Picard–Vessiot extensions for linear functional systems

Manuel Bronstein[*]
[*]INRIA – Café
2004 Route des Lucioles
06902 Sophia Antipolis, France
Manuel.Bronstein@inria.fr

Ziming Li[†]
[†]Key Lab of Math.-Mechan.
Acad. of Math. and Syst. Sci.
Zhong Guan Cun, Beijing
(100080), China
zmli@mmrc.iss.ac.cn

Min Wu[*,†]
Min.Wu@inria.fr
mwu@mmrc.iss.ac.cn

ABSTRACT

Picard-Vessiot extensions for ordinary differential and difference equations are well known and are at the core of the associated Galois theories. In this paper, we construct fundamental matrices and Picard-Vessiot extensions for systems of linear partial functional equations having finite linear dimension. We then use those extensions to show that all the solutions of a factor of such a system can be completed to solutions of the original system.

Categories and Subject Descriptors

I.1.2 [**Computing Methodologies**]: Symbolic and Algebraic Manipulation—*Algorithms*

General Terms

Algorithms

Keywords

Linear functional systems; Picard-Vessiot extensions; Fundamental matrices; Modules of formal solutions.

1. INTRODUCTION

A linear functional system is a system of form $A(Z) = 0$ where A is a matrix whose entries are (partial) linear operators, such as differential, shift or q-shift operators or any mixture thereof, and Z denotes a vector of unknowns. A common special case consists of *integrable systems*, which are of the form $\{\partial_i(Z) = A_i Z\}_{1\le i\le m}$, and correspond to the matrix A given by the stacking of blocks of the form $(\partial_i - A_i)$. We show in this paper that fundamental matrices[1] and Picard-Vessiot extensions[1] always exist for linear functional systems having finite linear dimension[1], which include in particular all integrable systems. In addition, if the field of coefficients has characteristic 0 and has an algebraically closed constant field, then Picard-Vessiot extensions for such systems contain no new constants.

In this paper, rings are not necessarily commutative and have arbitrary characteristic, unless otherwise specified. Ideals and modules are left ideals and left modules. Fields are however always commutative. The notation $(\cdot)^\tau$ denotes the transpose of vectors or matrices, while $R^{p\times q}$ denotes the set of $p \times q$ matrices with entries in (the ring) R. The commutator of $a, b \in R$ is $[a, b] = ab - ba$. We write $\mathbf{1}_R$ for the identity map on R and $\mathbf{0}_R$ for the zero map on R, and we omit the subscripts when the context is clear.

2. FULLY INTEGRABLE SYSTEMS

Let σ be an endomorphism of a ring R. A σ-*derivation* ([4]) is an additive map $\delta : R \to R$ satisfying $\delta(ab) = \sigma(a)\delta(b) + \delta(a)b$ for all $a, b \in R$. A Δ-*ring* (R, Φ) is a ring R together with a set $\Phi = \{(\sigma_1, \delta_1), \ldots, (\sigma_m, \delta_m)\}$, where each σ_i is an automorphism of R, each δ_i is a σ_i-derivation of R, and $[\sigma_i, \sigma_j] = [\delta_i, \delta_j] = [\sigma_i, \delta_j] = 0$ for all $i \ne j$. If R is also a field, then (R, Φ) is called a Δ-field. An element c of R is called a *constant* if $\sigma_i(c) = c$ and $\delta_i(c) = 0$ for all i. The set of all the constants of R is denoted C_R and is clearly a subring of R, and a subfield when R is a field. Remark that a Δ-ring is a (partial) differential ring if $\sigma_i = \mathbf{1}$ for all i, and a (partial) difference ring if $\delta_i = \mathbf{0}$ for all i.

Definition 1. *We say that the Δ-ring (R, Φ) is* orthogonal *if $\delta_i = \mathbf{0}$ for each i such that $\sigma_i \ne \mathbf{1}$. By reordering the indices, we can assume that there exists an integer $\ell \ge 0$ such that $\sigma_i = \mathbf{1}$ for $1 \le i \le \ell$ and $\delta_i = \mathbf{0}$ for $\ell < i \le m$. We write (R, Φ, ℓ) for such an orthogonal Δ-ring.*

All the δ_i are usual derivations in an orthogonal Δ-ring. Mixed systems of partial linear differential, difference and q-difference equations can be represented by matrices with entries in Ore algebras ([4]) over orthogonal Δ-rings. Let (F, Φ) be a Δ-field, and suppose that for each i such that $\sigma_i \ne \mathbf{1}$, there exists $a_i \in F$ such that $\sigma_i(a_i) \ne a_i$ and $\sigma_j(a_i) - a_i = \delta_j(a_i) = 0$ for all $j \ne i$. Replacing the x_i by the a_i in the proof of Theorem 1 in [6], one sees that linear functional equations over F can be rewritten as equations over an orthogonal Δ-field. There are however orthogonal Δ-rings that do not contain such a_i's, for example $F = \mathbb{C}(x)$ together with $\Phi = \{(\mathbf{1}, d/dx), (\sigma_x, \mathbf{0})\}$ where σ_x is the automorphism of F over $\mathbb{C}$ that sends x to $x - 1$. This field is used in modeling differential-delay equations, and does not match the definition of orthogonality given in [6].

[1]To be defined precisely in Sect. 3 and 5.

Let (F, Φ, ℓ) be an orthogonal Δ-field. We say that a commutative ring E containing F is an *orthogonal* Δ*-extension* of (F, Φ, ℓ) if the σ_i and δ_i can be extended to automorphisms and derivations of E satisfying: (i) the commutators $[\sigma_i, \sigma_j] = [\delta_i, \delta_j] = [\sigma_i, \delta_j] = 0$ on E for $1 \leq i \neq j \leq m$; (ii) $\sigma_i = \mathbf{1}_E$ for $i \leq \ell$ and $\delta_i = \mathbf{0}_E$ for $j > \ell$.

Let E and $\tilde{E}$ be two orthogonal Δ-extensions of F. A map ϕ from E to $\tilde{E}$ is called a Δ*-morphism* if ϕ is a ring homomorphism leaving F fixed and commuting with all the δ_i and σ_i. Two orthogonal Δ-extensions of F are said to be *isomorphic* if there exists a bijective Δ-morphism between them.

DEFINITION 2. *A system of form*

$$\delta_i(Z) = A_i Z \text{ for } i \leq \ell, \quad \sigma_i(Z) = A_i Z \text{ for } i > \ell\,, \qquad (1)$$

where $A_i \in F^{n\times n}$ and $Z = (z_1, \ldots, z_n)^\tau$ is called an integrable *system if the following conditions are satisfied:*

$$\sigma_i(A_j)A_i + \delta_i(A_j) = \sigma_j(A_i)A_j + \delta_j(A_i) \quad \text{for all } i, j. \quad (2)$$

The integrable system (1) is said to be fully integrable *if the matrices $A_{\ell+1}, \ldots, A_m$ are invertible.*

Using Ore algebra notation, we write $\{\partial_i(Z) = A_i Z\}_{1\leq i\leq m}$ for the system (1) where the action of ∂_i is meant to be δ_i for $i \leq \ell$ and σ_i for $i > \ell$. Note that the conditions (2) are derived from the condition $\partial_i(\partial_j(Z)) = \partial_j(\partial_i(Z))$ and are exactly the matrix-analogues of the compatibility conditions for first order scalar equations in [6].

EXAMPLE 1. *Let $F = \mathbb{C}(x, k)$ and δ_x and σ_k denote respectively the ordinary differentiation w.r.t. x and the shift operator w.r.t. k. Then $\{\delta_x(Z){=}A_x Z, \sigma_k(Z){=}A_k Z\}$ where*

$$A_x = \begin{pmatrix} \frac{x^2-kx-k}{x(x-k)(x-1)} & \frac{x^2-kx+3k-2x}{kx(x-k)(x-1)} \\ \frac{k(kx+x-x^2-2k)}{(x-k)(x-1)} & \frac{x^3+x^2-kx^2-2x+2k}{x(x-k)(x-1)} \end{pmatrix}$$

$$A_k = \begin{pmatrix} \frac{k+1+kx^2-xk^2-x}{(x-k)(x-1)} & -\frac{k+1+kx-k^2-x}{k(x-k)(x-1)} \\ \frac{x(k+1)(k+1+kx-k^2-x)}{(x-k)(x-1)} & \frac{(k+1)(x^2-2kx-x+k^2)}{k(x-k)(x-1)} \end{pmatrix}$$

is a fully integrable system.

3. FUNDAMENTAL MATRICES AND PICARD-VESSIOT EXTENSIONS

A square matrix with entries in a commutative ring is said to be *invertible* if its determinant is a unit in that ring. Let the orthogonal Δ-ring (F, Φ, ℓ) be as in the previous section and $\{\partial_i(Z) = A_i Z\}_{1\leq i\leq m}$ be a fully integrable system of size n over F. An $n \times n$ matrix U with entries in an orthogonal Δ-extension E of F is a *fundamental matrix* for $\{\partial_i(Z) = A_i Z\}_{1\leq i\leq m}$ if U is invertible and $\partial_i(U) = A_i U$ for each i, that is, each column of U is a solution of the system.

THEOREM 1. *For every fully integrable system, there exists a fundamental matrix whose entries lie in an orthogonal Δ-extension of F.*

Proof. Let $\{\partial_i(Z) = A_i Z\}_{1\leq i\leq m}$ be a fully integrable system of size n over F, $U = (u_{st})$ be a matrix of n^2 distinct indeterminates and $R = F[u_{11}, \ldots, u_{1n}, \ldots, u_{n1}, \ldots, u_{nn}]$. For $1 \leq i \leq \ell$, the δ_i are extended to derivations of R via $\delta_i(U) = A_i U$ and for $\ell + 1 \leq j \leq m$, the σ_j are extended to automorphisms of R via $\sigma_j(U) = A_j U$ (σ_j is bijective because A_j is invertible). It follows from the conditions (2) that these extended maps turn R into a well-defined orthogonal Δ-extension of F and that $\partial_i(U) = A_i U$ for each i. Let $D = \det(U)$ and $\overline{R}$ be the localization of R with respect to D. Extend the δ_i and σ_j via the formulas $\delta_i(1/D) = -\delta_i(D)/D^2$ and $\sigma_j(1/D) = 1/\sigma_j(D)$, respectively (note that $\sigma_j(D) = \det(A_j)D$ for $j > \ell$). Then $\overline{R}$ becomes an orthogonal Δ-extension of F, and U is a fundamental matrix of the system. $\square$

The following proposition reveals that any two fundamental matrices differ by a constant matrix.

PROPOSITION 1. *Let $\{\partial_i(Z) = A_i Z\}_{1\leq i\leq m}$ be a fully integrable system of size n over F and $U \in E^{n\times n}$ be a fundamental matrix where E is an orthogonal Δ-extension of F. If $V \in E^{n\times d}$ with $d \geq 1$ is a matrix whose columns are solutions of the system then $V = UT$ for some $T \in C_E^{n\times d}$. In particular, any solution of $\{\partial_i(Z) = A_i Z\}_{1\leq i\leq m}$ in E^n is a linear combination of the columns of U over C_E.*

Proof. Let $T = U^{-1}V$. A straightforward calculation implies that $\delta_i(T) = 0$ for $i \leq \ell$, and $\sigma_j(T) = T$ for $j > \ell$. Hence all the entries of T belong to C_E. $\square$

In [10, 11], Picard-Vessiot rings for linear ordinary differential and difference systems are defined. Picard-Vessiot fields for integrable systems of partial differential equations have been studied by Kolchin who proved their existence and developed the associated Galois theory [2, §2][5]. Picard-Vessiot extension fields have also been defined in [1] for fields with operators, which are more general Δ-fields where the operators do not necessarily commute. While the associated Galois theory was developed there, the existence of Picard-Vessiot extensions was not shown. Indeed, with automorphisms allowed, there are fully integrable systems for which no Picard-Vessiot field exists. Generalizing the definition of Picard-Vessiot rings used for difference equations [10, (Errata)], we obtain Picard-Vessiot rings together with a construction proving their existence. Our definition is compatible with the previous ones: for differential systems, Picard-Vessiot rings turn out to be integral domains, and the Picard-Vessiot fields of [5] are their fields of fractions; For Δ-rings, the Picard-Vessiot rings are generated by elements satisfying linear scalar operator equations, which is the defining property of the Picard-Vessiot fields of [1].
An ideal I of a commutative Δ-ring R is said to be *invariant* if $\delta_i(I) \subset I$ and $\sigma_i(I) \subset I$ for all $1 \leq i \leq m$. The ring R is said to be *simple* if its only invariant ideals are (0) and R.

DEFINITION 3. *Let $\{\partial_i(Z) = A_i Z\}_{1\leq i\leq m}$ be a fully integrable system over F. A* Picard-Vessiot ring *for this system is a (commutative) ring E such that:*

(i) *E is a simple orthogonal Δ-extension of F.*

(ii) *$E = F[U, \det(U)^{-1}]$ for some fundamental matrix U for the system.*

We now construct Picard-Vessiot rings by the same approach used in the ordinary differential and difference cases [10, 11].

LEMMA 1. *Let R be an orthogonal Δ-extension of F and I a maximal invariant ideal in R. Then, (i) $E := R/I$ is a simple orthogonal Δ-extension of F. (ii) C_E is a field. (iii) If F has characteristic 0, C_F is algebraically closed and E is a finitely generated algebra over F, then $C_E = C_F$.*

Proof. Let $\overline{I} = \{\sigma_{\ell+1}^{k_{\ell+1}} \cdots \sigma_m^{k_m}(a) | \, a \in I, k_{\ell+1}, \ldots, k_m \in \mathbb{Z}\}$. One can verify that $\overline{I}$ is an invariant ideal containing I but $1 \notin \overline{I}$, and hence $I = \overline{I}$ since I is maximal. The δ_i and σ_j can be viewed as derivations and surjective endomorphisms on $E = R/I$ via the formulas $\delta_i(a+I) = \delta_i(a) + I$ and $\sigma_j(a+I) = \sigma_j(a) + I$ for all a in R, respectively. If $\sigma_j(a+I) = I$ then $\sigma_j(a) \in I = \overline{I}$ and thus $a \in I$. So the σ_j are automorphisms of E and E is a simple orthogonal Δ-extension of F. To show the second statement, let c be a nonzero constant of E. Then the ideal (c) is invariant. Since E is simple, (c) contains 1. To show the last statement, suppose that $b \in C_E$ but $b \notin C_F$. By the argument used in the proof of Lemma 1.8 in [10], there exists a nonzero monic polynomial g over F with minimal degree d such that $g(b) = \left(b^d + \sum_{k=0}^{d-1} g_k b^k\right) = 0$. Apply the δ_i and σ_j to $g(b)$, respectively, we obtain $\left(\sum_{k=0}^{d-1} \delta_i(g_k) b^k\right) = 0$ for $i \le \ell$, and $\left(\sum_{k=0}^{d-1} (\sigma_j(g_k) - g_k) b^k\right) = 0$ for $j > \ell$. The minimality of d then implies $g_k \in C_F$ for $0 \le k < d$. So $b \in C_F$ since C_F is algebraically closed, a contradiction. □

The existence of the Picard-Vessiot extensions is stated in the next theorem.

THEOREM 2. *Every fully integrable system over F has a Picard-Vessiot ring E. If F has characteristic 0 and C_F is algebraically closed, then $C_E = C_F$. Furthermore, that extension is minimal, meaning that no proper subring of E satisfies condition (ii) of Definition 3.*

Proof. Let $\{\partial_i(Z) = A_i Z\}_{1 \le i \le m}$ be a fully integrable system over F. By Theorem 1, it has a fundamental matrix $U = (u_{st})$ with entries in the orthogonal Δ-extension

$$R = F[u_{11}, \ldots, u_{nn}, \det(U)^{-1}].$$

Let I be a maximal invariant ideal of R and $E = R/I$. Then E is a simple orthogonal Δ-extension of F by Lemma 1. Clearly, E is generated over F by the entries of the matrix $\overline{U} := (u_{st} + I)$ and by $\det(\overline{U})^{-1}$. Since $\overline{U}$ is a fundamental matrix for the system, E is a Picard-Vessiot ring for the system. Assume further that F has characteristic 0 and C_F is algebraically closed. Then $C_E = C_F$ by the third assertion of Lemma 1. Let $S = F[V, \det(V)^{-1}]$ be a subring of E where V is some fundamental matrix of the system. By Proposition 1, there exists $T \in C_E^{n \times n}$ such that $V = UT$. Since $C_E = C_F$, all the entries of U and the inverse of $\det(U)$ are contained in S. Hence $S = E$. □

Assume that the ground field F has characteristic 0 with an algebraically closed field of constants. Let E be a Picard-Vessiot ring for a fully integrable system of size n over F. Then Proposition 1 together with $C_E = C_F$ implies that all the solutions of this system in E^n form a C_F-vector space of dimension n. A direct generalization of Proposition 1.20 in [11] and Proposition 1.9 in [10] reveals that any two Picard-Vessiot rings for a fully integrable system over F are isomorphic as orthogonal Δ-extensions.

We present a few examples for Picard-Vessiot rings. Consider the fully integrable system of size one:

$$\partial_i(z) = a_i z \quad \text{where } a_i \in F \text{ and } i = 1, \ldots, m. \tag{3}$$

Let E be the orthogonal Δ-extension $F[T, T^{-1}]$ such that $\delta_i(T) = a_i T$ for $i \le \ell$ and $\sigma_j(T) = a_j T$ for $j > \ell$.
Case 1. There does not exist an integer $k > 0$ and $r \in F^*$ such that $\delta_i(r) = k a_i r$ for $i \le \ell$ and $\sigma_j(r) = a_j^k r$ for $j > \ell$. Then E is a Picard-Vessiot ring of (3).
Case 2. Assume that the integer $k > 0$ is minimal so that $\delta_i(r) = k a_i r$ and $\sigma_j(r) = a_j^k r$ for some $r \in F^*$ and for all $i \le \ell$ and $j > \ell$. Then $E/\left(T^k - r\right)$ is a Picard-Vessiot ring of (3). The verification of the above two assertions is similar to that in Example 1.19 in [11].
Unlike in the differential case, the elements of Picard-Vessiot rings cannot always be interpreted as complex functions: the system $\{dy/dx = y(x), y(x+1) = y(x)\}$ is in Case 1 above and has a Picard-Vessiot ring over $\mathbb{C}(x)$, but has no nonzero complex function solution.

Next, we show that a Picard-Vessiot ring of the system in Example 1 is $F[e^x, e^{-x}, \Gamma(k), \Gamma(k)^{-1}]$ where $F = \mathbb{C}(x, k)$. Note that the change of variable[1] $Z = MY$, where

$$M = \begin{pmatrix} \frac{x-k}{x} & x^2 \\ (x-k)k & x^2 k \end{pmatrix},$$

transforms the system into $\mathcal{B} : \{\delta_x(Y) = B_x Y, \sigma_k(Y) = B_k Y\}$,

$$\text{where} \quad B_x = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad B_k = \begin{pmatrix} 1 & 0 \\ 0 & k \end{pmatrix}.$$

Thus we need only to find a Picard-Vessiot ring of $\mathcal{B}$. First, let U be a 2×2 matrix with indeterminate entries u_{11}, u_{12}, u_{21} and u_{22}. Define $\delta_x(U) = B_x U$ and $\sigma_k(U) = B_k U$. This turns $R = F[u_{11}, u_{12}, u_{21}, u_{22}, 1/\det(U)]$ into an orthogonal Δ-extension of F. Clearly, $I = (u_{12}, u_{21})$ is an invariant ideal of R and $\sigma_k^{-1}(I)$ is contained in I. Hence R/I is an orthogonal Δ-ring. As the Δ-rings $E = F[u_{11}, u_{22}, u_{11}^{-1}, u_{22}^{-1}]$ and R/I are isomorphic, it suffices to show that E is simple. Suppose that J is a nontrivial invariant ideal of E. Let f be a nonzero polynomial in $I \cap F[u_{11}, u_{22}]$ with the smallest number of terms. It cannot be a monomial, for otherwise J would be E since u_{11}^{-1} and u_{22}^{-1} are in E. We write

$$f = u_{11}^{d_1} u_{22}^{d_2} + r u_{11}^{e_1} u_{22}^{e_2} + \text{other terms},$$

where $r \in F$ with $r \neq 0$, and $(d_1, d_2) \neq (e_1, e_2)$. It follows from $\delta_x(u_{11}) = u_{11}$ and $\delta_x(u_{22}) = 0$ that

$$\delta_x(f) = d_1 u_{11}^{d_1} u_{22}^{d_2} + (\delta_x(r) + e_1 r) u_{11}^{e_1} u_{22}^{e_2} + \text{other terms},$$

in which each monomial has already appeared in f. Thus $(\delta_x(f) - d_1 f)$ must be zero, because it is in I but has fewer terms. It follows that $(\delta_x(r) - (d_1 - e_1) r)$ is equal to zero. In the same way, one can show that $\left(\sigma_k(r) - k^{d_2 - e_2} r\right) = 0$, because $\sigma_k(u_{11}) = u_{11}$ and $\sigma_k(u_{22}) = k u_{22}$. But the existence

[1] which can be found, for example, by computing the hyperexponential solutions of the system ([6, 12])

of such a rational function r would imply $d_1{=}e_1$ and $d_2{=}e_2$, a contradiction. Thus E is simple, and so a Picard-Vessiot ring of $\mathcal{B}$, hence also of the system in Example 1. If we understand u_{11} as e^x and u_{22} as $\Gamma(k)$, then $V = \begin{pmatrix} e^x & 0 \\ 0 & \Gamma(k) \end{pmatrix}$ is a fundamental matrix for $\mathcal{B}$ in E, and hence MV is for the system in Example 1.

Last, we describe a simple orthogonal Δ-extension that contains a solution of the inhomogeneous system

$$\delta_i(z) = a_i \text{ for } i \le \ell \quad \text{and} \quad \sigma_j(z) = z + a_j \text{ for } j > \ell, \tag{4}$$

where the a_i and a_j are in a simple orthogonal Δ-*ring* E with characteristic zero. This is an extension of Example 1.18 in [11]. Note that the a_i and a_j have to satisfy some compatibility conditions due to the commutativity of the δ_i and σ_j. A more general form for these conditions are given in (8) in the next section.
If (4) has a solution in E, then there is nothing to do. Otherwise, Let $R = E[T]$ and extend the δ_i and σ_j on R by the formulas $\delta_i(T) = a_i$ and $\sigma_j(T) = T + a_j$. The compatibility conditions imply that R becomes a well-defined orthogonal Δ-ring. If R has a nontrivial invariant ideal I, let $f = f_d T^d + f_{d-1} T^{d-1} + \cdots + f_0$ be a nonzero element in I with minimal degree. Let J be the set consisting of zero and leading coefficients of elements in I with degree d. Our extensions of δ_i and σ_j imply that J is an invariant ideal of E. Hence $1 \in J$ and, therefore, we may also assume $d > 0$ and $f_d = 1$. Since d is minimal, both $\delta_i(f)$ and $(\sigma_j(f) - f)$ are 0. Consequently, $\frac{-f_{d-1}}{d}$ is a solution of (4), a contradiction. Thus R is simple and contains a solution T of (4).

4. COMPLETING PARTIAL SOLUTIONS

We now consider *reducible* systems, *i.e.* systems that can be put into simultaneous block-triangular form by a change of variable $Y = MZ$ for some $M \in \mathrm{GL}_n(F)$. Factorization algorithms for modules over Laurent–Ore algebras [12] yield such a change of variable for reducible systems, and we motivate them by showing that the solutions of a factor can always be extended to solutions of the complete system.

THEOREM 3. *Let $\mathcal{A}$: $\{\partial_i(Z) = A_i Z\}_{1 \le i \le m}$ be a fully integrable system of size n over F, and suppose that there exist a positive integer $d < n$ and matrices B_i in $F^{d\times d}$, C_i in $F^{(n-d)\times d}$ and D_i in $F^{(n-d)\times(n-d)}$ such that*

$$A_i = \begin{pmatrix} B_i & 0 \\ C_i & D_i \end{pmatrix} \quad \text{for } 1 \le i \le m\,. \tag{5}$$

Then

- **(i)** $\mathcal{B} : \{\partial_i(X){=}B_i X\}_{1\le i\le m}$ *and* $\mathcal{D} : \{\partial_i(X){=}D_i X\}_{1\le i\le m}$ *are both fully integrable systems.*
- **(ii)** $(0, \ldots, 0, \zeta_{d+1}, \ldots, \zeta_n)^\tau$ *is a solution of* $\mathcal{A}$ *whenever* $(\zeta_{d+1}, \ldots, \zeta_n)^\tau$ *is a solution of* $\mathcal{D}$.
- **(iii)** *For any solution $(\eta_1, \ldots, \eta_d)^\tau$ of $\mathcal{B}$ in an orthogonal Δ-extension of F, there exists an orthogonal Δ-extension of F containing $\eta_1, \ldots, \eta_d$ as well as $\eta_{d+1}, \ldots, \eta_n$ such that $(\eta_1, \ldots, \eta_n)^\tau$ is a solution of $\mathcal{A}$.*

Proof. Let $X = (z_1, \ldots, z_d)^\tau$ and $Y = (z_{d+1}, \ldots, z_n)^\tau$. The system $\mathcal{A}$ can then be rewritten into a homogeneous system and an inhomogeneous system:

$$\left\{ \begin{array}{lcl} \partial_i(X) &=& B_i X, \\ \partial_i(Y) &=& D_i Y + C_i X, \end{array} \right. \qquad \text{for } 1 \le i \le m\,. \tag{6}$$

Since $\mathcal{A}$ is fully integrable, the matrices A_i satisfy (2) and A_j is invertible for $j > \ell$. Hence, the B_j and D_j for $j > \ell$ must also be invertible since $\det(A_j) = \det(B_j)\det(D_j)$. In addition, a routine calculation shows that for all i, j,

$$\sigma_i(A_j)A_i + \delta_i(A_j) =$$

$$\begin{pmatrix} \sigma_i(B_j)B_i + \delta_i(B_j) & 0 \\ \sigma_i(C_j)B_i + \sigma_i(D_j)C_i + \delta_i(C_j) & \sigma_i(D_j)D_i + \delta_i(D_j) \end{pmatrix}, \tag{7}$$

which implies that the B_i and D_i also satisfy the compatibility conditions (2). Therefore $\mathcal{B}$ and $\mathcal{D}$ are both fully integrable. The first statement is proved. The second is immediate from (6).
From Theorem 1, there exist an orthogonal Δ-extension E of F and a fundamental matrix U with entries in E for $\mathcal{D}$. Let $\eta = (\eta_1, \ldots, \eta_d)^\tau$ be a solution of $\mathcal{B}$ in some orthogonal Δ-extension R of F. Viewing E and R as commutative F-algebras, we can extend the δ_i and σ_j to the commutative E-algebra $E \otimes_F R$ via $\delta_i(e \otimes r) = \delta_i(e) \otimes r + e \otimes \delta_i(r)$ and $\sigma_j(e \otimes r) = \sigma_j(e) \otimes \sigma_j(r)$ for $i \le \ell$ and $j > \ell$. Then $(1 \otimes \eta_1, \ldots, 1 \otimes \eta_d)^\tau$ is also a solution of $\mathcal{B}$, so, replacing R by $E \otimes_F R$, we can assume without loss of generality that R contains E. Substitute η into (6) to get $\partial_i(Y) = D_i Y + C_i \eta$ for each i. Let $v = (v_1, \ldots, v_{n-d})^\tau$, where the v_k are distinct indeterminates over R, and $G = R[v_1, \ldots, v_{n-d}]$. We extend the δ_i and σ_j to G via $\delta_i(v){=}b_i$ and $\sigma_j(v){=}v + b_j$ where $b_1, \ldots, b_m \in R^{n-d}$ are given by $b_i = U^{-1} C_i \eta$ for $i \le \ell$ and $b_j = U^{-1} {D_j}^{-1} C_j \eta$ for $j > \ell$.
To turn G into an orthogonal Δ-extension of R, all the δ_i and σ_j on G should commute, which is equivalent to the following integrability conditions:

$$\left\{ \begin{array}{ll} \delta_i(b_j) = \delta_j(b_i), & \text{for } \ 1 \le i, j \le \ell, \\ \delta_i(b_j) = \sigma_j(b_i) - b_i, & \text{for } \ i \le \ell,\ j > \ell, \\ \sigma_i(b_j) - b_j = \sigma_j(b_i) - b_i, & \text{for } \ \ell + 1 \le i, j \le m. \end{array} \right. \tag{8}$$

Although the conditions (8) are generally not satisfied for arbitrary b_i's, we show that they are satisfied in our case. Since the A_i satisfy the compatibility conditions (2), it follows from the bottom-left block in (7) that, for all i, j,

$$\sigma_i(C_j)B_i{+}\sigma_i(D_j)C_i{+}\delta_i(C_j){=}\sigma_j(C_i)B_j{+}\sigma_j(D_i)C_j{+}\delta_j(C_i). \tag{9}$$

For $1 \le i,\ j \le \ell$, we have

$$\begin{array}{rcl} \delta_i(b_j) &=& \delta_i\left(U^{-1} C_j \eta\right) \\ &=& -U^{-1}\delta_i(U)U^{-1}C_j\eta + U^{-1}\delta_i(C_j)\eta + U^{-1}C_j\delta_i(\eta) \\ &=& -U^{-1}\left(D_i C_j - \delta_i(C_j) - C_j B_i\right)\eta\,, \end{array}$$

which, together with $\sigma_i = \sigma_j = \mathbf{1}$ for $1 \le i,\ j \le \ell$, and (9) implies $\delta_i(b_j) = \delta_j(b_i)$. The last two integrability conditions in (8) are verified with similar calculations, using the fact that the D_i satisfy the compatibility conditions (2). Therefore G is an orthogonal Δ-extension of R, hence of F. Let $\zeta = Uv \in G^{n-d}$. Then, for $i \le \ell$,

$$\partial_i(\zeta) = \delta_i(\zeta) = \delta_i(U)v + U\delta_i(v) = D_i U v + U b_i = D_i \zeta + C_i \eta,$$

and, for $j > \ell$,

$$\partial_j(\zeta) = \sigma_j(\zeta) = \sigma_j(U)\sigma_j(v) = D_j U(v + b_j) = D_j\zeta + C_j\eta.$$

So $(\eta^\tau, \zeta^\tau)^\tau$ is a solution of the initial system $\mathcal{A}$. □

We point out here (but omitting the detailed explanation) that in the differential case, the quotient systems of [7] yield an alternative approach to completing solutions of factors.

EXAMPLE 2. *Let F, δ_x and σ_k be as in Example 1, and consider the fully integrable system*

$$\left\{\delta_x(Z) = \begin{pmatrix} B_x & 0 \\ C_x & D_x \end{pmatrix} Z,\ \sigma_k(Z) = \begin{pmatrix} B_k & 0 \\ C_k & D_k \end{pmatrix} Z\right\} \tag{10}$$

where $Z = (z_1, z_2, z_3)^\tau$, $B_x = \frac{x+k}{x}$, $B_k = \frac{(k+1)x}{k}$,

$$C_x = \begin{pmatrix} \frac{2x^2-k^2+2x-kx}{x(x-k)} \\ \frac{x^3-x^2k+2x^2-kx+2x-k^2}{(x-k)x} \end{pmatrix},$$

$$C_k = \begin{pmatrix} \frac{(k+1)(x^3-2x^2k-3x^2+k^2x+4kx+x-k^2)}{k(x-k-1)^2} \\ \frac{x^2(k+1)}{k} - \frac{(k+1)(x-k)^2}{k(x-k-1)^2} - xk(x-1) \end{pmatrix},$$

and

$$D_x = \begin{pmatrix} \frac{-2-x+k}{x-k} & 0 \\ \frac{-2x-x^2+k^2}{(x-k)x} & \frac{k}{x} \end{pmatrix},\quad D_k = \begin{pmatrix} \frac{(k+1)(x-k)^2}{k(x-k-1)^2} & 0 \\ \frac{(k+1)(x-k)^2}{k(x-k-1)^2} - kx & xk \end{pmatrix}.$$

We complete the solution $\eta_1 = ke^x x^k$ of the system given by B_x and B_k to a solution of (10). Note that

$$U = \begin{pmatrix} 0 & \frac{ke^{-x}}{(x-k)^2} \\ \Gamma(k)x^k & \frac{ke^{-x}}{(x-k)^2} \end{pmatrix}$$

is a fundamental matrix for the system given by D_x and D_k. By the proof of Theorem 3, we let

$$b_1 = \begin{pmatrix} \frac{kx}{\Gamma(k)} e^x \\ (x-k)(2x^2 - k^2 + 2x - kx)\, x^{k-1} e^{2x} \end{pmatrix},$$

$$b_2 = \begin{pmatrix} \frac{x+kx+k^2-xk^2-k-1}{\Gamma(k+1)} e^x \\ (x^3 - 2kx^2 - 3x^2 + k^2x + 4kx + x - k^2)x^k e^{2x} \end{pmatrix}.$$

We find that

$$v = \begin{pmatrix} \frac{\Gamma(k) - ke^x + xke^x}{\Gamma(k)} \\ x^{k+2}e^{2x} - 2x^{k+1}ke^{2x} + x^k k^2 e^{2x} + 1 \end{pmatrix}$$

satisfies $\delta_x(v) = b_1$ and $\sigma_k(v) - v = b_2$. Therefore,

$$\begin{pmatrix} \eta_1 \\ U^{-1}v \end{pmatrix} = \begin{pmatrix} ke^x x^k \\ ke^x x^k + \frac{ke^{-x}}{(x-k)^2} \\ x^{k+1}ke^x + \frac{ke^{-x}}{(x-k)^2} + \Gamma(k)x^k \end{pmatrix}$$

is a solution of (10).

Theorem 3 also yields fundamental matrices for reducible systems. Let $\{\partial_i(Z) = A_i Z\}_{1\le i\le m}$ be a fully integrable system where the A_i are as in (5). Suppose that $U = (u_{ij}) \in R^{d\times d}$ and $V \in E^{(n-d)\times(n-d)}$ are fundamental matrices for the systems $\{\partial_i(X)=B_i X\}_{1\le i\le m}$ and $\{\partial_i(X)=D_i X\}_{1\le i\le m}$ respectively, where R and E are orthogonal Δ-extensions of F. As in the procedure of completing solutions, we can assume without loss of generality that R contains E. Then a fundamental matrix for the initial system can be constructed as follows: for each $1 \le i \le d$, following the procedure of completing solutions, we can find an orthogonal Δ-extension G_i of R and $\xi_i \in G_i^{n-d}$ such that $(u_{1i}, \ldots, u_{di}, \xi_i^\tau)^\tau \in G_i^n$ is a solution of $\{\partial_i(Z) = A_i Z\}_{1\le i\le m}$. Viewing all the entries of U, V and the ξ_i as elements of $G = G_1 \otimes_F \cdots \otimes_F G_d$, $W = \begin{pmatrix} U & 0 \\ \xi_1\ \ldots\ \xi_d & V \end{pmatrix} \in G^{n\times n}$ is easily seen to be a fundamental matrix for $\{\partial_i(Z) = A_i Z\}_{1\le i\le m}$ (it is invertible because $\det(W) = \det(U)\det(V)$).

5. MODULES AND PICARD-VESSIOT RINGS FOR GENERAL LINEAR FUNCTIONAL SYSTEMS

We now generalize the previous notions and results to systems of the form $A(Z) = 0$ where A is a matrix of linear operators. As in previous sections, let (F, Φ, ℓ) be an orthogonal Δ-field and $S = F[\partial_1; \sigma_1, \delta_1] \cdots [\partial_m; \sigma_m, \delta_m]$ be the corresponding Ore algebra [4]. In the differential case, an S-module is classically associated to such a system [8, 11]. In the difference case, however, S-modules do not have appropriate dimensions, so modules over Laurent algebras are used instead [9, 10, 13]. It is therefore natural to introduce in our setting the following extension of S: let $\theta_{\ell+1}, \ldots, \theta_m$ be indeterminates independent of the ∂_i. Since the σ_j^{-1} are also automorphisms of F, $\overline{S} = S[\theta_{\ell+1}; \sigma_{\ell+1}^{-1}, \mathbf{0}] \cdots [\theta_m; \sigma_m^{-1}, \mathbf{0}]$ is also an Ore algebra. Since $(\partial_j\theta_j)a = \partial_j\sigma_j^{-1}(a)\theta_j = a\partial_j\theta_j$ for any $j > \ell$ and any $a \in F$, $\partial_j\theta_j$ is in the center of $\overline{S}$. Therefore the left ideal $I = \sum_{j=\ell+1}^m \overline{S}(\partial_j\theta_j - 1)$ is a two-sided ideal of $\overline{S}$, and we call the factor ring $R=\overline{S}/I$ the *Laurent-Ore algebra generated by Φ over F*. Writing ∂_j^{-1} for the image of θ_j in R, we can also write R (by convention) as

$$\begin{aligned} R \ :=\ & F[\partial_1; \mathbf{1}, \delta_1] \cdots [\partial_\ell; \mathbf{1}, \delta_\ell] \\ & [\partial_{\ell+1}, \partial_{\ell+1}^{-1}; \sigma_{\ell+1}, \mathbf{0}] \cdots [\partial_m, \partial_m^{-1}; \sigma_m, \mathbf{0}] \end{aligned}$$

and view it as an extension of S. For linear ordinary difference equations, $R = F[\sigma, \sigma^{-1}]$, is the algebra used in [10]. For linear partial difference equations with constant coefficients, R is the Laurent polynomial ring used in [9, 13]. Laurent-Ore algebras allow us to construct fundamental matrices and Picard-Vessiot extensions for linear functional systems of finite linear dimension, a concept that we now define precisely.

For our purposes, a linear functional system is a matrix $A = (a_{ij}) \in S^{p\times q} \subset R^{p\times q}$. For any R-module N, we can associate to A a C_F-linear map $\lambda : N^q \to N^p$ given by

$$\xi := \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_q \end{pmatrix} \mapsto A\xi = \begin{pmatrix} \sum_{j=1}^q a_{1j}\xi_j \\ \vdots \\ \sum_{j=1}^q a_{pj}\xi_j \end{pmatrix}.$$

We therefore say that $\xi \in N^q$ is a *solution "in N"* of the system $A(Z) = 0$ if $A(\xi) = 0$, and write $\mathrm{sol}_N(A(Z) = 0)$ for all its solutions in N. Clearly, $\mathrm{sol}_N(A(Z) = 0)$ is a vector space over C_F.

As in the case of $\mathcal{D}$-modules [8], we can associate to A an R-module as follows: the matrix $A \in R^{p\times q}$ induces the R-linear map $\rho : R^{1\times p} \to R^{1\times q}$ given by $\rho(r_1,\ldots,r_p) = (r_1,\ldots,r_p)A$. Let $M = \operatorname{coker}(\rho) = R^{1\times q}/R^{1\times p}A$, which is simply the quotient of $R^{1\times q}$ by the submodule generated by the rows of A. Then

$$R^{1\times p} \xrightarrow{\rho} R^{1\times q} \xrightarrow{\pi} M \longrightarrow 0 \qquad (11)$$

is an exact sequence of R-modules where $\pi : R^{1\times q} \to M$ is the canonical map. For every $s \geq 1$ and $1 \leq i \leq s$, let e_{is} be the unit vector in $R^{1\times s}$ with 1 in the ith position and 0 elsewhere. Then $e_{1p},\ldots,e_{pp}$ and $e_{1q},\ldots,e_{qq}$ are canonical bases of $R^{1\times p}$ and $R^{1\times q}$, respectively. Set $e_j = \pi(e_{jq})$ for $1 \leq j \leq q$. Since π is surjective, $e_1,\ldots,e_q$ generate M as an R-module. Since $\rho(e_{ip})$ is the i-th row of A, we have

$$0 = \pi(\rho(e_{ip})) = \pi\left(\sum_{j=1}^{q} a_{ij}e_{jq}\right) = \sum_{j=1}^{q} a_{ij}\pi(e_{jq}) = \sum_{j=1}^{q} a_{ij}e_j,$$

for $1 \leq i \leq p$, which implies that $(e_1,\ldots,e_q)^\tau$ is a solution of $A(Z) = 0$ in M.

Given two R-modules N_1 and N_2, let $\operatorname{Hom}_R(N_1,N_2)$ denote the C_F-vector space of all the R-linear maps from N_1 to N_2. We next show that the proof of Proposition 1.1 of [8] remains valid when $\mathcal{D}$ is replaced by R.

THEOREM 4. *Let $M{=}R^{1\times q}/R^{1\times p}A$. Then $\mathrm{sol}_N(A(Z){=}0)$ and $\operatorname{Hom}_R(M,N)$ are isomorphic as C_F-vector spaces for any R-module N.*

Proof. Applying the functor $\operatorname{Hom}_R(\cdot,N)$ to the exact sequence (11) of C_F-vector spaces and using the isomorphism $\operatorname{Hom}_R(R^{1\times s},N) \to N^s$ given by $f \mapsto (f(e_{1s}),\ldots,f(e_{ss}))^\tau$, we get the exact sequence:

$$0 \longrightarrow \operatorname{Hom}_R(M,N) \xrightarrow{\pi^*} N^q \xrightarrow{\lambda} N^p,$$

in which $\pi^*(f) = (f(e_1),\ldots,f(e_q))^\tau$ and $\lambda((n_1,\ldots,n_q)^\tau) = A(n_1,\ldots,n_q)^\tau$ for $n_1, \ldots, n_q$ in N. Since π^* is injective, $\operatorname{Hom}_R(M,N) \simeq \operatorname{Im}(\pi^*){=}\ker(\lambda){=}\mathrm{sol}_N(A(Z){=}0)$. □

Theorem 4 reveals that $e{:=}(e_1,\ldots,e_q)^\tau \in M^q$ is a "generic" solution of the system $A(Z) = 0$ in the sense that any solution of $A(Z) = 0$ is the image of e under some homomorphism. This means that M describes the properties of all the solutions of $A(Z) = 0$ "anywhere". So we define

DEFINITION 4. *Let $A \in S^{p\times q} \subset R^{p\times q}$. We call the R-module*

$$M = R^{1\times q}/R^{1\times p}A$$

the module of formal solutions *of the system $A(Z) = 0$. The dimension of M as an F-vector space is called the* linear dimension *of the system. The system is said to be* of finite linear dimension *if $0 < \dim_F M < +\infty$.*

Note that we choose to exclude systems with $\dim_F M = 0$ in our definition since such systems cannot have nonzero solutions in any R-module (which includes all orthogonal Δ-extensions of F). The next lemma is used to describe modules of formal solutions for finite-rank left ideals in S ([6]).

LEMMA 2. *Let J be a left ideal of S. Assume that J does not contain any monomial in $\partial_{\ell+1},\ldots,\partial_m$, and that S/J is finite dimensional over F. Let I be the left ideal generated by J in R and $\bar{J} = I \cap S$. Then $S/\bar{J}$ and R/I are isomorphic as vector spaces over F. In particular, R/I is finite dimensional over F.*

Proof. Let H be the set of all monomials in $\partial_{\ell+1},\ldots,\partial_m$. Since every element of H is invertible in R,

$$\bar{J} = \{a \in S \mid ha \in J \text{ for some } h \in H\}. \qquad (12)$$

Since $J \subset \bar{J}$, $\dim_F \left(S/\bar{J}\right)$ is finite. Let f_j be a nonzero polynomial in $F[\partial_j] \cap \bar{J}$ with minimal degree for $j > \ell$. Then each f_j is of positive degree with a nonzero coefficient of $\partial_j^0 = 1$, for otherwise, $\bar{J}$ would contain 1, and, hence, J would have a nonempty intersection with H by (12), a contradiction to our assumption. Since $\partial_j^{-1} f_j \in I$, ∂_j^{-1} is congruent to an element of $F[\partial_j]$ modulo I. It follows that every element of R is congruent to an element of S modulo I (note that every element of R can be written as an element of S multiplied by the inverse of an element of H from the right-hand side).
Let ϕ be the map from $S/\bar{J}$ to R/I that sends $a+\bar{J}$ to $a+I$ for $a \in S$. The map is well-defined, injective and linear over F because $\bar{J} = S \cap I$. By the conclusion made in the previous paragraph, for every element $(b + I)$ of R/I with $b \in R$, there exists b' in S such that $b \equiv b' \mod I$. Thus $\phi\left(b' + \bar{J}\right) = b + I$. The map ϕ is surjective. □

EXAMPLE 3. *Consider a $p{\times}1$ matrix $A = (L_1,\ldots,L_p)^\tau$, where the L_i are in S. The system $A(z) = 0$ corresponds to scalar equations $L_1(z) = \cdots = L_p(z) = 0$, whose R-module of formal solutions is $M = R/\rho(R^{1\times p}) = R/I$, where I is the left ideal $\sum_{i=1}^{p} RL_i$ of R. Let J be the left ideal $\sum_{i=1}^{p} SL_i$ of S. Then, by Lemma 2, $\dim_F M$ is finite if $\dim_F S/J$ is finite and J contains no monomial in $\partial_{\ell+1},\ldots,\partial_m$.*
Consider the case $\ell = 0$ and $m = 2$. If J is $S(\partial_1 + 1)$, then $\dim_F(M)$ is not finite. On the other hand, if J is equal to $S(\partial_1\partial_2(\partial_1 + 1)) + S(\partial_1\partial_2(\partial_2 + 1))$, then $\dim_F S/J$ is not finite, but $\dim_F M = 1$, because $I = R(\partial_1 + 1) + R(\partial_2 + 1)$.

EXAMPLE 4 (INTEGRABLE SYSTEMS). *Let $A_1,\ldots, A_m$ be in $F^{n\times n}$, $\mathbf{1}_n$ be the identity matrix in $F^{n\times n}$ and*

$$A = \begin{pmatrix} \partial_1 \cdot \mathbf{1}_n - A_1 \\ \vdots \\ \partial_m \cdot \mathbf{1}_n - A_m \end{pmatrix} \in S^{mn\times n}.$$

The system $A(Z) = 0$ corresponds to $\{\partial_i(Z) = A_iZ\}_{1\leq i\leq m}$, which is not necessarily fully integrable. Let M be its module of formal solutions and $e = (e_1,\ldots,e_n)^\tau \in M^n$ be as above. Then $A(e) = 0$ implies that $\partial_i e = A_i e$ for each i. Since the entries of A_i are in F, $\partial_i e_j \in \sum_{s=1}^{n} Fe_s$ for all i, j, and thus $Re_j \subset \sum_{s=1}^{n} Fe_s$ for all j. Hence $M = \sum_{s=1}^{n} Re_s = \sum_{s=1}^{n} Fe_s$. In particular, $\dim_F M \leq n$.

To check in practice whether a system is of finite linear dimension, we need to compute $\dim_F M$. As seen in Example 4, when the system is given as an integrable system, we have a set of generators for M over F, so computing $\dim_F M$ could be done by linear algebra over F as in Example 5. Note that in the purely differential case, we have $\dim_F M = n$ if the matrices A_i satisfy (2), $\dim_F M = 0$ otherwise. When the system is given by an ideal in S, then Lemma 2 shows that either $M = 0$ (if the ideal contains a monomial in $\partial_{\ell+1}, \ldots, \partial_m$) or an F-basis of M can be computed via Gröbner bases of S-modules. There are algorithms and implementations for this task [3, 4]. For more general matrices $A \in S^{p\times q}$, computing an F-basis of M involves computing Gröbner bases of R-modules. In the purely differential case, this is again Gröbner bases of S-modules. When difference operators are involved, the algorithms developed in [9, 13] for pure difference equations with constant coefficients are generalized in [12] to produce Gröbner bases of R-modules.

Let $A \in S^{p\times q}$ and M be the R-module of formal solutions for $A(Z){=}0$. Suppose that $\dim_F M = n$ and $b_1, \ldots, b_n$ form a basis of M over F. Then, for $b := (b_1, \ldots, b_n)^\tau$ there exists $B_i \in F^{n\times n}$ such that $\partial_i(b) = B_i b$ for each i. We can regard M as the module of formal solutions for the integrable system $\{\partial_i(X) = B_i X\}_{1\le i\le m}$. Indeed, suppose we find, as described in Example 4, its module M_B of formal solutions and $f := (f_1, \ldots, f_n)^\tau$ such that $M_B = \sum_{s=1}^n F f_s$ and $\partial_i(f) = B_i f$ for each i. Since $b \in M^n$ is a solution of $\{\partial_i(X) = B_i X\}_{1\le i\le m}$, there exists $\varphi \in \mathrm{Hom}_R(M_B, M)$ such that $b = \varphi(f)$ by Theorem 4. Since the b_i are linearly independent over F, so are the f_i. Hence $M_B = \oplus_{s=1}^n F f_s$ and φ is an isomorphism of R-modules.

Since ∂_i and ∂_j commute for any i and j, we have $\partial_i(\partial_j(b)) = \partial_j(\partial_i(b))$. From $\partial_i(b) = B_i b$ and the linear independence of $b_1, \ldots, b_n$ over F, it follows that

$$\sigma_i(B_j)B_i + \delta_i(B_j) = \sigma_j(B_i)B_j + \delta_i(B_j), \quad 1 \le i, j \le m,$$

i.e. $B_1, \ldots, B_m$ satisfy the compatibility conditions (2). Suppose that B_t is singular for some $t > \ell$. Then, there exists a nonzero $v \in F^{1\times n}$ such that $vB_t = 0$ and thus $v\partial_t(b) = vB_t b = 0$. Since M is an R-module on which ∂_t^{-1} acts, we have $0 = \partial_t^{-1}(v\partial_t(b)) = \sigma_t^{-1}(v)\partial_t^{-1}(\partial_t(b)) = \sigma_t^{-1}(v)b$, which implies that $b_1, \ldots, b_n$ are linearly dependent over F, a contradiction. So the B_j are invertible for $\ell + 1 \le j \le m$ and the system $\{\partial_i(X) = B_i X\}_{1\le i\le m}$ is fully integrable. We call it[2] the *fully integrable system associated to* M w.r.t. the basis $b_1, \ldots, b_n$.

Since any orthogonal Δ-extension E of F is turned into an R-module via the action $\partial_i(e) = \delta_i(e)$ for $i \le \ell$ and $\partial_i(e) = \sigma_i(e)$ for $i > \ell$, $\mathrm{sol}_E(A(Z) = 0)$ is well-defined. We now set up a correspondence between the solutions in E of $A(Z) = 0$ and those of its associated fully integrable system.

Proposition 2. *Let $A(Z) = 0$ with $A \in S^{p\times q}$ be a system of finite linear dimension, M be its module of formal solutions, $e_1, \ldots, e_q$ be R-generators for M and $b_1, \ldots, b_n$ be an F-basis of M such that $A(e_1, \ldots, e_q)^\tau = 0$ and*

$$\partial_i(b_1, \ldots, b_n)^\tau = B_i(b_1, \ldots, b_n)^\tau \quad \text{for each } i\,.$$

Let $P \in F^{q\times n}$ be given by $(e_1, \ldots, e_q)^\tau = P(b_1, \ldots, b_n)^\tau$. Then, for any orthogonal Δ-extension E of F, the correspondence $\xi \mapsto P\xi$ is an isomorphism of C_E-modules between $\mathrm{sol}_E(\{\partial_i(X) = B_i X\}_{1\le i\le m})$ and $\mathrm{sol}_E(A(Z) = 0)$.

[2]It is also called an *integrable connection.*

Proof. To simplify notation, we denote $\mathrm{sol}_E(A(Z){=}0)$ and $\mathrm{sol}_E(\{\partial_i(X) = B_i X\}_{1\le i\le m})$ by W_A and W_B, respectively. Write $e = (e_1, \ldots, e_q)^\tau$ and $b = (b_1, \ldots, b_n)^\tau$. According to Theorem 4, for any $\xi \in W_B$, there exists $\varphi \in \mathrm{Hom}_R(M, E)$ such that $\xi = \varphi(b)$. Hence

$$A(P\xi) = A(P\varphi(b)) = \varphi(A(Pb)) = \varphi(A(e)) = 0,$$

so $P\xi$ belongs to W_A. Thus the correspondence $\xi \mapsto P\xi$ is a homomorphism of C_E-modules from W_B to W_A.
For every $\eta \in W_A$ there exists $\psi \in \mathrm{Hom}_R(M, E)$ such that $\eta = \psi(e) = \psi(Pb) = P\psi(b)$. The correspondence $\xi \mapsto P\xi$ is then surjective, because $\psi(b)$ belongs to W_B. If $\xi \in W_B$ and $P\xi = 0$, then there exists $\varphi \in \mathrm{Hom}_R(M, E)$ such that $\xi = \varphi(b)$. Hence $0 = P\xi = \varphi(Pb) = \varphi(e)$. It follows that φ maps everything to 0 as M is generated by $e_1, \ldots, e_q$ over R. Thus $\xi = 0$ and the correspondence is bijective. □

Definition 5. *Let $A, M, b_1, \ldots, b_n$ and P be as in Proposition 2. A $q \times n$ matrix V with entries in an orthogonal Δ-extension E of F is called a* fundamental matrix *for $A(Z) = 0$ if $V = PU$ where $U \in E^{n\times n}$ is a fundamental matrix of the fully integrable system associated to M w.r.t. the basis $b_1, \ldots, b_n$.*
A Picard-Vessiot ring for any fully integrable system associated to M is called a Picard-Vessiot ring *for $A(Z) = 0$.*

Although this is not stated in the definition, it follows from Proposition 2 that the columns of a fundamental matrix form a C_E-basis of the C_E-module $\mathrm{sol}_E(A(Z){=}0)$: denote $\mathrm{sol}_E(A(Z){=}0)$ and $\mathrm{sol}_E(\{\partial_i(X) = B_i X\}_{1\le i\le m})$ by W_A and W_B respectively. Then the columns of $V = PU$ are in W_A by Proposition 2. Let $c \in C_E^{n\times 1}$ be such that $0{=}Vc = PUc$. Since $Uc \in W_B$, we have $Uc = 0$ by Proposition 2, hence $c{=}0$ since U is invertible. Thus the columns of V are linearly independent over C_E. For any $\eta \in W_A$ there exists $\xi \in W_B$ such that $\eta = P\xi$. By Proposition 1 there exists $c \in C_E^{n\times 1}$ such that $\xi = Uc$. Hence $\eta = PUc = Vc$.

Let $b_1, \ldots, b_n$ and $d_1, \ldots, d_n$ be two bases of M over F. Write $b = (b_1, \ldots, b_n)^\tau$ and $d = (d_1, \ldots, d_n)^\tau$, and let $T \in \mathrm{GL}_n(F)$ be given by $d = Tb$. For each i, let $B_i, D_i \in F^{n\times n}$ be such that $\partial_i(b) = B_i b$ and $\partial_i(d) = D_i d$. If E is a Picard-Vessiot ring for $\{\partial_i(X) = B_i X\}_{1\le i\le m}$ and $U \in E^{n\times n}$ is a corresponding fundamental matrix, then TU is a fundamental matrix for $\{\partial_i(Y) = D_i Y\}_{1\le i\le m}$ by Theorem 4, so E is a Picard-Vessiot ring for that system too. This justifies the second part of Definition 5.

As a final consequence of Theorems 1 and 2, we have

Theorem 5. *Every system $A(Z){=}0$ of finite linear dimension has a fundamental matrix and has a Picard-Vessiot ring E. If F has characteristic 0 and C_F is algebraically closed, then $C_E = C_F$.*

Proof. Let $A \in S^{p\times q}$ be such that $A(Z) = 0$ is of finite linear dimension $n > 0$, M be its module of formal solutions, $e_1, \ldots, e_q$ be R-generators for M and $b_1, \ldots, b_n$ be an F-basis of M such that $A(e_1, \ldots, e_q)^\tau{=}0$ and $\partial_i(b_1, \ldots, b_n)^\tau = B_i(b_1, \ldots, b_n)^\tau$ for each i. Let $P \in F^{q\times n}$ be given by $(e_1, \ldots, e_q)^\tau = P(b_1, \ldots, b_n)^\tau$. Since $\{\partial_i(X) = B_i X\}_{1\le i\le m}$

is a fully integrable system, there exists, by Theorem 1, a fundamental matrix $U \in E^{n\times n}$ for that system where E is some orthogonal Δ-extension of F. Then $V := PU \in E^{q\times m}$ is a fundamental matrix for $A(Z) = 0$. The existence of the Picard-Vessiot ring and the second statement follow directly from Theorem 2. $\square$

Assume that F has characteristic 0 with an algebraically closed field of constants. Let E be a Picard-Vessiot ring for the system $A(Z) = 0$. As mentioned after Theorem 2, $\mathrm{sol}_E(\{\partial_i(X) = B_iX\}_{1\le i\le m})$ is of dimension n over C_F. But that space is isomorphic to $\mathrm{sol}_E(A(Z) = 0)$ by Proposition 2. Therefore the dimension of $\mathrm{sol}_E(A(Z) = 0)$ as a C_F-vector space equals n, the linear dimension of $A(Z) = 0$.

Example 5. *Let F, δ_x and σ_k be as in Example 1, and the system $\mathcal{A}$ is given by*

$$A_x = \begin{pmatrix} \frac{x+1}{x} & \frac{k(x+1-k)}{x^2(k-1)} & -\frac{k(x+1-k)}{x^2(k-1)} \\ x+1 & \frac{xk-k^2+2x^2+kx^2+k-1}{x(k-1)} & -\frac{xk-k^2+2x^2+kx^2}{x(k-1)} \\ x+1 & \frac{xk+2x^2+kx^2-2k^2+k}{x(k-1)} & -\frac{xk+2x^2+kx^2-2k^2+1}{x(k-1)} \end{pmatrix},$$

$$A_k = \begin{pmatrix} \frac{k+1}{k} & \frac{k+1-xk-x}{x(k-1)} & \frac{xk+x-k-1}{x(k-1)} \\ \frac{x(k+1)}{k} & \frac{1-2x+k-xk+x^3}{k-1} & \frac{2x+xk-x^3-k-1}{k-1} \\ \frac{x(k+1)}{k} & \frac{1-2xk-2x+k+x^3}{k-1} & \frac{2xk+2x-k-x^3-1}{k-1} \end{pmatrix}.$$

Note that A_x and A_k satisfy the compatibility conditions (2) but A_k is singular, so the system is not fully integrable. Let $S = [\partial_x; \mathbf{1}, \delta_x][\partial_k; \sigma_k, \mathbf{0}]$ and R be the corresponding Laurent-Ore algebra. Let $A \in S^{6\times 3}$ be the matrix corresponding to the system given by A_x and A_k (see Example 4), $M = R^{1\times 3}/R^{1\times 6}A$ be the module of formal solutions for the system $A(Z) = 0$, and $\{e_1, e_2, e_3\}$ be a set of R-generators of M such that $\partial_x(e_1, e_2, e_3)^\tau = A_x(e_1, e_2, e_3)^\tau$ and $\partial_k(e_1, e_2, e_3)^\tau = A_k(e_1, e_2, e_3)^\tau$. Solving the linear system $(v_1, v_2, v_3)A_k = 0$ over F, we see that A_k has rank 2, and $\partial_k(e_1)$, $\partial_k(e_2)$ and $\partial_k(e_3)$ are linearly dependent over F (so are e_1, e_2 and e_3 by an application of ∂_k^{-1}). A nontrivial solution of $(v_1, v_2, v_3)A_k = 0$ and an application of ∂_k^{-1} yield

$$\begin{pmatrix} e_1 \\ e_2 \\ e_3 \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ \frac{x(k-1)}{x^2-1} & \frac{x^2-k}{x^2-1} \end{pmatrix}}_{P} \begin{pmatrix} e_1 \\ e_2 \end{pmatrix},$$

which, together with A_x and A_k, implies that $\partial_x(e_1, e_2)^\tau = B_x(e_1, e_2)^\tau$ and $\partial_k(e_1, e_2)^\tau = B_k(e_1, e_2)^\tau$ where

$$B_x = \begin{pmatrix} \frac{-x+x^3-1+x^2-xk-k+k^2}{x(x^2-1)} & \frac{k(x+1-k)}{x^2(x^2-1)} \\ \frac{-x-xk+x^3-1-x^2+k^2-kx^2}{x^2-1} & \frac{-k^2+xk+kx^2+3x^2-1}{x(x^2-1)} \end{pmatrix},$$

$$B_k = \begin{pmatrix} \frac{xk+x+k^2+2k+1}{k(x+1)} & -\frac{k+1}{x(x+1)} \\ -\frac{(kx^2-x-k^2-2k-1)x}{k(x+1)} & \frac{x^2+x-1-k}{x+1} \end{pmatrix}.$$

Since B_k is invertible, the system $\mathcal{B}$ given by B_x and B_k is fully integrable, and, hence, e_1 and e_2 form an F-basis of M. The same method to construct a fundamental matrix for the system in Example 1 yields a fundamental matrix for $\mathcal{B}$:

$$U = \begin{pmatrix} xke^x & -kx^k \\ kx^2e^x & (x^2-k-1)x^{k+1} \end{pmatrix},$$

hence PU is for $\mathcal{A}$. In addition, a Picard-Vessiot ring of $\mathcal{B}$ is a Picard-Vessiot ring of $\mathcal{A}$.

Acknowledgments: We would like to thank an anonymous referee for his useful and constructive remarks. The second and third authors were supported in part by a 973 key project (no. 2004CB31830), and by a *Bourse du Gouvernement Français* (BGF no. 2002915), respectively.

6. REFERENCES

[1] Bialynicki-Birula, A. On Galois theory of fields with operators. *Amer. J. Math. 84* (1962), 89–109.

[2] Cassidy, P. and Singer, M. *Galois Theory of Parameterized Differential Equations and Linear Differential Algebraic Groups.* Preprint, 2005.

[3] Chyzak, F., Quadrat, A., and Robertz, D. OreModules: A symbolic package for the study of multidimensional linear systems. In *Proc. of MTNS'04, Leuven (Belgium)* (2004), CDRom.

[4] Chyzak, F. and Salvy, B. Non-commutative elimination in Ore algebras proves multivariate identities. *J. Symbolic Comput. 26*, 2 (1998), 187–227.

[5] Kolchin, E. *Differential algebra and algebraic groups.* Academic Press, New York and London, 1973.

[6] Labahn, G. and Li, Z. Hyperexponential solutions of finite-rank ideals in orthogonal Ore rings. In *Proc. ISSAC'2004* (2004), J. Gutierrez, Ed., ACM, 213–220.

[7] Li, Z., Schwarz, F., and Tsarev, S. P. Factoring systems of linear PDEs with finite-dimensional solution spaces. *J. Symbolic Comput. 36*, 3–4 (2003), 443–471.

[8] Malgrange, B. Motivations and introduction to the theory of D-modules. In *Computer Algebra and Differential Equations* (1994), E. Tournier, Ed., vol. 193 of *LMS Lecture Note Series*, Cambridge University Press, pp. 3–20.

[9] Pauer, F. and Unterkircher, A. Gröbner bases for ideals in Laurent polynomial rings and their applications to systems of difference equations. *Appl. Algebra in Eng., Comm., and Comp. 9* (1999), 271–291.

[10] Singer, M. and van der Put, M. *Galois Theory of Difference Equations.* LNM 1666. Springer, 1997.

[11] Singer, M. and van der Put, M. *Galois Theory of Linear Differential Equations*, vol. 328 of *Grundlehren der Mathematischen Wissenschaften.* Springer, Heidelberg, 2003.

[12] Wu, M. *Factorization and decomposition of modules over Laurent-Ore algebras.* Thèse de mathématiques, Université de Nice, expected 2005.

[13] Zampieri, S. A solution of the Cauchy problem for multidimensional discrete linear shift-invariant systems. *Linear algebra and appl. 202* (1994), 143–162.