TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 374, Number 1, January 2021, Pages 61–96
https://doi.org/10.1090/tran/8143
Article electronically published on October 20, 2020

DIFFERENCE GALOIS GROUPS UNDER SPECIALIZATION

RUYONG FENG

Abstract. We present a difference analogue of a result given by Hrushovski on differential Galois groups under specialization. Let k be an algebraically closed field of characteristic zero and let $\mathbb{X}$ be an irreducible affine algebraic variety over k. Consider the linear difference equation

$$\sigma(Y) = AY,$$

where $A \in \mathrm{GL}_n(k(\mathbb{X})(x))$ and σ is the shift operator $\sigma(x) = x+1$. Assume that the Galois group G of the above equation over $\overline{k(\mathbb{X})}(x)$ is defined over $k(\mathbb{X})$, i.e., the vanishing ideal of G is generated by a finite set $S \subset k(\mathbb{X})[X, 1/\det(X)]$. For a $\mathbf{c} \in \mathbb{X}$, denote by $v_{\mathbf{c}}$ the map from $k[\mathbb{X}]$ to k given by $v_{\mathbf{c}}(f) = f(\mathbf{c})$ for any $f \in k[\mathbb{X}]$. We prove that the set of $\mathbf{c} \in \mathbb{X}$ satisfying that $v_{\mathbf{c}}(A)$ and $v_{\mathbf{c}}(S)$ are well-defined and the affine variety in $\mathrm{GL}_n(k)$ defined by $v_{\mathbf{c}}(S)$ is the Galois group of $\sigma(Y) = v_{\mathbf{c}}(A)Y$ over $k(x)$ is Zariski dense in $\mathbb{X}$.

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

1. Introduction

Let K be a function field of one variable over $\mathbb{Q}$ and let $\mathcal{L}$ be a linear differential operator with coefficients in the differential field $(K(t), \mathrm{d}/\mathrm{d}t)$. For a place $\mathfrak{p}$ in K, $\Sigma_{\mathfrak{p}}$ denotes its residue field, and $\mathcal{L}_{\mathfrak{p}}$ denotes the differential operator over $\Sigma_{\mathfrak{p}}(x)$ obtained by applying $\mathfrak{p}$ to the coefficients of $\mathcal{L}$. In [14], Hrushovski proved that for many places $\mathfrak{p}$ in K, the Galois group of $\mathcal{L}(y) = 0$ over $\bar{K}(t)$ specializes precisely to the Galois group of $\mathcal{L}_{\mathfrak{p}}(y) = 0$ over $\bar{\Sigma}_{\mathfrak{p}}(t)$. As a corollary, he proved a function field analogue of Grothendieck-Katz's conjecture on p-curvatures. The reader is referred to [15] for this conjecture and to ([5],[21]) for its generalizations. In particular, Di Vizio in [5] presented a positive answer of a q-analogue of Groethendieck-Katz's conjecture, i.e., an analogue statement for q-difference equations. The difference analogue of the Grothendieck-Katz's conjecture is not true (see a counterexample on page 58 of [26]). But one can still ask whether Hrushovski's result holds true for linear difference equations. The goal of this paper is to provide an affirmative answer to this question. Let us start with an example.

Example 1.1. Let $\mathbb{X} = \mathbb{A}^1(\mathbb{C})$ and denote $\mathbb{C}(\mathbb{X}) = \mathbb{C}(t)$. Consider

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

Received by the editors December 31, 2018, and, in revised form, August 26, 2019, October 29, 2019, November 29, 2019, January 1, 2020, and January 25, 2020.

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

Key words and phrases. Linear difference equations, difference Galois groups, specializations.

The author was supported in part by NSFC Grants No.11771433 and No.11688101.

where σ is the 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 [26]), $\mathbb{G}_m^3(\overline{\mathbb{C}(t)})$ 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 $c \in \mathbb{A}^1(\mathbb{C}) \setminus \{0\}$. By van der Put-Singer's method again, one sees that the Galois group of $\sigma(Y) = v_c(A)Y$ 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, the vanishing ideal of $\mathbb{G}_m^3(\mathbb{C})$ is generated by $S = \{X_{1,2}, X_{1,3}, X_{2,1}, X_{2,3}, X_{3,1}, X_{3,2}\}$. For any $c \in \mathbb{C}$, the variety in $\mathrm{GL}_3(\mathbb{C})$ defined by $v_c(S)$ is $\mathbb{G}_m^3(\mathbb{C})$.

This example implies that on the one hand there are infinitely many "good" $c \in \mathbb{A}^1(\mathbb{C})$ such that the Galois group of $\sigma(Y) = v_c(A)Y$ over $\mathbb{C}(x)$ is equal to $\mathbb{G}_m^3(\mathbb{C})$; on the other hand these good c do not form an open subset of $\mathbb{A}^1(\mathbb{C})$ in the sense of Zariski topology. Thus other algebraic structures rather than Zariski open sets are necessary to describe these good c. For this purpose, we introduce basic open subsets of the corresponding variety (see Definition 2.1).

Throughout this paper, k denotes an algebraically closed field of characteristic zero. Let $\mathbb{X}$ be an irreducible affine algebraic variety over k. $k[\mathbb{X}]$ (resp., $k(\mathbb{X})$) denotes the ring (resp., field) of regular (resp., rational) functions on $\mathbb{X}$, and $\overline{k(\mathbb{X})}(x)$ stands for the field of rational functions in x with coefficients in $\overline{k(\mathbb{X})}$, the algebraic closure of $k(\mathbb{X})$. Over $\overline{k(\mathbb{X})}(x)$, we can define a shift operator σ as the following: $\sigma(x) = x + 1$ and $\sigma(c) = c$ for all $c \in \overline{k(\mathbb{X})}$. Consider the linear difference equation

$$\sigma(Y) = AY, \tag{1.1}$$

where Y is an n-vector of indeterminates and $A \in \mathrm{GL}_n(k(\mathbb{X})(x))$. Let $X = (X_{i,j})$ be an $n \times n$ matrix of indeterminates and let $\overline{k(\mathbb{X})}(x)[X, 1/\det(X)]$ denote the ring over $\overline{k(\mathbb{X})}(x)$ generated by entries of X and $1/\det(X)$. The main result of this paper is as follows.

Theorem 1.2. *Suppose that G is the Galois group of $\sigma(Y) = AY$ over $\overline{k(\mathbb{X})}(x)$ and the vanishing ideal of G is generated by a finite set $S \subset k[\mathbb{X}][X]$. Then there is a basic open subset U of $\mathbb{X}$ such that for any $\mathbf{c} \in U$, the variety in $\mathrm{GL}_n(k)$ defined by $v_{\mathbf{c}}(S)$ is the Galois group of $\sigma(Y) = v_{\mathbf{c}}(A)Y$ over $k(x)$.*

We prove in Theorem 2.16 that every basic open subset of $\mathbb{X}$ is Zariski dense in $\mathbb{X}$. Theorem 1.2 together with Theorem 2.16 then gives a positive answer to the question posed at the beginning of this paper. Similar to the Hrushovski's treatment in [14], the proof of the above theorem relies on the computation of difference Galois groups and other algorithmic aspects of linear difference equations, which are developed in [9, 20, 26], etc. Our way to compute difference Galois groups is via the Picard-Vessiot theory. Recall that there is another way, the so-called Tannakian category method, to construct Galois groups. Based on this category approach, a similar result was obtained in [2] for differential Galois groups of quantum completely integrable systems.

Theorem 1.2 can be applied to van der Put-Singer's conjecture concerning the inverse problem in difference Galois theory. Let G be an algebraic subgroup of $\mathrm{GL}_n(k)$. Theorem 1.2 allows one to conclude that if $G(\overline{k(\mathbb{X})})$ is the Galois group of a linear difference equation over $\overline{k(\mathbb{X})}(x)$, then G is the Galois group of a linear difference equation with coefficients in $k(x)$. This enables us to reduce van der Put-Singer's conjecture to the case where the field of constants is the field of complex numbers. Note that in [18] the specialization technique is also applied to realize

a semisimple, simply-connected linear algebraic group defined over $\mathbb{F}_q$ as a Galois group of a Frobenuis difference equation.

Recently, parameterized Galois theories were developed in [4, 6, 11, 19], etc., for linear difference (or differential) equations with parameters admitting actions of the derivations or endomorphisms. These parameterized Galois theories provide a powerful tool to measure the differential (or difference) dependencies among solutions of the corresponding equations and have found many applications in combinatorics and the theory of special functions. However, the present paper focuses on linear difference equations with parameters where the derivations or endomorphisms act trivially. These equations can be regarded as a family of linear difference equations parameterized by an irreducible affine variety, and the Galois groups then measure the algebraic relations among solutions at generic points. The main result of this paper tells us for what specializations of the parameters these algebraic relations among solutions are preserved precisely. From Example 5.11, one may see that there are specializations which destroy the algebraic relations completely.

The rest of this paper is organized as follows. In Section 2, we introduce the notion of basic open subsets of an irreducible affine variety $\mathbb{X}$ over k and present the properties of these subsets. Sections 3 and 4 present some preliminary results for the proof of Theorem 1.2. In Section 3, we deal with algebraic groups defined over $k(\mathbb{X})$. Precisely, we prove that for almost all $\mathbf{c} \in \mathbb{X}$, $v_{\mathbf{c}}$ preserves the structure of algebraic groups and is bijective from the characters of a connected algebraic group G to those of $G_{\mathbf{c}}$, the specialized group of G. In Section 4, we consider σ-ideals. We show that given a ν-maximal σ-ideal of $\overline{k(\mathbb{X})}(x)[X, 1/\det(X)]$ (see Definition 4.2) generated by a finite set $S \subset k[\mathbb{X}][X]$, there is a basic open subset U of $\mathbb{X}$ such that $v_{\mathbf{c}}(S)$ generates a ν-maximal σ-ideal of $k(x)[X, 1/\det(X)]$ for all $\mathbf{c} \in U$. We prove Theorem 1.2 in Section 5 and apply this theorem to the inverse problem in difference Galois theory in Section 6.

Notation. When P is an element in $k[\mathbb{X}][X, 1/\det(X)]$ or a matrix with entries in $k[\mathbb{X}]$, we also use $P(\mathbf{c})$ to denote $v_{\mathbf{c}}(P)$. All varieties in this paper will be affine.

k, L	algebraically closed fields of characteristic zero
$\mathbb{G}_a$ (resp., $\mathbb{G}_m$)	additive (resp., multiplicative) group
$\mathbb{X}, \mathbb{Y}$	affine algebraic varieties over k
$k[\mathbb{X}]$	the ring of regular functions on $\mathbb{X}$
$k(\mathbb{X})$	the field of rational functions on $\mathbb{X}$
$p_{\mathbb{Y}/\mathbb{X}}$	the projection from $\mathbb{Y}$ to $\mathbb{X}$ induced by $k[\mathbb{X}] \subset k[\mathbb{Y}]$
$v_{\mathbf{c}}$	the map from $k[\mathbb{X}]$ to k given by $v_{\mathbf{c}}(f) = f(\mathbf{c})$
$\Gamma, \tilde{\Gamma}$	finitely generated subgroups of $\mathbb{G}_a(\overline{k(\mathbb{X})})$ or $\mathbb{G}_m(\overline{k(\mathbb{X})})$
$\tilde{U}, U, U_1, U_2, \cdots$	basic open subsets of $\mathbb{X}$ or $\mathbb{Y}$
$\mathbb{X}_f$	$\{\mathbf{c} \in \mathbb{X} \mid f(\mathbf{c}) \neq 0\}$, where $f \neq 0$
G	an algebraic subgroup of $\mathrm{GL}_n(\overline{k(\mathbb{X})})$ (or $\mathrm{GL}_n(k)$)
G°	the identity component of G
$\boldsymbol{\chi}(G)$	the group of characters of G
$G(\overline{k(\mathbb{X})}(x))$	the set of $\overline{k(\mathbb{X})}(x)$-points of G
$\mathbf{Z}(f)$	the set of integer zeros of f
X (resp., Z)	$n \times n$ matrix with indeterminate entries $X_{i,j}$ (resp., $Z_{i,j}$)
$L[X]_{\leq d}$	the set of polynomials in $L[X]$ with total degree $\leq d$

2. Basic open subsets of $\mathbb{X}$

In this section, we shall introduce an algebraic structure of $\mathbb{X}$ which is Zariski dense in $\mathbb{X}$ and consists of good specializations. Throughout this section, we fix an algebraic closed field L containing $k(\mathbb{X})$ and all k-algebras will be in L. Assume that Γ is a finitely generated subgroup of $\mathbb{G}_a(L)$ or $\mathbb{G}_m(L)$. Denote by $\mathbb{Y}$ the variety over k associated to $k[\mathbb{X}][\Gamma]$, the $k[\mathbb{X}]$-algebra in L generated by Γ and denote by $p_{\mathbb{Y}/\mathbb{X}}$ the morphism from $\mathbb{Y}$ to $\mathbb{X}$ induced by the inclusion $k[\mathbb{X}] \subset k[\mathbb{X}][\Gamma]$. Note that $k[\mathbb{Y}] = k[\mathbb{X}][\Gamma]$ and $\mathbb{Y}$ can be identified with the set of all k-homomorphisms from $k[\mathbb{X}][\Gamma]$ to k. Under this identification, for $\mathbf{c} \in \mathbb{Y}$, we use $v_{\mathbf{c}}$ to denote the k-homomorphism corresponding to $\mathbf{c}$. One sees that for $f \in k[\mathbb{X}][\Gamma]$, $v_{\mathbf{c}}(f)$ is equal to the value at $\mathbf{c}$ of f viewed as a regular function on $\mathbb{Y}$, i.e., $v_{\mathbf{c}}(f) = f(\mathbf{c})$. We are interested in those $\mathbf{c} \in \mathbb{Y}$ whose induced maps $v_{\mathbf{c}}$ are injective on Γ. Set

$$\mathcal{B}(\mathbb{X}, \Gamma) = p_{\mathbb{Y}/\mathbb{X}}\left(\{\mathbf{c} \in \mathbb{Y} | v_{\mathbf{c}} \text{ is injective on } \Gamma\}\right). \tag{2.1}$$

Definition 2.1. A basic open subset of $\mathbb{X}$ is defined to be the intersection of finitely many subsets of $\mathbb{X}$ of the form $\mathcal{B}(\mathbb{X}, \Gamma)$. When Γ is the subgroup of $\mathbb{G}_a(L)$ generated by a single $g \in L$, we will abbreviate $\mathcal{B}(\mathbb{X}, \Gamma)$ to $\mathbb{X}_g$.

Recall that when $\Gamma \subset k[\mathbb{X}]$, one can take $\mathbb{Y} = \mathbb{X}$ and then $p_{\mathbb{Y}/\mathbb{X}}$ is the identity map and $\mathcal{B}(\mathbb{X}, \Gamma) = \{\mathbf{c} \in \mathbb{X} | v_{\mathbf{c}} \text{ is injective on } \Gamma\}$. The reason that Γ is not restricted to $k[\mathbb{X}]$ is as follows. On the one hand, the extension of $k[\mathbb{X}]$ is necessary in some cases such as the defining field of characters of G° (see Example 5.10). On the other hand, if we restrict Γ to $k[\mathbb{X}]$ in Definition 2.1, then we do not know whether basic open sets are preserved by the projection map, although they do if they are only defined by additive groups (see Lemma 5A.1 of [14]). Two lemmas below imply that basic open sets without the above restriction are preserved by the projection map in some sense. The first one is due to Proposition 9 on page 34 of [16].

Lemma 2.2. *Assume that $\mathbb{Y}$ is a variety over k associated to a finitely generated $k[\mathbb{X}]$-algebra in L. For any $\tilde{f} \in k[\mathbb{Y}] \setminus \{0\}$, there is a nonzero $f \in k[\mathbb{X}]$ such that*

$$\mathbb{X}_f \subset p_{\mathbb{Y}/\mathbb{X}}(\mathbb{Y}_{\tilde{f}}).$$

Lemma 2.3. *Suppose that $\mathbb{Y}$ is as in Lemma 2.2 and U is a basic open subset of $\mathbb{Y}$. Then $p_{\mathbb{Y}/\mathbb{X}}(U)$ contains a basic open subset of $\mathbb{X}$.*

Proof. It suffices to show the assertion with $U = \mathcal{B}(\mathbb{Y}, \Gamma)$, where Γ is a finitely generated subgroup of $\mathbb{G}_a(L)$ or $\mathbb{G}_m(L)$. Assume that $k[\mathbb{Y}]$ is generated by a finite subset T of $L \setminus \{0\}$ as a $k[\mathbb{X}]$-algebra. Let $\tilde{\Gamma}$ be generated by $\Gamma \cup T$ as a group of the same type as Γ. Then $k[\mathbb{Y}][\Gamma] \subset k[\mathbb{X}][\tilde{\Gamma}] = k[\mathbb{Y}][\tilde{\Gamma}]$. Let $\tilde{\mathbb{Y}}$ and $\mathbb{Y}'$ be the varieties over k associated to $k[\mathbb{X}][\tilde{\Gamma}]$ and $k[\mathbb{Y}][\Gamma]$, respectively. Since $\tilde{\Gamma} \subset k[\tilde{\mathbb{Y}}]$, $\mathcal{B}(\tilde{\mathbb{Y}}, \tilde{\Gamma}) = \{\mathbf{c} \in \tilde{\mathbb{Y}} | v_{\mathbf{c}} \text{ is injective on } \tilde{\Gamma}\}$. Then by definition, one has that

$$\mathcal{B}(\mathbb{X}, \tilde{\Gamma}) = p_{\tilde{\mathbb{Y}}/\mathbb{X}}(\{\mathbf{c} \in \tilde{\mathbb{Y}} | v_{\mathbf{c}} \text{ is injective on } \tilde{\Gamma}\}) = p_{\tilde{\mathbb{Y}}/\mathbb{X}}(\mathcal{B}(\tilde{\mathbb{Y}}, \tilde{\Gamma})). \tag{2.2}$$

Similarly, $U = \mathcal{B}(\mathbb{Y}, \Gamma) = p_{\mathbb{Y}'/\mathbb{Y}}(\mathcal{B}(\mathbb{Y}', \Gamma))$. Furthermore, as the morphism $p_{\tilde{\mathbb{Y}}/\mathbb{Y}'}$ is induced by the inclusion $k[\mathbb{Y}][\Gamma] \subset k[\tilde{\mathbb{Y}}]$, for any $\mathbf{c} \in \tilde{\mathbb{Y}}$ and any $f \in \Gamma$, $v_{p_{\tilde{\mathbb{Y}}/\mathbb{Y}'}(\mathbf{c})}(f) = v_{\mathbf{c}}(f)$. This implies that if $v_{\mathbf{c}}$ is injective on Γ, then so is $v_{p_{\tilde{\mathbb{Y}}/\mathbb{Y}'}(\mathbf{c})}$. Hence $p_{\tilde{\mathbb{Y}}/\mathbb{Y}'}(\mathcal{B}(\tilde{\mathbb{Y}}, \Gamma)) \subset \mathcal{B}(\mathbb{Y}', \Gamma)$ and then

$$p_{\tilde{\mathbb{Y}}/\mathbb{X}}(\mathcal{B}(\tilde{\mathbb{Y}}, \Gamma)) = p_{\mathbb{Y}/\mathbb{X}}(p_{\mathbb{Y}'/\mathbb{Y}}(p_{\tilde{\mathbb{Y}}/\mathbb{Y}'}(\mathcal{B}(\tilde{\mathbb{Y}}, \Gamma)))) \subset p_{\mathbb{Y}/\mathbb{X}}(p_{\mathbb{Y}'/\mathbb{Y}}(\mathcal{B}(\mathbb{Y}', \Gamma))) = p_{\mathbb{Y}/\mathbb{X}}(U). \tag{2.3}$$

Finally as $\mathcal{B}(\tilde{\mathbb{Y}},\tilde{\Gamma})\subset\mathcal{B}(\tilde{\mathbb{Y}},\Gamma)$, the formulas (2.2) and (2.3) yield that

$$\mathcal{B}(\mathbb{X},\tilde{\Gamma})=p_{\tilde{\mathbb{Y}}/\mathbb{X}}(\mathcal{B}(\tilde{\mathbb{Y}},\tilde{\Gamma}))\subset p_{\tilde{\mathbb{Y}}/\mathbb{X}}(\mathcal{B}(\tilde{\mathbb{Y}},\Gamma))\subset p_{\mathbb{Y}/\mathbb{X}}(U).$$

□

Remark 2.4. We should remark that the set $\mathcal{B}(\mathbb{X},\Gamma)$ given in Definition 2.1 is nothing else but a subset of a basic gr-open subset of $\mathrm{Spec}(k[\mathbb{X}])$ introduced by Hrushovski in [14]. Let G be a commutative algebraic group scheme over $k[\mathbb{X}]$ and let Γ be a finitely generated subgroup of $G(k[\mathbb{X}])$. The set of primes $\mathfrak{p}\in\mathrm{Spec}(k[\mathbb{X}])$ satisfying that the canonical map $k[\mathbb{X}]\to k[\mathbb{X}]/\mathfrak{p}$ is injective on Γ is called a basic gr-open subset of $\mathrm{Spec}(k[\mathbb{X}])$, denoted by $\mathrm{W}(G,\Gamma)$. When $G=\mathbb{G}_a$ or $G=\mathbb{G}_m$, one has that

$$\mathcal{B}(\mathbb{X},\Gamma)=\mathrm{W}(G,\Gamma)\cap\max(k[\mathbb{X}]),$$

where $\max(k[\mathbb{X}])$ denotes the set of maximal ideals of $k[\mathbb{X}]$. Hrushovski proved that if k is a number field and $\dim\mathbb{X}=1$, then $\mathrm{W}(G,\Gamma)$ is infinite (see Lemma 5A.10 of [14]). 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 [17] or Section 11.1 of [23]). The case when $G=\mathbb{G}_a$ was proved in Lemma 5A.4 of [14]. 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. A similar claim was also made by Serre in Section 11.1 of [23] for the case when k is a number field and $k(\mathbb{X})$ is a purely transcendental extension of k. To be complete, we shall provide a detailed proof for the case when $G=\mathbb{G}_m$. Moreover, we remove the restrictions on k and $k[\mathbb{X}]$.

Now we turn to showing that basic open subsets of $\mathbb{X}$ are not empty. We first show that $\mathcal{B}(\mathbb{X},\Gamma)$ is not empty. From (2.1), it suffices to prove that the set $\{\mathbf{c}\in\mathbb{Y}|v_{\mathbf{c}}\text{ is injective on }\Gamma\}$ is not empty. Furthermore, since $\Gamma\subset k[\mathbb{Y}]$, one sees that $\mathcal{B}(\mathbb{Y},\Gamma)=\{\mathbf{c}\in\mathbb{Y}|v_{\mathbf{c}}\text{ is injective on }\Gamma\}$. So it suffices to prove that $\mathcal{B}(\mathbb{Y},\Gamma)\neq\emptyset$. Due to the Noetherian normalization lemma, it is reasonable to make the following assumption.

Convention 2.5. Suppose that $\mathbb{Y}\subset k^m$ and denote $k[\mathbb{Y}]=k[\eta_1,\cdots,\eta_m]$, where $\eta_1,\cdots,\eta_l\in L$ are algebraically independent over k and $\eta_{l+i}\in L$ is integral over $k[\eta_1,\cdots,\eta_l]$. Set $\boldsymbol{\eta}=(\eta_1,\cdots,\eta_m)$ and $\boldsymbol{\eta}_l=(\eta_1,\cdots,\eta_l)$.

To prove $\mathcal{B}(\mathbb{Y},\Gamma)\neq\emptyset$, we need a generalization of Hilbert sets (see Section 12.1 of [10]). Let $\tilde{k}\subset k$ be a field finitely generated over $\mathbb{Q}$ such that the minimal polynomial of η_{l+i} over $k(\boldsymbol{\eta}_l)$ has coefficients in $\tilde{k}[\boldsymbol{\eta}_l]$ for all $i=1,\cdots,m-l$. Assume that $\mathbf{f}$ is a finite set of polynomials in $\tilde{k}[\boldsymbol{\eta},z]$ irreducible over $\tilde{k}(\boldsymbol{\eta})$ and monic in z. Suppose that $g\in\tilde{k}[\boldsymbol{\eta}]\setminus\{0\}$, and $\mathbf{d}=(d_1,\cdots,d_l)\in\mathbb{Z}^l$ with positive d_i.

Notation 2.6. $\mathcal{H}_{\tilde{k},\mathbb{Y}}(\mathbf{d},\mathbf{f},g)$ denotes the set of $\mathbf{c}=(c_1,\cdots,c_m)\in\mathbb{Y}$ satisfying that

(1) for $1\leq i\leq l$, $[\tilde{k}(c_1,\cdots,c_i):\tilde{k}(c_1,\cdots,c_{i-1})]\geq d_i$, and
(2) $g(\mathbf{c})\neq 0$, and
(3) for each $f\in\mathbf{f}$, $f(\mathbf{c},z)$ is irreducible over $\tilde{k}(\mathbf{c})$.

We call such $\mathcal{H}_{\tilde{k},\mathbb{Y}}(\mathbf{d},\mathbf{f},g)$ a $\tilde{k}$-Hilbert set of $\mathbb{Y}$.

Assume that K is a field of characteristic zero, $\mathbf{T}=\{T_1,\cdots,T_m\}$, and $\mathbf{Y}=\{y_1,\cdots,y_n\}$. For $g\in K[\mathbf{T}]\setminus\{0\}$ and $h_1,\ldots,h_s\in K(\mathbf{T})[\mathbf{Y}]$ irreducible over $K(\mathbf{T})$, denote by $H_K(h_1,\ldots,h_s;g)$ the set of all $\mathbf{c}\in K^m$ with $g(\mathbf{c})\neq 0$ and

$h_1(\mathbf{c},\mathbf{Y}),\cdots,h_s(\mathbf{c},\mathbf{Y})$ defined and irreducible in $K[\mathbf{Y}]$. In Section 12.1 of [10], a set of the form $H_K(h_1,\ldots,h_s;g)$ is called a Hilbert subset of K^m and the field K is called a hilbertian field if for every positive integer m, each Hilbert subset of K^m is nonempty. One sees that $\mathcal{H}_{\tilde{k},\mathbb{Y}}((1,\cdots,1),\emptyset,g)=\mathbb{Y}_g$ and if $\mathbb{Y}=\tilde{k}^l$, then $\mathcal{H}_{\tilde{k},\mathbb{Y}}((1,\cdots,1),\mathbf{f},g)$ is a usual Hilbert set. Furthermore, one can easily verify that

$$\mathcal{H}_{\tilde{k},\mathbb{Y}}(\mathbf{d}_1,\mathbf{f}_1,g_1)\cap\mathcal{H}_{\tilde{k},\mathbb{Y}}(\mathbf{d}_2,\mathbf{f}_2,g_2)=\mathcal{H}_{\tilde{k},\mathbb{Y}}(\bar{\mathbf{d}},\mathbf{f}_1\cup\mathbf{f}_2,g_1g_2),$$

where the ith coordinate of $\bar{\mathbf{d}}$ is equal to the maximum of the ith coordinates of $\mathbf{d}_1$ and $\mathbf{d}_2$ for all $i=1,\cdots,l$. From this, one sees that the intersection of finitely many $\tilde{k}$-Hilbert sets is a $\tilde{k}$-Hilbert set. Recall that if $\tilde{k}$ is replaced by an Omega-free PAC field K, Lemma 27.2.1 on page 660 of [10] implies that $\mathcal{H}_{K,\mathbb{Y}}((1,\cdots,1),\mathbf{f},g)$ is not empty. We shall prove that every $\tilde{k}$-Hilbert set is nonempty.

Lemma 2.7. *Assume that K is a hilbertian field and $\tilde{K}$ is a finite extension of K. For any positive integer d, there is α algebraic over K satisfying that $[K(\alpha):K]=d$ and $K(\alpha)\cap\tilde{K}=K$.*

Proof. Consider the polynomial $z^d-t\in K[z,t]$ which is irreducible over $\tilde{K}(t)$. Since K is hilbertian, there is $c\in K$ such that z^d-c is irreducible in $\tilde{K}[z]$ by Corollary 1.8 on page 10 of [27]. Let α be a root of $z^d-c=0$ in $\bar{K}$. Then $[K(\alpha):K]=d$. If $K(\alpha)\cap\tilde{K}\neq K$, then $[K(\alpha):K(\alpha)\cap\tilde{K}]<d$. This implies that z^d-c is reducible over $\tilde{K}$, a contradiction. Hence $K(\alpha)\cap\tilde{K}=K$. □

Proposition 2.8. $\mathcal{H}_{\tilde{k},\mathbb{Y}}(\mathbf{d},\mathbf{f},g)\neq\emptyset$.

Proof. Suppose that $\mathbf{f}=\{f_1,\cdots,f_s\}$. For each $i=1,\cdots,s$, let $\alpha_i\in L$ satisfy that $f_i(\alpha_i)=0$ and let $\beta_i\in L$ be such that $\tilde{k}(\boldsymbol{\eta},\alpha_i)=\tilde{k}(\boldsymbol{\eta}_l,\beta_i)$. We may choose β_i to be integral over $\tilde{k}[\boldsymbol{\eta}_l]$. Let $\tilde{f}_i$ be the polynomial in $\tilde{k}[y_1,\cdots,y_l,z]$ irreducible over $\tilde{k}$ and monic in z such that $\tilde{f}_i(\boldsymbol{\eta}_l,\beta_i)=0$. Then

$$\begin{aligned}\deg_z(\tilde{f}_i)&=[\tilde{k}(\boldsymbol{\eta}_l,\beta_i):\tilde{k}(\boldsymbol{\eta}_l)]=[\tilde{k}(\boldsymbol{\eta}_l,\beta_i):\tilde{k}(\boldsymbol{\eta})][\tilde{k}(\boldsymbol{\eta}):\tilde{k}(\boldsymbol{\eta}_l)]\\&=[\tilde{k}(\boldsymbol{\eta},\alpha_i):\tilde{k}(\boldsymbol{\eta})][\tilde{k}(\boldsymbol{\eta}):\tilde{k}(\boldsymbol{\eta}_l)]=\deg_z(f_i)[\tilde{k}(\boldsymbol{\eta}):\tilde{k}(\boldsymbol{\eta}_l)].\end{aligned}$$

Assume that $\beta_i=h_i(\boldsymbol{\eta},\alpha_i)/r(\boldsymbol{\eta}_l)$ where $h_i\in\tilde{k}[y_1,\cdots,y_m,z]$ and $r\in\tilde{k}[y_1,\cdots,y_l]$. Let k' be a finite extension of $\tilde{k}$ such that all factors of the $\tilde{f}_i$ irreducible over k' are absolutely irreducible. Using Lemma 2.7 repeatedly, we have $c_1,\cdots,c_l\in k$ such that $\tilde{k}(c_1,\cdots,c_l)\cap k'=\tilde{k}$ and for each $j=1,\cdots,l$,

$$[\tilde{k}(c_1,\cdots,c_j):\tilde{k}(c_1,\cdots,c_{j-1})]=d_j.$$

Write $\mathbf{c}_l=(c_1,\cdots,c_l)$. We claim that all $\tilde{f}_i$ are irreducible over $\tilde{k}(\mathbf{c}_l)$. Otherwise, assume that $\tilde{f}_i$ is reducible over $\tilde{k}(\mathbf{c}_l)$ for some i and q is one of its irreducible factors. Then q is the product of some irreducible factors of $\tilde{f}_i$ in $k'[y_1,\cdots,y_l,z]$. Therefore the coefficients of q are all in $k'\cap\tilde{k}(\mathbf{c}_l)$, i.e., $q\in\tilde{k}[y_1,\cdots,y_l,z]$. This contradicts the irreducibility of $\tilde{f}_i$. This proves our claim. It is easy to see that all $\tilde{f}_i(y_1+c_1,\cdots,y_l+c_l,z)$ are also irreducible over $\tilde{k}(\mathbf{c}_l)$. As $\tilde{k}(\mathbf{c}_l)$ is a finite extension of the hilbertian field $\tilde{k}$, by Lemma 12.2.2 on page 224 of [10], there is a Hilbert set $H\subset\tilde{k}^l$ such that for each $\mathbf{a}\in H$, all $\tilde{f}_i(\mathbf{a}+\mathbf{c}_l,z)$ are irreducible over $\tilde{k}(\mathbf{c}_l)$. Let $\tilde{g}$ be the norm of g down to $\tilde{k}(\boldsymbol{\eta}_l)$. Since g is integral over $\tilde{k}[\boldsymbol{\eta}_l]$ and $\tilde{k}[\boldsymbol{\eta}_l]$ is integrally closed, $\tilde{g}\in\tilde{k}[\boldsymbol{\eta}_l]$. One sees that for any $\mathbf{c}\in\mathbb{Y}$ if $\tilde{g}(\mathbf{c})\neq0$, then $g(\mathbf{c})\neq0$. Let $\tilde{H}$ be the set of $\mathbf{a}\in H$ satisfying that $\tilde{g}(\mathbf{a}+\mathbf{c}_l)r(\mathbf{a}+\mathbf{c}_l)\neq0$. Then $\tilde{H}\neq\emptyset$ as H is

Zariski dense. Now let $\mathbf{b} = (b_1, \cdots, b_m) \in \mathbb{Y}$ satisfy that $(b_1, \cdots, b_l) = \mathbf{a} + \mathbf{c}_l$ for some $\mathbf{a} \in \tilde{H}$. Such $\mathbf{b}$ exists because $\eta_{l+1}, \cdots, \eta_m$ are integral over $k[\boldsymbol{\eta}_l]$. Let $\bar{\alpha}_i \in k$ be a zero of $f_i(\mathbf{b}, z)$. Set $\bar{\beta}_i = h_i(\mathbf{b}, \bar{\alpha}_i)/r(\mathbf{a} + \mathbf{c}_l)$. Then $\bar{\beta}_i$ is a zero of $\tilde{f}_i(\mathbf{a} + \mathbf{c}_l, z)$ and since $\tilde{f}_i(\mathbf{a} + \mathbf{c}_l, z)$ is irreducible over $\tilde{k}(\mathbf{c}_l)$,

$$\begin{aligned}\deg_z(\tilde{f}_i(\mathbf{a} + \mathbf{c}_l, z)) &= [\tilde{k}(\mathbf{a} + \mathbf{c}_l, \bar{\beta}_i) : \tilde{k}(\mathbf{a} + \mathbf{c}_l)] = [\tilde{k}(\mathbf{c}_l, \bar{\beta}_i) : \tilde{k}(\mathbf{c}_l)] \\ &\leq [\tilde{k}(\mathbf{b}, \bar{\alpha}_i) : \tilde{k}(\mathbf{c}_l)] = [\tilde{k}(\mathbf{b}, \bar{\alpha}_i) : \tilde{k}(\mathbf{b})][\tilde{k}(\mathbf{b}) : \tilde{k}(\mathbf{c}_l)] \\ &\leq \deg_z(f_i(\mathbf{b}, z))[\tilde{k}(\boldsymbol{\eta}) : \tilde{k}(\boldsymbol{\eta}_l)] = \deg_z(\tilde{f}_i).\end{aligned}$$

The last inequality holds because $\bar{\alpha}_i$ is a zero of $f_i(\mathbf{b}, z)$ and $\mathbf{b} \in \mathbb{Y}$ with $\boldsymbol{\eta}$ as a generic point. At the same time, because $\deg_z(\tilde{f}_i(\mathbf{a} + \mathbf{c}_l, z)) = \deg_z(\tilde{f}_i)$, one has that $\deg_z(f_i(\mathbf{b}, z)) = [\tilde{k}(\mathbf{b}, \bar{\alpha}_i) : \tilde{k}(\mathbf{b})]$. This implies that $f_i(\mathbf{b}, z)$ is irreducible over $\tilde{k}(\mathbf{b})$. It is obvious that for each $j = 1, \cdots, l$,

$$[\tilde{k}(b_1, \cdots, b_j) : \tilde{k}(b_1, \cdots, b_{j-1})] = [\tilde{k}(c_1, \cdots, c_j) : \tilde{k}(c_1, \cdots, c_{j-1})] \geq d_j.$$

Therefore $\mathbf{b} \in \mathcal{H}_{\tilde{k},\mathbb{Y}}(\mathbf{d}, \mathbf{f}, g)$. □

Corollary 2.9. *Suppose that $h \in \tilde{k}[\boldsymbol{\eta}][z]$ is monic and of degree ≥ 1 in z. Then there exists a $\tilde{k}$-Hilbert set V of $\mathbb{Y}$ such that for any $\mathbf{c} \in V$, $h(\mathbf{c}, z) = 0$ has a root in $\tilde{k}(\mathbf{c})$ if and only if $h = 0$ has a root in $\tilde{k}(\boldsymbol{\eta})$.*

Proof. Decompose h into irreducible polynomials in $\tilde{k}(\boldsymbol{\eta})[z]$, say $h_1, h_2, \cdots, h_s$. Pick a suitable nonzero $g \in \tilde{k}[\boldsymbol{\eta}]$ such that for each $i = 1, \cdots, s$, $g^{\deg_z(h_i)} h_i = f_i(gz)$ for some $f_i \in \tilde{k}[\boldsymbol{\eta}, z]$ being monic in z. One sees that f_i is irreducible over $\tilde{k}(\boldsymbol{\eta})$ and, moreover, h_i has a zero in $\tilde{k}(\boldsymbol{\eta})$ if and only if so does f_i. Let $\mathbf{f} = \{f_1, \cdots, f_s\}$ and $V = \mathcal{H}_{\tilde{k},\mathbb{Y}}((1, \cdots, 1), \mathbf{f}, g)$. Suppose that $\mathbf{c} \in V$. Then $f_i(\mathbf{c}, z)$ has a zero in $\tilde{k}(\mathbf{c})$ if and only if so does $h_i(\mathbf{c}, z)$. For an irreducible polynomial in z, it has a zero in its coefficient field if and only if it is of degree one. The corollary then follows from the fact that $h_i(\mathbf{c}, z)$ is irreducible and

$$\deg_z(h_i(\mathbf{c}, z)) = \deg_z(f_i(\mathbf{c}, z)) = \deg_z(f_i) = \deg_z(h_i).$$

□

Due to Lemma 5A.3 and Remark 5A.3R of [14], one has the following proposition.

Proposition 2.10. *Suppose that Γ is a finitely generated subgroup of $\mathbb{G}_a(\tilde{k}[\boldsymbol{\eta}])$. Then there is an l-tuple of positive integers $\mathbf{d}$ such that $\mathcal{H}_{\tilde{k},\mathbb{Y}}(\mathbf{d}, \emptyset, 1) \subset \mathcal{B}(\mathbb{Y}, \Gamma)$.*

Proof. We have that $\{\eta_1, \cdots, \eta_l\}$ is a transcendental basis of $\overline{k(\mathbb{Y})}/k$. Let V be the $\tilde{k}$-vector space in $\tilde{k}[\boldsymbol{\eta}]$ spanned by Γ. As Γ is finitely generated, V is of finite dimension. By Remark 5A.3R of [14], there are positive integers $d_1, \cdots, d_l$ such that for any $\tilde{k}$-homomorphism $h : \tilde{k}[\boldsymbol{\eta}] \to \tilde{k}^a \subset k$, if

$$[\tilde{k}(h(\eta_1), \ldots, h(\eta_i)) : \tilde{k}(h(\eta_1), \ldots, h(\eta_{i-1}))] \geq d_i \tag{2.4}$$

for every $i = 1, \cdots, l$, then h is injective on V. Here $\tilde{k}^a$ denotes the algebraic closure of $\tilde{k}$. Now let $\mathbf{c} \in \mathcal{H}_{\tilde{k},\mathbb{Y}}((d_1, \cdots, d_l), \emptyset, 1)$. Then the restriction of $v_{\mathbf{c}}$ on $\tilde{k}[\boldsymbol{\eta}]$ is a $\tilde{k}$-homomorphism from $\tilde{k}[\boldsymbol{\eta}]$ to k and $v_{\mathbf{c}}(\eta_i) = c_i$, where $\mathbf{c} = (c_1, \cdots, c_m)$. By

definition (see Notation 2.6 (1)),

$$[\tilde{k}(v_{\mathbf{c}}(\eta_1),\cdots,v_{\mathbf{c}}(\eta_i)):\tilde{k}(v_{\mathbf{c}}(\eta_1),\cdots,v_{\mathbf{c}}(\eta_{i-1}))]=[\tilde{k}(c_1,\cdots,c_i):\tilde{k}(c_1,\cdots,c_{i-1})]\geq d_i,$$

i.e., the restriction of $v_{\mathbf{c}}$ satisfies the conditions (2.4). The above statement following from Remark 5A.3R of [14] then implies that $v_{\mathbf{c}}$ is injective on V and thus on Γ. In other words, $\mathbf{c}\in\mathcal{B}(\mathbb{Y},\Gamma)$. □

Next, we are going to deal with the case that Γ is a finitely generated subgroup of $\mathbb{G}_m(\tilde{k}[\boldsymbol{\eta}])$. It has been claimed on page 154 of [23] and in Discussion 5A.8 (4) of [14] that the proof of Néron's theorem can be applied to proving that $\mathcal{B}(\mathbb{Y},\Gamma)\neq\emptyset$. The readers are referred to Section 6 in Chapter 9 of [17] or Section 11.1 of [23] for the proof of Néron's theorem. Here we present a detailed proof of the claim made by Hrushovski and Serre. Let $K\subset L$ 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

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

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 $\mathbb{G}_m(K)$. Moreover, we have the following proposition.

Proposition 2.12. *Suppose that K is a field finitely generated over $\mathbb{Q}$ and Γ is 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. We first prove the case that K is a number field. 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 verify that $\ker(\varphi)=\mathrm{rad}_K(\Gamma)\cap\mathcal{O}_K^\times$ and so the kernel 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.

Now assume that K is transcendental over $\mathbb{Q}$. Due to the results on page 99 of [28], 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 $1\leq j\leq m$. Similarly, consider the group homomorphism $\psi:\mathrm{rad}_K(\Gamma)\to\mathbb{Z}^\ell$ defined by

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

One can check that $\ker(\psi)=\tilde{\mathbb{Q}}\cap\mathrm{rad}_K(\Gamma)$ where $\tilde{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$ in K. The image of ψ is a subgroup of $\mathbb{Z}^\ell$ and so it is finitely generated. Therefore to show that $\mathrm{rad}_K(\Gamma)$ is finitely generated, it suffices to show that $\ker(\psi)$ is finitely generated. Let $R=\tilde{\mathbb{Q}}[a_1,1/a_1,\cdots,a_m,1/a_m]$ and let ϕ be a $\tilde{\mathbb{Q}}$-homomorphism from R to $\bar{\mathbb{Q}}$. 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 $\gamma\in\ker(\psi)$, 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 $\ker(\psi) \subset \mathrm{rad}_E(\tilde{\Gamma})$. Since E is a number field, $\mathrm{rad}_E(\tilde{\Gamma})$ is finitely generated as we have already proved. So $\ker(\psi)$ is finitely generated. □

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 2.13. Let $K = \mathbb{Q}(\xi_2, \xi_3, \cdots)$ where ξ_i is a primitive ith root of unity, and let $\Gamma = \{1\}$. Then $\mathrm{rad}_K(\Gamma)$ contains all ξ_i, and thus it is not finitely generated.

For a positive integer ℓ and a subgroup Γ of $\mathbb{G}_m(\tilde{k}[\boldsymbol{\eta}])$, denote

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

Lemma 2.14. *Suppose that ℓ is a positive integer and Γ is a finitely generated subgroup of $\mathbb{G}_m(\tilde{k}[\boldsymbol{\eta}])$ which is radical in $\tilde{k}(\boldsymbol{\eta})$. Then there exists a $\tilde{k}$-Hilbert set V of $\mathbb{Y}$ such that for any $\mathbf{c} \in V$, $v_{\mathbf{c}}(\Gamma)$ is a subgroup of $\mathbb{G}_m(\tilde{k}(\mathbf{c}))$ and $v_{\mathbf{c}}(\Gamma_\ell) = v_{\mathbf{c}}(\Gamma)_\ell$. Moreover, $v_{\mathbf{c}}(\Gamma)$ is finitely generated.*

Proof. Let h be a polynomial in $\tilde{k}[\boldsymbol{\eta}][z]$ such that

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

Then $h = 0$ has no roots in $\tilde{k}(\boldsymbol{\eta})$, because Γ is radical in $\tilde{k}(\boldsymbol{\eta})$. By Corollary 2.9, there exists a $\tilde{k}$-Hilbert set $\tilde{V}$ of $\mathbb{Y}$ such that for any $\mathbf{c} \in \tilde{V}$, $h(\mathbf{c}, z) = 0$ has no root in $\tilde{k}(\mathbf{c})$. Set $g = b_1 \cdots b_N$ where $b_1, \cdots, b_N$ are generators of Γ. Let $V = \tilde{V} \cap \mathbb{Y}_g$ and $\mathbf{c} \in V$. Then $b_i(\mathbf{c}) \neq 0$ for all $1 \leq i \leq N$ and thus the restriction of $v_{\mathbf{c}}$ on Γ is a group homomorphism. This implies that $v_{\mathbf{c}}(\Gamma)$ is a finitely generated subgroup of $\mathbb{G}_m(\tilde{k}(\mathbf{c}))$ because Γ is finitely generated. In addition, note that $\mathbf{c} \in \tilde{V}$ and

$$z^\ell - 1 = h(\mathbf{c}, z) \prod_{c \in \Gamma_\ell} (z - v_{\mathbf{c}}(c)).$$

One sees that $v_{\mathbf{c}}(\Gamma)_\ell$, the set of all roots of $z^\ell - 1 = 0$ in $v_{\mathbf{c}}(\Gamma)$, equals $\{v_{\mathbf{c}}(c) | c \in \Gamma_\ell\}$ and the latter set is nothing else but $v_{\mathbf{c}}(\Gamma_\ell)$. □

Proposition 2.15. *Suppose that Γ is a finitely generated subgroup of $\mathbb{G}_m(\tilde{k}[\boldsymbol{\eta}])$. There exists a $\tilde{k}$-Hilbert set V of $\mathbb{Y}$ such that $V \subset \mathcal{B}(\mathbb{Y}, \Gamma)$.*

Proof. Set $\tilde{\Gamma} = \mathrm{rad}_{\tilde{k}(\boldsymbol{\eta})}(\Gamma)$. Then due to Proposition 2.12, $\tilde{\Gamma}$ is finitely generated. Let $q \in \tilde{k}[\boldsymbol{\eta}_l]$ be a nonzero element such that $\tilde{\Gamma} \subset \tilde{k}[\boldsymbol{\eta}, 1/q]$. We will first show the proposition for $\mathbb{Y}_q$ and $\tilde{\Gamma}$.

Let T be the torsion group of $\tilde{\Gamma}$ and let ℓ be an integer greater than 1 and divided by $|T|$. By Lemma 2.14, there exists a $\tilde{k}$-Hilbert set V_1 of $\mathbb{Y}_q$ such that for any $\mathbf{a} \in V_1$, $v_{\mathbf{a}}(\tilde{\Gamma})$ is a finitely generated subgroup of $\mathbb{G}_m(\tilde{k}(\mathbf{a}))$ and $v_{\mathbf{a}}(\tilde{\Gamma}_\ell) = v_{\mathbf{a}}(\tilde{\Gamma})_\ell$. Suppose that $\{b_1 = 1, b_2, \cdots, b_\nu\}$ is a set of representatives of $\tilde{\Gamma}/\tilde{\Gamma}^\ell$. Corollary 2.9 implies that there exists a $\tilde{k}$-Hilbert set V_2 of $\mathbb{Y}_q$ such that for any $\mathbf{a} \in V_2$, $z^\ell - v_{\mathbf{a}}(b_i) = 0$ has a root in $\tilde{k}(\mathbf{a})$ if and only if $z^\ell - b_i = 0$ has a root in $\tilde{k}(\boldsymbol{\eta})$. Since $\tilde{\Gamma}$ is radical in $\tilde{k}(\boldsymbol{\eta})$, all roots of $z^\ell - b_i = 0$ in $\tilde{k}(\boldsymbol{\eta})$ are in $\tilde{\Gamma}$ and then $z^\ell - b_i = 0$ has a root in $\tilde{k}(\boldsymbol{\eta})$ only if $i = 1$. Thus for each $\mathbf{a} \in V_2$, $z^\ell - v_{\mathbf{a}}(b_i) = 0$ has a root in $\tilde{k}(\mathbf{a})$ only if $i = 1$. We claim that $V_1 \cap V_2 \subset \mathcal{B}(\mathbb{Y}_q, \tilde{\Gamma})$. Suppose that $\mathbf{a} \in V_1 \cap V_2$. Let $I = v_{\mathbf{a}}^{-1}(1) \cap \tilde{\Gamma}$. Then I is a finitely generated subgroup of $\tilde{\Gamma}$. We shall show that $I = I^\ell$ and I is free. This will imply $I = 1$ because $\ell > 1$, and thus $v_{\mathbf{a}}$ is injective on

$\tilde{\Gamma}$, i.e., $\mathbf{a} \in \mathcal{B}(\mathbb{Y}_q, \tilde{\Gamma})$. Since $|T|$ divides ℓ, if $I = I^\ell$, then 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 $v_{\mathbf{a}}(\bar{w})^{-\ell} = v_{\mathbf{a}}(b_i)$. In other words, $v_{\mathbf{a}}(\bar{w})^{-1}$ is a root of $z^\ell - v_{\mathbf{a}}(b_i) = 0$ in $\tilde{k}(\mathbf{a})$. The assumption on $\mathbf{a}$ indicates that $b_i = 1$. This implies $w = \bar{w}^\ell$ and then $v_{\mathbf{a}}(\bar{w})^\ell = 1$, i.e., $v_{\mathbf{a}}(\bar{w}) \in v_{\mathbf{a}}(\tilde{\Gamma})_\ell$. As $v_{\mathbf{a}}(\tilde{\Gamma}_\ell) = v_{\mathbf{a}}(\tilde{\Gamma})_\ell$, there is $u \in \tilde{\Gamma}_\ell$ such that $v_{\mathbf{a}}(\bar{w}) = v_{\mathbf{a}}(u)$. For such u, $\bar{w}u^{-1} \in I$. As $u^\ell = 1$, $w = \bar{w}^\ell = (\bar{w}u^{-1})^\ell \in I^\ell$. Therefore $I = I^\ell$. This proves our claim.

Now assume that $V_1 \cap V_2 = \mathcal{H}_{\tilde{k},\mathbb{Y}_q}(\mathbf{d}, \{\tilde{f}_1, \cdots, \tilde{f}_s\}, \tilde{g})$ where $\tilde{f}_i \in \tilde{k}[\boldsymbol{\eta}, 1/q][z]$ is irreducible over $\tilde{k}(\boldsymbol{\eta})$ and monic in z, and $\tilde{g} \in \tilde{k}[\boldsymbol{\eta}, 1/q]$. For each $i = 1, \cdots, s$, there are positive integers d_i, e_i and $f_i \in \tilde{k}[\boldsymbol{\eta}, z]$ irreducible over $\tilde{k}(\boldsymbol{\eta})$ and monic in z such that $q^{d_i}\tilde{f}_i = f_i(q^{e_i}z)$. Set $\mathbf{f} = \{f_1, \cdots, f_s\}$. Let μ be a positive integer such that $q^\mu \tilde{g} \in \tilde{k}[\boldsymbol{\eta}]$ and set $g = q^{\mu+1}\tilde{g}$. One then has that $\mathcal{H}_{\tilde{k},\mathbb{Y}}(\mathbf{d}, \mathbf{f}, g) \subset \mathcal{B}(\mathbb{Y}, \Gamma)$. □

Theorem 2.16. *Every basic open subset of $\mathbb{X}$ is Zariski dense.*

Proof. We first show that every basic open subset of $\mathbb{X}$ is not empty. Assume that $\Gamma_1, \cdots, \Gamma_s$ are subgroups of $\mathbb{G}_a(L)$ and $\Gamma_{s+1}, \cdots, \Gamma_\ell$ are subgroups of $\mathbb{G}_m(L)$. Let $\mathbb{Y}_i$ and $\tilde{\mathbb{Y}}$ be the varieties associated to $k[\boldsymbol{\eta}, \Gamma_i]$ and $k[\boldsymbol{\eta}, \bigcup_{i=1}^\ell \Gamma_i]$, respectively. By definition, one has that $\mathcal{B}(\mathbb{X}, \Gamma_i) = p_{\mathbb{Y}_i/\mathbb{X}}(\mathcal{B}(\mathbb{Y}_i, \Gamma_i))$ and $p_{\tilde{\mathbb{Y}}/\mathbb{Y}_i}(\mathcal{B}(\tilde{\mathbb{Y}}, \Gamma_i)) \subset \mathcal{B}(\mathbb{Y}_i, \Gamma_i)$. Applying $p_{\mathbb{Y}_i/\mathbb{X}}$ to the latter inclusion yields that

$$p_{\mathbb{Y}_i/\mathbb{X}}(p_{\tilde{\mathbb{Y}}/\mathbb{Y}_i}(\mathcal{B}(\tilde{\mathbb{Y}}, \Gamma_i))) \subset p_{\mathbb{Y}_i/\mathbb{X}}(\mathcal{B}(\mathbb{Y}_i, \Gamma_i)) = \mathcal{B}(\mathbb{X}, \Gamma_i).$$

Therefore to show that $\bigcap_{i=1}^\ell \mathcal{B}(\mathbb{X}, \Gamma_i) \neq \emptyset$, it suffices to show that $\bigcap_{i=1}^\ell \mathcal{B}(\tilde{\mathbb{Y}}, \Gamma_i) \neq \emptyset$. The latter assertion follows from Propositions 2.10 and 2.15 where $\tilde{k}$ is taken to be the field finitely generated over $\mathbb{Q}$ such that the Γ_i are in $\tilde{k}[\boldsymbol{\eta}]$.

Suppose that U is a basic open subset of $\mathbb{X}$ and U is not Zariski dense, i.e., there is a nonzero $g \in k[\mathbb{X}]$ which vanishes on U. By Definition 2.1, $v_{\mathbf{c}}(g) = g(\mathbf{c}) \neq 0$ for all $\mathbf{c} \in \mathbb{X}_g$. So $U \cap \mathbb{X}_g = \emptyset$. However by Definition 2.1 $U \cap \mathbb{X}_g$ is a basic open subset of $\mathbb{X}$ and thus it is not empty, a contradiction. □

The following two lemmas will be used later.

Lemma 2.17. *Suppose that $f \in k[\mathbb{X}][z]$. There is a finitely generated subgroup Γ of $\mathbb{G}_a(\overline{k(\mathbb{X})})$ such that for any $\mathbf{c} \in \mathcal{B}(\mathbb{X}, \Gamma)$, one has that $\mathbf{Z}(f) = \mathbf{Z}(f(\mathbf{c}, z))$.*

Proof. Let $\alpha_1, \cdots, \alpha_\ell$ be all zeros of f in $\overline{k(\mathbb{X})} \setminus \mathbb{Z}$ and let a be the leading coefficient of f. Set Γ to be the subgroup of $\mathbb{G}_a(\overline{k(\mathbb{X})})$ generated by $1, a, \alpha_1, \cdots, \alpha_\ell$ and let $\mathbb{Y}$ be the variety associated to $k[\mathbb{X}][\alpha_1, \cdots, \alpha_\ell]$. Suppose that $\mathbf{c} \in \mathcal{B}(\mathbb{X}, \Gamma)$. By the definition of basic open subsets, $\mathbf{c}$ can be extended to a point $\tilde{\mathbf{c}} \in \mathcal{B}(\mathbb{Y}, \Gamma)$. One sees that the $\mathbf{Z}(f) \subset \mathbf{Z}(f(\tilde{\mathbf{c}}, z))$ and $v_{\tilde{\mathbf{c}}}(\alpha_i) \notin \mathbb{Z}$ for all $1 \leq i \leq \ell$. Therefore $\mathbf{Z}(f) = \mathbf{Z}(f(\tilde{\mathbf{c}}, z)) = \mathbf{Z}(f(\mathbf{c}, z))$. □

In the following, for a matrix M with entries in $k[\mathbb{X}]$, the rank of M is defined to be the rank of M regarded as a matrix over $k(\mathbb{X})$.

Lemma 2.18. *Assume that M is a matrix in $k[\mathbb{X}]^{\ell \times n}$. Then there is a nonzero $g \in k[\mathbb{X}]$ such that for any $\mathbf{c} \in \mathbb{X}_g$, $\operatorname{rank}(M) = \operatorname{rank}(M(\mathbf{c}))$.*

Proof. Clearly, $\operatorname{rank}(M(\mathbf{c})) \leq \operatorname{rank}(M)$ for all $\mathbf{c} \in \mathbb{X}$. Let $r = \operatorname{rank}(M)$. If $r = 0$, there is nothing to prove. Suppose that $r > 0$ and g is a nonzero $r \times r$ minor of M. Suppose $\mathbf{c} \in \mathbb{X}_g$. It is easy to see that $v_{\mathbf{c}}(g)$ is an $r \times r$ minor of $M(\mathbf{c})$. Since $v_{\mathbf{c}}(g) \neq 0$, $\operatorname{rank}(M(\mathbf{c})) \geq r$. This implies that $r = \operatorname{rank}(M(\mathbf{c}))$. □

3. Algebraic groups under specialization

Assume that G is an algebraic subgroup of $\mathrm{GL}_n(\overline{k(\mathbb{X})})$ defined over $k[\mathbb{X}]$, i.e., the vanishing ideal of G is generated by a finite subset S in $k[\mathbb{X}][X]$. Let $\mathfrak{X}$ be a basis of $\boldsymbol{\chi}(G^\circ)$ as a free Abelian group. We further assume that every character in $\mathfrak{X}$ is represented by an element in $k[\mathbb{X}][X, 1/\det(X)]$. Recall that G° is also defined over $k[\mathbb{X}]$ (see (7.3) on page 210 of [13]). We shall use $G_{\mathbf{c}}$ to denote the variety in $\mathrm{GL}_n(k)$ defined by $v_{\mathbf{c}}(S)$ for $\mathbf{c} \in \mathbb{X}$. In this section, we shall prove that there is a nonzero $c \in k[\mathbb{X}]$ such that if $\mathbf{c} \in \mathbb{X}_c$, then $G_{\mathbf{c}}$ is an algebraic subgroup of $\mathrm{GL}_n(k)$ satisfying that $\dim(G_{\mathbf{c}}) = \dim(G)$ and $v_{\mathbf{c}}(\mathfrak{X})$ is a basis of $\boldsymbol{\chi}(G^\circ_{\mathbf{c}})$. Note that when G is commutative, the results of Lemma 3.3 and Proposition 3.5 have already appeared in [14] (see Example 5A.6 and Lemma 5.11, respectively).

Let us start with a few remarks which follow from the application of Remark 5A.5 of [14] to polynomial equalities with coefficients in $k(\mathbb{X})$.

Remark 3.1. (1) If $\tilde{S} \subset k[\mathbb{X}][X]$ is a finite set defining G, then there is a nonempty open subset U of $\mathbb{X}$ such that $G_{\mathbf{c}}$ is defined by $v_{\mathbf{c}}(\tilde{S})$ for all $\mathbf{c} \in U$. Thus the notation $G_{\mathbf{c}}$ makes sense. To see this, note that $\tilde{S}$ and S define the same variety if and only if they generate the same radical ideal, i.e., for every $P \in S, \tilde{P} \in \tilde{S}$, there are $\alpha_{P,\tilde{Q}}, \beta_{\tilde{P},Q} \in k(\mathbb{X})[X]$ such that

$$P^{d_P} = \sum_{\tilde{Q} \in \tilde{S}} \alpha_{P,\tilde{Q}} \tilde{Q}, \ \tilde{P} = \sum_{Q \in S} \beta_{\tilde{P},Q} Q,$$

where d_P is a positive integer. Any nonempty open subset of $\mathbb{X}$ on which all $\alpha_{P,\tilde{Q}}, \beta_{\tilde{P},Q}$ are well-defined will be the set as required. The open subsets in (2) and (3) below can be obtained similarly.

(2) $G_{\mathbf{c}}$ is an algebraic group for all $\mathbf{c}$ being in some nonempty open subset of $\mathbb{X}$. By Exercise 5 on page 57 of [13], for a variety H in $\mathrm{GL}_n(\overline{k(\mathbb{X})})$, H is an algebraic group if and only if $I_n \in H$ and H is closed under taking products. The latter condition can be described as follows: For each $P \in S$, there are $\alpha_{P,Q}, \beta_{P,Q} \in k(\mathbb{X})[X, Z, 1/\det(XZ)]$ such that

$$P(XZ) = \sum_{Q \in S} \alpha_{P,Q} Q(X) + \sum_{Q \in S} \beta_{P,Q} Q(Z).$$

Likewise, if χ is a character of G, then $v_{\mathbf{c}}(\chi)$ is a character of $G_{\mathbf{c}}$ for all $\mathbf{c}$ being in some nonempty open subset of $\mathbb{X}$.

(3) Suppose that H and $\tilde{H}$ are two varieties defined over $k[\mathbb{X}]$ and $H \cap \tilde{H} = \emptyset$. Then $H_{\mathbf{c}} \cap \tilde{H}_{\mathbf{c}} = \emptyset$ for all $\mathbf{c}$ being in some nonempty open subset of $\mathbb{X}$. Note that $H \cap \tilde{H} = \emptyset$ if and only if there are polynomials P and Q in the vanishing ideal of H and $\tilde{H}$, respectively, such that $P + Q = 1$.

We can view G as a family of algebraic varieties $G_{\mathbf{c}}$ in $\mathrm{GL}_n(k)$ parameterized by $\mathbb{X}$. More precisely, suppose that $\mathbb{X} \subset k^m$ and $\boldsymbol{\eta}$ is a generic point of $\mathbb{X}$. Denote

$$J = \{P \in k[y_1, \cdots, y_m, X, 1/\det(X)] \,|\, \forall\, \mathbf{b} \in G, P(\boldsymbol{\eta}, \mathbf{b}) = 0\}.$$

Let $\mathbb{Y} \subset k^m \times \mathrm{GL}_n(k)$ be the variety defined by J. Then $\mathbb{Y}$ is a variety over k of dimension $\dim(\mathbb{X}) + \dim(G)$. Define

$$\begin{array}{ccccccccc} \pi_1: & \mathbb{Y} & \longrightarrow & \mathbb{X} & & \pi_2: & \mathbb{Y} & \longrightarrow & \mathrm{GL}_n(k) \\ & (\mathbf{c}, \mathbf{b}) & \longrightarrow & \mathbf{c} & & & (\mathbf{c}, \mathbf{b}) & \longrightarrow & \mathbf{b} \end{array}.$$

One sees that $G = \pi_2(\pi_1^{-1}(\boldsymbol{\eta}))$. Note that $\pi_2(\pi_1^{-1}(\mathbf{c}))$ is the variety in $\mathrm{GL}_n(k)$ defined by $\{P(\mathbf{c}, X, 1/\det(X))|P \in J\}$.

Proposition 3.2. *There is a nonempty open subset U of $\mathbb{X}$ such that for any $\mathbf{c} \in U$, $G_{\mathbf{c}}$ is an algebraic subgroup of $\mathrm{GL}_n(k)$ with dimension $\dim(G)$ and*

$$[G_{\mathbf{c}} : G_{\mathbf{c}}^{\circ}] = [G : G^{\circ}] = \ell.$$

Proof. Note that $\{P(\boldsymbol{\eta}, X, 1/\det(X))|P \in J\}$ also defines G. The discussion in Remark 3.1(1) implies that there is a nonempty open subset $\tilde{U}$ of $\mathbb{X}$ such that $G_{\mathbf{c}} = \pi_2(\pi_1^{-1}(\mathbf{c}))$ for any $\mathbf{c} \in \tilde{U}$. Hence it suffices to prove the proposition for $\pi_2(\pi_1^{-1}(\mathbf{c}))$. Let $G_1, \cdots, G_\ell$ be all irreducible components of G. Let D be a finitely generated $k[\mathbb{X}]$-algebra in $\overline{k(\mathbb{X})}$ such that each G_i is defined over D, i.e., the vanishing ideal of each G_i in $\overline{k(\mathbb{X})}[X, 1/\det(X)]$ is generated by finitely many polynomials in $D[X, 1/\det(X)]$. Let $\tilde{\mathbb{X}}$ be the variety over k associated to D. By Lemma 2.2, for each nonempty open subset $\tilde{V}$ of $\tilde{\mathbb{X}}$, there is a nonempty open subset V of $\mathbb{X}$ such that $V \subset p_{\tilde{\mathbb{X}}/\mathbb{X}}(\tilde{V})$. Furthermore, as the morphism $p_{\tilde{\mathbb{X}}/\mathbb{X}}$ is induced by the inclusion $k[\mathbb{X}] \subset k[\tilde{\mathbb{X}}]$, one sees that $v_{\mathbf{c}}(\boldsymbol{\eta}) = v_{p_{\tilde{\mathbb{X}}/\mathbb{X}}(\mathbf{c})}(\boldsymbol{\eta})$ for all $\mathbf{c} \in \tilde{\mathbb{X}}$. This implies that $G_{\mathbf{c}} = G_{p_{\tilde{\mathbb{X}}/\mathbb{X}}(\mathbf{c})}$ for all $\mathbf{c} \in \tilde{\mathbb{X}}$. Therefore it suffices to prove the proposition with the variety $\tilde{\mathbb{X}}$ over whose coordinate ring all G_i are defined. In the following, for the sake of notation, we assume that all G_i are defined over $k[\mathbb{X}]$. Let $\boldsymbol{\xi}_i$ be a generic point of G_i over $\overline{k(\mathbb{X})}$ and set

$$J_i = \{Q \in k[y_1, \cdots, y_m, X, 1/\det(X)]|Q(\boldsymbol{\eta}, \boldsymbol{\xi}_i) = 0\}.$$

Let $\mathbb{Y}_i$ be the variety over k defined by J_i. Then $\mathbb{Y}_i$ is irreducible because it has a generic point $(\boldsymbol{\eta}, \boldsymbol{\xi}_i)$. Moreover, one can verify that $J = \bigcap_{i=1}^{\ell} J_i$. Hence $\mathbb{Y} = \bigcup_{i=1}^{\ell} \mathbb{Y}_i$. Additionally, one has that $G_i = \pi_2(\pi_1|_{\mathbb{Y}_i}^{-1}(\boldsymbol{\eta}))$ and $\pi_2(\pi_1^{-1}(\mathbf{c})) = \bigcup_{i=1}^{\ell} \pi_2(\pi_1|_{\mathbb{Y}_i}^{-1}(\mathbf{c}))$.

By Remark 3.1, there is a nonempty open subset U_1 of $\mathbb{X}$ such that $\pi_2(\pi_1^{-1}(\mathbf{c}))$ is an algebraic subgroup for any $\mathbf{c} \in U_1$. Note that $\pi_1|_{\mathbb{Y}_i}$ is dominant and because G_i is irreducible over $\overline{k(\mathbb{X})}$, so is $\pi_1|_{\mathbb{Y}_i}^{-1}(\boldsymbol{\eta})$ which is equal to $\boldsymbol{\eta} \times G_i$. By Theorem 1 on page 139 of [24] and Proposition on page 33 of [13], there is a nonempty open subset $U_2 \subset \mathbb{X}$ such that for any $\mathbf{c} \in U_2$, $\pi_1|_{\mathbb{Y}_i}^{-1}(\mathbf{c})$ is irreducible and of dimension $\dim(G)$. Since $G_i \cap G_j = \emptyset$ if $i \neq j$, by Remark 3.1 again, there is a nonempty open subset U_3 of $\mathbb{X}$ such that for any $\mathbf{c} \in U_3$ and $i \neq j$, $\pi_2(\pi_1|_{\mathbb{Y}_i}^{-1}(\mathbf{c})) \cap \pi_2(\pi_1|_{\mathbb{Y}_j}^{-1}(\mathbf{c})) = \emptyset$. Now set $U = U_1 \cap U_2 \cap U_3$. Then for any $\mathbf{c} \in U$, we have that $\pi_2(\pi_1^{-1}(\mathbf{c}))$ is an algebraic group and $[\pi_2(\pi_1^{-1}(\mathbf{c})) : \pi_2(\pi_1^{-1}(\mathbf{c}))^{\circ}] = [G : G^{\circ}] = \ell$. Finally, note that $\pi_1|_{\mathbb{Y}_i}^{-1}(\mathbf{c}) = \mathbf{c} \times \pi_2(\pi_1|_{\mathbb{Y}_i}^{-1}(\mathbf{c}))$. Hence for each $\mathbf{c} \in U$, $\pi_2(\pi_1|_{\mathbb{Y}_i}^{-1}(\mathbf{c}))$ is of dimension $\dim(G)$ and so is $\pi_2(\pi_1^{-1}(\mathbf{c}))$. □

Lemma 3.3. *Assume that G is generated by unipotent elements. Then there is a nonempty open subset U of $\mathbb{X}$ such that for any $\mathbf{c} \in U$, $G_{\mathbf{c}}$ is an algebraic group generated by unipotent elements and of dimension $\dim(G)$.*

Proof. Due to Lemma C on page 96 of [13], any unipotent element of G that is not equal to the identity generates a connected 1-dimensional algebraic subgroup of G. Let $\mathcal{U}$ be the set of all connected 1-dimensional algebraic subgroups of G and let $\tilde{G}$ be the algebraic subgroup of G generated by $\bigcup_{M \in \mathcal{U}} M$. Then $\tilde{G} = G$ and by the proposition on page 55 of [13], there are $M_1, \cdots, M_\ell$ in $\mathcal{U}$ such that

$\tilde{G} = M_1 M_2 \cdots M_\ell$. Furthermore, ℓ can be taken to be not greater than $2\dim(G)$. Now for each $i = 1, \cdots, \ell$, there is a nilpotent matrix $\mathbf{n}_i$ in $\mathrm{Mat}_n(\overline{k(\mathbb{X})})$ such that

$$M_i = \left\{ \sum_{j=0}^{n-1} \frac{\mathbf{n}_i^j c^j}{j!} \,\middle|\, c \in \overline{k(\mathbb{X})} \right\}.$$

Let D be a finitely generated $k[\mathbb{X}]$-algebra in $\overline{k(\mathbb{X})}$ such that all entries of each $\mathbf{n}_i$ are in D, and let $\tilde{\mathbb{X}}$ be the variety over k associated to D. By Lemma 2.2 and an argument similar to that in the proof of Proposition 3.2, one only needs to prove the lemma with $\tilde{\mathbb{X}}$. For the sake of notation, we may assume that all $\mathbf{n}_i$ are in $\mathrm{Mat}_n(k[\mathbb{X}])$. Set

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

where $t_1, \cdots, t_\ell$ are indeterminates. Then $(P_{i,j})$ is a generic point of G. Assume that $d = \dim(G)$ and $P_{i_1,j_1}, \cdots, P_{i_d,j_d}$ are algebraically independent over $k(\mathbb{X})$. We claim that there is a nonempty open subset of $\mathbb{X}$ such that for any $\mathbf{c}$ in this set, $v_{\mathbf{c}}(P_{i_1,j_1}), \cdots, v_{\mathbf{c}}(P_{i_d,j_d})$ are algebraically independent over k. For $\mathbf{c} \in \mathbb{X}$, denote by $I_{\mathbf{c}}$ the ideal generated by all $y_{i,j} - v_{\mathbf{c}}(P_{i,j})$ in $k[t_1, \cdots, t_\ell, y_{1,1}, \cdots, y_{n,n}]$. Let $S_{\mathbf{c}}$ be the reduced Gröbner basis of $I_{\mathbf{c}}$ with respect to a lexicographic ordering where every t_i is greater than every $y_{l,m}$ and every $y_{l,m}$ with $(l,m) \neq (i_s, j_s)$ for all $s = 1, \cdots, d$ is greater than every y_{i_s,j_s}. Then $v_{\mathbf{c}}(P_{i_1,j_1}), \cdots, v_{\mathbf{c}}(P_{i_d,j_d})$ are algebraically dependent over k if and only if $S_{\mathbf{c}}$ contains at least one polynomial in $k[y_{i_1,j_1}, \cdots, y_{i_d,j_d}]$. Moreover, for every $Q \in S_{\mathbf{c}} \cap k[y_{i_1,j_1}, \cdots, y_{i_d,j_d}]$ one has that $Q(v_{\mathbf{c}}(P_{i_1,j_1}), \cdots, v_{\mathbf{c}}(P_{i_d,j_d})) = 0$. By Corollary 8.3 of [7], there is an integer N only depending on n, ℓ such that for every $\mathbf{c} \in \mathbb{X}$, the total degree of each polynomial in $S_{\mathbf{c}}$ is not greater than N. These imply that if $v_{\mathbf{c}}(P_{i_1,j_1}), \cdots, v_{\mathbf{c}}(P_{i_d,j_d})$ are algebraically dependent over k, then there is a nonzero $Q_{\mathbf{c}}$ in $k[y_{i_1,j_1}, \cdots, y_{i_d,j_d}]$ of total degree not greater than N such that

$$Q_{\mathbf{c}}(v_{\mathbf{c}}(P_{i_1,j_1}), \cdots, v_{\mathbf{c}}(P_{i_d,j_d})) = 0.$$

Now for nonnegative integers $s_1, \cdots, s_d$ with $s_1 + \cdots + s_d \leq N$, write

$$P_{i_1,j_1}^{s_1} \cdots P_{i_d,j_d}^{s_d} = \sum_{\boldsymbol{\mu}=(\mu_1,\cdots,\mu_\ell)} c_{s_1,\cdots,s_d,\boldsymbol{\mu}} t_1^{\mu_1} t_2^{\mu_2} \cdots t_\ell^{\mu_\ell},$$

where $0 \leq \mu_i \leq N(n-1)$ and $c_{s_1,\cdots,s_d,\boldsymbol{\mu}} \in k[\mathbb{X}]$. Let C be the $\binom{N+d}{d} \times (N(n-1)+1)^\ell$ matrix formed by $c_{s_1,\cdots,s_d,\boldsymbol{\mu}}$. Since $P_{i_1,j_1}, \cdots, P_{i_d,j_d}$ are algebraically independent, C is of full rank $\binom{N+d}{d}$, i.e., there is a nonzero $\binom{N+d}{d} \times \binom{N+d}{d}$-minor g of C. Suppose that $v_{\mathbf{c}}(P_{i_1,j_1}), \cdots, v_{\mathbf{c}}(P_{i_d,j_d})$ are algebraically dependent over k for some $\mathbf{c} \in \mathbb{X}_g$. The choice of N implies that the left kernel of $v_{\mathbf{c}}(C)$ has a nonzero element. This contradicts the fact that $v_{\mathbf{c}}(C)$ is of full rank. Thus $v_{\mathbf{c}}(P_{i_1,j_1}), \cdots, v_{\mathbf{c}}(P_{i_d,j_d})$ are algebraically independent over k for all $\mathbf{c} \in \mathbb{X}_g$. This proves the claim. By Proposition 3.2, there is a nonempty open subset U_1 of $\mathbb{X}$ such that for any $\mathbf{c} \in U_1$, $G_{\mathbf{c}}$ is a connected algebraic group of dimension $\dim(G)$. Set $U = U_1 \cap \mathbb{X}_g$. Then for any $\mathbf{c} \in U$, since $(v_{\mathbf{c}}(P_{i,j}))$ is obviously a point of $G_{\mathbf{c}}$, it is a generic point of $G_{\mathbf{c}}$. Hence $G_{\mathbf{c}}$ is generated by unipotent elements. □

Let H be a connected algebraic subgroup of $\mathrm{GL}_n(\overline{k(\mathbb{X})})$. The following lemma gives a criterion for a finite subset $\mathfrak{X}$ to be a basis of $\boldsymbol{\chi}(H)$ as a free Abelian group. We say $\mathfrak{X}$ is multiplicatively independent if the equality $\prod_{\chi\in\mathfrak{X}}\chi^{d_\chi}=1$ with $d_\chi\in\mathbb{Z}$ implies that $d_\chi=0$ for all $\chi\in\mathfrak{X}$.

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

Proof. Since $\mathfrak{X}$ is a basis of $\boldsymbol{\chi}(H)$ as a free Abelian group, $\mathfrak{X}$ is multiplicatively independent and $\bigcap_{\chi\in\mathfrak{X}}\ker(\chi)=\bigcap_{\chi\in\boldsymbol{\chi}(H)}\ker(\chi)$. By Lemma B.10 of [8], $\bigcap_{\chi\in\boldsymbol{\chi}(H)}\ker(\chi)$, which is denoted by H^t in [8], is generated by unipotent elements. This proves the necessary part. For the sufficient part, it suffices to show that $\mathfrak{X}$ generates $\boldsymbol{\chi}(H)$. Denote $\bar{H}=H/\bigcap_{\chi\in\mathfrak{X}}\ker(\chi)$. For each $\chi\in\boldsymbol{\chi}(H)$, by Lemma B.10 of [8], any unipotent element of H is contained in $\ker(\chi)$ and thus from the assumption $\bigcap_{\chi'\in\mathfrak{X}}\ker(\chi')\subset\ker(\chi)$. This implies that $\bigcap_{\chi\in\boldsymbol{\chi}(H)}\ker(\chi)=\bigcap_{\chi\in\mathfrak{X}}\ker(\chi)$. Then one has that $\boldsymbol{\chi}(H)\cong\boldsymbol{\chi}(\bar{H})$ (see Exercise 12 on page 108 of [13]). Here the isomorphism sends χ to $\bar{\chi}$, where $\bar{\chi}:\bar{H}\to\mathbb{G}_m(\overline{k(\mathbb{X})})$ is given by $\bar{\chi}(\bar{\mathbf{c}})=\chi(\mathbf{c})$ for all $\mathbf{c}\in H$. Since $\mathfrak{X}$ is multiplicatively independent, so is $\{\bar{\chi}|\chi\in\mathfrak{X}\}$. Thus $\{\bar{\chi}|\chi\in\mathfrak{X}\}$ is a basis of $\boldsymbol{\chi}(\bar{H})$ and then $\mathfrak{X}$ is a basis of $\boldsymbol{\chi}(H)$. □

Proposition 3.5. *There is an open subset U of $\mathbb{X}$ satisfying that for any $\mathbf{c}\in U$, $G_\mathbf{c}$ is an algebraic group of $\dim(G)$ and $v_\mathbf{c}(\mathfrak{X})$ is a basis of $\boldsymbol{\chi}(G_\mathbf{c}^\circ)$.*

Proof. Let $p_\chi,\chi\in\mathfrak{X}$ be distinct primes. By Lemma C on page 104 of [13], there is $g\in G$ such that $\chi(g)=p_\chi$ for all $\chi\in\mathfrak{X}$. By Lemma 2.2 and an argument similar to that in the proof of Lemma 3.3, we may assume that the entries of g are in $k[\mathbb{X}]$. Applying Proposition 3.2 to G and G°, respectively, one gets a nonempty open subset U_1 of $\mathbb{X}$ such that for any $\mathbf{c}\in U_1$, $G_\mathbf{c}$ is an algebraic group of dimension $\dim(G)$ and $(G^\circ)_\mathbf{c}$ is a connected algebraic group of dimension $\dim(G^\circ)$. By an argument similar to that in Remark 3.1, we may assume that $(G^\circ)_\mathbf{c}\subset G_\mathbf{c}$ for all $\mathbf{c}\in U_1$. Then the dimension argument implies that $(G^\circ)_\mathbf{c}=G_\mathbf{c}^\circ$ for all $\mathbf{c}\in U_1$. We shall prove that $v_\mathbf{c}(\mathfrak{X})$ is a basis of $\boldsymbol{\chi}((G^\circ)_\mathbf{c})$ for all $\mathbf{c}$ being in some nonempty open subset of $\mathbb{X}$. By Remark 3.1, there is a nonempty open subset U_2 of $\mathbb{X}$ such that for any $\mathbf{c}\in U_2$, $v_\mathbf{c}(\mathfrak{X})\subset\boldsymbol{\chi}((G^\circ)_\mathbf{c})$. Set $H=\bigcap_{\chi\in\mathfrak{X}}\ker(\chi)$. Then H is defined over $k[\mathbb{X}]$ and by Lemma B.10 of [8], H is generated by unipotent elements. Let U_3 be a nonempty open subset of $\mathbb{X}$ such that $H_\mathbf{c}$ is an algebraic group generated by unipotent elements and $H_\mathbf{c}=\bigcap_{\chi\in\mathfrak{X}}\ker(v_\mathbf{c}(\chi))$. Such U_3 exists due to Lemma 3.3 and Remark 3.1. Now set $U=U_1\cap U_2\cap U_3\cap\mathbb{X}_f$ with $f=\det(g)$. Assume that $\mathbf{c}\in U$. We claim that $v_\mathbf{c}(\mathfrak{X})$ is a basis of $\boldsymbol{\chi}((G^\circ)_\mathbf{c})$. Since the p_χ are distinct primes, for any integers $\mu_\chi,\chi\in\mathfrak{X}$, not all zero,

$$\prod_{\chi\in\mathfrak{X}}v_\mathbf{c}(\chi)(g(\mathbf{c}))^{\mu_\chi}=v_\mathbf{c}\left(\prod_{\chi\in\mathfrak{X}}\chi(g)^{\mu_\chi}\right)=\prod_{\chi\in\mathfrak{X}}p_\chi^{\mu_\chi}\neq 1.$$

This implies that $v_\mathbf{c}(\mathfrak{X})$ is multiplicatively independent. Due to Lemma 3.4 and the fact that $\bigcap_{\chi\in\mathfrak{X}}\ker(v_\mathbf{c}(\chi))$ is generated by unipotent elements, $v_\mathbf{c}(\mathfrak{X})$ is a basis of $\boldsymbol{\chi}((G^\circ)_\mathbf{c})$ and thus a basis of $\boldsymbol{\chi}(G_\mathbf{c}^\circ)$. □

4. Difference equations under specialization

Let $B \in \mathrm{GL}_n(k(\mathbb{X})(x))$ and let σ be the $k(\mathbb{X})$-automorphism of $k(\mathbb{X})(x)$ which sends x to $x+1$. By setting $\sigma(X) = BX$, the automorphism σ can be extended to an automorphism of $k(\mathbb{X})(x)[X, 1/\det(X)]$. As we shall deal with a family of automorphisms, to avoid confusion, the automorphism of $k(\mathbb{X})(x)[X, 1/\det(X)]$ induced by $\sigma(X) = BX$ will be denoted by σ_B. An ideal I of $k(\mathbb{X})(x)[X, 1/\det(X)]$ is called a σ_B-ideal if $\sigma_B(I) = I$. Let A be given as in (1.1). For convenience, we introduce the following notation.

Notation 4.1. Denote by $\mathbb{X}_{\mathfrak{h}}$ the set of $\mathbf{c} \in \mathbb{X}$ satisfying that $A(\mathbf{c})$ is well-defined and invertible. One easily sees that $\mathbb{X}_{\mathfrak{h}}$ is open and nonempty.

Definition 4.2. Let ν be a positive integer and let $I \subset \overline{k(\mathbb{X})}(x)[X, 1/\det(X)]$ be a σ_A-ideal generated by some polynomials in $\overline{k(\mathbb{X})}(x)[X]_{\leq \nu}$. I is said to be a ν-maximal σ_A-ideal if it is not the whole ring and for any σ_A-ideal J generated by some polynomials in $\overline{k(\mathbb{X})}(x)[X]_{\leq \nu}$ if $I \subset J$, then either $I = J$ or J is the whole ring. Likewise we define ν-maximal $\sigma_{A(\mathbf{c})}$-ideals in $k(x)[X, 1/\det(X)]$.

Let I_ν be a ν-maximal σ_A-ideal and let $\mathcal{F}$ be a fundamental matrix of $\sigma_A(Y) = AY$ over $\overline{k(\mathbb{X})}(x)$ satisfying that it is a zero of I_ν. Then one has that

$$\left\langle \left\{ p \in \overline{k(\mathbb{X})}(x)[X]_{\leq \nu} \mid p(\mathcal{F}) = 0 \right\} \right\rangle_{\overline{k(\mathbb{X})}(x)} \subset I_\nu$$

where $\langle * \rangle_{\overline{k(\mathbb{X})}(x)}$ denotes the ideal in $\overline{k(\mathbb{X})}(x)[X, 1/\det(X)]$ generated by $*$. Proposition 3.5 of [9] implies that the above two sets coincide. From this, one sees that if J is another ν-maximal σ_A-ideal, then there is $g \in \mathrm{GL}_n(\overline{k(\mathbb{X})})$ such that

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

Let m be a nonnegative integer. Set

$$\mathrm{I}(m, I_\nu) = I_\nu \cap \overline{k(\mathbb{X})}[x]_{\leq m}[X]_{\leq \nu}, \tag{4.1}$$

where

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

As I_ν is finitely generated, there is an integer μ such that $\mathrm{I}(\mu, I_\nu)$ generates I_ν as an ideal in $\overline{k(\mathbb{X})}(x)[X, 1/\det(X)]$. 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 any ν-maximal σ_A-ideals. Hence the following definition is reasonable.

Definition 4.3. An integer μ is called a coefficient bound of ν-maximal σ_A-ideals if for every ν-maximal σ_A-ideal I_ν, $\mathrm{I}(\mu, I_\nu)$ generates I_ν as an ideal in $\overline{k(\mathbb{X})}(x)[X, 1/\det(X)]$.

Remark 4.4. Note that in [9] 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 (1.1).

Let us sketch the main results of this section. First, we show that there is a coefficient bound of I_ν, say μ, satisfying that it is a coefficient bound of ν-maximal $\sigma_{A(\mathbf{c})}$-ideals for all $\mathbf{c}$ in some basic open subset of $\mathbb{X}$ (see Lemma 4.17). Second, under the hypothesis that $\mathrm{I}(\mu, I_\nu)$ has a $\overline{k(\mathbb{X})}$-basis B contained in $k[\mathbb{X}][x, X]$, we prove that there is a basic open subset of $\mathbb{X}$ such that for each $\mathbf{c}$ in this set, $v_{\mathbf{c}}(B)$ is

a basis of $\mathrm{I}(\mu, \tilde{I}_\nu)$ as a k-vector space for some ν-maximal$\sigma_{A(\mathbf{c})}$-ideal $\tilde{I}_\nu$. The choice of μ implies that $v_{\mathbf{c}}(B)$ generates $\tilde{I}_\nu$ (see Proposition 4.22).

Before we go further, let us first introduce some notation. Let $X^{\mathbf{d}_1}, \cdots, X^{\mathbf{d}_\ell}$ be all monomials in X with degree not greater than ν, where $\ell = \binom{n^2+\nu-1}{\nu}$. Then $\{X^{\mathbf{d}_1}, \cdots, X^{\mathbf{d}_\ell}\}$ is a basis of $\overline{k(\mathbb{X})}(x)[X]_{\leq \nu}$ as a vector space over $\overline{k(\mathbb{X})}(x)$. Let Y be an $n \times n$ matrix with indeterminate entries and for a matrix M, let M^t denote its transpose.

Notation 4.5. Suppose that F is an $n \times n$ matrix with entries in a $\overline{k(\mathbb{X})}(x)$-algebra R. Then the map sending X to FX induces a map

$$\begin{aligned} \mathrm{Sym}_\nu : \mathrm{Mat}_n(R) &\longrightarrow \mathrm{Mat}_\ell(R) \\ F &\longrightarrow \mathrm{Sym}_\nu(F), \end{aligned}$$

where $\mathrm{Sym}_\nu(F)$ is defined to be the matrix satisfying that

$$(X^{\mathbf{d}_1}, \cdots, X^{\mathbf{d}_\ell})^t|_{X=FY} = \mathrm{Sym}_\nu(F)(X^{\mathbf{d}_1}, \cdots, X^{\mathbf{d}_\ell})^t|_{X=Y}.$$

Let l be a positive integer not greater than n. Denote by $\mathcal{I}_{n,l}$ the set of all subsets of $\{1, 2, \cdots, n\}$ containing exactly l elements. We define an order $\prec$ on $\mathcal{I}_{n,l}$ as follows: for $\mathbf{i}, \mathbf{j} \in \mathcal{I}_{n,l}$, $\mathbf{i} \prec \mathbf{j}$ if they satisfy that (1) $\min \mathbf{i} < \min \mathbf{j}$ or (2) $\min \mathbf{i} = \min \mathbf{j}$ and $\mathbf{i} \setminus \{\min \mathbf{i}\} \prec \mathbf{j} \setminus \{\min \mathbf{j}\}$.

Notation 4.6. We use $\Phi_{n,l}$ to denote the map defined as follows:

$$\begin{aligned} \mathrm{GL}_n(\overline{k(\mathbb{X})}(x)) &\longrightarrow \mathrm{GL}_{\binom{n}{l}}(\overline{k(\mathbb{X})}(x)) \\ Z &\longrightarrow (Z_{\mathbf{i},\mathbf{j}})_{\{1,2,\cdots,l\} \prec \mathbf{i},\mathbf{j} \prec \{n-l+1,\cdots,n\}}, \end{aligned}$$

where $Z_{\mathbf{i},\mathbf{j}}$ denotes the $l \times l$ minor of Z that corresponds to the rows with index in $\mathbf{i}$ and the columns with index in $\mathbf{j}$.

Remark 4.7. (1) By the definition, one sees that

$$\mathrm{Sym}_\nu(F_1 F_2) = \mathrm{Sym}_\nu(F_1)\mathrm{Sym}_\nu(F_2)$$

and if F is invertible, then so is $\mathrm{Sym}_\nu(F)$.

(2) Write $F = (f_{i,j})$ with $f_{i,j} \in R$. Then the vector space spanned by the entries of $\mathrm{Sym}_\nu(F)$ coincides with the one spanned by $\prod_{i,j} f_{i,j}^{s_{i,j}}$ with $0 \leq \sum_{i,j} s_{i,j} \leq \nu$. To see this, let V denote the latter vector space. Obviously, all entries of $\mathrm{Sym}_\nu(F)$ are in V. On the other hand, by the definition of Sym_ν, one has that

$$(\cdots, \prod_{i,j} f_{i,j}^{s_{i,j}}, \cdots)^t = (X^{\mathbf{d}_1}, \cdots, X^{\mathbf{d}_\ell})^t|_{X=F} = \mathrm{Sym}_\nu(F)(X^{\mathbf{d}_1}, \cdots, X^{\mathbf{d}_\ell})^t|_{X=I_n},$$

which implies that each $\prod_{i,j} f_{i,j}^{s_{i,j}}$ is a $\mathbb{Q}$-combination of the entries of $\mathrm{Sym}_\nu(F)$. Hence these vector spaces are equal to each other.

(3) One sees that $\Phi_{n,l}(I_n) = I_{\binom{n}{l}}$ and if M is a permutation matrix, then so is $\Phi_{n,l}(M)$. Furthermore, the Cauchy-Binet formula (see Proposition 2.1.2 on page 18 of [22]) implies that $\Phi_{n,l}$ is actually a group homomorphism.

4.1. **Coefficient bounds of ν-maximal σ_A-ideals.** In this subsection, we shall show that there is a coefficient bound N of ν-maximal σ_A-ideals and a basic open subset U of $\mathbb{X}$ such that N is also a coefficient bound of ν-maximal $\sigma_{A(\mathbf{c})}$-ideals for all $\mathbf{c} \in U$. Such a coefficient bound can be derived from a degree bound of the certificates of hypergeometric solutions of a suitable linear difference equation.

Definition 4.8. Let R be a σ-extension ring of $\overline{k(\mathbb{X})}(x)$. $h \in R$ is said to be hypergeometric over $\overline{k(\mathbb{X})}(x)$ if h is invertible in R and $\sigma(h)h^{-1} \in \overline{k(\mathbb{X})}(x)$, which is called the certificate of h. A solution $\mathbf{h}$ of (1.1) is called a hypergeometric solution if $\mathbf{h} = \mathbf{v}h$ where $\mathbf{v} \in \overline{k(\mathbb{X})}(x)^n$ and h is hypergeometric over $\overline{k(\mathbb{X})}(x)$.

Let us recall the method developed in [9] to compute a coefficient bound of a ν-maximal σ_A-ideal I_ν. Denote

$$S_\nu = I_\nu \cap \overline{k(\mathbb{X})}(x)[X]_{\leq \nu}.$$

Then S_ν is a $\overline{k(\mathbb{X})}(x)$-vector space of finite dimension and it generates I_ν. Suppose that $\{p_1, \cdots, p_l\}$ is a $\overline{k(\mathbb{X})}(x)$-basis of S_ν. Let $X^{\mathbf{d}_1}, \cdots, X^{\mathbf{d}_\ell}$ be as in Notation 4.5. After an invertible linear transformation of $p_1, \cdots, p_l$ if necessary, we may assume that for each $i = 1, \cdots, l$

$$p_i = X^{\mathbf{d}_i} + \sum_{j=l+1}^{\ell} c_{i,j} X^{\mathbf{d}_j} \tag{4.2}$$

with $c_{i,j} \in \overline{k(\mathbb{X})}(x)$. For $f \in \overline{k(\mathbb{X})}(x) \setminus \{0\}$, $\deg(f)$ stands for the degree of f which is defined to be the maximum of the degrees of its numerator and denominator. For convenience, set $\deg(0) = -\infty$. Then we have the following claim.

Claim 4.9. ℓm is a coefficient bound of I_ν if m is not less than $\deg(c_{i,j})$ for all i, j.

Clearing the denominators of $c_{i,j}$ in (4.2), we obtain $\tilde{p}_i \in \overline{k(\mathbb{X})}[x, X]$ with $\deg_X(\tilde{p}_i) \leq \nu$ and $\deg_x(\tilde{p}_i) \leq (\ell - l)m < \ell m$. In other words, $\tilde{p}_i \in \mathrm{I}(\ell m, I_\nu)$ and $\{\tilde{p}_1, \cdots, \tilde{p}_l\}$ is a basis of S_ν, where $\mathrm{I}(\ell m, I_\nu)$ is defined as in (4.1). Hence ℓm is a coefficient bound of I_ν. This proves our claim. So in order to obtain a coefficient bound of I_ν, it suffices to compute a degree bound of $c_{i,j}$. In the following, we show that a degree bound of $c_{i,j}$ can be achieved via computing the certificates of hypergeometric solutions of certain linear difference equations. We have that

$$\sigma_A((X^{\mathbf{d}_1}, \cdots, X^{\mathbf{d}_\ell})^t) = \mathrm{Sym}_\nu(A)(X^{\mathbf{d}_1}, \cdots, X^{\mathbf{d}_\ell})^t,$$

where Sym_ν is defined as in Notation 4.5. From (4.2), $\{p_1, \cdots, p_l, X^{\mathbf{d}_{l+1}}, \cdots, X^{\mathbf{d}_\ell}\}$ is another $\overline{k(\mathbb{X})}(x)$-basis of $\overline{k(\mathbb{X})}(x)[X]_{\leq \nu}$, and, moreover, one has that

$$(p_1, \cdots, p_l, X^{\mathbf{d}_{l+1}}, \cdots, X^{\mathbf{d}_\ell})^t = \begin{pmatrix} I_l & C \\ 0 & I_{\ell-l} \end{pmatrix} (X^{\mathbf{d}_1}, \cdots, X^{\mathbf{d}_\ell})^t, \tag{4.3}$$

where $C = (c_{i,j})_{1 \leq i \leq l, l+1 \leq j \leq \ell}$ with $c_{i,j}$ given in (4.2). Since S_ν is stable under the action of σ_A, one has that

$$\sigma_A((p_1, \cdots, p_l, X^{\mathbf{d}_{l+1}}, \cdots, X^{\mathbf{d}_\ell})^t) = \begin{pmatrix} B_1 & 0 \\ B_2 & B_3 \end{pmatrix} (p_1, \cdots, p_l, X^{\mathbf{d}_{l+1}}, \cdots, X^{\mathbf{d}_\ell})^t,$$

where $B_1 \in \mathrm{GL}_l(\overline{k(\mathbb{X})}(x)), B_3 \in \mathrm{GL}_{\ell-l}(\overline{k(\mathbb{X})}(x))$, and B_2 is an $(\ell - l) \times l$ matrix with entries in $\overline{k(\mathbb{X})}(x)$. Applying σ_A to (4.3) yields that

$$\begin{pmatrix} I_l & \sigma(C) \\ 0 & I_{\ell-l} \end{pmatrix} \mathrm{Sym}_\nu(A)(X^{\mathbf{d}_1}, \cdots, X^{\mathbf{d}_\ell})^t = \begin{pmatrix} B_1 & 0 \\ B_2 & B_3 \end{pmatrix} \begin{pmatrix} I_l & C \\ 0 & I_{\ell-l} \end{pmatrix} (X^{\mathbf{d}_1}, \cdots, X^{\mathbf{d}_\ell})^t.$$

As $X^{\mathbf{d}_1}, \cdots, X^{\mathbf{d}_\ell}$ are linearly independent over $\overline{k(\mathbb{X})}(x)$, the above equality implies

$$\begin{pmatrix} I_l & \sigma(C) \\ 0 & I_{\ell-l} \end{pmatrix} \mathrm{Sym}_\nu(A) = \begin{pmatrix} B_1 & 0 \\ B_2 & B_3 \end{pmatrix} \begin{pmatrix} I_l & C \\ 0 & I_{\ell-l} \end{pmatrix}. \tag{4.4}$$

Denote by $\mathbf{s}$ the first row of

$$\Phi_{\ell,l}\left(\begin{pmatrix} I_l & C \\ 0 & I_{\ell-l} \end{pmatrix}\right),$$

where $\Phi_{\ell,l}$ is defined as in Notation 4.6. Applying $\Phi_{\ell,l}$ to (4.4), we obtain that

$$\begin{pmatrix} \sigma(\mathbf{s}) \\ * \end{pmatrix} \Phi_{\ell,l}\left(\mathrm{Sym}_\nu(A)\right) = \begin{pmatrix} \det(B_1) & 0 \\ * & * \end{pmatrix} \begin{pmatrix} \mathbf{s} \\ 0 \end{pmatrix}$$

which implies that

$$\sigma(\mathbf{s})\Phi_{\ell,l}\left(\mathrm{Sym}_\nu(A)\right) = \det(B_1)\mathbf{s}.$$

Let h be the hypergeometric element in some σ-extension ring of $\overline{k(\mathbb{X})}(x)$ with $\det(B_1)$ as its certificate. Then $\mathbf{s}^t h$ is a hypergeometric solution of the following linear difference equation:

$$\sigma_{\Phi_{\ell,l}(\mathrm{Sym}_\nu(A))^{-t}}(Y) = \Phi_{\ell,l}\left(\mathrm{Sym}_\nu(A)\right)^{-t} Y, \tag{4.5}$$

where $*^{-t}$ denotes the transpose of the inverse of $*$. For each $\mathbf{i} \in \mathcal{I}_{\ell,l}$, denote by $s_{\mathbf{i}}$ the $l \times l$-minor of (I_l, C) corresponding to the columns with index in $\mathbf{i}$. Then $\mathbf{s} = (s_{\mathbf{i}})_{\mathbf{i}\in\mathcal{I}_{\ell,l}}$ and one can verify that

$$s_{\mathbf{i}} = \begin{cases} 1, & \mathbf{i} = \{1, 2, \cdots, l\}, \\ (-1)^{l-j} c_{i,j}, & \mathbf{i} = \{1, 2, \cdots, i-1, i+1, \cdots, l, j\} \end{cases} \tag{4.6}$$

for all $i \in \{1, 2, \cdots, l\}$ and all $j \in \{l+1, \cdots, \ell\}$. Therefore to compute a degree bound for $c_{i,j}$, we only need to compute a degree bound for entries of $\mathbf{s}$.

It is well known that the equation (4.5) is equivalent to a linear difference operator with coefficients in $\overline{k(\mathbb{X})}(x)$ (see Section 1 of [1]). Precisely, there is a matrix $T \in \mathrm{GL}_\mu(\overline{k(\mathbb{X})}(x))$ such that $\sigma(T)\Phi_{\ell,l}(\mathrm{Sym}_\nu(A))^{-t}T^{-1}$ is of the form

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ & & & 1 & 0 \\ 0 & \cdots & \cdots & 0 & 1 \\ -a_0 & -a_1 & \cdots & \cdots & -a_{\mu-1} \end{pmatrix},$$

where $\mu = \binom{\ell}{l} = |\mathcal{I}_{\ell,l}|$, the order of the matrix $\Phi_{\ell,l}(\mathrm{Sym}_\nu(A))$. In other words, under the transformation T, the equation (4.5) is equivalent to

$$\mathcal{L} = \sigma^\mu + a_{\mu-1}\sigma^{\mu-1} + \cdots + a_0,$$

and the solution $\mathbf{s}^t h$ of (4.5) is transformed into

$$T\mathbf{s}^t h = \begin{pmatrix} 1 \\ \tilde{r} \\ \vdots \\ \prod_{i=0}^{\mu-2} \sigma^i(\tilde{r}) \end{pmatrix} \tilde{h},$$

where $\tilde{h}$ is a hypergeometric solution of $\mathcal{L}(y) = 0$ and $\tilde{r}$ is the certificate of $\tilde{h}$. Denote by $\deg(T^{-1})$ the maximum of the degrees of entries of T^{-1} and denote

$$\begin{pmatrix} w_{\mathbf{i}_1} \\ w_{\mathbf{i}_2} \\ \vdots \\ w_{\mathbf{i}_\mu} \end{pmatrix} = T^{-1} \begin{pmatrix} 1 \\ \tilde{r} \\ \vdots \\ \prod_{i=0}^{\mu-2} \sigma^i(\tilde{r}) \end{pmatrix}.$$

Since $\deg(\prod_{i=0}^{j} \sigma^i(\tilde{r})) \leq (j+1)\deg(\tilde{r})$ for all $0 \leq j \leq \mu - 2$,

$$\deg(w_{\mathbf{i}_j}) \leq \mu \deg(T^{-1}) + \mu(\mu-1)\deg(\tilde{r})$$

for all $j = 1, \cdots, \mu$. On the other hand, since $\mathbf{s} = (w_{\mathbf{i}_1}, \cdots, w_{\mathbf{i}_\mu})h^{-1}\tilde{h}$, by (4.6),

$$\deg(c_{i,j}) = \deg(s_{\mathbf{j}}/s_{\mathbf{i}_1}) = \deg(w_{\mathbf{j}}/w_{\mathbf{i}_1}) \leq 2\mu \deg(T^{-1}) + 2\mu(\mu-1)\deg(\tilde{r}), \tag{4.7}$$

where $\mathbf{i}_1 = \{1, 2, \cdots, l\}, \mathbf{j} = \{1, \cdots, i-1, i+1, \cdots, l, j\}$. Therefore to bound the degree of $c_{i,j}$, it suffices to bound the degrees of the certificates of all hypergeometric solutions of $\mathcal{L}(y) = 0$. For the latter purpose, we introduce the following definition.

Definition 4.10. A nonnegative integer N is call a hyper-bound for $\mathcal{L}$ if the certificates of all hypergeometric solutions of $\mathcal{L}(y) = 0$ are of degree $\leq N$.

Remark 4.11. (1) In the above discussion, we need to already know how large the dimension of S_ν is. In the case when this dimension cannot be determined previously, we can compute hyper-bounds for linear difference operators corresponding to $\sigma_{\Phi_{\ell,l}(\mathrm{Sym}_\nu(A))^{-t}}(Y) = \Phi_{\ell,l}(\mathrm{Sym}_\nu(A))^{-t}Y$ with $l = 1, 2, \cdots, \ell$. Each hyper-bound gives a potential coefficient bound of I_ν. The maximum of these potential coefficient bounds will be what we need.

(2) The method described above also works for linear difference equations with coefficients in $k(x)$. Particularly, let $\mathbf{c} \in \mathbb{X}_\mathfrak{h}$ where $\mathbb{X}_\mathfrak{h}$ is given in Notation 4.1. We can find a coefficient bound for ν-maximal $\sigma_{A(\mathbf{c})}$-ideals from hyper-bounds for linear difference operators corresponding to $\sigma_{\Phi_{\ell,l}(\mathrm{Sym}_\nu(A(\mathbf{c})))^{-t}}(Y) = \Phi_{\ell,l}(\mathrm{Sym}_\nu(A(\mathbf{c})))^{-t}Y$ with $l = 1, 2, \ldots, \ell$.

In the rest of this subsection, we shall deal with hyper-bounds for a linear difference operator $\mathcal{L}$. After multiplying a polynomial in $\overline{k(\mathbb{X})}[x]$, we may assume that $\mathcal{L}$ has polynomial coefficients, i.e.,

$$\mathcal{L} = a_n(x)\sigma^n + \cdots + a_1(x)\sigma + a_0(x)$$

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

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

Definition 4.12. $\sum_{i=0}^{n} \mathrm{coeff}(\bar{a}_i, x, \rho)y^i$ is called the indicial polynomial of $\mathcal{L}$, denoted by $\mathrm{Ind}(\mathcal{L})$, where $\mathrm{coeff}(\bar{a}_i, x, \rho)$ denotes the coefficient of x^ρ in $\bar{a}_i$.

Remark 4.13. Let $p(x) = cx^m + c_{m-1}x^{m-1} + \cdots + c_0$ be a polynomial of degree m. Then for each $i = 0, \cdots, n$, one has that

$$\bar{\sigma}^i(p(x)) = cm^i x^m + \text{terms of lower degree.}$$

Furthermore,

$$\mathcal{L}(p(x)) = c\left(\sum_{i=0}^{n} \operatorname{coeff}(\bar{a}_i, x, \rho)m^i\right) x^{\rho+m} + \text{terms of lower degree.}$$

Therefore if $\mathcal{L}(p(x)) = 0$, then m is an integer zero of $\operatorname{Ind}(\mathcal{L})$.

Assume that $\mathcal{L} \in k[\mathbb{X}][x, \sigma]$. For $\mathbf{c} \in \mathbb{X}$, $\mathcal{L}_{\mathbf{c}}$ denotes the operator obtained by applying $v_{\mathbf{c}}$ to the coefficients of $\mathcal{L}$.

Lemma 4.14. *Let $N = \max \mathbf{Z}(\operatorname{Ind}(\mathcal{L})) \cup \{0\}$. Then there is a basic open subset U of $\mathbb{X}$ such that polynomial solutions of $\mathcal{L}_{\mathbf{c}}(y) = 0$ with $\mathbf{c} \in U$ are of degree not greater than N.*

Proof. By Lemma 2.17, there is a finitely generated subgroup Γ of $\mathbb{G}_a(\overline{k(\mathbb{X})})$ such that for any $\mathbf{c} \in \mathcal{B}(\mathbb{X}, \Gamma)$, $\mathbf{Z}(\operatorname{Ind}(\mathcal{L})) = \mathbf{Z}(v_{\mathbf{c}}(\operatorname{Ind}(\mathcal{L})))$. Let c be a nonzero element in $k[\mathbb{X}]$ such that for every $\mathbf{c} \in \mathbb{X}_c$, $\deg(\bar{a}_i) = \deg(v_{\mathbf{c}}(\bar{a}_i))$ for all $0 \le i \le n$. Let $U = \mathcal{B}(\mathbb{X}, \Gamma) \cap \mathbb{X}_c$. Suppose that $\mathbf{c} \in U$. One has that $v_{\mathbf{c}}(\operatorname{Ind}(\mathcal{L})) = \operatorname{Ind}(\mathcal{L}_{\mathbf{c}})$ and then

$$\begin{aligned}\max \mathbf{Z}(\operatorname{Ind}(\mathcal{L}_{\mathbf{c}})) \cup \{0\} &= \max \mathbf{Z}(v_{\mathbf{c}}(\operatorname{Ind}(\mathcal{L}))) \cup \{0\} \\ &= \max \mathbf{Z}(\operatorname{Ind}(\mathcal{L})) \cup \{0\} = N.\end{aligned}$$

By Remark 4.13, every polynomial solution of $\mathcal{L}_{\mathbf{c}}$ has degree not greater than N. □

To investigate the behavior of the certificates of hypergeometric solutions under specialization, we need to recall the algorithm given in [20] for finding hypergeometric solutions. Denote

$$\mathcal{S}_{\mathcal{L}} = \left\{ (p, q) \in \overline{k(\mathbb{X})}[x] \;\middle|\; p, q \text{ are monic and } p|a_0(x), q|a_n(x - n + 1) \right\}.$$

Algorithm 4.15. *Input: $\mathcal{L}(y) := \sum_{i=0}^{n} a_i(x)\sigma^i(y)$ with polynomial $a_i(x)$*
Output: the certificate of a hypergeometric solution of $\mathcal{L}(y) = 0$ if there exists; otherwise 0.

(a) *For each $(p, q) \in \mathcal{S}_{\mathcal{L}}$ 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 $\alpha_i := \operatorname{coeff}(P_i(x), x, m)$ for all $0 \le i \le n$;*
  (3) *let $\mathcal{Z}_{p,q} \subset \overline{k(\mathbb{X})}$ 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 the linear difference equation*

$$\mathcal{L}_{p,q,\beta} = \sum_{i=0}^{n} \beta^i P_i(x)\sigma^i = 0$$

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

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

Note that one can test if $\mathcal{L}_{p,q,\beta}(y) = 0$ has a polynomial solution by Algorithm Poly in [20].

(b) *Return* 0.

Let $\mathcal{S}_{\mathcal{L}}, \mathcal{Z}_{p,q}, \mathcal{L}_{p,q,\beta}$ be as in Algorithm 4.15. We set

$$N(\mathcal{L}) = \max\{0\} \cup \mathbf{Z}\left(\prod_{(p,q)\in\mathcal{S}_{\mathcal{L}},\beta\in\mathcal{Z}_{p,q}} \mathrm{Ind}(\mathcal{L}_{p,q,\beta})\right) + \max\{\deg(a_n), \deg(a_0)\}.$$

Recall that the above algorithm allows one to compute the certificates of all hypergeometric solutions of $\mathcal{L}$. The certificates in the output are of degree not greater than

$$\begin{aligned}\max_{(p,q)\in\mathcal{S}_{\mathcal{L}},Q\in\mathcal{P}}\left\{\deg\left(\frac{p(x)}{q(x)}\frac{Q(x+1)}{Q(x)}\right)\right\} &\le \max_{(p,q)\in\mathcal{S}_{\mathcal{L}},Q\in\mathcal{P}}\{\deg(p)+\deg(Q), \deg(q)+\deg(Q)\}\\ &\le \max\{\deg(a_0),\deg(a_n)\} + \max_{Q\in\mathcal{P}}\{\deg(Q)\},\end{aligned}$$

where $\mathcal{P}$ is the set of all polynomial solutions of $\mathcal{L}_{p,q,\beta}(y) = 0$ for all $(p,q) \in \mathcal{S}_{\mathcal{L}}$ and $\beta \in \mathcal{Z}_{p,q}$. If $Q(x)$ is a polynomial solution of $\mathcal{L}_{p,q,\beta}(y) = 0$, then $\deg(Q)$ is not greater than $\max\{0\} \cup \mathbf{Z}(\mathrm{Ind}(\mathcal{L}_{p,q,\beta}))$ by Remark 4.13. Therefore by definition $N(\mathcal{L})$ is a hyper-bound for $\mathcal{L}$. Moreover, we have the following result.

Lemma 4.16. *There is a basic open subset U of $\mathbb{X}$ such that for any $\mathbf{c} \in U$, $N(\mathcal{L})$ is a hyper-bound for $\mathcal{L}_{\mathbf{c}}$.*

Proof. Let $\mathcal{S}_{\mathcal{L}}, f_{p,q}, \mathcal{Z}_{p,q}, \mathcal{L}_{p,q,\beta}$ be as in Algorithm 4.15 and let

$$W = \{1, \mathrm{lc}(a_0(x)), \cdots, \mathrm{lc}(a_n(x))\} \bigcup \mathbb{V}(a_n(x)) \bigcup \mathbb{V}(a_0(x)) \bigcup \bigcup_{(p,q)\in\mathcal{S}_{\mathcal{L}}} \mathcal{Z}_{p,q},$$

where $\mathbb{V}(a_i(x))$ denotes the set of roots of $a_i(x) = 0$ in $\overline{k(\mathbb{X})}$. Let $\tilde{D} \subset \overline{k(\mathbb{X})}$ be a finitely generated $k[\mathbb{X}]$-algebra such that $W \subset \tilde{D}$ and let $\mathbb{Y}$ be the variety over k associated to $\tilde{D}$. Let Γ be the subgroup of $\mathbb{G}_a(\overline{k(\mathbb{X})})$ generated by W. Suppose that $\mathbf{c} \in \mathcal{B}(\mathbb{Y}, \Gamma)$. It is easy to see that $\mathcal{S}_{\mathcal{L}_{\mathbf{c}}} = v_{\mathbf{c}}(\mathcal{S}_{\mathcal{L}})$. Furthermore one sees that for each $(v_{\mathbf{c}}(p), v_{\mathbf{c}}(q)) \in \mathcal{S}_{\mathcal{L}_{\mathbf{c}}}$,

$$f_{v_{\mathbf{c}}(p),v_{\mathbf{c}}(q)} = v_{\mathbf{c}}(f_{p,q}),\ \mathcal{Z}_{v_{\mathbf{c}}(p),v_{\mathbf{c}}(q)} = v_{\mathbf{c}}(\mathcal{Z}_{p,q}),$$

and for each $\beta \in \mathcal{Z}_{p,q}$, $\mathcal{L}_{v_{\mathbf{c}}(p),v_{\mathbf{c}}(q),v_{\mathbf{c}}(\beta)} = v_{\mathbf{c}}(\mathcal{L}_{p,q,\beta})$. This together with Algorithm 4.15 implies that all certificates of hypergeometric solutions of $\mathcal{L}_{\mathbf{c}}(y) = 0$ are of the form

$$v_{\mathbf{c}}(\beta)\frac{v_{\mathbf{c}}(p)}{v_{\mathbf{c}}(q)}\frac{\bar{Q}(x+1)}{\bar{Q}(x)}, \tag{4.8}$$

where $(p,q) \in \mathcal{S}_{\mathcal{L}}, \beta \in \mathcal{Z}_{p,q}$ and $\bar{Q}(x)$ is a nonzero polynomial solution of the linear difference equation $\mathcal{L}_{v_{\mathbf{c}}(p),v_{\mathbf{c}}(q),v_{\mathbf{c}}(\beta)}(y) = 0$. Now let $\tilde{U}_{p,q,\beta}$ be a basic open subset of $\mathbb{Y}$ such that for any $\mathbf{c} \in \tilde{U}_{p,q,\beta}$, nonzero polynomial solutions of $v_{\mathbf{c}}(\mathcal{L}_{p,q,\beta})(y) = 0$, i.e., $\bar{Q}(x)$, are of degree not greater than

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

Such $\tilde{U}_{p,q,\beta}$ exists due to Lemma 4.14. Set

$$U = \mathcal{B}(\mathbb{Y}, \Gamma) \bigcap \bigcap_{(p,q)\in\mathcal{S}_{\mathcal{L}},\beta\in\mathcal{Z}_{p,q}} \tilde{U}_{p,q,\beta}.$$

Then for any $\mathbf{c} \in U$, the degrees of rational functions in (4.8) are not greater than $N(\mathcal{L})$ and so $N(\mathcal{L})$ is a hyper-bound for $\mathcal{L}_{\mathbf{c}}$. The lemma then follows from Lemma 2.3 and the fact that $\mathcal{L}_{\mathbf{c}} = \mathcal{L}_{p_{\mathbb{Y}/\mathbb{X}}(\mathbf{c})}$. □

Lemma 4.17. *There are a coefficient bound N of ν-maximal σ_A-ideals and a basic open subset U of $\mathbb{X}$ such that N is also a coefficient bound of ν-maximal $\sigma_{A(\mathbf{c})}$-ideals for all $\mathbf{c} \in U$.*

Proof. We keep notation as before. For each $l = 1, 2, \cdots, \ell$, by the method developed in Section 1 of [1], compute a matrix $T_l \in \mathrm{GL}_{\binom{\ell}{l}}(\overline{k(\mathbb{X})}(x))$ such that under the transformation T_l, $\sigma_{\Phi_{\ell,l}(\mathrm{Sym}_\nu(A))^{-t}}(Y) = \Phi_{\ell,l}(\mathrm{Sym}_\nu(A))^{-t}Y$ is equivalent to a linear difference operator $\mathcal{L}_l$. Let N_l be a hyper-bound for $\mathcal{L}_l$. Set

$$N = \ell \cdot \max_{1\le l\le \ell}\{2\tilde{\mu}\deg(T_l^{-1}) + 2\tilde{\mu}(\tilde{\mu}-1)N_l\},$$

where $\tilde{\mu} = \max\{\binom{\ell}{l} | 1 \le l \le \ell\}$. Then by (4.7) and Claim 4.9, N is a coefficient bound of ν-maximal σ_A-ideals. Let $\tilde{D} \subset \overline{k(\mathbb{X})}$ be a finitely generated $k[\mathbb{X}]$-algebra such that the entries of T_l, T_l^{-1} and $\Phi_{\ell,l}(\mathrm{Sym}_\nu(A))^{-t}$ are in the field of fractions of $\tilde{D}[x]$ for all $l = 1, 2, \cdots, \ell$, and let $\mathbb{Y}$ be the variety over k associated to $\tilde{D}$. Take a nonzero $\tilde{h} \in \tilde{D}$ such that for any $\tilde{\mathbf{c}} \in \mathbb{Y}_{\tilde{h}}$ and all $l = 1, 2, \cdots, \ell$, $v_{\tilde{\mathbf{c}}}(T_l)$ and $A(\tilde{\mathbf{c}})$ are well-defined and invertible, and $\sigma_{\Phi_{\ell,l}(\mathrm{Sym}_\nu(A(\tilde{\mathbf{c}})))^{-t}}(Y) = \Phi_{\ell,l}(\mathrm{Sym}_\nu(A(\tilde{\mathbf{c}})))^{-t}Y$ is equivalent to the linear difference operator $v_{\tilde{\mathbf{c}}}(\mathcal{L}_l)$ under the transformation $v_{\tilde{\mathbf{c}}}(T_l)$. Due to Lemma 4.16, there is a basic open subset U_1 of $\mathbb{X}$ such that N_l is a hyper-bound for $v_{\mathbf{c}}(\mathcal{L}_l)$ for all $l = 1, 2, \cdots, \ell$ and all $\mathbf{c} \in U_1$. By Lemma 2.2, there is a nonempty open subset U_2 of $\mathbb{X}$ such that $U_2 \subset p_{\mathbb{Y}/\mathbb{X}}(\mathbb{Y}_{\tilde{h}})$. Set $U = U_1 \cap U_2$ and suppose that $\mathbf{c} \in U$. Let $\tilde{\mathbf{c}}$ be an element in $\mathbb{Y}_{\tilde{h}} \cap p^{-1}_{\mathbb{Y}/\mathbb{X}}(\mathbf{c})$. One sees that $\deg(v_{\tilde{\mathbf{c}}}(T_l^{-1})) \le \deg(T_l^{-1})$, and by (4.7) and Claim 4.9 again,

$$\tilde{N} = \ell \cdot \max_{1\le l\le \ell}\{2\tilde{\mu}\deg(v_{\tilde{\mathbf{c}}}(T_l^{-1})) + 2\tilde{\mu}(\tilde{\mu}-1)N_l\}$$

is a coefficient bound of ν-maximal $\sigma_{A(\tilde{\mathbf{c}})}$-ideals. The lemma then follows from Lemma 2.3 and the facts that $N \ge \tilde{N}$ and $A(\tilde{\mathbf{c}}) = A(\mathbf{c})$. □

Remark 4.18. The coefficient bound N given in Lemma 4.17 only depends on the matrix A and the given integer ν.

4.2. **ν-Maximal σ_A-ideals under specialization.** Let I_ν be a ν-maximal σ_A-ideal in $\overline{k(\mathbb{X})}(x)[X, 1/\det(X)]$ and $\mathrm{I}(m, I_\nu)$ as in (4.1). The aim of this subsection is to prove that I_ν is sent to a ν-maximal $\sigma_{A(\mathbf{c})}$-ideal by $v_{\mathbf{c}}$ for all $\mathbf{c}$ in some basic open subset of $\mathbb{X}$. We shall first prove that for each $m \ge 0$ there exists a basic open subset U of $\mathbb{X}$ such that for any ν-maximal $\sigma_{A(\mathbf{c})}$-ideal $J_{\mathbf{c}}$ in $k[X, 1/\det(X)]$ with $\mathbf{c} \in U$, the dimension of $\mathrm{I}(m, J_{\mathbf{c}})$ is equal to that of $\mathrm{I}(m, I_\nu)$. To this end, we need the following definition.

Definition 4.19. The dimension of (1.1) is defined to be the dimension of the vector space over $\overline{k(\mathbb{X})}$ spanned by the entries of a fundamental matrix of (1.1), denoted by $\dim([A])$.

Given a fundamental matrix $\mathcal{F}$ of (1.1), there is a linear difference operator $\mathcal{L} \in \overline{k(\mathbb{X})}(x)[\sigma]$ whose solution space is spanned by the entries of $\mathcal{F}$. Moreover, for such $\mathcal{L}$ one has that $\mathrm{ord}(\mathcal{L}) = \dim([A])$. Such $\mathcal{L}$ can be constructed as follows. Let $\mathbf{v}_j$ be the jth column of $\mathcal{F}$. Then $\mathcal{L}$ is an operator of minimal order that annihilates all $\mathbf{v}_j$, i.e., all entries of $\mathbf{v}_j$ for all j. Note that as $\mathcal{F}$ has n^2 entries, by definition, $\dim([A]) \le n^2$ and thus $\mathrm{ord}(\mathcal{L}) \le n^2$. For each $l = 1, \cdots, n^2$, $\sigma^l(\mathbf{v}_j) = A_l\mathbf{v}_j$ for all $j = 1, \cdots, n$, where $A_l = \sigma^{l-1}(A)\cdots\sigma(A)A$. Assume that $a_0, \cdots, a_s \in \overline{k(\mathbb{X})}(x)$ with $s \le n^2$. Then $\sum_{l=0}^{s} a_l\sigma^l(\mathbf{v}_j) = 0$ for all $j = 1, \cdots, n$ if

and only if $a_0\mathbf{v}_j + \sum_{l=1}^{s} a_l A_l \mathbf{v}_j = 0$ for all $j = 1, \cdots, n$. The latter equalities are equivalent to

$$a_0 I_n + \sum_{l=1}^{s} a_l A_l = 0$$

because $\mathcal{F} = (\mathbf{v}_1, \cdots, \mathbf{v}_n)$ is invertible. Let $\{\mathbf{e}_1, \cdots, \mathbf{e}_n\}$ be the standard basis of $\overline{k(\mathbb{X})}(x)^n$. Set

$$\mathcal{M}_A = \begin{pmatrix} \mathbf{e}_1^t & \mathbf{e}_2^t & \cdots & \mathbf{e}_n^t \\ A_1^{[1]} & A_1^{[2]} & \cdots & A_1^{[n]} \\ A_2^{[1]} & A_2^{[2]} & \cdots & A_2^{[n]} \\ \vdots & \vdots & & \vdots \\ A_{n^2}^{[1]} & A_{n^2}^{[2]} & \cdots & A_{n^2}^{[n]} \end{pmatrix}, \tag{4.9}$$

where $A_i^{[j]}$ denotes the jth row of A_i. Then $\mathcal{M}_A$ is a $(1 + n^2) \times n^2$ matrix with entries in $\overline{k(\mathbb{X})}(x)$, and one sees that $a_0 I_n + \sum_{l=1}^{s} a_l A_l = 0$ if and only if $(a_0, \cdots, a_s, 0, \cdots, 0)$ is in the left kernel of $\mathcal{M}_A$. Let $(b_0, \cdots, b_s, 0, \cdots, 0)$ be an element of the left kernel of $\mathcal{M}_A$ satisfying that $b_s \neq 0$ and s is as small as possible. Then $\mathcal{L}$ can be chosen to be $\sum_{i=0}^{s} b_i \sigma^i$ and $s = \operatorname{ord}(\mathcal{L}) = \dim([A])$. The above construction indicates the following lemma.

Lemma 4.20. *There is a nonempty open subset U of $\mathbb{X}$ such that if $\mathbf{c} \in U$, then*

$$\dim([A]) = \dim([A(\mathbf{c})]).$$

Proof. We first show that $\dim([A]) = \operatorname{rank}(\mathcal{M}_A)$, where $\mathcal{M}_A$ is given as in (4.9). Denote $r = \dim([A])$. If $\operatorname{rank}(\mathcal{M}_A) < r$. then the first r rows of $\mathcal{M}_A$ are linearly dependent over $k(\mathbb{X})(x)$. This implies that the left kernel of $\mathcal{M}_A$ contains a nonzero element of the form $(b_0, \cdots, b_{r-1}, 0, \cdots, 0)$. The above construction then implies that $\dim([A]) \leq r - 1$, a contradiction. So $\operatorname{rank}(\mathcal{M}_A) \geq r$. On the other hand, assume that $\mathcal{L} = \sum_{i=0}^{r} b_i \sigma^i$. Without loss of generality, we may assume that $b_r = 1$. Then since $\mathcal{L}$ annihilates all entries of $\mathbf{v}_j$, one has that

$$\sigma^r(\mathbf{v}_j) = -\sum_{i=0}^{r-1} b_i \sigma^i(\mathbf{v}_j) \forall\, j = 1, \cdots, n, \tag{4.10}$$

where $\mathbf{v}_j$ is the jth column of $\mathcal{F}$. Applying σ to (4.10) successively yields that for each $l = 0, \cdots, n^2 - r$,

$$A_{r+l}\mathbf{v}_j = \sigma^{r+l}(\mathbf{v}_j) = \sum_{i=0}^{r-1} c_{l,i}\sigma^i(\mathbf{v}_j) = \sum_{i=0}^{r-1} c_{l,i} A_i \mathbf{v}_j \,\forall\, j = 1, \cdots, n,$$

where $c_{l,i} \in k(\mathbb{X})(x)$. Hence $A_{r+l} - \sum_{i=0}^{r-1} c_{l,i} A_i = 0$, because $\mathcal{F} = (\mathbf{v}_1, \cdots, \mathbf{v}_n)$ is invertible. Consequently, the $(r+l)$th row of $\mathcal{M}_A$ is a linear combination of the first r rows of $\mathcal{M}_A$. Hence $\operatorname{rank}(\mathcal{M}_A) \leq r$. This proves that $\operatorname{rank}(\mathcal{M}_A) = r$. Similarly, one has that

$$\dim([A(\mathbf{c})]) = \operatorname{rank}(v_{\mathbf{c}}(\mathcal{M}_A)) = \operatorname{rank}(\mathcal{M}_{A(\mathbf{c})})$$

for all $\mathbf{c} \in \mathbb{X}_{\mathfrak{h}}$, where $\mathbb{X}_{\mathfrak{h}}$ is given as in Notation 4.1.

Now take a nonzero $g \in k[\mathbb{X}]$ such that $\operatorname{rank}(\mathcal{M}_A) = \operatorname{rank}(v_{\mathbf{c}}(\mathcal{M}_A))$ for any $\mathbf{c} \in \mathbb{X}_g$. Then for $\mathbf{c} \in \mathbb{X}_g \cap \mathbb{X}_{\mathfrak{h}}$, one has that

$$\dim([A]) = \operatorname{rank}(\mathcal{M}_A) = \operatorname{rank}(v_{\mathbf{c}}(\mathcal{M}_A)) = \operatorname{rank}(\mathcal{M}_{A(\mathbf{c})}) = \dim([A(\mathbf{c})]). \qquad \square$$

Now let us turn to the dimension of $\mathrm{I}(m, I_\nu)$. Let $\mathcal{F} = (f_{i,j})$ be a fundamental matrix of $\sigma_A(Y) = AY$ such that

$$I_\nu = \left\langle \left\{ p \in \overline{k(\mathbb{X})}(x)[X]_{\leq \nu} \;\middle|\; p(\mathcal{F}) = 0 \right\} \right\rangle_{\overline{k(\mathbb{X})}(x)}.$$

By Remark 4.7, the vector space spanned by the entries of $\mathrm{Sym}_\nu(\mathcal{F})$ is equal to the one spanned by all $\prod f_{i,j}^{s_{i,j}}$ with $0 \leq \sum s_{i,j} \leq \nu$. Set

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

and

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

Note that

$$\sigma(\mathrm{Sym}_\nu(\mathcal{F})) = \mathrm{Sym}_\nu(\sigma(\mathcal{F})) = \mathrm{Sym}_\nu(A\mathcal{F}) = \mathrm{Sym}_\nu(A)\mathrm{Sym}_\nu(\mathcal{F}).$$

We have that $\tilde{\mathcal{F}}$ is a fundamental matrix of $\sigma_A(Y) = \mathcal{L}_m^\nu(A)Y$, and the set of the 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

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

This implies that

$$\dim(\mathrm{I}(m, I_\nu)) = (m+1)\binom{n^2+\nu-1}{\nu} - \dim([\mathcal{L}_m^\nu(A)]). \tag{4.11}$$

Corollary 4.21. *Let m be a positive integer and let I_ν be a ν-maximal σ_A-ideal. Suppose that B is a $\overline{k(\mathbb{X})}$-basis of $\mathrm{I}(m, I_\nu)$ and $B \subset k[\mathbb{X}][x, X]$. Then there is a nonempty open subset U of $\mathbb{X}$ such that for any $\mathbf{c} \in U$, $v_{\mathbf{c}}(B)$ is a basis of $\mathrm{I}(m, \tilde{I}_{\mathbf{c}})$ where $\tilde{I}_{\mathbf{c}}$ is a ν-maximal $\sigma_{A(\mathbf{c})}$-ideal in $k(x)[X, 1/\det(X)]$.*

Proof. By Proposition 1.20 on page 15 of [26], I_ν has a zero ξ in $\mathrm{GL}_n(\overline{k(\mathbb{X})}(x))$. Write $B = \{b_1, \cdots, b_l\}$. Since B generates I_ν that is a σ_A-ideal, there is a matrix M with entries in $\overline{k(\mathbb{X})}(x)[X, 1/\det(X)]$ such that

$$\sigma_A((b_1, \cdots, b_l)) = (b_1, \cdots, b_l)M.$$

Let $\tilde{D} \subset \overline{k(\mathbb{X})}$ be a finitely generated $k[\mathbb{X}]$-algebra such that the entries of ξ and the coefficients of the entries of M are all in the fraction field of $\tilde{D}[x]$ and let $\mathbb{Y}$ be the variety over k associated to $\tilde{D}$. There is a nonzero $g \in \tilde{D}$ such that for any $\tilde{\mathbf{c}} \in \mathbb{Y}_g$, $v_{\tilde{\mathbf{c}}}(\xi), v_{\tilde{\mathbf{c}}}(M)$ are well-defined and $v_{\tilde{\mathbf{c}}}(\xi)$ is invertible. Then

$$\begin{aligned}\sigma_{A(\tilde{\mathbf{c}})}((v_{\tilde{\mathbf{c}}}(b_1), \cdots, v_{\tilde{\mathbf{c}}}(b_l))) &= v_{\tilde{\mathbf{c}}}\left(\sigma_A((b_1, \cdots, b_l))\right) = v_{\tilde{\mathbf{c}}}\left((b_1, \cdots, b_l)M\right) \\ &= (v_{\tilde{\mathbf{c}}}(b_1), \cdots, v_{\tilde{\mathbf{c}}}(b_l))v_{\tilde{\mathbf{c}}}(M).\end{aligned}$$

Hence for any $\tilde{\mathbf{c}} \in \mathbb{Y}_g$, $\langle v_{\tilde{\mathbf{c}}}(B)\rangle_{k(x)}$ is a $\sigma_{A(\tilde{\mathbf{c}})}$-ideal. Furthermore, $v_{\tilde{\mathbf{c}}}(\xi)$ is a zero of this ideal in $\mathrm{GL}_n(k(x))$. This implies that for such $\tilde{\mathbf{c}}$, $1 \notin \langle v_{\tilde{\mathbf{c}}}(B)\rangle_{k(x)}$ and then $v_{\tilde{\mathbf{c}}}(B)$ is contained in some ν-maximal $\sigma_{A(\tilde{\mathbf{c}})}$-ideal, say $\tilde{I}_{\tilde{\mathbf{c}}}$, because every polynomial in $v_{\tilde{\mathbf{c}}}(B)$ is of degree in X not greater than ν. Using the arguments similar to those after Lemma 4.20, one has that

$$\dim(\mathrm{I}(m, \tilde{I}_{\tilde{\mathbf{c}}})) = (m+1)\binom{n^2+\nu-1}{\nu} - \dim([\mathcal{L}_m^\nu(A(\tilde{\mathbf{c}}))]). \tag{4.12}$$

Let $\tilde{U}$ be a nonempty open subset of $\mathbb{Y}$ satisfying that for any $\tilde{\mathbf{c}} \in \tilde{U}$,

(1) $\dim([\mathcal{L}_m^\nu(A)]) = \dim([v_{\tilde{\mathbf{c}}}(\mathcal{L}_m^\nu(A))])$ and $v_{\tilde{\mathbf{c}}}(\mathcal{L}_m^\nu(A)) = \mathcal{L}_m^\nu(A(\tilde{\mathbf{c}}))$; and
(2) $v_{\tilde{\mathbf{c}}}(B)$ is linearly independent over k and $|B| = |v_{\tilde{\mathbf{c}}}(B)|$.

Such $\tilde{U}$ exists due to Lemma 4.20. Combining equalities (4.11) and (4.12), one sees that for any $\tilde{\mathbf{c}} \in \mathbb{Y}_g \cap \tilde{U}$,

$$|v_{\tilde{\mathbf{c}}}(B)| = |B| = \dim(\mathrm{I}(m, I_\nu)) = \dim(\mathrm{I}(m, \tilde{I}_{\tilde{\mathbf{c}}})),$$

which implies that $v_{\tilde{\mathbf{c}}}(B)$ is a basis of $\mathrm{I}(m, \tilde{I}_{\tilde{\mathbf{c}}})$. The corollary then follows from Lemma 2.2 and the fact that $v_{\tilde{\mathbf{c}}}(B) = v_{p_{\mathbb{Y}/\mathbb{X}}(\tilde{\mathbf{c}})}(B)$. □

Proposition 4.22. *Let I_ν be a ν-maximal σ_A-ideal and let N be the integer obtained in Lemma 4.17. Suppose that $\mathrm{I}(N, I_\nu)$ has a $\overline{k(\mathbb{X})}$-basis B contained in $k[\mathbb{X}][x, X]$. Then there is a basic open subset U of $\mathbb{X}$ such that for any $\mathbf{c} \in U$, $v_{\mathbf{c}}(B)$ is a k-basis of $\mathrm{I}(N, \tilde{I}_{\mathbf{c}})$ for some ν-maximal $\sigma_{A(\mathbf{c})}$-ideal $\tilde{I}_{\mathbf{c}}$ in $k(x)[X, 1/\det(X)]$. In particular, $v_{\mathbf{c}}(B)$ generates $\tilde{I}_{\mathbf{c}}$.*

Proof. By Lemma 4.17, there is a basic open subset U_1 of $\mathbb{X}$ such that N is a coefficient bound for not only ν-maximal σ_A-ideals but also ν-maximal $\sigma_{A(\mathbf{c})}$-ideals for all $\mathbf{c} \in U_1$. By Corollary 4.21, there is a nonempty open subset U_2 of $\mathbb{X}$ such that for any $\mathbf{c} \in U_2$, one has that $v_{\mathbf{c}}(B)$ is a basis of $\mathrm{I}(N, \tilde{I}_{\mathbf{c}})$ for some ν-maximal $\sigma_{A(\mathbf{c})}$-ideal $\tilde{I}_{\mathbf{c}}$. Set $U = U_1 \cap U_2$. The proposition then follows from the fact that $\mathrm{I}(N, \tilde{I}_{\mathbf{c}})$ generates $\tilde{I}_{\mathbf{c}}$. □

5. Difference Galois groups under specialization

The aim of this section is to prove Theorem 1.2. To begin, let us recall some notation and basic concepts in difference Galois theory. Let $\mathfrak{m}$ be a maximal σ_A-ideal of $\overline{k(\mathbb{X})}(x)[X, 1/\det(X)]$ and let

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

Then $\mathcal{R}$ is the Picard-Vessiot ring of $\overline{k(\mathbb{X})}(x)$ for (1.1). The Galois group $\mathcal{G}$ of (1.1) over $\overline{k(\mathbb{X})}(x)$ is defined to be the set of $\overline{k(\mathbb{X})}(x)$-automorphisms of $\mathcal{R}$ which commute with σ_A. Set $\bar{X} = X \mod \mathfrak{m}$. Then $\bar{X}$ is a fundamental matrix of (1.1), which induces a group homomorphism from $\mathcal{G}$ to $\mathrm{GL}_n(\overline{k(\mathbb{X})})$ given by sending $\phi \in \mathcal{G}$ to $\bar{X}^{-1}\phi(\bar{X})$. The image of this homomorphism is an algebraic subgroup of $\mathrm{GL}_n(\overline{k(\mathbb{X})})$ and this image can be obtained by computing the stabilizer of $\mathfrak{m}$. The stabilizer of an ideal I in $\overline{k(\mathbb{X})}(x)[X, 1/\det(X)]$, denoted by $\mathrm{stab}(I)$, is defined to be the set of elements $g \in \mathrm{GL}_n(\overline{k(\mathbb{X})})$ satisfying that $\{p(Xg) | p \in I\} = I$, which is an algebraic subgroup of $\mathrm{GL}_n(\overline{k(\mathbb{X})})$. It is well known that the stabilizer of $\mathfrak{m}$ is the image of $\mathcal{G}$ under the homomorphism induced by a fundamental matrix that is a zero of $\mathfrak{m}$. Throughout this section, Galois groups always mean the stabilizers of maximal σ_A-ideals. The readers are referred to Chapter 1 of [26] for more details on difference Galois theory.

5.1. **A criterion for difference Galois groups.** Proto-Galois groups play an essential role in the computation of 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 below can be verified algorithmically. Let us first recall what proto-Galois groups are.

Definition 5.1. Let G, H be two algebraic subgroups of $\mathrm{GL}_n(\overline{k(\mathbb{X})})$. H is said to be a proto-group of G if it satisfies the following condition:

$$H^t \leq G^\circ \leq G \leq H,$$

where H^t denotes the algebraic subgroup of H generated by unipotent elements. In the case when G is the Galois group of $\sigma_A(Y) = AY$ over $\overline{k(\mathbb{X})}(x)$, H is called a proto-Galois group of $\sigma_A(Y) = AY$ over $\overline{k(\mathbb{X})}(x)$.

Remark 5.2. (1) Since H^t is connected, $H^t \subset H^\circ$. So 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 $g \in \mathrm{GL}_n(\overline{k(\mathbb{X})})$. Then H is a proto-group of gGg^{-1} if and only if $gGg^{-1} \subset H$. To see this, it suffices to prove the "if" part. Note that if $h \in \mathrm{GL}_n(\overline{k(\mathbb{X})})$ is unipotent, then so is ghg^{-1}. Thus $gH^tg^{-1} \subset H^t$, because $gH^tg^{-1} \subset gGg^{-1} \subset H$. As both gH^tg^{-1} and H^t are connected and have the same dimension, $gH^tg^{-1} = H^t$. This implies that $H^t = gH^tg^{-1} \subset gGg^{-1} \subset H$.

(3) Suppose that H is a proto-Galois group of $\sigma_A(Y) = AY$ over $\overline{k(\mathbb{X})}(x)$ and $A \in H(\overline{k(\mathbb{X})}(x))$. Let $\tilde{H}$ be an algebraic subgroup of H. We claim that if $\sigma(h^{-1})Ah \in \tilde{H}(\overline{k(\mathbb{X})}(x))$ for some $h \in \mathrm{GL}_n(\overline{k(\mathbb{X})}(x))$, then H is a proto-group of $\tilde{H}$. Let G be the Galois group of $\sigma_A(Y) = AY$ over $\overline{k(\mathbb{X})}(x)$ satisfying that H is a proto-group of G. Proposition 1.21 of [26] implies that there is $g \in \mathrm{GL}_n(\overline{k(\mathbb{X})})$ such that $gGg^{-1} \subset \tilde{H}$. By (2), 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 $\mathrm{GL}_n(\overline{k(\mathbb{X})})$ such that $A \in H(\overline{k(\mathbb{X})}(x))$. It was proved in Proposition 1.21 of [26] that H is the Galois group of (1.1) over $\overline{k(\mathbb{X})}(x)$ if and only if for any $g \in H(\overline{k(\mathbb{X})}(x))$ and any proper algebraic subgroup $\tilde{H}$ of H one has that $\sigma(g^{-1})Ag \notin \tilde{H}(\overline{k(\mathbb{X})}(x))$. We shall refine this criterion when H is a proto-Galois group of (1.1) over $\overline{k(\mathbb{X})}(x)$. As an analogue of finite algebraic extensions in a differential case, we need to consider the power of σ. Let i be a positive integer. Obviously, every σ-ring (resp., field) is also a σ^i-ring (resp., field) and an easy calculation yields that $\sigma_A^i(X) = A_iX$, where A_i stands for $\sigma^{i-1}(A)\cdots\sigma(A)A$.

Definition 5.3. Let $s \geq 0$. The rational functions $a_1, \cdots, a_m \in \overline{k(\mathbb{X})}(x) \setminus \{0\}$ are said to be multiplicatively σ^s-independent if for any $d_i \in \mathbb{Z}$ and any $f \in \overline{k(\mathbb{X})}(x) \setminus \{0\}$, $\prod_{i=1}^m a_i^{d_i} = \sigma^s(f)/f$ implies that $d_1 = \cdots = d_m = 0$.

Lemma 5.4. *Let H be a connected algebraic subgroup of $\mathrm{GL}_n(\overline{k(\mathbb{X})})$ and $B \in H(\overline{k(\mathbb{X})}(x))$. Suppose that H is a proto-Galois group of $\sigma_B(Y) = BY$ over $\overline{k(\mathbb{X})}(x)$. Then H is the Galois group of $\sigma_B(Y) = BY$ over $\overline{k(\mathbb{X})}(x)$ if and only if $\{\chi(B) | \chi \in \mathfrak{X}\}$ is multiplicatively σ-independent, where $\mathfrak{X}$ is a basis of $\boldsymbol{\chi}(H)$.*

Proof. Suppose that H is the Galois group and there are integers $d_\chi, \chi \in \mathfrak{X}$, not all zero, such that

$$\prod_{\chi \in \mathfrak{X}} \chi^{d_\chi}(B) = \frac{\sigma(f)}{f}$$

for some $f \in \overline{k(\mathbb{X})}(x) \setminus \{0\}$. Set $\chi = \prod_{\chi \in \mathfrak{X}} \chi^{d_\chi}$. Then χ is a nontrivial character. Let I be the ideal in $\overline{k(\mathbb{X})}(x)[X, 1/\det(X)]$ generated by all vanishing polynomials

of H. Since $B \in H(\overline{k(\mathbb{X})}(x))$ and H is the Galois group, I is a maximal σ_B-ideal (see Lemma 1.10 and its proof on page 8 of [26]). Furthermore as H is connected, I is a prime ideal. Let $\bar{X} = X \mod I$ and $E = \overline{k(\mathbb{X})}(x)(\bar{X})$. Then $\bar{X}$ is a fundamental matrix of $\sigma_B(Y) = BY$ and it belongs to $H(E)$. An easy calculation yields that $\sigma_B(\chi(\bar{X}))/\chi(\bar{X}) = \sigma(f)/f$ and then $\sigma_B\left(\chi(\bar{X})f^{-1}\right) = \chi(\bar{X})f^{-1}$. In other words, $\chi(\bar{X})f^{-1}$ is a constant of E. Since E is the total Picard-Vessiot ring of $\sigma_B(Y) = BY$ and $\overline{k(\mathbb{X})}$ is algebraically closed, the field of constants of E is equal to $\overline{k(\mathbb{X})}$. Hence $\chi(\bar{X}) = cf$ for some $c \in \overline{k(\mathbb{X})}$. This implies that $\chi(X) - cf \in I$. As elements of $H(\overline{k(\mathbb{X})}(x))$ are zeros of I, putting $X = I_n$ in $\chi(X) - cf$ yields that $cf = 1$, and then putting $X = B$ in $\chi(X) - 1$ yields that $\chi(B) = 1$, i.e., $B \in \ker(\chi)$. Proposition 1.21 on page 15 of [26] implies that $\ker(\chi)$ contains H as a subgroup. Hence $\ker(\chi) = H$, i.e., χ is trivial. This contradicts the fact that χ is nontrivial.

Conversely, suppose that H is not the Galois group. Due to Proposition 1.21 of [26] again, there is $g \in H(\overline{k(\mathbb{X})}(x))$ and a proper algebraic subgroup $\tilde{H}$ of H such that $\sigma(g^{-1})Bg \in \tilde{H}(\overline{k(\mathbb{X})}(x))$. By Remark 5.2, H is a proto-group of $\tilde{H}$. By Proposition 2.6 of [9], $\tilde{H} \subset \ker(\chi)$ for some nontrivial character χ of H. This implies that $\chi(\sigma(g^{-1})Bg) = 1$, i.e., $\chi(B) = \sigma(\chi(g))/\chi(g)$. Consequently, $\chi(B), \chi \in \mathfrak{X}$ are multiplicatively σ-dependent. □

Recall that the above lemma still holds if we replace σ, B, and σ_B with σ^s, B_s, and σ_B^s, respectively, for some positive integer s. Now let us consider the general case.

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

(a) *$A_m \notin H^\circ(\overline{k(\mathbb{X})}(x))$ for all positive m with $m|\ell$ and $m \neq \ell$, and*
(b) *$\{\chi(A_\ell) \,|\, \chi \in \mathfrak{X}\}$ is multiplicatively σ^ℓ-independent,*

where $\ell = [H : H^\circ]$ and $\mathfrak{X}$ is a basis of $\chi(H^\circ)$.

Proof. Assume that H is the Galois group of $\sigma_A(Y) = AY$ over $\overline{k(\mathbb{X})}(x)$. Let I be a maximal σ_A-ideal in $\overline{k(\mathbb{X})}(x)[X, 1/\det(X)]$ such that $H = \mathrm{stab}(I)$, the stabilizer of I. For each positive integer m, note that I is a proper σ_A^m-ideal in $\overline{k(\mathbb{X})}(x)[X, 1/\det(X)]$, so there is a maximal σ_A^m-ideal, say $\tilde{I}_m$, containing I. By Lemma 4.1 of [9], $\tilde{I}_m \cap \sigma_A(\tilde{I}_m) \cap \cdots \cap \sigma_A^{m-1}(\tilde{I}_m)$ is a maximal σ_A-ideal. It is clear that each $\sigma_A^i(\tilde{I}_m)$ contains I as so does $\tilde{I}_m$. Thus

$$I = \tilde{I}_m \cap \sigma_A(\tilde{I}_m) \cap \cdots \cap \sigma_A^{m-1}(\tilde{I}_m)$$

because I is a maximal σ_A-ideal. Denote $H_m = \mathrm{stab}(\tilde{I}_m)$. Then H_m is the Galois group of $\sigma_A^m(Y) = A_m Y$ over $\overline{k(\mathbb{X})}(x)$. Due to Lemma 4.1 of [9] agian, H_m is a subgroup of finite index in H and furthermore $[H : H_m] \leq m$. This implies that H_m contains H° by Proposition on page 53 of [13]. Now if $A_m \in H^\circ(\overline{k(\mathbb{X})}(x))$ for some positive m with $m|\ell$ and $m \neq \ell$, then by Proposition 1.21 of [26], H_m is a subgroup of H°. This implies that $H_m = H^\circ$ and thus $[H : H_m] = \ell$, a contradiction with $[H : H_m] \leq m < \ell$. Therefore $A_m \notin H^\circ(\overline{k(\mathbb{X})}(x))$ for all positive m with $m|\ell$ and $m \neq \ell$, i.e., (a) holds. In addition, note that $\sigma^i(A) \in H(\overline{k(\mathbb{X})}(x))$ for all $i \geq 0$. From this, one sees that $A_\ell = \sigma^{\ell-1}(A) \cdots A \in H^\circ(\overline{k(\mathbb{X})}(x))$. By Proposition 1.21 of [26] again, H_ℓ is a subgroup of H°. However, H_ℓ contains H°. This implies

that $H_\ell = H^\circ$ and H° is the Galois group of $\sigma_A^\ell(Y) = A_\ell Y$ over $\overline{k(\mathbb{X})}(x)$. Then Lemma 5.4 with $\sigma_B = \sigma_A^\ell$ implies (b). This proves the necessary part.

It remains to show that (a) and (b) are sufficient. Suppose to the contrary that H is not the Galois group under the assumption that (a) and (b) hold. By Proposition 1.21 on page 15 of [26], there are $g \in H(\overline{k(\mathbb{X})}(x))$ and a proper algebraic subgroup $\tilde{H}$ of H such that $\sigma(g^{-1})Ag \in \tilde{H}(\overline{k(\mathbb{X})}(x))$. Write $g = h\xi$ with $h \in H^\circ(\overline{k(\mathbb{X})}(x))$ and $\xi \in H(\overline{k(\mathbb{X})})$. Then for $i > 0$

$$\sigma^i(g^{-1})A_i g = \prod_{j=0}^{i-1} \sigma^{i-1-j}\left(\sigma(g^{-1})Ag\right) = \xi^{-1}\sigma^i(h^{-1})A_i h\xi. \tag{5.1}$$

We claim that the condition (b) implies that $\tilde{H}^\circ = H^\circ$. To see this, suppose that $H^\circ \neq \tilde{H}^\circ$. Setting $i = \ell$ in (5.1), one has that

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

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 [9], there is a nontrivial character $\chi \in \boldsymbol{\chi}(H^\circ)$ such that $\tilde{H} \cap H^\circ \subset \ker(\chi)$, and so $\chi\left(\xi^{-1}\sigma^\ell(h^{-1})A_\ell h\xi\right) = 1$. Set $\tilde{\chi} = \chi(\xi^{-1}X\xi)$. Then $\tilde{\chi}$ is still a nontrivial character of H° and $\tilde{\chi}(A_\ell) = \sigma^\ell(\tilde{\chi}(h))/\tilde{\chi}(h)$. Write $\tilde{\chi} = \prod_{\chi\in\mathfrak{X}} \chi^{d_\chi}$ where $d_\chi \in \mathbb{Z}$ and not all of them are zero. Then one sees that $\{\chi(A_\ell)|\chi \in \mathfrak{X}\}$ is not multiplicatively σ^ℓ-independent, which contradicts the condition (b). Hence $H^\circ = \tilde{H}^\circ$. This proves the claim. Now let $m = [\tilde{H} : \tilde{H}^\circ]$. Then $m|\ell$ and setting $i = m$ in (5.1) yields that

$$\sigma^m(g^{-1})A_m g = \xi^{-1}\sigma^m(h^{-1})A_m h\xi \in \tilde{H}^\circ(\overline{k(\mathbb{X})}(x)) = H^\circ(\overline{k(\mathbb{X})}(x)).$$

So $A_m \in \sigma^m(h)\xi H^\circ(\overline{k(\mathbb{X})}(x))\xi^{-1}h^{-1}$. As $\xi H^\circ\xi^{-1} = H^\circ$ and $h \in H^\circ(\overline{k(\mathbb{X})}(x))$, $A_m \in H^\circ(\overline{k(\mathbb{X})}(x))$. The assumption (a) then implies that $m = \ell$, i.e., $\tilde{H} = H$. This contradicts the assumption that $\tilde{H}$ is a proper subgroup of H. Therefore H is the Galois group. □

Remark 5.6. Let H and A be as in Proposition 5.5.

(1) If H is connected, i.e., $\ell = [H : H^\circ] = 1$, then the condition (a) always holds and the proposition reduces to Lemma 5.4.
(2) Assume that $\tilde{H}$ is the Galois group of $\sigma_A(Y) = AY$ over $\overline{k(\mathbb{X})}(x)$. From the proof of the sufficient part of the proposition, one sees that (b) implies $H^\circ = \tilde{H}^\circ$. We claim that the converse is also true. Suppose that $H^\circ = \tilde{H}^\circ$. Since $\tilde{H}$ is a subgroup of H by Proposition 1.21 of [26], $[H : \tilde{H}]|\ell$. Denote $m_1 = [H : \tilde{H}]$ and $m_2 = [\tilde{H} : \tilde{H}^\circ] = \ell/m_1$. By Lemma 1.26 and Corollary 1.17 of [26], $\tilde{H}^\circ$ is the Galois group of $\sigma_A^{m_2}(Y) = A_{m_2}Y$ over $\overline{k(\mathbb{X})}(x)$. Note that $\sigma_A^\ell = (\sigma_A^{m_2})^{m_1}$ and $A_\ell = (A_{m_2})_{m_1}$. Applying Lemma 4.1 of [9] to $\sigma_A^{m_2}(Y) = A_{m_2}Y$ yields that $[\tilde{H}^\circ : \tilde{H}_\ell] \leq m_1$, where $\tilde{H}_\ell$ is the Galois group of $\sigma_A^\ell(Y) = A_\ell Y$ over $\overline{k(\mathbb{X})}(x)$. Hence $\tilde{H}_\ell = \tilde{H}^\circ = H^\circ$. Lemma 5.4 with $\sigma_B = \sigma_A^\ell$ then implies (b). This proves our claim.

5.2. **Proof of Theorem 1.2.** Before we prove the following proposition, let us first recall some results in [9]. Note that the reference [9] used some different notation, for instance ν-maximal σ_A-ideals are denoted by $I_{\mathcal{F},\nu}$ and the stabilizer

of $I_{\mathcal{F},\nu}$ is denoted by $H_{\mathcal{F},\nu}$. By Proposition 3.10 of [9], the stabilizer of a ν-maximal σ_A-ideal with sufficiently large ν is a proto-Galois group of $\sigma_A(Y) = AY$ over $\overline{k(\mathbb{X})}(x)$. Precisely, let ν be an integer greater than the integer $\tilde{d}$ given in Proposition 2.5 of [9], and let I_ν be a ν-maximal σ_A-ideal. Suppose that I is a maximal σ_A-ideal containing I_ν. Let $G = \mathrm{stab}(I)$ and $H = \mathrm{stab}(I_\nu)$ where stab() denotes the stabilizer. Then G is the Galois group of $\sigma_A(Y) = AY$ over $\overline{k(\mathbb{X})}(x)$. Proposition 3.7 of [9] implies that $\mathrm{Zero}(I_\nu)$ and $\mathrm{Zero}(I)$ are trivial $\overline{k(\mathbb{X})}(x)$-torsors for $H(\overline{k(\mathbb{X})(x)})$ and $G(\overline{k(\mathbb{X})(x)})$, respectively, where Zero() denotes the set of zeros in $\mathrm{GL}_n(\overline{k(\mathbb{X})(x)})$. Let $g \in \mathrm{Zero}(I) \cap \mathrm{GL}_n(\overline{k(\mathbb{X})}(x))$. Then

$$\mathrm{Zero}(I_\nu) = gH(\overline{k(\mathbb{X})(x)}) \supset \mathrm{Zero}(I) = gG(\overline{k(\mathbb{X})(x)}).$$

Thus $G \subset H$ and, moreover, H is a proto-group of G.

Proposition 5.7. *Let G be the Galois group of $\sigma_A(Y) = AY$ over $\overline{k(\mathbb{X})}(x)$. Assume that $A \in G(k(\mathbb{X})(x))$ and G is defined over $k[\mathbb{X}]$. Then there is a basic open subset U of $\mathbb{X}$ such that $G_{\mathbf{c}}$ is a proto-Galois group of $\sigma_{A(\mathbf{c})}(Y) = A(\mathbf{c})Y$ over $k(x)$ for any $\mathbf{c} \in U$, where $G_{\mathbf{c}}$ is defined as in Section 3.*

Proof. Let d be an integer greater than the integer $\tilde{d}$ given in Proposition 2.5 of [9]. Let $S \subset k[\mathbb{X}][X]$ be a finite set generating the vanishing ideal of G, and let I be the ideal in $\overline{k(\mathbb{X})}(x)[X, 1/\det(X)]$ generated by S. Since $A \in G(k(\mathbb{X})(x))$ and G is the Galois group, I is a maximal σ_A-ideal (see Lemma 1.10 and its proof on page 8 of [26]). Suppose that m is a positive integer such that all polynomials in S are of total degree in X not greater than m. Set

$$\nu = \max\{m, d\}.$$

Then I is a ν-maximal σ_A-ideal. Due to Lemma 4.17, there is a coefficient bound of I, say N, and a basic open subset U_1 of $\mathbb{X}$ such that for every $\mathbf{c} \in U_1$, N is also a coefficient bound of ν-maximal $\sigma_{A(\mathbf{c})}$-ideals in $k(x)[X, 1/\det(X)]$. Let B be a basis of $\mathrm{I}(N, I)$ where $\mathrm{I}(N, I)$ is defined as in (4.1). Let $\tilde{D} \subset \overline{k(\mathbb{X})}$ be a finitely generated $k[\mathbb{X}]$-algebra such that $B \subset \tilde{D}[x, X]$ and let $\mathbb{Y}$ be the variety over k associated to $\tilde{D}$. Because S and B generate the same ideal I, using an argument similar to that in Remark 3.1, one can prove that there is a nonempty open subset $\tilde{U}_1$ of $\mathbb{Y}$ such that for each $\tilde{\mathbf{c}} \in \tilde{U}_1$, $v_{\tilde{\mathbf{c}}}(S)$ and $v_{\tilde{\mathbf{c}}}(B)$ generate the same ideal in $k(x)[X, 1/\det(X)]$. By Proposition 4.22, there is a basic open subset $\tilde{U}_2$ of $\mathbb{Y}$ such that for any $\tilde{\mathbf{c}} \in \tilde{U}_2$, $v_{\tilde{\mathbf{c}}}(B)$ is a k-basis of $\mathrm{I}(N, \tilde{I}_{\tilde{\mathbf{c}}})$ for some ν-maximal $\sigma_{A(\tilde{\mathbf{c}})}$-ideal $\tilde{I}_{\tilde{\mathbf{c}}}$ in $k(x)[X, 1/\det(X)]$. In particular, $v_{\tilde{\mathbf{c}}}(B)$ generates $\tilde{I}_{\tilde{\mathbf{c}}}$. Then for any $\tilde{\mathbf{c}} \in \tilde{U}_1 \cap \tilde{U}_2$, $v_{\tilde{\mathbf{c}}}(B)$ and $v_{\tilde{\mathbf{c}}}(S)$ generate the same ideal $\tilde{I}_{\tilde{\mathbf{c}}}$. By Lemma 2.3, there is a basic open subset U_2 of $\mathbb{X}$ that is contained in $p_{\mathbb{Y}/\mathbb{X}}(\tilde{U}_1 \cap \tilde{U}_2)$. Due to Proposition 3.2, there is a basic open subset U_3 of $\mathbb{X}$ such that for any $\mathbf{c} \in U_3$, $v_{\mathbf{c}}(S)$ defines an algebraic subgroup $G_{\mathbf{c}}$ of $\mathrm{GL}_n(k)$. Now set $U = U_1 \cap U_2 \cap U_3$ and suppose $\mathbf{c} \in U$. Let $\tilde{\mathbf{c}} \in \tilde{U}_1 \cap \tilde{U}_2 \cap p^{-1}_{\mathbb{Y}/\mathbb{X}}(\mathbf{c})$. Then $G_{\mathbf{c}}(\overline{k(x)})$ is the variety in $\mathrm{GL}_n(\overline{k(x)})$ defined by $\tilde{I}_{\tilde{\mathbf{c}}}$ that is generated by $v_{\mathbf{c}}(S) (= v_{\tilde{\mathbf{c}}}(S))$. Let $H = \mathrm{stab}(\tilde{I}_{\tilde{\mathbf{c}}})$. Since $\tilde{I}_{\tilde{\mathbf{c}}}$ is ν-maximal, due to Proposition 3.7 of [9], $G_{\mathbf{c}}(\overline{k(x)})$ is a trivial $k(x)$-torsor for $H(\overline{k(x)})$. As $I_n \in G_{\mathbf{c}}$ and both $G_{\mathbf{c}}$ and H are defined over k, we have that $G_{\mathbf{c}} = H$, i.e., $G_{\mathbf{c}}$ is the stabilizer of $\tilde{I}_{\tilde{\mathbf{c}}}$. Proposition 3.10 of [9] and the choice of ν then imply that $G_{\mathbf{c}}$ is a proto-Galois group of $\sigma_{A(\tilde{\mathbf{c}})}(Y) = A(\tilde{\mathbf{c}})Y$ over $k(x)$. The proposition then follows from the fact that $A(\tilde{\mathbf{c}}) = A(\mathbf{c})$. □

Suppose that $\mathbf{a}=(a_1,\cdots,a_m)$ with $a_i\in\overline{k(\mathbb{X})}(x)\setminus\{0\}$ and $\ell\geq 0$. Denote

$$\mathcal{Z}(\mathbf{a},\ell)=\left\{\mathbf{d}=(d_1,\cdots,d_m)\in\mathbb{Z}^m\,\middle|\,\exists\, f\in\overline{k(\mathbb{X})}(x)\setminus\{0\}\text{ s.t. }\mathbf{a}^{\mathbf{d}}=\frac{\sigma^\ell(f)}{f}\right\},$$

where $\mathbf{a}^{\mathbf{d}}=a_1^{d_1}\cdots a_m^{d_m}$. Then $\mathcal{Z}(\mathbf{a},\ell)$ is a finitely generated $\mathbb{Z}$-module. We say a_i is ℓ-standard if for any α,β in the set of zeros and poles of a_i, $\alpha-\beta\in\ell\mathbb{Z}$ implies that $\alpha=\beta$. One has that if $a_i\notin\overline{k(\mathbb{X})}$, then $\sigma^\ell(a_i)/a_i$ is not ℓ-standard. To see this, write $a_i=\lambda\prod_{j=1}^s(x-c_j)^{d_j}$ where $\lambda,c_1,\cdots,c_s\in\overline{k(\mathbb{X})}$, $\lambda\neq 0$, $c_{j_1}\neq c_{j_2}$ if $j_1\neq j_2$, and all d_j are nonzero integers. Then

$$\frac{\sigma^\ell(a_i)}{a_i}=\prod_{j=1}^s\frac{(x-(c_j-\ell))^{d_j}}{(x-c_j)^{d_j}}.$$

Set $m_1=\min\{l|\exists\ c_i\text{ s.t. }c_1=c_i-l\ell\}$ and $m_2=\max\{l|\exists\ c_i\text{ s.t. }c_1=c_i-l\ell\}$. Then both $x-(c_1+(m_1-1)\ell)$ and $x-(c_1+m_2\ell)$ cannot be cancelled in $\sigma^\ell(a_i)/a_i$. That is to say, both $c_1+(m_1-1)\ell$ and $c_1+m_2\ell$ are in the set of zeros and poles of $\sigma^\ell(a_i)/a_i$. As the difference of $c_1+(m_1-1)\ell$ and $c_1+m_2\ell$ is equal to $(m_1-m_2-1)\ell$, that is, a nonzero element in $\ell\mathbb{Z}$, $\sigma^\ell(a_i)/a_i$ is not ℓ-standard.

Lemma 5.8. *Suppose that $\mathbf{a}=(a_1,\cdots,a_m)$ with $a_i\in k(\mathbb{X})(x)\setminus\{0\}$ and $\ell\geq 0$. Then there is a basic open subset U of $\mathbb{X}$ such that for any $\mathbf{c}\in U$, $a_1(\mathbf{c}),\cdots,a_m(\mathbf{c})$ are well-defined and $\mathcal{Z}(\mathbf{a},\ell)=\mathcal{Z}(v_{\mathbf{c}}(\mathbf{a}),\ell)$.*

Proof. Let W be the set of zeros and poles of $a_1,\cdots,a_m$ in $\overline{k(\mathbb{X})}$, and let $\boldsymbol{\alpha}\subset W$ be the representative of W in the quotient group $\overline{k(\mathbb{X})}/\ell\mathbb{Z}$. Suppose $\beta\in W$. Then $\beta=\alpha+\ell d$ for some $\alpha\in\boldsymbol{\alpha}$ and $d\in\mathbb{Z}$. If $d=0$, set $g=1$, otherwise set

$$g=\begin{cases}\prod_{l=1}^{d}(x-\alpha-\ell l)^{-1}, & d>0,\\ \prod_{l=0}^{-d-1}(x-\alpha+\ell l), & d<0.\end{cases}$$

Then $x-\beta=\sigma^\ell(g)(x-\alpha)/g$. Under the multiplication with $\sigma^\ell(g)/g$, we can replace $x-\beta$ by $x-\alpha$ for all a_i. Hence for every $i=1,\cdots,m$, we can write

$$a_i=\xi_i\frac{\sigma^\ell(f_i)}{f_i}\prod_{\alpha\in\boldsymbol{\alpha}}(x-\alpha)^{e_{i,\alpha}},$$

where $\xi_i\in k(\mathbb{X})\setminus\{0\}$, $e_{i,\alpha}\in\mathbb{Z}$, and $f_i\in\overline{k(\mathbb{X})}(x)\setminus\{0\}$ whose numerator and denominator are both monic. Set $\bar{a}_i=\prod_{\alpha\in\boldsymbol{\alpha}}(x-\alpha)^{e_{i,\alpha}}$ for all $i=1,\cdots,m$. One sees easily that $\mathbf{a}^{\mathbf{d}}=\sigma^\ell(f)/f$ if and only if $\boldsymbol{\xi}^{\mathbf{d}}=1$ and $\bar{\mathbf{a}}^{\mathbf{d}}=\sigma^\ell(\tilde{f})/\tilde{f}$, where $\boldsymbol{\xi}=(\xi_1,\cdots,\xi_m)$ and $\bar{\mathbf{a}}=(\bar{a}_1,\cdots,\bar{a}_m)$. Since $\bar{\mathbf{a}}^{\mathbf{d}}$ is ℓ-standard, if $\bar{\mathbf{a}}^{\mathbf{d}}=\sigma^\ell(\tilde{f})/\tilde{f}$, then $\tilde{f}\in\overline{k(\mathbb{X})}$. Therefore $\mathbf{a}^{\mathbf{d}}=\sigma^\ell(f)/f$ if and only if $\boldsymbol{\xi}^{\mathbf{d}}=1$ and $\bar{\mathbf{a}}^{\mathbf{d}}=1$. Namely,

$$\mathcal{Z}(\mathbf{a},\ell)=\mathcal{Z}(\boldsymbol{\xi},0)\cap\mathcal{Z}(\bar{\mathbf{a}},0).$$

Let Γ_1 be the subgroup of $\mathbb{G}_m(k(\mathbb{X}))$ generated by $\xi_1,\cdots,\xi_m$. Let $\tilde{D}\subset\overline{k(\mathbb{X})}$ be a finitely generated $k[\mathbb{X}]$-algebra such that $\Gamma_1,W\subset\tilde{D}$, and let $\mathbb{Y}$ be the variety over k associated to $\tilde{D}$. Let Γ_2 be the subgroup of $\mathbb{G}_a(\tilde{D})$ generated by $\{1\}\cup\boldsymbol{\alpha}$. Now assume that $\tilde{\mathbf{c}}\in\mathcal{B}(\mathbb{Y},\Gamma_1)\cap\mathcal{B}(\mathbb{Y},\Gamma_2)$. Then

$$a_i(\tilde{\mathbf{c}})=\xi_i(\tilde{\mathbf{c}})\frac{\sigma^\ell(f_i(\tilde{\mathbf{c}}))}{f_i(\tilde{\mathbf{c}})}\prod_{\alpha\in\boldsymbol{\alpha}}(x-\alpha(\tilde{\mathbf{c}}))^{e_{i,\alpha}},$$

and, moreover, $\alpha(\tilde{\mathbf{c}}) - \alpha'(\tilde{\mathbf{c}}) \notin \ell\mathbb{Z}$ if $\alpha \neq \alpha'$. A similar argument as above implies that $v_{\tilde{\mathbf{c}}}(\mathbf{a})^{\mathbf{d}} = \sigma^{\ell}(f')/f'$ if and only if $v_{\tilde{\mathbf{c}}}(\boldsymbol{\xi})^{\mathbf{d}} = 1$ and $v_{\tilde{\mathbf{c}}}(\bar{\mathbf{a}})^{\mathbf{d}} = 1$. In other words,

$$\mathcal{Z}(v_{\tilde{\mathbf{c}}}(\mathbf{a}), \ell) = \mathcal{Z}(v_{\tilde{\mathbf{c}}}(\boldsymbol{\xi}), 0) \cap \mathcal{Z}(v_{\tilde{\mathbf{c}}}(\bar{\mathbf{a}}), 0).$$

Since $\tilde{\mathbf{c}} \in \mathcal{B}(\mathbb{Y}, \Gamma_1)$, $\mathcal{Z}(v_{\tilde{\mathbf{c}}}(\boldsymbol{\xi}), 0) = \mathcal{Z}(\boldsymbol{\xi}, 0)$. Moreover, one has $\mathcal{Z}(v_{\tilde{\mathbf{c}}}(\bar{\mathbf{a}}), 0) = \mathcal{Z}(\bar{\mathbf{a}}, 0)$ for both of them are equal to

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

Consequently, $\mathcal{Z}(\mathbf{a}, \ell) = \mathcal{Z}(v_{\tilde{\mathbf{c}}}(\mathbf{a}), \ell)$. Lemma 2.3 then completes the proof. □

Corollary 5.9. *Let $\mathbf{a} = (a_1, \cdots, a_m), \ell$ be as in Lemma 5.8. Then there is a basic open subset U of $\mathbb{X}$ such that for any $\mathbf{c} \in U$, $a_1, \cdots, a_m$ are multiplicatively σ^{ℓ}-independent if and only if so are $a_1(\mathbf{c}), \cdots, a_m(\mathbf{c})$.*

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

Now we are ready to prove Theorem 1.2.

Proof of Theorem 1.2. By Theorem 2.7 of [12], there is $g \in \mathrm{GL}_n(\overline{k(\mathbb{X})}(x))$ such that $\sigma(g^{-1})Ag \in G(\overline{k(\mathbb{X})}(x))$. Denote $\tilde{A} = \sigma(g^{-1})Ag$. It is well known that $\sigma_{\tilde{A}}(Y) = \tilde{A}Y$ and $\sigma_A(Y) = AY$ have the same Galois group. Let $D' \subset \overline{k(\mathbb{X})}$ be a finitely generated $k[\mathbb{X}]$-algebra with F' as a field of fractions such that $g \in \mathrm{GL}_n(F'(x))$ and let $\mathbb{X}'$ be the variety over k associated to D'. Then there is $c' \in D'$ such that for any $\mathbf{c}' \in \mathbb{X}'_{c'}$, both $g(\mathbf{c}')$ and $A(\mathbf{c}')$ are well-defined and invertible. For such $\mathbf{c}'$, $\sigma_{A(\mathbf{c}')}(Y) = A(\mathbf{c}')Y$ and $\sigma_{\tilde{A}(\mathbf{c}')}(Y) = \tilde{A}(\mathbf{c}')Y$ have the same Galois group. Recall that $\tilde{A} \in G(k(\mathbb{X}')(x))$. Suppose that the theorem holds for $\sigma_{\tilde{A}}(Y) = \tilde{A}Y$ and V' is the corresponding basic open subset of $\mathbb{X}'$. Then for $\mathbf{c}' \in V' \cap \mathbb{X}'_{c'}$, $G_{\mathbf{c}'}$ is the Galois group of $\sigma_{A(\mathbf{c}')}(Y) = A(\mathbf{c}')Y$ over $k(x)$. By Lemma 2.3, there is a basic open subset V of $\mathbb{X}$ contained in $p_{\mathbb{X}'/\mathbb{X}}(V' \cap \mathbb{X}'_{c'})$. From the fact that $A(\mathbf{c}') = A(p_{\mathbb{X}'/\mathbb{X}}(\mathbf{c}'))$ and $G_{\mathbf{c}'} = G_{p_{\mathbb{X}'/\mathbb{X}}(\mathbf{c}')}$, one has that $G_{\mathbf{c}}$ is the Galois group of $\sigma_{A(\mathbf{c})}(Y) = A(\mathbf{c})Y$ over $k(x)$ for all $\mathbf{c} \in V$. Consequently, one only needs to prove the theorem for the case with $A \in G(\overline{k(\mathbb{X})}(x))$.

Let $\mathfrak{X} \subset \overline{k(\mathbb{X})}[X, 1/\det(X)]$ be a basis of $\boldsymbol{\chi}(G^{\circ})$, and let T be a finite set in $k(\mathbb{X})[X, 1/\det(X)]$ generating the vanishing ideal of G°. Let $\tilde{D} \subset \overline{k(\mathbb{X})}$ be a finitely generated $k[\mathbb{X}]$-algebra such that $T, \mathfrak{X} \subset \tilde{D}[X, 1/\det(X)]$ and let $\mathbb{Y}$ be the variety over k associated to $\tilde{D}$. Set $\ell = [G : G^{\circ}]$. Since G is the Galois group of $\sigma_A(Y) = AY$ over $\overline{k(\mathbb{X})}(x)$ and $A \in G(k(\mathbb{X})(x))$, Proposition 5.5 implies that $A_m \notin G^{\circ}(\overline{k(\mathbb{X})}(x))$ for all positive m with $m|\ell$ and $m \neq \ell$, and $\{\chi(A_\ell) | \chi \in \mathfrak{X}\}$ is multiplicatively σ^{ℓ}-independent. Thus, for all such m, there is $q_m \in T$ such that $q_m(A_m) \neq 0$. By Propositions 5.7, 3.2, and 3.5, there is a basic open subset $\tilde{U}_1$ of $\mathbb{Y}$ such that for any $\tilde{\mathbf{c}} \in \tilde{U}_1$, one has that,

(a) $G_{\tilde{\mathbf{c}}}$ is a proto-Galois group of $\sigma_{A(\tilde{\mathbf{c}})}(Y) = A(\tilde{\mathbf{c}})Y$ over $k(x)$, and
(b) $[G_{\tilde{\mathbf{c}}} : G^{\circ}_{\tilde{\mathbf{c}}}] = [G : G^{\circ}] = \ell$, and
(c) $v_{\tilde{\mathbf{c}}}(\mathfrak{X})$ is a basis of $\boldsymbol{\chi}(G^{\circ}_{\tilde{\mathbf{c}}})$.

By Corollary 5.9, there is a basic open subset $\tilde{U}_2$ of $\mathbb{Y}$ such that for any $\tilde{\mathbf{c}} \in \tilde{U}_2$, $\{v_{\tilde{\mathbf{c}}}(\chi(A_\ell)) | \chi \in \mathfrak{X}\}$ is multiplicatively σ^{ℓ}-independent. Let c be a nonzero element

in $\tilde{D}$ such that for any $\tilde{\mathbf{c}} \in \mathbb{Y}_c$, $v_{\tilde{\mathbf{c}}}(q_m(A_m)) \neq 0$ for all positive m with $m|\ell$ and $m \neq \ell$. Set

$$\tilde{U} = \tilde{U}_1 \cap \tilde{U}_2 \cap \mathbb{Y}_c$$

and assume that $\tilde{\mathbf{c}} \in U$. Since $v_{\tilde{\mathbf{c}}}(\chi(A_\ell)) = v_{\tilde{\mathbf{c}}}(\chi)(A(\tilde{\mathbf{c}})_\ell)$, $\{v_{\tilde{\mathbf{c}}}(\chi)(A(\tilde{\mathbf{c}})_\ell)|\chi \in \mathfrak{X}\}$ is multiplicatively σ^ℓ-independent, that is to say, $\{\bar{\chi}(A(\tilde{\mathbf{c}})_\ell)|\bar{\chi} \in v_{\tilde{\mathbf{c}}}(\mathfrak{X})\}$ is multiplicatively σ^ℓ-independent. On the other hand, for all positive m with $m|\ell$ and $m \neq \ell$, since $v_{\tilde{\mathbf{c}}}(q_m)(A(\tilde{\mathbf{c}})_m) = v_{\tilde{\mathbf{c}}}(q_m(A_m)) \neq 0$, $A(\tilde{\mathbf{c}})_m \notin G^\circ_{\tilde{\mathbf{c}}}(k(x))$. By Proposition 5.5, $G_{\tilde{\mathbf{c}}}$ is the Galois group of $\sigma_{A(\tilde{\mathbf{c}})}(Y) = A(\tilde{\mathbf{c}})Y$ over $k(x)$. The theorem then follows from Lemma 2.3 and the fact that $A(\tilde{\mathbf{c}}) = A(p_{\mathbb{Y}/\mathbb{X}}(\tilde{\mathbf{c}}))$ and $G_{\tilde{\mathbf{c}}} = G_{p_{\mathbb{Y}/\mathbb{X}}(\tilde{\mathbf{c}})}$. □

Example 5.10. Consider the linear difference equation $\sigma_A(Y) = AY$ with

$$A = \begin{pmatrix} x & t_1 x & 0 \\ x & x & 0 \\ 0 & 0 & t_2 \end{pmatrix},$$

where t_1, t_2 are parameters. Set $k = \bar{\mathbb{Q}}$ and $\mathbb{X} = k^2$. Then $k(\mathbb{X}) = k(t_1, t_2)$ and $A \in \mathrm{GL}_n(k(\mathbb{X})(x))$. Let $S = \{X_{11} - X_{22}, X_{12} - t_1 X_{21}, X_{13}, X_{23}, X_{31}, X_{32}\}$, and denote by H the variety in $\mathrm{GL}_3(\overline{k(\mathbb{X})})$ defined by S, i.e.,

$$H = \left\{ \begin{pmatrix} a & t_1 b & 0 \\ b & a & 0 \\ 0 & 0 & c \end{pmatrix} \middle| a, b, c \in \overline{k(\mathbb{X})}, c(a^2 - t_1 b^2) \neq 0 \right\}.$$

One can verify that H is connected and a basis of $\boldsymbol{\chi}(H)$ can be represented by

$$\mathfrak{X} = \{\chi_1 = X_{11} - \sqrt{t_1} X_{21}, \chi_2 = X_{11} + \sqrt{t_1} X_{21}, \chi_3 = X_{33}\}.$$

Furthermore, one can verify that $A \in H(\overline{k(\mathbb{X})}(x))$ and H is the Galois group of $\sigma_A(Y) = AY$ over $\overline{k(\mathbb{X})}(x)$. We shall find a basic open subset U of $\mathbb{X}$ such that $H_{\mathbf{c}}$ is the Galois group of $\sigma_{A(\mathbf{c})} = A(\mathbf{c})Y$ over $k(x)$ for all $\mathbf{c} \in U$. For the sake of simplicity, at some steps, we do not follow the proofs of preceding lemmas or propositions to get the corresponding basic open sets.

First of all, $A(\mathbf{c})$ is invertible only if $\mathbf{c} \in \mathbb{X}_{(t_1-1)t_2}$. Moreover, if $\mathbf{c} \in \mathbb{X}_{(t_1-1)t_2}$, $H_{\mathbf{c}}$ is a connected algebraic subgroup of $\mathrm{GL}_3(k)$. It is easy to see that if $\mathbf{c} \in \mathbb{X}_{t_1(t_1-1)t_2}$, then $A(\mathbf{c}) \in H_{\mathbf{c}}(k(x))$ and $H^t_{\mathbf{c}} = \{\mathbf{1}\}$. Thus for such $\mathbf{c}$, $H_{\mathbf{c}}$ is a proto-Galois group of $\sigma_{A(\mathbf{c})}(Y) = A(\mathbf{c})Y$ over $k(x)$.

Second, since χ_i is defined over $k(\sqrt{t_1}, t_2)$, we need to extend $k[\mathbb{X}]$ to $k[t_1, t_2, \sqrt{t_1}]$ whose associated variety we denote by $\mathbb{Y}$. Because $H^t = \{\mathbf{1}\}$ and $H^t_{\tilde{\mathbf{c}}} = \{\mathbf{1}\}$ for any $\tilde{\mathbf{c}} \in \mathbb{Y}_{t_1(t_1-1)t_2}$, the proof of Proposition 3.5 implies that if $v_{\tilde{\mathbf{c}}}(\mathfrak{X})$ is multiplicatively independent, then it is a basis of $\boldsymbol{\chi}(H_{\tilde{\mathbf{c}}})$. In the proof of Proposition 3.5, take $g = (g_{i,j})$ with $g_{1,1} = g_{2,2} = 5/2, g_{1,2} = t_1 g_{2,1} = \sqrt{t_1}/2, g_{3,3} = 5$ and other entries being zero. Then one has that $\chi_1(g) = 2, \chi_2(g) = 3, \chi_3(g) = 5$. From this, one sees that if $\tilde{\mathbf{c}} \in \mathbb{Y}_{t_1(t_1-1)t_2}$, then $v_{\tilde{\mathbf{c}}}(\mathfrak{X})$ is multiplicatively independent and thus it is a basis of $\boldsymbol{\chi}(H_{\tilde{\mathbf{c}}})$.

Third, denote $\mathbf{a} = (\chi_1(A), \chi_2(A), \chi_3(A))$ where

$$\chi_1(A) = x(1 - \sqrt{t_1}), \chi_2(A) = x(1 + \sqrt{t_1}), \chi_3(A) = t_2.$$

Take $\boldsymbol{\xi} = (1 - \sqrt{t_1}, 1 + \sqrt{t_1}, t_2)$ and $\bar{\mathbf{a}} = (x, x, 1)$. It is easy to see that $\mathcal{Z}(\boldsymbol{\xi}, 0) = \{(0, 0, 0)\}$. Let $\tilde{\Gamma}$ be the subgroup of $\mathbb{G}_m(k(\mathbb{Y}))$ generated by $1 - \sqrt{t_1}, 1 + \sqrt{t_1}, t_2$. Then for any $\tilde{\mathbf{c}} \in \mathcal{B}(\mathbb{Y}, \tilde{\Gamma})$, $\mathcal{Z}(v_{\tilde{\mathbf{c}}}(\boldsymbol{\xi}), 0) = \{(0, 0, 0)\}$ and therefore

$$\mathcal{Z}(v_{\tilde{\mathbf{c}}}(\mathbf{a}), 1) = \mathcal{Z}(v_{\tilde{\mathbf{c}}}(\boldsymbol{\xi}), 0) \cap \mathcal{Z}(v_{\tilde{\mathbf{c}}}(\bar{\mathbf{a}}), 0) = \{(0, 0, 0)\},$$

i.e., $\{v_{\tilde{\mathbf{c}}}(\chi_i(A))|i=1,2,3\}$ is multiplicatively σ-independent. Let $\tilde{U}=\mathbb{Y}_{t_1(t_1-1)t_2}\cap\mathcal{B}(\mathbb{Y},\tilde{\Gamma})$. Then for any $\tilde{\mathbf{c}}\in\tilde{U}$, since $H_{\tilde{\mathbf{c}}}$ is connected, Lemma 5.4 implies that $H_{\tilde{\mathbf{c}}}$ is the Galois group of $\sigma_{A(\tilde{\mathbf{c}})}(Y)=A(\tilde{\mathbf{c}})Y$ over $k(x)$.

Finally, by (2.1), $\mathcal{B}(\mathbb{X},\tilde{\Gamma})=p_{\mathbb{Y}/\mathbb{X}}(\mathcal{B}(\mathbb{Y},\tilde{\Gamma}))$ and so $p_{\mathbb{Y}/\mathbb{X}}(\tilde{U})$ contains $\mathcal{B}(\mathbb{X},\tilde{\Gamma})\cap\mathbb{X}_{t_1(t_1-1)t_2}$. The latter set is what we need.

Example 5.11. Consider

$$\sigma_t(y)=ty$$

over $\mathbb{C}(x,t)$ where t is a parameter. This equation has a solution t^x.

(1) t is endowed with the usual derivation ∂_t. The differential Galois group is $\mathbb{G}_m(\mathbb{C})$ and Proposition 2.9 of [11] implies that t^x satisfies a first order linear differential equation over $\mathbb{C}(x,t)$ with respect to ∂_t. Actually, one easily sees that t^x is a solution of $\partial_t(y)=(x/t)y$.

(2) t is endowed with the shift operator $\tau(t)=t+1$. Example 3.8 of [19] implies that t^x does not satisfy any nonzero difference equation over $\mathbb{C}(x,t)$ with respect to τ.

(3) t is a usual parameter. The usual Galois group is $\mathbb{G}_m(\overline{\mathbb{C}(t)})$ and it implies that t^x is transcendental over $\mathbb{C}(x,t)$. One sees that c^x is algebraic over $\mathbb{C}(x)$ if and only if c is a root of unity. In particular, when $c=1$, the Galois group of the specialized equation is $\{\mathbf{1}\}$.

The above example provides one a glance at the difference between parameterized difference Galois theories and difference Galois theory with usual parameters. Recall that for higher order linear difference equations, the phenomenon appearing in (3) of Example 5.11 can also happen, i.e., the Galois group of the specialized equation is extremely small under some specialization even though the original one is as large as the whole general linear group.

6. An application

In this section, we apply Theorem 1.2 to the inverse problem in difference Galois theory. The notation will be as before, for instance k denotes an algebraically closed field of characteristic zero, σ_B with $B\in\mathrm{GL}_n(k(x))$ denotes the k-automorphism of $k(x)[X,1/\det(X)]$ induced by $\sigma_B(X)=BX$, and $\sigma(x)=x+1$, $v_{\mathbf{c}}$ denotes the map from $k[\mathbb{X}]$ to k given by $v_{\mathbf{c}}(f)=f(\mathbf{c})$ for $f\in k[\mathbb{X}]$ and $\mathrm{stab}(I)$ stands for the stabilizer of an ideal I. The inverse problem asks which algebraic subgroups of $\mathrm{GL}_n(k)$ occur as the Galois groups of $\sigma_B(Y)=BY$ over $k(x)$ with $B\in\mathrm{GL}_n(k(x))$. In Chapter 3 of [26], van der Put and Singer raised the following conjecture.

Conjecture 6.1. *An algebraic subgroup G of $\mathrm{GL}_n(k)$ is the Galois group of $\sigma_B(Y)=BY$ over $k(x)$ for some $B\in\mathrm{GL}_n(k(x))$ if and only if G/G° is cyclic.*

It was shown in Proposition 1.20 of [26] that G/G° is necessary to be cyclic if G is the Galois group of $\sigma_B(Y)=BY$ over $k(x)$. Therefore, to prove Conjecture 6.1, it suffices to prove the sufficient part, which we restate as the following conjecture.

Conjecture 6.2. *If G is an algebraic subgroup of $\mathrm{GL}_n(k)$ satisfying that G/G° is cyclic, then G is the Galois group of $\sigma_B(Y)=BY$ over $k(x)$ for some $B\in\mathrm{GL}_n(k(x))$.*

When $k=\mathbb{C}$, for connected algebraic groups and cyclic extensions of tori, analytic proofs of Conjecture 6.2 were presented in Corollary 8.6 and Lemma 8.12 of

[26], respectively. In Chapter 3 of the same book, an algebraic proof of Conjecture 6.2 was also given when k is any algebraically closed field of characteristic zero and G is connected. For the general case, Conjecture 6.2 remains open.

Using a similar argument as that in the proof of Theorem 4.4 of [25], we can prove the following theorem.

Theorem 6.3. *If Conjecture* 6.2 *holds for $k = \mathbb{C}$, then it holds for any algebraically closed field k of characteristic zero.*

Proof. Let G be an algebraic subgroup of $\mathrm{GL}_n(k)$ with G/G° cyclic. Suppose that the vanishing ideal of G is generated by a finite set $S \subset k[X, 1/\det(X)]$. Assume that the cardinality of k is at most the cardinality of $\mathbb{C}$. Then we can assume that $k \subset \mathbb{C}$, and thus $G(\mathbb{C})$ is an algebraic subgroup of $\mathrm{GL}_n(\mathbb{C})$ with $G(\mathbb{C})/G^\circ(\mathbb{C})$ cyclic. The assumption implies that $G(\mathbb{C})$ is the Galois group of $\sigma_B(Y) = BY$ over $\mathbb{C}(x)$ for some $B \in \mathrm{GL}_n(\mathbb{C}(x))$. Without loss of generality, we may assume that $B \in G(\mathbb{C}(x))$. Let $D \subset \mathbb{C}$ be a finitely generated k-algebra such that the entries of B are all in the field of fractions of $D[x]$, and let $\mathbb{X}$ be the variety over k associated to D. We claim that $G(\overline{k(\mathbb{X})})$ is the Galois group of $\sigma_B(Y) = BY$ over $\overline{k(\mathbb{X})}(x)$. Otherwise, by Proposition 1.21 of [26], there is $T \in G(\overline{k(\mathbb{X})}(x))$ and a proper $\overline{k(\mathbb{X})}$-subgroup H of $G(\overline{k(\mathbb{X})})$ such that $\sigma(T)BT^{-1} \in H(\overline{k(\mathbb{X})}(x))$. Since $\overline{k(\mathbb{X})} \subset \mathbb{C}$, $H(\mathbb{C})$ is a proper subgroup of $G(\mathbb{C})$ and $T \in G(\mathbb{C}(x))$. By Proposition 1.21 of [26] again, $G(\mathbb{C})$ is not the Galois group of $\sigma_B(Y) = BY$ over $\mathbb{C}(x)$, a contradiction. This proves our claim. Due to Theorem 1.2, there is $\mathbf{c} \in \mathbb{X}$ such that $G_{\mathbf{c}}$, the variety in $\mathrm{GL}_n(k)$ defined by $v_{\mathbf{c}}(S)$, is the Galois group of $\sigma_{B(\mathbf{c})}(Y) = B(\mathbf{c})Y$ over $k(x)$. On the other hand, since $S \subset k[X, 1/\det(X)]$, $S = v_{\mathbf{c}}(S)$ and then $G = G_{\mathbf{c}}$. Thus G is the Galois group of $\sigma_{B(\mathbf{c})}(Y) = B(\mathbf{c})Y$ over $k(x)$.

Now assume that the cardinality of k is larger than the cardinality of $\mathbb{C}$. Then we can assume that $\mathbb{C} \subset k$ and G is defined over $\mathbb{C}$. By the assumption again, $G(\mathbb{C})$ is the Galois group of $\sigma_B(Y) = BY$ over $\mathbb{C}(x)$ for some $B \in \mathrm{GL}_n(\mathbb{C}(x))$. Let I be a maximal σ_B-ideal of $\mathbb{C}(x)[X, 1/\det(X)]$ such that $G(\mathbb{C}) = \mathrm{stab}(I)$ and let $\tilde{I}$ be the ideal in $k(x)[X, 1/\det(X)]$ generated by I. Due to Proposition 2.4 of [3], $\tilde{I}$ is a maximal σ_B-ideal. One can verify that $\mathrm{stab}(\tilde{I}) = G$. So G is the Galois group of $\sigma_B(Y) = BY$ over $k(x)$. □

The above theorem together with Corollary 8.6 and Lemma 8.12 of [26] implies the following corollary.

Corollary 6.4. *Conjecture* 6.2 *holds when G is a connected affine algebraic group or a cyclic extension of a torus.*

Acknowledgment

The author would like to thank Michael F. Singer for many valuable conversations. In particular, he suggested considering the arguments in the proof of Theorem 4.4 of [25].

References

[1] George D. Birkhoff, *Formal theory of irregular linear difference equations*, Acta Math. **54** (1930), no. 1, 205–246, DOI 10.1007/BF02547522. MR1555307

[2] A. Braverman, P. Etingof, and D. Gaitsgory, *Quantum integrable systems and differential Galois theory*, Transform. Groups **2** (1997), no. 1, 31–56, DOI 10.1007/BF01234630. MR1439245

[3] Zoé Chatzidakis, Charlotte Hardouin, and Michael F. Singer, *On the definitions of difference Galois groups*, Model theory with applications to algebra and analysis. Vol. 1, London Math. Soc. Lecture Note Ser., vol. 349, Cambridge Univ. Press, Cambridge, 2008, pp. 73–109, DOI 10.1017/CBO9780511735226.006. MR2441376

[4] Phyllis J. Cassidy and Michael F. Singer, *Galois theory of parameterized differential equations and linear differential algebraic groups*, Differential equations and quantum groups, IRMA Lect. Math. Theor. Phys., vol. 9, Eur. Math. Soc., Zürich, 2007, pp. 113–155. MR2322329

[5] Lucia Di Vizio, *Arithmetic theory of q-difference equations: the q-analogue of Grothendieck-Katz's conjecture on p-curvatures*, Invent. Math. **150** (2002), no. 3, 517–578, DOI 10.1007/s00222-002-0241-z. MR1946552

[6] Lucia Di Vizio, Charlotte Hardouin, and Michael Wibmer, *Difference Galois theory of linear differential equations*, Adv. Math. **260** (2014), 1–58, DOI 10.1016/j.aim.2014.04.005. MR3209348

[7] Thomas W. Dubé, *The structure of polynomial ideals and Gröbner bases*, SIAM J. Comput. **19** (1990), no. 4, 750–775, DOI 10.1137/0219053. MR1053942

[8] Ruyong Feng, *Hrushovski's algorithm for computing the Galois group of a linear differential equation*, Adv. in Appl. Math. **65** (2015), 1–37, DOI 10.1016/j.aam.2015.01.001. MR3320755

[9] Ruyong Feng, *On the computation of the Galois group of linear difference equations*, Math. Comp. **87** (2018), no. 310, 941–965, DOI 10.1090/mcom/3232. MR3739224

[10] Michael D. Fried and Moshe Jarden, *Field arithmetic*, 3rd ed., Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], vol. 11, Springer-Verlag, Berlin, 2008. Revised by Jarden. MR2445111

[11] Charlotte Hardouin and Michael F. Singer, *Differential Galois theory of linear difference equations*, Math. Ann. **342** (2008), no. 2, 333–377, DOI 10.1007/s00208-008-0238-z. MR2425146

[12] Peter A. Hendriks, *An algorithm determining the difference Galois group of second order linear difference equations*, J. Symbolic Comput. **26** (1998), no. 4, 445–461, DOI 10.1006/jsco.1998.0223. MR1646675

[13] James E. Humphreys, *Linear algebraic groups*, Springer-Verlag, New York-Heidelberg, 1975. Graduate Texts in Mathematics, No. 21. MR0396773

[14] Ehud Hrushovski, *Computing the Galois group of a linear differential equation*, Differential Galois theory (Będlewo, 2001), Banach Center Publ., vol. 58, Polish Acad. Sci. Inst. Math., Warsaw, 2002, pp. 97–138, DOI 10.4064/bc58-0-9. MR1972449

[15] Nicholas M. Katz, *A conjecture in the arithmetic theory of differential equations* (English, with French summary), Bull. Soc. Math. France **110** (1982), no. 2, 203–239. MR667751

[16] E. R. Kolchin, *Differential algebra and algebraic groups*, Academic Press, New York-London, 1973. Pure and Applied Mathematics, Vol. 54. MR0568864

[17] Serge Lang, *Fundamentals of Diophantine geometry*, Springer-Verlag, New York, 1983. MR715605

[18] Annette Maier, *A difference version of Nori's theorem*, Math. Ann. **359** (2014), no. 3-4, 759–784, DOI 10.1007/s00208-014-1012-z. MR3231015

[19] Alexey Ovchinnikov and Michael Wibmer, *σ-Galois theory of linear difference equations*, Int. Math. Res. Not. IMRN **12** (2015), 3962–4018, DOI 10.1093/imrn/rnu060. MR3356746

[20] Marko Petkovšek, *Hypergeometric solutions of linear recurrences with polynomial coefficients*, J. Symbolic Comput. **14** (1992), no. 2-3, 243–264, DOI 10.1016/0747-7171(92)90038-6. MR1187234

[21] Anand Pillay, *Differential algebra and generalizations of Grothendieck's conjecture on the arithmetic of linear differential equations*, Model theory with applications to algebra and analysis. Vol. 1, London Math. Soc. Lecture Note Ser., vol. 349, Cambridge Univ. Press, Cambridge, 2008, pp. 25–39, DOI 10.1017/CBO9780511735226.003. MR2441373

[22] Denis Serre, *Matrices*, Graduate Texts in Mathematics, vol. 216, Springer-Verlag, New York, 2002. Theory and applications; Translated from the 2001 French original. MR1923507

[23] Jean-Pierre Serre, *Lectures on the Mordell-Weil theorem*, 3rd ed., Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 1997. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt; With a foreword by Brown and Serre. MR1757192

[24] Igor R. Shafarevich, *Basic algebraic geometry. 1*, 2nd ed., Springer-Verlag, Berlin, 1994. Varieties in projective space; Translated from the 1988 Russian edition and with notes by Miles Reid. MR1328833

[25] Michael F. Singer, *Moduli of linear differential equations on the Riemann sphere with fixed Galois groups*, Pacific J. Math. **160** (1993), no. 2, 343–395. MR1233356

[26] Marius van der Put and Michael F. Singer, *Galois theory of difference equations*, Lecture Notes in Mathematics, vol. 1666, Springer-Verlag, Berlin, 1997. MR1480919

[27] Helmut Völklein, *Groups as Galois groups*, Cambridge Studies in Advanced Mathematics, vol. 53, Cambridge University Press, Cambridge, 1996. An introduction. MR1405612

[28] Oscar Zariski and Pierre Samuel, *Commutative algebra. Vol. II*, Springer-Verlag, New York-Heidelberg, 1975. Reprint of the 1960 edition; Graduate Texts in Mathematics, Vol. 29. MR0389876

KLMM, Academy of Mathematics and Systems Science, and School of Mathematics, University of Chinese Academy of Sciences, Chinese Academy of Sciences, No.55 Zhongguancun East Road, Beijing 100190, People's Republic of China

Email address: ryfeng@amss.ac.cn