Iterative q-Difference Galois Theory

Charlotte Hardouin

IWR

14 january 2008

Contents

1 Introduction

Initially, the Galois theory of q-difference equations was built for q unequal to a root of unity (see for instance [25]). This choice was made in order to avoid the increase of the field of constants to a transcendental field. However, P.A. Hendricks studied this problem in his PhD work under the supervision of M. van der Put (see [12]). In Chapter 6 he gave a notion of Galois groups for q-difference equations over $\mathbb{C}(z)$ with $q^m = 1$. His idea was to compare the category $Diff_{\mathbb{C}(z)}$ of q-difference modules over $\mathbb{C}(z)$ with the category $FMod_Z$ of modules over the ring $\mathbb{C}(z^m)[t, t^{-1}]$. He thus obtained an equivalence of categories and a fiber functor from $Diff_{\mathbb{C}(z)}$ with values in the category $Vect_{\mathbb{C}(z^m)}$ of vector spaces of finite dimension over $\mathbb{C}(z^m)$. However, in his case there is no unique Picard-Vessiot ring of a q-difference equation. This construction is also not totally satisfying because we do not want to have such transcendental base fields for Galois groups.

In the same matter, the question of the constant field for differential modules in positive characteristic has given rise to the construction of a new differential Galois theory in positive characteristic. The first work in this direction was made by H. Hasse and F.K. Schmidt [11], but it was only in 2000 when B.H. Matzat and M. van der Put set up a modern and systematic approach to this theory (see [17] and [16]). The main idea is to consider not only one derivation but a whole family of derivations, called *higher derivations* or *iterative derivations*. By defining the constants as the elements annihilated by the whole family of derivations, they succeeded in getting a good constant field, for instance $\overline{\mathbb{F}_p}$ instead of $\overline{\mathbb{F}_p}(z^p)$. So they were able to give a complete description of the Picard-Vessiot theory of differential equations in positive characteristic and relate it to a Tannakian approach.

For q-difference theory, the problem is not the characteristic but the roots of unity. Inspired by the work of B.H. Matzat and M. van der Put, we consider in this paper a family of *iterative difference operators* instead of considering just one difference operator, and in this way we stop the increase of the constant field and succeed in setting up a Picard-Vessiot theory for q-difference equations where q is a root of unity. The theory we obtain is quite the exact translation of the iterative differential Galois theory developed by B.H. Matzat and M. van der Put to the q-difference world. This analogy between iterative differential Galois theory and iterative difference Galois theory could perhaps be explained in a more theoretical way, as it is done in the paper of Y. André [1] for classical theories. But for the moment, we will only focus on the construction of iterative q-difference Galois theory.

The interests of building such a theory are multiple. The first one is to fill in the gap in the classical q-difference Galois theory for roots of unity. The theory of iterative q-difference operators developed in this paper encompasses and extends the work of Singer and van der Put ([25]). For instance, this could provide a good functor of p-adic confluence from the world of q-difference to the world of differential equations, following the work of A. Pulita ([18]). However, instead of considering a (σ_q, ∂)-module at the roots of unity, (as

it is done in [18]), it will be more suitable to consider an iterative q-difference module. In a similar way, it will be very enlightening to build a confluence functor in characteristic p from iterative q-difference modules to iterative differential modules. Another goal of this theory will be to obtain an iterative q-difference version of the Grothendieck Conjecture following the work of L. Di Vizio [8] and the work of P.A. Hendricks [12]. In other words, we want to prove that our iterative q-difference groups are generated by the curvatures, which are linear operators in characteristic zero in the case of q a root of unity.
For the whole paper, we fix an algebraically closed field C and $q \in C$ with $q \neq 1$. Let $F = C(t)$ denote the field of rational functions over C and σ_q the automorphism of F which associates to a function $f(z)$ the function $f(qz)$.
In the second section, we introduce the arithmetic basis of iterative q-difference algebra. In this section we work in all generality, i.e., we do not make any assumptions wether q is a root of unity or not. With this choice we want to emphasize the fact that we just generalize the Galois theory of q-difference of M.F Singer and M. van der Put ([25]). From the third section until the end of the paper, we will restrict ourselves to the case of q a primitive root of unity, where the most peculiar phenomena appear. In Section 3 we define the category of iterative q-difference modules and their relation with some specific category of projective systems. As in [16], the equivalence of categories yields a family of q-difference equations, related to the fact that an iterative q-difference operator is a family of maps. Such a family of equations can be regarded in two different ways, a general and a relative one using the projective system. Both formulations are used in later sections.
In Section 4, we build a Picard-Vessiot theory for iterative q-difference equations by using the classical theory as formulated for instance in [25]. To be a little more concrete, at the end of the section, we give a method to realize groups in dimension one as iterative q-difference Galois groups.
In Section 5, we adopt Kolchin's way of thinking and show how an iterative q-difference Galois group is formed by the C-points of an affine group-scheme. We also obtain the analogue of Kolchin's theorem for our theory and the usual Galois correspondence.
As a conclusion to this paper, we state an analogue of the Grothendieck-Katz conjecture for iterative q-difference Galois groups as in the work of L. Di Vizio.
I would like to thank A. Roescheisen and J. Hartmann for all their help, remarks and so useful comments. Last but not least, I am sincerely grateful to the Professor B.H. Matzat for the inspiration his theory has provided to me and for all his help and encouragement to pursue this study.

2 Iterative q-difference rings

In considering an element q of a field C which may be a primitive root of unity and trying to construct a q-difference Galois theory, we have to deal with the problem that the field of constants of the usual q-difference operator extends to a transcendental field. To avoid this increase of the constants, we have to consider a more arithmetic approach, such as the one introduced by H. Hasse and F.K. Schmidt [11] for differential equations. Until the end

of this article, we let $F = C(t)$ denote the field of rational functions over C and σ_q the q-difference operator of F defined as follows : $\sigma_q(f(z)) := f(qz)$.

2.1 q-Arithmetic properties

In this paragraph, we just recall the most usual q-arithmetical objects.

Definition 2.1 *Let $k \in \mathbb{Z}$. Put $[k]_q := \frac{q^k-1}{q-1}$.*

1. *Let $[k]_q!$ denote the element of C defined by $[k]_q[k-1]_q...[1]_q$. We will say that $[k]_q!$ is the q-factorial of k.*
2. *Let $\binom{r}{k}_q$ denote the element of C defined by $\frac{[r]_q!}{[k]_q![(r-k)]_q!}$. We will say that $\binom{r}{k}_q$ is the q-binomial coefficient of r over k.*
3. *$(1-t)_m := (1-t)(1-qt)...(1-q^{m-1}t)$.*

Proposition 2.2 1. *$\binom{r}{0}_q = \binom{r}{r}_q = 1$.*

2. *$\binom{0}{k}_q = 0$ if $k \neq 0$ and $\binom{0}{0}_q = 1$.*
3. *Assume that q is a primitive n-th root of unity. Then for two integers $a > b$,*

$$\binom{an}{bn}_q = \binom{a}{b}. \tag{1}$$

4. *$\sum_{i+j=k, i\leq s, j\leq r} \binom{r}{j}_q \binom{s}{i}_q q^{i(r-j)} = \binom{r+s}{k}_q$ for all $(k,r,s) \in \mathbb{N}^3$ with $r+s \geq k$.*

Proof of part 4
Let $m \in \mathbb{N}$. The function $(1-t)_m$ of $C(t)$ defined in 2.1 part 3 gives

$$(1-t)_m = \sum_{j=0}^{m} (-1)^j \binom{m}{j}_q q^{j(j-1)/2} t^j. \tag{2}$$

Because $q^n = 1$ and n is the order of q, we have $(1-t)_{an} = (1-t)_n^a$. Using Equation (2), we obtain

$$\sum_{j=0}^{an} (-1)^j \binom{an}{j}_q q^{j(j-1)/2} t^j = \sum_{j=0}^{a} \binom{a}{j} (-1)^{nj} q^{n(n-1)j/2} t^{nj}.$$

By comparing the terms in t^{bn}, we obtain $\binom{an}{bn}_q q^{\frac{bn(bn-1)}{2}} = \binom{a}{b} q^{b\frac{n(n-1)}{2}}$.
Proof of part 5
Let $(k,r,s) \in \mathbb{N}^3$ with $r+s \geq k$. We have

$$(1-t)_{r+s} = (1-t)_r (1-q^r t)_s. \tag{3}$$

By comparing the terms in t^k, we obtain

$$(-1)^k q^{k(k-1)/2} \binom{r+s}{k}_q = \sum_{i+j=k, i\leq s, j\leq r} (-1)^{i+j} q^{k(k-1)/2} \binom{r}{j}_q \binom{s}{i}_q q^{i(r-j)}.$$

Remark 2.3 *If C is of characteristic $p > 0$, then for $p^j > i$ we get from equation (1) $\binom{np^j}{ni}_q = 0$.*

2.2 Iterative q-difference ring

In this paragraph, we define the formal properties of the iterative q-difference operator. In the world of q-difference the analogue of the derivation $\frac{d}{dt}$ is the operator $\delta_q := \frac{\sigma_q - id}{(q-1)t}$ (see for instance [20]). Heuristically speaking, when q goes to 1, δ_q goes to the usual derivation $\frac{d}{dt}$. Thus the main idea of our constructions is to deform the iterative derivations into iterative difference operators by replacing ∂ by δ_q and all the arithmetical factors occurring in their Definition 1.1 in [16] by q-analogues. The only change appears at the part 4 of Definition 2.4, where a twist by σ_q occurs.

Definition 2.4 *Let R be a q-difference extension of $C(t)$ in the sense of [25], let σ_q be the q-difference operator of R and let $\delta_R^* := (\delta_R^{(k)})_{k\in\mathbb{N}}$ be a collection of maps from R to R. The family δ_R^* is called an **iterative q-difference operator** on R, if for all $a, b \in R$ and all $i, j, k \in \mathbb{N}$, the following properties are satisfied*

1. $\delta_R^{(0)} = id$,
2. $\delta_R^{(1)} = \frac{\sigma_q - id}{(q-1)t}$,
3. $\delta_R^{(k)}(x+y) = \delta_R^{(k)}(x) + \delta_R^{(k)}(y)$,
4. $\delta^{(k)}(ab) = \sum_{i+j=k} \sigma_q^i(\delta_R^{(j)}(a))\delta_R^{(i)}(b)$,
5. $\delta_R^{(i)} \circ \delta_R^{(j)} = \binom{i+j}{i}_q \delta_R^{(i+j)}$.

*The set of iterative q-difference operators is denoted by $ID_q(R)$. For $\delta_R^* \in ID_q(R)$, the tuple (R, δ_R^*) is called an **iterative q-difference ring** (ID_q-ring). We say that an element c of R is a constant if $\delta_R^{(k)}(c) = 0$ for all $k \in \mathbb{N}^*$. We denote by $C(R)$ the ring of constants of R.*

Remark 2.5 1. *If R is a ring, then $C(R)$ is a ring. If R is a field, then $C(R)$ is a field.*

2. *We have for all $j, i \in \mathbb{N}$,*

$$\sigma_q^j \delta_R^{(i)} = \frac{1}{q^{ji}} \delta_R^{(i)} \sigma_q^j. \tag{4}$$

Proof
In order to prove Equation (4), it is sufficient to prove it for $j = 1$, the general case obviously follows from this case.
For all $k > 0$, we have

$$\delta_R^{(k)}(t\frac{1}{t}) = 0 = \delta_R^{(k)}(t^{-1})t + \sigma_q(\delta_R^{(k-1)}(t^{-1})). \tag{5}$$

By part 5 of Definition 2.4, we get $\delta_R^{(1)} \circ \delta_R^{(i)} = \delta_R^{(i)} \circ \delta_R^{(1)}$ for all $i \in \mathbb{N}$. Using part 2 and 4, we obtain that

$$\frac{\sigma_q - id}{t} \circ \delta_R^{(i)}(x) = \delta_R^{(i)} \circ (\frac{\sigma_q - id}{t})(x) = \sum_{k=1}^{i} \sigma_q^k(\delta_R^{(i-k)}(\sigma_q - id)(x))\delta_R^{(k)}(t^{-1}) + \delta_R^{(i)}((\sigma_q - id)(x))t^{-1}$$

for all $x \in R$ and $i \in \mathbb{N}$. By Equation (5), we get

$$\frac{\sigma_q}{t} \circ \delta_R^{(i)}(x) = \frac{-1}{t}\sigma_q[\sum_{k=0}^{i-1} \sigma_q^k(\delta_R^{(i-1-k)}(\sigma_q - id)(x))\delta_R^{(k)}(t^{-1})] + \frac{\delta_R^{(i)} \circ \sigma_q(x)}{t},$$

i.e.,

$$\frac{\sigma_q}{t} \circ \delta_R^{(i)}(x) = \frac{-1}{t}\sigma_q(\delta_R^{(i-1)} \circ \delta_R^{(1)}(x)) + \frac{\delta_R^{(i)} \circ \sigma_q(x)}{t}$$

that is,

$$\frac{\sigma_q}{t} \circ \delta_R^{(i)}(x) = -\frac{q-1}{t}\sigma_q \circ (\frac{q^i - 1}{q-1}\delta_R^{(i)})(x) + \frac{\delta_R^{(i)} \circ \sigma_q(x)}{t}.$$

This last equation gives

$$\sigma_q\delta_R^{(i)}(x) = \frac{1}{q^i}\delta_R^{(i)}\sigma_q(x)$$

which concludes the proof.

Remark 2.6 (Classical case) *If q is not a root of unity then $\delta_R^{(k)} = \frac{(\delta_R^{(1)})^k}{[k]_q!}$ and the iterative q-difference rings that we consider are the q-difference rings studied by M. van der Put and M.F Singer in [25].*

Main example : The field of rational functions over C

Definition 2.7 *Let $k \in \mathbb{N}$. Let $\delta_q^{(k)}$ denote the additive map from $C[t]$ to $C[t]$ defined by $\delta_q^{(k)}(\lambda t^r) := \lambda\binom{r}{k}_q t^{r-k}$, for all $r \in \mathbb{N}$, and $\lambda \in C$. Using the formula $\delta^{(k)}(ab) = \sum_{i+j=k} \sigma_q^i(\delta_q^{(j)}(a))\delta_q^{(i)}(b)$, we extend $\delta_q^{(k)}$ to $F = C(t)$.*

Proposition 2.8 *The collection $(\delta_q^{(k)})_{k\in\mathbb{N}}$ of maps from F to F, defined previously, satisfy*

1. $\delta_q^{(0)} = id$,
2. $\delta_q^{(1)} = \frac{\sigma_q - id}{(q-1)t}$,
3. *for all $k \in \mathbb{N}$, the map $\delta_q^{(k)}$ is additive,*
4. $\delta_q^{(i)} \circ \delta_q^{(j)} = \binom{i+j}{i}_q \delta_q^{(i+j)}$.

Proof

By construction of $(\delta_q^{(k)})_{k\in\mathbb{N}}$, it is sufficient to prove that all the formulas hold upon evaluation on t^r with $r \in \mathbb{N}$.

1. Because $\binom{k}{0}_q = 1$, it is obvious that $\delta_q^{(0)} = id$.
2. For all $r \in \mathbb{N}$, we have $\delta_q^{(1)}(t^r) = \binom{r}{1}_q t^{r-1} = \frac{q^r t^r - t^r}{(q-1)t} = \frac{\sigma_q - id}{(q-1)t}(t^r)$.
3. Let $r \in \mathbb{N}$. We have
$$\delta_q^{(i)} \circ \delta_q^{(j)}(t^r) = \binom{r-j}{i}_q \binom{r}{j}_q t^r$$
and
$$\binom{r-j}{i}_q \binom{r}{j}_q = \binom{i+j}{i}_q \binom{r}{i+j}_q,$$
which gives
$$\delta_q^{(i)} \circ \delta_q^{(j)}(t^r) = \binom{i+j}{i}_q \delta_q^{(i+j)}(t^r).$$

Proposition 2.9 *The field $F = C(t)$ endowed with the collection of maps $(\delta_q^{(k)})_{k\in\mathbb{N}}$ as in Definition 2.7 is an iterative q-difference field with $\delta_q^{(n)}(t^n) = 1$ for all $n \in \mathbb{N}$ and thus $C(F) = C$.*

Tensor product of ID_q-rings

Lemma 2.10 *Let $(R_1, \delta_{R_1}^*)$ and $(R_2, \delta_{R_2}^*)$ be two iterative q-difference rings. We have*
$$\sum_{i+j=k} \sigma_q^i(\delta_{R_1}^{(j)}(a)) \otimes \delta_{R_2}^{(i)}(b) = \sum_{i+j=k} \delta_{R_1}^{(j)}(a) \otimes \sigma_q^j(\delta_{R_2}^{(i)}(b)) \tag{6}$$
for all $k \in \mathbb{N}$, $(a, b) \in R_1 \times R_2$.

Proof
The formula (6) is obviously true for $k = 1$, using the definition of $\delta^{(1)}$. If (6) holds for k and l in $\mathbb{N}$, we have

$$\binom{k+l}{k}_q \sum_{i+j=k+l} \sigma_q^i(\delta_{R_1}^{(j)}(a)) \otimes \delta_{R_2}^{(i)}(b) = \left(\sum_{r+s=l} \sigma_q^r(\delta_{R_1}^{(s)}) \otimes \delta_{R_2}^{(r)}\right) \left(\sum_{i+j=k} \sigma_q^i(\delta_{R_1}^{(j)}(a)) \otimes \delta_{R_2}^{(i)}(b)\right)$$

that is

$$(\sum_{r+s=l} \sigma_q^r(\delta_{R_1}^{(s)}) \otimes \delta_{R_2}^{(r)}) \left(\sum_{i+j=k} \sigma_q^i(\delta_{R_1}^{(j)}(a)) \otimes \delta_{R_2}^{(i)}(b)\right) = \left(\sum_{r+s=l} \delta_{R_1}^{(r)} \otimes \sigma_q^r(\delta_{R_2}^{(s)})\right) \left(\sum_{i+j=k} \delta_{R_1}^{(j)}(a) \otimes \sigma_q^j(\delta_{R_2}^{(i)}(b))\right)$$

and thus

$$\binom{k+l}{k}_q \sum_{i+j=k+l} \sigma_q^i(\delta_{R_1}^{(j)}(a)) \otimes \delta_{R_2}^{(i)}(b) = \binom{k+l}{k}_q \sum_{i+j=k+l} \delta_{R_1}^{(j)}(a) \otimes \sigma_q^j(\delta_{R_2}^{(i)}(b)).$$

Then, if $\binom{k+l}{k}_q \neq 0$, the formula (6) holds for $k + l$. If q is not a root of unity, we can conclude by induction.
Assume now that $q^n = 1$. It remains to show that Formula (6) holds for $k \in n\mathbb{N}$. We will first prove it for $k = n$.
Because $\sum_{i+j=n} \sigma_q^i(\delta_{R_1}^{(j)}(a)) \otimes \delta_{R_2}^{(i)}(b) = \delta_{R_1}^{(n)}(a) \otimes b + a \otimes \delta_{R_2}^{(n)}(b) + \sum_{i=1}^{n-1} \sigma_q^i(\delta_{R_1}^{(n-i)}(a)) \otimes \delta_{R_2}^{(i)}(b)$, the proof for $k = n$ will be complete if we show that

$$\sum_{i=1}^{n-1} \sigma_q^i(\delta_{R_1}^{(n-i)}(a)) \otimes \delta_{R_2}^{(i)}(b) = \sum_{i=1}^{n-1} \delta_{R_1}^{(i)}(a) \otimes \sigma_q^i(\delta_{R_2}^{(n-i)}(b)). \tag{7}$$

We have $\delta^{(k)} = \frac{(\delta^{(1)})^k}{[k]_q!}$ and

$$(\delta^{(1)})^k = \frac{(-1)^k}{((q-1)t)^k} \sum_{j=0}^{k} (-1)^j \binom{k}{j}_{q^{-1}} q^{-\frac{j(j-1)}{2}} \sigma_q^j = \frac{1}{((q-1)t)^k} \sum_{j=0}^{k} a_{j,k} \sigma_q^j$$

for $0 < k < n$ (see [8], Lemma 1.1.10). Then,

$$\sum_{i=1}^{n-1} \sigma_q^i(\delta_{R_1}^{(n-i)}(a)) \otimes \delta_{R_2}^{(i)}(b) = \frac{1}{((q-1)t)^n} \sum_{l=1}^{n} \sum_{k=0}^{l} \sigma_q^l(a) \otimes \sigma_q^k(b) \left(\sum_{i=k, i\neq 0}^{i=l, i\neq n} \frac{a_{l-i,n-i} a_{k,i} q^{-i(n-i)}}{[n-i]_q! [i]_q!}\right). \tag{8}$$

If $l \neq n$, $k \neq 0$ and $l \neq k$, we have

$$\sum_{i=k, i\neq 0}^{i=l, i\neq n} \frac{a_{l-i,n-i} a_{k,i} q^{-i(n-i)}}{[n-i]_q! [i]_q!} = \frac{(-1)^{l+n} q^{-\frac{n(n-1)}{2}}}{[n-l]_{q^{-1}}! [k]_q! [l-k]_q!} \sum_{i=0}^{l-k} (-1)^i \binom{l-k}{i}_q q^{\frac{i(i-1)}{2}} = 0$$

(expand $(1-1)_{l-k}$). If $l=n$, then

$$\sum_{i=k,i\neq 0}^{i=n,i\neq n}\frac{a_{n-i,n-i}a_{k,i}q^{-i(n-i)}}{[n-i]_q![i]_q!}=\frac{(-1)^{n+k+1}q^{-\frac{n(n-1)}{2}}}{[k]_q![n-k]_{q^{-1}}}=\sum_{i=0,i\neq 0}^{i=k,i\neq n}\frac{a_{k-i,n-i}a_{0,i}q^{-i(n-i)}}{[n-i]_q![i]_q!}$$

(expand $(1-1)_k$ and $(1-1)_{n-k}$). Because $\sigma_q^n=id$, it follows that the equation (8) is symmetric in a and b. Thus the formula (7) holds and the equation (6) is true for $k=n$. For $k=2n$, we have

$$\sum_{i+j=n}\sigma_q^i(\delta_{R_1}^{(j)}(a))\otimes\delta_{R_2}^{(i)}(b)=\delta_{R_1}^{(2n)}(a)\otimes b+a\otimes\delta_{R_2}^{(2n)}(b)+$$

$$\sum_{i=1}^{n-1}\sigma_q^i(\delta_{R_1}^{(2n-i)}(a))\otimes\delta_{R_2}^{(i)}(b)+\delta_{R_1}^{(n)}(a)\otimes\delta_{R_2}^{(n)}(b)+\sum_{i=n+1}^{2n-1}\sigma_q^i(\delta_{R_1}^{(2n-i)}(a))\otimes\delta_{R_2}^{(i)}(b).$$

Because $\delta^{(2n-i)}=\delta^{(n-i)}\circ\delta^{(n)}$ for all $i=1,...,n-1$, we obtain by (7)

$$\sum_{i=1}^{n-1}\sigma_q^i(\delta_{R_1}^{(2n-i)}(a))\otimes\delta_{R_2}^{(i)}(b)=\sum_{i=1}^{n-1}\sigma_q^i(\delta_{R_1}^{(n-i)}(\delta_{R_1}^{(n)}(a)))\otimes\delta_{R_2}^{(i)}(b)=\sum_{i=1}^{n-1}\delta_{R_1}^{(n+i)}(a)\otimes\sigma_q^i(\delta_{R_2}^{(n-i)}(b))$$

$$=\sum_{i=n+1}^{2n-1}\delta_{R_1}^{(i)}(a)\otimes\sigma_q^i(\delta_{R_2}^{(2n-i)}(b)).$$

We also have

$$\sum_{i=n+1}^{2n-1}\sigma_q^i(\delta_{R_1}^{(2n-i)}(a))\otimes\delta_{R_2}^{(i)}(b)=\sum_{i=1}^{n-1}\delta_{R_1}^{(i)}(a)\otimes\sigma_q^i(\delta_{R_2}^{(2n-i)}(b)).$$

This concludes the proof for $k=2n$. The same arguments gives the other cases.

Proposition 2.11 (proposition, definition) *Let $(R_1,\delta_{R_1}^*)$ and $(R_2,\delta_{R_2}^*)$ be two iterative q-difference rings. We define a collection of maps $(\delta_{R_1\otimes R_2}^{(k)})_{k\in\mathbb{N}}$ from $R_1\otimes_F R_2$ to $R_1\otimes_F R_2$ as follows :*

$$\delta_{R_1\otimes R_2}^{(k)}(r_1\otimes r_2):=\sum_{i+j=k}\sigma_q^i(\delta_{R_1}^{(j)}(r_1))\otimes\delta_{R_2}^{(i)}(r_2)\quad \textit{for all } k\in\mathbb{N}, r_1\in R_1 \textit{ and } r_2\in R_2.$$

Then $(R_1\otimes_F R_2,\delta_{R_1\otimes R_2}^*)$ is an iterative q-difference ring.

Proof
It is obvious that the family $(\delta_{R_1\otimes R_2}^{(k)})_{k\in\mathbb{N}}$ satisfies the three first parts of Definition 2.4. By Lemma 2.10 we have

$$\delta_{R_1\otimes R_2}^{(k)}(r_1\otimes r_2)=\sum_{i+j=k}\sigma_q^i(\delta_{R_1}^{(j)}(r_1))\otimes\delta_{R_2}^{(i)}(r_2)=\sum_{i+j=k}\delta_{R_1}^{(j)}(r_1)\otimes\sigma_q^j(\delta_{R_2}^{(i)}(r_2))$$

for all $k \in \mathbb{N}$. Let $(a, c) \in R_1^2$ and $(b, d) \in R_2^2$. We have

$$\delta^{(k)}_{R_1\otimes R_2}((a\otimes b)(c\otimes d)) = \sum_{i+j=k} \sigma_q^i(\delta^{(j)}_{R_1}(ac)) \otimes \delta^{(j)}_{R_2}(bd),$$

$$\delta^{(k)}_{R_1\otimes R_2}((a\otimes b)(c\otimes d)) = \sum_{i_1+i_2+j_1+j_2=k} \sigma_q^{i_1+i_2+j_1}(\delta^{(j_2)}_{R_1}(a))\sigma_q^{i_1+i_2}(\delta^{(j_1)}_{R_1}(c)) \otimes \sigma_q^{i_1}(\delta^{(i_2)}_{R_2}(b))\delta^{(i_2)}_{R_2}(d),$$

and thus,

$$\delta^{(k)}_{R_1\otimes R_2}((a\otimes b)(c\otimes d)) = \sum_{i_1+j_2+i=k} \sigma_q^{i_1+i}(\delta^{(j_2)}_{R_1}(a)) \otimes \delta^{(i_1)}_{R_2}(d)(\sigma_q^{i_1}(\delta^{(i)}_{R_1\otimes R_2}(c\otimes b))).$$

This gives

$$\delta^{(k)}_{R_1\otimes R_2}((a\otimes b)(c\otimes d)) = \sum_{i_1+i_2+j_1+j_2=k} \sigma_q^{i_1+i_2+j_1}(\delta^{(j_2)}_{R_1}(a))\sigma_q^{i_1}(\delta^{(i_2)}_{R_1}(c)) \otimes \sigma_q^{i_1+i_2}(\delta^{(j_1)}_{R_2}(b))\delta^{(i_1)}_{R_2}(d),$$

and thus

$$\delta^{(k)}_{R_1\otimes R_2}((a\otimes b)(c\otimes d)) = \sum_{i+j=k} \sigma_q^{i}(\delta^{(j)}_{R_1\otimes R_2}(a\otimes b))\delta^{(i)}_{R_1\otimes R_2}(c\otimes d).$$

This is part 4 of Definition 2.4.
We now prove part 5. Let $(k, l) \in \mathbb{N}^2$ and $(a, b) \in R_1 \times R_2$. We have

$$\delta^{(k)}_{R_1\otimes R_2} \circ \delta^{(l)}_{R_1\otimes R_2}(a\otimes b) = \sum_{i+j=l, i_1+j_1=k} q^{ij_1} \binom{j_1+j}{j_1}_q \binom{i_1+i}{i}_q \sigma_q^{i_1+i}(\delta^{(j_1+j)}_{R_1}(a)) \otimes \delta^{(i_1+i)}_{R_2}(b),$$

that is

$$\delta^{(k)}_{R_1\otimes R_2} \circ \delta^{(l)}_{R_1\otimes R_2}(a\otimes b) = \sum_{r+s=k+l} \sigma_q^{r}(\delta^{(s)}_{R_1}(a)) \otimes \delta^{(r)}_{R_2}(b)(\sum_{i+j=k, i\leq s, j\leq r} \binom{r}{j}_q \binom{s}{i}_q q^{i(r-j)}).$$

Using part 5 of Proposition 2.2, we obtain

$$\delta^{(k)}_{R_1\otimes R_2} \circ \delta^{(l)}_{R_1\otimes R_2}(a\otimes b) = \binom{k+l}{k}_q \sum_{r+s=k+l} \sigma_q^{r}(\delta^{(s)}_{R_1}(a)) \otimes \delta^{(r)}_{R_2}(b),$$

that is

$$\delta^{(k)}_{R_1\otimes R_2} \circ \delta^{(l)}_{R_1\otimes R_2}(a\otimes b) = \binom{k+l}{k}_q \delta^{(k+l)}_{R_1\otimes R_2}(a\otimes b).$$

2.3 Twisted ring of formal power series

This paragraph is devoted to the relations between ID_q-rings and rings of formal power series. By encoding all properties of an iterative q-difference operator into twisted formal power series, Property 2.15 provides us with a very powerful tool for the proofs to come. This kind of twisted ring appears already in the work of Yves André (see [1]).

Definition 2.12 *Let (R, δ_R^*) be an iterative q-difference ring. The twisted ring $R^{\sigma_q}[[T]]$ of formal series with coefficients in R is defined as follows : the additive structure of $R^{\sigma_q}[[T]]$ is the same as the one of $R[[T]]$, the multiplicative structure is given by*

$$\lambda T^r * \mu T^k := \sigma_q^r(\mu)\lambda T^{r+k}$$

and extended by distributivity to $R[[T]]$.

We will denote by "." the usual multiplication law on $R[[T]]$.

Lemma 2.13 *The twisted ring $(R^{\sigma_q}[[T]], +, *)$ as in Definition 2.12 is a non commutative ring with unity. We will denote by "." the usual multiplication law on $R[[T]]$.*

Proof
We have :

$$\lambda T^r * 1 = \lambda T^r * T^0 = \sigma_q^r(1)\lambda T^{r+0} = \lambda T^r = 1 * \lambda T^r = \sigma_q^0(\lambda)T^r = \lambda T^r.$$

Thus 1 is a neutral element for the twisted multiplication $*$.
Let us prove then, that $*$ is associative.

$$\nu T^s * (\lambda T^r * \mu T^k) = \nu T^s * (\sigma_q^r(\mu)\lambda T^{r+k}) = \sigma_q^{r+s}(\mu)\sigma_q^s(\lambda)\nu T^{r+s+k}$$

and

$$(\nu T^s * \lambda T^r) * \mu T^k = (\sigma_q^s(\lambda)\mu T^{r+s}) * \mu T^k = \sigma_q^{r+s}(\mu)\sigma_q^s(\lambda)\nu T^{r+s+k}$$

give

$$\nu T^s * (\lambda T^r * \mu T^k) = (\nu T^s * \lambda T^r) * \mu T^k.$$

The product $*$ is therefore associative.
Now, we want to introduce an iterative q-difference operator on $(R^{\sigma_q}[[T]], +, .)$, that is to say a collection of maps δ_T^* which satisfies all the properties of Definition 2.4.
First we need an automorphism σ_q on $(R^{\sigma_q}[[T]], +, .)$ such that $(R^{\sigma_q}[[T]], +, .)$ is a q-difference ring extension of F. We put $\sigma_q(aT^i) := \sigma_q(a)q^iT^i$ for all $i \in \mathbb{N}$ and $a \in R$. By extending this definition R-linearly, $R^{\sigma_q}[[T]]$ becomes a q-difference ring extension of F. We put $\delta_T^{(k)}(T^r) := \binom{r}{k}_q T^{r-k}$ for all $(k, r) \in \mathbb{N}^2$ and extend this definition by R-linearity. Obviously $(\delta_T^{(k)})_{k\in\mathbb{N}}$ is an iterative q-difference operator over $(R^{\sigma_q}[[T]], +, .)$ (see Definition 2.4).

Definition 2.14 *For all $a \in R$,*

$$\mathbf{T}_a(T) := \sum_{k\in\mathbb{N}} \delta_R^{(k)}(a)T^k.$$

*is called the q-**iterative Taylor series** of a.*
Two iterative q-difference operators δ_R^* and $\tilde{\delta}_R^*$ are called equivalent (viz $\delta_R^* \sim \tilde{\delta}_R^*$), if there exist numbers n and m in $\mathbb{N}$ such that $\mathbf{T}_a(T^n) = \tilde{\mathbf{T}}_a(T^m)$ for all $a \in R$, where $\mathbf{T}_a$ denotes the q-iterative Taylor series associated to $\tilde{\delta}_R^*$.

Proposition 2.15 *Let R be a q-difference ring extension of F and let $\delta_R^* = (\delta_R^{(k)})_{k\in\mathbb{N}}$ be a sequence of maps from R to R. Let δ_T^* be the iterative q-difference operator of $(R^{\sigma_q}[[T]], +, .)$ defined previously, and let $\mathbf{I}$ denote the map*

$$\mathbf{I}: \qquad R^{\sigma_q}[[T]] \longrightarrow R, \qquad \textstyle\sum_{k\in\mathbb{N}} a_k T^k \longmapsto a_0\ .$$

Then δ_R^* is an iterative q-difference operator for R if and only if

1. *$\mathbf{T}$ is a ring homomorphism from R to $(R^{\sigma_q}[[T]], +, *)$, with $\mathbf{I} \circ \mathbf{T} = id_R$,*
2. *$\delta_T^{(k)} \circ \mathbf{T} = \mathbf{T} \circ \delta_R^{(k)}$ for all $k \in \mathbb{N}$.*

Proof
The fact that $\mathbf{T}$ is additive is equivalent to statement 3 in Definition 2.4. The compatibility of $\mathbf{T}$ with the multiplication law in R and the twisted law $*$ in $R^{\sigma_q}[[T]]$, in the case where δ_R^* is an iterative q-difference operator comes from the equations

$$\mathbf{T}_{ab}(T) := \sum_{k\in\mathbb{N}} \delta_R^{(k)}(ab)T^k = \sum_{k\in\mathbb{N}} (\sum_{i+j=k} \sigma_q^i(\delta_R^{(j)}(a))\delta_R^{(i)}(b))T^k = \mathbf{T}_a(T) * \mathbf{T}_b(T).$$

The second property is equivalent to the property 5 of the same definition.

2.4 Iterative q-difference morphisms and iterative q-difference ideals

Definition 2.16 *Let (R, δ_R^*) and (S, δ_S^*) be two iterative q-difference rings. We say that a ring morphism ϕ from R to S is an **iterative q-difference morphism** if and only if $\delta_S^{(k)} \circ \phi = \phi \circ \delta_R^{(k)}$ for all $k \in \mathbb{N}$.*

The set of all iterative q-difference morphisms from R to S is denoted by $Hom_{ID_q}(R, S)$.
An iterative q-difference ideal $I \subset R$ (ID_q-ideal) is an ideal of R stable by $\delta_R^{(k)}$ for all $k \in \mathbb{N}$.

Lemma 2.17 *Let I be an ID_q-ideal of an iterative q-difference ring R, that is to say that I is stable under the action of δ_R^*. Then the radical of I is a ID_q-ideal.*

Proof
Assume that q is a n-th primitive root of unity. From $\delta_R^{(1)} = \frac{\sigma_q - id}{(q-1)t}$, we get

$$\sigma_q(a) = (q-1)t(\delta_R^{(1)}(a) - a), \text{for all } a \in I.$$

This shows that $\sigma_q(a) \in I$ for all $a \in I$. Thus I is a σ_q-ideal. Conversely, if I is a σ_q-ideal then it is a $\delta_R^{(1)}$-ideal. Now, let us consider $a \in \sqrt{I}$. There exists $m \in \mathbb{N}$ such that $a^m \in I$. But, $\sigma_q(a^m) = (\sigma_q(a))^m \in I$. Thus $\sigma_q(a) \in \sqrt{I}$.
Now, we will prove by induction that for all $i < n$, $\delta_R^{(i)}$ stabilizes $\sqrt{I}$.
It is true for $i = 1$. If it is true for $k < n-1$, then $k < n$ and we have :

$$\delta_R^{(1)} \circ \delta_R^{(k-1)} = \binom{k}{1}_q \delta_R^{(k)}$$

where $\binom{k}{1}_q \neq 0$ because $k < n$. We have that $\delta_R^{(1)}$ and $\delta_R^{(k-1)}$ stabilize $\sqrt{I}$ (by first step and by inductive assumption). Thus $\delta_R^{(k)}$ stabilizes $\sqrt{I}$. This concludes the proof by induction. It remains to consider the case where $k = n$. Let $a \in \sqrt{I}$ and $m \in \mathbb{N}$ such that $a^m \in I$. We have:

$$\delta_R^{(nm)}(a^m) = \sum_{i_1+\ldots+i_m=nm} \sigma_q^{i_2+\ldots+i_m}(\delta_R^{(i_1)}(a))\ldots\sigma_q^{i_m}(\delta_R^{(i_{m-1})}(a))\delta_R^{(i_m)}(a). \tag{9}$$

Because $\sigma_q^n = id$, we can rewrite the equation (9) as follows $\delta_R^{(nm)}(a^m) = (\delta_R^{(n)}(a))^m + B$ with

$$B = \sum_{i_1+\ldots+i_m=nm}^{*} \sigma_q^{i_2+\ldots+i_m}(\delta_R^{(i_1)}(a))\ldots\sigma_q^{i_m}(\delta_R^{(i_{m-1})}(a))\delta_R^{(i_m)}(a)$$

where $\sum^*_{i_1+\ldots+i_m=nm}$ means that we only consider the $(i_1, \ldots, i_m)$ such that there exists at least one j with $i_j < n$. We have already proved by induction that $\sqrt{I}$ is stable by σ_q and by $\delta_R^{(i)}$ for $i < n$. This implies that $B \in \sqrt{I}$. Then $(\delta_R^{(n)}(a))^m$ belongs to $\sqrt{I}$ since $\delta_R^{(nm)}(a^m) \in I$ because I itself is an ID_q-ideal. It follows $\delta_R^{(n)}(a) \in \sqrt{I}$.

So we have proved that $\sqrt{I}$ is stable under $\delta_R^{(k)}$ for all $k \leq n$. Using the formula $\delta_R^{(i)} \circ \delta_R^{(k-i)} = \binom{k}{i}_q \delta_R^{(k)}$ and an inductive proof, we easily show that $\sqrt{I}$ is stable under $\delta_R^{(k)}$ for all $k \notin n\mathbb{N}$. The proof for $k \in n\mathbb{N}$ is an analogue of the case $k = n$. Therefore $\sqrt{I}$ is an ID_q-ideal.

Remark 2.18 (Classical case) *For q not equal to a root of unity, the proof of the previous lemma is more elementary (see Lemma 1.7 in [25]). The reason is that if I is a σ_q-ideal then its radical is obviously a σ_q-ideal because σ_q is an automorphism.*

2.4.1 Extending iterative q-difference operator

Proposition 2.19 *Let R be an integral domain, and let $S \subset R$ be a multiplicatively closed subset of R* ***stable under the action of*** *σ_q such that $0 \notin S$. Let δ_R^* be an iterative q-difference operator on R. Then there exists a unique iterative q-difference operator $\delta_{S^{-1}R}^*$ extending δ_R^* to $S^{-1}R$.*

Proof
Because δ_R^* is an iterative q-difference operator, the application $\mathbf{T} : R \mapsto (R^{\sigma_q}[[T]], +, *)$ defined by $a \mapsto \mathbf{T}_a(T)$ is a ring homomorphism (see 2.15). Since R is commutative, we have

$$\mathbf{T}_{ab}(T) = \mathbf{T}_a(T) * \mathbf{T}_b(T) = \mathbf{T}_b(T) * \mathbf{T}_a(T) \text{ for all } a, b \in R.$$

This allows us to define the quotient $\frac{\mathbf{T}_a(T)}{\mathbf{T}_b(T)}^*$ of $\mathbf{T}_a(T)$ by $\mathbf{T}_b(T)$ with respect to the multiplication $*$ for all $(a, b) \in R \times R^*$. Thereby, the map $\mathbf{T}$ uniquely extends to a homomorphism $\tilde{\mathbf{T}} : S^{-1}R \mapsto ((S^{-1}R)^{\sigma_q}[[T]], +, *)$ via $\frac{a}{b} \mapsto \tilde{\mathbf{T}}_{\frac{a}{b}}(T) := \frac{\mathbf{T}_a(T)}{\mathbf{T}_b(T)}^*$. Define $\delta_{S^{-1}R}^{(k)}(\frac{a}{b})$ to be the coefficient of T^k in $\tilde{\mathbf{T}}_{\frac{a}{b}}(T)$. Then the collection of maps $(\delta_{S^{-1}R}^{(k)})_{k\in\mathbb{N}}$ of $S^{-1}R$ to itself satisfy conditions 1 and 2 of Proposition 2.15. Thus $(\delta_{S^{-1}R}^{(k)})_{k\in\mathbb{N}}$ is an iterative q-difference operator for $S^{-1}R$. We also have

$$\tilde{\mathbf{T}}_{\delta_{S^{-1}R}^{(k)}(a)}(T) = \delta_T^{(k)}(\tilde{\mathbf{T}}_a(T)) \text{ for all } a \in R,\ k \in \mathbb{N}.$$

The Taylor series associated to both sides of the previous equation extend uniquely to $(S^{-1}R)^{\sigma_q}[[T]]$ and since they coincide on $R^{\sigma_q}[[T]]$, they have to be equal. Then

$$\tilde{\mathbf{T}}_{\delta_{S^{-1}R}^{(k)}(a)}(T) = \delta_T^{(k)}(\tilde{\mathbf{T}}_a(T)) \text{ for all } a \in S^{-1}R,\ k \in \mathbb{N}.$$

By Proposition 2.15, we get that $(\delta_{S^{-1}R}^{(k)})_{k\in\mathbb{N}}$ is an iterative q-difference operator of $S^{-1}R$ which uniquely extends $(\delta_R^{(k)})_{k\in\mathbb{N}}$.

Remark 2.20 *Let (R, δ_R^*) be an integral iterative q-difference ring. It is obvious that the set S of non zero divisors of R is a multiplicatively closed set and moreover stable under the action of σ_q.*

Remark 2.21 *In this paragraph we did not mention the possibilities of extending an iterative q-difference operator over a field K to a finitely generated separable field extension E/K. In fact, this problem appears already in the classical q-difference Galois theory : extending σ_q to an algebraic extension gives rise to uniqueness problems. Here is an example. Consider a difference field (K, σ_q), where σ_q is the identity on some algebraically closed field C containing $\mathbb{Q}$, K contains a solution y of $\sigma(x) = cx$, where $c \in C$ is non-zero and is not a root of unity. Moreover assume that K does not contain the n-th roots of y for some $n > 1$. Consider the extension of K given by $b^n = y$. Then $\sigma(b) = rb$, where $r^n = c$. The possible choices for σ on $K(b)$ depend on the choices of r, and there are n possibilities, which give rise to n non-isomorphic difference field extensions of K.*
But by chance, we will not have to handle such kind of extension till the end of the paper.

2.5 The Wronskian determinant

In classical Galois theory of q-difference equations, there exists an analogue of the Wronskian called the q-Wronskian or the Casoratian. If we consider a σ_q-module $\mathcal{M}$ over a field K and a family $\mathcal{F} := \{y_1, ..., y_m\}$ of elements of $\mathcal{M}$, we will define the q-Wronskian of the family $\mathcal{F}$ as

$$W_q(y_1, ..., y_m) := det((\sigma_q^{i-1}(y_j))_{1 \leq i,j \leq m}).$$

The nullity of the q-Wronskian gives a criterion for linear independence of the y_i's (see for instance [15]). But when q is a root of unity, the q-Wronskian could vanish for other reasons (for instance because $\sigma_q^n = id$). Thus, we have to change the notion of q-Wronskian for iterative q-difference operators in order to get a similar criterion to the one in the classical theory.

Theorem 2.22 *Let (K, δ_K^*) be an iterative q-difference field with field of constants C. Then for any elements $x_1, ..., x_r$ of K linearly independent over C, the iterative Taylor series $\mathbf{T}_{x_1}, ..., \mathbf{T}_{x_r}$ are linearly independent over K.*

Proof
This statement is obviously true for $r = 1$. We will proceed by induction on r. Let (H_r) be the hypothesis of induction, i.e., for any elements $x_1, ..., x_r$ of K linearly independent over C, the iterative Taylor series $\mathbf{T}_{x_1}, ..., \mathbf{T}_{x_n}$ are linearly independent over K. Suppose that (H_{r-1}) is true and let $x_1, ..., x_r \in K$ be linearly independent over C. Assume that $\mathbf{T}_{x_1}, ..., \mathbf{T}_{x_r}$ are linearly dependent over K, i.e. :

$$\mathbf{T}_{x_r} = \sum_{j=1}^{r-1} a_j \mathbf{T}_{x_j}$$

where $a_j \in K$ not all equal to zero. This relation implies that

$$\delta^{(k)}(x_r) = \sum_{j=1}^{r-1} a_j \delta^{(k)}(x_j) \text{ for all } k \in \mathbb{N} \tag{10}$$

We will prove that $\sigma_q(a_j) = a_j$ for all $1 \leq j \leq r-1$. First of all, let us remark that if $x_1, ..., x_{r-1} \in K$ are linearly independent over C then $\sigma_q(x_1), ..., \sigma_q(x_{r-1}) \in K$ are linearly independent over C.
Because of $\delta^{(1)} = \frac{\sigma_q - id}{(q-1)t}$ and from Equation (10), we have :

$$\sigma_q(\delta^{(k)}(x_r)) - \delta^{(k)}(x_r) = \sum_{j=1}^{r-1} a_j \sigma_q(\delta^{(k)}(x_j)) - \sum_{j=1}^{r-1} a_j \delta^{(k)}(x_j)$$

and

$$\sigma_q(\delta^{(k)}(x_r)) = \sum_{j=1}^{r-1} \sigma_q(a_j) \sigma_q(\delta^{(k)}(x_j)).$$

We also obtain that

$$\sum_{j=1}^{r-1}(\sigma_q(a_j)-a_j)\sigma_q(\delta^{(k)}(x_j))=0$$

for all $k\in\mathbb{N}$. Because $\sigma_q(\delta^{(k)}(x_j))=\frac{1}{q^k}\delta^{(k)}(\sigma_q(x_j))$, we get

$$\sum_{j=1}^{r-1}(\sigma_q(a_j)-a_j)(\delta^{(k)}(\sigma_q(x_j)))=0$$

for all $k\in\mathbb{N}$. This means that $\sum_{j=1}^{r-1}(\sigma_q(a_j)-a_j)\mathbf{T}_{\sigma_q(x_j)}=0$. Since $x_1,...,x_{r-1}\in K$ are linearly independent over C, $\sigma_q(x_1),...,\sigma_q(x_{r-1})\in K$ are linearly independent over C. Thus we can apply the induction hypothesis (H_{r-1}) to the set of elements $\sigma_q(x_1),...,\sigma_q(x_{r-1})$ of K and so $\sigma_q(a_j)=a_j$ for $1\leq j\leq r-1$ as desired.
For all $k,i\in\mathbb{N}$, we have

$$\binom{i+k}{k}_q\delta^{(i+k)}(x_r)=\delta^{(i)}\delta^{(k)}(x_r)=\sum_{j=1}^{r-1}\sum_{l=0}^{i}\sigma_q^{i-l}(\delta^{(l)}(a_j))\binom{i+k-l}{k}_q\delta^{(i+k-l)}(x_j)$$

and

$$\binom{i+k}{k}_q\delta^{(i+k)}(x_r)=\binom{i+k}{k}_q\sum_{j=1}^{r-1}a_j\delta^{(k)}(x_j).$$

Because $\sigma_q(a_j)=a_j$ for $1\leq j\leq r-1$, the term for $l=0$ on the right hand side is equal to the left hand side, thus

$$\sum_{j=1}^{r-1}\sum_{l=1}^{i}\sigma_q^{i-l}(\delta^{(l)}(a_j))\binom{i+k-l}{k}_q\delta^{(i+k-l)}(x_j)=0. \tag{11}$$

For $i=1$, we deduce from equation (11) that

$$\sum_{j}^{r-1}\delta^{(1)}(a_j)\delta^{(k)}(x_j)=0.$$

By applying $\delta^{(1)}$, we obtain :

$$\sum_{j}^{r-1}\sigma_q(\delta^{(1)}(a_j))\delta^{(1)}(\delta^{(k)}(x_j))+\sum_{j}^{r-1}\delta^{(1)}(\delta^{(1)}(a_j))\delta^{(k)}(x_j)=0,$$

i.e., since $\sigma_q^r\delta^{(s)}=\frac{1}{q^{rs}}\delta_R^{(s)}\sigma_q^r$ for all $r,s\in\mathbb{N}$, and the a_j's are fixed by σ_q,

$$\sum_{j}^{r-1}\frac{q(q^{k+1}-1)}{q-1}\delta^{(1)}(a_j)\delta^{(k+1)}(x_j)+\sum_{j}^{r-1}(q+1)(\delta^{(2)}(a_j))\delta^{(k)}(x_j)=0.$$

For $i = 2$, we deduce from equation (11) that

$$\sum_j^{r-1} \sigma_q(\delta^{(1)}(a_j)) \binom{k+l}{k}_q \delta^{(k+1)}(x_j) + \sum_j^{r-1} \delta^{(2)}(a_j)\delta^{(k)}(x_j) = 0.$$

By subtracting this from the equality above, we find :

$$\sum_j^{r-1} \delta^{(2)}(a_j)\delta^{(k)}(x_j) = 0.$$

By induction, the same arguments yields

$$\sum_j^{r-1} \delta^{(i)}(a_j)\delta^{(k)}(x_j) = 0 \text{ for } k \geq 0 \text{ and } i \geq 1.$$

This leads to

$$\sum_j^{r-1} \delta^{(i)}(a_j)\mathbf{T}_{x_j} = 0.$$

By hypothesis of induction (H_{r-1}), this implies that $\delta^{(i)}(a_j) = 0$ for all $i \geq 1$ and all $1 \leq j \leq r-1$. Hence all the a_j's are constants and lie in C. But we have $x_n = \sum_{j=1}^{r-1} a_j x_j$ (see equation (11) for $k = 0$) and thus by assumption of C-linearly independence of $x_1, ..., x_r$, we get that $a_j = 0$ for all $1 \leq j \leq r-1$. This is the end of the proof.

Corollary 2.23 *In the notation of Theorem 2.22, there exist numbers $d_1, ..., d_r \in \mathbb{N}$ such that*

$$det((\delta^{(d_i)}(x_j))_{i,j=1}^r) \neq 0.$$

Definition 2.24 *Let (K, δ_K^*) be an ID_q field with $C(K) = C$ and let $x_1, ..., x_r \in K$ be linearly independent over C. The smallest numbers $d_1, ..., d_r \in \mathbb{N}$ (in lexicographical order) such that $det((\delta^{(d_i)}(x_j))_{i,j=1}^r) \neq 0$ (which exist by Corollary 2.23) are called the **difference orders** of $x_1, ..., x_r$. The determinant*

$$wr(x_1, ..., x_r) := det((\delta^{(d_i)}(x_j))_{i,j=1}^r)$$

*is called the **Wronskian determinant** of $x_1, ..., x_r$.*

3 Iterative q-difference modules

Until the end of this article, we will assume that q is a n-th primitive root of unity contained in an algebraically closed field C. But we do not make any assumption about the characteristic of the field C.
In Section 2, we have defined iterative q-difference rings. Following the classical way, we extend this concept to modules, in order to get a suitable notion of iterative q-difference equations associated to these modules.

Definition 3.1 *Let (R, δ_R^*) be an iterative q-difference ring. Let M be a a free R-module of finite type over R. We will say that (M, δ_M^*) is an* ***iterative q-difference module*** *if there exists a family of maps $\delta_M^* = (\delta_M^{(k)})_{k\in\mathbb{N}}$, such that for all $i, j, k \in \mathbb{N}$*

1. $\delta_M^{(0)} = id_M$,
2. $\phi_M := (q-1)t\delta_M^{(1)} + id_M$ *is a bijective map from M to M,*
3. $\delta_M^{(k)}$ *is an additive map from M to M,*
4. $\delta_M^{(k)}(am) = \sum_{i+j=k} \sigma_q^i(\delta_R^{(j)}(a))\delta_M^{(i)}(m)$ *for $a \in R$ and $m \in M$,*
5. $\delta_M^{(i)} \circ \delta_M^{(j)} = \binom{i+j}{i}_q \delta_M^{(i+j)}$.

The set of all iterative q-difference modules over R is denoted by $IDM_q(R)$.

Remark 3.2 (Classical case) *If q is not a root of unity, it is easy to see that $\phi_M(am) = \sigma_q(a)\phi_M(m)$ for all $a \in R$ and $m \in M$. Moreover, $\delta_M^{(k)} = \frac{\delta_M^{(1)^k}}{[k]_q!}$. Thus, in the case where q is not a root of unity, an ID_q-module is nothing else than a q-difference module in the sense of [25].*

As in 2.5, we easily show that we have for all $j, i \in \mathbb{N}$,

$$\phi_M^j \delta_M^{(i)} = \frac{1}{q^{ji}} \delta_M^{(i)} \phi_M^j. \tag{12}$$

Definition 3.3 *Let (M, δ_M^*) and (N, δ_N^*) be two iterative q-difference modules over R and let $\phi \in Hom_R(M, N)$. We will say that ϕ is an* ***iterative q-difference homomorphism*** *if $\delta_N^{(k)} \circ \phi = \phi \circ \delta_M^{(k)}$ for all $k \in \mathbb{N}$.*

Definition 3.4 *Let (R, δ_R^*) be an iterative q-difference ring. Let (M, δ_M^*) be an iterative q-difference module over R. The $C(R)$-module*

$$V_M := \bigcap_{k\in\mathbb{N}} Ker(\delta_M^{(k)})$$

is called the ***solution space*** *of the iterative q-difference module M. We will say that M is a* ***trivial*** *iterative q-difference module if $M \simeq V_M \otimes_{C(R)} R$.*

Theorem 3.5 *Let (L, δ_L^*) be an iterative q-difference field. Let us denote by $IDM_q(L)$ the category with objects the iterative q-difference modules over L and morphisms the iterative q-difference morphisms. Then $IDM_q(L)$ is a neutral Tannakian category over $C(L)$. The unit object is (L, δ_L^*).*

We refer to [16] for the fact that $IDM_q(L)$ is an abelian category, the case for iterative differential modules being the same as the one of iterative q-difference modules. For M and N two objects of $IDM_q(L)$, we define the tensor product $M \otimes N := M \otimes_L N$ by the usual tensor product as L-modules and turn it to an ID_q-module via

$$\delta^{(k)}_{M\otimes N}(x \otimes y) = \sum_{i+j=k} \phi^j_M(\delta^{(i)}_M(x)) \otimes \delta^{(j)}_N(y)$$

for all $x \in M, y \in N$. The proof that $(\delta^{(k)}_{M\otimes N})_{k\in\mathbb{N}}$ is an iterative q-difference operator on $M \otimes N$ is analogous to the proof of Proposition 2.11.
The dual of an object M of $IDM_q(L)$ is then given by $M^* = Hom_L(M, L)$ together with

$$\delta^{(k)}_{M^*}(f) = \sum_{i+j=k} (-1)^i q^{\frac{i(i+1)}{2}} \sigma^i_q(\delta^{(j)}_L) \circ f \circ \delta^{(i)}_M \circ \phi^{-i}_M$$

for all $f \in M^*$. The proof that $(M, \delta^*_{M^*})$ is an iterative q-difference module is left to the reader. We just recall that if (M, ϕ_M) is a q-difference module in the sense of [25], then the M^* is endowed with a q-difference module structure via

$$\phi_{M^*}(f) := \sigma_q \circ f \circ \phi^{-1}_M.$$

The evaluation $\epsilon : M \otimes M^* \to \mathbf{1}_{IDM_q(L)} = L$ sends $x \otimes f$ to $f(x)$, and the coevaluation $\eta : L \to M^* \otimes M$ is defined by mapping 1 to $\sum_{i=1}^n x^*_i \otimes x_i$, where $\{x_i\}_{i=1}^n$ denotes an L-basis of M and $\{x^*_i\}_{i=1}^n$ the associated dual basis of M^*. Note that the definition of η does not depend on the chosen basis. It remains to show that ϵ and η are ID_q-homomorphism and that they satisfy $(\epsilon \otimes id_M) \circ (id_M \otimes \eta) = id_M$ and $(id_{M^*} \otimes \epsilon) \circ (\eta \otimes id_{M^*}) = id_{M^*}$ for all objects M of $IDM_q(L)$. We have

$$\begin{aligned}
\epsilon \circ \delta^{(k)}_{M\otimes M^*}(x \otimes f) &= \epsilon\left(\textstyle\sum_{i+j=k} \delta^{(i)}_M(x) \otimes \phi^i_{M*}(\delta^{(j)}_{M^*}(f))\right) = \textstyle\sum_{i+j=k} \phi^i_{M^*}(\delta^{(j)}_{M^*}(f))(\delta^{(i)}_M(x)) \\
&= \textstyle\sum_{i+j=k} \sum_{l=0}^j (-1)^l q^{l(l+1)/2} \sigma^{i+l}_q(\delta^{(j-l)}_L) \circ f \circ \delta^{(l)}_M \circ \phi^{-(i+l)}_M(\delta^{(i)}_M(x)) \\
&= \textstyle\sum_{i+j=k} \sum_{l=0}^j (-1)^l q^{l(l+1)/2} \sigma^{l+i}_q(\delta^{(j-l)}_L) \circ f \circ q^{i(i+l)} \binom{i+l}{i}_q \delta^{(i+l)}_M(\phi^{-(i+l)}_M(x))
\end{aligned}$$

and thus

$$\epsilon \circ \delta^{(k)}_{M\otimes M^*}(x \otimes f) = \sum_{i_*+j_*=k} \sigma^{i_*}_q(\delta^{(j_*)}_L) \circ f \circ \delta^{(i_*)}_M(\phi^{-i_*}_M(x)) \left(\sum_{i=0}^{i_*} (-1)^i q^{i(i-1)/2} \binom{i_*}{i}_q \right).$$

By expanding $(1-1)_{i_*}$, we see that the inner sum equals zero if and only if $i_* \neq 0$. We thus get

$$\epsilon \circ \delta^{(k)}_{M\otimes M^*}(x \otimes f) = \delta^{(k)}_L f(x) = \delta^{(k)}_L \circ \epsilon(x \otimes f).$$

The proof for η is analogous.

Let $x = \sum_{i=1}^{n} a_i x_i$ be in M, then $(\epsilon \otimes id_M) \circ (id_M \otimes \eta)(x) = \epsilon \otimes id_M(x \otimes (\sum_{i=1}^{n} x_i^* \otimes x_i)) = \epsilon \otimes id_M(\sum_{i=1}^{n}(x \otimes x_i^*) \otimes x_i) = \sum_{i=1}^{n} x_i^*(x) \otimes x_i = \sum_{i=1}^{n} a_i x_i = x$. Again, the second statement is proved analogously. Finally,we note that

$$End_{IDM_q(L)}(\mathbf{1}_{IDM_q(L)}) = End_{ID_q}(L) = C(L),$$

finishing the proof.

3.1 Iterative q-difference modules and projective systems

In this paragraph, we will show that iterative q-difference operators and iterative derivations are closely related. First of all, let us consider the following proposition :

Proposition 3.6 *Let q be a n-th root of unity. Let (L, δ_L^*) be an iterative q-difference field and let (M, δ_M^*) be an iterative q-difference module over L. Set $L_0 = \cap_{j \notin n\mathbb{N}} Ker(\delta_L^{(j)})$ and $M_0 = \cap_{j \notin n\mathbb{N}} Ker(\delta_M^{(j)})$. Then $(M_0, (\delta_M^{(nk)})_{k \in \mathbb{N}})$ is an iterative differential module over L_0 (see [16]).*

Therefore, one could hope to get as in [16] some projective system deeply associated to our iterative q-difference module. But the problem is the following. In the case of characteristic zero we may regain all the iterative q-difference operators only with the knowledge of $\delta_M^{(1)}$ and $\delta_M^{(n)}$. This is due to the formula $(\delta_M^{(n)})^{n^{k-1}} = (n^{k-1})! \delta_M^{(n^k)}$ and to the fact that the family $\{\delta_M^{(1)}, (\delta_M^{(n^k)})_{k \in \mathbb{N}}\}$ generates the iterative q-difference operator. But in positive characteristic, we have to consider the whole family $\{\delta_M^{(1)}, (\delta_M^{(np^k)})_{k \in \mathbb{N}}\}$ to recover the iterative q-difference operator. Therefore, we can only obtain projective systems in positive characteristic. But, this fact is not a hindrance to the construction of iterative q-difference equations in characteristic 0.
As we have mentioned in the introduction, we will show that in positive characteristic, the category of iterative q-difference modules is closely related to the category of some specific projective systems. In this paragraph we obtain an equivalence between these two categories. This is a very nice tool because it allows us translate our computations from the non commutative world of iterative q-difference modules to the world of linear algebra, via the vector spaces associated to the projective systems.
This comparison between iterative differential modules and specific projective systems appears already in the work of B.H. Matzat and M. van der Put. But to obtain an equivalence of categories between the projective systems linked to iterative derivations and the ones associated to iterative q-difference, we need to have $q^p = 1$ and this assumption makes no sense. A hope for realizing this equivalence will be perhaps to rebuild both theories over non-algebraically closed base rings, such as $\mathbb{Z}/p^m\mathbb{Z}$ and try to reach the Witt vectors. But this is a a future research topic.
However, it is very easy to obtain from a iterative q-difference module an iterative differential module (see 3.6).

3.1.1 Case of characteristic p

Let (L, δ_L^*) be an iterative q-difference field of characteristic p and let (M, δ_M^*) be an iterative q-difference module over L. In positive characteristic, we have the exact analogue of the equivalence of categories obtained by Matzat in [16] Theorem 2.8.
Put $L_1 = Ker(\delta_L^{(1)})$ and $L_{k+1} = \cap_{0 \leq j < k} Ker(\delta_L^{(np^j)}) \cap L_1$ for $k > 1$ and $L_0 = L$.
Put $M_1 = Ker(\delta_M^{(1)})$, $M_{k+1} = \cap_{0 \leq j < k} Ker(\delta_M^{(np^j)}) \cap M_1$ for all $k > 1$ and $M_0 = M$.

Proposition 3.7 *1. M_k is an L_k-vector space of finite dimension,*

2. $(M_k, \phi_k)_{k \in \mathbb{N}}$, where ϕ_k denotes the obvious injection from M_{k+1} to M_k, is a projective system,

3. the map ϕ_k extends to an isomorphism of L_k-vector-spaces from $M_{k+1} \otimes L_k$ to M_k.

Proof
The two first statements are obvious. Let us prove the third one. Let $(m_1, ..., m_s)$ be s elements of M_{k+1} linearly independent over L_{k+1}. Suppose that there are linearly dependent over L_k and let

$$\sum_{i=i_0, i \in \mathcal{I}} \lambda_i m_i = 0 \tag{13}$$

be a non trivial linear combination of the m_i's over L_k where $\mathcal{I}$ denotes a set of index of minimal length. Without loss of generality we may assume that $\lambda_{i_0} = 1$.
For $np^k \leq j < np^{k+1}$, apply $\delta_M^{(j)}$ to Equation (13). We thus have, since $m_i \in M_{k+1}$,

$$\sum_{i=i_0, i \in \mathcal{I}} \sum_{s=0}^{j} \sigma_q^s(\delta_L^{(j-s)}(\lambda_i)) \delta_M^{(s)}(m_i) = \sum_{i=i_0, i \in \mathcal{I}} \delta_L^{(j)}(\lambda_i) m_i = 0. \tag{14}$$

Substracting (17) from (16), we obtain

$$\sum_{i=i_0, i \in \mathcal{I}} (\delta_L^{(j)}(\lambda_i) - \lambda_i) m_i = 0. \tag{15}$$

By minimality, we have $\delta_L^{(j)}(\lambda_i) - \lambda_i = 0$ for all $i > i_0$ and for all $np^k \leq j < np^{k+1}$. That is to say that $\lambda_i \in L_{k+1}$. Because $(m_1, ..., m_s)$ are linearly independent over L_{k+1}, we get that $\lambda_i = 0$ for all i. This is a contradiction. We thus have $dim_{L_{k+1}}(M_{k+1}) \leq dim_{L_k}(M_k)$. For all $k \in \mathbb{N}$, the application $\delta_M^{(np^k)}$ is L_{k+2}-linear on M_{k+1} and $(\delta_M^{(np^k)})^p = 0$, so $dim_{L_{k+2}}(M_{k+2}) = dim_{L_{k+2}}(\mathrm{Ker}(\delta_{\mathrm{M}}^{(\mathrm{np^k})})|_{\mathrm{M_{k+1}}}) \geq \frac{1}{\mathrm{p}} \mathrm{dim_{L_{k+2}}(M_{k+1})} \geq \mathrm{dim_{L_{k+1}}(M_{k+1})}$, where the last inequality comes from the fact that $\delta_L^{(np^k)}$ is an L_{k+2}-linear endomorphism of L_{k+1} of order of nilpotence p.
But we also have $(\delta_M^{(1)})^n = 0$. Therefore, we have $dim_{L_1}(M_1) = dim_{L_1}(Ker(\delta_M^{(1)}|_M) \geq \frac{1}{n} dim_{L_1}(M) \geq dim_L(M)$, where the last inequality comes from the fact that $\delta_L^{(1)}$ is an L_1-linear endomorphism of L of order of nilpotence n (q is a n-th primitive root of unity).

3.1.2 Case of characteristic 0

Let (L, δ_L^*) be an iterative q-difference field of zero characteristic and let (M, δ_M^*) be an iterative q-difference module over L. Put, for all $k \in \mathbb{N}^*$, $L_k = \cap_{0\leq j<k} Ker(\delta_L^{(n^j)})$, $L_0' = Ker(\delta_L^{(1)})$ and $L_0 = L$.
Put, for all $k \in \mathbb{N}^*$, $M_k = \cap_{0\leq j<k} Ker(\delta_M^{(n^j)})$, $M_0' = Ker(\delta_M^{(1)})$ and $M_0 = M$.

Proposition 3.8 *1. M_k is a L_k-vector space of finite dimension.*

2. $M_k = M_1$ for all $k \geq 1$.

3. Let ϕ_1 be the obvious injection from M_1 to M_0'. Then the map ϕ_1 extends to a monomorphism of L_0'-vector-spaces from $M_1 \otimes L_0'$ to M_0'.

4. Let ϕ_0 be the obvious injection from M_0' to M_0. Then the map ϕ_0 extends to an isomorphism of L-vector-spaces from $M_0' \otimes L$ to M_0.

Proof
The first statement is obvious. Because $(\delta_M^{(n)})^{n^{k-1}} = (n^{k-1})!\delta_M^{(n^k)}$ for all $k \geq 1$ (see part 4 of Proposition 2.2), we have $M_k = M_1$ for all $k \geq 1$. The third statement is obvious.
We now prove the fourth statement. Let $(m_1, ..., m_s)$ be s elements of M_0' linearly independent over L_0'. Let us assume that they are linearly dependent over L and let us consider a non trivial linear combination of the m_i's over L where $\mathcal{I}$ denotes a set of index of minimal length :

$$\sum_{i=i_0, i\in\mathcal{I}} \lambda_i m_i = 0. \tag{16}$$

Without loss of generality we may assume that $\lambda_{i_0} = 1$.
Let us apply $\delta_M^{(1)}$ to Equation (16). We then have, since $m_i \in M_0'$,

$$\sum_{i=i_0, i\in\mathcal{I}} \sum_{s=0}^{1} \sigma_q^s(\delta_L^{(1-s)}(\lambda_i))\delta_M^{(s)}(m_i) = \sum_{i=i_0, i\in\mathcal{I}} \delta_L^{(1)}(\lambda_i)m_i = 0. \tag{17}$$

By subtracting (17) from (16), we obtain :

$$\sum_{i>i_0, i\in\mathcal{I}} (\delta_L^{(1)}(\lambda_i) - \lambda_i)m_i = 0. \tag{18}$$

By minimality, we have $\delta_L^{(1)}(\lambda_i) - \lambda_i = 0$ for all $i > i_0$, that is to say that $\lambda_i \in L_0'$. Because $(m_1, ..., m_s)$ are linearly independent over L_0', we get $\lambda_i = 0$ for all i. This is a contradiction. We then have $dim_{L_0'}(M_0') \leq dim_L(M)$.

Conversely, from $(\delta_M^{(1)})^n = 0$ and $(\delta_L^{(1)})^n = 0$ follows

$$dim_{L_0'}(M_0') = dim_{L_0'}(Ker(\delta_M^{(1)}|_M)) \geq \frac{1}{n} dim_{L_0'}(M) \geq dim_L(M).$$

3.1.3 Equivalence of categories in the case of positive characteristic

In this paragraph, we keep the notation of Paragraph 3.1.1.

Notation 3.9 *Let (L, δ_L^*) be an iterative q-difference field of characteristic p. Let us denote by $Proj_q(L)$ the category of projective systems $(N_k, \psi_k)_{k\in\mathbb{N}}$ over L with the properties:*

1. *N_k is an L_k-vector space of finite dimension and ψ_k is L_{k+1}-linear,*
2. *each ψ_k uniquely extends to an L_k-isomorphism*

$$\tilde{\psi}_k : L_k \otimes_{L_{k+1}} M_{k+1} \longrightarrow M_k.$$

Theorem 3.10 *Let (L, δ_L^*) be an iterative q-difference field of positive characteristic. Then the category $Proj_q(L)$ is equivalent to the category $IDM_q(L)$.*

Proof
We already saw in Proposition 3.7 how an object of $IDM_q(L)$ leads to an object of $Proj_q(L)$. Conversely, let us consider $(N_k, \psi_k)_{k\in\mathbb{N}}$ in the category $Proj_q(L)$. We will now construct its associated iterative q-difference module.
Put $M_0 := N_0$ and define $M_k := \psi_0 \circ \psi_1 \circ ... \psi_{k-1}(N_k)$. Then $M_k \subset M_{k+1} \subset ... \subset M_0$. Let $B_k = \{b_1, ..., b_m\}$ be an L_k-basis for M_k, then by property 2, B_k is an L-basis of M. Let $x \in M$, there exits $(\lambda_i)_{i=1,...,m} \in L^m$ such that $x = \sum_{i=1}^m \lambda_i b_i$. Then, for all $j < k$, set

$$\delta_M^{(j)}(x) := \sum_{i=1}^{m} \delta_L^{(j)}(\lambda_i) b_i.$$

This is possible because we want B_k to lie in the kernel of $\delta_M^{(j)}$ for $j < k$. Obviously the definition is independent of the choice of the basis. Therefore, $(M_0, \delta_{M_0}^*)$ is an object $IDM_q(L)$.
Let us consider two objects $\mathcal{M} := (M_k, \phi_k)_{k\in\mathbb{N}}$ and $\mathcal{N} := (N_k, \psi_k)_{k\in\mathbb{N}}$ of $Proj_q(L)$ and α a morphism from $\mathcal{M}$ to $\mathcal{N}$ in the category $Proj_q(L)$, i.e. α_k is L_k linear and the diagram

$$\begin{array}{ccc} M_k & \xrightarrow{\alpha_k} & N_k \\ {\scriptstyle \phi_k}\uparrow & & \uparrow{\scriptstyle \psi_k} \\ M_{k+1} & \xrightarrow{\alpha_{k+1}} & N_{k+1} \end{array}$$

is commutative. Then we have $\delta_N^* \circ \alpha_0 = \alpha_0 \circ \delta_M^*$. Also, with this property, it is then easy to verify that

$$Proj_q(L) \longrightarrow IDM_q(L)$$

$$(N_k, \psi_k) \longmapsto (M_0, \delta_{M_0}^*)$$

(with $\delta_{M_0}^*$ as defined above) is in fact an equivalence of categories.

3.2 Iterative q-difference equations

As we expect from standard q-difference Galois theory, any iterative q-difference module should give rise to an iterative q-difference equation consisting of a family of equations. Proposition 3.12 in the case of positive characteristic and Proposition 3.17 for characteristic zero show how to obtain this equation from a given ID_q-module.

3.2.1 Case of the characteristic p

Proposition 3.11 *Let (L, δ_L^*) be an iterative q-difference field of characteristic p, and let (M, δ_M^*) be an object of $IDM_q(L)$. Let us consider the canonical projective system $(M_k, \phi_k)_{k\in\mathbb{N}}$ associated to M. For all $k \in \mathbb{N}$, let us choose an L_k-basis B_k of M_k with $\phi_k B_k = B_{k+1}$ and let $D_k \in Gl_n(L_k)$ denote the matrix of ϕ_k with respect to that basis, i.e., $B_k D_k = B_{k+1}$.*

Then, for any $l \in \mathbb{N}$ and for any $X \in L^n$, we have :

1. *$B_0 X = B_l X_l$ where $X_l = D_{l-1}^{-1} ... D_0^{-1} X$,*
2. *$\delta_M^{(k)}(B_0 X) = B_l \delta_L^{(k)}(X_l)$ for $k < l$.*

Proof
Part 1 is obvious by definition. Part 2 follows from

$$\delta_M^{(k)}(B_0 X) = \delta_M^{(k)}(B_l X_l) = B_l \delta_L^{(k)}(X_l) \text{ for } k < l.$$

Proposition 3.12 *With the previous notation, and a basis $B_0 = \{b_1, ..., b_n\}$ of M, the following statements are equivalent*

1. *$B_0 \mathbf{y} = \sum_{i=1}^n y_i b_i \in V_M = \cap_{k\in\mathbb{N}} M_k$.*
2. *For all $l \in \mathbb{N}$, we have $\delta_L^{(1)}(\mathbf{y}_1) = 0$ and $\delta_L^{(np^k)}(\mathbf{y}_l) = 0$ for $0 \leq k < l$, where $\mathbf{y}_l = D_{l-1}^{-1} ... D_0^{-1} \mathbf{y}$.*
3. $$\delta_L^{(np^k)}(\mathbf{y}) = A_{k+1}\mathbf{y},$$
   for all $k \geq 0$ where $A_{k+1} = \delta_L^{(np^k)}(D_0 ... D_{k+1})(D_0 ... D_{k+1})^{-1}$ and $\delta_L^{(1)}(\mathbf{y}) = A_1 \mathbf{y}$ where $A_1 = \delta_L^{(1)}(D_0 D_1)(D_0 D_1)^{-1}$.

Proof
First, we show that statements 1 and 2 are equivalent : $B_0 \mathbf{y} \in V_M$ if and only if $\delta_M^{(k)}(B_0 \mathbf{y}) = 0$ for all $k \in \mathbb{N}^*$. The claim is obvious by using the equation

$$\delta_M^{(k)}(B_0 \mathbf{y}) = B_l \delta_L^{(k)}(\mathbf{y}_l)$$

which holds for $k < l$ (see the previous proposition).
Finally, the equivalence of 2 and 3 is obtained using:

$$\delta_L^{(np^l)}(\mathbf{y}) = \delta_L^{(np^l)}(D_{l+1}\mathbf{y}_{l+2}) = \delta_L^{(np^l)}(D_0...D_{l+1})\mathbf{y}_{l+2} + D_0...D_{l+1}\delta_L^{(np^l)}(\mathbf{y}_{l+2}) = A_{l+1}\mathbf{y} + \delta_L^{(np^l)}(\mathbf{y}_{l+2})$$

and

$$\delta_L^{(1)}(\mathbf{y}) = \delta_L^{(1)}(D_1\mathbf{y}_2) = \delta_L^{(1)}(D_0...D_1)\mathbf{y}_2 + D_0...D_1\delta_L^{(1)}(\mathbf{y}_2) = A_1\mathbf{y} + \delta_L^{(1)}(\mathbf{y}_2).$$

Definition 3.13 *The family of equations* $\{\delta_L^{(1)}(\mathbf{y}) = A_1\mathbf{y}, \delta_L^{(np^k)}(\mathbf{y}) = A_k\mathbf{y}\}_{k\geq 0}$ *related to the* IDM_q*-module* (M, δ_M^*) *by Proposition 3.12 is called an* ***iterative*** q***-difference equation*** *(*ID_qE*).*

We now give some examples of iterative q-difference equations over fields of positive characteristic.

Example 3.14 *Let* p *be a prime number, let* $C = \overline{\mathbb{F}_p}$ *be an algebraic closure of* $\mathbb{F}_p$ *and let* $F = C(t)$ *be the rational function field with coefficients in* C*. Let* $(a_l)_{l\geq 0}$ *be a set of elements in* C*. Let* $M = Fb_1$*. Suppose that,* $D_{l+1} = (t^{a_l np^l}) \in Gl_1(F_{l+1})$ *for* $l \in \mathbb{N}$ *and* $D_1 = (1)$*. We have*

$$A_{k+1} = \delta_L^{(np^k)}(D_0...D_{k+1})(D_0...D_{k+1})^{-1} = \delta_L^{(n^k)}(t^{\sum_{l=0}^k a_l np^l})t^{-\sum_{l=0}^k a_l np^l} = \frac{a_k}{t^{np^k}}$$

because $\binom{\sum_{j=0}^k a_j np^j}{np^k}_q = a_k$*. Hence* $\delta_M^{(np^k)}(y) = \frac{a_k}{t^{np^k}}y$ *for all* $k \in \mathbb{N}$*.*

Example 3.15 *Let* p *be a prime number, let* $C = \overline{\mathbb{F}_p}$ *be an algebraically closure of* $\mathbb{F}_p$ *and let* $F = C(t)$ *be the rational function field with coefficients in* C*. Let* $(a_l)_{l\geq 0}$ *be a set of elements in* C*. Let* $M = Fb_1 \oplus Fb_2$*. Suppose that,*

$$D_{l+1} := \begin{pmatrix} 1 & a_l t^{np^l} \\ 0 & 1 \end{pmatrix} \text{ for all } l \in \mathbb{N}$$

and

$$D_1 := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Using the formula (1), we obtain,

$$A_{k+1} = \begin{pmatrix} 1 & a_k \\ 0 & 1 \end{pmatrix}$$

and $A_1 = 0$*. So, the associated* ID_qE *associated to* M *is*

$$\delta^{(np^k)}(Y) = A_kY = \begin{pmatrix} 0 & a_k \\ 0 & 0 \end{pmatrix} Y \text{ for all } k \in \mathbb{N}.$$

3.2.2 Case of characteristic zero

Let (L, δ_L^*) be an iterative q-difference field of characteristic zero and let (M, δ_M^*) be an iterative q-difference module over L. As in Paragraph 3.1.2, $L_1 = \cap_{0\leq j<1} Ker(\delta_L^{(n^j)})$, $L_0' = Ker(\delta_L^{(1)})$, $L_0 = L$, $M_1 = \cap_{0\leq j<1} Ker(\delta_M^{(n^j)})$, $M_0' = Ker(\delta_L^{(1)})$ and $M_0 = M$.

Notation 3.16 *Let $B_0' = \{b_1', ..., b_n'\}$ (resp. B_0) be a L_0'-basis of M_0' (resp. a L_0-basis of M_0). Because of Proposition 3.8, we have $M_0' \otimes L \simeq M$. Now let us denote by $D_0 \in Gl_n(L_0')$ the matrix of ϕ_0 with respect to the basis B_0' and B_0, i.e., $B_0 D_0 = B_0'$. Let C_k be the matrix of $\delta_M^{(k)}$ with respect to the basis B_0 and let $\Phi \in Gl_n(L)$ be the matrix of the action of σ_q with respect to the basis B_0. Set*

1. *$A_0 := Id$, $A_1 := -\Phi^{-1} C_1$, and*
2. *$A_k := -\Phi^{-k}(\sum_{j=0}^{k-1} \Phi^j C_{k-j} A_j)$ for $k > 1$ inductively.*

Proposition 3.17 *Using the previous notation, the following statements are equivalent:*

1. *$B_0 \mathbf{y} = \sum_{i=1}^n y_i b_i \in V_M = \cap_{k\in\mathbb{N}} M_k$.*
2. *For $k \in \mathbb{N}$, we have $\delta_L^{(k)}(\mathbf{y}) = A_k \mathbf{y}$, with A_k defined in Notation 3.16.*

Proof
If $B_0 \mathbf{y} = \sum_{i=1}^n y_i b_i \in V_M$, then for all $k \in \mathbb{N}$ we have $\delta_M^{(k)}(B_0 \mathbf{y}) = 0$.
Let us first consider the case $k = 1$. We have

$$\delta_M^{(1)}(B_0 \mathbf{y}) = \sigma_q(B_0)\delta^{(1)}(\mathbf{y}) + \delta_M^{(1)}(B_0)\mathbf{y},$$

and thus

$$\delta^{(1)}(\mathbf{y}) = -\Phi^{-1} C_1.$$

We will proceed by induction and assume that we have $\delta_L^{(j)}(\mathbf{y}) = A_j \mathbf{y}$ for all $j < k$. Then

$$\delta_M^{(k)}(B_0 \mathbf{y}) = 0 = \sum_{j=0}^{k} \sigma_q^j(\delta_M^{(k-j)}(B_0))\delta^{(j)}(\mathbf{y}) = \sum_{j=0}^{k-1} B_0 \Phi^j C_{k-j} A_j \mathbf{y} + B_0 \Phi^k \delta^{(k)}(\mathbf{y}),$$

and thus

$$\delta^{(k)}(\mathbf{y}) = -\Phi^{-k}(\sum_{j=0}^{k-1} \Phi^j C_{k-j} A_j)\mathbf{y} = A_k \mathbf{y}.$$

Hence the first statement implies the second. By going through the computation backwards, we obtain the equivalence between the two statements.

Definition 3.18 *The family of equations $\{\delta_L^{(k)}(\mathbf{y}) = A_k \mathbf{y}\}_{k\in\mathbb{N}}$ related to the IDM_q-module (M, δ_M^*) by Proposition 3.17 is called an* ***iterative q-difference equation*** *(ID_qE).*

Remark 3.19 *We shall recall the introduction of Paragraph 3.1.2 : in the case of characteristic zero we may regain the iterative q-difference operator from the knowledge of $\delta^{(1)}$ and $\delta^{(n)}$. Therefore, for the study of an iterative q-difference equation in zero characteristic, it is sufficient to know the iterative q-difference equations at level 1 and n.*

Remark 3.20 *We keep using Notation 3.16 and we will show how to compute C_j by induction for $j < n$. We have by definition $C_1 = \frac{\Phi - Id}{(q-1)t}$. This implies*

$$\frac{q^j - 1}{q-1}\delta_M^{(j)}(B_0) = \delta_M^{(1)}\delta_M^{(j-1)}(B_0) = \delta_M^{(1)}(C_{j-1}B_0) = (\sigma_q(C_{j-1})C_1 + \delta^{(1)}(C_{j-1}))B_0,$$

and thus

$$C_j = \frac{q-1}{q^j - 1}(\sigma_q(C_{j-1})C_1 + \delta^{(1)}(C_{j-1})). \tag{19}$$

Example 3.21 *Let $L = \mathbb{C}(t)$ and let q be a n-th primitive root of unity. Let $M = Fb_1$ be a rank one $IDM_q(L)$-module and suppose that $\Phi(b_1) = b_1$. Then an easy computation leads to $C_j = 0$ for all $1 \leq j < n$ and $A_j = 0$ for $1 \leq j < n$. Now, let a_1 be an integer and set $C_n = \frac{a_1}{t^n}$. Then $A_n = \frac{a_1}{t^n}$. By induction we get*

$$A_{kn} = \frac{a_k}{t^{kn}}, \text{ for all } k \in \mathbb{N} \text{ where } a_{k+1} = \frac{1}{k+1}(ka_k + a_k a_1).$$

4 Iterative q-difference Picard-Vessiot extensions

In this section, we develop a Picard-Vessiot theory for iterative q-difference equations. We build the Picard-Vessiot ring inspired by the usual construction, but we have to adapt our construction to a infinite set of variables, and thus some modifications are necessary.

4.1 Iterative Picard-Vessiot rings

Notation 4.1 *Let (L, δ_L^*) be an iterative q-difference field. If,*

1. *the characteristic of the constants field C of L is zero then let us denote by (k_C) the family $(k)_{k\in\mathbb{N}}$,*
2. *the characteristic of the constants field C of L is positive equal to p then let us denote by (k_C) the family $\{1, (np^k)_{k\in\mathbb{N}}\}$.*

Remark 4.2 (Classical case) *As mentioned before, when q is not a root of unity, an iterative q-difference module is the same object as a q-difference module. Moreover, in this case the iterative q-difference equation is just obtained by considering the equation of level 1 and if there exists $Y \in Gl_n(R)$ such that $\delta_L^{(1)}(Y) = A_1 Y$ then for all $k \in \mathbb{N}$ we have $\delta_L^{(k_C)}(Y) = A_k Y$. Thereby, when q is not a root of unity, an iterative q-difference equation is simply a q-difference equation in the sense of [25].*

Definition 4.3 *Let (L, δ_L^*) be an iterative q-difference field, let (M, δ_M^*) be an object of $IDM_q(L)$, and let $\{\delta_L^{(k_C)}(\mathbf{y}) = A_k\mathbf{y}\}_{k\in\mathbb{N}}$ be an* ***iterative q-difference equation*** *related to the IDM_q-module (M, δ_M^*), denoted by $ID_qE(M)$.*
Let (R, δ_R^*) be an iterative q-difference extension of (L, δ_L^*). A matrix $Y \in Gl_n(R)$ is called a ***fundamental solution matrix*** *for $ID_qE(M)$ if $\delta_R^{(k_C)}(Y) = A_kY$, for all $k \in \mathbb{N}$.*
The ring R is called an ***iterative q-difference Picard-Vessiot ring*** *for $ID_qE(M)$ (IPV_q-ring for short) if it fulfills the following conditions :*

1. *R is a simple ID_q ring (that means that R contains no proper iterative q-difference ideal),*
2. *$ID_qE(M)$ has a fundamental solution matrix Y with coefficients in R,*
3. *R is generated by the coefficients of Y and $det(Y)^{-1}$,*
4. *$C(R) = C(L)$.*

Remark 4.4 (Classical case) *As in Remark 4.2, we easily see that if q is not a root of unity, the notion of an iterative Picard-Vessiot ring is exactly the same as the notion of Picard-Vessiot ring in the sense of Singer, van der Put ([25]).*

Proposition 4.5 *Let (L, δ_L^*) be an iterative q-difference field, with algebraically closed field of constants $C(L)$, and let R/L be a simple ID_q-ring. Then R is a reduced ID_q-ring. Moreover, if R is finitely generated over L, we have $C(L) = C(E)$ where E denotes the localization of R by its set of non zeros divisors.*

Proof
The fact that R is a reduced ID_q-ring is a consequence of Lemma 2.17 where it is shown that if I is an ID_q-ideal the same is true for its radical. For the second statement, let us assume that R is finitely generated over L. Let c be a non zero constant of E and put $J = \{a \in R | a.c \in R\}$. First of all, because $\delta_E^{(1)} = \frac{\sigma_q - id}{(q-1)t}$, we have that $\sigma_q^k(c) = c$ for all $k \in \mathbb{N}$. It is then quite clear that J is an ID_q-ideal of R because of $\delta_R^{(k)}(a.c) = \sigma_q^k(c).\delta_R^{(k)}(a) = c.\delta_R^{(k)}(a)$ for all $k \in \mathbb{N}$. Since R is simple, and J is a non trivial ID_q-ideal, we have $J = R$, and thus $1.c = c \in R$. Suppose that $c \notin C(L)$. Thus for all $d \in C(L)$ the ideal $(c - d)R$ is a non trivial ID_q-ideal in R and also equal to R. This means that $(c - d) \in R^*$ for all $d \in C(L)$. Let $\phi_c : Spec(R) \mapsto \mathbb{A}_L^1$ be the morphism induced by

$$\phi : \qquad L[T] \longrightarrow R, \qquad T \longmapsto c.$$

Since $Im(\phi_{\mathbf{c}}) \cap \mathbb{A}_L^1(C(L))$ is empty, $Im(\phi_c)$ does not contain any open subset of $\mathbb{A}_L^1$. Therefore the image of ϕ_c in $\mathbb{A}_L^1$ is finite and closed. This implies that c is algebraic over L. Let $P \in L[X]$ be the minimal monic polynomial annihilating c. We have $\delta_L^{(k)}(P(c)) = P^{\delta_L^{(k)}}(c) = 0$ where $P^{\delta_L^{(k)}}$ denotes the element of $L[X]$ obtained from P by applying $\delta_L^{(k)}$ on the coefficients of P. By minimality of P we conclude that $P \in C(L)[X]$. Because $C(L)$ is algebraically closed, we then have $c \in C(L)$. This is a contradiction!

Proposition 4.6 *Let (L, δ_L^*) be an ID_q-field and (R, δ_R^*) be an ID_q-ring with q-difference operator extending the one given on L. Let Y and $\tilde{Y}$ be two elements of $Gl_n(R)$, fundamental matrices of solutions for the ID_qE, $\delta_R^{(k_C)}(\mathbf{y}) = A_k\mathbf{y}$. Then, there exists a matrix $P \in Gl_n(C(R))$ such that $\tilde{Y} = YP$. Moreover, if both L and R satisfy the conditions of Proposition 4.5 then $P \in Gl_n(C(L))$.*

Proof

It is obvious that there exists $P \in Gl_n(R)$ such that $\tilde{Y} = YP$. We want to show by induction that for all $k \in \mathbb{N}^*$, we have $\delta_R^{(k)}(P) = 0$. For $k = 1$ we obtain

$$\delta_R^{(1)}(\tilde{Y}) = \delta_R^{(1)}(Y)P + \sigma_q(Y)\delta_R^{(1)}(P) = A_1\tilde{Y} + \sigma_q(Y)\delta_R^{(1)}(P).$$

Thus, $\delta_R^{(1)}(P) = 0$ (because σ_q is an automorphism of $Gl_n(R)$). Using the formula

$$\delta_R^{(k)}(\tilde{Y}) = \sum_{i+j=k} \sigma_q^i(\delta_R^{(j)}(Y))\delta_R^{(i)}(P),$$

we get by induction that $\delta_R^{(k)}(P) = 0$ for all $k \in \mathbb{N}^*$. This implies that $P \in Gl_n(C(R))$.

Theorem 4.7 *Let (L, δ_L^*) be an iterative q-difference field with $C(L)$ algebraically closed and let (M, δ_M^*) be an object of $IDM_q(L)$ with iterative q-difference equation $\delta_L^{(k_C)}(\mathbf{y}) = A_k\mathbf{y}$ ($ID_qE(M)$). Then there exists an iterative q-difference Picard-Vessiot ring for the iterative q-difference equation which is unique up to iterative q-difference isomorphism.*

Proof
Let m be the dimension of M over L and set $U = L[x_{(i,j)}, det(x_{(i,j)})^{-1}]$. The algebra $U_0 := L[x_{(i,j)}]$ is given a structure of q-difference extension of L via $\sigma_q(X) := \frac{A_1}{(q-1)t}X + X$ where $X = (x_{(i,j)})_{(i,j)}$. Because σ_q is a ring-automorphism, we have that the ideal S generated in U_0 by $det(x_{i,j})$ is a σ_q-ideal and a multiplicatively closed set. U_0 has a non trivial ID_q-structure via

$$\delta_{U_0}^* := \delta_P^{(k_C)}(X) = A_kX, \text{ for all } k \in \mathbb{N}.$$

Because S satisfies the condition of Proposition 2.19, there exists a unique iterative q-difference operator $\delta_{S^{-1}U_0}^*$ extending $\delta_{U_0}^*$ on $U = S^{-1}U_0$. Let $P \subset U$ be a maximal ID_q-ideal of U. Then $R := U/P$ is a simple ID_q-ring and $Y := \overline{X}$, the image of X under the projection of U to R, is a fundamental solution matrix of $ID_qE(M)$. Moreover R/L is generated by the coefficients of Y and $det(Y)^{-1}$. Thus R is an iterative q-difference Picard-Vessiot ring.
Assume that $(R_1, \delta_{R_1}^*)$ and $(R_2, \delta_{R_2}^*)$ are two iterative q-difference Picard-Vessiot rings for M with fundamental solution matrix Y_1 (resp. Y_2) in R_1 (resp. R_2). Put $N = R_1 \otimes_L R_2$.

As in Proposition 2.11 we endow N with an ID_q-structure. Let $P \subset N$ be a maximal ID_q-ideal, then $R' := N/P$ is a simple ID_q ring. The two maps :

$$\phi_1 : \qquad R_1 \longrightarrow R', \qquad r_1 \longmapsto \overline{(r_1 \otimes 1)}$$

and

$$\phi_2 : \qquad R_2 \longrightarrow R', \qquad r_2 \longmapsto \overline{(1 \otimes r_2)}\,.$$

induced by the natural inclusions are ID_q-monomorphisms, and $\phi_1(Y_1)$ and $\phi_2(Y_2)$ are two fundamental matrix solutions for M in R'. By Proposition 4.6, there exists $P \in Gl_n(C(L))$ such that $\phi_1(Y_1) = \phi_2(Y_2)P$ $(C(L) = C(R_1) = C(R_2) = C(R'))$, which implies that $\phi_1(R_1) \simeq \phi_2(R_2)$. This concludes the proof.

4.2 The iterative q-difference Galois group

In this section, we will define the iterative q-difference Galois group associated to an iterative q-difference module. The way of describing such a group is the exact translation in the q-difference world of the work of A. Roescheisen (see [19]) in the case of iterative differential Galois theory. Until the end of this section, (L, δ_L^*) will be an iterative q-difference field with algebraically closed field of constants C, (R, δ_R^*) an iterative q-difference Picard-Vessiot ring for the iterative q-difference equation $\{\delta_L^{(k_C)}Y = A_kY,\ k \in \mathbb{N}\}$ defined over L.

Notation 4.8 *Let S be a ring. We denote by $Loc(S)$ its localization by its set of non-zero divisors.*

4.2.1 Functorial definition

First of all, let us remark that, given an algebra A over C and an iterative q-difference ring (S, δ_S^*), we define an iterative q-difference operator on $S \otimes_C A$ by setting $\delta^{(k)}_{S\otimes_C A}(s \otimes f) := \delta_S^{(k)}(s) \otimes f$ for all $k \in \mathbb{N}$. As in [19], we say that δ_S^* is **extended trivially** to $S \otimes_C A$.

Definition 4.9 *Let us define the functor*

$$\underline{Aut}(R/L) : \qquad (Algebras/C) \longrightarrow (Groups), \qquad A \longmapsto Aut_{ID_q}(R \otimes_C A/L \otimes_C A)$$

where δ_R^* (resp. δ_L^*) is extended trivially to $R \otimes_C A$ (resp. $L \otimes_C A$).

In the following, we will show that the functor $\underline{Aut}(R/L)$ is representable by a certain C-algebra of finite type and hence is an affine group-scheme of finite type over C.

Lemma 4.10 *Let R be a simple ID_q-ring with $C(R) = C$, let A be a finitely generated C-algebra and $R_A := R \otimes_C A$ with ID_q-structure trivially extended from R. Then there is a bijection*

$$\mathcal{I}(A) \longleftrightarrow \mathcal{I}_{ID_q}(R_A)$$

$$I \longmapsto R_A(1 \otimes_C I) = R \otimes_C I,$$

$$J \cap (1 \otimes_C A) \longmapsfrom J$$

between the ideals of A and the ID_q-ideals of R_A.

Proof

Obviously, the two maps are well defined, and we only have to prove that they are inverse to each other.

1. We will prove that for $I \in \mathcal{I}(A)$, we have $(R \otimes_C I) \cap (1 \otimes_C A) = I$. It is obvious that I is contained in the ideal on the left side. Now let us consider a C-basis $\{e_i | i \in \tilde{N}\}$ of I ; then $R \otimes_C I$ is a free R-module with basis $\{1 \otimes e_i | i \in \tilde{N}\}$ and an element $f = \sum_{i \in \tilde{N}} r_i \otimes e_i \in R \otimes_C I$ is constant if and only if all the r_i's are constants, i.e., if $f \in I$.

2. Conversely we have to prove that for $J \in \mathcal{I}_{ID_q}(R_A)$, we have $R \otimes_C J \cap (1 \otimes_C A) = J$. It is clear that J contains the ideal on the left side. Now, let $\{e_i | i \in N\}$ a C-basis of A, where N denotes an index set. Then, $\{1 \otimes e_i | i \in N\}$ is also a basis for the free R-module R_A.
   For any subset N_0 of N and $i_0 \in N_0$, let Ann_{N_0,i_0} be the ideal of all $r \in R$ such that there exists an element $g = \sum_{i \in N_0} s_i \otimes e_i \in J$ with $s_{i_0} = r$. Since the iterative q-difference operator of R_A acts trivially on A and J is an ID_q-ideal, it is clear that Ann_{N_0,i_0} is an ID_q-ideal. Because R is simple, Ann_{N_0,i_0} is equal to (0) or R.
   Now, let $N_0 \subset N$ be minimal for the property that $Ann_{N_0,i_0} \neq (0)$ for at least one index $i_0 \in N_0$ (minimal in the lattice of subsets). So there exists $g = \sum_{i \in N_0} s_i \otimes e_i \in J$ with $s_{i_0} = 1$ and by minimality of N_0 we conclude that for all $k \in \mathbb{N}^*$, $\delta^{(k)}(g) = \sum_{i \in N_0, i \neq i_0} \delta_R^{(k)}(s_i) \otimes e_i = 0$. This implies $g \in J \cap (1 \otimes_C A)$. Now let $g = \sum_{i \in N} s_i \otimes e_i \in J$ be an arbitrary element and denote by N_1 the set of indices i with $s_i \neq 0$. It follows from the definition that $Ann_{N_1,i} \neq (0)$ for all $i \in N_1$. Hence there exists $N_0 \subset N_1$ minimal as above, $i_0 \in N_0$ and $f = \sum_{i \in N_0} r_i \otimes e_i \in J \cap (1 \otimes_C A)$ with $r_{i_0} = 1$. By induction on the cardinality of N_1, we may assume that $g - s_{i_0} f \in R \otimes_C J \cap (1 \otimes_C A) \subset J$. Therefore $g = g - s_{i_0} f + s_{i_0} f \in R \otimes_C J \cap (1 \otimes_C A)$ and hence $R \otimes_C J \cap (1 \otimes_C A) = J$.

Proposition 4.11 *Let R/L be an iterative q-difference Picard-Vessiot ring associated to an iterative q-difference equation and let T be a ID_q-simple ring containing L with $C(T) = C = C(L)$ such that there exists a fundamental matrix of solutions $Y \in Gl_n(T)$. Then*

there exists a finitely generated C-algebra U (with trivial ID_q-structure) and a T-linear ID_q-isomorphism

$$\gamma_T : T \otimes_L R \longrightarrow T \otimes_C U.$$

where the ID_q-structure is extended trivially to $T \otimes_C U$.
(Actually U is isomorphic to the ring of constants of $T \otimes_L R$.)

Proof
R is obtained as a quotient of $L[X_{i,j}, (det(X))^{-1}]$ with iterative q-difference operator given by $\delta^{(k)}(X) = A_k X$ for all $k \in \mathbb{N}$ by a maximal ID_q-ideal $P \subset L[X_{i,j}, (det(X))^{-1}]$. We then define a T-linear homomorphism

$$\gamma_T : T \otimes_L L[X_{i,j}, det(X)^{-1}] \longrightarrow T \otimes_C C[Z_{i,j}, det(Z)^{-1}]$$

by $X_{i,j} \mapsto \sum_{k=1}^{n} Y_{i,k} \otimes Z_{k,j}$. The morphism γ_T is indeed a T-linear isomorphism and if we extend the ID_q-structure trivially to $L[Z_{i,j}, (det(Z))^{-1}]$, γ_T induces an ID_q-isomorphism. By the previous lemma, the ID_q-ideal $\gamma_T(T \otimes P)$ is equal to $T \otimes I$ for an ideal $I \subset C[Z_{i,j}, (det(Z))^{-1}]$. So for $U := C[Z_{i,j}, (det(Z))^{-1}]/I$, γ_T induces an ID_q-isomorphism

$$\gamma_T : T \otimes_L R \longrightarrow T \otimes_C U.$$

Theorem 4.12 *Let R/L be an iterative q-difference Picard-Vessiot ring. Then the group functor $\underline{Aut}(R/L)$ is representable by the finitely generated C-algebra $U = C(R \otimes_L R)$, i.e., $\underline{Aut}(R/L)$ is an affine group-scheme of finite type over C.*

Definition 4.13 *We call the affine group scheme $\underline{Aut}(R/L)$ the **Galois group scheme** $\underline{Gal}(R/L)$ of R over L.*

Proof of theorem 4.12
First we will show that for every C-algebra A any L_A-linear ID_q-homomorphism $f : R_A \longrightarrow R_A$ is an isomorphism. The kernel of such a homomorphism f is an ID_q-ideal of R_A. So by Lemma 4.10, it is generated by constants, i.e., elements in $1 \otimes A$. But f is A-linear so its kernel is zero. If $X \in Gl_n(R)$ is a fundamental solution matrix, then $f(X) \in Gl_n(R_A)$ is also a fundamental solution matrix and so there exists a matrix $D \in Gl_n(C_{R_A}) = Gl_n(A)$ such that $X = f(X)D = f(XD)$. Hence $X_{i,j}, det(X)^{-1} \in Im(f)$ and since R is generated by $X_{i,j}, det(X)^{-1}$ over L, the homomorphism f is also surjective. Using the isomorphism $\gamma := \gamma_R$ of Proposition 4.11, for a C-algebra A, we obtain a chain of isomorphisms

$$Aut^{ID_q}(R_A/L_A) = Hom_{L_A}^{ID_q}(R_A, R_A) \simeq Hom_{R_A}^{ID_q}(R_A \otimes_L R, R_A)$$

$$\simeq Hom_{R_A}^{ID_q}(R_A \otimes_C U, R_A) \simeq Hom_C^{ID_q}(U, R_A) \simeq Hom_C(U, A).$$

Hence U represents the functor $\underline{Aut}(R/L)$.

Remark 4.14 *By taking a closer look on the isomorphisms in the previous proof, we see that the universal object* $id_U \in Hom_C(U,U)$ *gives birth to the* ID_q*-automorphism* $\rho \otimes id_U : R \otimes_C U \longrightarrow R \otimes_C U$ *where* $\rho = \gamma_R \circ (1 \otimes id_R) : R \longrightarrow R \otimes_L R \longrightarrow R \otimes_C U$.

Corollary 4.15 *Let* R/L *be an iterative q-difference Picard-Vessiot ring over* L *and* $\mathcal{G} := \underline{Gal}(R/L)$ *the Galois group scheme of* R*. Then* $Spec(R)$ *is a* $\mathcal{G}_L$*-torsor.*

Proof
The isomorphism $\gamma := \gamma_R$ of proposition 4.11, determines an isomorphism of schemes

$$Spec(\gamma) : Spec(R) \times_L \mathcal{G}_L = Spec(R) \times_C \mathcal{G} \longrightarrow Spec(R) \times_L Spec(R).$$

By the previous remark and R-linearity of γ, the composition of $Spec(\gamma)$ with the projection on the second factor gives the action of $\mathcal{G}_L$ on $Spec(R)$ and the composition with the projection on the first factor equals the map $Spec(R) \times_L \mathcal{G}_L \to Spec(R)$. In other words, $Spec(R)$ is a $\mathcal{G}_L$-torsor.

4.2.2 Galois correspondence

Proposition 4.16 (Structure of the iterative q-difference ring) *Let* R/L *be an iterative q-difference Picard-Vessiot ring over* L*. Then, there exist idempotents* $e_1, .., e_s \in R$ *such that*

1. $R = R_1 \oplus ... \oplus R_s$ *where* $R_i = e_i R$ *and is a domain,*
2. *The direct sum* E *of the fraction fields of the* R_i*'s is an iterative q-difference ring.* E *is called the total iterative q-difference Picard-Vessiot extension of* R*.*

Proof
Here, we give a partial analogue of Corollary 1.16 of [25]. We will thus follow the proof of Singer, van der Put. But because we work in any characteristic, it will be necessary to appeal to the book of Demazure, Gabriel ([7]) to assure smoothness.
Let $\overline{L}$ be an algebraic closure of L and $R = O(\mathcal{Z})$ for some $\mathcal{G}_L$-torsor $\mathcal{Z}$. Since $\mathcal{G}_L(\overline{L})$ acts transitively on $\mathcal{Z}(\overline{L})$, this latter algebraic subset must be smooth ([7]). Therefore the L-irreducible components $\mathcal{Z}_1, ..., \mathcal{Z}_s$ must be disjoint. Thus $O(\mathcal{Z})$ is equal to the product of the integral domains $R_i = O(\mathcal{Z}_i)$. Now let us consider the set S of non zero divisors in R. It is a multiplicatively closed set which does not contain 0, stable under the action of σ_q. By Proposition 2.19, the ring RS^{-1} is endowed with an iterative q-difference structure and it is obvious that $RS^{-1} = \bigoplus_{i=1}^{s} Frac(R_i)$ where $Frac(R_i)$ denotes the fraction field of R_i.

The next proposition shows that to be a torsor for an ID_q-simple ring means, roughly speaking, to be an iterative q-difference Picard-Vessiot ring.

Proposition 4.17 *Let R/L be a simple ID_q-ring with algebraically closed field of constants $C(R) = C$. Further let $\mathcal{G} \subset Gl_{n,C}$ be an affine group scheme over C. Assume that $Spec(R)$ is a $\mathcal{G}_L$-torsor such that the corresponding isomorphism $\gamma : R \otimes_L R \to R \otimes_C C[\mathcal{G}]$ is an ID_q-isomorphism. Then R is an iterative q-difference Picard-Vessiot ring over L.*

Proof
Since $Spec(R)$ is a $\mathcal{G}_L$-torsor, the fiber product $Spec(R) \times_{\mathcal{G}_L} Gl_{n,L}$ is a $Gl_{n,L}$-torsor. ($Spec(R) \times_{\mathcal{G}_L} Gl_{n,L}$ is obtained as the quotient of the direct product by the $\mathcal{G}_L$-action given by $(x, h).g := (xg, g^{-1}h)$ and is a right $Gl_{n,L}$-scheme acting on the second factor.) By Hilbert's Theorem 90, every $Gl_{n,L}$-torsor is trivial, i.e., we have an $Gl_{n,L}$-equivariant isomorphism

$$Spec(R) \times_{\mathcal{G}_L} Gl_{n,L} \longrightarrow Gl_{n,L} .$$

Then the closed embedding $Spec(R) \longrightarrow Spec(R) \times_{\mathcal{G}_L} Gl_{n,L} \longrightarrow Gl_{n,L}$ leads to an epimorphism $L[X_{i,j}, (det(X))^{-1}] \longrightarrow R$, which is $\mathcal{G}_L$-equivariant. Denote the image of X by Y. Then we obtain that the action of $\mathcal{G}$ on Y is given by $Y \mapsto Yg$ for any L-valued point $g \in \mathcal{G}_L(L)$. Since by assumption for every C-algebra A with trivial ID_q-structure, the action of $\mathcal{G}(A)$ commutes with the iterative q-difference operator $\delta^{(k)}(Y).Y^{-1}$ is $\mathcal{G}$-invariant for all $k \in \mathbb{N}$. So $\delta^{(k)}(Y).Y^{-1} = A_k$ belongs to $Gl_n(L)$ and Y is a fundamental solution matrix for the equation $\{\delta^{(k)}(Y).Y^{-1}\}_{k\in\mathbb{N}}$. Hence R is an ID_q-Picard-Vessiot ring.

In order to get a convenient Galois correspondence, we are obliged to define the notion of an invariant in a functorial way. Let S be a C-algebra and $\mathcal{H}/C$ be a subgroup functor of the functor $\underline{Aut}(S/C)$, i.e., for every C-algebra A, the set $\mathcal{H}(A)$ is a group acting on S_A and this action is functorial. An element $s \in S$ is called invariant if for all A, the element $s \otimes 1 \in S_A$ is invariant under $\mathcal{H}(A)$. The ring of invariants is denoted by $S^{\mathcal{H}}$. Let $E = Loc(S)$ be the localization of S by all non zero-divisors. We call an element $e = \frac{r}{s} \in E$ invariant under $\mathcal{H}$, if for each C-algebra A and all $h \in \mathcal{H}(A)$,

$$h.(r \otimes 1).(s \otimes 1) = (r \otimes 1).h.(s \otimes 1).$$

$E^{\mathcal{H}}$ denotes the ring of invariants (for the independence of this definition of the choice of representation of e see [19]).

Lemma 4.18 *Let R/L be an iterative q-difference Picard-Vessiot ring over L, let E denote its total iterative q-difference Picard-Vessiot extension and $\mathcal{G} := \underline{Gal}(R/L)$ the Galois group scheme of R. Let $\mathcal{H} \subset \mathcal{G}$ be a closed subgroup-scheme. Denote by $\pi^{\mathcal{G}}_{\mathcal{H}} : C[\mathcal{G}] \longrightarrow C[\mathcal{H}]$ the epimorphism corresponding to the inclusion $\mathcal{H} \hookrightarrow \mathcal{G}$. Then an element of $\frac{r}{s} \in E$ is invariant under the action of $\mathcal{H}$ if and only if $r \otimes s - s \otimes r$ is in the kernel of the map*

$$(id_R \otimes \pi^{\mathcal{G}}_{\mathcal{H}}) \circ \gamma : R \otimes_L R \longrightarrow R \otimes_C C[\mathcal{H}].$$

Proof
The following proposition is a special case of the Galois correspondence stated in Theorem 4.20.

Proposition 4.19 *For every closed subgroup scheme $\mathcal{H} \subset \mathcal{G}$, the ring $E^{\mathcal{H}}$ is an ID_q-ring in which every non zero divisor is a unit. Furthermore we have $E^{\mathcal{H}} = L$ if and only if $\mathcal{H} = \mathcal{G}$.*

Proof
By the previous lemma, it is obvious that $E^{\mathcal{H}}$ is an ID_q-ring in which every non-zero divisor is a unit. Next, let $\frac{r}{s} \in E^{\mathcal{H}}$. Then for all $k \in \mathbb{N}$, we have

$$\delta^k(r \otimes s - s \otimes r).(s^k \otimes s^k) =$$

$$\sum_{i_1+i_2+i_3=k} \sigma_q^{i_1+i_3}(\delta^{(i_2)}(\frac{r}{s}))s^k\sigma_q^{i_3}(\delta^{(i_1)}(s)) \otimes \delta^{(i_3)}(s)s^k - \delta^{(i_1)}(s)s^k \otimes \sigma_q^{i_1+i_3}(\delta^{(i_2)}(\frac{r}{s}))s^k\sigma_q^{i_1}(\delta^{(i_3)}(s))$$

$$= \sum_{i_1+i_2+i_3=k} (\sigma_q^{i_3}(\delta^{(i_1)}(s)) \otimes \delta^{(i_3)}(s))(\sigma_q^{i_1+i_3}(\delta^{(i_2)}(\frac{r}{s}))s^k \otimes s^k) -$$

$$\sum_{i_1+i_2+i_3=k} (\delta^{(i_1)}(s) \otimes \sigma_q^{i_1}(\delta^{(i_3)}(s)))(s^k \otimes \sigma_q^{i_1+i_3}(\delta^{(i_2)}(\frac{r}{s}))s^k) =$$

$$\sum_{i+j=k} (\delta^{(i)}(s \otimes s))(\sigma_q^{i}(\delta^{(j)}(\frac{r}{s}))s^k \otimes s^k - s^k \otimes \sigma_q^{i}(\delta^{(j)}(\frac{r}{s}))s^k).$$

The left hand side lies in $Ker(id_R \otimes \pi_{\mathcal{H}}^{\mathcal{G}})$, since this kernel is an ID_q-ideal . So by induction, we get that $(s \otimes s)(\delta^{(k)}(\frac{r}{s})s^k \otimes s^k - s^k \otimes \delta^{(k)}(\frac{r}{s})s^k) \in Ker(id_R \otimes \pi_{\mathcal{H}}^{\mathcal{G}})$ and hence $\delta^{(k)}(\frac{r}{s}) \in E^{\mathcal{H}}$. For the second statement : if $\mathcal{H} = \mathcal{G}$, then $\pi_{\mathcal{H}}^{\mathcal{G}} = id_{C[\mathcal{G}]}$ and the considered kernel is trivial. Hence $r \otimes s = s \otimes r \in R \otimes_L R$ is trivial for all $\frac{r}{s} \in E^{\mathcal{G}}$. Thus, there exists $c \in L$ such that $r = cs$, i.e., $\frac{r}{s} = c \in L$.
Assume $\mathcal{H} \subsetneq \mathcal{G}$.Since $\mathcal{Z} = Spec(R)$ is a $\mathcal{G}_L$-torsor, the quotient scheme $\mathcal{Z}/\mathcal{G}_L$ is equal to $Spec(L)$, in particular it is a scheme, and since $\mathcal{G}_L$ and $\mathcal{H}_L$ are affine, $\mathcal{G}_L/\mathcal{H}_L$ also is a scheme. So by [13],$I.5.16.(1)$, $\mathcal{Z}/\mathcal{H}_L \simeq \mathcal{Z} \times^{\mathcal{G}_L} (\mathcal{G}_L/\mathcal{H}_L)$ is a scheme. According to Proposition 4.16, $\mathcal{Z}$ is equal to the disjoint union of its irreducible components $\{\mathcal{Z}_i\}_{i=1,\dots,s}$. Let $pr : \mathcal{Z} \mapsto \mathcal{Z}/\mathcal{H}_L$ denote the canonical projection. Now let $\overline{U} \subseteq \mathcal{Z}/\mathcal{H}_L$ be an affine open subset such that its inverse image $\mathcal{U}$ by pr has a non empty intersection with all the $\mathcal{Z}_i$. We have a monomorphism $pr_* : \mathcal{O}_{\mathcal{Z}/\mathcal{H}_L}(\overline{U}) \to \mathcal{O}_{\mathcal{Z}}(\mathcal{U})$ whose image is $\mathcal{O}_{\mathcal{Z}}(\mathcal{U})^{\mathcal{H}}$. By construction of $\overline{U}$, we have $\mathcal{O}_{\mathcal{Z}}(\mathcal{U})^{\mathcal{H}} \subset E^{\mathcal{H}}$. If $E^{\mathcal{H}} = L$, then also $\mathcal{O}_{\mathcal{Z}}(\mathcal{U})^{\mathcal{H}} = L$. So, for every affine open subset $\overline{U} \subseteq \mathcal{Z}/\mathcal{H}_L$ such that its inverse image $\mathcal{U}$ by pr has a non empty intersection with all the $\mathcal{Z}_i$, we have $\mathcal{O}_{\mathcal{Z}/\mathcal{H}_L}(\overline{U}) = L$, i.e., $\overline{U} \simeq Spec(L)$ is a single point. Hence $\mathcal{Z}/\mathcal{H}_L = Spec(L)$, which contradicts the assumption $\mathcal{H} \subsetneq \mathcal{G}$.

Theorem 4.20 (Galois correspondence) *Let R/L be an iterative q-difference Picard-Vessiot ring over L, let E denotes its total iterative q-difference Picard-Vessiot extension and let $\mathcal{G} := \underline{Gal}(R/L)$ be the Galois group scheme of R.*

1. *Then there is an antiisomorphism of lattices between:*

$$\mathfrak{H} := \{\mathcal{H} | \mathcal{H} \subset \mathcal{G} \text{ closed subgroup scheme of } \mathcal{G}\}$$

and

$$\mathfrak{T} := \{T | L \subset T \subset E \text{ intermediate } ID_q - \text{ring s.t. any non zero divisor of } T \text{ is a unit of } T\}$$

given by $\Psi : \mathfrak{H} \to \mathfrak{T}$, $\mathcal{H} \mapsto E^{\mathcal{H}}$ *and* $\Phi : \mathfrak{T} \to \mathfrak{H}$, $T \mapsto \underline{Gal}(RT/T)$.

2. *If* $\mathcal{H} \subset \mathcal{G}$ *is normal then* $R^{\mathcal{H}}$ *is an iterative q-difference Picard-Vessiot ring over* L *and* $E^{\mathcal{H}}$ *is its total iterative q-difference Picard-Vessiot extension; the Galois group scheme of* $R^{\mathcal{H}}$ *over* L *is isomorphic to* $\mathcal{G}/\mathcal{H}$.

3. *For* $\mathcal{H} \in \mathfrak{H}$, *the extension* $E/E^{\mathcal{H}}$ *is separable if and only if* $\mathcal{H}$ *is reduced.*

Proof

1. Let $T \in \mathfrak{T}$ be an intermediate ID_q ring such that any non zero divisor of T is a unit of T. Then the compositum $RT \subset E$ is a ID_q-Picard-Vessiot ring over T. Furthermore, the canonical ID_q-epimorphism $RT \otimes_C C[\mathcal{G}] \mapsto RT \otimes_T RT$ gives rise to an ID_q-epimorphism

$$RT \otimes_C C[\mathcal{G}] \xrightarrow{\gamma_{RT}^{-1}} RT \otimes LR \longrightarrow RT \otimes_T RT \ .$$

   By Lemma 4.10, the kernel of this epimorphism is given by $RT \otimes_C I$ for some ideal $I \subset C[\mathcal{G}]$. Denote by $\mathcal{H}$ the closed sub-scheme of $\mathcal{G}$ defined by I, then γ_{RT} induces a isomorphism

$$RT \otimes_T RT \simeq RT \otimes_C C[\mathcal{H}].$$

   By construction, this isomorphism is the isomorphism for the base ring T, hence the sub-scheme $\mathcal{H}$ equals the Galois group scheme $\underline{Gal}(RT/T)$. Thus $\underline{Gal}(RT/T)$ is indeed a closed subgroup scheme of $\mathcal{G}$.
   Now let us apply Proposition 4.19 to the extension E/T. It follows that $E^{\underline{Gal}(RT/T)} = T$, so $\Psi \circ \Phi = id_{\mathfrak{T}}$. On the other hand, for given $\mathcal{H} \in \mathfrak{H}$ and $T := E^{\mathcal{H}}$, we get an ID_q- epimorphism $RT \otimes_T RT \mapsto RT \otimes_C C[\mathcal{H}]$ induced by γ_{RT}. This embeds $\mathcal{H}$ as a closed subgroup scheme in $\underline{Gal}(RT/T)$. But the localization $Loc(RT)$ of RT by its set of non zero divisors is equal to E, so $Loc(RT)^{\mathcal{H}} = E^{\mathcal{H}} = T$ and so by Proposition 4.19, we have $\mathcal{H} = \underline{Gal}(RT/T)$. Thereby $\Phi \circ \Psi = id_{\mathfrak{H}}$.

2. Let $\mathcal{H} \subset \mathcal{G}$ be normal. The isomorphism γ is $\mathcal{H}$-equivariant and hence we get an ID_q-isomorphism
$$R \otimes_L R^{\mathcal{H}} \simeq R \otimes_C C[\mathcal{G}]^{\mathcal{H}}.$$
Since R is normal, $\mathcal{G}/\mathcal{H}$ is an affine group scheme with $C[\mathcal{G}/\mathcal{H}] = C[\mathcal{G}]^{\mathcal{H}}$ ([7], III, Sec. 3, Thm. 5.6). Again by taking invariants the isomorphism above restricts to an isomorphism
$$R^{\mathcal{H}} \otimes_L R^{\mathcal{H}} \simeq R^{\mathcal{H}} \otimes_C C[\mathcal{G}/\mathcal{H}].$$
The ring $R^{\mathcal{H}}$ is ID_q-simple, because for every ID_q-ideal $P \subset R^{\mathcal{H}}$, the ideal $P.R \subset R$ is an ID_q-ideal, hence equals (0) or R and so $P = (P.R)^{\mathcal{H}}$ is (0) or $R^{\mathcal{H}}$. Since $L \subset R^{\mathcal{H}} \subset R$, we also have $C(R^{\mathcal{H}}) = C$. So by proposition 4.17, $R^{\mathcal{H}}$ is an ID_q Picard-Vessiot ring over L with Galois group scheme $\mathcal{G}/\mathcal{H}$. It remains to show that $E^{\mathcal{H}} = Loc(R^{\mathcal{H}})$.
Let $\tilde{L} := Loc(R^{\mathcal{H}})$ and $\tilde{\mathcal{G}} := \underline{Gal}(E/\tilde{L})$. Then $\mathcal{H}$ is a normal subgroup of $\tilde{\mathcal{G}}$ and by the previous $(R.\tilde{L})^{\mathcal{H}}$ is a $\tilde{\mathcal{G}}/\mathcal{H}$-torsor. But $(R.\tilde{L})^{\mathcal{H}} = R^{\mathcal{H}}.\tilde{L} = \tilde{L}$, so $\tilde{\mathcal{G}} = \mathcal{H}$, and hence $E^{\mathcal{H}} = E^{\tilde{\mathcal{G}}} = \tilde{L} = Loc(R^{\mathcal{H}})$.

3. Without loss of generality we may assume that $\mathcal{H} = \mathcal{G}$. Let us denote by $\mathcal{G}_{red} \subset \mathcal{G}$ the closed reduced subgroup given by the nilradical ideal . Since $\mathcal{G}_{red}$ is normal in $\mathcal{G}$, by the second statement $\tilde{L} := Loc(R^{\mathcal{G}_{red}})$ is an ID_q Picard-Vessiot extension of L with Galois group scheme $\underline{Gal}(\tilde{L}/L) = \mathcal{G}_{red}$. But this group scheme is infinitesimal and so by [4], Cor. 1.12, $\tilde{L}/L$ is purely inseparable. On the other hand, if E/L is inseparable and $p = char(L)$, then $\tilde{L} := E \cap L^{\frac{1}{p}} \neq L$ is a finitely purely inseparable ID_q-ring extension of L. Since every such extension is an ID_q- Picard-Vessiot ring with an infinitesimal Galois group scheme, $\mathcal{G}$ has a non reduced quotient and therefore $\mathcal{G}$ is not reduced.

4.2.3 Examples of Galois groups

The Galois group $\mathbb{G}_m$ in characteristic p Let us denote by $C = \overline{\mathbb{F}_p}$ the algebraic closure of $\mathbb{F}_p$, where p is a prime number. Let $F = C(t)$ be a rational function field with coefficients in C. Let $(a_l)_{l \geq 0}$ be a set of elements in $\mathbb{F}_p$. Let $M = Fb_1$ be the ID_q-module with corresponding ID_qE:
$$\delta_M^{(np^k)}(y) = \frac{a_k}{t^{np^k}} y$$
where $k \in \mathbb{N}$ and
$$\delta_M^{(1)}(y) = \frac{y}{t}.$$

Theorem 4.21 *Let M be as above with its associated ID_qE, and let $\alpha = \sum_{l \geq 0} a_l p^l \in \mathbb{Q}_p$. Then for an iterative Picard-Vessiot extension E/F for M, we have*
$\underline{\mathrm{Gal}}(E/F) \simeq \mathbb{Z}/m\mathbb{Z}$ *for some m if $\alpha \in \mathbb{Q}$ and* $\underline{\mathrm{Gal}}(E/F) \simeq \mathbb{G}_m$ *if $\alpha \notin \mathbb{Q}$.*

Proof
First of all, let us show that $\underline{\mathrm{Gal}}(E/F)$ is a subgroup of $\mathbb{G}_m$. Let y be a solution of the ID_qE associated to M, then $E = F(y)$. Let $\tau \in \underline{\mathrm{Gal}}(E/F)$ and $l \in \mathbb{N}$, we have $\delta^{(np^l)}(\frac{\tau(y)}{y}) = 0$ and $\delta^{(1)}(\frac{\tau(y)}{y}) = 0$. Thus, there exist $c \in C^*$ such that $\tau(y) = cy$. Therefore, $\underline{\mathrm{Gal}}(E/F) \subseteq \mathbb{G}_m$.

Let us assume that $\alpha = \frac{a}{m}$ where $(a, m) \in \mathbb{Z} \times \mathbb{N}^*$. Put $z = t^{a/m}$. Because $z = t^\alpha$, we have $\delta^{(j)}(z) = 0$ if $j \neq n^k$. We have

$$\delta^{(np^k)}(z^m) = \sum_{i_1+\ldots+i_m=np^k} \sigma_q^{i_2+\ldots+i_m}(\delta^{(i_1)}(z))\ldots\sigma_q^{i_m}(\delta^{(i_{m-1})}(z))\delta^{(i_m)}(z).$$

If one of the i_j is not equal to np^k, there exists i_l such that $i_l \neq p^j$ for $j \leq np^k$. Then, an easy computation shows that for all $k \in \mathbb{N}$,

$$\delta^{(np^k)}(z^m) = mz^{m-1}\delta^{(np^k)}(z).$$

It follows that

$$mz^{m-1}\delta^{(np^k)}(z) = \binom{a}{np^k}_q t^{a-np^k}.$$

By Proposition 2.2, we have $\binom{a}{np^k}_q = ma_k$ and thus $\delta_M^{(np^k)}(z) = \frac{a_k}{t^{np^k}}z$. Because $E = F(z)$ and $z^m \in F$, we get that $\underline{\mathrm{Gal}}(E/F)$ is a cyclic group.

Conversely, suppose that y is an algebraic solution of the ID_qE associated to M, then $E = F(y)$ is algebraic over F and $\underline{\mathrm{Gal}}(E/F)(C) \subsetneq \mathbb{G}_m(C)$ is a cyclic group of order m. So there exist $s \in \mathbb{Z}$ and $(b_i)_{i\geq s}$ with $b_s = 1$ such that $y^m = \sum_{i\geq s} b_i t^i \in F$. Thus,

$$my^{m-1}\delta^{(n)}(y) = y^m\frac{a_0}{t^n} = \delta^{(n)}(y^m) = \sum_{i\geq s} b_i\binom{i}{n}_q t^{i-n}.$$

By comparing the coefficient of t^l, we obtain

$$ma_o = b_i\binom{i}{n}_q \text{ for all} i \geq s.$$

Since $b_s = 1$ and because of the properties of q-binomials coefficients, we obtain

1. $s = k_s n$ with $k_s \in \mathbb{Z}$ and $a_0 = \frac{k_s}{m}$,
2. $b_i = 0$ for all $i \neq 0 \bmod n$.

Induction using the higher iterative differences shows that $b_i = 0$ for all $i > s$ and hence that $y^m = t^s$. By an argument used in the first part of the proof it follows that $\alpha = \frac{s}{m}$.

The Galois group $\mathbb{G}_m$ in characteristic 0 Let $L = \mathbb{C}(t)$ and let q be a n-th primitive root of unity. Let $M = Fb_1$ be a rank one $IDM_q(L)$-module and suppose that $\Phi(b_1) = b_1$. Let $a \in \mathbb{C}$. Then, let us consider the ID_qE associated to M, that is $\delta^{(1)}(\mathbf{y}) = 0$ and $\delta^{(n)}(\mathbf{y}) = \frac{a}{nt^n}\mathbf{y}$.

Theorem 4.22 *Let M be as above with its associated ID_qE. Then for an iterative Picard-Vessiot extension E/F for M, we have*

$\underline{\mathrm{Gal}}(E/F)$ is finite cyclic if $a \in \mathbb{Q}$ and $\underline{\mathrm{Gal}}(E/F) \simeq \mathbb{G}_m$ if $a \notin \mathbb{Q}$.

Proof

First of all, let us show that $\underline{\mathrm{Gal}}(E/F)$ is a subgroup of $\mathbb{G}_m$. Let y be a solution of the ID_qE associated to M, then $E = F(y)$. Let $\tau \in \underline{\mathrm{Gal}}(E/F)$. Then, we have

1. $$\delta^{(1)}(\frac{\tau(y)}{y}) = \sigma_q(\frac{1}{y})\tau(\delta^{(1)}y) + \delta^{(1)}(\frac{1}{y})\tau(y) = 0,\ (\delta^{(1)}(y) = 0),$$

2. $$\delta^{(n)}(\frac{\tau(y)}{y}) = (\frac{1}{y})\tau(\delta^{(n)}y) + \delta^{(n)}(\frac{1}{y})\tau(y) = -\frac{a}{nt^n}\frac{\tau(y)}{y} + \frac{1}{y}\tau(\frac{a}{nt^n}y) = 0$$

Thus, there exist $c \in C^*$ such that $\tau(y) = cy$. Therefore, $\underline{\mathrm{Gal}}(E/F) \leq \mathbb{G}_m$.

Let us assume that $a = \frac{nb}{m}$ where $(b, m) \in \mathbb{Z} \times \mathbb{N}^*$. Put $z = t^{nb/m}$. Because $z = t^a$, we have $\delta^{(j)}(z) = 0$ if $j \notin n\mathbb{N}$. We have

$$\delta^{(n)}(z^m) = \sum_{i_1+\ldots+i_m=n} \sigma_q^{i_2+\ldots+i_m}(\delta^{(i_1)}(z))\ldots\sigma_q^{i_m}(\delta^{(i_{m-1})}(z))\delta^{(i_m)}(z).$$

If one of the i_j is not equal to n, there exists i_l such that $i_l \neq n$. Then, an easy computation shows that

$$\delta^{(n)}(z^m) = mz^{m-1}\delta^{(n)}(z).$$

It follows that,

$$mz^{m-1}\delta^{(n)}(z) = \binom{nb}{n}_q t^{nb-n}.$$

By Proposition 2.2, we have $\binom{nb}{n}_q = b = m\frac{a}{n}$ and thus $\delta_M^{(n)}(z) = \frac{a}{nt^n}z$. Thus $E = F(z)$ and $z^m \in F$. It follows that $\underline{\mathrm{Gal}}(E/F)$ is a finite cyclic group.

Conversely, suppose that y is an algebraic solution of the ID_qE associated to M, then $E = F(y)$ is algebraic over F and $\underline{\mathrm{Gal}}(E/F) \subsetneq \mathbb{G}_m$ is a cyclic group of order m. So there exist $s \in \mathbb{Z}$ and $(b_i)_{i\geq s}$ with $b_s = 1$ such that $y^m = \sum_{i\geq s} b_i t^i \in F$. Thus,

$$my^{m-1}\delta^{(n)}(y) = y^m\frac{a}{nt^n} = \delta^{(n)}(y^m) = \sum_{i\geq s} b_i \binom{i}{n}_q t^{i-n}.$$

By comparing the coefficient of t^l, we obtain that $\frac{a}{n} = b_i \binom{i}{n}_q$ for all $i \geq s$. Since $b_s = 1$ and because of properties of the q-binomials coefficients, we get that:

1. $s = k_s n$ with $k_s \in \mathbb{N}$ and $a = \frac{nk_s}{m}$;
2. $b_i = 0$ for all $i \neq 0 \bmod n$.

Induction using the higher iterative difference shows that $b_i = 0$ for all $i > s$. It follows that $y^m = t^s$ and $a = \frac{nk_s}{m}$.

The Galois group $\mathbb{G}_a$ in positive characteristic Let us denote by $C = \overline{\mathbb{F}_p}$ the algebraic closure of $\mathbb{F}_p$, where p is a prime number. Let $F = C(t)$ be a rational function field with coefficients in C. Let $(a_l)_{l\geq 0}$ be a set of elements in $\mathbb{F}_p$. We choose $q \in C$ a n-th primitive root of unity with n prime to p.

Let $M = Fb_1 \oplus Fb_2$ be the ID_q-module with corresponding ID_qE:

$$\delta^{(np^k)}(Y) = A_k Y = \begin{pmatrix} 0 & a_k \\ 0 & 0 \end{pmatrix} Y$$

for $k \in \mathbb{N}$.

Theorem 4.23 *Let M be as above with its associated ID_qE. Let $\alpha = \sum_{l\geq 0} a_l p^l \in \mathbb{Q}_p$. Then for an iterative Picard-Vessiot extension E/F for M, we have*
$\underline{\mathrm{Gal}}(E/F)$ is a finite subgroup of order r of $\mathbb{G}_a$ if $\alpha \in \mathbb{Q}$ and $\underline{\mathrm{Gal}}(E/F) \simeq \mathbb{G}_a$ if $\alpha \notin \mathbb{Q}$.

For the proof, we need the following lemma.

Lemma 4.24 *Let $(a_l)_{l\geq 0}$ be a sequence of elements in $\mathbb{F}_p$. The following statements are equivalent :*

1. *The sequence $(a_l)_{l\geq 0}$ is periodic from a certain rank;*
2. *$g = \sum_{l\in\mathbb{N}} a_l t^{np^l} \in C((t))$ is separable algebraic over $C(t)$.*

Proof
see [16] p.30 and replace t by t^n.
Proof of Theorem 4.23
We start with the iterative differential equation,

$$\delta^{(np^k)}(Y) = A_k = \begin{pmatrix} 0 & a_k \\ 0 & 0 \end{pmatrix} Y$$

for $k \in \mathbb{N}$.

Writing $Y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$, we find that $\delta^{(k)}(y_2) = 0$ for all $k \in \mathbb{N}$, which implies $y_2 \in C$. Using this result we obtain $\delta^{(np^k)}(y_1) = a_k y_2$ for all $k \in \mathbb{N}$ and $\delta^{(1)}(y_1) = a_{-1} y_2$. Thus, the formal solution y_1 is equal to

$$y_1 = y_2(\sum_{l \in \mathbb{N}} a_l t^{np^l}).$$

Then $E = F(y_1, y_2) = F(y_1)$, and for any $\tau \in \underline{\mathrm{Gal}}(E/F)$ we get

$$\delta^{(np^l)}(\tau(y_1) - y_1) = \tau(\delta^{(np^l)}(y_1)) - \delta^{(np^l)}(y_1) = \tau(y_2 a_l) - y_2 a_l = 0.$$

thus there exists $d \in c$ such that $\tau(y_1) = y_1 + d$. Therefore $\underline{\mathrm{Gal}}(E/F)$ is a subgroup of $\mathbb{G}_a$.

Using Lemma 4.24, we obtain

1. the solution y_1 is separable algebraic over F if $\alpha \in \mathbb{Q}$ (the sequence $(a_l)_{l \geq 0}$ is periodic from a certain index if and only if $\alpha \in \mathbb{Q}$), so the Galois group is actually finite.

2. If $\alpha \notin \mathbb{Q}$, then y_1 is transcendent over F, and hence E/F is purely transcendental of degree 1, showing that $\underline{\mathrm{Gal}}(E/F) \simeq \mathbb{G}_a$.

Remark 4.25 *These examples of iterative q-difference equations are obtained by q-deformation of the examples of B.H. Matzat in [16] example* 2.14 *and* 2.15. *The Galois groups obtained here are the same as those obtained by Matzat. The fact that simple Galois groups such as* $\mathbf{G}_m$ *and* $\mathbf{G}_a$ *do not degenerate by q-deformation give us a nice hope for confluence studies.*

5 An analogue of the Grothendieck-Katz conjecture

In this section, we state an analogue of the Grothendieck-Katz conjecture for iterative q-difference equations. In [8], L. Di Vizio proves this conjecture for q-difference equations with q non equal to a root of unity. Briefly, she shows that given a q-difference equation, $\mathcal{L}y = 0$ with coefficients in $\mathbb{Q}(t)$, one can describe the behavior of the solutions of $\mathcal{L}$ by considering the reduction of $\mathcal{L}$ modulo the prime numbers.
Here is the iterative q-difference version of this conjecture.

Let K be a number field and $\mathcal{O}_K$ the ring of integers of K. We choose an element q in K^*, non equal to 1. We denote by Σ_f the set of all finite places v of K. The uniformizer of the finite place v is denoted by π_v and $||_v$ denotes the v-adic absolute value of K. We denote by p_v be the characteristic of the residue field k_v of π_v. For almost all finite places v, let κ_v be the multiplicative order of the image of q in k_v. If q is not a root of unity, let $\pi_{q,v}$ be the integer power of π_v such that $|\pi_{q,v}|_v = |1 - q^{\kappa_v}|_v$. If q is a root of unity, let $\pi_{q,v} = \pi_v$.

Conjecture 5.1 *Let $(\mathcal{M}, \phi_M, \delta_M^*)$ be an iterative q-difference module defined over $K(t)$. The iterative q-difference module $\mathcal{M}$ is isotrivial, i.e. becomes trivial after a finite base field extension if and only if for almost all finite places v, the reduction modulo $\pi_{q,v}$ of $\phi_M^{\kappa_v}$ is the identity and the one of $(\delta_M^{(\kappa_v)})^{p_v}$ is equal to zero.*

If q is not a root of unity, Conjecture 5.1 is equivalent to Theorem 7.1.1 in [8] and when q goes to 1, we retrieve the classical Grothendieck's conjecture on p-curvatures, which predicts :

The differential equation $Ly = 0$ with $L \in \mathbb{Q}[\partial]$ has a full set of algebraic solutions if and only if for almost all primes $p \in \mathbb{Z}$ the reduction modulo p of $Ly = 0$ has a full set of solutions in $\mathbf{F}_p(t)$ i.e. the p-curvature of L is equal to zero.

Here is an example where Conjecture 5.1 holds.

Example 5.2 (Example 3.21) *Let $a \in K$. Then, let us consider the ID_qE : $\delta^{(1)}(\mathbf{y}) = 0$ and $\delta^{(n)}(\mathbf{y}) = \frac{a}{nt^n}\mathbf{y}$. Let v be a place of K. A simple calculation shows that the reduction of $\delta_M^{(\kappa_v)})^{p_v}$ modulo $\pi_{q,v}$ is equal to $a(a-1)...(a-(p_v-1))$. If, we assume that for almost all finite places v, the reduction modulo $\pi_{q,v}$ of $\phi_M^{\kappa_v}$ is the identity and the one of $(\delta_M^{(\kappa_v)})^{p_v}$ is equal to zero, we get that for almost all finite places v there exists $a_v \in \mathbb{Z}$ such that the valuation of $a - a_v$ in π_v is strictly positive. By the Density Theorem of Chebotarev, we obtain that $a \in \mathbb{Q}$. We have proved in Theorem 4.22 that $a \in \mathbb{Q}$ if and only if $\mathcal{M}$ has a finite Galois group.*

References

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

[2] Y. André and Lucia Di Vizio. q difference equations and p-adic local monodromy, *Astrisque* , 296: 55–111, 2004. Analyse complexe, sytèmes dynamiques, sommabilité des séries divergentes et théories galoisiennes.I.

[3] A. Borel. *Linear algebraic groups.* Springer-Verlag, New York, 1991.

[4] S.U. Chase. Infinitesimal Group scheme Actions on Finite Field Extensions, *Am.J.Math*, Vol 98, No.2, pp. 441-480 (1976).

[5] Z. Chatzidakis, C. Hardouin and M.F. Singer. On the definitions of difference Galois groups, Model Theory with applications to algebra and analysis, I and II, (Z. Chatzidakis, H.D. Macpherson, A. Pillay, A.J. Wilkie editors), Cambridge University Press, Cambridge, to appear.

[6] P. Deligne. *Catégories tannakiennes*, volume 87 of Progr. Math. Birkhäuser Boston, Boston, MA, 1990, 111-195.

[7] M. Demazure, P. Gabriel. *Groupes algébriques, tome 1* North-Holland Pub. Comp., Amsterdam, (1970).

[8] L. Di Vizio. Arithmetic theory of q-difference equations: the q-analogue of Groethendieck-Katz's conjecture on p-curvature, *Invent. Math.,* 150(3): 517-578, 2002.

[9] D. Eisenbud. *Commutative Algebra.* Springer-Verlag, New York, 1995.

[10] D. Goss. *Basis structures of function field arithmetic.* Springer-Verlag, Berlin, 1996.

[11] H. Hasse and F.K. Schmidt. Noch eine Begründung der Theorie des höheren Differentialquotienten in einem algebraischen Funktionenkörper in einer Unbestimmten, *J.Reine Angew. Math.,* 177: 215-237, 1937.

[12] P.A. Hendriks. Algebraic aspects of linear differential and difference equations, Ph.D Thesis, University of Groeningen, 1996.

[13] J.C. Jantzen. *Representations of algebraic groups, second edition.* American Mathematical Society 2003.

[14] S. Lang. *Algebra.* Addison-Wesley Publishing Company, Inc.,1965.

[15] F. Marotte, C. Zhang. Multisommabilité des séries entières solutions formelles d'une équation aux q-différences linéaire analytique, *Annales de l'Institut Fourier*, 50 no. 6 (2000), p. 1859-1890.

[16] B.H. Matzat. Differential Galois theory in positive characteristic, Preprint IWR 2001 - 35, 2001.

[17] B.H. Matzat and M. van der Put. Iterative differential equations and the Abhyankar conjecture, *J.reine angew. Math.*, 557 (2003),1–52.

[18] A. Pulita. p-adic confluence of q-difference equations, submitted December 4, 2006.

[19] A. Röscheisen. Galois Theory of Iterative Connections and Nonreduced Galois Groups. available from arXiv at http://arxiv.org/abs/0712.3748.

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

[21] J.-P. Serre. *Cohomologie Galoisienne*, volume 5 of Lecture Notes in Mathematics. Springer-Verlag, Berlin, fifth edition, 1994.

[22] M. van der Put. Skew differential fields, differential and difference equations, *Astérisque*, (296):191–205,vol. I, 2004.

[23] M. van der Put. Differential equations in characteristic p, *Compos.Math*, 97 (1-2): 227–251, 1995.

[24] M. van der Put and M. Reversat. Galois theory of q-difference equations, Prepub. n298 Lab. E.Picard, 2005.

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

[26] T. A. Springer. *Linear algebraic groups*, volume 9 of Progress in Mathematics. Birkhäuser Boston Inc., Boston, 1998.