Eigenring and Reducibility of Difference Equations

Raphaël Bomboy
Café Project, INRIA Sophia-Antipolis

March 6, 2000

Summary by Frédéric Chyzak and Pierre Nicodème

Abstract

The Galois theory for differential equations is now classical. We consider here a Galois theory for difference equations whose development is more recent. In analogy with the differential case, a concept of Liouvillian solutions of a difference equation is introduced, in relation to equations with solvable Galois group. In the first part of this talk, Bomboy presents the Galois theory for linear finite difference operators. Next he adapts the concept of eigenring introduced in the differential case by Singer [11] to suggest an algorithm searching for Liouvillian solutions of linear difference equations. This direct algorithm solves a subclass of the difference equations without using Petkovšek’s algorithm [8].

Introduction

We review in Section 1 the basic notions of Galois theory for difference equations, following the presentation of [7]. As in the differential case, the Galois group is a linear algebraic group. In Section 2 we present the main properties of reducible and completely reducible systems, from the point of view of the structure of their associated matrices. In the differential case, a Liouvillian extension of a differential field is done by algebraic extensions and by the operations of exponentiation and integration of a function of the field. In Section 3 we define Liouvillian solutions in the difference case; these solutions are essentially interlacings of hypergeometric sequences. We describe the notion of eigenring in Section 4 and summarize relevant properties. We finish by presenting Bomboy’s algorithm for searching Liouvillian solutions in Section 5, and by concluding comments.

1. Difference Galois Theory

A difference ring \((k, \phi)\) is a ring \(k\) with an automorphism \(\phi\). (Note that all rings considered here are rings with identity.) For example, let \(k\) be the ring \(\mathbb{C}[z]\) of polynomials or the field \(\mathbb{C}(z)\) of fractions, and \(\phi\) the automorphism that substitutes \(z + 1\) for \(z\). When \(\phi(x) = x\) for \(x \in k\), \(x\) is called a constant of \((k, \phi)\). The set \(C(k)\) of constants is a subring of \(k\).

From now on we assume that \(k\) is a field. A (scalar) difference equation has the form

\[
L(y) = \phi^m(y) + a_{m-1}\phi^{m-1}(y) + \cdots + a_0 y = 0,
\]

where the \(a_i\)’s are in \(k\) and \(L = \phi^m + a_{m-1}\phi^{m-1} + \cdots + a_0\) is the difference operator associated to the equation. The set of difference operators or skew polynomials in \(\phi\) with multiplication \(\phi a = \phi(a)\phi\) is a non-commutative ring \(\mathcal{P}_k(\phi)\). Equation (1) can be transformed into the system \(\phi(Y) = A_L Y\),
where \( \phi \) is applied componentwise to the vector \( Y \) and

\[
A_L = \begin{pmatrix}
0 & 1 & 0 & \ldots & 0 \\
0 & 0 & 1 & \ldots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
-a_0 & -a_1 & \ldots & \ldots & (-a_m - 1)
\end{pmatrix}.
\]

One sees that \( y \) is a solution of \( L(y) = 0 \) if and only if \( (y, \phi(y), \ldots, \phi^{m-1}(y))^T \) is a solution of \( \phi(Y) = A_L Y \).

More generally, we will consider systems of difference equations of the form

\[
(2) \quad \phi(Y) = AY
\]

for an element \( A \) of \( \text{GL}_n(k) \), the space of invertible matrices of dimension \( n \) over \( k \). If \( R \) is a difference ring extension of \( k \), a fundamental matrix for Equation (2) is an element \( U = (u_{i,j}) \in \text{GL}_n(R) \) such that \( \phi(U) = AU \) where \( \phi \) maps componentwise to matrices. A difference ring extension \( R \) of \( k \) is called a Picard–Vessiot extension of \( k \) for Equation (2) if \( R \) is a simple difference ring (the only \( \phi \)-invariants ideals are \((0)\) and \( R \)) and \( R = k [u_{1,1}, \ldots, u_{n,n}, (\det U)^{-1}] \) with \( U \) a fundamental matrix. The following theorem describes the structure of such extensions.

**Theorem 1** ([12]). If the set of constants \( C(k) \) is algebraically closed, Picard–Vessiot extensions \( R \) of \( k \) exist and are unique up to isomorphism.

The Galois group \( \text{Gal}(R/k) \) of \( R \) over \( k \) is the set of linear maps that are the identity on \( k \) and commute with \( \phi \). As in the differential case, it can be proved to have a structure of a linear algebraic group over \( C(k) \). The set \( V \) of solutions of Equation (2) in \( R^n \) is a \( \eta \)-dimensional vector space over \( C(k) \) that is invariant by \( \text{Gal}(R/k) \). This yields a representation of \( \text{Gal}(R/k) \) in \( C(k)^n \).

Let \( \phi(Y) = AY \) and \( \phi(Y) = BY \) be two systems with \( A \) and \( B \) in \( \text{GL}_n(k) \) and let \( V_A \) and \( V_B \) be the corresponding solution spaces in Picard–Vessiot extensions \( R_A \) and \( R_B \). Both systems are equivalent if there is a matrix \( T \in \text{GL}_n(k) \) such that \( B = \phi(T)AT^{-1} \). Then, if \( U \) is a fundamental matrix of \( \phi(Y) = AY \), it follows that \( TU \) is a fundamental matrix for \( \phi(Y) = BY \); in this case, one can identify the rings \( R_A \) and \( R_B \), and \( V_A \) and \( V_B \) are isomorphic as \( \text{Gal}(R/k) \)-modules (defined as modules over the group algebra of \( \text{Gal}(R/k) \) with coefficients in \( C(k) \)). For a large class of difference fields, any system \( \phi(Y) = AY \) is equivalent to the companion system of a scalar equation [7].

We conclude this section with an illustration on the ring \( S \) of germs of sequences over \( \mathbb{C} \).

**Definition 1.** Consider two elements \( (a_n)_{n \in \mathbb{N}} \) and \( (b_n)_{n \in \mathbb{N}} \) of \( C^n \) (where \( C \subset \mathbb{C} \) is a ring). We define the following equivalence relation: \( (x_n) \equiv (y_n) \) if and only if \( (x_n) \) and \( (y_n) \) only differ by a finite number of terms. We now consider the quotient ring \( S = (C^n) \equiv \) where addition and multiplication are defined componentwise; an element of this ring is called a germ.

Note that this gives us a natural embedding \( \nu \) of the rational function ring \( \mathbb{C}(z) \) into \( S \), where for \( F \in \mathbb{C}(z) \), \( \nu(F) \) is given as the germ of any \( (s_n)_{n \in \mathbb{N}} \) such that \( s_n = F(n) \) for sufficiently large \( n \).

**Definition 2.** The shift \( \sigma \) of \( S \) maps \( \nu((x_0, \ldots, x_n, \ldots)) \) to \( \nu((x_1, \ldots, x_{n+1}, \ldots)) \).

From now on, the ring \( C \) is an algebraically closed subfield of \( \mathbb{C} \) and \( k = \nu(C(z)) \).

**Property 1** ([12]). Let \( C \subset \mathbb{C} \) be an algebraically closed field. There exists a Picard–Vessiot extension of the equation \( \sigma(Y) = AY \) over \( C(z) \subset S \) that also lies in \( S \).

**Example.** Consider \( k = \nu(C(z)) \) and the equation \( \sigma(x) = -x \). The Picard–Vessiot extension \( R \) of \( k \) is the ring generated by \( k \) and the sequence \( s = (1,-1,1,-1,\ldots) \). Note that if \( t = s + (1,1,\ldots) = (2,0,2,\ldots) \) then \( t \times \sigma(t) = 0 \). The Picard–Vessiot extension therefore has zero divisors and cannot be a field.
2. Reducibility

The following theorem gives a criterion of reducibility for operators.

**Theorem 2** ([3]). Consider an operator $L \in \mathcal{P}_k(\phi)$ with Picard–Vessiot extension $R$. The following statements are equivalent:

1. $L$ is reducible (i.e., $L = L_1 L_2$ in $\mathcal{P}_k(\phi)$);
2. the solution space $V$ has a strict subspace $W$ that is stable under the action of the Galois group $G = \text{Gal}(R/k)$;
3. the system $\phi(X) = A_L X$ is equivalent to a system with block upper triangular companion matrix.

We also consider the class of completely reducible operators.

**Definition 3.** Let lcm stand for least common left multiple. An operator $L \in \mathcal{P}_k(\phi)$ is completely reducible if there exist $L_1, \ldots, L_k$ such that $L = \text{lcm}(L_1, \ldots, L_k)$.

Beware that an irreducible operator $L$ is completely reducible because $L = \text{lcm}(L)$.

**Property 2 ([3]).** The following statements are equivalent:

1. $L$ is completely reducible;
2. the solution space $V$ is expressible as a direct sum $V = V_1 \oplus \cdots \oplus V_k$ where $V_i$ is a stable $G$-module for each $i$, and the corresponding operators are irreducible;
3. the system $\phi(X) = AX$ is equivalent to a system with block diagonal companion matrix where each block corresponds to an irreducible $G$-module.

3. Liouvillian Solutions

We begin this section by defining **Liouvillian solutions** of an equation in terms of interlaces of sequences and hypergeometric sequences. Next we give the expected Galois-theoretic characterization of Liouvillian solutions of a difference equation, before giving another characterization in terms of interlaces of hypergeometric solutions.

**Definition 4.** The interlacing of sequences $x^1, \ldots, x^i$ of $\mathbb{C}^n$ is the sequence $(x^1_0, x^2_0, \ldots, x^i_0, x^1_1, \ldots)$. This definition extends to interlacing of germs in a natural way.

**Definition 5.** Hypergeometric sequences are germs $x \in \mathcal{S}$ such that $\sigma(x) = ax$ for some $a \in k$.

**Definition 6.** The set $\mathcal{L}$ of Liouvillian sequences is the smallest subring of $\mathcal{S}$ such that:

1. constants belong to $\mathcal{L}$, where it is understood that $\gamma \in \mathbb{C}(k)$ is identified to the germ $(\gamma, \gamma, \ldots) \in \mathcal{S}$;
2. if $x$ is hypergeometric, $x$ belongs to $\mathcal{L}$;
3. if $x$ is solution of $\sigma(x) = x + a$ with $a \in \mathcal{L}$, then $x$ belongs to $\mathcal{L}$;
4. if $x$ belongs to $\mathcal{L}$, the interlacing of $x$ with zero germs (i.e., the interlacing of $x^1 = \cdots = x^{i-1} = 0$ and $x^i = x$) belongs to $\mathcal{L}$.

**Example.** Elements of $k$ are hypergeometric, thus belong to $\mathcal{L}$; on the other hand, the germs $(2^n)_{n \in \mathbb{N}}$ and $(n!)_{n \in \mathbb{N}}$ are two examples of hypergeometric, thus Liouvillian, sequences that are not in $k$.

**Example (Harmonic numbers).** If $k = \mathbb{C}(z)$ and $x = \left(\sum_{j=1}^{n} j \right)_{n \in \mathbb{N}}^n$ we have $(1/(n + 1))_{n \in \mathbb{N}} = \nu(1/(z + 1)) \in k$ and $\sigma(x) = x + (1/(n + 1))_{n \in \mathbb{N}}$. The germ $\nu(x)$ thus belongs to $\mathcal{L}$.

**Example.** The sequence $(0, 1, 0, 1, \ldots)$ is the interlacing of both constant sequences $0$ and $1$, and therefore belongs to $\mathcal{L}$.

The following theorem gives the expected Galois-theoretic characterization of Liouvillian sequences.
Theorem 3 ([7]). A solution $x \in S$ of Equation (1) is Liouvillian if and only if the Galois group of any Picard–Vessiot extension of this equation is solvable.

We come to another characterization of Liouvillian sequences. Let $Z$ be a fundamental system of $\sigma(X) = AX$. Then by iteratively applying $\sigma$ to $\sigma(Z) = AZ$ we see that $Z$ is solution of $\sigma^m(Z) = \Pi_{\sigma}^m Z$ where $\Pi_{\sigma}^m = \sigma^{m-1}(A) \ldots A$. Let $\tau$ be the automorphism of $\mathbb{C}(z)$ substituting $mz$ for $z$. Then $\tau \circ \sigma^m = \sigma^m \circ \tau$; for $i$ from 0 to $m - 1$, the $i$th $m$-section $\tau \circ \sigma^i(Z)$ of $Z$ satisfies the equation $\sigma^i(O) = (\Pi_{\sigma}^m, A)O$ in the unknown $O$, where $\Pi_{\sigma}^m, A = \tau \circ \sigma^i(\Pi_{\sigma}^m, A)$. This gives the following theorem and corollary.

Theorem 4 ([7]). Let $L$ be an operator of order $n$ over $k$. The following statements are equivalent:

1. there is a Liouvillian solution for the equation $L(y) = 0$;
2. there exists an $m$ less than or equal to $n$, such that the equation $L(y) = 0$ has a solution that is the interlacing of $m$ hypergeometric series;
3. there exists an $m$ such that, for all $i$ between 0 and $m - 1$, the equation $\sigma(y) = (\Pi_{\sigma}^m, A_L)(y)$ has an hypergeometric solution;
4. there exist $m$ and $i$, with $i \leq m$, such that the equation $\sigma(y) = (\Pi_{\sigma}^m, A_L)(y)$ has an hypergeometric solution.

Corollary 1 ([7]). Let $L$ be an operator with coefficients in $k$. One can find operators $H_1, \ldots, H_i, R$ with coefficients in $k$ such that

1. $L = RH_1 \ldots H_i$;
2. the solution space of each $H_i$ is spanned by interlacings of hypergeometric sequences;
3. any Liouvillian solution of $L(y) = 0$ is a solution of $H_1 \ldots H_i(y) = 0$.

4. Eigenrings and their Structure

We consider the non-commutative ring $A = \mathcal{P}_k(\sigma)$ and a difference operator $L \in A$ with Picard–Vessiot extension $R$. Let $V$ be the space of solutions of $L$ in $R$. We now describe isomorphisms between three classes of objects:

1. eigenrings, that are rings that essentially contain operators that follow some special commutation relation with $L$;
2. endomorphisms of $V$ that commute with the Galois group $G = \text{Gal}(R/k)$;

Eigenring of $L$. Given an operator $L$, the elements $U + AL \in A/AL$ such that there exists $U^t \in A$ satisfying $LU = U^t L$ clearly form a ring. We call it the eigenring $E(L)$ of $L$. Note that $E(L)$ is never empty: $C(k)$ is always part of $E(L)$.

$G$-endomorphisms of the solution space $V$. For $P \in A$, consider the mapping $\eta_P$ of $R$ into $R$ defined by $\eta_P(v) = P \cdot v$ for all $v \in R$. This $C(k)$-linear mapping clearly commutes with $G$, since $G$ commutes with $\sigma$. We are interested in the situation when the mapping $\eta_P$ induces a linear map of $\text{End}_G V$, the algebra of $C(k)$-linear mappings of $V$ into $V$ that commute with $G$. Take $v$ in $V$; we have $L \cdot v = 0$. Consider $L \cdot \eta_P(v) = LP \cdot v$. This is zero if and only if $P + AL$ belongs to $E(L)$, for then there is $P^t$ such that $LP = P^t L$. In this latter case, $\eta_P$ induces a $G$-endomorphism of $V$.

$A$-linear endomorphisms of $A/AL$. Consider the $C(k)$-algebra $\text{End}_A(A/AL)$ of $A$-linear endomorphisms of $A/AL$, and $\lambda$ an element of this algebra. Recall that the module $A/AL$ can be viewed as the $A$-module generated by any “generic solution” of $L$; the linear map $\lambda$ is thus completely
described by the image of the generator $1 + AL$ of $A/AL$. The map $\lambda$ is well-defined as an $A$-linear map if and only if the image $\lambda(1 + AL) = U + AL$ abides by the relation

$$L(U + AL) = L\lambda(1 + AL) = \lambda(L(1 + AL)) = \lambda(0) = 0,$$

which implies that there exists $U'$ such that $LU = U'L$; in other words, $U + AL$ is in the eigenring. The converse property is proved similarly.

With a closer look on the bijections above, one gets the following result.

**Proposition 1.** The three rings $E(L)$, $\text{End}_G V$, and $\text{End}_A(A/AL)$ are isomorphic.

The classical representation theory for semi-simple modules [6] applies to the study of the structure of eigenrings, yielding the following proposition and corollary.

**Proposition 2** ([4]). For an operator $L$ with Galois group $G$ and space of solutions $V$, there are ring isomorphisms between:

1. the eigenring $E(L)$;
2. the endomorphism algebra $\text{End}_G V$;
3. the set of matrices $P \in M_n(k)$ satisfying $A_L P = \sigma(P) A_L$.

**Proposition 3** ([4]). Let $L$ be a completely reducible operator with solution space $V$. Then $V$ is isomorphic to a direct sum $V_1^{n_1} \oplus \cdots \oplus V_r^{n_r}$ where no $V_i$ and $V_j$ are isomorphic for $i \neq j$; the eigenring $E(L)$ is isomorphic to the direct sum $\bigoplus_{i=1}^r M_{n_i}(C(k))$.

**Corollary 2** ([4]). Let $L$ be a difference operator with eigenring $E(L)$. Then:

1. $L$ is irreducible implies that $E(L)$ is isomorphic to $C(k)$;
2. $L$ is completely reducible and $E(L)$ is isomorphic to $C(k)$ imply that $L$ is irreducible.

5. **Algorithms**

**Eigenring.** An algorithm to compute the eigenring of a differential operator was given by Singer [11]. A similar algorithm computes the eigenring in the difference case. The method proceeds by undetermined coefficients: an element of the eigenring of an operator $L$ of order $n$ is viewed as a residue $U$ modulo $L$; it is thus represented by $n$ undetermined rational function coefficients. One then performs the multiplication by $L$ on the left, then the Euclidean division by $L$ on the right. This yields a first-order linear difference system in the $n$ unknowns. This system is then solved for rational function solutions by algorithms based on Abramov’s algorithm [1].

**Linear Difference Equations of Order 2.** We consider the search for Liouvillian solutions of linear difference operators in the case of order 2. As follows from the analysis in Section 3, the search for Liouvillian solutions reduces to searching for hypergeometric solutions of associated equations. Petkovšek gave an algorithm for this purpose [8], but with exponential complexity. Bomboy’s algorithm proceeds by determining hypergeometric solutions from the computation of successive eigenrings, so as to derive the shape of the Galois group $G$ little by little, while avoiding Petkovšek’s algorithm as much as possible.

In order to help to solve for hypergeometric solutions, note that each non-trivial element $U + AL$ of $E(L)$ yields a right factor of $L$. Indeed, viewed as an element of $\text{End}_G V$, it necessarily has an eigenvalue $\lambda$ and a corresponding eigenvector $v$. The right gcd $G$ of $U - \lambda$ and $L$ can be expressed by a Bézout relation and satisfies $G \cdot v = 0$. It is therefore a non-constant right-hand factor of $L$.

---

1Note that the same idea was used in the context of symbolic summation/integration in Chyzak’s work [5].
Let $x$ be a hypergeometric solution: there exists $a \in \mathbb{C}(x)$ such that $\sigma(x) = a \cdot x$. For all $g$ in the Galois group $G$ we have

$$\sigma(g(x)) = g(\sigma(x)) = g(a \cdot x) = a \cdot g(x).$$

Therefore the subspace $\mathbb{C}x$ is globally invariant under the action of $G$. This entails that the space of hypergeometric solutions is a $G$-module, as is the total solution space of $L$. From this and Proposition 3, it follows that the eigenring is either not a semi-simple $G$-module, or has dimension 1, 2, or 4.

If the space of hypergeometric solutions is 2-dimensional, $G$ is isomorphic to the group of diagonal matrices with two independent non-zero entries, and $E(L)$ has dimension 2 or 4. If there is only a 1-dimensional space of hypergeometric solutions, a classification of the algebraic subgroups of $\text{GL}_2(\mathbb{C})$ then shows that $G$ is isomorphic to the group of upper triangular matrices $(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix})$; moreover, either the solution space $V$ is semi-simple as $G$-module and the eigenring $E(L)$ has dimension 2, or it is not semi-simple, and in view of $E(L) \simeq \text{End}_G(V)$, $E(L)$ consists of matrices that commute with all the upper triangular matrices above, and has dimension 1 or 2. If there are no hypergeometric solutions, the same classification shows that the Galois group $G$ contains the special linear group $\text{SL}_2(\mathbb{C})$ of matrices of determinant 1, and $E(L)$ has dimension 1.

If $L$ has a Liouvillian solution, it also has a one that is either hypergeometric or the interlacing of two hypergeometric sequences. Bomboy’s algorithm to decide the existence of Liouvillian solutions and compute a basis of their vector space therefore first computes the eigenring $E(L)$. If it is not trivial (i.e., does not reduce to homotheties), it provides all hypergeometric solutions, then all Liouvillian solutions; otherwise, the eigenring corresponding to the system $\Pi^2 A_L$ is computed and:

1. if it is not trivial, we obtain an hypergeometric solution of this system, which gives a solution of $L$ by interlacing of hypergeometric sequences;
2. otherwise, the classification of algebraic groups shows that either $L$ has a unique hypergeometric solution, and it is necessary to search this solution by Petkovšek’s algorithm, or $L$ has no hypergeometric solutions, and therefore $L$ provedly has no Liouvillian solution.

6. Conclusion

Finally, the authors of this summary wish to do full justice to Petkovšek, and want to emphasize that the search for Liouvillian solutions can be entirely performed by means of (variants of) algorithms by Petkovšek, and with no need of Galois theory.\(^2\)

Indeed, Petkovšek showed in an unpublished work [9]\(^3\) how to use his algorithm for finding hypergeometric solutions [8] in a recursive fashion and in combination with reduction of order so as to produce all *Alemberrian solutions* of an operator. (The class of Alemberrian sequences is obtained by the same closure operations as the Liouvillian case, except for interlacements.) This algorithm corresponds to factorizations into first-order operators $H_i$ in Corollary 1.

In fact, Petkovšek’s hypergeometric algorithm extends in a simple way to an algorithm for finding the solutions of a recurrence

$$a_0(n)u_n + \cdots + a_{m-1}u_{n+m-1} + u_{n+m} = 0$$

that are interlacings of hypergeometric sequences:

1. derive a recurrence on $u_n$ in which the index is shifted by multiples of $m$: since we know that the $\mathbb{C}(n)$-vector space generated by $u_n$ is finite-dimensional with basis $(u_n, u_{n+1}, \ldots, u_{n+m-1})$,

\(^2\)This section is the result of stimulating discussions with Bruno Salvy.

\(^3\)seemingly subsumed by [2],
the particular shifts \( u_n, u_{n+m}, u_{n+2m}, \ldots \) rewrite onto this basis, and a linear dependency can be found by Gaussian elimination;
2. for each \( i \) between 0 and \( m - 1 \), derive a recurrence on \( v_p^{(i)} = u_{mp+i} \) by substituting \( mp + i \) for \( n \) in the obtained recurrence, and solve it for hypergeometric solutions;
3. return the interlacing of the sequences \( v_p^{(0)}, v_p^{(1)}, \ldots, v_p^{(m-1)} \).

A variant algorithm (corresponding to Steps 1. and 2. above) is derived in [10] by a different approach.

Corollary 1, or equivalently a direct analysis mimicking that in [9], can now be used to derive an algorithm for finding all Liouvillian solutions of a recurrence. This algorithm is essentially Petkovšek’s algorithm for Alemberian solutions where searches for hypergeometric solutions—and first-order right-hand factors—is replaced with searches for interlacings of hypergeometric solutions—and higher-order right-hand factors. The main difference is that reduction of order is simultaneously performed by as many independent particular solutions as the order of the interlacings, instead of by just 1.

One can thus view Bomboy’s contribution as providing a variant algorithm in terms of eigenrings. A complexity of both approaches still has to be performed so as to compare them conclusively.

Bibliography