as field of fractions such that $A \in \mathrm{GL}_n(F(x))$. It is easy to see that there is a nonzero $c \in D$ such that for any $\varphi \in \mathcal{B}(D, c)$ one has that $\varphi(A)$ is well-defined and is invertible. In the following, when a homomorphism $\varphi \in \mathrm{Hom}_k(D, \bar{k})$ is applied to $\sigma(Y) = AY$, we always assume that $\varphi(A)$ is well-defined and is invertible.

Definition 4.1 *Let ν be a positive integer and $I \subset \Omega(x)[X, 1/\det(X)]$ be a σ_A-ideal generated by some polynomials in $\Omega(x)[X]_{\leq \nu}$. I is said to be a ν-maximal σ_A-ideal if it satisfies that for any σ_A-ideal J generated by some polynomials in $\Omega(x)[X]_{\leq \nu}$ if $I \subset J$ then $I = J$. Similarly, we define ν-maximal $\sigma_{\varphi(A)}$-ideals in $\bar{k}(x)[X, 1/\det(X)]$.*

Let I_ν be a ν-maximal σ_A-ideal. It is shown in [3] that there exists a fundamental matrix of $\sigma(Y) = AY$ over $\Omega(x)$, say $\mathcal{F}$, such that

$$I_\nu = \langle \{p \in \Omega(x)[X]_{\leq \nu} \mid p(\mathcal{F}) = 0\} \rangle_{\Omega(x)}.$$

Furthermore, if J is another ν-maximal σ_A-ideal, then there is an invertible matrix $g \in \mathrm{GL}_n(\Omega)$ such that

$$J = \{\ p(Xg) \mid p \in I_\nu\ \}.$$

Let m be a nonnegative integer. Set

$$\mathrm{I}(m, I_\nu) = I_\nu \cap \Omega[x]_{\leq m}[X]_{\leq \nu}$$

where

$$\Omega[x]_{\leq m}[X]_{\leq \nu} = \{p \in \Omega[x, X] \mid \deg_x(p) \leq m, \deg_X(p) \leq \nu\}.$$

One sees that there is an integer μ such that $\mathrm{I}(\mu, I_\nu)$ generates I_ν. We call such μ a coefficient bound of I_ν. The discussion above implies that if μ is a coefficient bound of I_ν then it is a coefficient bound of all ν-maximal σ_A-ideals. Hence the following definition is reasonable.

Definition 4.2 *An integer μ is called a coefficient bound of ν-maximal σ_A-ideals if $\mathrm{I}(\mu, I_\nu)$ generates I_ν for every ν-maximal σ_A-ideal I_ν.*

Remark 4.3 *Note that in [3] we use the symbol $I_{\mathcal{F},\nu}$ to denote the ν-maximal σ_A-ideal I_ν, where $\mathcal{F}$ is a fundamental matrix of (1).*

This section is aimed at proving the follow proposition.

Proposition 4.4 *Suppose that I_ν is a ν-maximal σ_A-ideal and it is generated by a finite set P. Let $D \subset \Omega$ be a finitely generated k-algebra with F as field of fractions such that $A \in \mathrm{GL}_n(F(x))$ and $P \subset F(x)[X, 1/\det(X)]$. Then there exists a basic open subset U of $\mathrm{Hom}_k(D, \bar{k})$ such that for any $\varphi \in U$, $\varphi(P)$ generates a ν-maximal $\sigma_{\varphi(A)}$-ideal of $\bar{k}(x)[X, 1/\det(X)]$.*

Let us sketch the proof. First, we show that there is a coefficient bound of I_ν, say μ, satisfying that it is a coefficient bound of ν-maximal $\sigma_{\varphi(A)}$-ideals for all φ in some basic open subset of $\mathrm{Hom}_k(D, \bar{k})$. Second, we prove that there is a basic open subset of $\mathrm{Hom}_k(D, \bar{k})$ such that for each φ in this set a basis of $\mathrm{I}(\mu, I_\nu)$ specializes to a basis of $\mathrm{I}(\mu, \tilde{I}_\varphi)$ for some ν-maximal $\sigma_{\varphi(A)}$-ideal $\tilde{I}_\varphi$. By the choice of μ, any basis of $\mathrm{I}(\mu, \tilde{I}_\varphi)$ generates $\tilde{I}_\varphi$. Lemma 3.1 then concludes the proposition.

4.1 Coefficient bounds of ν-maximal σ_A-ideals

In this subsection, we shall show that there is a coefficient bound of ν-maximal σ_A-ideals such that it is also a coefficient bound of ν-maximal $\sigma_{\varphi(A)}$-ideals for all φ in some basic open subset of $\mathrm{Hom}_k(D, \bar{k})$. Such coefficient bound can be derived from a degree bound of hypergeometric solutions of a suitable linear difference equation.

Let R be the Picard-Vessiot extension ring of $\Omega(x)$ for (1). An element $h \in R$ is said to be hypergeometric over $\Omega(x)$ if $h \neq 0$ and $\sigma(h) = rh$ with a nonzero $r \in \Omega(x)$. A solution $\mathbf{h}$ of (1) is called a hypergeometric solution if $\mathbf{h} = \mathbf{v}h$ where $\mathbf{v} \in \Omega(x)^n$ and h is a hypergeometric element over $\Omega(x)$.

Definition 4.5 *A positive integer N is called a hyper-bound of (1) if every hypergeometric solution of (1) is of the form $\mathbf{v}h$ where h is a hypergeometric element over $\Omega(x)$ and $\mathbf{v} \in \Omega(x)^n$ with $\deg(\mathbf{v}) \leq N$. Here*

$$\deg(\mathbf{v}) = \max\{\deg(v_1), \cdots, \deg(v_n)\}.$$

with $\mathbf{v} = (v_1, \cdots, v_n)^T$.

Let I_ν be a ν-maximal σ_A-ideal. By the method described in Appendix A of [3], one can compute a coefficient bound as follows. Let $g \in \mathrm{GL}_n(\Omega(x))$. The map $X \to gX$ induces an isomorphism of the $\Omega(x)$-vector space $\Omega(x)[X]_{\leq \nu}$. If we take a basis of $\Omega(x)[X]_{\leq \nu}$ to be all monomials in X with degree not greater than ν , then having chosen a monomial order on these monomials, we obtain a representation of the isomorphism induced by g which is an invertible matrix of order $\binom{n^2+\nu}{\nu}$. We shall denote this matrix by $\mathrm{Sym}^{\leq \nu}(g)$. Note that $\mathrm{Sym}^{\leq \nu}$ is a group homomorphism. Let $\{\mathbf{v}_1, \cdots, \mathbf{v}_\ell\}$ be a basis of the solution space of $\sigma(Y) = \mathrm{Sym}^{\leq \nu}(A)Y$. For each $1 \leq i \leq \ell$, set $\mathbf{w}_i$ to be the vector formed by all $i \times i$ minors of the matrix $(\mathbf{v}_1, \cdots, \mathbf{v}_i)$ and set

$$\mathbf{u} = \begin{pmatrix} \mathbf{w}_1 \\ \mathbf{w}_2 \\ \vdots \\ \mathbf{w}_\ell \end{pmatrix}.$$

Using the equality $\sigma(\mathbf{v}_i) = \mathrm{Sym}^{\leq \nu}(A)\mathbf{v}_i$, we can construct an invertible matrix M such that $\sigma(\mathbf{u}) = M\mathbf{u}$. One sees that M is only dependent on A and ν. For convenience, denote by $\mathcal{M}_\nu(A)$ the matix M obtained by the above construction. Let D be a finitely generated k-algebra with F as field of fractions such that both A and $\mathcal{M}_\nu(A)$ have entries in $F(x)$. For any $\varphi \in \mathrm{Hom}_k(D, \bar{k})$, the above construction can also be applied to $\sigma(Y) = \varphi(A)Y$. In particular, one sees that there is a nonzero $c \in D$ such that for any $\varphi \in \mathcal{B}(D, c)$, $\varphi(\mathcal{M}_\nu(A)) = \mathcal{M}_\nu(\varphi(A))$. Appendix A of [3] shows that an integer twice any hyper-bound of $\sigma(Y) = \mathcal{M}_\nu(A)Y$ (resp. $\sigma(Y) = \mathcal{M}_\nu(\varphi(A))Y$) can be taken as a coefficient bound of ν-maximal σ_A-ideals (resp. ν-maximal $\sigma_{\varphi(A)}$-ideals). Therefore, in order to show that there is an integer μ which is a coefficient bound of ν-maximal σ_A-ideals as well as a coefficient bound of ν-maximal $\sigma_{\varphi(A)}$-ideals with all φ in some basic open subset U, it suffices to show that there is an integer N which is a hyper-bound of $\sigma(Y) = \mathcal{M}_\nu(A)Y$ as well as a hyper-bound of $\sigma(Y) = \mathcal{M}_\nu(\varphi(A))Y$ with all $\varphi \in U$.

Now let us deal with hyper-bounds of (1). It is well-known that the equation (1) is equivalent to a linear difference operator with coefficients in $\Omega(x)$. To estimate hyper-bounds, it is more convenient to consider linear difference operators. Note that for linear difference operators, a solution is called a hypergeometric solution if this solution is a hypergeometric element. By a similar way, one can define hyper-bounds of $L = 0$. Let L be a linear difference operator in $\Omega[x][\sigma]$ of the form

$$a_n(x)\sigma^n + \cdots + a_1(x)\sigma + a_0(x)$$

with $a_i(x) \in \Omega[x]$ and $a_n(x)a_0(x) \neq 0$. Let us first investigate polynomial solutions. Set $\bar{\sigma} = x(\sigma - 1)$. Multiplying L with a suitable polynomial in $\mathbb{Z}[x]$, one obtains a new operator of the form $\sum_{i=0}^n \bar{a}_i(x)\bar{\sigma}^m \in \Omega[x][\bar{\sigma}]$. Denote

$$\rho = \max\{\deg(\bar{a}_0), \cdots, \deg(\bar{a}_n)\}.$$

Definition 4.6 $\sum_{i=0}^n \mathrm{coeff}(\bar{a}_i, x, \rho)y^i$ *is called the indicial polynomial of* L, *denoted by* $\mathrm{Ind}(L)$, *where* $\mathrm{coeff}(\bar{a}_i, x, \rho)$ *is the coefficient of* x^ρ *in* $\bar{a}_i$.

Let $D \subset \Omega$ be a finitely generated k-algebra such that $L \in D[x][\sigma]$.

Lemma 4.7 *Let* $N = \max \mathbf{Z}(\mathrm{Ind}(L)) \cup \{0\}$. *Then there is a basic open subset* U *of* $\mathrm{Hom}_k(D, \bar{k})$ *such that if* $\varphi \in U$ *then polynomial solutions of* $\varphi(L)$ *are of degree not greater than* N.

Proof. Suppose that $\varphi \in \mathrm{Hom}_k(D, \bar{k})$. One can easily verify that if m is the degree of a polynomial solution of $\varphi(L) = 0$ then m is an integer zero of $\mathrm{Ind}(\varphi(L))$. Lemma 2.19 implies that there is a finitely generated subgroup Γ_1 of $\mathbb{G}_a(\Omega)$ such that for any $\varphi \in \mathcal{B}(D, \Gamma_1)$, $\mathbf{Z}(\mathrm{Ind}(L)) = \mathbf{Z}(\varphi(\mathrm{Ind}(L)))$. Let c be a nonzero elment in D such that for every $\varphi \in \mathcal{B}(D, c)$, $\deg(\bar{a}_i) = \deg(\varphi(\bar{a}_i))$ for all $0 \le i \le n$. Let $U = \mathcal{B}(D, \Gamma_1) \cap \mathcal{B}(D, c)$. Suppose that $\varphi \in U$. One has that $\varphi(\mathrm{Ind}(L)) = \mathrm{Ind}(\varphi(L))$ and then

$$\begin{aligned} \max \mathbf{Z}(\mathrm{Ind}(\varphi(L))) \cup \{0\} &= \max \mathbf{Z}(\varphi(\mathrm{Ind}(L))) \cup \{0\} \\ &= \max \mathbf{Z}(\mathrm{Ind}(L)) \cup \{0\} = N. \end{aligned}$$

Thus every polynomial solution of $\varphi(L)$ has degree not greater than N. $\square$

Denote

$$\mathcal{S}_L = \{\, (p,q) \in \Omega[x] \mid p,q \text{ are monic and } p|a_0(x), q|a_n(x-n+1) \,\}.$$

We recall the algorithm given in [10] for finding hypergeometric solutions of $L = 0$ as follows.

Algorithm 4.8 *Input: Polynomials $a_i(x)$ for $i = 0, 1, \cdots, n$;*
Output: a hypergeometric solution of $L = \sum_{i=0}^n a_i(x)\sigma^i = 0$ if it exists; otherwise 0.

(a) *For each $(p,q) \in \mathcal{S}_L$ do*

(1) $P_i(x) := a_i(x) \prod_{j=0}^{i-1} p(x+j) \prod_{j=i}^{n-1} q(x+j)$ *for all* $i = 0, 1, \cdots, n$;

(2) $m := \max\{\deg(P_i(x))\}$ *and* $\alpha_i := \mathrm{coeff}(P_i(x), x, m)$ *for all* $0 \le i \le n$;

(3) *let $\mathcal{Z}_{p,q} \subset \Omega$ be the set of all nonzero solutions of*

$$f_{p,q}(y) = \sum_{i=0}^n \alpha_i y^i = 0$$

(4) *for each $\beta \in \mathcal{Z}_{p,q}$ do if*

$$L_{p,q,\beta} = \sum_{i=0}^n \beta^i P_i(x) \sigma^i = 0.$$

has a nonzero polynomial solution $Q(x)$, then return h with

$$h(x+1) = \beta \frac{p(x)}{q(x)} \frac{Q(x+1)}{Q(x)} h(x).$$

(b) *Return 0.*

Let $\mathcal{S}_L, \mathcal{Z}_{p,q}, L_{p,q,\beta}$ be as in Algorithm 4.8. We define an integer

$$\begin{aligned} N(L) = &\max \mathbf{Z}\left(\prod_{(p,q)\in\mathcal{S}_L, \beta\in\mathcal{Z}_{p,q}} \mathrm{Ind}(L_{p,q,\beta}) \right) \bigcup \{0\} \\ &+ \max\{\deg(a_n(x)), \deg(a_0(x))\}. \end{aligned}$$

Due to the above algorithm, $N(L)$ is a hyper-bound of $L = 0$. Moreover, we have the following result.

Lemma 4.9 *There is a basic open subset U of $\mathrm{Hom}_k(D,\bar{k})$ such that for any $\varphi \in U$, $N(L)$ is a hyper-bound of $\varphi(L)=0$.*

Proof. Let $\mathcal{S}_L, f_{p,q}, \mathcal{Z}_{p,q}, L_{p,q,\beta}$ be as in Algorithm 4.8 and let

$$\begin{aligned} W = &\{1\} \bigcup \{\mathrm{lc}(a_i(x)) | i=0,\cdots,n\} \bigcup \mathbb{V}_\Omega(a_n(x)) \bigcup \mathbb{V}_\Omega(a_0(x)) \\ &\bigcup \bigcup_{(p,q)\in\mathcal{S}_L} \mathcal{Z}_{p,q} \end{aligned}$$

where $\mathbb{V}_\Omega(a_i(x))$ denotes the set of roots of $a_i(x)=0$ in Ω. Let $\tilde{D} \subset \Omega$ be a finitely generated D-algebra such that $W \subset \tilde{D}$. Let Γ_1 be the subgroup of $\mathbb{G}_a(\Omega)$ generated by W. Suppose that $\varphi \in \mathcal{B}(\tilde{D},\Gamma_1)$. It is easy to see that $\mathcal{S}_{\varphi(L)} = \varphi(\mathcal{S}_L)$. Furthermore for each $(\varphi(p),\varphi(q)) \in \mathcal{S}_{\varphi(L)}$, one has that

$$f_{\varphi(p),\varphi(q)} = \varphi(f_{p,q}), \mathcal{Z}_{\varphi(p),\varphi(q)} = \varphi(\mathcal{Z}_{p,q}),$$

and for each $\beta \in \mathcal{Z}_{p,q}$, one has that $L_{\varphi(p),\varphi(q),\varphi(\beta)} = \varphi(L_{p,q,\beta})$. This together with Algorithm 4.8 implies that for every hypergeometric solution h of $\varphi(L)=0$, there is $(p,q) \in \mathcal{S}_L$ and $\beta \in \mathcal{Z}_{p,q}$ such that $\sigma(h)/h$ is of the form

$$\varphi(\beta)\frac{\varphi(p(x))}{\varphi(q(x))}\frac{\bar{Q}(x+1)}{\bar{Q}(x)}$$

where $\bar{Q}(x)$ is a nonzero polynomial solution of $L_{\varphi(p),\varphi(q),\varphi(\beta)}=0$. Let $\Gamma_{p,q,\beta}$ be a finitely generated subgroup of $\mathbb{G}_a(\Omega)$ such that for any $\varphi \in \mathcal{B}(\tilde{D},\Gamma_{p,q,\beta})$, polynomial solutions of $\varphi(L_{p,q,\beta})=0$ i.e. $\bar{Q}(x)$, are of degree not greater than

$$\max \mathbf{Z}(\mathrm{Ind}(L_{p,q,\beta})) \cup \{0\}.$$

Set

$$U = \mathcal{B}(\tilde{D},\Gamma_1) \bigcap \bigcap_{(p,q)\in\mathcal{S}_L, \beta\in\mathcal{Z}_{p,q}} \mathcal{B}(\tilde{D},\Gamma_{p,q,\beta}).$$

Then for any $\varphi \in U$, $N(L)$ is a hyper-bound of $\varphi(L)=0$. The lemma then follows from Lemma 2.1. □

By Lemma 4.9 and by means of cyclic vector method, one has the following corollary.

Corollary 4.10 *Let $D \subset \Omega$ be a finitely generated k-algebra with F as field of fractions such that A has entries in $F(x)$. Then there is a hyper-bound N of (1) and a basic open subset U of $\mathrm{Hom}_k(D,\bar{k})$ such that for any $\varphi \in U$, N is also a hyper-bound of $\sigma(Y)=\varphi(A)Y$.*

The above corollary together with the discussion after Definition 4.5 implies the following result.

Lemma 4.11 *There is a coefficient bound μ of ν-maximal σ_A-ideals and a basic open subset U of $\mathrm{Hom}_k(D,\bar{k})$ such that μ is also a coefficient bound of ν-maximal $\sigma_{\varphi(A)}$-ideals for each $\varphi \in U$.*

4.2 ν-Maximal σ_A-ideals under specialization

It is well-known that the solution space of (1) has dimension n. Here, to our purpose, we need to introduce the following.

Definition 4.12 *The dimension of (1) is defined to be the dimension of the vector space spanned by entries of a fundamental matrix of (1) over Ω, denoted by* $\dim([A])$.

Let $\mathcal{F}$ be a fundamental matrix of (1). There is a linear difference operator $L \in \Omega(x)[\sigma]$ whose solution space is formed by entries of $\mathcal{F}$. This operator L can be constructed as follows. Let $\mathbf{v} = (v_1, \cdots, v_n)^T$ be a generic solution of (1). Then L is a minimal operator annihilating all v_i. For each $i = 1, \cdots, n^2$, $\sigma^i(\mathbf{v}) = A_i\mathbf{v}$ where $A_i = \sigma^{i-1}(A)\cdots\sigma(A)A$ and furthermore for $j = 1, \cdots, n$, $\sigma^i(v_j) = A_i^{[j]}\mathbf{v}$ where $A_i^{[j]}$ is the j-th row of A_i. Note that $v_1, \cdots, v_n$ are linearly independent over $\Omega(x)$ as $\mathbf{v}$ is generic. Therefore for $a_0, \cdots, a_l \in \Omega(x)$, $\sum_{i=0}^{l} a_i\sigma^i(v_j) = 0$ for all $j = 1, \cdots, n$ if and only if

$$a_0\mathbf{e}_j^T + \sum_{i=1}^{l} a_i A_i^{[j]} = 0, \ j = 1, \cdots, n,$$

where $\{\mathbf{e}_1, \cdots, \mathbf{e}_n\}$ is the standard basis of $\Omega(x)^n$. Set

$$M = \begin{pmatrix} \mathbf{e}_1^T & \mathbf{e}_2^T & \cdots & \mathbf{e}_n^T \\ A_1^{[1]} & A_1^{[2]} & \cdots & A_1^{[n]} \\ A_2^{[1]} & A_2^{[2]} & \cdots & A_2^{[n]} \\ \vdots & \vdots & & \vdots \\ A_{n^2}^{[1]} & A_{n^2}^{[2]} & \cdots & A_{n^2}^{[n]} \end{pmatrix}. \tag{3}$$

Let $(b_0, \cdots, b_\ell, 0, \cdots, 0)$ be an element of the left kernel of M satisfying that $b_\ell \neq 0$ and ℓ is as small as possible. Then L can be chosen to be $\sum_{i=0}^{\ell} b_i\sigma^i$. For such L, we have that $\dim([A]) = \mathrm{ord}(L)$. The above construction indicates the following lemma.

Lemma 4.13 *Let D be a finitely generated k-algebra with F as field of fractions such that A has entries in $F(x)$. Then there is a nonzero $c \in D$ such that if $\varphi \in \mathcal{B}(D, c)$ then* $\dim([A]) = \dim([\varphi(A)])$.

Proof. From the above construction of L for (1), L has coefficients in $F(x)$. There is a nonzero $c \in D$ such that if $\varphi \in \mathcal{B}(D, c)$ then $\mathrm{ord}(\varphi(L)) = \mathrm{ord}(L)$ and $\mathrm{rank}(M) = \mathrm{rank}(\varphi(M))$ where M is given in (3). Suppose that $\varphi \in \mathcal{B}(D, c)$. Then the solution space of $\varphi(L) = 0$ is spanned by entries of a fundamental matrix of $\sigma(Y) = \varphi(A)Y$. The lemma then follows from the fact that $\dim([A]) = \mathrm{ord}(L)$ and $\dim([\varphi(A)]) = \mathrm{ord}(\varphi(L))$. $\square$

Lemma 4.14 *Let m be a positive integer and I_ν be a ν-maximal σ_A-ideal. Suppose that B is a basis of $\mathrm{I}(m, I_\nu)$ and $D \subset \Omega$ is a finitely generated k-algebra with F as field of fractions such that A has entries in $F(x)$ and $B \subset D[x, X]$. Then there is a nonzero $c \in D$ such that for any $\varphi \in \mathcal{B}(D, c)$, $\varphi(B)$ is a basis of $\mathrm{I}(m, \tilde{I}_\varphi)$ where $\tilde{I}_\varphi$ is a ν-maximal $\sigma_{\varphi(A)}$-ideal in $\bar{k}(x)[X, 1/\det(X)]$.*

Proof. Let us first compute the dimension of $\mathrm{I}(m, I_\nu)$. Let $\mathcal{F} = (f_{i,j})$ be a fundamental matrix of $\sigma(Y) = AY$ such that

$$I_\nu = \langle \{ p \in \Omega(x)[X]_{\leq \nu} \mid p(\mathcal{F}) = 0 \} \rangle_{\Omega(x)} .$$

From the construction of $\mathrm{Sym}^{\leq \nu}$ (see the discussion after Definition 4.5), the vector space spanned by entries of $\mathrm{Sym}^{\leq \nu}(\mathcal{F})$ is the same as that spanned by all $\prod f_{i,j}^{s_{i,j}}$ with $0 \leq \sum s_{i,j} \leq \nu$. Set

$$\mathcal{L}_m^\nu(A) = \mathrm{diag}\left(\mathrm{Sym}^{\leq \nu}(A), \left(\frac{x+1}{x}\right) \mathrm{Sym}^{\leq \nu}(A), \cdots, \left(\frac{x+1}{x}\right)^m \mathrm{Sym}^{\leq \nu}(A) \right)$$

and

$$\tilde{\mathcal{F}} = \mathrm{diag}\left(\mathrm{Sym}^{\leq \nu}(\mathcal{F}), x\mathrm{Sym}^{\leq \nu}(\mathcal{F}), \cdots, x^m \mathrm{Sym}^{\leq \nu}(\mathcal{F}) \right).$$

We have that $\tilde{\mathcal{F}}$ is a fundamental matrix of $\sigma(Y) = \mathcal{L}_m^\nu(A)Y$, and the set of entries of $\tilde{\mathcal{F}}$ and the set of all $x^i \prod f_{i,j}^{s_{i,j}}$ with $0 \leq i \leq m$ and $0 \leq \sum s_{i,j} \leq \nu$ span the same vector space. Notice that

$$\mathrm{I}(m, I_\nu) = \{ p \in \Omega[x]_{\leq m}[X]_{\leq \nu} \mid p(\mathcal{F}) = 0 \}.$$

This implies that

$$\dim(\mathrm{I}(m, I_\nu)) = (m+1)\binom{n^2+\nu}{\nu} - \dim([\mathcal{L}_m^\nu(A)]). \tag{4}$$

As B is contained in the ν-maximal ideal I_ν, there is a nonzero $c_1 \in D$ such that for any $\varphi \in \mathcal{B}(D, c_1)$, $\varphi(B)$ is contained in a $\sigma_{\varphi(A)}$-ideal generated by some polynomials in $\bar{k}(x)[X]_{\leq \nu}$ and therefore in a ν-maximal $\sigma_{\varphi(A)}$-ideal, say $\tilde{I}_\varphi$. Using the arguments similar to the above, one has that

$$\dim(\mathrm{I}(m, \tilde{I}_\varphi)) = (m+1)\binom{n^2+\nu}{\nu} - \dim([\mathcal{L}_m^\nu(\varphi(A))]). \tag{5}$$

Let c_2 be a nonzero element in D satisfying that for any $\varphi \in \mathcal{B}(D, c_2)$,

(1) $\dim([\mathcal{L}_m^\nu(A)]) = \dim([\varphi(\mathcal{L}_m^\nu(A))])$ and $\varphi(\mathcal{L}_m^\nu(A)) = \mathcal{L}_m^\nu(\varphi(A))$;

(2) $\varphi(B)$ is linearly independent over $\bar{k}$ and $|B| = |\varphi(B)|$.

Such c_2 exists due to Lemma 4.13. Take $c = c_1 c_2$. Combining equalities (4) and (5), one sees that for any $\varphi \in \mathcal{B}(D, c)$,

$$|\varphi(B)| = |B| = \dim(\mathrm{I}(m, I)) = \dim(\mathrm{I}(m, \tilde{I}_\varphi)),$$

which implies that $\varphi(B)$ is a basis of $\mathrm{I}(m, \tilde{I}_\varphi)$. $\square$

Proof of Proposition 4.4 By Lemma 4.11, there is a positive integer μ and a basic open subset U_1 of $\mathrm{Hom}_k(D, \bar{k})$ such that μ is both a coefficient bound of ν-maximal σ_A-ideals and a coefficient bound of ν-maximal $\sigma_{\varphi(A)}$-ideals for each $\varphi \in U_1$. Let B be a basis of $\mathrm{I}(\mu, I_\nu)$ and let $\tilde{D}$ be a finitely generated D-algebra such that $B \subset \tilde{D}[x, X]$. By Lemmas 3.1 and 4.14, there is a nonzero $c \in \tilde{D}$ such that for any $\psi \in \mathcal{B}(\tilde{D}, c)$, one has that

(a) $\langle\psi(P)\rangle_{\bar{k}(x)} = \langle\psi(B)\rangle_{\bar{k}(x)}$;

(b) $\psi(B)$ is a basis of $\mathrm{I}(\mu, \tilde{I}_\psi)$ for some ν-maximal $\sigma_{\psi(A)}$-ideal $\tilde{I}_\psi$;

By Lemma 2.1, there is a basic open subset U_2 of $\mathrm{Hom}_k(D, \bar{k})$ which is included in $\{\psi|_D \,|\, \psi \in \mathcal{B}(\tilde{D}, c)\}$. Let $U = U_1 \cap U_2$. Assume that $\varphi \in U$ and $\psi \in \mathrm{Hom}_k(\tilde{D}, \bar{k})$ with $\psi|_D = \varphi$. Then $\psi(B)$ generates $\tilde{I}_\psi$, because $\mathrm{I}(\mu, \tilde{I}_\psi)$ generates $\tilde{I}_\psi$. By (a), $\psi(P)$ generates $\tilde{I}_\psi$ that is a ν-maximal $\sigma_{\psi(A)}$-ideal. The proposition then follows from the fact that $\psi(P) = \varphi(P)$ and $\psi(A) = \varphi(A)$. □

5 Difference Galois groups under specialization

This section is aimed at proving Theorem 1.3. We first present a criterion for difference Galois groups.

5.1 A criterion for difference Galois groups

Proto-Galois groups plays an essential role in algorithms for computing difference Galois groups as well as differential Galois groups. In this subsection, we shall give a necessary and sufficient condition for a proto-Galois group to be a difference Galois group. One will see that the condition given by us can be verified algorithmically. Let us recall what proto-Galois groups are.

Definition 5.1 *Let G, H be two algebraic subgroups of $\mathrm{GL}_n(\Omega)$. H is said to be a proto-group of G if they satisfy the following condition*

$$H^t \le G^\circ \le G \le H$$

where H^t denotes the algebraic subgroup of H generated by unipotent elements. In the case when G is the Galois group of $\sigma(Y) = BY$ over $\Omega(x)$ with $B \in \mathrm{GL}_n(\Omega(x))$, H is called a proto-Galois group of $\sigma(Y) = BY$ over $\Omega(x)$.

Remark 5.2 (1) *H^t is a connected algebraic subgroup of H. Hence if H is a proto-group of G, then H° is a proto-group of $G \cap H^\circ$.*

(2) *Suppose that H is a proto-group of G and $g \in \mathrm{GL}_n(\Omega)$. Generally, H is not a proto-group of gGg^{-1} any more. While, if $gGg^{-1} \subset H$ then H is still a proto-group of gGg^{-1}. This can be shown as follows. Note that if $h \in \mathrm{GL}_n(\Omega)$ is unipotent then so is ghg^{-1}. Therefore $gH^tg^{-1} = H^t$, because $gH^tg^{-1} \subset gGg^{-1} \subset H$. This implies that*

$$H^t = gH^tg^{-1} \subset gGg^{-1} \subset H.$$

(3) *Suppose that H is a proto-Galois group of $\sigma(Y) = BY$ over $\Omega(x)$ and $B \in H(\Omega(x))$. Let $\tilde{H}$ be an algebraic subgroup of H. We claim that if there is $h \in \mathrm{GL}_n(\Omega(x))$ such that $\sigma(h^{-1})Bh \in \tilde{H}(\Omega(x))$ then H is a proto-group of $\tilde{H}$. Let G be the Galois group of $\sigma(Y) = BY$ over $\Omega(x)$ satisfying that H is a proto-group of G. Proposition 1.21 of [13] implies that there is $g \in \mathrm{GL}_n(\Omega)$ such that $gGg^{-1} \subset \tilde{H}$. By (1), H is a proto-group of gGg^{-1} and then it is a proto-group of $\tilde{H}$ by the definition. This proves the claim.*

Let H be an algebraic subgroup of $\mathrm{GL}_n(\Omega)$ such that $A \in H(\Omega(x))$. It was proved in Proposition 1.21 of [13] that H is the Galois group of (1) over $\Omega(x)$ if and only if for any $g \in H(\Omega(x))$ and any proper algebraic subgroup $\tilde{H}$ of H one has that $\sigma(g^{-1})Ag \notin H(\Omega(x))$. We shall improve this criterion when H is a proto-Galois group of (1) over $\Omega(x)$.

Definition 5.3 *Suppose that ℓ is a nonnegative integer and K is a subfeild of Ω. We call $a_1, \cdots, a_m \in K(x) \setminus \{0\}$ are multiplicatively σ^ℓ-independent if they satisfy that for any $d_i \in \mathbb{Z}$ and any $f \in K(x) \setminus \{0\}$ if $\prod_{i=1}^m a_i^{d_i} = \sigma^\ell(f)/f$ then $d_1 = \cdots = d_m = 0$.*

Lemma 5.4 *Let H be a connected algebraic subgroup of $\mathrm{GL}_n(\Omega)$ and $A \in H(\Omega(x))$. Suppose that H is a proto-Galois group of $\sigma(Y) = AY$ over $\Omega(x)$, and $\{\chi_1, \cdots, \chi_l\}$ is a basis of $X(H)$. Then H is the Galois group of $\sigma(Y) = AY$ over $\Omega(x)$ if and only if $\chi_1(A), \cdots, \chi_l(A)$ are multiplicatively σ-independent.*

Proof. Suppose that H is the Galois group and there are $d_1, \cdots, d_l \in \mathbb{Z}$, not all zero, such that

$$\prod_{i=1}^{l} \chi_i^{d_i}(A) = \frac{\sigma(f)}{f}$$

for some $f \in \Omega(x) \setminus \{0\}$. Set $\chi = \prod_{i=1}^l \chi_i^{d_i}$. Then χ is a nontrivial character. Let I be the ideal in $\Omega(x)[X, 1/\det(X)]$ generated by all vanishing polynomials of H. Since $A \in H(\Omega(x))$ and H is the Galois group, I is a maximal σ_A-ideal. Furthermore as H is connected, I is a prime ideal. Let $\bar{X} = X \mod I$ and E be the field of fractions of $\Omega(x)[X, 1/\det(X)]/I$. Then $\bar{X}$ is a fundamental matrix of $\sigma(Y) = AY$ and it belongs to $H(E)$. It is easy to see that $\sigma(\chi(\bar{X}))/\chi(\bar{X}) = \sigma(f)/f$. The Galois theory tells us that $\chi(\bar{X}) = cf$ for some $c \in \Omega$. This implies that $\chi(X) - cf \in I$. As $H \subset \mathbb{V}_{\Omega(x)}(I)$, putting $X = \mathbf{1}$ in $\chi(X) - cf$ yields that $cf = 1$, and then putting $X = A$ in $\chi(X) - 1$ yields that $\chi(A) = 1$, i.e. $A \in \ker(\chi)$. Proposition 1.21 of [13] implies that $\ker(\chi) = H$. This contradicts the fact that χ is nontrivial.

Suppose on the contrary that H is not the Galois group. Due to Proposition 1.21 of [13], there is $g \in H(\Omega(x))$ and a proper algebraic subgroup $\tilde{H}$ of H such that $\sigma(g^{-1})Ag \in \tilde{H}(\Omega(x))$. By Remark 5.2, H is a proto-group of $\tilde{H}$. By Proposition 2.6 of [3], there is a nontrivial character χ of H such that $\tilde{H} \subset \ker(\chi)$. This implies that $\chi(\sigma(g^{-1})Ag) = 1$, i.e. $\chi(A) = \sigma(\chi(g))/\chi(g)$. Consequently, $\chi_1(A), \cdots, \chi_l(A)$ are multiplicatively σ-dependent. □

For a positive integer i, let A_i stand for $\sigma^{i-1}(A) \cdots \sigma(A)A$. Note that the above lemma remains true if we replace $\sigma(Y) = AY$ by $\sigma^\ell(Y) = A_\ell Y$ and "multiplicatively σ-independent" by "multiplicatively σ^ℓ-independent". As a generalization of the above lemma, we have the following proposition.

Proposition 5.5 *Let H be an algebraic subgroup of $\mathrm{GL}_n(\Omega)$ such that $A \in H(\Omega(x))$. Suppose that H is a proto-Galois group of $\sigma(Y) = AY$ over $\Omega(x)$. Then H is the Galois group of $\sigma(Y) = AY$ over $\Omega(x)$ if and only if*

(a) $A_i \notin H^\circ(\Omega(x))$ for all $1 \le i \le \ell - 1$;

(b) $\chi_1(A_\ell), \cdots, \chi_l(A_\ell)$ are multiplicatively σ^ℓ-independent,

where $\ell = [H : H^\circ]$ and $\{\chi_1, \cdots, \chi_l\}$ is a basis of $X(H^\circ)$.

Proof. Suppose that H is the Galois group. Write $A = \bar{A}\eta$ where $\bar{A} \in H^\circ(\Omega(x))$ and $\eta \in H$. Then for all $1 \leq i \leq \ell - 1$,

$$A_i = \sigma^{i-1}(\bar{A})\eta \cdots \sigma(\bar{A})\eta\bar{A}\eta = \left(\prod_{j=1}^{i} \eta^{j-1}\sigma^{i-j}(\bar{A})\eta^{1-j}\right)\eta^i \in H^\circ(\Omega(x))\eta^i,$$

because H° is normal. Thus $A_i\eta^{-i} \in H^\circ(\Omega(x))$ for all $1 \leq i \leq \ell-1$. Assume that $A_{i_0} \in H^\circ(\Omega(x))$ for some $1 \leq i_0 \leq \ell - 1$. Then $\eta^{i_0} \in H^\circ$. Let $\tilde{H} = \cup_{j=0}^{i_0-1} H^\circ\eta^j$. Then $\tilde{H}$ is a proper algebraic subgroup of H and $A \in \tilde{H}(\Omega(x))$. By Proposition 1.21 of [13], H is not the Galois group. This contradicts the assumption. So (a) holds. By Lemma 1.26 and Corollary 1.17 of [13], H° is the Galois group of $\sigma^\ell(Y) = A_\ell Y$ over $\Omega(x)$. Then (b) follows from Lemma 5.4.

Suppose that both (a) and (b) hold. We first claim that for any algebraic subgroup $\tilde{H}$ of H if there is $g \in H(\Omega(x))$ such that $\sigma(g^{-1})Ag \in \tilde{H}(\Omega(x))$ then $\tilde{H}^\circ = H^\circ$. Suppose on the contrary that there exists such an $\tilde{H}$ with $H^\circ \neq \tilde{H}^\circ$. One has that

$$\sigma^\ell(g^{-1})A_\ell g \in \tilde{H}(\Omega(x)) \cap H^\circ(\Omega(x)).$$

Write $g = h\xi$ with $h \in H^\circ(\Omega(x))$ and $\xi \in H$. Then

$$\xi^{-1}\sigma^\ell(h^{-1})A_\ell h\xi \in \tilde{H}(\Omega(x)) \cap H^\circ(\Omega(x)).$$

Notice that H is a proto-group of $\tilde{H}$ as shown in Remark 5.2. Thus H° is a proto-group of $\tilde{H} \cap H^\circ$. Furthermore, since $\tilde{H}^\circ \neq H^\circ$, $\tilde{H} \cap H^\circ$ is a proper subgroup of H°. Due to Proposition 2.6 of [3], there is a nontrivial character $\chi \in X(H^\circ)$ such that $\tilde{H} \cap H^\circ \subset \ker(\chi)$, and so

$$\chi\left(\xi^{-1}\sigma^\ell(h^{-1})A_\ell h\xi\right) = 1. \tag{6}$$

Set $\tilde{\chi} = \chi(\xi^{-1}X\xi)$. Then $\tilde{\chi}$ is still a nontrivial character of H°. Equality (6) implies that $\tilde{\chi}(A_\ell) = \sigma^\ell(\tilde{\chi}(h))/\tilde{\chi}(h)$. Write $\tilde{\chi} = \prod_{i=1}^{l} \chi_i^{d_i}$ where $d_i \in \mathbb{Z}$ and not all of them are zero. Then one has that

$$\prod_{i=1}^{l} \chi_i^{d_i}(A_\ell) = \frac{\sigma^\ell(\tilde{\chi}(h))}{\tilde{\chi}(h)}$$

which contradicts the condition (b). Hence $H^\circ = \tilde{H}^\circ$. Now assume that H is not the Galois group. Then by Proposition 1.21 of [13] there is $g \in H(\Omega(x))$ and a proper algebraic subgroup $\tilde{H}$ of H such that $\sigma(g^{-1})Ag \in \tilde{H}(\Omega(x))$. The above claim implies that $\tilde{H}^\circ = H^\circ$. Let $m = [\tilde{H} : \tilde{H}^\circ]$. Then $1 \leq m < \ell$ and

$$\sigma^m(g^{-1})A_m g \in \tilde{H}^\circ(\Omega(x)) = H^\circ(\Omega(x)). \tag{7}$$

Write $g = h\xi$ with $h \in H^\circ(\Omega(x))$ and $\xi \in H$. One easily sees that

$$\sigma^m(g)H^\circ(\Omega(x))g^{-1} = \sigma^m(h)\xi H^\circ(\Omega(x))\xi^{-1}h^{-1} \subset H^\circ(\Omega(x)). \tag{8}$$

Equalities (7) and (8) yield that $A_m \in H^\circ(\Omega(x))$, which contradicts the assumption (a). Therefore H is the Galois group. □

5.2 Proof of Theorem 1.3

Let $K \subset \Omega$ be algebraically closed. The stabilizer of an ideal or a K-vector space I in $K(x)[X, 1/\det(X)]$ is defined to be the set of elements $g \in \mathrm{GL}_n(K)$ such that $\{p(Xg)|p \in I\} = I$. The stabilizer of I will be denoted by $\mathrm{stab}(I)$ which is an algebraic subgroup of $\mathrm{GL}_n(K)$.

Lemma 5.6 *Assume that $S \subset \Omega[X, 1/\det(X)]$ is a finite set such that $\mathbb{V}_\Omega(S) = \mathrm{stab}(I_\nu)$ where I_ν is a ν-maximal σ_A-ideal in $\Omega(x)[X, 1/\det(X)]$. Let $D \subset \Omega$ be a finitely generated k-algebra with F as field of fractions such that $A \in \mathrm{GL}_n(F(x))$ and $S \subset D[X, 1/\det(X)]$. Then there is a basic open subset U of $\mathrm{Hom}_k(D, \bar{k})$ such that for each $\varphi \in U$, $\mathbb{V}_{\bar{k}}(\varphi(S))$ is the stabilizer of a ν-maximal $\sigma_{\varphi(A)}$-ideal in $\bar{k}(x)[X, 1/\det(X)]$.*

Proof. Due to Lemma 4.11, there is a coefficient bound of I_ν, say μ, and a basic open subset U_1 of $\mathrm{Hom}_k(D, \bar{k})$ such that for every $\varphi \in U_1$, μ is also a coefficient bound of ν-maximal $\sigma_{\varphi(A)}$-ideals in $\bar{k}(x)[X, 1/\det(X)]$. For such μ and φ, it is easy to verify that $\mathrm{stab}(\mathrm{I}(\mu, I_\nu)) = \mathrm{stab}(I_\nu)$ and $\mathrm{stab}(\mathrm{I}(\mu, \tilde{I})) = \mathrm{stab}(\tilde{I})$ where $\tilde{I}$ is a ν-maximal $\sigma_{\varphi(A)}$-ideal in $\bar{k}(x)[X, 1/\det(X)]$. Let B be a basis of $\mathrm{I}(\mu, I_\nu)$ and let W be a set of monomials in x and X such that $B \cup W$ forms a basis of $\Omega[x]_{\leq\mu}[X]_{\leq\nu}$ as an Ω-vector space. Let $Z = (Z_{i,j})$ be an $n \times n$ matrix of indeterminates. For every $b \in B$, write

$$b(XZ) = \sum_{q \in B} \alpha_{b,q}(Z) q + \sum_{w \in W} \beta_{b,w}(Z) w \tag{9}$$

where $\alpha_{b,q}(Z), \beta_{b,w}(Z) \in \Omega[Z]$. Let $T = \{\beta_{b,w}(X)|b \in B, w \in W\}$ where $\beta_{b,w}(X)$ denotes the polynomial obtained by replacing Z by X in $\beta_{b,w}(Z)$. The definition of stabilizers implies that $\mathbb{V}_\Omega(T) = \mathrm{stab}(\mathrm{I}(\mu, I_\nu))$. Hence $\sqrt{\langle S\rangle_\Omega} = \sqrt{\langle T\rangle_\Omega}$. Let $\tilde{D} \subset \Omega$ be a finitely generated D-algebra such that $B \subset \tilde{D}[x, X]$ and $\alpha_{b,q}, \beta_{b,w} \in \tilde{D}[Z]$ for all $b, q \in B, w \in W$. By Lemma 4.14, there is a basic open subset $\tilde{U}$ of $\mathrm{Hom}_k(\tilde{D}, \bar{k})$ such that for every $\psi \in \tilde{U}$, $\psi(B)$ is a basis of $\mathrm{I}(\mu, \tilde{I}_\psi)$ for some ν-maximal $\sigma_{\psi(A)}$-ideal $\tilde{I}_\psi$. Let c be a nonzero element in $\tilde{D}$ such that for any $\psi \in \mathcal{B}(\tilde{D}, c)$, one has that

(a) $\psi(B) \cup W$ forms a basis of $\bar{k}[x]_{\leq\mu}[X]_{\leq\nu}$ as a $\bar{k}$-vector space;

(b) $\sqrt{\langle\psi(S)\rangle_{\bar{k}}} = \sqrt{\langle\psi(T)\rangle_{\bar{k}}}$.

By Lemma 2.1, there is a basic open subset U_2 of $\mathrm{Hom}_k(D, \bar{k})$ such that

$$U_2 \subset \{\psi|_D \,|\, \psi \in \tilde{U} \cap \mathcal{B}(\tilde{D}, c)\}.$$

Set $U = U_1 \cap U_2$ and suppose that $\varphi \in U$. Let $\psi \in \tilde{U} \cap \mathcal{B}(\tilde{D}, c)$ be such that $\psi|_D = \varphi$. Since $\psi(B)$ is a basis of $\mathrm{I}(\mu, \tilde{I}_\psi)$, the application of ψ to (9) yields that $\psi(T)$ defines the stabilizer of $\mathrm{I}(\mu, \tilde{I}_\psi)$ and thus the stabilizer of $\tilde{I}_\psi$. The lemma then follows from (b) and the fact that $\psi(S) = \varphi(S)$ and $\psi(A) = \varphi(A)$. $\square$

Proposition 5.7 *Let $S \subset \Omega[X, 1/\det(X)]$ be a finite set such that $\mathbb{V}_\Omega(S)$ is the Galois group of $\sigma(Y) = AY$ over $\Omega(x)$. Let $D \subset \Omega$ be a finitely generated k-algebra with F as field of fractions such that $A \in \mathrm{GL}_n(F(x))$ and $S \subset D[X, 1/\det(X)]$. There is a basic open subset U of $\mathrm{Hom}_k(D, \bar{k})$ such that for any $\varphi \in U$, $\mathbb{V}_{\bar{k}}(\varphi(S))$ is a proto-Galois group of $\sigma(Y) = \varphi(A)Y$ over $\bar{k}(x)$.*

Proof. Let $\tilde{d}$ be the integer given in Proposition 2.5 of [3] and $d \geq \tilde{d}$. Proposition 3.8 of [3] implies that the stabilizer of any d-maximal $\sigma_{\varphi(A)}$-ideal is a proto-Galois group of $\sigma(Y) = \varphi(A)Y$ over $\bar{k}(x)$ for each $\varphi \in \mathrm{Hom}_k(D, \bar{k})$ such that $\varphi(A) \in \mathrm{GL}_n(\bar{k}(x))$. Let I be a maximal σ_A-ideal in $\Omega(x)[X, 1/\det(X)]$ satisfying that $\mathrm{stab}(I) = \mathbb{V}_\Omega(S)$. Suppose that m is a positive integer such that I is generated by some polynomials in $\Omega(x)[X]_{\leq m}$. Set

$$\nu = \max\left\{m, \tilde{d}\right\}.$$

Then I is a ν-maximal σ_A-ideal, because it is a maximal σ_A-ideal and is generated by some polynomials whose degrees are not greater than ν. Due to Lemma 5.6, there is a basic open subset U of $\mathrm{Hom}_k(D, \bar{k})$ such that for any $\varphi \in U$, $\mathbb{V}_{\bar{k}}(\varphi(S))$ is the stabilizer of a ν-maximal $\sigma_{\varphi(A)}$-ideal. Consequently, for any $\varphi \in U$, $\mathbb{V}_{\bar{k}}(\varphi(S))$ is a proto-Galois group of $\sigma(Y) = \varphi(A)Y$ over $\bar{k}(x)$. $\square$

Suppose that $a_1, \cdots, a_m \in \Omega(x) \setminus \{0\}$ and $\ell \geq 0$. Denote

$$\mathcal{Z}(a_1, \cdots, a_m; \ell) = \left\{ (d_1, \cdots, d_m) \in \mathbb{Z}^m \,\middle|\, \prod_{i=1}^m a_i^{d_i} = \frac{\sigma^\ell(f)}{f}, f \in \Omega(x) \setminus \{0\} \right\}.$$

Then $\mathcal{Z}(a_1, \cdots, a_m; \ell)$ is a finitely generated $\mathbb{Z}$-module.

Lemma 5.8 *Suppose that $a_1, \cdots, a_m \in \Omega(x) \setminus \{0\}$ and $\ell \geq 0$. Let $D \subset \Omega$ be a finitely generated k-algebra with F as field of fractions such that $a_i \in F(x)$ for all $1 \leq i \leq m$. Then there is a basic open subset U of $\mathrm{Hom}_k(D, \bar{k})$ such that for any $\varphi \in U$,*

$$\mathcal{Z}(a_1, \cdots, a_m; \ell) = \mathcal{Z}(\varphi(a_1), \cdots, \varphi(a_m); \ell).$$

Proof. For every $i = 1, \cdots, m$, write

$$a_i = \eta_i \frac{\sigma^\ell(f_i)}{f_i} \prod_{j=1}^s (x - \alpha_j)^{e_{i,j}}$$

where $\eta_i \in \mathbb{G}_m(\Omega)$, $f_i \in \mathbb{G}_m(\Omega(x))$, $e_{i,j} \in \mathbb{Z}$ and $\alpha_j \in \Omega$ with $\alpha_i - \alpha_j \notin \ell\mathbb{Z}$ if $i \neq j$. Set $\bar{a}_i = \prod_{j=1}^s (x - \alpha_j)^{e_{i,j}}$ for all $i = 1, \cdots, m$. Then Lemma 2.1 of [13] implies that $\prod_{i=1}^m a_i^{d_i} = \sigma^\ell(f)/f$ if and only if $\prod_{i=1}^m \eta_i^{d_i} = 1$ and $\prod_{i=1}^m \bar{a}_i^{d_i} = 1$. Namely,

$$\mathcal{Z}(a_1, \cdots, a_m; \ell) = \mathcal{Z}(\eta_1, \cdots, \eta_m; 0) \cap \mathcal{Z}(\bar{a}_1, \cdots, \bar{a}_m; 0).$$

Let Γ_1 be the subgroup of $\mathbb{G}_m(\Omega)$ generated by $\eta_1, \cdots, \eta_m$. Let $\tilde{D} \subset \Omega$ be a finitely generated D-algebra such that $\Gamma_1 \subset \tilde{D}$, $\alpha_j \in \tilde{D}$ and f_i belongs to the field of fractions of $\tilde{D}[x]$ for all $1 \leq i \leq m, 1 \leq j \leq s$. Let Γ_2 be the subgroup of $\mathbb{G}_a(\tilde{D})$ generated by $1, \gamma, \alpha_1, \cdots, \alpha_s$ where γ is a nonzero element in $\tilde{D}$ such that $\varphi(f_i)$ is well-defined and $\varphi(f_i) \neq 0$ for any $\varphi \in \mathcal{B}(\tilde{D}, \gamma)$. Now assume that $\varphi \in \mathcal{B}(\tilde{D}, \Gamma_1) \cap \mathcal{B}(\tilde{D}, \Gamma_2)$. One has that $\varphi(\alpha_i) - \varphi(\alpha_j) \notin \ell\mathbb{Z}$ if $i \neq j$. Therefore $\prod_{i=1}^m \varphi(a_i)^{d_i} = \sigma^\ell(f')/f'$ if and only if $\prod_{i=1}^m \varphi(\eta_i)^{d_i} = 1$ and $\prod_{i=1}^m \varphi(\bar{a}_i)^{d_i} = 1$. In other words,

$$\mathcal{Z}(\varphi(a_1), \cdots, \varphi(a_m); \ell) = \mathcal{Z}(\varphi(\eta_1), \cdots, \varphi(\eta_m); 0) \cap \mathcal{Z}(\varphi(\bar{a}_1), \cdots, \varphi(\bar{a}_m); 0).$$

Since φ is injective on Γ_1, $\mathcal{Z}(\varphi(\eta_1), \cdots, \varphi(\eta_m); 0) = \mathcal{Z}(\eta_1, \cdots, \eta_m; 0)$. At the same time, $\mathcal{Z}(\varphi(\bar{a}_1), \cdots, \varphi(\bar{a}_m); 0) = \mathcal{Z}(\bar{a}_1, \cdots, \bar{a}_m; 0)$ for both of them are equal to

$$\left\{ (d_1, \cdots, d_m) \in \mathbb{Z}^m \left| \sum_{i=1}^{m} d_i e_{i,j} = 0, \ \forall\, j = 1, \cdots, s \right. \right\}.$$

Consequently,

$$\mathcal{Z}(a_1, \cdots, a_m; \ell) = \mathcal{Z}(\varphi(a_1), \cdots, \varphi(a_m); \ell).$$

Lemma 2.1 then completes the proof. □

Corollary 5.9 *Let $a_1, \cdots, a_m, \ell$ and D be as in Lemma 5.8. Then there is a basic open subset U of $\mathrm{Hom}_k(D, \bar{k})$ such that for any $\varphi \in U$, $a_1, \cdots, a_m$ are multiplicatively σ^ℓ-independent if and only if so are $\varphi(a_1), \cdots, \varphi(a_m)$.*

Proof. Note that $a_1, \cdots, a_m$ are multiplicatively σ^ℓ-independent if and only if $\mathcal{Z}(a_1, \cdots, a_m; \ell) = \{(0, \cdots, 0)\}$. Corollary then follows from Lemma 5.8. □

Now we are ready to prove Theorem 1.3.

Proof of Theorem 1.3 Denote $G = \mathbb{V}_\Omega(S)$. Proposition 1.20 of [13] implies that there is $g \in \mathrm{GL}_n(\Omega(x))$ such that $\sigma(g^{-1})Ag \in G(\Omega(x))$. It is well-known that $\sigma(Y) = AY$ and $\sigma(Y) = \sigma(g^{-1})AgY$ have the same Galois groups. Let D' be a finitely generated D-algebra in Ω with F' as field of fractions such that $g \in \mathrm{GL}_n(F'(x))$. Then there is $c_1 \in F'$ such that for any $\varphi \in \mathcal{B}(D', c_1)$, $\varphi(\sigma(g))$, $\varphi(g)$ and $\varphi(A)$ are all well-defined and invertible. For such φ, $\sigma(Y) = \varphi(A)Y$ and $\sigma(Y) = \varphi(\sigma(g^{-1})Ag)Y$ have the same Galois groups. Hence we only need to prove the assertion for the case that $A \in G(\Omega(x))$.

Let $\mathcal{X} \subset \Omega[X, 1/\det(X)]$ be a basis of $X(G^\circ)$. Let $T \subset \Omega[X, 1/\det(X)]$ be a finite set that defines G° and let $\tilde{D} \subset \Omega$ be a finitely generated D-algebra such that $T, \mathcal{X} \subset \tilde{D}[X, 1/\det(X)]$. Set $\ell = [G : G^\circ]$. Since G is the Galois group of $\sigma(Y) = AY$ over $\Omega(x)$ and $A \in G(\Omega(x))$, Proposition 5.5 implies that $A_i \notin G^\circ(\Omega(x))$ for all $1 \leq i \leq \ell - 1$ and $\{\chi(A_\ell) | \chi \in \mathcal{X}\}$ is multiplicatively σ^ℓ-independent. Thus, for each $i = 1, \cdots, \ell - 1$, there is $p_i \in T$ such that $p_i(A_i) \neq 0$. By Proposition 5.7 and Lemma 3.2, there is a basic open subst U_1 of $\mathrm{Hom}_k(\tilde{D}, \bar{k})$ such that for any $\varphi \in U_1$, one has that

(*a*) $\mathbb{V}_{\bar{k}}(\varphi(S))$ is a proto-Galois group of $\sigma(Y) = \varphi(A)Y$ over $\bar{k}(x)$;

(*b*) $[\mathbb{V}_{\bar{k}}(\varphi(S)) : \mathbb{V}_{\bar{k}}(\varphi(S))^\circ] = [G : G^\circ]$ and $\dim(\mathbb{V}_{\bar{k}}(\varphi(S))) = \dim(G)$.

By Proposition 3.5 and Lemma 3.1, there is a basic open subset U_2 of $\mathrm{Hom}_k(\tilde{D}, \bar{k})$ such that for any $\varphi \in U_2$,

(a') $\mathbb{V}_{\bar{k}}(\varphi(T))$ is a connected algebraic group and its dimension equals $\dim(G^\circ)$;

(b') $\varphi(\mathcal{X})$ is a basis of $X(\mathbb{V}_{\bar{k}}(\varphi(T)))$;

(c') $\mathbb{V}_{\bar{k}}(\varphi(T))$ is an algebraic subgroup of $\mathbb{V}_{\bar{k}}(\varphi(S))$.

By Corollary 5.9, there is a basic open subset U_3 of $\mathrm{Hom}_k(\tilde{D}, \bar{k})$ such that for any $\varphi \in U_3$, $\{\varphi(\chi(A_\ell)) | \chi \in \mathcal{X}\}$ is multiplicatively σ^ℓ-independent. Let c_2 be a nonzero element in Ω such that for any $\varphi \in \mathcal{B}(\tilde{D}, c_2)$, $\varphi(A_i) \in \mathrm{GL}_n(\bar{k}(x))$ for all $1 \le i \le \ell$ and $\varphi(p_j(A_j)) \neq 0$ for all $1 \le j \le \ell - 1$. Set

$$U = U_1 \cap U_2 \cap U_3 \cap \mathcal{B}(\tilde{D}, c_2)$$

and assume that $\varphi \in U$. From $(a'), (c')$ and (b), $\mathbb{V}_{\bar{k}}(\varphi(T))$ is the identity component of $\mathbb{V}_{\bar{k}}(\varphi(S))$. Hence from (b'), $\varphi(\mathcal{X})$ is a basis of $X(\mathbb{V}_{\bar{k}}(\varphi(S))^\circ)$. Now since $\varphi(\chi(A_\ell)) = \varphi(\chi)(\varphi(A)_\ell)$ for all $\chi \in \mathcal{X}$, one sees that $\{\varphi(\chi)(\varphi(A)_\ell) | \chi \in \mathcal{X}\}$ is multiplicatively σ^ℓ-independent, i.e. $\{\bar{\chi}(\varphi(A)_\ell) | \bar{\chi} \in \varphi(\mathcal{X})\}$ is multiplicatively σ^ℓ-independent. On the other hand, for each $1 \le i \le \ell - 1$, one has that $\varphi(A)_i \notin \mathbb{V}_{\bar{k}(x)}(\varphi(T))$, since $\varphi(p_i)(\varphi(A)_i) = \varphi(p_i(A_i)) \neq 0$. By Proposition 5.5, $\mathbb{V}_{\bar{k}}(\varphi(S))$ is the Galois group of $\sigma(Y) = \varphi(A)Y$ over $\bar{k}(x)$. The theorem then follows from Lemma 2.1. $\square$

Remark 5.10 *Example 1.1 in the Introduction implies that the basic open subset which we construct in Theorem 1.3 may not contain all good specializations. Actually, in Example 1.1, the specializations sending t to a rational number that is not an integer are good specializations, but they are not injective on the subgroup of $\mathbb{G}_a(\mathbb{C}(t))$ generated by t and 1. So they do not belong to the basic open subset obtained by our construction. To find all good specializations, one possible way is replacing finitely generated subgroups of $\mathbb{G}_a(\Omega)$ by a finite union of cyclic groups in $\mathbb{G}_a(\Omega/\mathbb{Z})$. For instance, in Example 1.1, if we take Γ_1 to be the subgroup of $\mathbb{G}_a(\mathbb{C}(t)/\mathbb{Z})$ generated by $\bar{t}$ where $\bar{t} = t \mod \mathbb{Z}$ then $\varphi \in \mathrm{Hom}_{\mathbb{C}}(\mathbb{C}[t, 1/t], \mathbb{C})$ is injective on Γ_1 if and only if $\varphi(t) \notin \mathbb{Z}$. In this case, the specializations that are injective on both Γ_1 and Γ_2 contains all good specializations.*

6 An application

In this section, we apply Theorem 1.3 to the inverse problem in difference Galois theory, which asks which algebraic subgroups of $\mathrm{GL}_n(\Omega)$ occur as the Galois groups of (1) over $\Omega(x)$. In Chapter 3 of [13], van der Put and Singer raised the following conjecture.

Conjecture 1 *An algebraic subgroup G of $\mathrm{GL}_n(\Omega)$ is the Galois group of a linear difference equation $\sigma(Y) = AY$ over $\Omega(x)$ if and only if G/G° is cyclic.*

It was shown in Proposition 1.20 of [13] that G/G° is necessary to be cyclic if G is the Galois group of $\sigma(Y) = AY$ over $\Omega(x)$. Therefore, to prove Conjecture 1, one only needs to prove the sufficient part, which we restate as a conjecture.

Conjecture 2 *Any algebraic subgroup G of $\mathrm{GL}_n(\Omega)$ admitting the cyclic G/G° is the Galois group of a linear difference equation $\sigma(Y) = AY$ over $\Omega(x)$.*

So far, Conjecture 2 remains open except for some special cases. When $\Omega = \mathbb{C}$, for connected algebraic groups and cyclic extensions of tori, analytic proofs of Conjecture 2 were presented in Corollary 8.6 and Lemma 8.12 of [13], respectively. In Chapter 3 of the same book, an algebraic proof of Conjecture 2 was also given when Ω is any algebraically closed field of characteristic zero and G is connected. Unfortunately, there is a gap in that algebraic proof: the second assertion of Proposition 3.2 of [13] is not true. That assertion states that the Galois group G of $\sigma(Y) = AY$ over $\Omega(x)$ is a subgroup of H and $\dim(H) \leq 1+\dim(G)$, where H is the smallest algebraic subgroup of $\mathrm{GL}_n(\Omega)$ such that $A \in H(\Omega(x))$. The following example shows that the inequality $\dim(H) \leq 1 + \dim(G)$ does not always hold.

Example 6.1 *Consider*

$$\sigma(Y) = \mathrm{diag}(x+2, x+1, x)Y$$

over $\mathbb{C}(x)$. *Then* $H = \mathbb{G}_m^3(\mathbb{C})$ *is the smallest algebraic subgroup of* $\mathrm{GL}_3(\mathbb{C})$ *such that* $\mathrm{diag}(x+2, x+1, x) \in H(\mathbb{C}(x))$ *for if there are* $d_0, d_1, d_2 \in \mathbb{Z}$ *such that* $\prod_{i=0}^{2}(x+i)^{d_i} = 1$ *then* $d_0 = d_1 = d_2 = 0$. *On the other hand, the Galois group* G *of the above equation over* $\mathbb{C}(x)$ *is equal to* $\{\mathrm{diag}(c, c, c) | c \in \mathbb{G}_m(\mathbb{C})\}$, *because the above equation is equivalent to* $\sigma(Y) = \mathrm{diag}(x, x, x)Y$ *under the transformation* $\mathrm{diag}(x(x+1), x, 1)$. *One sees that*

$$\dim(G) = 1 < \dim(H) - 1 = 2.$$

Using a similar argument as that in the proof of Theorem 4.4 of [12], one can prove the following theorem.

Theorem 6.2 *If Conjecture 2 holds for* $\Omega = \mathbb{C}$, *then it holds for* Ω *to be any algebraically closed field of characteristic zero.*

Proof. Let G be an algebraic subgroup of $\mathrm{GL}_n(\Omega)$ admitting the cyclic G/G°. Suppose that G is defined by a finite set $S \subset \Omega[X, 1/\det(X)]$. Let $k \subset \Omega$ be a field finitely generated over $\mathbb{Q}$ such that $S \subset k[X, 1/\det(X)]$. Then $G(\bar{k})$ is an algebraic subgroup of $\mathrm{GL}_n(\bar{k})$ satisfying that $G(\bar{k})/G^\circ(\bar{k})$ is cyclic. We can view $\bar{k}$ as a subfield of $\mathbb{C}$. Then $G(\mathbb{C})$ is an algebraic subgroup of $\mathrm{GL}_n(\mathbb{C})$ admitting the cyclic $G(\mathbb{C})/G^\circ(\mathbb{C})$. Hence $G(\mathbb{C})$ is the Galois group of $\sigma(Y) = AY$ over $\mathbb{C}(x)$ for some $A \in \mathrm{GL}_n(\mathbb{C}(x))$. Let $D \subset \mathbb{C}$ be a finitely generated k-algebra with F as field of fractions such that $A \in \mathrm{GL}_n(F(x))$. Theorem 1.3 implies that there is $\varphi \in \mathrm{Hom}_k(D, \bar{k})$ such that $\mathbb{V}_{\bar{k}}(\varphi(S))$ is the Galois group of $\sigma(Y) = \varphi(A)Y$ over $\bar{k}(x)$. Namely, $G(\bar{k})$ is the Galois group of $\sigma(Y) = \varphi(A)Y$ over $\bar{k}(x)$, because $S = \varphi(S)$. Now we view $\bar{k}$ as a subfield of Ω. Let I be a maximal $\sigma_{\varphi(A)}$-ideal of $\bar{k}(x)[X, 1/\det(X)]$ such that $G(\bar{k}) = \mathrm{stab}(I)$ and let $\tilde{I}$ be the ideal in $\Omega(x)[X, 1/\det(X)]$ generated by I. Due to Proposition 2.4 of [1], $\tilde{I}$ is a maximal $\sigma_{\varphi(A)}$-ideal. One can verify that $\mathrm{stab}(\tilde{I}) = G$. So G is the Galois group of $\sigma(Y) = \varphi(A)Y$ over $\Omega(x)$. □

The above theorem together with Corollary 8.6 and Lemma 8.12 of [13] implies the following.

Corollary 6.3 *Conjecture 2 holds when* G *is a connected affine algebraic group or a cyclic extension of a torus.*

References

[1] Chatzidakis, Z.; Hardouin, C. and Singer, M.F. On the definitions of difference Galois groups. *Model theory with applications to algebra and analysis.* Vol. 1, 73-109, London Math. Soc. Lecture Note Ser., 349, Cambridge Univ. Press, Cambridge (2008).

[2] Feng, R. Hrushovski's algorithm for computing the Galois group of a linear differential equation. *Adv. in Appl. Math.* 65, 1-37 (2015).

[3] Feng, R. On the computation of the Galois groups of linear difference equations, *Math of Computation* (2017). DOI:10.1090/mcom/3232.

[4] Fried, D.M. and Jarden, M., *Field arithmetic*, Springer-Verlag, Berlin (1986).

[5] Goldman, L. Specialization and Picard-Vessiot theory. *Trans. Amer. Math. Soc.* 85, 327356 (1957).

[6] Humphreys, J.E. *Linear Algebraic Groups*, Springer-Verlag New York (1981).

[7] Hrushovski, E. Computing the Galois group of a linear differential equation. *Banach Center Publ.* 58, 97-138 (2002).

[8] Lang, S. *Fundamentals of Diophantine geometry.* Springer-Verlag, New York (1983).

[9] Maier, A. A difference version of Nori's theorem. *Math. Ann.* 359, no.3-4, 759-784 (2014).

[10] Petkovšek, M. Hypergeometric solutions of linear recurrences with polynomial coefficients, *J. Symbol. Comput.*,11,1-22 (1998).

[11] Serre, J.P. *Lectures on the Mordell-Weil theorem.* Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt. With a foreword by Brown and Serre. Third edition. Aspects of Mathematics. Friedr. Vieweg & Sohn, Braunschweig (1997).

[12] Singer, M.F. Moduli of linear differential equations on the Riemann sphere with fixed Galois groups. *Pacific J. Math.* 160, no. 2, 343-395 (1993).

[13] van der Put, M. and Singer, M.F., *Galois Theory of Difference Equations*, LNM1666, Springer-Verlag, Berlin (1997).

[14] Völklein H., *Groups as Galois groups: An introduction*, Cambridge Studies in Advanced Mathematics, 53. Cambridge University Press, Cambridge (1996).

[15] Zariski, O.; Samuel, P. *Commutative algebra.* Vol. II. Reprint of the 1960 edition. Graduate Texts in Mathematics, Vol. 29. Springer-Verlag, New York-Heidelberg (1975).