# AN INTRODUCTION TO DIFFERENCE GALOIS THEORY

JULIEN ROQUES

Abstract. These are notes for my lectures at the summer school "Abecedarian of SIDE" held at CRM (Montréal) in June 2016. They are intended to give a short introduction to difference Galois theory, leaving aside the technicalities.

Contents



---

*Date*: September 9, 2016.

2010 *Mathematics Subject Classification.* 39A06,12H10.

*Key words and phrases.* Linear difference equations, difference Galois theory.

The second author is partially funded by the french ANR project QDIFF (ANR-2010-JCJC-010501).

## 1. Introduction

These are notes for my lectures at the summer school "Abecedarian of SIDE" held at CRM (Montréal) in June 2016. They are intended to give a short introduction to difference Galois theory, leaving aside the technicalities. There already exist several nice introductory papers/surveys about differential Galois theory, *e.g.* [Ber92, Beu92, VdP98, Sin09, Sau12], and (parameterized) difference Galois theory, *e.g.* [HSS16, DV12]. For complete proofs and further results concerning difference Galois theory, we refer the reader to van der Put and Singer's [vdPS97].

## 2. First steps : from classical Galois theory to difference Galois theory

### 2.1. The classical Galois groups.

The Galois group over $\mathbb{Q}$ of a polynomial $P(X) \in \mathbb{Q}[X]$ can be defined as follows. We start with the base field $\mathbb{Q}$. We then consider a splitting field $K$ of $P(X)$ over $\mathbb{Q}$ *i.e.* a minimal field extension of $\mathbb{Q}$ over which $P(X)$ decomposes as a product a polynomials of degree 1. Then, the Galois group of $P(X)$ over $\mathbb{Q}$ is made of the field automorphisms $\sigma$ of $K$ such that $\sigma_{|\mathbb{Q}} = \mathrm{Id}_{\mathbb{Q}}$.

**Ex. 1** — Recall why we can describe the elements of this Galois group as the permutations of the roots of $P(X)$ preserving the algebraic relations with coefficients in $\mathbb{Q}$ between these roots. This was Galois's original approach.

### 2.2. The differential Galois groups.

This construction can be extended to linear differential equations with coefficients in $\mathbb{C}(z)$ as follows. Instead of a polynomial $P(X)$ with coefficients in $\mathbb{Q}$, we consider a linear differential system

$$Y'(z) = A(z)Y(z) \text{ with } A(z) \in \mathbb{C}(z)^{n\times n}.$$

The base field $\mathbb{Q}$ of Section 2.1 above is now replaced by the field $\mathbb{C}(z)$ or, better, by the field $\mathbb{C}(z)$ endowed with the derivation $d/dz : \mathbb{C}(z) \to \mathbb{C}(z)$. Consider some complex number $z_0$ which is not a pole of $A(z)$. According to Cauchy's theorem, there exists $\mathfrak{Y}(z) \in \mathrm{GL}_n(\mathbb{C}\{z-z_0\})$ such that

$$\mathfrak{Y}'(z) = A(z)\mathfrak{Y}(z)$$

(we have denoted by $\mathbb{C}\{z-z_0\}$ the ring of analytic functions near $z_0$). The analogue of the splitting field of the polynomial $P(X)$ over $\mathbb{Q}$ is the field extension

$$K = \mathbb{C}(z)(\mathfrak{Y}(z))$$

of $\mathbb{C}(z)$ generated by the entries of $\mathfrak{Y}(z)$. Note that $K$ is stable by the usual derivation $d/dz$, which is an extension of the derivation $d/dz$ attached to the base field $\mathbb{C}(z)$. The field $K$ endowed with the derivation $d/dz : K \to K$ is called a Picard-Vessiot field for $Y'(z) = A(z)Y(z)$ over $\mathbb{C}(z)$. The corresponding differential Galois group of $Y'(z) = A(z)Y(z)$ over $\mathbb{C}(z)$ is then made of the field automorphisms $\sigma$ of $K$ such that

$$\sigma_{|\mathbb{C}(z)} = \mathrm{Id}_{\mathbb{C}(z)} \text{ and } \sigma \circ d/dz = d/dz \circ \sigma.$$

The commutation condition ensures that any element of the differential Galois group transforms any solution of $Y'(z) = A(z)Y(z)$ with coefficients in $K$ into another solution : for any element $\sigma$ of the differential Galois group and for all $F \in M_{n,1}(K)$ such that $F'(z) = A(z)F(z)$, we have $\sigma(F)'(z) = A(z)\sigma(F)(z)$.

**Ex. 2** — Let $\sigma$ be a field automorphism of $K$ such that $\sigma_{|\mathbb{C}(z)} = \mathrm{Id}_{\mathbb{C}(z)}$. Prove that the following properties are equivalent :
—$\sigma$ transforms any solution of $Y'(z) = A(z)Y(z)$ with coefficients in $K$ into another solution;
—$\sigma \circ d/dz = d/dz \circ \sigma$.

2.3. **Toward difference Galois groups.** Can we extend the construction of Section 2.2 to other linear functional equations? Let us consider this question for very simple difference systems of rank one of the form

$$y(z+1) = a(z)y(z) \text{ with } a(z) \in \mathbb{C}(z)^{\times}.$$

The base field is still $\mathbb{C}(z)$, but the role played by the derivation $d/dz$ in Section 2.2 is now played by the field automorphism $\tau$ of $\mathbb{C}(z)$ defined by $\tau : f(z) \mapsto f(z+1)$. Inspired by Section 2.2, it seems natural to look for a field extension $K$ of $\mathbb{C}(z)$ such that :

(1) $K$ can be endowed with a field automorphism extending $\tau$, still denoted by $\tau$;
(2) there exists $\mathfrak{y} \in K^{\times}$ such that
$$\tau(\mathfrak{y}) = a(z)\mathfrak{y};$$
(3) $K$ is minimal for the above properties *i.e.*
$$K = \mathbb{C}(z)(\mathfrak{y});$$

and, then, to define the difference Galois group of $y(z+1) = a(z)y(z)$ over $\mathbb{C}(z)$ as the group made of the field automorphisms $\sigma$ of $K$ such that

$$\sigma_{|\mathbb{C}(z)} = \mathrm{Id}_{\mathbb{C}(z)} \text{ and } \sigma \circ \tau = \tau \circ \sigma.$$

Let us first study the case $a(z) = 1$ *i.e.* the equation

$$y(z+1) = y(z).$$

Note that

$$\mathfrak{y}(z) = 1 \text{ and } K = \mathbb{C}(z)(\mathfrak{y}(z)) = \mathbb{C}(z)$$

endowed with $\tau : f(z) \mapsto f(z+1)$ have the required properties. It is easily seen that the corresponding difference Galois group is trivial *i.e.* reduced to $\{\mathrm{Id}_{\mathbb{C}(z)}\}$. This is coherent with fact that the equation $y(z+1) = y(z)$ is the simplest possible ("trivial").

However, the choice $\mathfrak{y}(z) = 1$ may seem somewhat arbitrary. For instance, one could have chosen $\mathfrak{y}(z) = \sin(2\pi z)$ instead of 1 and $K = \mathbb{C}(z)(\mathfrak{y}(z))$ endowed with $\tau : f(z) \mapsto f(z+1)$. The corresponding difference Galois group contains a subgroup isomorphic to $\mathrm{PGL}_2(\mathbb{C})$ (*i.e.* the automorphisms of $K$ defined by $r(z, \mathfrak{y}(z)) \mapsto r(z, \frac{a\mathfrak{y}(z)+b}{c\mathfrak{y}(z)+d})$ with $a, b, c, d \in \mathbb{C}$ such that $ad - bc \neq 0$). This is not reasonable and not coherent with what precedes... Actually, the problem is that, in the process of going from $\mathbb{C}(z)$ to $K$ by adjoining $\mathfrak{y} = \sin(2\pi z)$, we have introduced new constants *i.e.* elements of $K$ fixed by $\tau$ which do not belong to the base field $\mathbb{C}(z)$ (or, equivalently, to $\mathbb{C}$). This leads us to require the further condition that

(4) $K^{\tau} := \{f \in K \mid \tau(f) = f\}$ must be equal to $\mathbb{C}$.

This condition excludes the choice $\mathfrak{y}(z) = \sin(2\pi z)$.

Let us now consider the case $a(z) = -1$ *i.e.* the equation

$$y(z+1) = -y(z).$$

We claim that, in this case, it is impossible to find a field $K$ satisfying to the conditions (1) to (4) above. Indeed, assume at the contrary that such a field $K$ exists. Then, $\mathfrak{y}^2$ is fixed by $\tau$ and hence belongs to $\mathbb{C}$. Therefore, $\mathfrak{y}$ belongs to $\mathbb{C}$. This is a contradiction: the equation $\tau(\mathfrak{y}) = -\mathfrak{y}$ does not have any solution in $\mathbb{C}(z)$.

Actually, we will have to work with rings and to accept zero divisors. More precisely, the basic objects will be rings endowed with an automorphism : these will be called difference rings. In the present case, we will see that a correct analogue of the splitting field is given by the quotient ring $\mathbb{C}(z)[X, X^{-1}]/(X^2 - 1)$ endowed with its unique ring automorphism $\phi$ such that $\phi_{|\mathbb{C}(z)} = \tau$ and $\phi(\overline{X}) = -\overline{X}$.

2.4. **Organization of the lecture notes.** Section 4 is devoted to the difference rings. The analogue(s) for difference equations of the splitting fields of Section 2.1, called Picard-Vessiot rings and total Picard-Vessiot rings, are defined and studied in Section 5. The difference Galois groups are introduced in Section 6, where their first properties are studied. This study is pursued in Section 7 (where we describe the algebraic relations between the solutions of difference equations in terms of the difference Galois groups) and in Section 8 (devoted to the Galois correspondence). In section 9, we focus our attention on regular $q$-difference systems. In Section 9.2, we introduce Birkhoff's connection matrices and explain their galoisian meaning. In Section 9.3, we consider the $q$-difference equations as deformations of differential systems and explain in which sense the connection matrices deform the monodromy representations attached to differential equations. Section 10 is concerned with the explicit calculation of difference Galois groups (mainly references). Section 11 is a brief introduction to parameterized difference Galois theory.

## 3. A table of analogies

The following table summarizes some analogies between the classical Galois theory and difference Galois theory. The concepts in the right hand column will be introduced in the next sections.

| Galois theory | Difference Galois theory |
|---|---|
| Polynomial equations | Difference equations |
| Rings | Difference rings |
| Fields | Difference fields |
| Splitting fields | Picard-Vessiot rings and total Picard-Vessiot rings |
| Galois groups | Difference Galois groups |
| Finite groups | Linear algebraic groups |

## 4. Difference rings and difference fields

**Definition 1.** *A difference ring is a couple $(R, \phi)$ where $R$ is a ring and $\phi$ is a ring automorphism of $R$. If $R$ is a field, then $(R, \phi)$ is called a difference field.*

**Example 2.** *The couple $(R, \phi)$ is a difference ring in the following cases :*

*(1) any ring $R$ and $\phi = \mathrm{Id}_R$;*

*(2) $R = \mathbb{C}(z)$ and $\phi : f(z) \mapsto f(qz)$ where $q \in \mathbb{C}^\times$;*

*(3) $R = \mathbb{C}(z)$ and $\phi : f(z) \mapsto f(z+1)$;*

*(4) $R = \cup_{j \geq 0} \mathbb{C}(z^{p^{-j}})$ and $\phi : f(z) \mapsto f(z^p)$ where $p$ is a positive integer. Note that $\mathbb{C}(z)$ endowed with $\phi : f(z) \mapsto f(z^p)$ is not a difference field because $\phi$ is not surjective.*

*(5) $R = \mathbb{C}^{\mathbb{Z}}$ and $\phi : (x_n)_{n \in \mathbb{Z}} \mapsto (x_{n+1})_{n \in \mathbb{Z}}$.*

**Definition 3.** *Let $(R, \phi)$ be a difference ring. An ideal $I$ of $R$ such that $\phi(I) \subset I$ is called a difference ideal of $(R, \phi)$. We say that $(R, \phi)$ is a simple difference ring if its difference ideals are $\{0\}$ and $R$.*

**Ex. 3** — Let $(R, \phi)$ be a difference ring. Let $I$ be a maximal difference ideal of $(R, \phi)$ *i.e.* a proper difference ideal of $(R, \phi)$ which is maximal among the difference ideals of $(R, \phi)$ (be careful, $I$ is not necessarily a maximal ideal). Prove that $\phi(I) = I$.

**Ex. 4** — Let $I$ be a difference ideal of the difference ring $(R, \phi)$. Then, $\phi$ induces a ring endomorphism $\overline{\phi}$ of $R/I$.

Prove that $(R/I, \overline{\phi})$ is a difference ring if and only if $\phi(I) = I$.

**Ex. 5** — Let $(R, \phi)$ be a difference ring.

1. Prove that if $R$ is a noetherian ring and if $I$ is a difference ideal of $(R, \phi)$ then $\phi(I) = I$.
2. Give an example of difference ring $(R, \phi)$ such that $\phi(I) \subsetneq I$.

**Example 4.** *(1) Any difference field is a simple difference ring.*

*(2) Let $\Gamma(z)$ be Euler's Gamma function. Recall that*

$$\Gamma(z+1) = z\Gamma(z).$$

*Consider the difference ring $(R, \phi)$ with $R = \mathbb{C}(z)[\Gamma(z), \Gamma(z)^{-1}]$ and $\phi : f(z) \mapsto f(z+1)$. We claim that $(R, \phi)$ is a simple difference ring. Indeed, let $I$ be a non zero difference ideal of $(R, \phi)$. Note that $R$ is a principal ideal domain (in particular, it is noetherain, so $\phi(I) = I$ according to exercise 5). Let $P(z, Y) \in \mathbb{C}(z)[Y, Y^{-1}] \setminus \{0\}$ be such that $I = (P(z, \Gamma(z)))$. We have $\phi(I) = (P(z+1, z\Gamma(z)))$. Since $\phi(I) = I$, we get $P(z+1, z\Gamma(z)) = c(z)\Gamma(z)^i P(z, \Gamma(z))$ for some $c(z) \in \mathbb{C}(z)^\times$ and $i \in \mathbb{Z}$. It follows easily that $P(z, Y)$ is a monomial in $Y$. So $P(z, \Gamma(z)) \in R^\times$ and, hence, $I = R$.*

*(3) The difference ring $(R, \phi)$ with $R = \mathbb{C}(z)[\Gamma(z)]$ and $\phi : f(z) \mapsto f(z+1)$ is not a simple difference ring. Indeed, $(\Gamma(z))$ is a proper non trivial difference ideal.*

**Definition 5.** *A morphism (resp. isomorphism) from the difference ring* $(R, \phi)$ *to the difference ring* $(\widetilde{R}, \widetilde{\phi})$ *is a ring morphism (resp. isomorphism)* $\varphi : R \to \widetilde{R}$ *such that* $\varphi \circ \phi = \widetilde{\phi} \circ \varphi$.

**Ex. 6 —** Prove that, for difference rings, "being isomorphic" is an equivalence relation.

**Ex. 7 —** We have already seen that $\mathbb{C}(z)$ endowed with the ring automorphism $\sigma_q : f(z) \mapsto f(qz)$ ($q \in \mathbb{C}^\times$) or $\tau : f(z) \mapsto f(z+1)$ is a difference field. Prove that, up to isomorphism, these are the only difference fields of the form $(\mathbb{C}(z), \phi)$.

**Definition 6.** *A difference ring* $(\widetilde{R}, \widetilde{\phi})$ *is a difference ring extension of a difference ring* $(R, \phi)$ *if* $\widetilde{R}$ *is a ring extension of* $R$ *and if* $\widetilde{\phi}_{|R} = \phi$*; in this case, we will often denote* $\widetilde{\phi}$ *by* $\phi$.

*A difference ring* $(R, \phi)$ *is a difference subring of a difference ring* $(\widetilde{R}, \widetilde{\phi})$ *if* $(\widetilde{R}, \widetilde{\phi})$ *is a difference ring extension of* $(R, \phi)$.

*Two difference ring extensions* $(\widetilde{R}_1, \widetilde{\phi}_1)$ *and* $(\widetilde{R}_2, \widetilde{\phi}_2)$ *of a difference ring* $(R, \phi)$ *are isomorphic over* $(R, \phi)$ *if there exists a difference ring isomorphism* $\varphi$ *from* $(\widetilde{R}_1, \widetilde{\phi}_1)$ *to* $(\widetilde{R}_2, \widetilde{\phi}_2)$ *such that* $\varphi_{|R} = \mathrm{Id}_R$.

**Definition 7.** *The ring of constants* $R^\phi$ *of the difference ring* $(R, \phi)$ *is defined by*

$$R^\phi := \{f \in R \mid \phi(f) = f\}.$$

**Ex. 8 —** Let $(R, \phi)$ be a difference ring.

1. Prove that the ring of constants $R^\phi$ is a ring (!).
2. Prove that if $R$ is a field then $R^\phi$ is a field.

**Ex. 9 —** Let $(k', \phi)$ be a difference field extension of a difference field $(k, \phi)$.

1. Prove that if $k'$ is an algebraic extension of $k$, then ${k'}^\phi$ is an algebraic extension of $k^\phi$. In particular, if $k'$ is an algebraic extension of $k$ and if $k^\phi$ is algebraically closed, then ${k'}^\phi = k^\phi$.
2. Prove that if $k$ is algebraically closed, then $k^\phi$ is not necessary algebraically closed.

**Ex. 10 —** Let $(k, \phi)$ be a difference field. Prove that $\phi$ can be extended into a ring automorphism of $\overline{k}$. In other words, $\overline{k}$ can be endowed with a structure of difference field extension of $(k, \phi)$.

In what follows, we will frequently denote the difference ring $(R, \phi)$ by $R$.

## 5. Picard-Vessiot theory

Let $(k, \phi)$ be a difference field and denote by $C := k^\phi$ its field of constants.

5.1. **Picard-Vessiot rings.** Consider a difference system

$$\phi(Y) = AY \text{ with } A \in \mathrm{GL}_n(k). \tag{1}$$

**Definition 8.** *A Picard-Vessiot ring for (4) over* $(k, \phi)$ *is a difference ring extension* $R$ *of* $(k, \phi)$ *such that*

*1) there exists $\mathfrak{Y} \in \mathrm{GL}_n(R)$ such that $\phi(\mathfrak{Y}) = A\mathfrak{Y}$ (such a $\mathfrak{Y}$ is called a fundamental matrix of solutions of (4));*
*2) $R$ is generated, as a $k$-algebra, by the entries of $\mathfrak{Y}$ and $\det(\mathfrak{Y})^{-1}$;*
*3) $R$ is a simple difference ring.*

The Picard-Vessiot rings will play the same role as the splitting fields in classical Galois theory.

We shall now address the following questions :

(1) Do Picard-Vessiot rings exist?

(2) Are Picard-Vessiot extensions unique?

The answer to the first question is given by the following result.

**Proposition 9** ([vdPS97, §1.1])**.** *There exists a Picard-Vessiot ring for (4) over $(k,\phi)$.*

*Proof.* We shall first construct a difference ring extension of $(k,\phi)$ satisfying to conditions 1) and 2) of definition 8. We let $X = (X_{i,j})_{1\leq i,j\leq n}$ be a matrix of indeterminates and we consider the ring $k[X,\det(X)^{-1}]$ of polynomials with coefficients in $k$, in $n^2$ indeterminates, and localized at $\det(X)$. We consider the unique difference ring extension $(k[X,\det(X)^{-1}],\psi)$ of $(k,\phi)$ defined by $\psi(X) = AX$. The first two conditions of definition 8 are satisfied by $(k[X,\det(X)^{-1}],\psi)$, but not necessarily the last one.

**Example 10.** *(1) Consider the case $k = \mathbb{C}(z)$, $\phi : f(z) \mapsto f(qz)$, $q \in \mathbb{C}^\times$, and $A(z) = -1 \in \mathrm{GL}_1(\mathbb{C})$. Then, the difference ring $(k[X,\det(X)^{-1}] = k[X,X^{-1}],\psi)$ is not simple. For instance, $(X^2-1)$ is a proper non trivial difference ideal.*

*(2) Consider the case $k = \mathbb{C}(z)$, $\phi : f(z) \mapsto f(qz)$, $q \in \mathbb{C}^\times$, and $A(z) = q^{1/2} \in \mathrm{GL}_1(\mathbb{C})$. Then, the difference ring $(k[X,\det(X)^{-1}] = k[X,X^{-1}],\psi)$ is not simple. For instance, $(X^2-z)$ is a proper non trivial difference ideal.*

*(3) Consider the case $k = \mathbb{C}(z)$, $\phi : f(z) \mapsto f(qz)$, $q \in \mathbb{C}^\times$, and $A(z) = z \in \mathrm{GL}_1(\mathbb{C})$. Then, the difference ring $(k[X,\det(X)^{-1}] = k[X,X^{-1}],\psi)$ is simple. Indeed, let $I$ be a non zero difference ideal. Let $P(z,X) \in k[X,\det(X)^{-1}]$ be such that $I = (P(z,X))$. Since $(P(qz,zX)) = \psi(I) = I = (P(X))$, there exists $c(z) \in k^\times$ and $i \in \mathbb{Z}$ such that $P(qz,zX) = c(z)X^iP(z,X)$. So, $i = 0$ and it is easily seen that $P(z,X)$ is a monomial in $X$ and, hence, is invertible in $k[X,\det(X)^{-1}]$. Thus, $I = k[X,\det(X)^{-1}]$.*

In order to remedy this problem, we consider a maximal difference ideal $I$ of $R$ *i.e.* a proper difference ideal of $R$ which is maximal among the difference ideals of $R$ (be careful, $I$ is not necessarily a maximal ideal) and we consider the difference ring extension

$$(R,\phi) = (k[X,\det(X)^{-1}]/I,\overline{\psi})$$

of $(k,\phi)$ where $\phi = \overline{\psi} : R \to R$ is the ring automorphism induced by $\psi$ (see exercises 3 and 4). It is clear that the first two conditions of definition 8 are satisfied by $(R,\phi)$. Moreover, the 1-1 correspondance between the difference ideals of $k[X, \det(X)^{-1}]/I$ and the difference ideals of $k[X, \det(X)^{-1}]$ containing $I$ (see exercise 4) shows that $(R, \phi)$ is a simple difference ring. This concludes the proof of the existence of the Picard-Vessiot rings.

**Example 11.** *(1) We come back to the case $k = \mathbb{C}(z)$, $\phi : f(z) \mapsto f(qz)$, $q \in \mathbb{C}^{\times}$, $A(z) = -1 \in \mathrm{GL}_1(\mathbb{C})$. Then, $(X^2-1)$ is a maximal difference ideal of $(k[X, X^{-1}], \psi)$. Indeed, the proper ideals of $k[X, X^{-1}]$ containing $(X^2-1)$ are $(X-1)$ and $(X+1)$ and none of them is stable by $\phi$. Therefore, a Picard-Vessiot ring is given by $(k[X, X^{-1}]/(X^2-1), \overline{\psi})$.*

*(2) We come back to the case $k = \mathbb{C}(z)$, $\phi : f(z) \mapsto f(qz)$, $q \in \mathbb{C}^{\times}$, $A(z) = q^{1/2} \in \mathrm{GL}_1(\mathbb{C})$. Then, $(X^2 - z)$ is a maximal ideal of $k[X, X^{-1}]$ (because $X^2 - z$ is irreducible) and, hence, a maximal difference ideal of $(k[X, X^{-1}], \psi)$. Therefore, a Picard-Vessiot ring is given by $(k[X, X^{-1}]/(X^2 - z), \overline{\psi})$, which is isomorphic over $(k, \phi)$ to $k[z^{1/2}, z^{-1/2}]$ endowed with the automorphism $f(z^{1/2}) \mapsto f(q^{1/2}z^{1/2})$.*

*(3) We come back to the case $k = \mathbb{C}(z)$, $\phi : f(z) \mapsto f(qz)$, $q \in \mathbb{C}^{\times}$, $A(z) = z \in \mathrm{GL}_1(\mathbb{C})$. Then, a Picard-Vessiot ring is given by $(k[X, X^{-1}], \psi)$.*

□

Note the following fundamental property of the Picard-Vessiot rings:

**Proposition 12** ([vdPS97, Lemma 1.18])**.** *Assume that the characteristic of $k$ is $0$ and that $C$ is algebraically closed. Then, for any Picard-Vessiot ring $R$ for (4) over $(k, \phi)$, we have*

$$R^{\phi} = C.$$

This is coherent with the discussion of Section 2. We will see later, in proposition 20, another characterization of the Picard-Vessiot rings very close to the spirit of the discussion of Section 2.

Our question concerning uniqueness is answered by the following result.

**Theorem 13** ([vdPS97, Proposition 1.19])**.** *Assume that the characteristic of $k$ is $0$ and that $C$ is algebraically closed. Then, any two Picard-Vessiot rings for (4) over $(k, \phi)$ are isomorphic over the difference ring $(k, \phi)$.*

**Remark 14.** *If $C$ is not algebraically closed, then the previous two results may fail. Indeed, let us come back to the case $k = \mathbb{C}(z)$, $\phi : f(z) \mapsto f(qz)$, $A(z) = -1 \in \mathrm{GL}_1(\mathbb{C})$ in the special case $q = -1$. Then $\mathbb{C}(z)^{\phi} = \mathbb{C}(z^2)$ is not algebraically closed. The proof of theorem 9 yields the Picard-Vessiot ring $(R, \phi) = (\mathbb{C}(z)[X, X^{-1}]/(X^2-1), \phi)$ where $\phi$ is determined by $\phi(\overline{X}) = -\overline{X}$. This difference ring has new constants with respect to the base difference field $(k, \phi)$ e.g. $\overline{zX}$ belongs to $R^{\phi}$ but not to $k^{\phi} = \mathbb{C}(z)^{\phi} = \mathbb{C}(z^2)$. On the other hand, $\mathbb{C}(z)$ endowed with $\phi$ is itself is a Picard-Vessiot ring for $\phi(y) = -y$ over $k$ (because $z$ is a fundamental matrix of solutions of $\phi(y) = -y$). The two difference rings $R$ and $k$ are not isomorphic.*

**Hypothesis 1.** *From now on, we assume that the characteristic of $k$ is $0$ and that $C$ is algebraically closed.*

We shall now study the structure of the Picard-Vessiot rings in more details. We start with an example.

**Example 15.** *We pursue the study of the example $k = \mathbb{C}(z)$, $\phi : f(z) \mapsto f(qz)$, $q \in \mathbb{C}^\times$, and $A(z) = -1 \in \mathrm{GL}_1(\mathbb{C})$. A Picard-Vessiot ring is given by the unique difference ring extension $(R, \phi) = (k[X, X^{-1}]/(X^2 - 1), \phi)$ of $(k, \phi)$ such that $\phi(\overline{X}) = -\overline{X}$. Note that $R$ is not a domain, so that the Picard-Vessiot rings are not integral domains in general (in particular, it is in general impossible to realize the Picard-Vessiot rings as subrings of some field of meromorphic functions). Letting $R'_0 = k[X, X^{-1}]/(X - 1)$ and $R'_1 = k[X, X^{-1}]/(X + 1)$, the Chinese reminders theorem ensures that*

$$\begin{array}{rcl} f : R & \to & R'_0 \oplus R'_1 = R' \\ \overline{P} & \mapsto & (\widehat{P}, \widetilde{P}) \end{array}$$

*is a ring isomorphism. This is even a difference ring isomorphism if $R'$ is endowed with the automorphism*

$$\phi' = f \circ \phi \circ f^{-1}.$$

*We let $e'_0 = (\widehat{1}, \widetilde{0}) = f(\frac{X+1}{2}) \in R'_0 \oplus R'_1$ and $e'_1 = (\widehat{0}, \widetilde{1}) = f(\frac{-X+1}{2}) \in R'_0 \oplus R'_1$. We have*

$$R'_0 = R'e'_0 \text{ and } R'_1 = R'e'_1.$$

*Moreover, we have*

$$\phi'(e'_0) = f \circ \phi \circ f^{-1}(e'_0) = f(\phi(\frac{X+1}{2})) = f(\frac{-X+1}{2}) = e'_1$$

*and*

$$\phi'(e'_1) = f \circ \phi \circ f^{-1}(e'_1) = f(\phi(\frac{-X+1}{2})) = f(\frac{X+1}{2}) = e'_0.$$

*So, letting $R_0 = f^{-1}(R'_0)$, $e_0 = f^{-1}(e'_0)$ and $R_1 = f^{-1}(R'_1)$, $e_1 = f^{-1}(e'_1)$, we have decomposed $R$ as a direct product of rings*

$$R = R_0 \oplus R_1 \text{ with } R_i = Re_i$$

*where*

- *$e_0$ and $e_1$ are idempotent elements of $R$,*
- *$R_0$ and $R_1$ are integral domains,*
- *$\phi(e_0) = e_1$ and $\phi(e_1) = e_0$, hence, $\phi(R_0) = R_1$ and $\phi(R_1) = R_0$.*

**Remark 16.** *In the case $k = \mathbb{C}(z)$, $\phi : f(z) \mapsto f(qz)$, $q \in \mathbb{C}^\times$, $A(z) = q^{1/2}$ or $z \in \mathrm{GL}_1(\mathbb{C})$, the Picard-Vessiot rings described in example 11 are integral domains.*

Actually, the property discovered in the previous example is a special case of a general fact.

**Theorem 17** ([vdPS97, Corollary 1.16])**.** *We can decompose $R$ as a direct product of rings*

$$R = \oplus_{x \in X} R_x \text{ with } R_x = Re_x$$

*where*

- *$X = \mathbb{Z}/t\mathbb{Z}$ for some integer $t \geq 1$,*
- *for all $x \in X$, $e_x$ is an idempotent element of $R$ (and, hence, $e_x = 1_{R_x}$),*
- *for all $x \in X$, $R_x$ is an integral domain,*
- *for all $x \in X$, $\phi(e_x) = e_{x+1_X}$ and, hence, $\phi(R_x) = R_{x+1_X}$.*

5.2. **Total Picard-Vessiot rings.** We maintain the notations and hypotheses of the previous section. In particular, we assume that $k$ has characteristic 0 and that $C$ is algebraically closed. We let $R$ be a Picard-Vessiot ring over $k$ attached to the system (4). Since $R$ is not necessary an integral domain, we cannot consider its field of fractions in general. But, we can consider its total ring of fractions $K$ *i.e.*

$$K = S^{-1}R$$

where $S$ is the multiplicative subset of $R$ made of the non zero divisors (if $R$ is an integral domain, then $K$ is nothing but the field of fractions of $R$). Recall that

$$S^{-1}R = R \times R / \sim$$

where $\sim$ is the equivalence relation on $R \times R$ defined by

$$(r, s) \sim (r', s') \Leftrightarrow \exists t \in S, t(rs' - r's) = 0.$$

The equivalence class of $(r, s)$ will be denoted by $r/s$. There is a natural ring structure on $S^{-1}R$ given by

$$r/s + r'/s' = (rs' + r's)/(ss') \text{ and } (r/s)(r'/s') = (rr')/(ss').$$

Moreover, $\phi : R \to R$ admits a unique extension into a ring automorphism $\phi : K \to K$, and it is given by

$$\phi(r/s) = \phi(r)/\phi(s).$$

**Definition 18.** *In this way, $K$ is a difference ring extension of $R$, called the total Picard-Vessiot ring of (4) over $(k, \phi)$.*

In the process of taking the total quotient ring, we have not increased the ring of constants:

**Proposition 19.** *We have $K^{\phi} = C$.*

*Proof.* Indeed, consider $r/s \in K^{\phi}$. Then, $I = \{a \in R \mid ar/s \in R\}$ is a difference ideal of $R$ containing $s$, so $I = R$. In particular, $1 \in I$ and hence $r/s \in R$. Therefore, $K^{\phi} = R^{\phi} = C$. □

We consider a decomposition of $R$ as given by theorem 17 :

$$R = \oplus_{x \in X} R_x.$$

It is easily seen that $K$ can be identified with the direct product of fields

$$K = \oplus_{x \in X} K_x$$

where $K_x$ is the field of fractions of $R_x$.

Collecting the previous results, we obtain the direct implication of the following result, which gives a new characterization of the Picard-Vessiot rings; for the proof of the other implication, we refer to [vdPS97, Corollary 1.24].

**Proposition 20** ([vdPS97, Corollary 1.24])**.** *Let $R$ be a difference ring extension of $(k, \phi)$. Then, $R$ is a Picard-Vessiot ring for (4) if and only if the following properties hold:*

*(1) $R$ has no nilpotent element;*

*(2) the ring of constants of the total quotient ring of $R$ (i.e. of the associated total Picard-Vessiot ring) is $C$;*

*(3) there exists $\mathfrak{Y} \in \mathrm{GL}_n(R)$ such that $\phi(\mathfrak{Y}) = A\mathfrak{Y}$*

*(4) $R$ is minimal with respect to the above properties.*

**Remark 21.** *In the previous result, it is important to consider the ring of constants of the total Picard-Vessiot ring associated to $R$, and not only of the Picard-Vessiot ring $R$; see* [vdPS97, Example 1.25].

## 6. Difference Galois groups

Let $(k, \phi)$ be a difference field. We assume that $k$ is of characteristic 0 and that the field of constants $C := k^{\phi}$ is algebraically closed.

Consider a difference system

$$\phi(Y) = AY \text{ with } A \in \mathrm{GL}_n(k). \tag{2}$$

We let $R$ be a Picard-Vessiot ring for this system over $k$, and we denote by $K$ the corresponding total Picard-Vessiot ring.

**Definition 22.** *The corresponding difference Galois group $\mathrm{Gal}^{\phi}(R/k)$ over $(k, \phi)$ of (2) is the group of the $k$-linear ring automorphisms of $R$ commuting with $\phi$ :*

$$\mathrm{Gal}^{\phi}(R/k) := \{\sigma \in \mathrm{Aut}(R/k) \mid \phi \circ \sigma = \sigma \circ \phi\}.$$

**Example 23.** *(1) We come back to the case $k = \mathbb{C}(z)$, $\phi : f(z) \mapsto f(qz)$, $q \in \mathbb{C}^{\times}$ not a root of the unity, $A(z) = -1 \in \mathrm{GL}_1(\mathbb{C})$. We recall that a Picard-Vessiot ring is given by $(R, \phi) = (k[X, X^{-1}]/(X^2 - 1), \phi)$ where $\phi$ is determined by $\phi(\overline{X}) = -\overline{X}$. Let $\sigma \in \mathrm{Gal}^{\phi}(R/k)$. Then, we have $\phi(\sigma(\overline{X})) = \sigma(\phi(\overline{X})) = \sigma(-\overline{X}) = -\sigma(\overline{X})$. Therefore, there exists $c \in k^{\phi} = \mathbb{C}$ such that $\sigma(\overline{X}) = c\overline{X}$. Moreover, we have $\overline{X}^2 = 1 \in k$ so $\sigma(\overline{X})^2 = \sigma(\overline{X}^2) = \sigma(1) = 1$ i.e. $c^2\overline{X}^2 = c^2 = 1$ and, hence, $c = \pm 1$. It follows that $\mathrm{Gal}^{\phi}(R/k) \subset \{\mathrm{Id}_R, \sigma\}$ where $\sigma$ is the unique automorphism of $R/k$ such that $\sigma(\overline{X}) = -\overline{X}$. It is easily seen that this inclusion is actually an equality.*

*(2) We come back to the case $k = \mathbb{C}(z)$, $\phi : f(z) \mapsto f(qz)$, $q \in \mathbb{C}^{\times}$ not a root of the unity, $A(z) = q^{1/2} \in \mathrm{GL}_1(\mathbb{C})$. We recall that a Picard-Vessiot ring is given by $R = k[z^{1/2}, z^{-1/2}]$ endowed with the automorphism $f(z^{1/2}) \mapsto f(q^{1/2}z^{1/2})$. Arguing as in the previous example, one can prove that $\mathrm{Gal}^{\phi}(R/k) = \{\mathrm{Id}_R, \sigma\}$ where $\sigma$ is the unique automorphism of $R/k$ such that $\sigma(z^{1/2}) = -z^{1/2}$.*

*(3) We come back to the case $k = \mathbb{C}(z)$, $\phi : f(z) \mapsto f(qz)$, $q \in \mathbb{C}^{\times}$ not a root of the unity, $A(z) = z \in \mathrm{GL}_1(\mathbb{C})$. Then, a Picard-Vessiot ring is given by $(R, \phi) = (k[X, X^{-1}], \phi)$, where $\phi$ is determined by $\phi(X) = zX$. Then, we have $\mathrm{Gal}^{\phi}(R/k) = \{\sigma_c \mid c \in \mathbb{C}^{\times}\}$ where $\sigma_c$ is the unique automorphism of $R/k$ such that $\sigma(X) = cX$.*

**Ex. 11** — Set

$$\mathrm{Gal}^{\phi}(K/k) := \{\sigma \in \mathrm{Aut}(K/k) \mid \phi \circ \sigma = \sigma \circ \phi\}.$$

Prove that the map

$$\begin{array}{rcl}\mathrm{Gal}^{\phi}(K/k) & \to & \mathrm{Gal}^{\phi}(R/k)\\ \sigma & \mapsto & \sigma_{|R}\end{array}$$

is well-defined (*i.e.* takes its values in $\mathrm{Gal}^{\phi}(R/k)$) and gives a group isomorphism between $\mathrm{Gal}^{\phi}(K/k)$ and $\mathrm{Gal}^{\phi}(R/k)$.

**Ex. 12** — What happens if we choose another Picard-Vessiot ring?

One can identify $\mathrm{Gal}^{\phi}(R/k)$ with a subgroup of $\mathrm{GL}_n(C)$ as follows (this is analogous to the identification of the Galois group of an algebraic equation to a group of permutations of its roots). Let $\mathfrak{Y} \in \mathrm{GL}_n(R)$ be a fundamental matrix of solutions of (2). For any $\sigma \in \mathrm{Gal}^{\phi}(R/k)$, there exists a unique $C(\sigma) \in \mathrm{GL}_n(C)$ such that

$$\sigma(\mathfrak{Y}) = \mathfrak{Y}C(\sigma).$$

Indeed, we have $\phi(\mathfrak{Y}) = A\mathfrak{Y}$ so $\sigma(\phi(\mathfrak{Y})) = \sigma(A\mathfrak{Y})$ and, hence, $\phi(\sigma(\mathfrak{Y})) = A\sigma(\mathfrak{Y})$. It follows that $\mathfrak{Y}^{-1}\sigma(\mathfrak{Y})$ is left invariant by $\phi$ and, hence, has coefficients in $C$. Moreover, $\det(\mathfrak{Y}^{-1}\sigma(\mathfrak{Y})) = \det(\mathfrak{Y})^{-1}\sigma(\det(\mathfrak{Y})) \in R^{\times}$. Therefore, $\mathfrak{Y}^{-1}\sigma(\mathfrak{Y})$ belongs to $M_n(C) \cap \mathrm{GL}_n(R) = \mathrm{GL}_n(C)$, as expected.

The proof of the following result is left as an exercise.

**Proposition 24.** *The map*

$$\begin{array}{rcl}\rho_{gal} : \mathrm{Gal}^{\phi}(R/k) & \to & \mathrm{GL}_n(C)\\ \sigma & \mapsto & C(\sigma)\end{array}$$

*is faithful linear representation of* $\mathrm{Gal}^{\phi}(R/k)$ *(i.e. an injective group morphism). Its image is denoted by* $G_{gal}$*.*

**Ex. 13** — What happens to $\rho_{gal}$ if we choose another fundamental matrix of solutions $\mathfrak{Y} \in \mathrm{GL}_n(R)$?

**Example 25.** *For the cases (1) to (3) considered in example 23, we have* $G_{gal} = \{\pm 1\}, \{\pm 1\}$ *and* $\mathbb{C}^{\times}$ *for the choices* $\mathfrak{Y} = \overline{X}, z^{1/2}$ *and* $X$ *respectively.*

We now come to a crucial property of the difference Galois groups.

**Theorem 26** ([vdPS97, Theorem 1.13])**.** *The image* $G_{gal}$ *of* $\rho_{gal}$ *is an algebraic subgroup of* $\mathrm{GL}_n(C)$*.*

Recall that this means that $G_{gal}$ is
— a subgroup of $\mathrm{GL}_n(C)$ and
— the zero-locus of a set of polynomials in $C[(X_{i,j})_{1\leq i,j\leq n}, \det X^{-1}]$.

## 7. Galois groups and algebraic relations

We let $(k,\phi)$ be a difference field. We assume that $k$ is of characteristic 0 and that the field of constants $C := k^{\phi}$ is algebraically closed.

Consider a difference system

$$\phi(Y) = AY \text{ with } A \in \mathrm{GL}_n(k). \tag{3}$$

We let $R$ be a Picard-Vessiot ring for this system over $k$. Let $\mathfrak{Y} \in \mathrm{GL}_n(R)$ be a fundamental matrix of solutions of (3). We denote by

$$\begin{array}{rcl} \rho_{gal} : \mathrm{Gal}^{\phi}(R/k) & \rightarrow & \mathrm{GL}_n(C) \\ \sigma & \mapsto & C(\sigma) \end{array}$$

the faithful linear representation attached to $\mathfrak{Y}$ as in Section 6, so that, for all $\sigma \in \mathrm{Gal}^{\phi}(R/k)$, $\sigma(\mathfrak{Y}) = \mathfrak{Y}C(\sigma)$. We set

$$G_{gal} = Im(\rho_{gal}).$$

The aim of this section is to give a precise meaning to the following assertion :

> "the difference Galois group $\mathrm{Gal}(R/k)$ measures the algebraic relations between the solutions of the difference system (3)".

We let $I$ be the ideal of the algebraic relations in $k[X, \det(X)^{-1}]$ between the entries of $\mathfrak{Y}$, *i.e.*, $I$ is the kernel of the unique $k$-algebra morphism $\varphi : k[X, \det(X)^{-1}] \rightarrow R$ such that $\varphi(X) = \mathfrak{Y}$. So, $I$ is a maximal difference ideal of $k[X, \det(X)^{-1}]$. We will use the following excercise in what follows.

**Ex. 14 —** Prove that $I$ is a radical ideal.

7.1. **The case when $k$ is algebraically closed.** We shall first assume that $k$ is algebraically closed.

We let $V$ be the $k$-algebraic subset of $\mathrm{GL}_n(k)$ defined by $I$ *i.e.*

$$V = \{v \in \mathrm{GL}_n(k) \mid \forall P(X) \in I, P(v) = 0\}.$$

We have a natural map

$$\begin{array}{rcl} V \times G_{gal} & \rightarrow & V \\ (v, M) & \mapsto & vM. \end{array}$$

Indeed, for any $(v, M = C(\sigma)) \in V \times G_{gal}$, we have, for all $P \in I$, $P(v) = 0$ so $P(vC(\sigma)) = P(\sigma(v)) = \sigma(P(v)) = 0$ so $vC(\sigma) \in V$. One deduces easily that we have the natural map

$$\begin{array}{rcl} V \times G_{gal}(k) & \rightarrow & V \\ (v, M) & \mapsto & vM \end{array}$$

where $G_{gal}(k)$ is the $C$-algebraic subgroup of $\mathrm{GL}_n(k)$ defined by the equations of $G_{gal}$ seen as an algebraic subgroup of $\mathrm{GL}_n(C)$. This group action is actually transitive :

**Theorem 27** ([vdPS97, Theorem 1.13])**.** *For all $v, w \in V$, there exists a unique $M \in G_{gal}(k)$ such that*

$$w = vM.$$

We denote by $J_C$ the ideal of $C[X, \det(X)^{-1}]$ defining $G_{gal}$, *i.e.*,

$$J_C = \{P(X) \in C[X, \det(X)^{-1}] \mid \forall M \in G_{gal}, P(M) = 0\}.$$

We denote by $J_k$ the ideal of $k[X, \det(X)^{-1}]$ defining $G_{gal}(k)$, *i.e.*,

$$J_k = \{P(X) \in k[X, \det(X)^{-1}] \mid \forall M \in G_{gal}(k), P(M) = 0\}.$$

We have

$$J_k = kJ_C.$$

Consider $v \in V$ ($V$ is non empty). Theorem 27 ensures that

$$V = vG_{gal}(k).$$

This yields the following description of the algebraic relations with coefficients in $k$ between the entries of $\mathfrak{Y}$ in terms of the algebraic equations defining the algebraic group $G_{gal}$ :

**Proposition 28.** *We have*

$$I = \{P(v^{-1}X) \mid P(X) \in J_k\} = \{P(v^{-1}X) \mid P(X) \in kJ_C\}.$$

**Example 29.** *For instance, if*

$$G_{gal} = \{M \in \mathrm{GL}_n(C) \mid (\det M)^m = 1\}$$

*for some positive integer $m$, then*

$$I = ((\det X)^m - \lambda)$$

*for some $\lambda = \det(v)^m \in k^\times$.*

**Ex. 15** — Another way to state this is that the $k$-algebras $C[G_{gal}] \otimes_C k$ and $R$ are isomorphic. Prove this and give an isomorphism.

7.2. **The general case.** We no longer assume that $k$ is algebraically closed. Then, the previous results are false in general, as shown by the following example.

**Example 30.** *Consider the case $k = \mathbb{C}(z)$, $\phi = \sigma_q$, $q \in \mathbb{C}^\times$ not a root of the unity, $\phi(y) = q^{1/2}y$. A Picard-Vessiot ring is given by $R = k[z^{1/2}, z^{-1/2}]$ with $\phi(z^{1/2}) = q^{1/2}z^{1/2}$. A fundamental solution is given by $\mathfrak{Y} = z^{1/2} \in$ $\mathrm{GL}_1(R)$. The Galois group is $G_{gal} = \{\pm 1\} \subset \mathrm{GL}_1(\mathbb{C})$ so that $C[G_{gal}] =$ $C[X, X^{-1}]/(X^2 - 1)$. Then, $R$ and $C[G_{gal}] \otimes_C k$ are not isomorphic since the former is an integral domain, but not the latter. However, these rings become isomorphic if we tensorize by $\overline{k}$ over $k$.*

Actually, we have the following result:

**Proposition 31** ([vdPS97, Theorem 1.13])**.** *We have*

$$\overline{k}I = \{P(v^{-1}X) \mid P \in \overline{k}J_C\}.$$

**Ex. 16** — Another way to state this is that the rings $C[G_{gal}] \otimes_C \overline{k}$ and $R \otimes_k \overline{k}$ are isomorphic. Prove this and give an isomorphism.

**Remark 32.** *Actually, what precedes can be (and must be) rephrased in terms of torsors.*

*In some circumstances, we do not need to go to $\overline{k}$. For instance, if $G_{gal}$ is connected and $k$ is a $\mathcal{C}^1$-field, then proposition 28 is true even if $k$ is not algebraically closed. (The $G_{gal} \otimes k$-torsors are trivial in this case.)*

## 8. Galois correspondence

Let $(k, \phi)$ be a difference field. We assume that $k$ is of characteristic 0 and that the field of constants $C := k^\phi$ is algebraically closed.

Consider a difference system

$$\phi(Y) = AY \text{ with } A \in \mathrm{GL}_n(k). \tag{4}$$

Let $R$ be a Picard-Vessiot ring for this system over $k$ and denote by $K$ the corresponding total Picard-Vessiot ring. We consider its difference Galois group $\mathrm{Gal}^{\phi}(R/k) = \mathrm{Gal}^{\phi}(K/k)$ (see exercise 11 for the identification between the two groups), endowed with its structure of linear algebraic group.

There is a Galois correspondence in difference Galois theory. Note that the total Picard-Vessiot rings are used instead of the Picard-Vessiot rings themselves.

**Theorem 33** ([vdPS97, Theorem 1.29])**.** *Let $\mathcal{F}$ be the set of difference subrings $F$ of $K$ such that $k \subset F$ and such that every non zero divisor of $F$ is actually a unit of $F$. Let $\mathcal{G}$ be the set of algebraic subgroups of $\mathrm{Gal}^{\phi}(K/k)$. Then,*

- *for any $F \in \mathcal{F}$, the set $G(K/F)$ of elements of $\mathrm{Gal}^{\phi}(K/k)$ which fix $F$ pointwise is an algebraic subgroup of $\mathrm{Gal}^{\phi}(K/k)$;*
- *for any algebraic subgroup $H$ of $\mathrm{Gal}^{\phi}(K/k)$, $K^H := \{f \in K \mid \forall \sigma \in H, \sigma(f) = f\}$ belongs to $\mathcal{F}$;*
- *the maps $\mathcal{F} \to \mathcal{G}$, $F \mapsto G(K/F)$ and $\mathcal{G} \to \mathcal{F}$, $H \mapsto K^H$ are each other's inverses.*

**Remark 34.** *Note that, if $R$ is an integral domain, then theorem 33 gives a correspondence between the difference subfields of $K$ containing $k$, on the one hand, and the algebraic subgroups of $\mathrm{Gal}^{\phi}(K/k)$, on the other hand.*

In particular, for any subgroup $H$ of $\mathrm{Gal}^{\phi}(K/k)$, if $K^H = k$, then $H$ is Zariski-dense in $\mathrm{Gal}^{\phi}(K/k)$. We will use this fact in Section 9.

We also have the following property: if $H$ is a normal algebraic subgroup of $\mathrm{Gal}^{\phi}(K/k)$, then the restriction morphism $\mathrm{Gal}^{\phi}(K/k) \to \mathrm{Gal}^{\phi}(K^H/k)$ induces an isomorphism $\mathrm{Gal}^{\phi}(K/k)/H \cong \mathrm{Gal}^{\phi}(K^H/k)$.

## 9. Galoisian ambiguities coming from analysis for regular $q$-difference equations

In this section, we study the Galois groups of the regular $q$-difference equations and their relationship with transcendental invariants introduced by Birkhoff, namely the connection matrices. The main references are Etingof's [Eti95] and Sauloy's [Sau00].

We shall first recall some classical facts concerning the monodromy of linear differential equations.

### 9.1. Monodromy and differential Galois groups.

Consider a linear differential system

$$Y'(z) = A(z)Y(z) \text{ with } A(z) \in \mathrm{M}_n(\mathbb{C}(z)). \tag{5}$$

Its set of singularities on $\mathbb{P}^1(\mathbb{C})$ is denoted by $S$.

We shall first recall the definition of the monodromy representation attached to this differential system. Let $z_0 \in \mathbb{P}^1(\mathbb{C})\setminus S$. According to Cauchy's theorem, there exists $\mathfrak{Y}(z) \in \mathrm{GL}_n(\mathcal{O}_{\mathbb{P}^1(\mathbb{C}),z_0})$ such that

$$\mathfrak{Y}'(z) = A(z)\mathfrak{Y}(z)$$

(we have denoted by $\mathcal{O}_{\mathbb{P}^1(\mathbb{C})}$ the sheaf of analytic functions over $\mathbb{P}^1(\mathbb{C})$ and by $\mathcal{O}_{\mathbb{P}^1(\mathbb{C}),z_0}$ its stalk at $z_0$). Let

$$\gamma : [0,1] \to \mathbb{P}^1(\mathbb{C}) \setminus S$$

be a continuous path such that $\gamma(0) = \gamma(1) = z_0$. It turns out that $\mathfrak{Y}(z)$ can be analytically continued along $\gamma$.

**Ex. 17** — Prove this !

After analytic continuation along $\gamma$, we get a new solution $\gamma\mathfrak{Y}(z) \in \mathrm{GL}_n(\mathcal{O}_{\mathbb{P}^1(\mathbb{C}),z_0})$ of $Y'(z) = A(z)Y(z)$. Therefore, there exists $M(\gamma) \in \mathrm{GL}_n(\mathbb{C})$ such that

$$\gamma\mathfrak{Y}(z) = \mathfrak{Y}(z)M(\gamma).$$

This matrix $M(\gamma)$ is called the monodromy matrix along $\gamma$ of the differential equation (5). This matrix only depends on the homotopy class of $\gamma$ in $\mathbb{P}^1(\mathbb{C}) \setminus S$. Therefore, we have a map

$$\begin{array}{rcl}\rho_{mono} : \pi_1(\mathbb{P}^1(\mathbb{C}) \setminus S, z_0) & \to & \mathrm{GL}_n(\mathbb{C}) \\ {[\gamma]} & \mapsto & M([\gamma]) := M(\gamma).\end{array}$$

This is a group morphism.

**Definition 35.** *The map $\rho_{mono}$ is a linear representation of $\pi_1(\mathbb{P}^1(\mathbb{C})\setminus S, z_0)$ called the monodromy representation.*

*Its image is called the monodromy group and denoted by $G_{mono}$.*

**Ex. 18** — We emphasize that the monodromy representation and group depends on the choice of $\mathfrak{Y}(z)$ and $z_0$. Study the dependence of the monodromy representation and group on $z_0$ and $\mathfrak{Y}(z)$.

On the other hand, we recall (see Section 2.2) that the differential Galois group of the differential system (5) can be described as

$$\mathrm{Gal}^{d/dz}(K/\mathbb{C}(z)) = \{\sigma \in Aut(K/\mathbb{C}(z)) \mid \sigma \circ d/dz = d/dz \circ \sigma\}$$

where

$$K = \mathbb{C}(z)(\mathfrak{Y}(z))$$

is the field generated over $\mathbb{C}(z)$ by the entries of $\mathfrak{Y}(z)$. We can realize $\mathrm{Gal}^{d/dz}(K/\mathbb{C}(z))$ as an algebraic subgroup $G_{gal}$ of $\mathrm{GL}_n(\mathbb{C})$ as follows (this is similar to what we did in Section 6). For any $\sigma \in \mathrm{Gal}^{d/dz}(K/\mathbb{C}(z))$, there exists a unique $C(\sigma) \in \mathrm{GL}_n(C)$ such that

$$\sigma(U) = UC(\sigma).$$

Then,

$$\begin{array}{rcl}\rho_{gal} : \mathrm{Gal}^{d/dz}(K/\mathbb{C}(z)) & \to & \mathrm{GL}_n(C) \\ \sigma & \mapsto & C(\sigma)\end{array}$$

is faithful linear representation of $\mathrm{Gal}^{d/dz}(K/\mathbb{C}(z))$ and its image, denoted by $G_{gal}$, is an algebraic subgroup of $\mathrm{GL}_n(\mathbb{C})$.

We shall now prove that the monodromy is Galoisian. Indeed, any element of $K$ can be continued meromorphically along any coninuous path $\gamma : [0,1] \to \mathbb{P}^1(\mathbb{C}) \setminus S$ such that $\gamma(0) = \gamma(1) = z_0$ (because the entries of

$\mathfrak{Y}(z)$ can be analytically continued along any such path). This induces an element $\sigma_\gamma$ of $\mathrm{Gal}^{d/dz}(K/\mathbb{C}(z))$ such that

$$C(\sigma_\gamma) = M(\gamma).$$

Therefore, we have proved the following result.

**Proposition 36.** *We have*

$$G_{mono} \subset G_{gal}.$$

In case the system is regular singular [1], the differential Galois group is "what algebra see of analysis" :

**Theorem 37** (Schlesinger; [vdPS03, Theorem 5.8])**.** *Assume that the differential system (5) is regular singular. Then, the monodromy group $G_{mono}$ is Zariski-dense in the Galois group $G_{gal}$.*

**Remark 38.** *If the system is irregular, then this result may be false. The typical counter-example is $y'(z) = y(z)$. There is an extension of this result to arbitrary linear differential equations due to Ramis.*

9.2. **Birkhoff connection matrices and difference Galois groups.** Let $q$ be a non zero complex number such that $|q| < 1$. We consider the difference field $(\mathbb{C}(z), \sigma_q)$ where $\sigma_q : f(z) \mapsto f(qz)$ and a $q$-difference system

$$\sigma_q Y = AY \text{ with } A \in \mathrm{GL}_n(\mathbb{C}(z)). \tag{6}$$

Note that $\mathbb{C}(z)$ is of characteristic 0 and that the field of constants $\mathbb{C}(z)^{\sigma_q} = \mathbb{C}$ is algebraically closed. Thus, we can apply most of the results of the previous sections.

In this section, we assume that the following hypothesis is satisfied:

**Hypothesis 2.** *The $q$-difference system (6) is regular at 0 and $\infty$, i.e., $A(z)$ is analytic at 0 and $\infty$ and*

$$A(0) = A(\infty) = I_n.$$

Our first task is to construct fundamental matrices of solutions attached to 0 and $\infty$.

The infinite product

$$\mathfrak{Y}_0(z) = A(z)^{-1}A(qz)^{-1}A(q^2z)^{-1}\cdots$$

defines an element of $\mathrm{GL}_n(\mathcal{O}_{\mathbb{P}^1(\mathbb{C}),0})$ such that

$$\mathfrak{Y}_0(qz) = A(z)\mathfrak{Y}_0(z) \text{ and } \mathfrak{Y}_0(0) = I_n.$$

This functional equation shows that $\mathfrak{Y}_0(z)$ can be extended into a meromorphic function over $\mathbb{C}$ :

$$\mathfrak{Y}_0(z) \in \mathrm{GL}_n(\mathcal{M}(\mathbb{C})).$$

We let

$$R_0 = \mathbb{C}(z)[\mathfrak{Y}_0(z), (\det(\mathfrak{Y}_0(z)))^{-1}]$$

be the $\mathbb{C}(z)$-algebra generated by the entries of $\mathfrak{Y}_0(z)$ and the inverse of its determinant. This ring has a natural structure of difference ring extension

1. This means that, for any $s \in S$, the growth of the entries of $\mathfrak{Y}(z)$ as $z$ tends to $s$ along any sector of finite aperture and centered at $s$ is at most polynomial.

of $(\mathbb{C}(z), \sigma_q)$. It is an integral domain, therefore its total Picard-Vessiot ring $K_0$ is nothing but the field of fractions of $R_0$ :

$$K_0 = \mathbb{C}(z)(\mathfrak{Y}_0(z)).$$

**Proposition 39** ([Eti95, Section 3]). *The difference ring $R_0$ is a Picard-Vessiot ring for the $q$-difference system (6) over $\mathbb{C}(z)$. Hence, the difference field $K_0$ is a total Picard-Vessiot ring for this system over $\mathbb{C}(z)$.*

*Proof.* We use the characterization of the Picard-Vessiot rings given by proposition 20. The only non trivial point is that $K_0^{\sigma_q} = \mathbb{C}$. This is true because any element $f$ of $K_0^{\sigma_q}$ is meromorphic over $\mathbb{C}$ and satisfies $f(qz) = f(z)$. In particular, $f(z)$ induces an analytic function over the compact Riemann surface $\mathbb{C}^\times/q^{\mathbb{Z}}$. Such a function is necessarily constant. It follows that $f(z)$ itself is constant over $\mathbb{C}^\times$ and, hence, over $\mathbb{C}$. □

We have similar results at $\infty$. Indeed,

$$\mathfrak{Y}_\infty(z) = A(q^{-1}z)A(q^{-2}z)A(q^{-3}z)\cdots$$

defines an element of $\mathrm{GL}_n(\mathcal{O}_{\mathbb{P}^1(\mathbb{C}),\infty})$ such that

$$\mathfrak{Y}_\infty(qz) = A(z)\mathfrak{Y}_\infty(z) \text{ and } \mathfrak{Y}_\infty(\infty) = I_n.$$

This functional equation shows that $\mathfrak{Y}_\infty(z)$ can be extended into a meromorphic function over $\mathbb{P}^1(\mathbb{C}) \setminus \{0\}$ :

$$\mathfrak{Y}_0(z) \in \mathrm{GL}_n(\mathcal{M}(\mathbb{P}^1(\mathbb{C}) \setminus \{0\})).$$

We let

$$R_\infty = \mathbb{C}(z)[\mathfrak{Y}_\infty(z), (\det(\mathfrak{Y}_\infty(z)))^{-1}]$$

be the $\mathbb{C}(z)$-algebra generated by the entries of $\mathfrak{Y}_\infty(z)$ and the inverse of its determinant. This ring has a natural structure of difference ring extension of $(\mathbb{C}(z), \sigma_q)$. It is an integral domain, therefore its total Picard-Vessiot ring $K_\infty$ is nothing but the field of fractions of $R_\infty$ :

$$K_\infty = \mathbb{C}(z)(\mathfrak{Y}_\infty(z)).$$

**Proposition 40** ([Eti95, Section 3]). *The difference ring $R_\infty$ is a Picard-Vessiot ring for the $q$-difference system (6) over $\mathbb{C}(z)$. Hence, the difference field $K_\infty$ is a total Picard-Vessiot ring for this system over $\mathbb{C}(z)$*

So, we have two Picard-Vessiot rings $R_0$ and $R_\infty$. Theorem 12 ensures that they are isomorphic as difference rings extensions of $(\mathbb{C}(z), \sigma_q)$. In order to describe such an isomorphism, we introduce Birkhoff's connection matrix.

**Definition 41.** *The Birkhoff connection matrix is defined by*

$$\mathscr{P}(z) = \mathfrak{Y}_0(z)^{-1}\mathfrak{Y}_\infty(z) \in \mathrm{GL}_n(\mathcal{M}(\mathbb{C}^\times)).$$

It is easily seen that

$$\mathscr{P}(qz) = \mathscr{P}(z).$$

So, one can consider $\mathscr{P}(z)$ as meromorphic function over the complex torus $\mathbb{C}^\times/q^{\mathbb{Z}}$ (*i.e.* as an elliptic function).

We let $S$ be the set of poles of $\mathscr{P}(z)$ or $\mathscr{P}(z)^{-1}$ in $\mathbb{C}^\times$.

**Theorem 42** ([Eti95, Theorem 3.1])**.** *For any $v \in \mathbb{C}^\times \setminus S$, there exists a unique isomorphism of difference ring extensions of $(\mathbb{C}(z), \sigma_q)$*

$$\tau_v : R_\infty \to R_0$$

*such that*

$$\tau_v(\mathfrak{Y}_\infty(z)) = \mathfrak{Y}_0(z)\mathscr{P}(v).$$

*It induces an isomorphism of difference field extensions of $(\mathbb{C}(z), \sigma_q)$*

$$\tau_v : K_\infty \to K_0.$$

*Proof.* Let $X = (X_{i,j})_{1\leq i,j\leq n}$ be indeterminates over $\mathbb{C}(z)$. Consider the unique $\mathbb{C}(z)$-algebra morphism

$$\varphi_0 : \mathbb{C}(z)[X] \to \mathbb{C}(z)[\mathfrak{Y}_0(z)]$$

such that $\varphi_0(X) = \mathfrak{Y}_0(z)$ and let $I_0 = \ker(\varphi_0)$ (*i.e.* $I_0$ is the ideal of the algebraic relations with coefficients in $\mathbb{C}(z)$ between the entries of $\mathfrak{Y}_0(z)$). We denote by

$$\overline{\varphi_0} : \mathbb{C}(z)[X]/I_0 \to \mathbb{C}(z)[\mathfrak{Y}_0(z)]$$

the $\mathbb{C}(z)$-algebra isomorphism induced by $\varphi_0$.

We define $\varphi_\infty$, $I_\infty$ and $\overline{\varphi_\infty}$ similarly.

Consider $P(X) \in I_\infty$, so that $P(\mathfrak{Y}_\infty(z)) = P(\mathfrak{Y}_0(z)\mathscr{P}(z)) = 0$. Therefore, the function $P(\mathfrak{Y}_0(z)\mathscr{P}(v))$, meromorphic over $\mathbb{C}$, vanishes at $q^k v$ for all integer $k$ large enough. It follows that $P(\mathfrak{Y}_0(z)\mathscr{P}(v)) = 0$ *i.e.* $P(X\mathscr{P}(v)) \in I_0$. Hence, we have a well-defined ring morphism

$$\begin{array}{ccc} \mathbb{C}(z)[X]/I_\infty & \to & \mathbb{C}(z)[X]/I_0 \\ P(X) & \mapsto & P(X\mathscr{P}(v)). \end{array}$$

This is actually a ring isomorphism; its inverse is given by

$$\begin{array}{ccc} \mathbb{C}(z)[X]/I_0 & \to & \mathbb{C}(z)[X]/I_\infty \\ P(X) & \mapsto & P(X\mathscr{P}(v)^{-1}). \end{array}$$

Therefore,

$$\overline{\varphi_0} \circ \iota \circ \overline{\varphi_\infty}^{-1} : \mathbb{C}(z)[\mathfrak{Y}_\infty(z)] \to \mathbb{C}(z)[\mathfrak{Y}_0(z)]$$

is a ring isomorphism. It induces (by localization) ring isomorphisms $R_\infty \to R_0$ and $K_\infty \to K_0$ with the expected properties. □

Therefore, for all $v, w \in \mathbb{C}^\times \setminus S$,

$$\tau_v^{-1}\tau_w \in \mathrm{Gal}^\phi(R_\infty/\mathbb{C}(z))$$

and, hence,

$$\mathscr{P}(v)^{-1}\mathscr{P}(w) \in G_{gal}$$

where $G_{gal}$ denotes the image of the linear representation

$$\rho_{gal} : \mathrm{Gal}^\phi(R_\infty/\mathbb{C}(z)) \to \mathrm{GL}_n(\mathbb{C})$$

attached to the fundamental matrix of solutions $\mathfrak{Y}_\infty(z)$.

**Definition 43.** *We denote by $G_{Bir}$ the subgroup of $\mathrm{GL}_n(\mathbb{C})$ generated by $\mathscr{P}(v)^{-1}\mathscr{P}(w)$ for all $v, w \in \mathbb{C}^\times \setminus S$.*

**Theorem 44** ([Eti95, Theorem 3.3])**.** *We have*

$$G_{gal} = G_{Bir}.$$

*Proof.* We admit that $G_{Bir}$ is Zariski-closed and refer to [Eti95, Proposition 3.2] for the proof. According to Galois correspondence, it is sufficient to prove that $K_{\infty}^{G_{Bir}} \subset \mathbb{C}$. Consider $f(z) \in K_{\infty}^{G_{Bir}}$. So, $f(z) = P(\mathfrak{Y}_{\infty}(z))$ for some $P(X) = A(X)/B(X)$ with $A(X), B(X) \in \mathbb{C}(z)[X]$ such that $B(\mathfrak{Y}_{\infty}(z)) \neq 0$. Since $f(z) \in K_{\infty}^{G_{Bir}}$, we have $f(z) = P(\mathfrak{Y}_{\infty}(z)) = P(\mathfrak{Y}_{\infty}(z)\mathscr{P}(v)^{-1}\mathscr{P}(w))$ for all $v, w \in \mathbb{C}^{\times} \setminus S$. For $v = z$ and for $w$ fixed, we get $f(z) = P(\mathfrak{Y}_0(z)\mathscr{P}(w)^{-1})$. Therefore, $f(z)$, which is a priori meromorphic over $\mathbb{P}^1(\mathbb{C}) \setminus \{0\}$, is also meromorphic at 0; thus, it is meromorphic over the whole $\mathbb{P}^1(\mathbb{C})$ and, hence, belongs to $\mathbb{C}(z)$. The Galois correspondence ensures that $G_{Bir} = G_{gal}$. □

**Remark 45.** *What says $\mathscr{P}(z)$ about $\sigma_q Y = AY$? Consider two $q$-difference systems $\sigma_q Y = A_1 Y$ and $\sigma_q Y = A_2 Y$ with $A_1, A_2 \in \mathrm{GL}_n(\mathbb{C}(z))$. We denote by $\mathscr{P}_1(z) = \mathfrak{Y}_{1,0}(z)^{-1}\mathfrak{Y}_{1,\infty}(z)$ and $\mathscr{P}_2(z) = \mathfrak{Y}_{2,0}(z)^{-1}\mathfrak{Y}_{2,\infty}(z)$ the corresponding connection matrices (with obvious notations). Assume that*

$$\mathscr{P}_1(z) = \mathscr{P}_2(z).$$

*Then, we have*

$$\mathfrak{Y}_{2,0}(z)\mathfrak{Y}_{1,0}(z)^{-1} = \mathfrak{Y}_{2,\infty}(z)\mathfrak{Y}_{1,\infty}(z)^{-1} =: R(z).$$

*Note that $R(z)$ is meromorphic over $\mathbb{P}_1(\mathbb{C}) \setminus \{\infty\}$ (this follows from the first expression for $R(z)$) and $\mathbb{P}_1(\mathbb{C}) \setminus \{0\}$ (this follows from the second expression for $R(z)$) so it is meromorphic over $\mathbb{P}_1(\mathbb{C})$ and, hence,*

$$R(z) \in \mathrm{GL}_n(\mathbb{C}(z)).$$

*Moreover, we have $R(qz) = A_2(z)R(z)A_1(z)^{-1}$. So, the $q$-difference system $\sigma_q Y = A_2 Y$ is obtained form $\sigma_q Y = A_1 Y$ by using the linear change of unknown function*

$$Y \rightsquigarrow RY.$$

*We say that the two $q$-difference systems above are isomorphic over $\mathbb{C}(z)$.*

9.3. **From connection matrices to monodromy.** One can consider the differential equations as degenerations of $q$-difference equations as $q$ tends to 1. We have attached (galoisian) analytic invariants to both differential and $q$-difference systems, namely the monodromy representation and the connection matrices. The aim of this section is to understand what happens to the connection matrices as $q$ tends to 1. We follow Sauloy in [Sau00].

We fix $\tau \in \mathbb{C}$ such that $\Im(\tau) > 0$. For all $\epsilon > 0$, we set $q_\epsilon = e^{2\pi i \tau \epsilon}$. So, $|q_\epsilon| < 1$ and $q_\epsilon$ tends to 1 as $\epsilon > 0$ tends to 0.

Consider a differential system

$$Y'(z) = \widetilde{B}(z)Y(z) \text{ with } \widetilde{B}(z) \in \mathrm{M}_n(\mathbb{C}(z)). \tag{7}$$

We deform this differential system into a family of $q_\epsilon$-difference equations

$$Y(q_\epsilon z) = A_\epsilon(z)Y(z) \text{ with } A_\epsilon(z) \in \mathrm{GL}_n(\mathbb{C}(z)) \tag{8}$$

parameterized by $\epsilon > 0$. By deformation, we mean the following. The previous $q_\epsilon$-difference systems can be rewritten as follows :

$$D_{q_\epsilon} Y(z) = B_\epsilon(z)Y(z) \tag{9}$$

where
$$B_\epsilon(z) = \frac{A_\epsilon(z) - I_n}{(q_\epsilon - 1)z} \text{ and } D_{q_\epsilon} Y(z) = \frac{Y(q_\epsilon z) - Y(z)}{(q_\epsilon - 1)z}.$$
Roughly speaking, we say that the family of systems (8) deforms the differential system (7) if $B_\epsilon(z)$ tends to $\widetilde{B}(z)$ as $\epsilon > 0$ tends to 0, so that the systems (9) tend to the differential system (7) as $\epsilon > 0$ tends to 0.

We shall now state more precisely our hypotheses :

- We assume that the differential system (7) is regular at 0 and $\infty$, *i.e.*, that there exists $\mathfrak{Y}_0(z) \in \mathrm{GL}_n(\mathcal{O}_{\mathbb{P}^1(\mathbb{C}),0})$ such that
$$\mathfrak{Y}_0'(z) = \widetilde{B}(z)\mathfrak{Y}_0(z) \text{ and } \mathfrak{Y}_0(0) = I_n$$
and that there exists $\mathfrak{Y}_\infty(z) \in \mathrm{GL}_n(\mathcal{O}_{\mathbb{P}^1(\mathbb{C}),\infty})$ such that
$$\mathfrak{Y}_\infty'(z) = \widetilde{B}(z)\mathfrak{Y}_\infty(z) \text{ and } \mathfrak{Y}_\infty(\infty) = I_n.$$
- We assume that the $q_\epsilon$-difference systems (8) are regular at 0 and $\infty$, and we denote by $\mathscr{P}_\epsilon(z)$ the corresponding connection matrices.
- We denote the singularities of $\widetilde{B}(z)$ (in $\mathbb{C}^\times$) by $\widetilde{z}_1, \ldots, \widetilde{z}_r$. We set $\widetilde{z}_0 = 1$. We assume that the spirals $\widetilde{z}_j e^{2\pi i\tau\mathbb{R}}$ are pairwise distinct. We index $\widetilde{z}_0, \ldots, \widetilde{z}_r$ in such a way that a positive circle around 0 meats the spirals $\widetilde{z}_0 e^{2\pi i\tau\mathbb{R}}, \ldots, \widetilde{z}_r e^{2\pi i\tau\mathbb{R}}$ in this order.
- We assume that $B_\epsilon(z)$ converges uniformly to $\widetilde{B}(z)$ on every compact subset of $\mathbb{C}^\times \setminus \{\widetilde{z}_0, \ldots, \widetilde{z}_r\}$ as $\epsilon > 0$ tends to 0.

We denote by $\widetilde{U}_0, ..., \widetilde{U}_r$ the connected components of $\mathbb{C}^\times \setminus \cup_{j=1}^r \widetilde{z}_j e^{2\pi i\tau\mathbb{R}}$ where $\widetilde{U}_j$ has $\widetilde{z}_j$ and $\widetilde{z_{j+1}}$ on its boundary.

**Theorem 46** ([Sau00, Section 4]). *Under the previous assumptions, we have :*

- *For all $j \in \{0, \ldots, r\}$, there exists $\widetilde{\mathscr{P}_j} \in \mathrm{GL}_n(\mathbb{C})$ such that $\mathscr{P}_\epsilon(z)$ tends to $\widetilde{\mathscr{P}_j}$ on $\widetilde{U}_j$ as $\epsilon > 0$ tends to 0.*
- *The monodromy matrix around $\widetilde{z}_j$ in the basis $\mathfrak{Y}_0(z)$ is given by $\widetilde{\mathscr{P}_j}\widetilde{\mathscr{P}}_{j-1}^{-1}$.*

**Remark 47.** *For a very general study of the behavior of the q-difference Galois groups as q tends to 1, we refer to André's* [And01].

**Remark 48.** *The results established by Etingof have been extended to the regular singular q-difference systems by van der Put and Singer in* [vdPS97] *and by Sauloy in* [Sau03]*, following distinct approaches.*

## 10. Computing difference Galois groups

Hendricks developed algorithms in [Hen97, Hen98] in order to compute the difference Galois groups of linear difference or $q$-difference equations of order 2 with coefficients in $\overline{\mathbb{Q}}(z)$ and $\cup_{j\geq 1}\overline{\mathbb{Q}}(z^{1/j})$ respectively. It relies on the classification of the algebraic subgroups of $\mathrm{GL}_2(\overline{\mathbb{Q}})$. For the difference Galois groups of Mahler equations of order 2 with coefficients in $\cup_{j\geq 1}\overline{\mathbb{Q}}(z^{1/j})$, we refer to [Roq16]. For calculations of difference Galois groups of finite difference equations of order 2 on an elliptic curve, we refer to [DR15].

What about equations of higher order ?

Feng has recently given in [Fen15] an algorithm to compute the Galois groups of linear difference equations over $\overline{\mathbb{Q}}(z)$.

For the galoisian properties of "classical equations", especially of the generalized $q$-hypergeometric equations, we refer to [Roq08, Roq11, Roq12]. The methods combine algebra and analysis.

We also emphasize that André's main result in [And01] gives a powerful tool to compute the difference Galois groups of difference equations deforming a given differential equations whose differential Galois group is known.

## 11. Parameterized difference Galois theory

In the recent years, several authors have developed "parameterized" differential or difference Galois theories. The starting point was the seminal work of Cassidy and Singer in [CS07]. This section is a brief introduction to the parameterized difference Galois theory developed by Hardouin and Singer in [HS08]. This theory is typically adapted to the study of the algebraic relations between the successive derivatives of the entries of a fundamental matrix of solutions of a given difference system. For instance, it has been used in *loc. cit.* to give a short proof of Hölder's theorem, concerning Euler's Gamma function, which satisfies

$$\Gamma(z+1) = z\Gamma(z).$$

**Theorem 49** (Hölder)**.** *Euler's Gamma function is hypertranscendental i.e. the successive derivatives* $\Gamma(z), \Gamma'(z), \Gamma''(z), \ldots$ *are algebraically independent over* $\mathbb{C}(z)$*.*

Another application given by Hardouin and Singer is the following.

**Theorem 50** ([HS08, Introduction])**.** *Let* $y_1(z)$*,* $y_2(z)$ *be linearly independent solutions of the q-hypergeometric equation*

$$y(q^2z) - \frac{2az-2}{a^2z-1}y(qz) + \frac{z-1}{a^2z-q^2}y(z) = 0$$

*where* $a \in \mathbb{C}^\times \setminus q^{\mathbb{Z}}$ *and* $a^2 \in q^{\mathbb{Z}}$ *and* $|q| \neq 1$*. Then* $y_1(z), y_2(z), y_1(qz)$ *and their successive derivatives are algebraically independent over the field of q-invariant meromorphic functions over* $\mathbb{C}^\times$*.*

Also, the parameterized difference Galois theory has been used by Dreyfus, Hardouin and Roques [DHR16] in order to study the generating series of automatic sequences. Let us recall that the generating series $f(z) = \sum_{k\geq 0} s_k z^k$ of any $p$-automatic sequence $(s_k)_{k\geq 0} \in \overline{\mathbb{Q}}^{\mathbb{N}}$ (and, actually, of any $p$-regular sequence) satisfies a mahlerian difference system *i.e.* a difference system of the form

$$F(z^p) = A(z)F(z)$$

where

$$F(z) = (f(z), f(z^p), \ldots, f(z^{p^{n-1}}))^t \text{ and } A(z) \in \mathrm{GL}_n(\mathbb{C}(z))$$

for some positive integer $n$; see Mendès France's [MF80], Randé's [Ran92], Dumas' [Dum93], Becker's [Bec94], Adamczewski and Bell's [AB13], and the references therein. The famous examples are the generating series of the

Thue-Morse, the paper-folding, the Baum-Sweet and the Rudin-Shapiro sequences (see Allouche and Shallit's book [AS03]). The study of the algebraic relations between such series and their successive derivatives is a classical problem, and we have shown in [DHR16] that the parameterized difference Galois theory is a very convenient tool in this context. For instance, we were able to prove the following result, where $f_{BS}(z)$ and $f_{RS}(z)$ are the generating series of the Baum-Sweet and Rudin-Shapiro series.

**Theorem 51** ([DHR16, Introduction]). *The series $f_{BS}(z), f_{BS}(z^2), f_{RS}(z), f_{RS}(-z)$ and all their successive derivatives are algebraically independent over $\mathbb{C}(z)$.*

11.1. **A short introduction to parameterized difference Galois theory.** The general setting of the parameterized difference Galois theory developed in [HS08] is the following. Instead of a difference field $(k, \phi)$, we consider a differential difference field $(k, \phi, \delta)$ *i.e.* $k$ is a field, $\phi$ is a field automorphism of $k$ and $\delta : k \rightarrow k$ is a derivation (this means that $\delta$ is an additive map satisfying Leibniz rule) such that

$$\phi \circ \delta = \delta \circ \phi.$$

**Example 52.** *(1) In the example of Hölder's theorem, one can take $k = \mathbb{C}(z)$, $\phi : f(z) \mapsto f(z+1)$, $\delta = d/dz$.*

*(2) $k = \mathbb{C}(z)$, $\phi : f(z) \mapsto f(qz)$, $\delta = zd/dz$.*

We want to study (the solutions of) a linear difference system

$$\phi(Y) = AY \text{ with } A \in \mathrm{GL}_n(k). \tag{10}$$

The difference rings used in difference Galois theory are replaced by the differential difference rings *i.e.* by 3-uples $(R, \phi, \delta)$ where $R$ is a ring, $\phi : R \rightarrow R$ is a ring automorphism and $\delta : R \rightarrow R$ is a derivation such that $\phi \circ \delta = \delta \circ \phi$. We denote by $C$ the field of constants of the difference field $(k, \phi)$.

There are natural notions of differential difference ring extensions, ideals, isomorphisms, *etc*, similar to the notions of difference ring extensions, ideals, isomorphisms, *etc*, introduced in Section 4. For instance, a differential difference ring $(\widetilde{R}, \widetilde{\phi}, \widetilde{\delta})$ is a differential difference ring extension of the differential difference ring $(R, \phi, \delta)$ if $\widetilde{R}$ is a ring extension of $R$, $\widetilde{\phi}_{|R} = \phi$ and $\widetilde{\delta}_{|R} = \delta$; in this case, we will often denote $\widetilde{\phi}$ by $\phi$ and $\widetilde{\delta}$ by $\delta$. We refer the reader to [HS08] for the details.

**Definition 53** ([HS08, Definition 2.3]). *A parameterized Picard-Vessiot ring for (10) over $(k, \phi, \delta)$ is a differential difference ring extension $R$ of $(k, \phi, \delta)$ such that*

*1) there exists $\mathfrak{Y} \in \mathrm{GL}_n(R)$ such that $\phi(\mathfrak{Y}) = A\mathfrak{Y}$ (such a $\mathfrak{Y}$ is called a fundamental matrix of solutions of (4));*

*2) $R$ is generated, as a $(k, \delta)$-algebra, by the entries of $\mathfrak{Y}$ and $\det(\mathfrak{Y})^{-1}$ i.e. $R$ is generated as a $k$-algebra by the entries of $\mathfrak{Y}$ and $\det(\mathfrak{Y})^{-1}$ and they successive transforms by $\delta$.*

*3) $R$ is a simple differential difference ring i.e. the only ideals of $R$ stable by $\phi$ and $\delta$ are $\{0\}$ and $R$.*

As in difference Galois theory, we need to impose restrictions on the field of constants $C$ in order to have a nice parameterized Picard-Vessiot theory. Unfortunately, the requirement that $C$ is algebraically closed is not sufficient. The usual requirement is that $C$ is differentially closed. This is not only a property of the field $C$ but a property of $C$ endowed with the derivation $\delta : C \to C$ ($\delta$ induces a map $C \to C$ because $\phi$ and $\delta$ commute). Roughly speaking, the fact that $(C, \delta)$ is differentially closed means that, for any polynomials $P_1(y_1, \ldots, y_s), \ldots, P_r(y_1, \ldots, y_s), Q(y_1, \ldots, y_s)$ in the $\delta^i(y_j)$ (here, $\delta^i(y_j)$ is a suggestive notation for indeterminates over $C$) and with coefficients in $C$, if

$$P_1(y_1, \ldots, y_s) = 0, \ldots, P_r(y_1, \ldots, y_s) = 0, Q(y_1, \ldots, y_s) \neq 0 \tag{11}$$

has a solution $\widetilde{y}_1, \ldots, \widetilde{y}_s$ is some differential field extension $(F, D)$ of $(C, \delta)$ (*i.e.* $F$ is a field extension of $C$, $D : F \to F$ is a derivation such that $D_{|C} = \delta$, and the equations (11) are satisfied if we replace $y_i$ by $\widetilde{y}_i$ and $\delta$ by $D$), then it has a solution in $(C, \delta)$.

**Proposition 54** ([HS08, Proposition 2.4])**.** *Assume that $k$ is of characteristic 0 and that $C$ is differentially closed. Then, up to ismorphism of differential difference fields over $(k, \phi, \delta)$, there exists a unique parameterized Picard-Vessiot ring for the difference system (10) over $(k, \phi)$.*

*Moreover, we have $R^\phi = C$.*

We let $R$ be a parameterized Picard-Vessiot rings for the difference system (10) over $(k, \phi, \delta)$. The parameterized difference Galois group is then defined as follows.

**Definition 55** ([HS08, Definition 2.5])**.** *The parameterized difference Galois group $\mathrm{Gal}^{(\phi,\delta)}(R/k)$ over $(k, \phi, \delta)$ of (10) is the group of the $k$-linear ring automorphisms of $R$ commuting with $\phi$ and $\delta$ :*

$$\mathrm{Gal}^{(\phi,\delta)}(R/k) := \{\sigma \in \mathrm{Aut}(R/k) \mid \phi \circ \sigma = \sigma \circ \phi \text{ and } \delta \circ \sigma = \sigma \circ \delta\}.$$

As in difference Galois theory, one can see $\mathrm{Gal}^{(\phi,\delta)}(R/k)$ as a subgroup of $\mathrm{GL}_n(C)$ *via* the faithful representation

$$\begin{array}{rcl} \rho_{gal} : \mathrm{Gal}^{(\phi,\delta)}(R/k) & \to & \mathrm{GL}_n(C) \\ \sigma & \mapsto & C(\sigma) \end{array}$$

where $C(\sigma)$ is determined by the equality $\sigma(\mathfrak{Y}) = \mathfrak{Y}C(\sigma)$.

A crucial result is then:

**Theorem 56** ([HS08, Theorem 2.6])**.** *The image of $\rho_{gal}$, which will be denoted by $G_{gal}^{(\phi,\delta)}$, is a differential algebraic subgroup of $\mathrm{GL}_n(C)$.*

This means that the image of $\rho_{gal}$ is

— a subgroup of $\mathrm{GL}_n(C)$ and

— the zero-locus in $\mathrm{GL}_n(C)$ of a set of differential polynomials in $C[(\delta^k(X_{i,j}))_{1 \leq i,j \leq n}, \det X^{-1}]$.

One can prove that the parameterized difference Galois groups reflect the algebraic relations between the entries of a fondamental matrix of solutions and their successive derivatives, in a similar way that the difference Galois groups reflect the algebraic relations between the entries of a fondamental matrix of solutions.

11.2. **From parameterized to non parameterized difference Galois theory. Applications.** We maintain the hypotheses and notations of the previous section. We let $S$ be the $k$-algebra generated by the entries of $\mathfrak{Y}$ and $\det(\mathfrak{Y})^{-1}$. Then, it can be shown that $(S, \phi)$ is a Picard-Vessiot ring for the difference system (10) over $(k, \phi)$. We denote by $G^{\phi}_{gal}$ the group $\mathrm{Gal}^{\phi}(S/k)$ seen as a subgroup of $\mathrm{GL}_n(C)$ *via* the faithful representation attached to $\mathfrak{Y}$.

**Theorem 57** ([HS08, Proposition 2.8])**.** *The differential algebraic group $G^{(\phi,\delta)}_{gal}$ is a Zariski-dense subgroup of the algebraic group $G^{\phi}_{gal}$.*

In some cases, *e.g.* if $G^{\phi}_{gal}$ has few differential algebraic subgroups, this is a strong information. For instance, it has been proved by Cassidy in [Cas89] that the Zariki-dense proper algebraic subgroups of $\mathrm{SL}_n(C)$ are conjugate to $\mathrm{SL}_n(C^{\delta})$, where

$$C^{\delta} = \{f \in C \mid \delta(f) = 0\}.$$

Whence the following result.

**Theorem 58.** *Assume that $G^{\phi}_{gal} = \mathrm{SL}_n(C)$. Then, we have:*

— *either $G^{(\phi,\delta)}_{gal} = G^{\phi}_{gal} = \mathrm{SL}_n(C)$;*

— *or $G^{(\phi,\delta)}_{gal}$ is conjugate to a subgroup of $\mathrm{SL}_n(C^{\delta})$.*

Moreover, the difference between the former and the later case can be reformulated as an integrability condition :

**Proposition 59** ([HS08, Proposition 2.9])**.** *The differential algebraic group $G^{(\phi,\delta)}_{gal}$ is conjugate to a subgroup of $\mathrm{GL}_n(C^{\delta})$ if and only if there exists $B \in k^{n\times n}$ such that*

$$\phi(B) = ABA^{-1} + \delta(A)A^{-1}.$$

*In this case, there exists $Y \in \mathrm{GL}_n(R)$ such that*

$$\phi(Y) = AY \text{ and } \delta(Y) = BY.$$

For instance, these are the main ingredients behind the proofs of theorem 50: it is proved in [Roq08] that, in this case, the difference Galois group is $\mathrm{SL}_2(C)$ and Hardouin and Singer managed to prove that the parameterized difference Galois group is $\mathrm{SL}_2(C)$ by using the previous two results.

## 12. Answers to selected exercises

### Answer of exercise 3

Indeed, we have $\phi(I) \subset I$, thus $I \subset \phi^{-1}(I)$. But $\phi^{-1}(I)$ is a difference ideal of $R$. So, we have either $\phi^{-1}(I) = I$ or $\phi^{-1}(I) = R$. The latter case is excluded.

### Answer of exercise 4

Assume that $(R/I, \overline{\phi})$ is a difference ring. Prove that there is a 1-1 correspondance between the difference ideals of $R$ containing $I$ and the difference ideals of $R/I$ given by $J \mapsto \pi^{-1}(J)$ where $\pi : R \to R/I$ is the canonical morphism.

### Answer of exercise 5

1. Indeed, we have $\phi(I) \subset I$ and, hence, $I \subset \phi^{-1}(I)$. Therefore, we have the ascending chain of ideals $I \subset \phi^{-1}(I) \subset \phi^{-2}(I) \subset \cdots$. Since $R$ is noetherian, there exists a positive integer $j$ such that $\phi^{-j}(I) = \phi^{-(j+1)}(I)$, whence $\phi(I) = I$.
2. Let $(X_n)_{n\in\mathbb{Z}}$ be a family of indeterminates over a field $k$ and consider the difference ring $(R, \phi)$ where $R = k[(X_n)_{n\in\mathbb{Z}}]$ and where $\phi$ is the unique $k$-algebra endomorphism of $R$ such that $\phi(X_n) = X_{n+1}$. Then, $I = (X_0, X_1, \ldots)$ is a difference ideal of $(R, \phi)$ and we have $\phi(I) \subsetneq I$.

### Answer of exercise 9

1. Let $f \in k'^{\phi}$. Let $P(X) \in k[X]$ be the minimal polynomial of $f$ over $k$ (in particular, $P(X)$ is monic). Then, $P^{\phi}(X) - P(X) \in k[X]$ has degree $< \deg P(X)$ and vanishes at $f$. Therefore, $P^{\phi}(X) - P(X) = 0$ *i.e.* the coefficients of $P(X)$ belong to $k^{\phi}$ and, hence, $f$ is algebraic over $k^{\phi}$.
2. Consider for instance $\mathbb{C}$ endowed with the complex conjugation.

## References

[AB13] Boris Adamczewski and Jason P. Bell. A problem about Mahler functions. *arXiv:1303.2019*, 2013.

[And01] Y. André. Différentielles non commutatives et théorie de Galois différentielle ou aux différences. *Ann. Sci. École Norm. Sup. (4)*, 34(5):685–739, 2001.

[AS03] Jean-Paul Allouche and Jeffrey Shallit. *Automatic sequences*. Cambridge University Press, Cambridge, 2003. Theory, applications, generalizations.

[Bec94] P.-G. Becker. $k$-regular power series and Mahler-type functional equations. *J. Number Theory*, 49(3):269–286, 1994.

[Ber92] Daniel Bertrand. Groupes algébriques et équations différentielles linéaires. *Séminaire Bourbaki*, 34:183–204, 1991-1992.

[Beu92] F. Beukers. Differential Galois theory. In *From number theory to physics (Les Houches, 1989)*, pages 413–439. Springer, Berlin, 1992.

[Cas89] Phyllis Joan Cassidy. The classification of the semisimple differential algebraic groups and the linear semisimple differential algebraic Lie algebras. *J. Algebra*, 121(1):169–238, 1989.

[CS07] Phyllis J. Cassidy and Michael F. Singer. Galois theory of parameterized differential equations and linear differential algebraic groups. In *Differential equations and quantum groups*, volume 9 of *IRMA Lect. Math. Theor. Phys.*, pages 113–155. Eur. Math. Soc., Zürich, 2007.

[DHR16] T. Dreyfus, C. Hardouin, and J. Roques. Jour. europ. math. soc. *Hypertranscendence of solutions of Mahler equations*, 2016.

[DR15] Thomas Dreyfus and Julien Roques. Galois groups of difference equations of order two on elliptic curves. *SIGMA, Symmetry Integrability Geom. Methods Appl.*, 11:paper 003, 23, 2015.

[Dum93] Philippe Dumas. Récurrences mahlériennes, suites automatiques, études asymptotiques. *Thèse de l'Université Bordeaux I available at https://tel.archives-ouvertes.fr/tel-00614660*, 1993.

[DV12] L. Di Vizio. *Approche galoisienne de la transcendance différentielle*. Journée annuelle 2012 de la SMF. ArXiv:1404.3611, 2012.

[Eti95] P. I. Etingof. Galois groups and connection matrices of $q$-difference equations. *Electron. Res. Announc. Amer. Math. Soc.*, 1(1):1–9 (electronic), 1995.

[Fen15] R. Feng. On the computation of the galois group of linear difference equations. *arXiv:1503.02239*, 2015.

[Hen97] P. A. Hendriks. An algorithm for computing a standard form for second-order linear $q$-difference equations. *J. Pure Appl. Algebra*, 117/118:331–352, 1997. Algorithms for algebra (Eindhoven, 1996).

[Hen98] P. A. Hendriks. An algorithm determining the difference Galois group of second order linear difference equations. *J. Symbolic Comput.*, 26(4):445–461, 1998.

[HS08] C. Hardouin and M. F. Singer. Differential Galois theory of linear difference equations. *Math. Ann.*, 342(2):333–377, 2008.

[HSS16] C. Hardouin, J Sauloy, and M. F. Singer. *Galois theories of linear difference equations: an introduction*, volume 211 of *Mathematical Surveys and Monographs*. American Mathematical Society, 2016.

[MF80] Michel Mendès France. Nombres algébriques et théorie des automates. *Enseign. Math. (2)*, 26(3-4):193–199 (1981), 1980.

[Ran92] Bernard Randé. Équations fonctionnelles de Mahler et applications aux suites $p$-régulières. *Thèse de l'Université Bordeaux I available at https://tel.archives-ouvertes.fr/tel-01183330*, 1992.

[Roq08] J. Roques. Galois groups of the basic hypergeometric equations. *Pacific J. Math.*, 235(2):303–322, 2008.

[Roq11] J. Roques. Generalized basic hypergeometric equations. *Invent. Math.*, 184(3):499–528, 2011.

[Roq12] J. Roques. On classical irregular $q$-difference equations. *Compositio Math.*, 148(5):1624–1644, 2012.

[Roq16] J. Roques. On the algebraic relations between mahler functions. *Trans. Amer. Math. Soc.*, 2016.

[Sau00] J. Sauloy. Systèmes aux $q$-différences singuliers réguliers: classification, matrice de connexion et monodromie. *Ann. Inst. Fourier (Grenoble)*, 50(4):1021–1071, 2000.

[Sau03] J. Sauloy. Galois theory of Fuchsian $q$-difference equations. *Ann. Sci. École Norm. Sup. (4)*, 36(6):925–968 (2004), 2003.

[Sau12] Jacques Sauloy. Introduction to differential galois theory. *available at http://www.math.univ-toulouse.fr/ sauloy/PAPIERS/GalDiffWuhan.pdf*, 2012.

[Sin09] Michael F. Singer. Introduction to the Galois theory of linear differential equations. In *Algebraic theory of differential equations*, volume 357 of *London Math. Soc. Lecture Note Ser.*, pages 1–82. Cambridge Univ. Press, Cambridge, 2009.

[VdP98] Marius Van der Put. Recent work on differential galois theory. *Séminaire Bourbaki*, 40:341–367, 1997-1998.

[vdPS97] M. van der Put and M. F. Singer. *Galois theory of difference equations*, volume 1666 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1997.

[vdPS03] Marius van der Put and Michael F. Singer. *Galois theory of linear differential equations*, volume 328 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 2003.

Institut Fourier, Université Grenoble Alpes, CNRS UMR 5582, 100 rue des Maths, BP 74, 38402 St Martin d'Hères

*E-mail address*: `Julien.Roques@ujf-grenoble.fr`