



A primitive element theorem for fields with commuting derivations and automorphisms

Gleb Pogudin¹

Published online: 18 September 2019
© Springer Nature Switzerland AG 2019

Abstract

We establish a Primitive Element Theorem for fields equipped with several commuting operators such that each of the operators is either a derivation or an automorphism. More precisely, we show that for every extension $F \subset E$ of such fields of zero characteristic such that

- E is generated over F by finitely many elements using the field operations and the operators,
- every element of E satisfies a nontrivial equation with coefficient in F involving the field operations and the operators,
- the action of the operators on E is irredundant

there exists an element $a \in E$ such that E is generated over F by a using the field operations and the operators. This result generalizes the Primitive Element Theorems by Kolchin and Cohn in two directions simultaneously: we allow any numbers of derivations and automorphisms and do not impose any restrictions on the base field F .

Keywords Primitive element · Differential field · Difference field · Fields with operators

Mathematics Subject Classification Primary 12H05, 12H05; Secondary 12F99

1 Introduction

1.1 Overview and prior results

The Primitive Element Theorem [37, Section 40] is a fundamental result in the field theory that says that for every separable finitely generated algebraic extension of fields

✉ Gleb Pogudin
pogudin.gleb@gmail.com

¹ Courant Institute of Mathematical Sciences, New York University, New York, USA

$F \subset E$, there exists $a \in E$ such that $E = F(a)$. Apart from its theoretical importance, it is also one of the main tools for computing with algebraic extensions [22, Section 5].

Fields with commuting derivations. Consider an extension $\mathbb{C} \subset \mathbb{C}(x, e^x)$. The field $\mathbb{C}(x, e^x)$ cannot be generated over \mathbb{C} by one element because the functions x and e^x are algebraically independent. However, the formulas

$$x = \alpha - \alpha' + 1 \quad \text{and} \quad e^x = \alpha' - 1, \quad \text{where } \alpha := x + e^x$$

imply that $\mathbb{C}(x, e^x)$ is generated over \mathbb{C} by α if we allow taking derivatives as well as the field operations.

Fields equipped with commuting derivations are central objects in the algebraic studies of differential equations initiated by Ritt [31] and Kolchin [18]. In this setting, Kolchin proved the following analogue of the Primitive Element Theorem:

Theorem 1.1 (Kolchin, [17, Section 4]) *Let $F \subset E$ be an extension of fields of zero characteristic and E be equipped with commuting derivations $\delta_1, \dots, \delta_s$ such that F is closed under the derivations. Assume that*

- (1) *there exist $a_1, \dots, a_n \in E$ such that*

$$E = F(\delta_1^{\alpha_1} \dots \delta_s^{\alpha_s} a_j \mid 1 \leq j \leq n, \alpha_1, \dots, \alpha_s \in \mathbb{Z}_{\geq 0}).$$

- (2) *for every $1 \leq j \leq n$, a_j satisfies a nonzero polynomial PDE over F , that is, the elements of $\{\delta_1^{\alpha_1} \dots \delta_s^{\alpha_s} a_j \mid \alpha_1, \dots, \alpha_s \in \mathbb{Z}_{\geq 0}\}$ are algebraically dependent over F ;*
- (3) *there exist $b_1, \dots, b_s \in F$ with nondegenerate Jacobian, that is, $\det(\delta_i b_j)_{i,j=1}^s \neq 0$.*

Then there exists $a \in E$ such that $E = F(\delta_1^{\alpha_1} \dots \delta_s^{\alpha_s} a \mid \alpha_1, \dots, \alpha_s \in \mathbb{Z}_{\geq 0})$.

Theorem 1.1 and its improvements [30, 35] have been used, for example, in algorithms and effective bounds for differential-algebraic equations [8, 9, 11, 13, 25], Galois theory of differential and difference equations [5, 15], model theory of differential fields [23, 38], control theory [3, 12], and for connecting algebraic and analytic approaches to differential-algebraic equations [33, 34, 36].

In our earlier paper [30], for the case of one derivation ($m = 1$), condition (3) has been relaxed to the condition that E contains a nonconstant, i.e. that the derivation is not zero. Unlike Theorem 1.1, this refined statement is applicable, for example, to the extension $\mathbb{C} \subset \mathbb{C}(x, e^x)$ discussed above and to extensions of the form $\mathbb{C} \subset \mathbb{C}(X)$, where \mathbb{C} is the field of rational functions on an irreducible algebraic variety X and the derivation on $\mathbb{C}(X)$ is induced by a vector field on X . It is an open problem whether such relaxation is true for the case of several commuting derivations.

Problem 1 *Prove or disprove that Theorem 1.1 is still true if condition (3) is replaced with (3') there exist $b_1, \dots, b_s \in E$ (not F) with nondegenerate Jacobian.*

Fields with an automorphism. Consider the extension $\mathbb{C} \subset \mathbb{C}(x, \Gamma(x))$, where $\Gamma(x)$ is the gamma function. Since x and $\Gamma(x)$ are algebraically independent, $\mathbb{C}(x, \Gamma(x))$ cannot be generated over \mathbb{C} by one element. The difference equation for the gamma function $\Gamma(x+1) = x\Gamma(x)$ implies that the shift of the argument $f(x) \mapsto f(x+1)$ induces an automorphism on $\mathbb{C}(x, \Gamma(x))$. Then the formula $x = \frac{\Gamma(x+1)}{\Gamma(x)}$ implies that $\mathbb{C}(x, \Gamma(x))$ is generated over \mathbb{C} by $\Gamma(x)$ if we allow integer shifts of the argument as well as the field operations.

Algebraic theory of nonlinear difference equations founded by Ritt and Cohn extensively uses fields equipped with an automorphism. Cohn established the following version of the Primitive Element Theorem (to keep the presentation simple, we restrict ourselves to the zero characteristic case):

Theorem 1.2 (Cohn [10, p. 203, Theorem III]) *Let $F \subset E$ be an extension of fields of zero characteristic and $\sigma : E \rightarrow E$ be an automorphism such that $\sigma(F) \subset F$. Assume that*

- (1) *there exist $a_1, \dots, a_n \in E$ such that $E = F(\sigma^i(a_j) \mid i \in \mathbb{Z}, 1 \leq j \leq n)$;*
- (2) *for every $1 \leq j \leq n$, a_j satisfies a nonzero difference-algebraic equation over F , that is, the elements of $\{\sigma^i(a_j) \mid i \in \mathbb{Z}\}$ are algebraically dependent over F ;*
- (3) *σ has infinite order on F , that is, there is no integer $k \geq 1$ such that, for every $a \in F$, $\sigma^k(a) = a$.*

Then there exists $a \in E$ such that $E = F(\sigma^j(a) \mid j \in \mathbb{Z})$.

Theorem 1.2 has been used, for example, in model theory of fields with an automorphism [7] and for proving approximation theorem for difference equations [2]. However, Theorem 1.2 is not applicable to our example $\mathbb{C} \subset \mathbb{C}(x, \Gamma(x))$ because the automorphism acts trivially on the base field \mathbb{C} .

Problem 2 *Prove or disprove that Theorem 1.2 is still true if Condition (3) is replaced with (3') σ has infinite order on E (not F).*

Positive solution (i.e., “prove”) to Problem 2 would have, for example, the following application. Let $\mathbb{C} \subset \mathbb{C}(X)$, where $\mathbb{C}(X)$ is the field of rational functions on an irreducible algebraic variety X . Consider an automorphism α of X of infinite order. The dual $\alpha^\sharp : \mathbb{C}(X) \rightarrow \mathbb{C}(X)$ is an automorphism of $\mathbb{C}(X)$ of infinite order. Then the positive solution to Problem 2 would imply that there exists $f \in \mathbb{C}(X)$ such that the orbit of f under α^\sharp generates $\mathbb{C}(X)$ over \mathbb{C} . In particular, our main result, Theorem 2.1, implies the existence of such f .

More general cases. Although fields with several commuting automorphisms and fields with several derivations and automorphisms commuting with each other have been studied from the standpoints of algebra [10,21], model theory [6,24,32], and symbolic computation [14,20], we are not aware of any analogues of the Primitive Element Theorem for such fields.

Problem 3 Derive an analogue of the Primitive Element Theorem for fields with several commuting derivations and automorphisms.

Another common generalization of fields equipped with a derivations and fields equipped with an automorphism is the theory of fields with free operators introduced in [26,27] (see also [4,16]). We are not aware of any analogues of the Primitive Element Theorem for such fields.

1.2 Our contribution

Our main result, Theorem 2.1, generalizes Theorems 1.1 and 1.2 in two directions simultaneously

- We establish a Primitive Element Theorem for fields equipped with s derivations and t automorphisms such that all these operators commute. This solves Problem 3.
- We remove all the assumptions on the base field F other than being closed under the operators. Instead of this, we require the derivations and automorphisms to be “independent” on the bigger field E . In particular, this solves Problems 1 and 2 (see Remark 2.1). We show (see Example 3.4) that the condition on E cannot be removed.

1.3 Outline of the approach

One of the main challenges in proving such a general version of the Primitive Element Theorem is to find an appropriate general form of a primitive element. Proofs of Kolchin [17] and Cohn [10] follow the same strategy as the standard proof of the algebraic Primitive Element Theorem, namely they construct a primitive element of an extension $F \subset E$ as a F -linear combination of the original generators.

However, Examples 3.2 and 3.3 show that if F is a constant field, then it can happen that none of the linear combinations of the original generators is a primitive element even in the case of only one operator. To strengthen Kolchin’s theorem (Theorem 1.1) in the case of one derivation, in our earlier paper [30], we used an involved two-stage construction of a primitive element as a *polynomial in the original generators*.

In this paper, we approach finding a primitive element from the perspective of the *Taylor series expansion*. More precisely, a primitive element is constructed as a truncated multivariate Taylor series in the original generators and their derivatives (see formulas (4) and (14)). The order of truncation is derived based on the Kolchin polynomial of the extension. Formally, a truncated Taylor series is simply a polynomial written in a special form with factorials in the denominators, so the search space for a primitive element is almost the same as in [30]. However, this representation turns out to be a key to interpreting a polynomial system that relates the original generators and a potential primitive element in terms of solutions some special system of linear PDEs. This interpretation allows us to show that the original generators can be expressed in terms of the potential primitive element (see Lemmas 5.3 and 6.6), so this element is indeed primitive. As was pointed out to me by Jonathan Kirby, one can view the difference between the representations of a primitive element in [30] and in the present

paper as the difference between usual generating series and exponential generating series.

We refer a reader who wants to see more details but does not want to read the whole proof to Sect. 5. This section contains a proof of the main theorem for differential fields (i.e., fields equipped with a derivation). It is much shorter than the main proof but demonstrates some of the key techniques we developed.

1.4 Structure of the paper

The rest of the paper is organized as follows. Sect. 2 contains definitions used in the statement of the main result and the main result, Theorem 2.1. Section 3 contains examples that illustrate the main result. Section 4 contains the definitions and notation used in the proofs. Section 5 contains the proof of the main result in the special case of fields with a derivation. This proof demonstrates some of the key ingredients of the proof of Theorem 2.1 in a simpler setting allowing the reader to understand of the general approach without going into technical details. Section 6 contains the proof of the main result. For the convenience of the reader, the corresponding lemmas in Sect. 5 and 6 are cross-referenced.

2 Definitions and the main result

All fields are assumed to be of zero characteristic.

Definition 2.1 (Δ - Σ -rings) Let $\Delta = \{\delta_1, \dots, \delta_s\}$ and $\Sigma = \{\sigma_1, \dots, \sigma_t\}$ be finite sets of symbols. We say that a commutative ring R is a Δ - Σ -ring if

1. $\delta_1, \dots, \delta_s$ act on R as derivations, that is, $\delta_i(a + b) = \delta_i(a) + \delta_i(b)$ and $\delta_i(ab) = \delta_i(a)b + a\delta_i(b)$ for every $1 \leq i \leq s$ and $a, b \in R$;
2. $\sigma_1, \dots, \sigma_t$ act on R as automorphisms;
3. every two operators in $\Delta \cup \Sigma$ commute.

A Δ - Σ -ring that is a field is called Δ - Σ -field.

Example 2.1 Natural examples of Δ - Σ -fields include the following.

- Let $E = \mathbb{C}(x)$, $\Delta = \{\partial\}$, and $\Sigma = \{\sigma\}$. We can define a structure of Δ - Σ -field on E by

$$\delta(f(x)) = \frac{\partial}{\partial x} f(x), \quad \text{and} \quad \sigma(f(x)) = f(x+1) \quad \text{for every } f(x) \in E.$$

In the same way, one can define n derivations and n automorphisms on $\mathbb{C}(x_1, \dots, x_n)$.

- Let E be the field of meromorphic functions on \mathbb{C} , $\Delta = \{\delta\}$, and $\Sigma = \{\sigma_1, \sigma_2\}$. We can define a structure of Δ - Σ -field on E by

$$\delta(f(z)) = f'(z), \quad \sigma_1(f(z)) = f(z+1), \quad \sigma_2(f(z)) = f(z+i) \quad \text{for every } f \in E.$$

- Let E be the field of meromorphic functions on \mathbb{C} , $\Delta = \{\delta\}$, and $\Sigma = \{\sigma\}$. For every nonzero $q \in \mathbb{C}$, we can define a structure of Δ - Σ -field on E by

$$\delta(f(z)) = zf'(z), \quad \sigma(f(z)) = f(qz) \text{ for every } f \in E.$$

Definition 2.2 (*Extension of Δ - Σ -fields*) An extension of fields $F \subset E$ where E and F are Δ - Σ -fields is said to be *an extension of Δ - Σ -fields* if the action of $\Delta \cup \Sigma$ on F coincides with the restriction to F of the action of $\Delta \cup \Sigma$ on E .

Notation 2.1 For every $\alpha := (\alpha_1, \dots, \alpha_s) \in \mathbb{Z}_{\geq 0}^s$ and every $\beta := (\beta_1, \dots, \beta_t) \in \mathbb{Z}^t$, we introduce

$$\delta^\alpha := \delta_1^{\alpha_1} \dots \delta_s^{\alpha_s} \quad \text{and} \quad \sigma^\beta := \sigma_1^{\beta_1} \dots \sigma_t^{\beta_t}.$$

Theorem 2.1 (Main result) *Let $F \subset E$ be an extension of Δ - Σ -fields such that*

- (1) *there exist $a_1, \dots, a_n \in E$ such that $E = F(\delta^\alpha \sigma^\beta(a_j) \mid 1 \leq j \leq n, \alpha \in \mathbb{Z}_{\geq 0}^s, \beta \in \mathbb{Z}^t)$;*
- (2) *for every $1 \leq j \leq n$, the elements of $\{\delta^\alpha \sigma^\beta(a_j) \mid \alpha \in \mathbb{Z}_{\geq 0}^s, \beta \in \mathbb{Z}^t\}$ are algebraically dependent over F ;*
- (3a) *$\delta_1, \dots, \delta_s$ are linearly independent over E ;*
- (3c) *$\sigma_1, \dots, \sigma_t$ are multiplicatively independent over \mathbb{Z} , that is, for every $\beta \in \mathbb{Z}^t$, $\sigma^\beta|_E = \text{id} \iff \beta = 0$.*

Then there exists $a \in E$ such that $E = F(\delta^\alpha \sigma^\beta(a) \mid \alpha \in \mathbb{Z}_{\geq 0}^s, \beta \in \mathbb{Z}^t)$.

Remark 2.1 Setting $s = 0$ and $t = 1$, we obtain a statement stronger than Cohn's theorem [10, p. 203, Theorem III] in the case of zero characteristic. Lemma 6.1 implies that the requirement on the base field F in Kolchin's theorem [17, Section 4] is the same as the condition (3c) on E in Theorem 2.1. Thus, Theorem 2.1 strengthens Kolchin's theorem as well.

3 Examples

Notation 3.1 Let $F \subset E$ be an extension of Δ - Σ -fields. For $a_1, \dots, a_n \in E$, we set

$$F\langle a_1, \dots, a_n \rangle := F(\delta^\alpha \sigma^\beta(a_j) \mid 1 \leq j \leq n, \alpha \in \mathbb{Z}_{\geq 0}^s, \beta \in \mathbb{Z}^t).$$

Example 3.1 This example illustrates how Theorem 2.1 can be applied to classical special functions. Let $\Delta = \{\partial_z, \partial_\tau\}$ and $\Sigma = \emptyset$. Let $\mathcal{M}(\mathbb{C}, \mathcal{H})$ denote the field of bivariate meromorphic functions on $\mathbb{C} \times \mathcal{H}$ in variables z and τ , where $\mathcal{H} = \{\tau \in \mathbb{C} \mid \text{Im}(\tau) > 0\}$. We consider $\mathcal{M}(\mathbb{C}, \mathcal{H})$ as a Δ -field by letting ∂_z and ∂_τ act as the partial derivatives with respect to z and τ , respectively. Let

$$\theta_1(z, \tau) := -i \sum_{j=-\infty}^{\infty} (-1)^j e^{(j+1/2)^2 \pi i \tau} e^{(2j+1)\pi i z}$$

be one of the Jacobi theta functions [1, § 10.7]. $\theta_1(z, \tau)$ satisfies the following form of the heat equation [28, p. 433]

$$\partial_z^2 \theta_1(z, \tau) = 4\pi i \partial_\tau \theta_1(z, \tau).$$

This implies that $\theta_1(z, \tau)$ as well as $\theta_1(2z, \tau)$ and $\theta_1(3z, \tau)$ are Δ - Σ -algebraic over \mathbb{C} . Thus, Theorem 2.1 applied to the extension

$$F := \mathbb{C} \subset E := \mathbb{C}(\theta_1(z, \tau), \theta_1(2z, \tau), \theta_1(3z, \tau))$$

implies that there exists a function $f(z, \tau) \in E$ such that $\theta_1(z, \tau)$, $\theta_1(2z, \tau)$, and $\theta_1(3z, \tau)$ can be written as rational functions in f and its partial derivatives. Note that the original Kolchin's theorem (Theorem 1.1) is not applicable to this extension.

Examples 3.2 and 3.3 show that it might be impossible to construct a primitive element of an extension as a linear combination of the original generators even in the case of one operator (see also [30, Remark 2]).

Example 3.2 Let $\Delta = \{\delta\}$ and $\Sigma = \emptyset$. Field $E := \mathbb{C}(x, \ln x, \ln(1-x))$ is a Δ - Σ -field with $\delta(f(x)) = f'(x)$ for every $f \in E$. Since $x = \frac{1}{(\ln x)'} \in E$, $E = \mathbb{C}(\ln x, \ln(1-x))$. Since each of $\ln x$ and $\ln(1-x)$ satisfies an algebraic differential equation with constant coefficients, the extension

$$F := \mathbb{C} \subset E = \mathbb{C}(\ln x, \ln(1-x))$$

satisfies the conditions of Theorem 2.1. Consider arbitrary $\alpha, \beta \in F$ and set $a = \alpha \ln x + \beta \ln(1-x)$. Since $a' \in \mathbb{C}(x)$, $F\langle a \rangle \subset F(a, x)$. The latter has the transcendence degree at most two over F but Ostrowski's theorem [29] implies that $\ln x$, $\ln(1-x)$, and x are algebraically independent, so $\text{trdeg}_F E = 3$. Hence, $F\langle a \rangle \neq E$. Thus, such a cannot be a primitive element of the extension $F \subset E$.

Example 3.3 Let $\zeta(z, s) = \sum_{n=0}^{\infty} \frac{1}{(z+n)^s}$ be the Hurwitz zeta function [1, § 1.3]. Let $\mathcal{M}(\mathbb{C})$ be the field of meromorphic functions on \mathbb{C} . Let $E := \mathbb{C}(z, \zeta(z, 2), \zeta(1-z, 2))$ be a subfield in $\mathcal{M}(\mathbb{C})$. We define a Δ - Σ -structure on $\mathcal{M}(\mathbb{C})$ with $\Delta = \emptyset$ and $\Sigma = \{\sigma\}$ by

$$\sigma(f(z)) = f(z+1) \text{ for every } f \in \mathbb{C}.$$

Since

$$\sigma(\zeta(z, 2)) = \zeta(z, 2) - \frac{1}{z^2} \quad \text{and} \quad \sigma(\zeta(1-z, 2)) = \zeta(1-z, 2) + \frac{1}{z^2}, \quad (1)$$

E is a Δ - Σ -subfield of $\mathcal{M}(\mathbb{C})$, and $E = \mathbb{C}(\zeta(z, 2), \zeta(1-z, 2))$. (1) implies that $\zeta(z, 2)$ and $\zeta(1-z, 2)$ are Δ - Σ -algebraic over \mathbb{C} , so the extension

$$F := \mathbb{C} \subset E = \mathbb{C}(\zeta(z, 2), \zeta(1-z, 2))$$

satisfies the conditions of Theorem 2.1. We claim that $\text{trdeg}_F E = 3$. Assume the contrary, that is, $\zeta(z, 2), \zeta(1-z, 2)$, and z are algebraically dependent over \mathbb{C} . Let $\mathcal{C} := \{f \in \mathcal{M}(\mathbb{C}) \mid \sigma(f) = f\}$. Since $\zeta(z, 2) + \zeta(1-z, 2) \in \mathcal{C}$, the algebraic dependence between $\zeta(z, 2), \zeta(1-z, 2)$, and z implies that $\zeta(z, 2)$ is algebraic over $\mathcal{C}(z)$. Let $P(z, t) \in \mathcal{C}(z)[t]$ be its minimal monic polynomial and we set $d := \deg_t P$. By applying σ to $P(z, \zeta(z, 2))$ and using the minimality of P , we show that

$$P(z, t) = P(z + 1, t - 1/z^2).$$

Then the coefficient $g(z) \in \mathcal{C}(z)$ of t^{d-1} in P satisfies $g(z + 1) = g(z) + \frac{d}{z^2}$. One can check (using, for example, the function ratpolysols in MAPLE) that there is no such rational function for $d \neq 0$. Thus, $\text{trdeg}_F E = 3$.

Consider arbitrary $\alpha, \beta \in F$ and set $a := \alpha\zeta(z, 2) + \beta\zeta(1-z, 2)$. (1) implies that $\sigma(a) \in \mathbb{C}(z)$, so $F\langle a \rangle \subset F(a, z)$. Hence $\text{trdeg}_F F\langle a \rangle \leq 2$. Hence, $F\langle a \rangle \neq E$. Thus, such a cannot be a primitive element of the extension $F \subset E$.

Example 3.4 This example shows that neither of the conditions (3δ) and (3σ) in Theorem 2.1 can be removed. We fix $s, t \in \mathbb{Z}_{\geq 0}$, $\Delta = \{\delta_1, \dots, \delta_s\}$, and $\Sigma = \{\sigma_1, \dots, \sigma_t\}$. Consider a free Δ - Σ -extension of \mathbb{Q} with two generators, x_1 and x_2 :

$$\mathbb{Q} \subset E := \mathbb{Q}(\delta^\alpha \sigma^\beta x_i \mid \alpha \in \mathbb{Z}_{\geq 0}, \beta \in \mathbb{Z}, i = 1, 2),$$

where all $\delta^\alpha \sigma^\beta x_i$ are algebraically independent and $\Delta \cup \Sigma$ acts naturally (see (2)). [19, Theorem 3.5.38] implies that this extension $\mathbb{Q} \subset E$ cannot be generated by one element as a Δ - Σ -field extension.

Let $\Delta_1 := \Delta \cup \{\delta_{s+1}\}$. We choose rational numbers c_1, \dots, c_s and make E a Δ_1 - Σ -field by defining $\delta_{s+1}(a) := c_1\delta_1(a) + \dots + c_s\delta_s(a)$ for every $a \in E$. For every $a \in E$, the subfield generated by a using $\Delta_1 \cup \Sigma$ is the same as the subfield generated by $\Delta \cup \Sigma$. Thus, $\mathbb{Q} \subset E$ cannot be generated by one element as an extension of Δ_1 - Σ -fields. On the other hand, every $a \in E$ is Δ_1 - Σ -algebraic over \mathbb{Q} because it satisfies $c_1\delta_1 a + \dots + c_s\delta_s a - \delta_{s+1} a = 0$. Thus, the condition (3δ) in Theorem 2.1 cannot be removed. A similar argument with a superfluous automorphism $\sigma_{t+1} := \sigma_1^{k_1} \sigma_2^{k_2} \dots \sigma_t^{k_t}$, where $k_1, \dots, k_t \in \mathbb{Z}$, show that the condition (3σ) cannot be removed.

4 Definitions and notation used in proofs

In the proofs, we will write $\delta^\alpha \sigma^\beta a$ instead of $\delta^\alpha \sigma^\beta(a)$

Definition 4.1 (Δ - Σ -algebraicity) Let $F \subset E$ be an extension of Δ - Σ -fields. An element $a \in E$ is Δ - Σ -algebraic over F if the set

$$\{\delta^\alpha \sigma^\beta a \mid \alpha \in \mathbb{Z}_{\geq 0}^s, \beta \in \mathbb{Z}_{\geq 0}^t\}$$

is algebraically dependent over F .

Definition 4.2 (*Nondegenerate Δ - Σ -field*) A Δ - Σ -field E is called *nondegenerate* if it satisfies conditions (3 δ) and (3 σ) of Theorem 2.1, namely,

- (3 δ) $\delta_1, \dots, \delta_s$ are linearly independent over E ;
- (3 σ) $\sigma_1, \dots, \sigma_t$ are multiplicatively independent over \mathbb{Z} , that is, for every $\beta \in \mathbb{Z}^t$, $\sigma^\beta|_E = \text{id} \iff \beta = \mathbf{0}$.

Definition 4.3 (*Δ - Σ -constants*) An element $a \in E$ of a Δ - Σ -field E is said to be a *constant* if $\delta_i a = 0$ for every $1 \leq i \leq s$ and $\sigma_j a = a$ for every $1 \leq j \leq t$. Constants form a subfield in E . We will denote this subfield by $C(E)$.

Definition 4.4 (*Δ - Σ -polynomials*) Let R be a Δ - Σ -ring. Consider the following ring of polynomials over R

$$R\{x\} := R \left[\delta^\alpha \sigma^\beta x \mid \alpha \in \mathbb{Z}_{\geq 0}^s, \beta \in \mathbb{Z}_{\geq 0}^t \right],$$

where each $\delta^\alpha \sigma^\beta x$ is a separate variable. We can extend the structure of Δ - Σ -ring from R to $R\{x\}$ by

$$\delta_i \left(\delta^\alpha \sigma^\beta x \right) := \delta^{\alpha + \mathbf{1}_i} \sigma^\beta x \quad \text{and} \quad \sigma_j \left(\delta^\alpha \sigma^\beta x \right) := \delta^\alpha \sigma^{\beta + \mathbf{1}_j} x, \quad (2)$$

where $\mathbf{1}_i$ and $\mathbf{1}_j$ denote the i -th basis vector in \mathbb{Z}^s and the j -th basis vector in \mathbb{Z}^t , respectively. Elements of $R\{x\}$ are called *Δ - Σ -polynomials in x* .

Notation 4.1 Let n be a positive integer.

- For $\mathbf{v} = (v_1, \dots, v_n) \in \mathbb{Z}^n$, we define $|\mathbf{v}| := |v_1| + \dots + |v_n|$. If $\mathbf{v} \in \mathbb{Z}_{\geq 0}^n$, then we also define $\mathbf{v}! := v_1! \dots v_n!$.
- For a positive integer m , we define $\mathbb{Z}_{\geq 0}^n(m) := \{\mathbf{v} \in \mathbb{Z}_{\geq 0}^n \mid |\mathbf{v}| \leq m\}$.

Definition 4.5 (*Nonperiodic elements*) Let E be a Δ - Σ -field.

- An element $a \in E$ is said to be *nonperiodic* if, for every nonzero $\beta \in \mathbb{Z}^t$, $\sigma^\beta a \neq a$.
- For a positive integer m , an element $a \in E$ is called *m -nonperiodic* if

$$\left(\sigma^\alpha a = \sigma^\beta a \quad \& \quad \alpha, \beta \in \mathbb{Z}_{\geq 0}^t(m) \right) \implies \beta = \alpha.$$

Notation 4.2 Let K be a field and $K\llbracket x_1, \dots, x_n \rrbracket$ be the formal power series ring over K . For an element

$$f = \sum_{k \in \mathbb{Z}_{\geq 0}^n} c_k x^k \in K\llbracket x_1, \dots, x_n \rrbracket,$$

we denote its truncation at order m by

$$[f]_m := \sum_{k \in \{0, 1, \dots, m\}^n} c_k x^k \in K[x_1, \dots, x_n].$$

5 Proof for differential fields

In this section, we consider the case $\Delta = \{\delta\}$ and $\Sigma = \emptyset$. We will denote δa by a' and say “differential field” and “differentially algebraic” instead of “ Δ - Σ -field” and “ Δ - Σ -algebraic”, respectively.

Lemma 5.1 (Special case of Lemma 6.4) *Let $\partial = \frac{\partial}{\partial x}$ be the standard derivation on $K[[x]]$. Let $D \in K[\partial]$ be a differential operator of order m . Then, for every $f \in K[[t]]$,*

$$(Df = 0 \ \& \ [f]_m = 0) \implies f = 0.$$

Proof Since D has ∂ -constant coefficients, every solution of D is uniquely defined by its first m Taylor coefficients. Since f has the same first m Taylor coefficients as the zero solution, $f = 0$. \square

For the rest of the section, for a differential field E , we extend the derivation from E to $E[[x]]$ by

$$\left(\sum_{i=0}^{\infty} c_i x^i \right)' = \sum_{i=0}^{\infty} c'_i x^i \quad \text{for every } \sum_{i=0}^{\infty} c_i x^i \in E[[x]]. \quad (3)$$

Lemma 5.2 (Special case of Lemma 6.5) *Let E be a differential field. Let $a \in E$ be a nonconstant element. For $m \in \mathbb{Z}_{\geq 0}$, we introduce the following subset of $E[[x]]$ (with the derivation defined in (3))*

$$S_m := \left\{ (e^{ax})^{(r)} \mid 0 \leq r \leq m \right\}.$$

Then the elements of S_m are linearly independent over E .

Proof. We will prove the lemma by induction on m . The base case $m = 0$ is true because $S_0 = \{e^{ax}\}$. Assume that we have proved the lemma for some $m \geq 0$. Let V be a space of all polynomials from $E[x]$ of degree at most m . Then $S_m \subset V_e := V e^{ax}$. Hence it is sufficient to prove that $S_{m+1} \setminus S_m = \{(e^{ax})^{(m+1)}\}$ does not belong to V_e . This is true because

$$(e^{ax})^{(m+1)} \equiv (a' x)^{m+1} e^{ax} \pmod{V_e} \quad \text{and} \quad a' \neq 0. \quad \square$$

Lemma 5.3 (Special case of Lemma 6.6) *Let $F \subset E$ be an extension of differential fields, and the derivation on $E[[x]]$ is defined as in (3). Let $a \in E$ be a nonconstant element such that there exists a nontrivial F -linear combination of the truncations*

$$[e^{ax}]_{2(m+1)}, \quad [(e^{ax})']_{2(m+1)}, \quad \dots, \quad [(e^{ax})^{(m)}]_{2(m+1)}$$

that belongs to $F[x]$. Then $a \in F$.

Proof We are given that there exist $c_0, \dots, c_m \in F$ not all zero such that

$$c_0[e^{ax}]_{2(m+1)} + \dots + c_m[(e^{ax})^{(m)}]_{2(m+1)} = f \in F[x].$$

□

Step 1 There exists a nonzero polynomial $C(x) \in E[x]$ of degree at most m such that

$$c_0e^{ax} + \dots + c_m(e^{ax})^{(m)} = C(x)e^{ax}.$$

Note that every E -linear combination of $e^{ax}, \dots, (e^{ax})^{(m)}$ is a product of e^{ax} and an element of $E[x]$ of degree at most m . Since not all c_0, \dots, c_m are zeros, Lemma 5.2 implies that $C(x) \neq 0$.

Step 2 Let $\overline{E} \supset E$ be an algebraic closure of E . For every field automorphism $\tau: \overline{E} \rightarrow \overline{E}$ such that $\tau|_F = \text{id}$, we have $\tau(a) = a$.

Let $S := Ce^{ax} - \tau(C)e^{\tau(a)x}$. Since $\tau|_F = \text{id}$, $[S]_{2(m+1)} = 0$. Since $\deg C(x) \leq m$, we have

$$DS = 0, \quad \text{where} \quad D := (\partial - a)^{m+1}(\partial - \tau(a))^{m+1}.$$

Since the order of D is $2(m+1)$ and $[S]_{2(m+1)} = 0$, Lemma 5.1 implies that $S = 0$. Then e^{ax} and $e^{\tau(a)x}$ are linearly dependent over $E(x)$. This is possible only if $a = \tau(a)$.

Step 3 $a \in F$.

If $a \notin F$, then there exists an automorphism $\tau: \overline{E} \rightarrow \overline{E}$ such that $\tau|_F = \text{id}$ and $a \neq \tau(a)$. This is impossible due to Step 2.

Theorem 5.1 Let $F \subset E$ be an extension of differential fields such that

- (1) there exist $a_1, \dots, a_n \in E$ such that $E = F\langle a_1, \dots, a_n \rangle$;
- (2) for every $1 \leq j \leq n$, a_j is differentially algebraic over F ;
- (3) E contains a nonconstant element.

Then there exists $a \in E$ such that $E = F\langle a \rangle$.

Proof Since each of a_1, \dots, a_n is differentially algebraic over F , $M := \text{trdeg}_F E < \infty$ [18, Corollary 1, p. 112]. We will prove by induction on ℓ that, for every $0 \leq \ell \leq n$, there exists $b_\ell \in E$ such that

- $b'_\ell \neq 0$;
- $E = F\langle b_\ell, a_{\ell+1}, \dots, a_n \rangle$.

Since $E = F\langle b_n \rangle$, proving the existence of such b_0, \dots, b_n will prove the theorem.

For the base case $\ell = 0$, we choose b_0 to be any nonconstant element of E . Assume that we have constructed b_ℓ for some $\ell \geq 0$. We introduce a set of variables

$$\Theta := \{\theta_i \mid -1 \leq i \leq 2(M+1)\}$$

and extend the derivation from E to $E[\Theta]$ by making the elements of Θ constants. Let

$$B_{\ell+1} := \theta_{-1} a_{\ell+1} + \sum_{i=0}^{2(M+1)} \frac{\theta_i}{i!} b_{\ell}^i. \quad (4)$$

We regard any point $\varphi \in \mathbb{Q}^{|\Theta|}$ as a function $\varphi: \Theta \rightarrow \mathbb{Q}$ and extend it to a E -algebra homomorphism $\varphi: E[\Theta] \rightarrow E$.

Claim 1 *There exists a Zariski open nonempty subset $U_1 \subset \mathbb{Q}^{|\Theta|}$ such that*

$$F\langle \varphi(B_{\ell+1}) \rangle = F\langle b_{\ell}, a_{\ell+1} \rangle \text{ for every } \varphi \in U_1.$$

Since

$$\text{trdeg}_{F(\Theta)} F(\Theta, B_{\ell+1}, B'_{\ell+1}, \dots, B_{\ell+1}^{(M)}) \leq \text{trdeg}_F F\langle a_{\ell+1}, b_{\ell} \rangle \leq M,$$

$B_{\ell+1}, B'_{\ell+1}, \dots, B_{\ell+1}^{(M)}$ are algebraically dependent over $F(\Theta)$. Thus, there exists a differential polynomial $R \in F(\Theta)[z, z', \dots, z^{(M)}]$ such that $R(B_{\ell+1}) = 0$. We will assume that R is chosen to be of the minimal possible total degree. We introduce

$$\begin{aligned} R_i &:= \frac{\partial R}{\partial z^{(i)}}(B_{\ell+1}) \text{ for } 0 \leq i \leq M \quad \text{and} \\ R_{\theta_j} &:= \frac{\partial R}{\partial \theta_j}(B_{\ell+1}) \text{ for } -1 \leq j \leq 2(M+1). \end{aligned}$$

The minimality of the degree of R implies that not all of R_i are zero. Consider any $0 \leq j \leq 2(M+1)$. Differentiating $R(B_{\ell}) = 0$ with respect to θ_j , we obtain

$$\sum_{i=0}^M R_i \frac{(b_{\ell}^j)^{(i)}}{j!} = -R_{\theta_j}. \quad (5)$$

Consider the power series ring $E[[x]]$ with the derivation defined in (3). We multiply (5) by x^j and sum such equations over all $0 \leq j \leq 2(M+1)$. We obtain

$$\sum_{i=0}^M R_i \left[(e^{b_{\ell}x})^{(i)} \right]_{2(M+1)} = \sum_{j=0}^{2(M+1)} -R_{\theta_j} x^j. \quad (6)$$

We apply Lemma 5.3 to (6) with $a = b_{\ell}$ and $F = F\langle \Theta, B_{\ell+1} \rangle$, and deduce that $b_{\ell} \in F\langle \Theta, B_{\ell+1} \rangle$. Then there exist nonzero differential polynomials $P_1, P_2 \in F[\Theta]\{z\}$ such that

$$b_{\ell} = \frac{P_1(B_{\ell})}{P_2(B_{\ell})}. \quad (7)$$

We define $U_1 := \{\varphi \in \mathbb{Q}^{|\Theta|} \mid \varphi(P_2(B_{\ell})) \neq 0 \text{ and } \varphi(\theta_{-1}) \neq 0\}$. Since P_2 is a nonzero polynomial, U_1 is nonempty. For every $\varphi \in U_1$, (17) implies that $b_{\ell} \in F\langle \varphi(B_{\ell+1}) \rangle$.

Since $\varphi(\theta_{-1}) \neq 0$, $a_{\ell+1} \in F\langle\varphi(B_{\ell+1})\rangle$, so $F\langle\varphi(B_{\ell+1})\rangle = F\langle b_\ell, a_{\ell+1}\rangle$. The claim is proved.

Claim 2 *Let $U_2 := \{\varphi \in \mathbb{Q}^{|\Theta|} \mid \varphi(B_{\ell+1})' \neq 0\}$. Then U_2 is a nonempty Zariski open set.*

Since U_2 is defined by an inequation, it is open. Consider $\varphi_0 \in \mathbb{Q}^{|\Theta|}$ defined by $\varphi_0(\theta_1) = 1$ and $\varphi_0(\theta_j) = 0$ for $j \neq 1$. Then $\varphi_0(B_{\ell+1}) = b_\ell$. Thus, $\varphi_0 \in U_2$, $U_2 \neq \emptyset$. The claim is proved.

We finish the proof by considering $\varphi \in U_1 \cap U_2$ and defining $b_{\ell+1} := \varphi(B_{\ell+1})$. \square

6 Proof for the general case

6.1 Choosing a sufficiently nonconstant element

Notation 6.1 Let F be a Δ - Σ -field. For $a_1, \dots, a_n \in F$, we denote their Jacobian matrix by

$$J(a_1, \dots, a_n) := \begin{pmatrix} \delta_1 a_1 & \delta_2 a_1 & \dots & \delta_s a_1 \\ \delta_1 a_2 & \delta_2 a_2 & \dots & \delta_s a_2 \\ \vdots & \vdots & \ddots & \vdots \\ \delta_1 a_n & \delta_2 a_n & \dots & \delta_s a_n \end{pmatrix}.$$

For $n = s = 0$, we will use a convention $\det J(a_1, \dots, a_n) = 1$.

Lemma 6.1 *Let E be a Δ - Σ -field. Then the following statements are equivalent*

- (1) $\delta_1, \dots, \delta_s$ are linearly independent over $C(E)$ (see Definition 4.3);
- (2) $\delta_1, \dots, \delta_s$ are linearly independent over E ;
- (3) there exist $a_1, a_2, \dots, a_s \in E$ such that $\det J(a_1, \dots, a_s) \neq 0$.

Proof (3) \implies (1). Assume that (1) does not hold. Then there exist $\mathbf{b} = (b_1, \dots, b_s) \in E^s$ such that $\delta|_E = 0$, where $\delta := b_1\delta_1 + \dots + b_s\delta_s$. We have

$$\delta(a_1, \dots, a_s)^T = J(a_1, \dots, a_s)\mathbf{b}^T.$$

Since $J(a_1, \dots, a_s)$ is nondegenerate, the latter is nonzero for every nonzero \mathbf{b} . Thus, δa_j is nonzero for at least one $1 \leq j \leq s$, so we arrived at the contradiction.

(1) \implies (3). Let r be the maximal integer such that there exist $a_1, \dots, a_r \in E$ such that $J(a_1, \dots, a_r)$ has rank r . If $r = s$, then we are done. If $r < s$ then we will arrive at the contradiction with (1) in the two following steps.

Step 1: *There exist $b_1, \dots, b_s \in E$ not all zero such that $b_1\delta_1 + \dots + b_s\delta_s$ defines a zero derivation on E . Reenumerating $\delta_1, \dots, \delta_s$ if necessary, we can assume that the first r columns in $J(a_1, \dots, a_r)$ are linearly independent. For every $1 \leq i \leq r+1$, we denote the determinant of the matrix consisting of the first $r+1$*

columns of $J(a_1, \dots, a_r)$ except the i -th by A_i . Then $A_{r+1} \neq 0$. Consider an arbitrary $a \in E$. The maximality of r implies that $\text{rank } J(a, a_1, \dots, a_r) = r$, so every $(r+1) \times (r+1)$ -minor of $J(a, a_1, \dots, a_r)$ is degenerate. Expanding the determinant of the matrix consisting of the first $r+1$ columns of $J(a, a_1, \dots, a_r)$ along the first row, we obtain

$$A_1(\delta_1 a) - A_2(\delta_2 a) + \dots + (-1)^r A_{r+1}(\delta_r a) = 0.$$

Since $A_{r+1} \neq 0$, $A_1\delta_1 - A_2\delta_2 + \dots + (-1)^r A_{r+1}\delta_r$ is a nontrivial E -linear combination of $\delta_1, \dots, \delta_s$ that defines a zero derivation on E .

Step 2: *There exist $b_1, \dots, b_s \in C(E)$ not all zero such that $b_1\delta_1 + \dots + b_s\delta_s$ is a zero derivation on E .* Among all nontrivial linear combinations of $\delta_1, \dots, \delta_s$ defining a zero derivation on E , consider a combination with the minimal possible number, say q , of nonzero coefficients. Reenumerating $\delta_1, \dots, \delta_s$, we can assume that this combination is of the form $\delta = b_1\delta_1 + \dots + b_q\delta_q$ for some nonzero $b_1, \dots, b_q \in E$. Moreover, by dividing the combination by b_1 , we can further assume that $b_1 = 1$. If $b_2, \dots, b_q \in C(E)$, then we are done. If at least one of them, say b_2 , does not belong to $C(E)$, then there are two options:

- There exists $1 \leq i \leq s$ such that $\delta_i b_2 \neq 0$. Then consider

$$[\delta_i, \delta] = (\delta_i b_2)\delta_2 + \dots + (\delta_i b_q)\delta_q.$$

Then $[\delta_i, \delta]$ is a nontrivial E -linear combination of $\delta_1, \dots, \delta_s$ such that $[\delta_i, \delta]|_E = 0$. This contradicts the minimality of q .

- There exists $1 \leq i \leq t$ such that $\sigma_i b_2 \neq b_2$. Then consider

$$\sigma_i \delta \sigma_i^{-1} - \delta = (\sigma_i b_2 - b_2)\delta_2 + \dots + (\sigma_i b_q - b_q)\delta_q.$$

Then $\sigma_i \delta \sigma_i^{-1} - \delta$ is a nontrivial E -linear combination of $\delta_1, \dots, \delta_s$ such that $(\sigma_i \delta \sigma_i^{-1} - \delta)|_E = 0$. This contradicts the minimality of q .

□

Lemma 6.2 *Let E be a Δ - Σ -field. Let a_1, \dots, a_n be elements of E such that $s \leq n$ and $\det J(a_1, \dots, a_s) \neq 0$. Then there exists a nonempty Zariski open subset $U \subset \{P \in \mathbb{Q}[x_1, \dots, x_n] \mid \deg P \leq 2\}$ such that, for every $P \in U$,*

$$\det J(\delta_1 P_a, \dots, \delta_s P_a) \neq 0, \text{ where } P_a := P(a_1, \dots, a_n). \quad (8)$$

Proof The inequation (8) defines an open subset in $\{P \in \mathbb{Q}[x_1, \dots, x_n] \mid \deg P \leq 2\}$. It remains to show that this subset is nonempty. We introduce new variables $\Lambda := \{\lambda_1, \dots, \lambda_s\}$ and set $\delta_i \lambda_j = 0$ for every $1 \leq i, j \leq s$. Consider

$$P(x_1, \dots, x_n) = \sum_{\ell=1}^s \lambda_\ell a_\ell + a_1^2 + \dots + a_s^2.$$

Then $J(\Lambda) := \det J(\delta_1 P_a, \dots, \delta_s P_a) \in E[\Lambda]$. We will consider $J(\Lambda)$ as a polynomial in Λ over E and show that $J(\Lambda) \neq 0$. $J(\Lambda)$ is the determinant of the matrix whose (i, j) -th entry is

$$\delta_i \delta_j \left(\sum_{\ell=1}^s \lambda_\ell a_\ell + a_1^2 + \dots + a_s^2 \right) = \sum_{\ell=1}^s \lambda_\ell \delta_i \delta_j a_\ell + \sum_{\ell=1}^s (2a_\ell \delta_i \delta_j a_\ell + 2(\delta_i a_\ell)(\delta_j a_\ell)). \quad (9)$$

If we set $\lambda_\ell = -2a_\ell$ for $1 \leq \ell \leq s$, then the right-hand side of (9) can be written as

$$\sum_{\ell=1}^s -2a_\ell \delta_i \delta_j a_\ell + \sum_{\ell=1}^s (2a_\ell \delta_i \delta_j a_\ell + 2(\delta_i a_\ell)(\delta_j a_\ell)) = 2 \sum_{\ell=1}^s (\delta_i a_\ell)(\delta_j a_\ell).$$

Thus, we can write

$$J(-2a_1, \dots, -2a_s) = 2 \det \left(J(a_1, \dots, a_s) J^T(a_1, \dots, a_s) \right) \neq 0.$$

Since $J(\Lambda)$ is a nonzero polynomial, there exist $\lambda_1^*, \dots, \lambda_s^* \in \mathbb{Q}$ such that $J(\lambda_1^*, \dots, \lambda_s^*) \neq 0$. Then $P^* := \lambda_1^* x_1 + \dots + \lambda_s^* x_s + x_1^2 + \dots + x_s^2$ is a witness of the nonemptiness of U . \square

Lemma 6.3 *Consider an extension of Δ - Σ fields $F \subset E$ such that*

- $E = F\langle a_1, \dots, a_n \rangle$ with $s \leq n$;
- E is nondegenerate (see Definition 4.2);
- $\det J(a_1, \dots, a_s) \neq 0$.

Then, for every m , there exists a polynomial $P \in F[x_1, \dots, x_n]$ of degree at most two such that $P_a := P(a_1, \dots, a_n)$ is m -nonperiodic (see Definition 4.5) and $\det J(\delta_1 P_a, \dots, \delta_s P_a) \neq 0$.

Proof We will extend the set a_1, \dots, a_n of generators of E over F by some elements of F as follows. For every pair $\alpha, \beta \in \mathbb{Z}_{\geq 0}^t(m)$ such that $\alpha \neq \beta$, since $\sigma^{\alpha-\beta}|_E \neq \text{id}$, there are two options:

- if $\sigma^{\alpha-\beta}|_F \neq \text{id}$, then we take $a \in F$ such that $\sigma^\alpha a \neq \sigma^\beta a$ and add it to the set of generators;
- otherwise, if $\sigma^{\alpha-\beta}|_F = \text{id}$, there exists $1 \leq i \leq n$ such that $\sigma^{\alpha-\beta} a_i \neq a_i$.

Using this procedure we construct an extended set of generators a_1, \dots, a_N such that

- $a_{n+1}, \dots, a_N \in F$ and
- for every pair $\alpha, \beta \in \mathbb{Z}_{\geq 0}^t(m)$ such that $\alpha \neq \beta$, there exists $1 \leq i(\alpha, \beta) \leq N$ such that $\sigma^\alpha a_{i(\alpha, \beta)} \neq \sigma^\beta a_{i(\alpha, \beta)}$.

Let $V := \{P \in \mathbb{Q}[x_1, \dots, x_N] \mid \deg P \leq 2\}$. Let $U \subset V$ be a nonempty open Zariski subset given by Lemma 6.2.

For every pair $\alpha, \beta \in \mathbb{Z}_{\geq 0}^t(m)$ such that $\alpha \neq \beta$, consider

$$U_{\alpha, \beta} := \{P \in V \mid \sigma^\alpha P(a_1, \dots, a_N) \neq \sigma^\beta P(a_1, \dots, a_N)\} \subset V.$$

Since $U_{\alpha, \beta}$ is defined by an inequation, it is an open subset of V . Moreover, since $x_{i(\alpha, \beta)} \in U_{\alpha, \beta}$, $U_{\alpha, \beta} \neq \emptyset$. Then the intersection of U and all the subsets $U_{\alpha, \beta}$ with $\alpha, \beta \in \mathbb{Z}_{\geq 0}^t$ and $\alpha \neq \beta$ is a nonempty open subset of V . Let P_0 be an element of this subset. Then $P_1 := P_0(x_1, \dots, x_n, a_{n+1}, \dots, a_N) \in F[x_1, \dots, x_n]$ is a desired polynomial. \square

6.2 Core lemmas

The following lemma generalizes Lemma 5.1.

Lemma 6.4 *Let K be a field. We denote the partial derivatives of $K[[x_1, \dots, x_n]]$ with respect to x_1, \dots, x_n by $\partial_1, \dots, \partial_n$, respectively. Let $D_1 \in K[\partial_1], \dots, D_n \in K[\partial_n]$ be differential operators of order at most m . For every $f \in K[[x_1, \dots, x_n]]$,*

$$(D_1 f = \dots = D_n f = 0 \ \& \ [f]_m = 0) \implies f = 0.$$

Proof Let

$$f = \sum_{\mathbf{k} \in \mathbb{Z}_{\geq 0}^n} c_{\mathbf{k}} x^{\mathbf{k}} \in K[[x_1, \dots, x_n]].$$

We will show that $c_{\mathbf{k}} = 0$ for every $\mathbf{k} \in \mathbb{Z}_{\geq 0}^n$ by induction on $|\mathbf{k}|$. Let $\mathbf{k} = (k_1, \dots, k_n)$. If $k_i < m$ for every $1 \leq i \leq n$, then $c_{\mathbf{k}} = 0$ because $[f]_m = 0$. Assume that there exists $1 \leq i \leq n$ such that $k_i \geq m$. Then $D_i f = 0$ implies that $c_{\mathbf{k}}$ is a linear combination of $c_{\mathbf{k}-\mathbf{1}_i}, \dots, c_{\mathbf{k}-m\mathbf{1}_i}$, where $\mathbf{1}_i$ is the i -th basis vector of \mathbb{Z}^n . Due to the induction hypothesis, these coefficients are all equal to zero, so $c_{\mathbf{k}} = 0$. \square

For every positive integer n , throughout the rest of the paper, for a Δ - Σ -field E , we extend the operators from E to $E[[x_1, \dots, x_n]]$ by

$$\phi\left(\sum_{\mathbf{k} \in \mathbb{Z}_{\geq 0}^n} c_{\mathbf{k}} x^{\mathbf{k}}\right) = \sum_{\mathbf{k} \in \mathbb{Z}_{\geq 0}^n} \phi(c_{\mathbf{k}}) x^{\mathbf{k}} \quad \text{for every } \sum_{\mathbf{k} \in \mathbb{Z}_{\geq 0}^n} c_{\mathbf{k}} x^{\mathbf{k}} \in E[[x_1, \dots, x_n]] \\ \text{and } \phi \in \Delta \cup \Sigma. \tag{10}$$

The following lemma generalizes Lemma 5.2.

Lemma 6.5 *Let E be a Δ - Σ -field and a_1, \dots, a_n be elements of E such that $\text{rank } J(a_1, \dots, a_n) = s$. We extend $\Delta \cup \Sigma$ to $E[[x_1, \dots, x_n]]$ as in (10). For $m \in \mathbb{Z}_{\geq 0}$, we introduce the following subset of $E[[x_1, \dots, x_n]]$*

$$S_m := \left\{ \delta^{\alpha} e^{a_1 x_1 + \dots + a_n x_n} \mid \alpha \in \mathbb{Z}_{\geq 0}^s(m) \right\}.$$

Then the elements of S_m are linearly independent over E .

Proof We will use notation $(\mathbf{a}, \mathbf{x}) := a_1x_1 + \dots + a_nx_n$. We will prove the lemma by induction on m . The base case $m = 0$ is true because $S_0 = \{e^{(\mathbf{a}, \mathbf{x})}\}$.

Assume that we have proved the lemma for some $m \geq 0$. Let V be a space of all polynomials from $E[x_1, \dots, x_n]$ of degree at most m . Then $S_m \subset V_e := Ve^{(\mathbf{a}, \mathbf{x})}$. Hence it is sufficient to prove that the elements of $S_{m+1} \setminus S_m$ are linearly independent modulo V_e . For every $\alpha = (\alpha_1, \dots, \alpha_s) \in \mathbb{Z}_{\geq 0}^s(m+1)$, we have

$$\delta^\alpha e^{(\mathbf{a}, \mathbf{x})} \equiv \prod_{i=1}^s (\delta_i(\mathbf{a}, \mathbf{x}))^{\alpha_i} e^{(\mathbf{a}, \mathbf{x})} \pmod{V_e}.$$

Thus, it is sufficient to prove that the elements of $\{\prod_{i=1}^s (\delta_i(\mathbf{a}, \mathbf{x}))^{\alpha_i} \mid \alpha \in \mathbb{Z}_{\geq 0}^s(m+1)\}$ are linearly independent over E . Assume the contrary. Then there exists a nonzero homogeneous polynomial $P \in E[y_1, \dots, y_s]$ of degree $m+1$ such that

$$P(\delta_1(\mathbf{a}, \mathbf{x}), \dots, \delta_s(\mathbf{a}, \mathbf{x})) = 0.$$

However, since $\text{rank } J(a_1, \dots, a_n) = s$, linear forms $\delta_1(\mathbf{a}, \mathbf{x}), \dots, \delta_s(\mathbf{a}, \mathbf{x})$ are linearly independent, so P cannot vanish on them. \square

The following lemma generalizes Lemma 5.3.

Lemma 6.6 *Let $F \subset E$ be an extension of Δ - Σ -fields. Let a_1, \dots, a_n be elements of E such that*

- $\text{rank } J(a_1, \dots, a_n) = s$;
- a_1 is $2M$ -nonperiodic.

Let $N = 2(M+1)^{t+1}$. We extend $\Delta \cup \Sigma$ to $E[\![x_1, \dots, x_n]\!]$ as in (10). If there exists a nontrivial F -linear combination of

$$\left\{ [\delta^\alpha \sigma^\beta e^{a_1x_1 + \dots + a_nx_n}]_N \mid \alpha \in \mathbb{Z}_{\geq 0}^s(M), \beta \in \mathbb{Z}_{\geq 0}^t(M) \right\} \quad (11)$$

that belongs to $F[x_1, \dots, x_n]$, then $a_1 \in F$.

Proof We are given that there exist $c_{\alpha, \beta} \in F$ not all zero such that

$$\begin{aligned} \sum_{\substack{\alpha \in \mathbb{Z}_{\geq 0}^s(M), \\ \beta \in \mathbb{Z}_{\geq 0}^t(M)}} c_{\alpha, \beta} [\delta^\alpha \sigma^\beta e^{a_1x_1 + \dots + a_nx_n}]_N &= \left[\sum_{\substack{\alpha \in \mathbb{Z}_{\geq 0}^s(M), \\ \beta \in \mathbb{Z}_{\geq 0}^t(M)}} c_{\alpha, \beta} \delta^\alpha \sigma^\beta e^{a_1x_1 + \dots + a_nx_n} \right]_N \\ &= f \in F[x_1, \dots, x_n]. \end{aligned} \quad (12)$$

Collecting together the terms with the same exponential part, we can write

$$\sum_{\substack{\alpha \in \mathbb{Z}_{\geq 0}^s(M), \\ \beta \in \mathbb{Z}_{\geq 0}^t(M)}} c_{\alpha, \beta} \delta^\alpha \sigma^\beta e^{a_1x_1 + \dots + a_nx_n} = \sum_{\beta \in \mathbb{Z}_{\geq 0}^t(M)} C_\beta e^{(\sigma^\beta a_1)x_1 + \dots + (\sigma^\beta a_n)x_n},$$

where $C_\beta \in E[x_1, \dots, x_n]$.

Step 1 *There exists $\beta \in \mathbb{Z}_{\geq 0}^t(M)$ such that $C_\beta \neq 0$.*

Consider any β such that $C_\beta = 0$. Since

$$\operatorname{rank} J(a_1, \dots, a_n) = s \implies \operatorname{rank} J(\sigma^\beta a_1, \dots, \sigma^\beta a_n) = s,$$

Lemma 6.5 implies that $\{\delta^\alpha e^{(\sigma^\beta a_1)x_1 + \dots + (\sigma^\beta a_n)x_n} \mid \alpha \in \mathbb{Z}_{\geq 0}^s(M)\}$ are E -linearly independent. Thus, $C_\beta = 0$ implies that, for every $\alpha \in \mathbb{Z}_{\geq 0}^s(M)$, $c_{\alpha, \beta} = 0$. Thus, if $C_\beta = 0$ for every $\beta \in \mathbb{Z}_{\geq 0}^t(M)$, we arrive at contradiction with the fact that not all $c_{\alpha, \beta}$ are zeros.

Step 2 *Let \bar{E} be an algebraic closure of E (we do not assume that \bar{E} has a structure of Δ - Σ -field). Let $\Lambda_0 := \{\beta \mid C_\beta \neq 0\} \subset \mathbb{Z}_{\geq 0}^t(M)$. For every field automorphism $\tau: \bar{E} \rightarrow \bar{E}$ such that $\tau|_F = \operatorname{id}$ and every $\beta_1 \in \Lambda_0$, there exists $\beta_2 \in \Lambda_0$ such that $\tau(\sigma^{\beta_1} a_1) = \sigma^{\beta_2} a_1$.*

Let τ act on $\bar{E}[[x_1, \dots, x_n]]$ coefficient-wise. Applying τ to (12), we obtain

$$\begin{aligned} & \left[\sum_{\beta \in \mathbb{Z}_{\geq 0}^t(M)} C_\beta e^{(\sigma^\beta a_1)x_1 + \dots + (\sigma^\beta a_n)x_n} \right]_N \\ &= f = \left[\sum_{\beta \in \mathbb{Z}_{\geq 0}^t(M)} \tau(C_\beta) e^{\tau(\sigma^\beta a_1)x_1 + \dots + \tau(\sigma^\beta a_n)x_n} \right]_N \end{aligned}$$

Let

$$S := \sum_{\beta \in \mathbb{Z}_{\geq 0}^t(M)} C_\beta e^{(\sigma^\beta a_1)x_1 + \dots + (\sigma^\beta a_n)x_n} - \sum_{\beta \in \mathbb{Z}_{\geq 0}^t(M)} \tau(C_\beta) e^{\tau(\sigma^\beta a_1)x_1 + \dots + \tau(\sigma^\beta a_n)x_n}.$$

Since, for every $\beta \in \mathbb{Z}_{\geq 0}^t(M)$, the total degree of C_β does not exceed M , we have

$$D_i S = 0, \text{ where } D_i := \prod_{\beta \in \mathbb{Z}_{\geq 0}^t(M)} (\partial_i - \sigma^\beta a_i)^{M+1} \cdot \prod_{\beta \in \mathbb{Z}_{\geq 0}^t(M)} (\partial_i - \tau(\sigma^\beta a_i))^{M+1}$$

for every $1 \leq i \leq n$. Since the order of D_i is does not exceed $2(M+1) \cdot |\mathbb{Z}_{\geq 0}^t(M)| \leq 2(M+1)^{t+1} = N$ and $[S]_N = 0$, Lemma 6.4 implies that $S = 0$.

Since a_1 is $2M$ -nonperiodic, the set $\{\sigma^\beta a_1 \mid \beta \in \Lambda_0\}$ contains $|\Lambda_0|$ distinct elements. If the number of distinct elements in the set

$$\{\sigma^\beta a_1 \mid \beta \in \Lambda_0\} \cup \{\tau(\sigma^\beta a_1) \mid \beta \in \Lambda_0\}$$

is greater than $|\Lambda_0|$, then there is $\beta_0 \in \Lambda_0$ such that

$$\tau\sigma^{\beta_0}a_1 \notin \{\sigma^\beta a_1 \mid \beta \in \Lambda_0\} \cup \{\tau(\sigma^\beta a_1) \mid \beta \in \Lambda_0, \beta \neq \beta_0\}.$$

Then the equation $S = 0$ implies that the exponential power series $e^{\tau(\sigma^{\beta_0}a_1)x_1 + \dots + \tau(\sigma^{\beta_0}a_n)x_n}$ can be written as a $E(x_1, \dots, x_n)$ -linear combination of exponential power series with the exponents different from $\tau(\sigma^{\beta_0}a_1)x_1 + \dots + \tau(\sigma^{\beta_0}a_n)x_n$, and this is impossible. Thus, for every $\beta_0 \in \Lambda_0$, $\tau(\sigma^{\beta_0}a_1) \in \{\sigma^\beta a_1 \mid \beta \in \Lambda_0\}$.

Step 3 $a_1 \in F$.

Consider $\beta_0 \in \Lambda_0$. Step 2 implies that every element conjugate to $\sigma^{\beta_0}a_1$ in \overline{E} over F is of the form $\sigma^\beta a_1$, where $\beta \in \Lambda_0$. In particular, $\sigma^{\beta_0}a_1$ is algebraic over F . Consider the minimal polynomial $P(t) \in F[t]$ for $\sigma^{\beta_0}a_1$ over F . The roots of $P(t)$ form a subset in $\{\sigma^\beta a_1 \mid \beta \in \Lambda_0\}$. We define $\Lambda_P := \{\beta \in \Lambda_0 \mid P(\sigma^\beta a_1) = 0\}$. Let β_1 and β_2 be the smallest and the largest elements of Λ_P with respect to the lexicographic ordering, respectively. Let

$$Q(t) := \sigma^{\beta_2 - \beta_1} P(t) \in F[t].$$

Then the set of roots of Q in \overline{E} is exactly $\{\sigma^\beta a_1 \mid \beta \in \beta_2 - \beta_1 + \Lambda_P\}$. We will show that

$$\Lambda_P \cap (\beta_2 - \beta_1 + \Lambda_P) = \{\beta_2\}. \quad (13)$$

Assume that there is an element β_3 in the intersection such that $\beta_3 \neq \beta_2$. Then $\beta_3 - \beta_2 + \beta_1 \in \Lambda_P$. The maximality of β_2 implies that $\beta_3 - \beta_2 <_{lex} \mathbf{0}$. Then $\beta_3 - \beta_2 + \beta_1 <_{lex} \beta_1$, and this contradicts the minimality of β_1 and proves (13).

Consider any common root of P and Q . This root can be written as $\sigma^{\beta_3}a_1$ where $\beta_3 \in \Lambda_P$ and as $\sigma^{\beta_4}a_1$ where $\beta_4 \in \beta_2 - \beta_1 + \Lambda_P$. Then $\sigma^{\beta_3 + \beta_1}a_1 = \sigma^{\beta_4 + \beta_1}a_1$. Since $|\beta_3 + \beta_1| \leq 2M$, $|\beta_4 + \beta_1| \leq 2M$, and the a_1 is $2M$ -nonperiodic, we obtain $\beta_3 = \beta_4$. Using (13), we see that $\beta_2 = \beta_3 = \beta_4$, so the only common root of P and Q is $\sigma^{\beta_2}a_1$. Then $\sigma^{\beta_2}a_1$ is the only root of $\gcd(P, Q) \in F[t]$, so $\sigma^{\beta_2}a_1 \in F$. Applying $\sigma^{-\beta_2}$, we obtain $a_1 \in F$. \square

6.3 Proof of Theorem 2.1

Proof of Theorem 2.1 Lemma 6.1 implies that there are elements $c_1, \dots, c_s \in E$ such that $\det J(c_1, \dots, c_s) \neq 0$. Adding these elements to the set a_1, \dots, a_n of generators of E over F if necessary, we will further assume that $\text{rank } J(a_1, \dots, a_n) = s$.

For $f_1, \dots, f_r \in E$ and a positive integer m , we introduce

$$\text{trdeg}(f_1, \dots, f_r; m) := \text{trdeg}_F F \left(\delta^\alpha \sigma^\beta f_i \mid 1 \leq i \leq r, \alpha \in \mathbb{Z}_{\geq 0}^s(m), \beta \in \mathbb{Z}_{\geq 0}^t(m) \right).$$

Since every element of E is Δ - Σ -algebraic over F , [20, Theorem 2.1] implies that there exists a polynomial $p(z) \in \mathbb{Q}[z]$ of degree less than $s + t$ such that

$$\operatorname{trdeg}(a_1, \dots, a_n; m) < p(m) \quad \text{for every } m \in \mathbb{Z}_{\geq 0}.$$

Since

$$\left| \{(\alpha, \beta) \mid \alpha \in \mathbb{Z}_{\geq 0}^s(m), \beta \in \mathbb{Z}_{\geq 0}^t(m) \} \right| = \binom{m+s}{s} \binom{m+t}{t}$$

and $\binom{m+s}{s} \binom{m+t}{t}$ is a polynomial of degree $s + t$ in m , there exists $M \in \mathbb{Z}_{\geq 0}$ such that

$$\operatorname{trdeg}(a_1, \dots, a_n; M + n) = p(M + n) < \left| \{(\alpha, \beta) \mid \alpha \in \mathbb{Z}_{\geq 0}^s(M), \beta \in \mathbb{Z}_{\geq 0}^t(M) \} \right|.$$

We will prove by induction on ℓ that, for every $0 \leq \ell \leq n$, there exists $b_\ell \in E$ such that

- (R1) b_ℓ is $2M$ -nonperiodic;
- (R2) $\det J(\delta_1 b_\ell, \dots, \delta_s b_\ell) \neq 0$;
- (R3) $E = F\langle b_\ell, a_{\ell+1}, \dots, a_n \rangle$;
- (R4) $\operatorname{trdeg}(b_\ell, a_{\ell+1}, \dots, a_n; M + n - \ell) < D_M := \left| \{(\alpha, \beta) \mid \alpha \in \mathbb{Z}_{\geq 0}^s(M), \beta \in \mathbb{Z}_{\geq 0}^t(M) \} \right|$.

Since $E = F\langle b_n \rangle$, proving the existence of such b_0, \dots, b_n will prove the theorem.

Consider the base case $\ell = 0$. Lemma 6.3 implies that there exists a polynomial $P \in F[x_1, \dots, x_n]$ such that $b_0 := P(a_1, \dots, a_n)$ is $2M$ -nonperiodic and $\det J(\delta_1 b_0, \dots, \delta_s b_0) \neq 0$. Thus, b_0 satisfies (R1) and (R2). (R3) is trivially satisfied. Finally, since $b_0 \in F(a_1, \dots, a_n)$, we have

$$\operatorname{trdeg}(b_0, a_1, \dots, a_n; M + n) = \operatorname{trdeg}(a_1, \dots, a_n; M + n),$$

so (R4) also holds.

Assume that we have constructed b_ℓ for some $\ell \geq 0$. We set $N := 2(M + 1)^{t+1}$ (as in Lemma 6.6) and $\Gamma := \{0, \dots, N\}^{s+1} \subset \mathbb{Z}^{s+1}$, introduce a set variables

$$\Theta := \{\theta_\gamma \mid \gamma \in \Gamma\} \cup \{\theta_{-1}\},$$

and extend the action of $\Delta \cup \Sigma$ from E to $E(\Theta)$ by making all elements of Θ to be Δ - Σ -constants. Let

$$B_{\ell+1} := \theta_{-1} a_{\ell+1} + \sum_{\gamma \in \Gamma} \frac{\theta_\gamma}{\gamma!} b_\ell^{\gamma_0} (\delta_1 b_\ell)^{\gamma_1} \dots (\delta_s b_\ell)^{\gamma_s}. \quad (14)$$

We regard any point $\varphi \in \mathbb{Q}^{|\Theta|}$ as a function $\varphi: \Theta \rightarrow \mathbb{Q}$ and extend it to a E -algebra homomorphism $\varphi: E[\Theta] \rightarrow E$.

Claim 1 There exists a Zariski open nonempty subset $U_1 \subset \mathbb{Q}^{|\Theta|}$ such that

$$F\langle\varphi(B_{\ell+1})\rangle = F\langle b_\ell, a_{\ell+1}\rangle \quad \text{for every } \varphi \in U_1.$$

Since

$$\begin{aligned} \text{trdeg}_{F(\Theta)} F(\Theta, \{\delta^\alpha \sigma^\beta B_{\ell+1} \mid \alpha \in \mathbb{Z}_{\geq 0}^s(M), \beta \in \mathbb{Z}_{\geq 0}^t(M)\}) \\ \leq \text{trdeg}(a_{\ell+1}, b_\ell, \delta_1 b_\ell, \dots, \delta_s b_\ell; M) \\ \leq \text{trdeg}(a_{\ell+1}, b_\ell; M+1) \leq \text{trdeg}(b_\ell, a_{\ell+1}, \dots, a_n; M+1) < D_M, \end{aligned}$$

the elements of $\{\delta^\alpha \sigma^\beta B_{\ell+1} \mid \alpha \in \mathbb{Z}_{\geq 0}^s(M), \beta \in \mathbb{Z}_{\geq 0}^t(M)\}$ are algebraically dependent over $F(\Theta)$. Thus, there exists a Δ - Σ -polynomial $R \in F(\Theta)[\delta^\alpha \sigma^\beta z \mid \alpha \in \mathbb{Z}_{\geq 0}^s(M), \beta \in \mathbb{Z}_{\geq 0}^t(M)]$ such that $R(B_{\ell+1}) = 0$. We will assume that R is chosen to be of the minimal possible total degree. We introduce

$$\begin{aligned} R_{\alpha, \beta} &:= \frac{\partial R}{\partial \delta^\alpha \sigma^\beta z}(B_{\ell+1}) \text{ for } \alpha \in \mathbb{Z}_{\geq 0}^s(M), \beta \in \mathbb{Z}_{\geq 0}^t(M) \quad \text{and} \\ R_{\theta_\gamma} &:= \frac{\partial R}{\partial \theta_\gamma}(B_{\ell+1}) \text{ for } \gamma \in \Gamma. \end{aligned}$$

The minimality of the degree of R implies that not all of $R_{\alpha, \beta}$ are zero. Consider any $\gamma \in \Gamma$. Differentiating $R(B_\ell) = 0$ with respect to θ_γ , we obtain

$$\sum_{\substack{\alpha \in \mathbb{Z}_{\geq 0}^s(M), \\ \beta \in \mathbb{Z}_{\geq 0}^t(M)}} R_{\alpha, \beta} \delta^\alpha \sigma^\beta \left(\frac{b_\ell^{\gamma_0} (\delta_1 b_\ell)^{\gamma_1} \dots (\delta_s b_\ell)^{\gamma_s}}{\gamma!} \right) = -R_{\theta_\gamma}. \quad (15)$$

We extend the action of $\Delta \cup \Sigma$ from $E(\Theta)$ to $E(\Theta)[[x_1, \dots, x_s]]$ as in (10). We multiply (15) by $x_0^{\gamma_0} \dots x_s^{\gamma_s}$ and sum such equations over all $\gamma \in \Gamma$. We obtain

$$\sum_{\substack{\alpha \in \mathbb{Z}_{\geq 0}^s(M), \\ \beta \in \mathbb{Z}_{\geq 0}^t(M)}} R_{\alpha, \beta} \left[\delta^\alpha \sigma^\beta e^{b_\ell x_0 + (\delta_1 b_\ell) x_1 + \dots + (\delta_s b_\ell) x_s} \right]_N = \sum_{\gamma \in \Gamma} -R_{\theta_\gamma} x_0^{\gamma_0} \dots x_s^{\gamma_s}. \quad (16)$$

We apply Lemma 6.6 to (16) with $a_1 = b_\ell, a_2 = \delta_1 b_\ell, \dots, a_{s+1} = \delta_s b_\ell$ and $F = F\langle\Theta, B_{\ell+1}\rangle$, and deduce that $b_\ell \in F\langle\Theta, B_{\ell+1}\rangle$. Then there exist nonzero Δ - Σ polynomials $P_1, P_2 \in F[\Theta]\{z\}$ such that

$$b_\ell = \frac{P_1(B_{\ell+1})}{P_2(B_{\ell+1})}. \quad (17)$$

We define $U_1 := \{\varphi \in \mathbb{Q}^{|\Theta|} \mid \varphi(P_2(B_{\ell+1})) \neq 0 \text{ and } \varphi(\theta_{-1}) \neq 0\}$. Since P_2 is a nonzero polynomial, U_1 is nonempty. Consider $\varphi \in U_1$. Then (17) implies that $b_\ell \in$

$F\langle\varphi(B_{\ell+1})\rangle$. Since $\varphi(\theta_{-1}) \neq 0$, $a_{\ell+1} \in F\langle\varphi(B_{\ell+1})\rangle$, so $F\langle\varphi(B_{\ell+1})\rangle = F\langle b_\ell, a_{\ell+1}\rangle$. The claim is proved.

Claim 2 *Let*

$$U_2 := \{\varphi \in \mathbb{Q}^{|\Theta|} \mid \det J(\delta_1\varphi(B_{\ell+1}), \dots, \delta_s\varphi(B_{\ell+1})) \neq 0 \text{ and } \varphi(B_{\ell+1}) \text{ is } 2M\text{-nonperiodic}\}.$$

Then U_2 is a nonempty Zariski open set.

The fact that $\varphi(B_{\ell+1})$ is $2M$ -nonperiodic can be expressed by a system of inequations as in the proof of Lemma 6.3. Thus, U_2 is defined by a system of inequations, so it is open. Consider $\varphi_0 \in \mathbb{Q}^{|\Theta|}$ defined by

$$\varphi_0(\theta_\gamma) = \begin{cases} 1, & \text{if } \gamma = (1, 0, \dots, 0), \\ 0, & \text{otherwise,} \end{cases} \quad \varphi_0(\theta_{-1}) = 0.$$

Then $\varphi_0(B_{\ell+1}) = b_\ell$. We have $\det J(\delta_1 b_\ell, \dots, \delta_s b_\ell) \neq 0$ due to (R2) and b_ℓ is $2M$ -nonperiodic due to (R1). Thus, $\varphi_0 \in U_2$, so $U_2 \neq \emptyset$. The claim is proved.

Consider $\varphi \in U_1 \cap U_2$ and define $b_{\ell+1} := \varphi(B_{\ell+1})$. Then (R3) holds because $\varphi \in U_1$, (R1) and (R2) hold because $\varphi \in U_2$. Since $b_{\ell+1} \in F(a_{\ell+1}, b_\ell, \delta_1 b_\ell, \dots, \delta_s b_\ell)$, we have

$$\begin{aligned} \text{trdeg}(b_{\ell+1}, a_{\ell+2}, \dots, a_n; M + n - \ell - 1) \\ \leq \text{trdeg}(b_\ell, a_{\ell+1}, \dots, a_n; M + n - \ell) < D_M. \end{aligned}$$

This proves (R4) for $b_{\ell+1}$ and finishes the proof of the existence of b_0, \dots, b_n such that (R1), (R2), (R3), and (R4) hold. \square

Acknowledgements The author is grateful to Lei Fu, Alexey Ovchinnikov, Thomas Scanlon, and the referee for their suggestions and helpful discussions. This work has been partially supported by NSF Grants CCF-1564132, CCF-1563942, DMS-1853482, DMS-1853650, and DMS-1760448, by PSC-CUNY Grants #69827-0047 and #60098-0048.

References

1. Andrews, G. E., Askey, R., Roy, R.: Special Functions. Encyclopedia of Mathematics and its Applications. Cambridge University Press, Cambridge (1999). <https://doi.org/10.1017/CBO9781107325937>
2. Bélair, L.: Approximation for Frobenius algebraic equations in Witt vectors. J. Algebra **321**(9), 2353–2364 (2009). <https://doi.org/10.1016/j.jalgebra.2009.01.021>
3. Bell, D.J., Lu, X.Y.: Differential algebraic control theory. IMA J. Math. Control Inf. **9**(4), 361–383 (1992). <https://doi.org/10.1093/imamci/9.4.361>
4. Blossier, T., Hardouin, C., Martin-Pizarro, A.: Sur les automorphismes bornés de corps munis d’opérateurs. Math. Res. Lett. **24**(4), 955–978 (2017). <https://doi.org/10.4310/MRL.2017.v24.n4.a2>
5. Brouette, Q., Point, F.: On differential Galois groups of strongly normal extensions. Math. Logic Q. **64**(3), 155–169 (2018). <https://doi.org/10.1002/malq.201600098>
6. Chatzidakis, Z.: Model theory of fields with operators—a survey. In : Villaveces A, Kossak R, Kontinen J, Hirvonen Å (eds) Logic Without Borders—Essays on Set Theory, Model Theory, Philosophical Logic and Philosophy of Mathematics, pp. 91–114. (2015). <https://doi.org/10.1515/9781614516873.91>

7. Chatzidakis, Z., Hrushovski, E.: Model theory of difference fields. *Trans. Am. Math. Soc.* **351**, 2997–3071 (1999). <https://doi.org/10.1090/S0002-9947-99-02498-8>
8. Cluzeau, T., Hubert, E.: Resolvent representation for regular differential ideals. *Appl. Algebra Eng. Commun. Comput.* **13**(5), 395–425 (2003). <https://doi.org/10.1007/s00200-002-0110-4>
9. Cluzeau, T., Hubert, E.: Probabilistic algorithms for computing resolvent representations of regular differential ideals. *Appl. Algebra Eng. Commun. Comput.* **19**(5), 365–392 (2008). <https://doi.org/10.1007/s00200-008-0079-8>
10. Cohn, R.M.: *Difference Algebra*. Interscience Publishers, Geneva (1965)
11. D'Alfonso, L., Jeronimo, G., Solerno, P.: Quantitative aspects of the generalized differential Lüroth's theorem. *J. Algebra* **507**, 547–570 (2018). <https://doi.org/10.1016/j.jalgebra.2018.01.050>
12. Fliess, M.: Generalized controller canonical form for linear and nonlinear dynamics. *IEEE Trans. Autom. Control* **35**(9), 994–1001 (1990). <https://doi.org/10.1109/9.58527>
13. Freitag, J., Li, W.: Simple Differential Field Extensions and Effective Bounds. *Lecture Notes in Computer Science*, vol. 9582, pp. 343–357. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-32859-1_29
14. Gao, X., Van der Hoeven, J., Yuan, C., Zhang, G.: Characteristic set method for differential-difference polynomial systems. *J. Symb. Comput.* **44**(9), 1137–1163 (2009). <https://doi.org/10.1016/j.jsc.2008.02.010>
15. Hardouin, C., Singer, M.F.: Differential Galois theory of linear difference equations. *Math. Ann.* **342**(2), 333–377 (2008). <https://doi.org/10.1007/s00208-008-0238-z>
16. Kamensky, M.: Tannakian formalism over fields with operators. *Int. Math. Res. Notices* **2013**(24), 5571–5622 (2013). <https://doi.org/10.1093/imrn/rns190>
17. Kolchin, E.R.: Extensions of differential fields. *Ann. Math.* **43**(4), 724–729 (1942)
18. Kolchin, E.R.: *Differential Algebra and Algebraic Groups*. Academic Press, New York (1973)
19. Kondratieva, M.V., Levin, A.B., Mikhalev, A.V., Pankratiev, E.V.: *Differential and Difference Dimension Polynomials*. Springer, Dordrecht (2010)
20. Levin, A.B. : Multivariate difference-differential dimension polynomials and new invariants of difference-differential field extensions. In: *Proceedings of the 38th International Symposium on Symbolic and Algebraic Computation, ISSAC '13*, pp. 267–274, (2013). <https://doi.org/10.1145/2465506.2465521>
21. Levin, A.B.: *Difference Algebra*. Springer, Dordrecht (2008). <https://doi.org/10.1007/978-1-4020-6947-5>
22. Loos, R.: Computing in Algebraic Extensions, pp. 173–187. Springer, Vienna (1983). https://doi.org/10.1007/978-3-7091-7551-4_12
23. Marker, D.: Chapter 2: Model Theory of Differential Fields, of *Lecture Notes in Logic*, vol. 5, pp. 38–113. Springer, Berlin, (1996). <https://projecteuclid.org/euclid.lnl/1235423156>
24. Medina, R.F.B.: Differentially closed fields of characteristic zero with a generic automorphism. *Rev. de Mat. Teor. y Appl.* **14**(1), 81–100 (2007). <https://doi.org/10.15517/rmta.v14i1.282>
25. Miller, R., Ovchinnikov, A., Trushin, D.: Computing constraint sets for differential fields. *J. Algebra* **407**, 316–357 (2014). <https://doi.org/10.1016/j.jalgebra.2014.02.032>
26. Moosa, R., Scanlon, T.: Jet and prolongation spaces. *J. Inst. Math. Jussieu* **9**(2), 391–430 (2010). <https://doi.org/10.1017/S1474748010000010>
27. Moosa, R., Scanlon, T.: Model theory of fields with free operators in characteristic zero. *J. Math. Logic* **14**(2), 1450009 (2014). <https://doi.org/10.1142/S0219061314500093>
28. Ohyama, Y.: Differential relations of theta functions. *Osaka J. Math.* **32**(2), 431–450 (1995)
29. Ostrowski, A.: Über Dirichletsche Reihen und algebraische Differentialgleichungen. *Math. Z.* **8**(3–4), 241–298 (1920). <https://doi.org/10.1007/BF01206530>
30. Pogudin, G.: The primitive element theorem for differential fields with zero derivation on the base field. *J. Pure Appl. Algebra* **219**(9), 4035–4041 (2015). <https://doi.org/10.1016/j.jpaa.2015.02.004>
31. Ritt, J.F.: *Differential Equations from the Algebraic Standpoint*. Colloquium Publications. American Mathematical Society, Providence (1932)
32. Sánchez, O.L.: On the model companion of partial differential fields with an automorphism. *Isr. J. Math.* **212**(1), 419–442 (2016). <https://doi.org/10.1007/s11856-016-1292-y>
33. Seidenberg, A.: Abstract differential algebra and the analytic case. II. In: *Proceedings of the American Mathematical Society*, vol. 23, no. 3, pp. 689–691, (1969). URL <https://www.jstor.org/stable/2036611>
34. Seidenberg, A.: Abstract differential algebra and the analytic case. In: *Proceedings of the American Mathematical Society*, vol. 9, no. 1, pp. 159–164, (1958). URL <https://www.jstor.org/stable/2033416>

35. Seidenberg, A.: Some basic theorems in differential algebra (characteristic p , arbitrary). *Trans. Am. Math. Soc.* **73**(1), 174–190 (1952)
36. Singer, M.F.: The model theory of ordered differential fields. *J. Symb. Logic* **43**(1), 82–91 (1978)
37. van der Waerden, B.: *Algebra*. Springer, New York (1991)
38. Wood, C.: Prime model extensions for differential fields of characteristic $p \neq 0$. *J. Symb. Logic* **39**(3), 469–477 (1974). <https://doi.org/10.2307/2272889>

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.