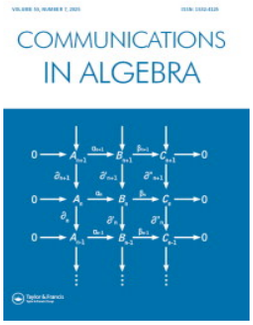
Taylor & Francis
Taylor & Francis Group



Communications in Algebra

ISSN: 0092-7872 (Print) 1532-4125 (Online) Journal homepage: www.tandfonline.com/journals/lagb20

Hilbert's irreducibility theorem for linear differential operators

Ruyong Feng, Zewang Guo & Wei Lu

To cite this article: Ruyong Feng, Zewang Guo & Wei Lu (2025) Hilbert's irreducibility theorem for linear differential operators, Communications in Algebra, 53:7, 2625-2633, DOI: 10.1080/00927872.2024.2448247

To link to this article: https://doi.org/10.1080/00927872.2024.2448247

COMMUNICATIONS IN ALGEBRA®
2025, VOL. 53, NO. 7, 2625–2633
https://doi.org/10.1080/00927872.2024.2448247

Hilbert's irreducibility theorem for linear differential operators

Ruyong Feng[a], Zewang Guo[a], and Wei Lu[b]

[a]KLMM, Academy of Mathematics and Systems Science, Chinese Academy of Sciences and School of Mathematics, University of Chinese Academy of Sciences, Beijing; [b]Hubei Key Laboratory of Applied Mathematics, Faculty of Mathematics and Statistics, Hubei University, Wuhan, China

ABSTRACT

We prove a differential analogue of Hilbert's irreducibility theorem. Let $\mathcal{L}$ be a linear differential operator with coefficients in $C(\mathbb{X})(x)$ that is irreducible over $\overline{C(\mathbb{X})}(x)$, where $\mathbb{X}$ is an irreducible affine algebraic variety over an algebraically closed field C of characteristic zero. We show that the set of $c \in \mathbb{X}(C)$ such that the specialized operator $\mathcal{L}^c$ of $\mathcal{L}$ remains irreducible over $C(x)$ is Zariski dense in $\mathbb{X}(C)$.

ARTICLE HISTORY
Received 21 March 2024
Revised 7 September 2024
Communicated by
Adrian Wadsworth

KEYWORDS
Ad-open set; Hilbert's irreducibility theorem; linear differential operator

2020 MATHEMATICS SUBJECT CLASSIFICATION:
16S32; 68W30

1. Introduction

Linear differential operators, as typical non-commutative polynomials, share many algebraic properties with usual polynomials. Concepts such as the Euclidean algorithm, irreducibility, Eisenstein's criterion, greatest common divisor, and least common multiple from the polynomial ring have counterparts in the realm of linear differential operators. Readers can refer to [14] for an algebraic framework for skew polynomials, including not only linear differential operators but also linear difference and q-difference operators. Similar to the polynomial case, testing irreducibility and factorization are fundamental tasks in the algorithmic aspect of linear differential operators. However, factorizing linear differential operators is more complicated, as they may have infinitely many irreducible divisors, and their factorization is not usually unique. To address the uniqueness of factorization, one has to introduce the notion of similarity (see [14] for the definition and [9, 13] for methods of testing similarity). Despite these complexities, various methods have been developed for the aforementioned tasks, see, for example, [2, 3, 7, 12, 16, 17] for algorithms of factorization and see [1, 7, 11, 15] for methods of testing irreducibility.

In this paper, our emphasis is not on the development of algorithms for testing irreducibility or factorization. Instead, we concentrate on addressing the following problem: given an irreducible linear differential operator with parameters, describe the set of values for which the specializations of the linear differential operator at these values remain irreducible. This can be viewed as a differential analog of Hilbert's irreducibility theorem. Let $f \in \mathbb{Q}[\mathbf{x}, y]$ be an irreducible polynomial, where $\mathbf{x} = x_1, \ldots, x_m$. Hilbert's irreducibility theorem asserts that there exist infinitely many $\mathbf{c} \in \mathbb{Q}^m$ such that $f(\mathbf{c}, y)$ remains irreducible. Fields where Hilbert's irreducibility theorem holds are referred to as Hilbertian fields. For precise definition, readers can refer to Chapter 12 of [5]. By leveraging Hilbert's irreducibility theorem,

CONTACT Wei Lu weilu23@hubu.edu.cn Hubei Key Laboratory of Applied Mathematics, Faculty of Mathematics and Statistics, Hubei University, Wuhan 430062, China.

one can effectively reduce the inverse problem of classical Galois theory over $\mathbb{Q}$ to the problem over $\mathbb{Q}(t)$. Notably, Hilbert demonstrated that both symmetric and alternating groups can be realized as the Galois groups of polynomials over $\mathbb{Q}$.

In the context of this paper, we present an irreducibility theorem for linear differential operators. Precisely, assume that $\mathbb{X}$ is an irreducible affine algebraic variety over an algebraically closed field C of characteristic zero, and $C(\mathbb{X})$ stands for the field of all rational functions on $\mathbb{X}$. Let $C(\mathbb{X})(x)$ be the differential field with usual derivative $\delta = \frac{d}{dx}$, and let $C(\mathbb{X})(x)[\delta]$ be the ring of differential operators with coefficients in $C(\mathbb{X})(x)$, where $\delta x = x\delta + 1$. As usual, $\mathbb{X}(C)$ denotes the set of C-points of $\mathbb{X}$, which is identified with $\mathrm{Hom}_C(C[\mathbb{X}], C)$. For $c \in \mathbb{X}(C)$ and $f \in C[\mathbb{X}]$, the ring of regular functions on $\mathbb{X}$, we shall denote by f^c the image of f under the homomorphism c. Furthermore, if $f \in C[\mathbb{X}][x]$ then f^c represents the polynomial obtained by applying c to the coefficients of f. Set

$$\mathcal{L} = a_n(x)\delta^n + a_{n-1}(x)\delta^{n-1} + \cdots + a_0(x) \tag{1}$$

where $a_i(x) \in C(\mathbb{X})(x)$ and $a_n(x) \neq 0$. The order of $\mathcal{L}$, denoted by $\mathrm{ord}(\mathcal{L})$, is defined as n. For $c \in \mathbb{X}(C)$, $\mathcal{L}^c$ denotes the operator in $C(x)[\delta]$ obtained by applying c to the coefficients of $\mathcal{L}$. It is said that $\mathcal{L}^c$ is well-defined if the denominators of all coefficients of $\mathcal{L}$ do not vanish under the application of c and $a_n^c \neq 0$. The main result of this paper is the following theorem.

Theorem 1.1. *Assume that $\mathcal{L} \in C(\mathbb{X})(x)[\delta]$ and $\mathrm{ord}(\mathcal{L}) > 0$. Then there exists an ad-open subset U of $\mathbb{X}(C)$ such that for each $c \in U$, $\mathcal{L}^c$ is well-defined, and $\mathcal{L}$ is reducible over $\overline{C(\mathbb{X})}(x)$ if and only if $\mathcal{L}^c$ is reducible over $C(x)$.*

The concept of ad-open sets (see Definition 2.1) was initially introduced by Hrushovski in [8] and further explored in [4]. In particular, it has been demonstrated in [4, 8] that every ad-open subset of $\mathbb{X}(C)$ is Zariski dense in $\mathbb{X}(C)$. This concept plays important role in characterizing the set of $c \in \mathbb{X}(C)$ for which the specialization of the Galois group of $\mathcal{L}$ under c precisely matches the Galois group of $\mathcal{L}^c$. The proof of Theorem 1.1 relies on several intermediate results from [4], particularly one asserting the existence of a positive integer N and an ad-open subset U of $\mathbb{X}(C)$ such that the certificates $\delta(h)/h$ for all exponential solutions h of $\mathcal{L}^c(y) = 0$ have a degree not exceeding N for all $c \in U$. Here, the degree of a rational function is defined as the maximum of the degrees of its numerator and denominator. Theorem 1.1 and the denseness of ad-open sets imply the following corollary.

Corollary 1.2. *Assume that $\mathcal{L} \in C(\mathbb{X})(x)[\delta]$ is irreducible over $\overline{C(\mathbb{X})}(x)$. Then there exists an ad-open subset U of $\mathbb{X}(C)$ such that for any $c \in U$, $\mathcal{L}^c$ is well-defined and $\mathcal{L}^c$ is irreducible over $C(x)$*

It is worth noting that a weaker version of Corollary 1.2, which replaces ad-open sets with ad×Jac open sets, can be directly deduced from Theorem 2.60 of [4]. This relies on the fact that a linear differential operator is irreducible if and only if the (canonical) representation of its Galois group is irreducible. Compared to [4], the proof presented in this paper is more elementary and avoids the complexities of differential Galois theory. Before concluding this section, let us provide an example to illustrate the above corollary.

Example 1.3. *Consider the linear differential operator*

$$\mathcal{L} = \delta^2 + \frac{1}{x}\delta + \frac{x^2 - \alpha^2}{x^2}$$

corresponding to Bessel's differential equation, where α is a parameter. The above operator is irreducible over $\overline{\mathbb{C}(\alpha)}(x)$. From [10], for $c \in \mathbb{C}$, $\mathcal{L}^c = \delta^2 + \frac{1}{x}\delta + \frac{x^2 - c^2}{x^2}$ is irreducible over $\mathbb{C}(x)$ if and only if $c - \frac{1}{2}$ is not an integer. In particular, if $c \notin \mathbb{Q}$ then $\mathcal{L}^c$ is irreducible over $\mathbb{C}(x)$, and obviously the set $\mathbb{C} \setminus \mathbb{Q}$ is Zariski dense in $\mathbb{C}$.

The paper is organized as follows. In Section 2, we shall recall some notation and several results in [4], and deduce from these that there exists a uniform bound for the degrees of irreducible right-hand divisors of $\mathcal{L}$, and this degree bound is well-behaved under specializations. In Section 3, we shall prove Theorem 1.1.

2. Degree bound for the coefficients of irreducible divisors

In this section, leveraging results from [4], we are going to deduce that there exists a positive integer N and an ad-open subset U of $\mathbb{X}(C)$ such that for all $c \in U$, the coefficients of every irreducible right-hand divisor of $\mathcal{L}^c$ are uniformly bounded by N. Let's begin by recalling the notion of ad-open sets.

Definition 2.1. *Let Γ be a finitely generated subgroup of $(C[\mathbb{X}], +)$. The set*

$$\mathcal{B}(\Gamma, \mathbb{X}) = \{c \in \mathbb{X}(C) \mid c \text{ is injective on } \Gamma\}$$

is called a basic ad-open subset of $\mathbb{X}$. An ad-open subset of $\mathbb{X}(C)$ is defined to be an intersection of finitely many basic ad-open subsets of $\mathbb{X}(C)$. The complement of an ad-open subset is called an ad-closed subset.

Assume that U is a principal Zariski open subset of $\mathbb{X}(C)$ defined by a nonzero $p \in C[\mathbb{X}]$. Let Γ be the subgroup of $(C[\mathbb{X}], +)$ generated by p. Then $U = \mathcal{B}(\Gamma, \mathbb{X})$. Therefore, every non-empty Zariski open subset of $\mathbb{X}(C)$ is ad-open. Additionally, note that every finite dimensional $\mathbb{Q}$-vector subspace of $C[\mathbb{X}]$ is ad-closed, for instance, $\mathbb{Q}$ is an ad-closed subset of $\mathbb{C}$.

Let k be an algebraically closed field of characteristic zero, and consider $\mathcal{L} \in k(x)[\delta]$ with $\operatorname{ord}(\mathcal{L}) > 0$. Write

$$\mathcal{L} = b_n\delta^n + b_{n-1}\delta^{n-1} + \cdots + b_0, \ \ b_i \in k(x), b_n \neq 0. \tag{2}$$

Recall that for a nonzero $f = \frac{p}{q} \in k(x)$, where p and q are relatively prime polynomials in $k[x]$, the degree of f is defined as $\deg(f) = \max\{\deg(p), \deg(q)\}$. By convention, we set $\deg(0) = -\infty$. For convenience, we introduce the following definition.

Definition 2.2. *We call $\max\limits_{0\leq i\leq n-1} \left\{\deg\left(\frac{b_i}{b_n}\right)\right\}$ the degree of $\mathcal{L}$, denoted by $d(\mathcal{L})$.*

Suppose that $\mathcal{L}_1 \in k(x)[\delta]$ is an irreducible right-hand divisor of $\mathcal{L}$, meaning that $\mathcal{L} = \mathcal{L}_2\mathcal{L}_1$ for some $\mathcal{L}_2 \in k(x)[\delta]$ and $\mathcal{L}_1$ can not be factored further. Our goal is to establish a bound for $d(\mathcal{L}_1)$ and investigate its behavior under specializations. It is worth noting that a degree bound in terms of the order and bit-size of $\mathcal{L}$ has been provided in [6, 7]. To investigate the behavior of this bound under specializations, we now present an alternative degree bound for irreducible right-hand divisors.

Definition 2.3. *A positive integer N is called an exponential bound for $\mathcal{L}$ if $\deg(a) \leq N$ for any $a \in k(x)$ such that $\delta - a$ is a right-hand divisor of $\mathcal{L}$. We shall use $N(\mathcal{L})$ to denote an exponential bound for $\mathcal{L}$.*

Note that $\delta - a$ is a right-hand divisor of $\mathcal{L}$ if and only if $\mathcal{L}$ has an exponential solution h with $a = \delta(h)/h$. Therefore, if N is an exponential bound of $\mathcal{L}$ then for any exponential solution h of $\mathcal{L}$, the certificate $\delta(h)/h$ is of degree not greater than N. The following result, proved in [4], demonstrates that there is an exponential bound that remains consistent under specializations

Proposition 2.4 (Proposition 5.10 of [4]). *There exists an ad-open subset U of $\mathbb{X}(C)$ and an integer N such that N is an exponential bound for $\mathcal{L}$ and $\mathcal{L}^c$ for all $c \in U$.*

In the remainder of this section, we shall establish a bound for the degrees of all irreducible right-hand divisors of $\mathcal{L}$ in terms of an exponential bound for some exterior system of $\mathcal{L}$. To do so, we first

recall some notation from [4]. Let $\mathcal{L}$ be as in (2), and let $A_{\mathcal{L}}$ denote the companion matrix of $\mathcal{L}$, i.e.

$$A_{\mathcal{L}} = \begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & 0 & 1 \\ -\frac{b_0}{b_n} & -\frac{b_1}{b_n} & \cdots & \cdots & -\frac{b_{n-1}}{b_n} \end{pmatrix}.$$

Let T_i be a transformation matrix that transforms the matrix equation $\delta(Y) = (\wedge^i A_{\mathcal{L}})Y$ into the scalar equation $\mathcal{L}_{[i]}(y) = 0$, where $\delta(Y) = (\wedge^i A_{\mathcal{L}})Y$ denotes the ith exterior system of $\delta(Y) = A_{\mathcal{L}}Y$, see [7] for the construction. Set

$$b(\mathcal{L}) = \max_{1\le i\le n}\left\{2\binom{n}{i}\deg(T_i) + \binom{n}{i}\left(\binom{n}{i}-1\right)N(\mathcal{L}_{[i]})\right\}. \tag{3}$$

Proposition 2.5. *Suppose that $\mathcal{L}_1$ is an irreducible right-hand divisor of $\mathcal{L}$ and $\operatorname{ord}(\mathcal{L}_1) < \operatorname{ord}(\mathcal{L})$. Then $d(\mathcal{L}_1) \le n^3 b(\mathcal{L})$.*

Proof. Note that $\beta\mathcal{L}_1$ is also an irreducible right-hand divisor of $\mathcal{L}$ for any nonzero $\beta \in k(x)$ and $d(\beta\mathcal{L}_1) = d(\mathcal{L}_1)$. Therefore, after multiplying a suitable element in $k(x)$, we may assume that $\mathcal{L}_1$ is monic. Set $\nu = \operatorname{ord}(\mathcal{L}_1)$. Let R be the Picard-Vessiot ring over $k(x)$ for $\mathcal{L}(y) = 0$, and $u \in R$ be a nonzero solution of $\mathcal{L}_1(y) = 0$. As in [4], set

$$\operatorname{LinRel}(u, k(x)) = \left\{ f \in k(x)[z_1, \dots, z_n] \;\middle|\; \begin{array}{c} f \text{ is linear homogeneous, and} \\ f(u, \delta(u), \dots, \delta^{n-1}(u)) = 0 \end{array} \right\}.$$

Then $\operatorname{LinRel}(u, k(x))$ is a vector space over $k(x)$ of finite dimension. Denote $s = \dim_{k(x)}(\operatorname{LinRel}(u, k(x)))$. Then $s = n-\nu$. To see this, write $\mathcal{L}_1 = \delta^\nu + \beta_{\nu-1}\delta^{\nu-1} + \cdots + \beta_0$, where $\beta_i \in k(x)$. Since $\mathcal{L}_1$ is irreducible, $u, \delta(u), \dots, \delta^{\nu-1}(u)$ are linearly independent over $k(x)$ and $\delta^\nu(u) = -(\beta_0 u + \cdots + \beta_{\nu-1}\delta^{\nu-1}(u))$. By applying δ to the equality $\delta^\nu(u) = -(\beta_0 u + \cdots + \beta_{\nu-1}\delta^{\nu-1}(u))$ iteratively, one sees that $\delta^i(u)$ can be written as the $k(x)$-linear combination of $u, \delta(u), \dots, \delta^{\nu-1}(u)$, for all $i \ge \nu$. Hence $s = n - \nu$. Due to Lemma 5.11 of [4], the vector space $\operatorname{LinRel}(u, k(x))$ has a $k(x)$-basis consisting of elements of the form $\alpha_1 z_1 + \cdots + \alpha_n z_n$ with $\alpha_i \in k(x)$ and

$$\deg(\alpha_i) \le 2\binom{n}{s}\deg(T_s) + \binom{n}{s}\left(\binom{n}{s}-1\right)N(\mathcal{L}_{[s]}) \le b(\mathcal{L}), \tag{4}$$

where $\mathcal{L}_{[s]}$ is the scalar linear differential operator corresponding to the matrix equation $\delta(Y) = (\wedge^s A_{\mathcal{L}})Y$ and T_s is the corresponding transformation as described above.

Let $\{p_i := \alpha_{i,1}z_1 + \cdots + \alpha_{i,n}z_n \mid 1 \le i \le s\}$ be a $k(x)$-basis of $\operatorname{LinRel}(u, k(x))$ with the degree bound for $\alpha_{i,j}$ as stated in (4). One has that $q := \beta_0 z_1 + \cdots + \beta_{\nu-1}z_\nu + z_{\nu+1} \in \operatorname{LinRel}(u, k(x))$. Therefore there exist uniquely $c_1, \dots, c_s \in k(x)$ such that $q = \sum_{i=1}^s c_i p_i$. Consider the system of linear equations

$$(x_1, x_2, \dots, x_s)\underbrace{\begin{pmatrix} \alpha_{1,\nu+1} & \alpha_{1,\nu+2} & \cdots & \alpha_{1,n} \\ \alpha_{2,\nu+1} & \alpha_{2,\nu+2} & \cdots & \alpha_{2,n} \\ \vdots & \vdots & & \vdots \\ \alpha_{s,\nu+1} & \alpha_{s,\nu+2} & \cdots & \alpha_{s,n} \end{pmatrix}}_{B} = (1, 0, \dots, 0). \tag{5}$$

From $q = \sum_{i=1}^s c_i p_i$, it is evident that $(c_1, \dots, c_s)$ is a solution of (5). Suppose that $(\tilde{c}_1, \dots, \tilde{c}_s)$ with $\tilde{c}_i \in k(x)$ is another solution of (5) then $0 \ne \sum_{i=1}^s (c_i - \tilde{c}_i)p_i \in \operatorname{LinRel}(u, k(x))$ is of the form $\gamma_1 z_1 + \cdots + \gamma_{\nu-1}z_{\nu-1}$. This implies that $u, \delta(u), \dots, \delta^{\nu-1}(u)$ are linearly dependent over $k(x)$, leading to a contradiction. Consequently, $(c_1, \dots, c_s)$ is the unique solution of (5) and thus the coefficient matrix B is invertible.

Let's estimate a bound for the $\deg(c_i)$. Set D to be the least common multiple of all denominators of $\alpha_{i,j}$, and write $\alpha_{i,j} = \frac{\tilde{\alpha}_{i,j}}{D}$ with $\tilde{\alpha}_{i,j} \in k[x]$. Then neither $\deg(D)$ nor $\deg(\tilde{\alpha}_{i,j})$ is greater than $s^2 \max_{i,j}\{\deg(\alpha_{i,j})\}$. Write $\det(B) = M/D^s$, where $M \in k[x]$ and $\deg(M) \leq s^3 \max_{i,j}\{\deg(\alpha_{i,j})\}$. By Cramer's rule, one has that $c_i = \frac{\det(E_i)}{\det(B)}$, where E_i is the matrix obtained by replacing the ith row of B with $(1, 0, \ldots, 0)$. One sees that $\det(E_i) = \frac{\tilde{c}_i}{D^{s-1}}$, where $\tilde{c}_i \in k[x]$ and

$$\deg(\tilde{c}_i) \leq (s-1) \max_{i,j}\{\deg(\tilde{\alpha}_{i,j})\} \leq (s-1)s^2 \max_{i,j}\{\deg(\alpha_{i,j})\}.$$

Since each

$$\beta_i = \sum_{j=1}^{s} c_j \alpha_{j,i+1} = \sum_{j=1}^{s} \frac{D\tilde{c}_j}{M} \frac{\tilde{\alpha}_{j,i+1}}{D} = \frac{\sum_{j=1}^{s} \tilde{c}_j \tilde{\alpha}_{j,i+1}}{M}$$

and $s < n$, it follows that

$$\deg(\beta_i) \leq n^3 \max_{i,j}\{\deg(\alpha_{i,j})\} \leq n^3 b(\mathcal{L}).$$

Consequently, $d(\mathcal{L}_1) \leq n^3 b(\mathcal{L})$. □

By employing a reasoning analogous to that presented in the proof of Proposition 5.12 of [4], we demonstrate that the degree bound stated in Proposition 2.5 behaves consistently under specializations.

Proposition 2.6. *Suppose that $\mathcal{L} \in C(\mathbb{X})(x)[\delta]$ and $n = \operatorname{ord}(\mathcal{L})$. Then there exists an ad-open subset U of $\mathbb{X}(C)$ such that for any $c \in U$ and any irreducible right-hand divisor P of $\mathcal{L}^c$ with $\operatorname{ord}(P) < n$, $d(P) \leq n^3 b(\mathcal{L})$.*

Proof. Let $A_{\mathcal{L}}, T_i$ be as discussed before Proposition 2.5. Let U_1 be a non-empty Zariski open subset of $\mathbb{X}(C)$ such that for any $c \in U_1$, the following conditions hold:

(1) $(A_{\mathcal{L}})^c \in \mathrm{GL}_n(C(x))$;
(2) $(A_{\mathcal{L}})^c$ is the companion matrix of $\mathcal{L}^c$, i.e. $(A_{\mathcal{L}})^c = A_{\mathcal{L}^c}$;
(3) For all $1 \leq i \leq n$, T_i^c is invertible and is the transformation matrix that transforms $\delta(Y) = (\wedge^i A_{\mathcal{L}^c})Y$ into $(\mathcal{L}^c)_{[i]}(y) = 0$;
(4) For all $1 \leq i \leq n$, $(\mathcal{L}^c)_{[i]} = (\mathcal{L}_{[i]})^c$

For each $1 \leq i \leq n$, due to Proposition 2.4, there exists an exponential bound $N(\mathcal{L}_{[i]})$ for $\mathcal{L}_{[i]}$ and an ad-open subset V_i of $\mathbb{X}(C)$ such that for all $c \in V_i$, $N(\mathcal{L}_{[i]})$ is an exponential bound for $(\mathcal{L}_{[i]})^c$. Set $U = U_1 \cap V_1 \cap \cdots \cap V_n$. For each $c \in U$, applying Proposition 2.5 to $\mathcal{L}^c$ with $k = C$ yields that $d(P) \leq n^3 b(\mathcal{L}^c)$ for any irreducible right-hand divisor P of $\mathcal{L}^c$, where

$$b(\mathcal{L}^c) = \max_{1 \leq i \leq n} \left\{ 2\binom{n}{i} \deg(T_i^c) + \binom{n}{i} \left(\binom{n}{i} - 1 \right) N((\mathcal{L}^c)_{[i]}) \right\}.$$

For each $1 \leq i \leq n$, $\deg(T_i^c) \leq \deg(T_i)$ and $N(\mathcal{L}_{[i]})$ is an exponential bound for $(\mathcal{L}^c)_{[i]}$ for all $c \in U$ because $(\mathcal{L}^c)_{[i]} = (\mathcal{L}_{[i]})^c$ by the choice of c. Therefore, $b(\mathcal{L}^c) \leq b(\mathcal{L})$ for all $c \in U$. This concludes the proposition. □

3. Proof of Theorem 1.1

In this section, we shall prove our main result. Let's start with a lemma. Let $T = (T_1, \ldots, T_m)$ be a vector with indeterminate entries. Since we need to deal with ideals over different commutative rings, we shall use $\langle \cdot \rangle_R$ to denote the ideal in $R[T, y]$ generated by a subset of polynomials in $R[T, y]$, where R is a commutative ring and y is a new indeterminate.

Lemma 3.1. *Let $r_0(T), \ldots, r_{s-1}(T), q(T)$ be polynomials in $C[\mathbb{X}][T]$ with $q(T) \neq 0$. Then there exists a non-empty Zariski open subset U of $\mathbb{X}(C)$ such that for each $c \in U$, the following conditions hold:*

(a) $q^c(T) \neq 0$;
(b) The system

$$r_0(T) = \cdots = r_{s-1}(T) = 0, q(T) \neq 0 \tag{6}$$

has a solution in $\overline{C(\mathbb{X})}^m$ if and only if the specialized system

$$r_0^c(T) = \cdots = r_{s-1}^c(T) = 0, q^c(T) \neq 0 \tag{7}$$

has a solution in C^m.

Proof. Let y be a new indeterminate. Then the system (6) has a solution in $\overline{C(\mathbb{X})}^m$ if and only if the system

$$r_0(T) = \cdots = r_{s-1}(T) = yq(T) - 1 = 0 \tag{8}$$

has a solution in $\overline{C(\mathbb{X})}^{m+1}$. A similar statement holds for the specialized systems. Fix a term order $<$ on $T \cup \{y\}$. Let G be the reduced Gröbner basis of the ideal $\langle r_0(T), \ldots, r_{s-1}(T), yq(T) - 1\rangle_{C(\mathbb{X})}$ with respect to $<$. Let $h \in C[\mathbb{X}]$ be a nonzero element such that

$$G \cup \{r_0(T), \ldots, r_{s-1}(T), yq(T) - 1\} \subset C[\mathbb{X}]_h[T, y],$$

and G and $\{r_0(T), \ldots, r_{s-1}(T), yq(T) - 1\}$ generate the same ideal in $C[\mathbb{X}]_h[T, y]$. Set $\tilde{I} = \langle r_0(T), \ldots, r_{s-1}(T), yq(T) - 1\rangle_{C[\mathbb{X}]_h}$. We claim that G^c is the reduced Gröbner basis of $\langle \tilde{I}^c\rangle_C$ for all $c \in \mathbb{X}(C)$ with $h^c \neq 0$. Assume that $c \in \mathbb{X}(C)$ with $h^c \neq 0$ and $g_1, g_2 \in G$. Let $S(g_1, g_2)$ denote the S-polynomial of g_1, g_2. Since G is a Gröbner basis of $\langle G\rangle_{C(\mathbb{X})}$, the remainder of the division of $S(g_1, g_2)$ by G is zero. As all elements of G are monic and $G \subset C[\mathbb{X}]_h[T, y]$, it follows that $S(g_1^c, g_2^c) = S(g_1, g_2)^c$. Moreover, applying c to the division process, we see that the remainder of the division of $S(g_1^c, g_2^c)$ by G^c is also zero. Thus, G^c is a Gröbner basis of $\langle G^c\rangle_C$. Furthermore, it is straightfoward to verify that G^c is indeed the reduced Gröbner basis. The claim then follows from the fact that $\langle G^c\rangle_C = \langle \tilde{I}^c\rangle_C$.

Let U be a non-empty Zariski open subset of $\mathbb{X}(C)$ such that $h^c \neq 0$ and $q^c(T) \neq 0$ for all $c \in U$. Suppose that $c \in U$. The system (8) has a solution in $\overline{C(\mathbb{X})}^{m+1}$ if and only if $G \neq \{1\}$. On the other hand, since all elements of G are monic, $G \neq \{1\}$ if and only if $G^c \neq \{1\}$, which is equivalent to the system $r_0^c(T), \ldots, r_{s-1}^c(T), q^c(T)y - 1$ (and thus the system (7)) having a solution in C^{m+1}. □

Let k be an algebraically closed field of characteristic zero. Suppose that $\mathcal{P}, \mathcal{Q} \in k(x)[\delta]$ and $\mathcal{Q} \neq 0$. The Euclidean algorithm (see [14]) implies that there exist $\mathcal{T}, \mathcal{R} \in k(x)[\delta]$ such that $\mathcal{P} = \mathcal{T}\mathcal{Q} + \mathcal{R}$ with $\mathcal{R} = 0$ or $\mathrm{ord}(\mathcal{R}) < \mathrm{ord}(\mathcal{Q})$. The operator $\mathcal{R}$ is called a remainder of $\mathcal{P}$ with respect to $\mathcal{Q}$, denoted by $\mathrm{rem}(\mathcal{P}, \mathcal{Q})$. Furthermore, $\mathcal{Q}$ is a right-hand divisor of $\mathcal{P}$ if and only if $\mathrm{rem}(\mathcal{P}, \mathcal{Q}) = 0$. The connection between the coefficients of the remainder $\mathcal{R}$ and the coefficients of $\mathcal{P}$ is described in the following lemma. Let T be a vector with indeterminate entries. By setting $\delta(t) = 0$ for any entry t of T, $k(T)(x)$ becomes a differential field extension of $k(x)$.

Lemma 3.2. *Suppose that $\mathcal{L} \in k[T, x][\delta]$ and $\mathcal{P} \in k(T)(x)[\delta]$. Assume further that*

$$\mathcal{P} = \delta^s + \frac{p_{s-1}}{q}\delta^{s-1} + \cdots + \frac{p_0}{q}$$

where $p_i, q \in k[T][x]$. Then there exist $\mathcal{Q}, \mathcal{R} \in k(T, x)[\delta]$ of the following form:

$$\frac{r_\mu}{q^m}\delta^\mu + \cdots + \frac{r_0}{q^m}, \mu \geq 0, m \geq 0, r_i \in k[T][x] \tag{9}$$

such that $\mathcal{L} = \mathcal{Q}\mathcal{P} + \mathcal{R}$ and $\mathrm{ord}(\mathcal{R}) < s$.

Proof. We will prove the lemma by induction on $n = \mathrm{ord}(\mathcal{L})$. If $n < s$ then set $\mathcal{Q} = 0, \mathcal{R} = \mathcal{L}$, and the lemma is obvious. Now, assume that $n \geq s$ and the assertion holds for operators with orders less than n. A straightforward calculation yields that

$$a\delta^{n-s}\mathcal{P} = a\delta^n + \frac{b_{n-1}}{q^{n-s+1}}\delta^{n-1} + \cdots + \frac{b_0}{q^{n-s+1}}$$

where a is the leading coefficient of $\mathcal{L}$ and $b_i \in k[T][x]$. Hence $q^{n-s+1}(\mathcal{L} - a\delta^{n-s}\mathcal{P}) \in k[T,x][\delta]$ and its order is less than n. By the induction hypothesis, there exist $\tilde{\mathcal{Q}}, \tilde{\mathcal{R}}$ of the form (9) such that

$$q^{n-s+1}(\mathcal{L} - a\delta^{n-s}\mathcal{P}) = \tilde{\mathcal{Q}}\mathcal{P} + \tilde{\mathcal{R}}$$

and $\mathrm{ord}(\tilde{\mathcal{R}}) < s$. Then

$$\mathcal{L} = \left(a\delta^{n-s} + \frac{\tilde{\mathcal{Q}}}{q^{n-s+1}}\right)\mathcal{P} + \frac{\tilde{\mathcal{R}}}{q^{n-s+1}}.$$

So $a\delta^{n-s} + \frac{\tilde{\mathcal{Q}}}{q^{n-s+1}}$ and $\frac{\tilde{\mathcal{R}}}{q^{n-s+1}}$ are the operators as required. □

Set $\nu = n^4 b(\mathcal{L})$, and set

$$T = (t_{0,0}, t_{1,0}, \ldots, t_{s,\nu})$$

to be a vector with indeterminate entries $t_{i,j}$. Let $k = C(\mathbb{X})(T)$. By setting $\delta(t_{i,j}) = 0$ for all i, j, $k(x)$ becomes a differential extension field of $C(\mathbb{X})(x)$. Set $q = \sum_{j=0}^{\nu} t_{s,j}x^j$ and

$$\mathcal{P}(T) = \delta^s + \left(\frac{\sum_{j=0}^{\nu} t_{s-1,j}x^j}{q}\right)\delta^{s-1} + \cdots + \left(\frac{\sum_{j=0}^{\nu} t_{0,j}x^j}{q}\right). \tag{10}$$

Proposition 3.3. *Suppose that $\mathcal{L} \in C(\mathbb{X})(x)[\delta]$ is an operator with $\mathrm{ord}(\mathcal{L}) > 1$, and $0 < s < \mathrm{ord}(\mathcal{L})$. Let $\mathcal{P}(T)$ be as in (10). Then there exists a non-empty Zariski open subset V_s of $\mathbb{X}(C)$ such that for each $c \in V_s$, the following hold:*

(a) $\mathcal{L}^c$ is well-defined;

(b) $\mathcal{L}$ has a right-hand divisor of the form $\mathcal{P}(\mathbf{d})$, where $\mathbf{d} \in \overline{C(\mathbb{X})}^{(s+1)(\nu+1)}$ and $q(\mathbf{d}) \neq 0$, if and only if $\mathcal{L}^c$ has a right-hand divisor of the form $\mathcal{P}(\bar{\mathbf{d}})$, where $\bar{\mathbf{d}} \in C^{(s+1)(\nu+1)}$ and $q(\bar{\mathbf{d}}) \neq 0$.

Proof. Let a be an element in $C[\mathbb{X}][x]$ such that $a\mathcal{L} \in C[\mathbb{X}][x][\delta]$. Due to Lemma 3.2, there exist $\tilde{\mathcal{Q}}, \tilde{\mathcal{R}}$ of the form (9) such that $a\mathcal{L} = \tilde{\mathcal{Q}}\mathcal{P} + \tilde{\mathcal{R}}$ and $\mathrm{ord}(\tilde{\mathcal{R}}) < s$. Therefore, we have

$$\mathcal{L} = \left(\frac{p_{n-s}}{aq^{m_1}}\delta^{n-s} + \cdots + \frac{p_0}{aq^{m_1}}\right)\mathcal{P} + \frac{r_{s-1}}{aq^{m_2}}\delta^{s-1} + \cdots + \frac{r_0}{aq^{m_2}}, \tag{11}$$

where $p_i, r_j \in C(\mathbb{X})[T][x]$. By substituting T with $\mathbf{d} \in \overline{C(\mathbb{X})}^{(s+1)(\nu+1)}$ such that $q(\mathbf{d}) \neq 0$ in (11), we obtain

$$\mathcal{L} = \left(\frac{p_{n-s}(\mathbf{d})}{aq(\mathbf{d})^{m_1}}\delta^{n-s} + \cdots + \frac{p_0(\mathbf{d})}{aq(\mathbf{d})^{m_1}}\right)\mathcal{P}(\mathbf{d}) + \frac{r_{s-1}(\mathbf{d})}{aq(\mathbf{d})^{m_2}}\delta^{s-1} + \cdots + \frac{r_0(\mathbf{d})}{aq(\mathbf{d})^{m_2}}.$$

Let W be the set of the coefficients of $r_{s-1}, \ldots, r_0$, viewed as polynomials in x. Then $W \subset C(\mathbb{X})[T]$. For each $0 \leq j \leq \nu$, define

$$S_j = \{f(T) = 0, \forall f \in W, t_{s,j} \neq 0\}.$$

Then $\mathcal{L}$ has a right-hand divisor of the form $\mathcal{P}(\mathbf{d})$, where $\mathbf{d} \in \overline{C(\mathbb{X})}^{(s+1)(\nu+1)}$ and $q(\mathbf{d}) \neq 0$, if and only if $\mathbf{d}$ is a solution of some S_j.

By multiplying a by a suitable element in $C[\mathbb{X}]$, we can assume that $p_i, r_j \in C[\mathbb{X}][T][x]$. Each element of $\mathbb{X}(C)$ can be lifted to a C-homomorphism from $C[\mathbb{X}][T]$ to $C[T]$ by assigning $c(t_{i,j}) = t_{i,j}$ for all i, j. For the sake of simplicity, we still use c to denote the lifted homomorphism. Note that $c(\delta(f)) = \delta(c(f))$ for any $f \in C[\mathbb{X}][x]$, and $q^c = q, \mathcal{P}^c = \mathcal{P}$. For $c \in \mathbb{X}(C)$ such that $a^c \neq 0$, one has that

$$\mathcal{L}^c = \left(\frac{p^c_{n-s}}{a^c q^{m_1}}\delta^{n-s} + \cdots + \frac{p^c_0}{a^c q^{m_1}}\right)\mathcal{P} + \frac{r^c_{s-1}}{a^c q^{m_2}}\delta^{s-1} + \cdots + \frac{r^c_0}{a^c q^{m_2}}.$$

Observe that W^c is the set of coefficients of $r^c_{s-1}, \ldots, r^c_0$, viewed as polynomials in x. Using a similar argument as before, we see that for each $c \in \mathbb{X}(C)$ such that $a^c \neq 0$, $\mathcal{L}^c$ has a right-hand divisor of the form $\mathcal{P}(\bar{\mathbf{d}})$, where $\bar{\mathbf{d}} \in C^{(s+1)(\nu+1)}$ and $q(\bar{\mathbf{d}}) \neq 0$, if and only if $\bar{\mathbf{d}}$ is a solution of some S^c_j.

Set $U = \{c \in \mathbb{X}(C) \mid a^c \neq 0, \mathrm{lc}(a\mathcal{L})^c \neq 0\}$, where $\mathrm{lc}(a\mathcal{L})$ is the leading coefficient of $a\mathcal{L}$. Then for each $c \in U$, $\mathcal{L}^c$ is well-defined. Let $V_{s,j}$ be a non-empty open subset of $\mathbb{X}(C)$ such that for each $c \in V_{s,j}$, S_j has a solution in $\overline{C(\mathbb{X})}^{(s+1)(\nu+1)}$ if and only if S^c_j has a solution in $C^{(s+1)(\nu+1)}$. Such $V_{s,j}$ exists due to Lemma 3.1. Set $V_s = U \cap V_{s,0} \cap \cdots \cap V_{s,\nu}$. Then V_s satisfies the requirement. □

We are now ready to prove our main result.

Proof of Theorem 1.1. Let W be an ad-open subset of $\mathbb{X}(C)$ such that for all $c \in W$, and for all irreducible right-hand divisors $\bar{P}$ of $\mathcal{L}^c$ with $\mathrm{ord}(\bar{P}) < \mathrm{ord}(\mathcal{L}^c)$, we have $d(\bar{P}) \leq n^3 b(\mathcal{L})$. Such W exists due to Proposition 2.6. For $1 \leq s \leq n-1$, let V_s be the non-empty Zariski open subset obtained in Proposition 3.3. Set $U = W \cap V_1 \cap \cdots \cap V_{n-1}$. We claim that U is the subset we are seeking.

Suppose that $c \in U$. Assume that $\mathcal{L}$ is reducible over $\overline{C(\mathbb{X})}(x)$. Then $\mathcal{L}$ has an irreducible right-hand divisor P of order s for some $1 \leq s \leq n-1$. Without loss of generality, we may assume that P is monic. By Proposition 2.5, $d(P) \leq n^3 b(\mathcal{L})$. By taking a common denominator of the coefficients of P, each coefficient of P can be rewritten as the quotient of two polynomials in x with degrees not greater than $\nu = n^4 b(\mathcal{L})$. In other words, we may write

$$P = \delta^s + \left(\frac{\sum_{j=0}^{\nu} d_{s-1,j}x^j}{\sum_{j=0}^{\nu} d_{s,j}x^j}\right)\delta^{s-1} + \cdots + \left(\frac{\sum_{j=0}^{\nu} d_{0,j}x^j}{\sum_{j=0}^{\nu} d_{s,j}x^j}\right)$$

where $d_{i,j} \in \overline{C(\mathbb{X})}$ and not all $d_{s,0}, \ldots, d_{s,\nu}$ are zero. Set $\mathbf{d} = (d_{0,0}, d_{1,0}, \ldots, d_{s,\nu})$. Then $P = \mathcal{P}(\mathbf{d})$, meaning $\mathcal{L}$ has a right-hand divisor of the form $\mathcal{P}(\mathbf{d})$. Since $c \in V_s$, by Proposition 3.3, $\mathcal{L}^c$ has a right-hand divisor of order s. So $\mathcal{L}^c$ is reducible. Conversely, assume that $\mathcal{L}^c$ is reducible. Then $\mathcal{L}^c$ has an irreducible right-hand divisor $\bar{P}$ of order s for some $1 \leq s \leq n-1$. Since $c \in W$, we have $d(\bar{P}) \leq n^3 b(\mathcal{L})$. By a similar argument as before, $\mathcal{L}^c$ has a right-hand divisor of the form $\mathcal{P}(\bar{\mathbf{d}})$, where $\bar{\mathbf{d}} \in C^{(s+1)(\nu+1)}$ and $q(\bar{\mathbf{d}}) \neq 0$. Since $c \in V_s$, Proposition 3.3 implies that $\mathcal{L}$ has a right-hand divisor of order s. Thus $\mathcal{L}$ is reducible. This completes the proof. □

Acknowledgments

We are deeply grateful to the reviewer for the thorough reading of the manuscript and for offering many valuable suggestions, which have greatly improved the paper, particularly the main result.

Funding

This work was supported by the National Key Research and Development Project under grant No. 2020YFA0712300 and No. 2023YFA1009401, and by Postdoctoral Fellowship Program of CPSF (GZC20230750).

References

[1] Churchill, R. C., Zhang, Y. (2009). Irreducibility criteria for skew polynomials. *J. Algebra* 322(11):3797–3822.

[2] Compoint, E., Singer, M. F. (1999). Computing Galois groups of completely reducible differential equations. *J. Symbolic Comput.* 28:473–494. Differential algebra and differential equations.
[3] Compoint, E., Weil, J. A. (2004). Absolute reducibility of differential operators and Galois groups. *J. Algebra* 275(1):77–105.
[4] Feng, R., Wibmer, M. (2022). Differential galois groups, specializations and matzat's conjecture. arXiv.2209.01581.
[5] Fried, M. D., Jarden, M. (2008). *Field Arithmetic*, volume 11 of 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], 3rd ed. Berlin: Springer-Verlag. Revised by Jarden.
[6] Grigorév, D. Y. (1989). Complexity of factorization and g.c.d. calculation for linear ordinary differential operators. *Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI)*, 176:68–103, 152–153.
[7] Grigorév, D. Y. (1990). Complexity of irreducibility testing for a system of linear ordinary differential equations. In: *ISSAC 1990—Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation*, ACM, New York, pp. 225–230.
[8] Hrushovski, E. (2002). Computing the galois group of a linear differential equation. In: *Differential Galois Theory (Bedlewo, 2001)*, volume 58 of Banach Center Publ., pp. 97–138. Warsaw: Polish Acad. Sci. Inst. Math..
[9] Jacobson, N. (1996). *Finite-Dimensional Division Algebras Over Fields*. Berlin: Springer-Verlag.
[10] Kolchin, E. R. (1968). Algebraic groups and algebraic dependence. *Amer. J. Math.* 90:1151–1164.
[11] Kovacic, J. J. (1972). An Eisenstein criterion for noncommutative polynomials. *Proc. Amer. Math. Soc.* 34:25–29.
[12] Li, Z., Schwarz, F., Tsarev, S. P. (2003). Factoring systems of linear PDEs with finite-dimensional solution spaces. In: *International Symposium on Symbolic and Algebraic Computation (ISSAC'2002) (Lille)*, Vol. 36, pp. 443–471.
[13] Li, Z., Wang, H. (2011). A criterion for the similarity of length-two elements in a noncommutative PID. *J. Syst. Sci. Complex.* 24(3):580–592.
[14] Ore, O. (1933). Theory of non-commutative polynomials. *Ann. Math. (2)* 34(3):480–508.
[15] Singer, M. F. (1996). Testing reducibility of linear differential operators: a group-theoretic perspective. *Appl. Algebra Eng. Commun. Comput.* 7(2):77–104.
[16] Tsarev, S. P. (1994). Some problems that arise in the factorization of linear ordinary differential operators. *Programmirovanie* 1:45–48.
[17] van Hoeij, M. (1997). Factorization of differential operators with rational functions coefficients. *J. Symbolic Comput.* 24(5):537–561.