Deuxième partie.

Sur la théorie arithmétique

des équations aux q-différences

Section III.
The q-analogue of Grothendieck's conjecture on p-curvatures

Introduction.

The Grothendieck conjecture on p-curvatures is related to the classical problem of finding algebraic solutions of differential equations. More precisely, when we consider a differential equation

$$\mathcal{L}y = a_\mu(x)\frac{d^\mu y}{dx^\mu} + a_{\mu-1}(x)\frac{d^{\mu-1}y}{dx^{\mu-1}} + \ldots + a_0(x)y = 0 \ ,$$

with coefficients in the field $\mathbb{Q}(x)$ of rational function in the variable x over the field of rational numbers, for almost all prime $p \in \mathbb{Z}$ we can reduce the equation $\mathcal{L}y = 0$ modulo p; then the Grothendieck conjecture predicts:

Grothendieck's conjecture on p-curvatures. *The equation $\mathcal{L}y = 0$ has a full set of algebraic solutions if and only if for almost all primes $p \in \mathbb{Z}$ the reduction modulo p of $\mathcal{L}y = 0$ has a full set of solutions in $\mathbb{F}_p(x)$.*

The conjecture is proved essentially for differential equations of order one over a Riemann surface and for connections *coming from geometry*: the general case is still open.

In the present paper we prove an analogue of Grothendieck's conjecture on p-curvatures for q-difference equations. Let q be a non zero rational number. We consider the operator

$$\begin{array}{rccc} \varphi_q : & \mathbb{Q}(x) & \longrightarrow & \mathbb{Q}(x) \\ & f(x) & \longmapsto & f(qx) \end{array}$$

and the q-difference equation

$$\mathcal{L}y = a_\mu(x)y(q^\mu x) + a_{\mu-1}(x)y(q^{\mu-1}x) + \ldots + a_0(x)y(x) = 0 \ , \ a_\mu(x) \neq 0 \ ,$$

with $a_i(x) \in \mathbb{Q}(x)$. For almost all rational primes p the image $\overline{q}$ of q in $\mathbb{F}_p$ is non zero and generates a cyclic subgroup of $\mathbb{F}_p^\times$ of order κ_p. For almost all p there exists a positive integer ℓ_p

such that $1-q^{\kappa_p}=p^{\ell_p}\frac{h}{g}$, with $h,g\in\mathbb{Z}$ primes to p and we can consider the reduction $\mathcal{L}_p y=0$ of $\mathcal{L}y=0$ modulo p^{ℓ_p}. Let as consider a $\mathbb{Z}$-algebra $\mathcal{A}=\mathbb{Z}\left[x,\frac{1}{P(q^i x)},i\geq 1\right]$, with $P(x)\in\mathbb{Z}[x]$, such that $a_i(x)\in\mathbb{Z}\left[x,\frac{1}{P(q^i x)},i\geq 1\right]$, for all $i=0,\ldots,\mu$.

Our main result is (*cf.* (7.1.1) below):

Theorem 1. *The q-difference equation $\mathcal{L}y=0$ has a full set of solutions in $\mathbb{Q}(x)$ if and only if for almost all rational primes p the equations $\mathcal{L}_p y=0$ has a full set of solutions in $\mathcal{A}\otimes_{\mathbb{Z}}\mathbb{Z}/p^{\ell_p}\mathbb{Z}$.*

The techniques employed in the proof of Theorem 1 are borrowed from the theory of G-functions. There are essentially two properties of arithmetic q-difference equations which allow us to obtain stronger results than in the differential case:
1) A formal power series with a non zero radius of convergence solution of a q-difference equation has infinite radius of meromorphy whenever $|q|>1$. If the algebraic number q is not a root of unity, we can always find a place, archimedean or not, such that the associated norm of q is greater than 1. This is the very key-point of the proof: if we had good meromorphic uniformization of solutions of arithmetic differential equations, Grothendieck's conjecture would become a corollary of G-functions theory.
2) An arithmetic differential equation, whose reduction modulo p can be written as a product of trivial factors for almost every p, is regular singular and has rational exponents (*cf.* [K1, 13.0]). A q-difference equation, whose reduction modulo p can be written as a product of trivial factors for almost every p, is not only regular singular, but its "exponents" are in $q^{\mathbb{Z}}$. If, moreover, its reduction is trivial for almost every p the equation has a complete system of solutions in $K((x))$.

In one instance the techniques used in G-function theory give a weaker result in the q-difference case: the q-analogue of the Katz's estimates for the p-adic generic radius of convergence is very unsatisfactory (*cf.* §5 below). This is at the origin of many complications in the text (*cf.* (8.1)): actually the naive q-analogue of the notion of nilpotent reduction does not allow us to conclude the proof of our main result. A deeper analysis of the definition of p-curvatures for arithmetic differential equation has shown that we can define two q-analogue of the notion of trivial reduction (*cf.* §1). Both of them are natural and useful. The first one permits only to obtain the triviality over $K((x))$, the second one leads to the triviality over $K(x)$.

Finally, we want to put the accent on the fact that we have very poor information on the sequence of integers $(\kappa_p)_p$ and no control at all on $(\ell_p)_p$. We are just able to prove (*cf.* (6.1.2)) that the sequence $(\kappa_p)_p$ determines completely q. The difficulties linked to these numbers and their distribution are the arithmetical counterpart of the classical (archimedean) problem of small divisors. This becomes more clear if we translate the definition of κ_p and ℓ_p as follows:

$$\kappa_p=\min\{m\in\mathbb{Z}:\ m>0,\ |1-q^m|_p<1\}$$

and $p^{-\ell_p}=|1-q^{\kappa_p}|_p$, where $|\ |_p$ is the p-adic norm over $\mathbb{Q}$, such that $|p|_p=p^{-1}$.

In this arithmetical framework it would seem natural to assume that for all embeddings $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$, the image of q in $\mathbb{C}$ does not have complex norm 1, in order to avoid the problem of small divisors. Actually, this assumption is not needed since q is an algebraic number. In (8.3) we need to show that a formal power series $y(x) \in \mathbb{C}[\![x]\!]$ solution of a regular singular q-difference equation with coefficients in $\mathbb{C}(x)$ is convergent. In [Be], the author gives some technical sufficient conditions on the estimate of $|1 - q^n|_{\mathbb{C}}$ to assure the convergence of the power series $y(x)$. It is a consequence of the Baker's theorem on linear forms in logarithms that these conditions are always verified when q is an algebraic number. It is possible that the technique of (8.3) can be applied to more general problems of small divisors.

* * *

The Grothendieck conjecture on p-curvatures is a classical problem in arithmetic theory of differential equations. Gothendieck proved the conjecture [Ho] for differential equations of order 1 on the affine line and G. and D. Chudnovsky [CC] proved it for differential equations on the affine line, coming from differential equations of order one on curves of higher genus. Recently Y. André [A2] has proved the conjecture for connections *coming from geometry* and their deformations, generalizing previous results of Katz [K2]. Finally we mention a very recent result by J-B. Bost about some arithmetic criteria of algebraicity for foliations, which is deeply linked to the conjecture above. The general case of the conjecture is still open.

On the other hand, the arithmetic theory of q-difference equations is still at its beginning, and the literature on this topic is not very ample. About the problem of finding rational solutions of q-difference equations, we cite the following theorem:

[BB, 7.1] *Let $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ and let $q_1, q_2 \in \overline{\mathbb{Q}}$ be multiplicatively independent. If the formal power series $y(x)$ with coefficients in $\overline{\mathbb{Q}}$ is solution of the system:*

$$\begin{cases} a_\mu(x)y(q_1^\mu x) + a_{\mu-1}(x)y(q_1^{\mu-1}x) + \ldots + a_0(x)y(x) = 0 \\ b_\mu(x)y(q_2^\mu x) + b_{\mu-1}(x)y(q_2^{\mu-1}x) + \ldots + b_0(x)y(x) = 0 \end{cases},$$

with $a_0(x), \ldots, a_\mu(x), b_0(x), \ldots, b_\mu(x) \in \overline{\mathbb{Q}}[x]$, and $a_0(x)b_0(x) \neq 0$, then $y(x)$ is the Taylor expansion of a rational function $\in \overline{\mathbb{Q}}(x)$.

In any case, our approach is completely different from the one in [BB].

* * *

We think that the topic of the present paper may be developped much further. As in the differential case, we can formulate an analogue of Katz's conjectural description of the generic Galois group (*cf.* [K3], and [DV] for the q-difference case) and prove that it is equivalent to theorem 1. In some cases, it permits to calculate in a quite simple way the Galois group of a q-difference module. It is quite surprising to remark that the conjectural description of the differential Galois group in [K3] doesn't seem as powerful as its q-analogue.

Another problem related to our results is the construction of an analogue of the theory

of G-functions for q-difference equations, including Heine's series having rational coefficients: the problem is that by (8.4) any G-function solution of a q-difference equation is a rational function. This question is already proposed in [A3] and it is fundamental in the construction of an arithmetic Gevrey theory for q-difference equations.

Finally, we recall that, in [PS], a counterexample is shown to the naive analogue of Grothendieck's conjecture for finite difference equations. However the authors suggest a link between the property of having p-curvature zero for almost all primes and arithmetic properties of the solutions, but they do not formulate any precise statement. It seems to us that the proof of theorem 1 should partially work in the case of finite difference equations and that it is reasonable to conjecture:

Conjecture. *Let us consider the finite difference equation:*

$$\mathcal{L}y(x) = a_\mu(x)y(x+\mu) + a_{\mu-1}(x)y(x+\mu-1) + \ldots + a_0(x)y(x) = 0\ ,$$

with $a_i(x) \in \mathbb{Q}(x)$ *and let* $\mathcal{L}_p y(x) = 0$ *be the reduction of* $\mathcal{L}y(x) = 0$ *modulo* p*, existing for almost all primes* $p \in \mathbb{Z}$*. If* $\mathcal{L}_p y(x) = 0$ *has a full set of solutions in* $\mathbb{F}_p(x)$ *then the equation* $\mathcal{L}y(x) = 0$ *has a full set of solutions in* $\mathbb{Q}[\![x]\!]$*, which are G-functions.*

* * *

The paper is organized as follows.

The first section contains some considerations on arithmetic differential module, with the purpose of motivating the choice of considering two different q-analogues of the notion of nilpotent reduction.

In the second section we introduce some basic properties of q-difference modules, in particular a q-analogue of the cyclic vector lemma. Moreover we recall some results on the formal classification of q-difference modules.

In §3 we prove a characterization of trivial q-difference modules and of q-difference modules which are extensions of trivial ones, when q is a root of unity and K is a commutative ring. This degree of generality is motivated by theorem 1, where we consider a q-difference equation over a $\mathbb{Z}/p^{\ell_p}\mathbb{Z}$-algebra.

Sections §4and §5 are devoted to the p-adic situation. In §4 we introduce p-adic q-difference modules and we establish their first properties. In particular we prove a q-analogue of the Dwork-Frobenius-Young theorem. In §5 we introduce the two notions of nilpotent reduction and revisit and translate some classical estimates for differential modules having nilpotent reduction in the q-difference setting (*cf.* [DGS, page 96]). The results of this section are crucial for the proof of the main theorem (7.1.1), together with the results of §6.

Finally, in sections §6, §7and §8 we consider the arithmetic situation. In §6 we prove a q-analogue of [K1, 13.0]: as we have already pointed out we obtain a stronger result than in differential setting. Section §7 contains the statement of the main theorem and §8 its proof.

Acknowledgements. I am very grateful to Y. André for suggesting this subject to me, and for his assistance at every step in the preparation of this work. I would like to thank M. van der

Put for a manuscript, containing a prove of (6.2.2, 1) and some notes on the reduction modulo p of q-difference equations of rang 1, he gave to me in April 1999, and the many conversations we had in the same occasion. I am indebted to P. Colmez for his suggestion concerning (6.1.2).

Table of contents

1. Considerations on the differential case.

We would like to recall some properties of arithmetic differential modules that are supposed to motivate the structures we will introduce in the sequel. In particular the considerations below show that the two notions of nilpotent reduction introduced in §5 are both natural q-analogues of the notion of nilpotent reduction for differential modules.

Let us consider the field of rational numbers $\mathbb{Q}$. For all prime $p \in \mathbb{Z}$ we consider the p-adic norm $|\ |_p$ over $\mathbb{Q}$, normalized so that $|p|_p = p^{-1}$. By the Gauss lemma, the norm $|\ |_p$ can be extended to the p-adic Gauss norm $|\ |_{p,Gauss}$ over $\mathbb{Q}(x)$, by setting

$$\left| \frac{\sum_{i=0}^{n} a_i x^i}{\sum_{j=0}^{m} b_j x^j} \right|_{p,Gauss} = \frac{\sup_{i=0,\dots,n} |a_i|_p}{\sup_{j=0,\dots,m} |b_j|_p} \ .$$

Let us consider a differential module (M, Δ) over $\mathbb{Q}(x)$, *i.e.* a $\mathbb{Q}(x)$-vector space M of finite dimension μ equipped with a $\mathbb{Q}$-linear morphism $\Delta : M \longrightarrow M$ such that $\Delta(fm) = \frac{df}{dx} m + f\Delta(m)$, for all $f \in \mathbb{Q}(x)$ and $m \in M$. We fix a basis $\underline{e}$ of M over $\mathbb{Q}(x)$ and set $\Delta^n \underline{e} = \underline{e} G_n(x)$, for all $n \geq 1$, where $G_n(x) \in M_{\mu\times\mu}(\mathbb{Q}(x))$ is a square matrix of order μ with coefficients in $\mathbb{Q}(x)$. The matrix $\sum_{n\geq 0} \frac{G_n(t)}{n!}(x-t)^n \in M_{\mu\times\mu}(\mathbb{Q}(t)[\![x-t]\!])$ is a formal solution of $\frac{dY}{dx} = Y G_1(x)$ at any t in the algebraic closure of $\mathbb{Q}$, such that $G_1(x)$ has no pole at t.

For almost all primes $p \in \mathbb{Z}$ we have $|G_1(x)|_{p,Gauss} \leq 1$ and we can consider the image of $G_1(x)$ in $M_{\mu\times\mu}(\mathbb{F}_p(x))$. We usually say that (M, Δ) has *p-adic nilpotent reduction of order n* if $|G_{np}(x)|_{p,Gauss} < 1$ or, which is equivalent, if $G_{np}(x) \equiv 0$ modulo p. If $n = 1$ we say that (M, Δ) has *p-curvature zero*.

Another equivalent statement of the Grothendieck conjecture is:

Grothendieck's conjecture. *If (M, Δ) has p-curvature zero for almost all primes p, then (M, Δ) becomes trivial over an algebraic extension of $\mathbb{Q}(x)$.*

Let us consider the *p-adic generic radius of convergence*

$$R_p(M) = \inf\left(1, \liminf_{n\to\infty} \left| \frac{G_n(x)}{n!} \right|_{p,Gauss}^{-1/n}\right) \ .$$

If (M, Δ) has p-adic nilpotent reduction we have:

$$R_p(M) \geq p^{1/np} p^{-1/(p-1)} \ ;$$

in particular if (M, Δ) has p-curvature zero the previous inequality specializes to $R_p(M) \geq p^{-1/p(p-1)}$. An important property of arithmetic differential modules is that (*cf.* (8.1))

$$\sum_{p\text{-curvature zero}} \log \frac{1}{R_p(M)} \leq \sum_{p\text{-curvature zero}} \frac{\log p}{p(p-1)} < \infty \ .$$

For the case of q-difference modules, a naive translation of these definitions gives deceiving results. A more accurate analysis of the case of p-curvature zero leads to the following remark. Let $\overline{G}_1(x)$ be the image of $G_1(x)$ in $M_{\mu\times\mu}(\mathbb{F}_p(x))$. By imposing that $G_p(x) \equiv 0$ modulo p we are actually requiring that the differential system in positive characteristic

$$\frac{dY}{dx} = Y \overline{G}_1(x)$$

has a fundamental matrix of solutions $Y(x) \in Gl_\mu(\mathbb{F}_p(x))$. Since the derivation $\frac{1}{p!}\frac{d^p}{dx^p}$ makes sense in characteristic p this implies that $\frac{1}{p!}\frac{d^pY}{dx^p} \equiv \frac{G_p(x)}{p!}Y$ modulo p, with $|G_p(x)|_{p,Gauss} \leq p^{-1} = |p!|_p$.

The problem is that in the q-difference case one defines some q-analogue of factorials, but they generally are p-adically smaller than the uniformizer p. It turns out that the q-analogue of the condition $G_p(x) \equiv 0$ modulo p is not equivalent to the q-analogue of the condition $\left|\frac{G_p(x)}{p!}\right|_{p,Gauss} \leq 1$, but both of them are linked to the property of a suitable q-difference system of having a fundamental matrix of solution in some polynomial ring over a quotient of $\mathbb{Z}$. Therefore for a q-difference module we have two natural notions of nilpotent reduction: from a *local* point of view the notions are not equivalent (*cf.* §5), but we conjecture that they are *globally* equivalent.

2. q-difference modules.

2.1. Summary of q-difference algebra.

Let R be a commutative ring.

2.1.1. q-binomials. For any $a, q \in R$ and any integer $n \geq 1$, we shall use the following standard notation:

$$\begin{aligned}
&(0)_q = 0\ ,\ (n)_q = 1 + q + \ldots + q^{n-1}\ ,\\
&[0]!_q = 1\ , [n]_q! = 1_q \cdots (n)_q\ ,\\
&(x-a)_0 = 1\ ,\ (x-a)_n = (x-a)(x-qa)\cdots(x-q^{n-1}a)\ ,\\
&(a,q)_0 = 1\ ,\ (a;q)_n = (1-a)_n\ .
\end{aligned}$$

If $q \neq 1$, we have $(n)_q = \frac{1-q^n}{1-q}$.

The *q-binomial coefficients* $\binom{n}{i}_q$ are the elements of R defined by the polynomial identity

$$(1-x)_n = \sum_{j=0}^{n} (-1)^j \binom{n}{j}_q q^{j(j-1)/2} x^j\ . \tag{2.1.1.1}$$

It was already known to Gauss that these are polynomials in q, which have the following properties:

$$\begin{aligned}
&\binom{n}{0}_q = \binom{n}{n}_q = 1\\
&\binom{n}{i}_q = \frac{[n]_q!}{[n-i]!_q[i]!_q} = \frac{(n)_q(n-1)_q\cdots(n-i+1)_q}{[i]!_q}\ ,\\
&\binom{n}{i}_q = \binom{n-1}{i-1}_q + \binom{n-1}{i}_q q^i = \binom{n-1}{i-1}_q q^{n-i} + \binom{n-1}{i}_q\ ,\ \text{for } n \geq i \geq 1.
\end{aligned} \tag{2.1.1.2}$$

2.1.2. q-dilatation. We fix a *unit* q in R. We shall consider several rings of functions of one variable x and uniformly denote by φ_q the automorphism "of dilatation" induced by $x \mapsto qx$. We shall denote this automorphism either by $f(x) \longmapsto f(qx)$ or by $f \longmapsto \varphi_q(f)$.

We shall informally refer to a R-algebra $\mathcal{F}$ of functions endowed with the operator φ_q as a *q-difference algebra over R*. A morphism $\mathcal{F} \longrightarrow \mathcal{F}'$ of q-difference algebra is a morphism of R-algebra commuting to the action of φ_q. Moreover, we shall say that a q-difference algebra $\mathcal{F}$ over R is *essentially of finite type* if there exist $P_1, \ldots, P_n \in \mathcal{F}$ such that $\mathcal{F} = R[P_1(q^i x), \ldots, P_n(q^i x); i \geq 0]$.

Examples. Typical examples of q-difference algebras are:
(i) $R((x))$, with the obvous action of φ_q.
(ii) When R is a field, the subfield $R(x)$ of $R((x))$ is a q-difference algebra over R.
(iii) The R-algebra

$$R[\![x-a]\!]_q = \left\{ \sum_{n=0}^{\infty} a_n (x-a)_n : a_n \in R \right\} \text{ , for } a \in R,\ a \neq 0,$$

with $\varphi_q(x-a)_n = q^n(x-a)_n + q^{n-1}(q^n-1)a(x-a)_{n-1}$.

Let us consider the q-difference algebra $R[x]$ and $P_1(x), \ldots, P_n(X) \in R[x]$. Then the R-algebra

$$R\left[x, \frac{1}{P_1(q^i x)}, \ldots, \frac{1}{P_n(q^i x)}, i \geq 0\right]$$

is a q-difference algebra essentially of finite type over R.

Definition 2.1.3. *The ring $C = \{f \in \mathcal{F} : \varphi(f) = f\}$ is the subring of constant of $\mathcal{F}$.*

Example 2.1.4. Let $\mathcal{F} = R((x))$. If q is not a root of unity, then $\varphi_q(f)(x) = 0$ if and only if $f \in R$. If q is a primitive root of unity of order κ, then $\varphi_q(f)(x) = f$ if and only if $f \in R((x^\kappa))$.

Definition 2.1.5. *A q-difference module $\mathcal{M} = (M, \Phi_q)$ over a q-difference algebra $\mathcal{F}$ is a free $\mathcal{F}$-module M of finite rank together with a R-linear automorphism:*

$$\Phi_q : M \longrightarrow M$$

satisfying the rule

$$\Phi_q(f(x)m) = f(qx)\Phi_q(m) \text{ , for every } f(x) \in \mathcal{F} \text{ and every } m \in M.$$

Remark. The operator Φ_q is nothing but a φ_q-semilinear automorphism of the $\mathcal{F}$-module M.

Definition 2.1.6. *A morphism $\psi : (M, \Phi_q) \longrightarrow (M', \Phi'_q)$ is a R-linear morphism $M \longrightarrow M'$ which commutes with the semilinear automorphisms Φ_q and Φ'_q.*

Let us consider a morphism $\mathcal{F} \longrightarrow \mathcal{F}'$ of q-difference algebras and a q-difference module $\mathcal{M} = (M, \Phi_q)$ over $\mathcal{F}$.

Definition 2.1.7. *The q-difference module $\mathcal{M}_{\mathcal{F}'}$ obtained form $\mathcal{M}$ by extension of coefficients from $\mathcal{F}$ to $\mathcal{F}'$ is the $\mathcal{F}'$-module $M \otimes_{\mathcal{F}} \mathcal{F}'$ equipped with the operator $\Phi_q \otimes \varphi_q$.*

2.1.8. q-derivations. Let $q \neq 1$. In this subsection, we assume that $\mathcal{F}$ is stable with respect to the operator

$$\begin{array}{rccc} d_q : & \mathcal{F} & \longrightarrow & \mathcal{F} \\ & f(x) & \longmapsto & \dfrac{\varphi_q - id}{(q-1)x} f(x) = \dfrac{f(qx) - f(x)}{(q-1)x} \end{array} .$$

Remark. The operator d_q verifies the twisted Leibniz rule:

$$d_q(fg)(x) = d_q(f)(x)g(x) + f(qx)d_q(g)(x) .$$

More generally, for any positive integer n, we have

$$d_q^n(fg)(x) = \sum_{j=0}^{n} \binom{n}{j}_q d_q^{n-j}(f)(q^j x) d_q^j(g)(x) . \tag{2.1.8.1}$$

Example 2.1.9.

1) Let us consider the q-difference algebra $\mathcal{F} = R((x))$. For any positive integer n, $d_q x^n = (n)_q x^{n-1}$. More generally

$$\frac{d_q^s}{[s]!_q} x^n = \begin{cases} 0 & \text{if } n < s \\ \binom{n}{s}_q x^{n-s} & \text{otherwise} \end{cases} .$$

2)Let $\mathcal{F} = R[\![x-a]\!]_q$; then $d_q(x-a)_n = (n)_q(x-a)_{n-1}$.

We have the following relations between d_q and φ_q:

Lemma 2.1.10. *We set $d_q^0 = \varphi_q^0 = 1$. For any integer $n \geq 1$ we obtain:*

$$\varphi_q^n = \sum_{i=0}^{n} \binom{n}{i}_q (q-1)^i q^{i(i-1)/2} x^i d_q^i$$

and

$$d_q^n = \frac{(\varphi_q - 1)_n}{(q-1)^n q^{n(n-1)/2} x^n} = \frac{(-1)^n}{(q-1)^n x^n} \sum_{j=0}^{n} (-1)^j \binom{n}{j}_{q^{-1}} q^{-\frac{j(j-1)}{2}} \varphi_q^j .$$

Proof. We remark that $xd_q \circ x^i d_q^i = q^i x^{i+1} d_q^{i+1} + (i)_q x^i d_q^i$, for all $i \geq 1$. For $n = 2$ one has:

$$\varphi_q^2 = (q-1)^2 q x^2 d_q^2 + (2)_q (q-1) x d_q + 1 \ .$$

It follows by induction that

$$\begin{aligned}
\varphi_q^{n+1} &= ((q-1)xd_q + 1)\,\varphi_q^n \\
&= \sum_{i=0}^{n} \binom{n}{i}_q (q-1)^i q^{i(i-1)/2} \left((q-1)q^i x^{i+1} d_q^{i+1} + (q-1)(i)_q x^i d_q^i + x^i d_q^i\right) \\
&= (q-1)^{n+1} q^{n(n+1)/2} x^{n+1} d_q^{n+1} + \sum_{i=1}^{n} \left(\binom{n}{i}_q q^i + \binom{n}{i-1}_q \right) (q-1)^i q^{i(i-1)/2} x^i d_q^i + 1 \\
&= \sum_{i=0}^{n+1} \binom{n+1}{i}_q (q-1)^i q^{i(i-1)/2} x^i d_q^i \ .
\end{aligned}$$

The second formula in (2.1.10) holds for $n = 1$ by definition of d_q. By induction we obtain

$$\begin{aligned}
d_q^{n+1} &= \frac{\varphi_q - 1}{(q-1)x} \circ \frac{(\varphi_q - 1)_n}{(q-1)^n q^{n(n-1)/2} x^n} \\
&= \frac{(\varphi_q - q^n)\,(\varphi_q - 1)_n}{(q-1)^{n+1} q^{n(n+1)/2} x^{n+1}} \\
&= \frac{(\varphi_q - 1)_{n+1}}{(q-1)^{n+1} q^{n(n+1)/2} x^{n+1}} \\
&= \frac{(-1)^n}{(q-1)^{n+1} x^{n+1}} (1 - \varphi_q)\left(1 - q^{-1}\varphi_q\right) \cdots \left(1 - q^{-n}\varphi_q\right) \ .
\end{aligned}$$

We conclude by using (2.1.1.1). ■

Remark. Let M be a free $\mathcal{F}$-module of finite rank. Let $\Delta_q : M \longrightarrow M$ be a R-linear endomorphism satisfying the twisted Leibniz rule:

(2.1.10.1) $\Delta_q(f(x)m) = f(qx)\Delta_q(m) + d_q(f)(x)m$, for every $f(x) \in \mathcal{F}$ and every $m \in M$.

Then $\Phi_q = (q-1)x\Delta_q + 1$ is φ_q-semilinear. Therefore, if it is invertible, it defines a q-difference module.

Conversely, if $(q-1)x$ is a unit in $\mathcal{F}$, any Φ_q gives rise to a twisted derivation Δ_q as before.

We remark that Δ_q satisfies the generalized Leibniz formula:

(2.1.10.2) $$\Delta_q^n(f(x)m) = \sum_{i=0}^{n} \binom{n}{i}_q d_q^{n-i}(f)(q^i x)\Delta_q^i(m) \ , \text{ for all } f \in \mathcal{F} \text{ and } m \in M.$$

Lemma 2.1.11. *The analogue of the formulas in (2.1.10) holds:*

(2.1.11.1) $$\Phi_q^n = \sum_{i=0}^{n} \binom{n}{i}_q (q-1)^i q^{i(i-1)/2} x^i \Delta_q^i$$

and

$$\Delta_q^n = \frac{(\Phi_q - 1)_n}{(q-1)^n q^{n(n-1)/2} x^n} = \frac{(-1)^n}{(q-1)^n x^n} \sum_{j=0}^{n} (-1)^j \binom{n}{j}_{q^{-1}} q^{-\frac{j(j-1)}{2}} \Phi_q^j \ . \tag{2.1.11.2}$$

Proof. The proof is similar to the proof of (2.1.10). ∎

2.2. The q-analogue of the Wronskian lemma.

Lemma 2.2.1. *We assume that q is not a primitive root of unity of order $\leq \mu$ and that the ring of constants $C = \{f \in \mathcal{F} : \varphi_q(f) = f\}$ is a field. Let $u_0, \dots, u_{\mu-1} \in \mathcal{F}$, then*

$$\dim_C \sum_{i=0}^{\mu-1} C u_i = \text{rank } Cas(u_0, \dots, u_{\mu-1}) \ ,$$

where $Cas(u_0, \dots, u_{\mu-1})$ is the so-called Casorati matrix

$$Cas(u_0, \dots, u_{\mu-1}) = \begin{pmatrix} u_0 & \cdots & u_{\mu-1} \\ \varphi_q u_0 & \cdots & \varphi_q u_{\mu-1} \\ \vdots & \ddots & \vdots \\ \varphi_q^{\mu-1} u_0 & \cdots & \varphi_q^{\mu-1} u_{\mu-1} \end{pmatrix}$$

Remark. Of course, if $(q-1)x$ is a unit of $\mathcal{F}$, (2.1.10) implies that

$$\text{rank} \begin{pmatrix} u_0 & \cdots & u_{\mu-1} \\ d_q u_0 & \cdots & d_q u_{\mu-1} \\ \vdots & \ddots & \vdots \\ d_q^{\mu-1} u_0 & \cdots & d_q^{\mu-1} u_{\mu-1} \end{pmatrix} = \text{rank} \begin{pmatrix} u_0 & \cdots & u_{\mu-1} \\ \varphi_q u_0 & \cdots & \varphi_q u_{\mu-1} \\ \vdots & \ddots & \vdots \\ \varphi_q^{\mu-1} u_0 & \cdots & \varphi_q^{\mu-1} u_{\mu-1} \end{pmatrix} \ .$$

Proof. Obviously we have

$$\dim_C \sum_{i=0}^{\mu-1} C u_i \geq \text{rank} \left(\varphi_q^j u_0, \dots, \varphi_q^j u_{\mu-1} \right)_{j=0,\dots,\mu-1} \ .$$

Let us suppose that the rank of $Cas(u_0, \dots, u_{\mu-1})$ is $< \mu$. Changing the order of $u_0, \dots, u_{\mu-1}$, we may assume that

$$r = \text{rank} \left(\varphi_q^j u_0, \dots, \varphi_q^j u_{\mu-1} \right)_{j=0,\dots,\mu-1} = \text{rank} \left(\varphi_q^j u_0, \dots, \varphi_q^j u_{r-1} \right)_{j=0,\dots,\mu-1} \ , \tag{2.2.1.1}$$

with $r < \mu$. It is enough to show that u_r is in $\sum_{i=0}^{r-1} C u_i$. By (2.2.1.1), there exists $(a_0, \dots, a_{r-1}) \in \mathcal{F}^r$, such that:

$$\left(\varphi_q^j u_0, \dots, \varphi_q^j u_{r-1} \right)_{j=0,\dots,\mu-1} \begin{pmatrix} a_0 \\ \vdots \\ a_{r-1} \end{pmatrix} = \left(\varphi_q^j u_r \right)_{j=0,\dots,\mu-1} \ . \tag{2.2.1.2}$$

If we apply φ_q to (2.2.1.2) and substract the expression obtained to (2.2.1.2) we get

$$(\varphi_q^j u_0(x), \ldots, \varphi_q^j u_{r-1}(x))_{j=1,\ldots,\mu-1} \begin{pmatrix} \varphi_q(a_0) - a_0 \\ \vdots \\ \varphi_q(a_{r-1}) - a_{r-1} \end{pmatrix} = 0$$

Hence $(\varphi_q a_0, \ldots, \varphi_q a_{r-1}) = (a_0, \ldots, a_{r-1})$ and therefore $a_i \in C$. ■

2.3. The q-analogue of the cyclic vector lemma.

The following q-analogue of the classical cyclic vector lemma for differential modules can be deduced from the theory of skew fields (*cf.* for instance [Ch]) but we prefer to give here an elementary proof.

Lemma 2.3.1. *Let us assume that $\mathcal{F}$ is a field of characteristic zero and that q is not a root of unity. Let (M, Φ_q) be a q-difference module of rank μ over $\mathcal{F}$. Then there exists a cyclic vector $m \in M$, i.e. an element m such that $(m, \Phi_q(m), \ldots, \Phi_q^{\mu-1}(m))$ is a $\mathcal{F}$-basis of M.*

Remark. If $(q-1)x$ is a unit of $\mathcal{F}$ and m is a cyclic vector for $\mathcal{M}$, then m is also a cyclic vector with respect to the operator Δ_q.

Proof. Let us denote by $\wedge$ the exterior product. Let

$$\nu = \max\{l \in \mathbb{Z} : \exists m \in M \text{ s.t. } m \wedge \Phi_q(m) \wedge \ldots \wedge \Phi_q^{l-1}(m) \neq 0\} \ ;$$

we suppose that ν is smaller than μ. We choose $m \in M$ such that

$$m \wedge \Phi_q(m) \wedge \ldots \wedge \Phi_q^{\nu-1}(m) \neq 0 \ .$$

Let $\lambda \in R$, $s \in \mathbb{Z}$, $s \geq 1$, and $m' \in M$. Then we have

$$\begin{aligned} 0 &= (m + \lambda x^s m') \wedge \Phi_q(m + \lambda x^s m') \wedge \ldots \wedge \Phi_q^{\nu}(m + \lambda x^s m') \\ &= m_0 + m_1\lambda + \ldots + m_\nu \lambda^\nu \ , \text{ for all } \lambda \in R, \end{aligned}$$

with $m_i \in \wedge^\nu M$. Since the field R is infinite, we have $m_0 = \ldots = m_\nu = 0$; in particular

$$m_1 = x^s \left(\sum_{i=0}^{\nu} q^{si} m \wedge \Phi_q(m) \wedge \ldots \wedge \Phi_q^{i-1}(m) \wedge \Phi_q^i(m') \wedge \Phi_q^{i+1}(m) \wedge \ldots \wedge \Phi_q^{\nu}(m) \right) = 0$$

for all positive integers s. It follows that for all $m' \in M$ and all $i = 0, \ldots, \nu$ we have

$$m \wedge \Phi_q(m) \wedge \ldots \wedge \Phi_q^{i-1}(m) \wedge \Phi_q^i(m') \wedge \Phi_q^{i+1}(m) \wedge \ldots \wedge \Phi_q^{\nu}(m) = 0 \ .$$

In particular, for $i = \nu$ we obtain

$$m \wedge \Phi_q(m) \wedge \ldots \wedge \Phi_q^{\nu-1}(m) \wedge \Phi_q^{\nu}(m') = 0 \ , \ \forall m' \in M,$$

which implies that $m \wedge \Phi_q(m) \wedge \ldots \wedge \Phi_q^{\nu-1}(m) = 0$. This contradictsthe premises and hence $\nu = \mu$. ■

2.4. Formal classification of q-difference modules.

We recall the definition of regular singularity in the q-difference case, when $K = R$ *is a field of characteristic zero and* q *is not a root of unity.* Let $\mathcal{M} = (M, \Phi_q)$ be a q-difference module over $K((x))$ of finite rank μ.

Definition 2.4.1. *One says that* $\mathcal{M}$ *is regular singular if there exists a* $K((x))$*-basis* $\underline{e}$ *of* M *in which the matrix* $A(x)$ *of* Φ_q *(a priori an element of* $Gl_\mu(K((x)))$*) belongs to* $Gl_\mu(K[\![x]\!])$.

Remark 2.4.2. It is in fact equivalent to require the existence of a basis $\underline{e}$ in which the matrix of Φ_q is a constant matrix (*cf.* [PS, Ch. 12]).

One can say more: if $\mathcal{M}$ is regular singular at zero and $\Phi_q(\underline{e}) = \underline{e}A(x)$ with $A(x) \in Gl_\mu(K[\![x]\!])$, then we can find a basis $\underline{f}$ of M over $K((x))$ such that $\Phi_q(\underline{f}) = \underline{f}A(0)$. This remark will be useful in §6.

Definition 2.4.3. *The exponents of a regular singular* q*-difference module* $\mathcal{M}$*, with respect to a given basis* $\underline{e}$ *as above, are the* q*-orbits* $q^{\mathbb{Z}}a$ *of the eigenvalues* a *of* $A(0)$.

Let us consider an extension of $K((x))$ of the form $L((t))$, where $x = t^d$ and L is a finite extension of K containing a root $\widetilde{q}$ of q of order d. Then φ_q extends canonically to $L((t))$ in the following way:

$$\begin{array}{rccc} \varphi_{\widetilde{q}}: & L((t)) & \longrightarrow & L((t)) \\ & t & \longmapsto & \widetilde{q}t \end{array} .$$

The module $L((t)) \otimes_{K((x))} M$, equipped with the operator:

$$\begin{array}{rccc} \Phi_{\widetilde{q}}: & L((t)) \otimes_{K((x))} M & \longrightarrow & L((t)) \otimes_{K((x))} M \\ & f(t) \otimes m & \longmapsto & \varphi_{\widetilde{q}}(f(t)) \otimes \Phi_q(m) \end{array}$$

is a $\widetilde{q}$-difference module over $L((t))$. We recall the following result, that will be useful in the sequel:

Theorem 2.4.4. [P, Cor. 9 and §9, 3)] *Let* K *be a field of zero characteristic,* q *not a root of unity,* $\mathcal{M}$ *a* q*-difference module over* $K((x))$ *of rank* μ*. There exists a divisor* d *of* $\mu!$ *and a finite extension* $L((t))$ *of* $K((x))$ *as above, such that the* $\widetilde{q}$*-difference module* $L((t)) \otimes_{K((x))} M$ *has a* $L((t))$*-basis* $\underline{e}$ *with the following property: the matrix* $A(t)$ *defined by* $\Phi_{\widetilde{q}}(\underline{e}) = \underline{e}A(t)$ *is a diagonal block matrix and each block has the form*

$$t^{1-\lambda_i} \begin{pmatrix} \alpha_i & 0 & 0 & \cdots & 0 \\ 1 & \alpha_i & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 & \alpha_i \end{pmatrix} ,$$

where $\lambda_i \in (1/d)\mathbb{Z}$, $\alpha_i \in \sum_{h=0}^{d} \frac{\alpha_{i,h}}{t^h}$, *with* $\alpha_{i,h} \in L$ *and* $\alpha_{i,d} \neq 0$.

The matrix $A(t)$ *is unique up to permutation of the blocks.*

Remark 2.4.5. One can prove that a q-difference submodule of a regular singular q-difference module is regular singular (*cf.* [P]).

3. Unipotent q-difference modules.

In this section R is again an arbitrary commutative ring and $q \in R$ *is a root of unity.* Let κ denote its order:

$$\kappa = \min\{m \in \mathbb{Z} : m > 0,\ q^m = 1\}\ . \tag{3.0.5.1}$$

Let $\mathcal{F}$ be a q-difference algebra over R and $C = \{f \in \mathcal{F} : \varphi_q(f) = f\}$. We notice that $\varphi_q^\kappa = id_{\mathcal{F}}$.

Remark. Let $\mathcal{M} = (M, \Phi_q)$ be a q-difference module over $\mathcal{F}$. The κ-fold iterate Φ_q^κ is a $\mathcal{F}$-linear automorphism of M.

3.1. Trivial q-difference modules.

Definition 3.1.1. *The q-difference module* $\mathcal{M} = (M, \Phi_q)$ *over* $\mathcal{F}$ *is trivial if it is isomorphic to a q-difference module of the form* $(N \otimes_C \mathcal{F}, id_N \otimes \varphi_q)$, *where* N *is a free* C*-module.*

Proposition 3.1.2.
1) If $\mathcal{M}$ *is trivial over* $\mathcal{F}$ *then* Φ_q^κ *is the identity morphism.*
2) Let R *be a field and* $\mathcal{F} = R(x)$. *If* Φ_q^κ *is the identity, then* $\mathcal{M}$ *is trivial over* $\mathcal{F}$.

Proof.
1) Let us suppose that $\mathcal{M}$ is trivial over $\mathcal{F}$. By hypothesis there exists a basis $\underline{e}$ of M over $\mathcal{F}$ such that $\Phi_q(\underline{e}) = \underline{e}$, which implies that $\Phi_q^\kappa = 1$.
2) Since R is a field we can consider the operator $\Delta_q = (\Phi_q - 1)/(q-1)x$ on M. When q is a root of unity the formula (2.1.11.1) simplifies to

$$\Phi_q^\kappa = 1 + (q-1)^\kappa x^\kappa \Delta_q^\kappa\ . \tag{3.1.2.1}$$

Therefore, under the assumption $\Phi_q^\kappa = 1$, Δ_q is a C-linear nilpotent morphism of order κ. Let $\mu = \dim_{\mathcal{F}} M$. There exists a basis $\underline{m} = (m_1, \ldots, m_{\mu\kappa})$ of M over C such that the matrix of Δ_q with respect to $\underline{m}$ is a nilpotent matrix in the canonical form. If $\mu = 1$ then $\Delta_q m_1 = 0$. Let us suppose $\mu > 2$. If for all $i = 2, \ldots, \mu\kappa$ we have $\Delta_q(m_i) = m_{i-1}$, then Δ_q would be a nilpotent C-linear morphism of order $\mu\kappa > \kappa$, therefore there exists $j \in \{2, \ldots, \mu\kappa\}$ such that $\Delta_q(m_j) = 0$. We can suppose $j = 2$. Repeating the reasoning we find that $\Delta_q(m_1) = \ldots = \Delta_q(m_\mu) = 0$. We want to show that $m_1, \ldots, m_\mu$ is a basis of M over $\mathcal{F}$. Let us suppose that $\sum_{i=1}^{\mu} a_i(x) m_i = 0$ with $a_i(x) \in R[x]$, $a_1(x) \neq 0$ and that the degree $\deg_x a_1(x)$

of $a_1(x)$ with respect to x is minimal. Then $\Delta_q\left(\sum_{i=1}^{\mu} a_i(x)m_i\right) = \sum_{i=1}^{\mu} d_q(a_i)(x)m_i = 0$, with $\deg_x d_q(a_1)(x) \leq \deg_x a_1(x) - 1$, so we get a contradiction.

Finally we have found a basis $\underline{m}' = (m_1, \ldots, m_\mu)$ of M over $\mathcal{F}$ such that $\Delta_q(\underline{m}') = 0$, which is equivalent to $\Phi_q(\underline{m}') = \underline{m}'$. This implies that $\mathcal{M}$ is trivial over $\mathcal{F}$. ■

If $(q-1)x$ is a unit of $\mathcal{F}$, the operator Δ_q is defined over M and (3.1.2.1) shows that:

Corollary 3.1.3. *The operator Φ_q^κ is unipotent if and only if Δ_q^κ is nilpotent.*

3.2. Extensions of trivial q-difference modules.

Proposition 3.2.1.
1) If the q-difference module $\mathcal{M}$ is an extension of trivial q-difference modules then the $\mathcal{F}$-linear morphism Φ_q^κ is unipotent.
2) If R is a field , $\mathcal{F} = R(x)$ and Φ_q^κ is unipotent, then $\mathcal{M}$ is extension of trivial q-difference modules.

Proof.
1) We have to prove that $\Phi_q^\kappa - id_M$ is a nilpotent endomorphism.

If $\mathcal{M}$ is extension of trivial q-difference modules over $\mathcal{F}$, by (3.1.2) we can find a basis $\underline{e}$ of M over $\mathcal{F}$ such that $\Phi_q^\kappa \underline{e} = \underline{e}(\mathbb{I} + H_\kappa(x))$, where $\mathbb{I}$ is the identity matrix and $H_\kappa(x)$ is a block matrix with entries in $\mathcal{F}$ of the form

$$H_\kappa(x) = \left(\begin{array}{c|c|c} 0 & * & * \\ \hline 0 & \ddots & * \\ \hline 0 & 0 & 0 \end{array}\right) .$$

The matrix $H_\kappa(x)$ is nilpotent, hence Φ_q^κ is an unipotent endomorphism.
2) If R is a field we can consider the operator Δ_q associated to Φ_q. Since Φ_q^κ is unipotent, the C-linear morphism Δ_q is nilpotent (*cf.* (3.1.3)), therefore there exists $m_1 \in M$ such that $\Delta_q m_1 = 0$. Let $\mu = \dim_{\mathcal{F}} M$. If $\mu = 1$ there is nothing more to prove. Let μ be greater than 1. The operator Δ_q induces a structure of q-difference module over the quotient $\mathcal{F}$-vector space $M/\mathcal{F}m_1$, which satisfies the hypothesis. By induction we can find a filtration of $M/\mathcal{F}m_1$

$$\widetilde{M}_0 = \{0\} \subset \widetilde{M}_1 \subset \ldots \subset \widetilde{M}_l = M/\mathcal{F}m_1 ,$$

such that:
1) for all $i = 0, \ldots, l$ the sub-vector space $\widetilde{M}_i$ is stable by the operator induced by Δ_q;
2) for all $i = 1, \ldots, l$ the quotient module $\widetilde{M}_i/\widetilde{M}_{i-1}$ equipped with its natural structure of q-difference module is trivial over $\mathcal{F}$.
Let $\iota : M \longrightarrow M/\mathcal{F}m_1$ be the canonical projection. Then

$$M_{-1} = \{0\} \subset M_0 = \iota^{-1}(\widetilde{M}_0) = \mathcal{F}m_1 \subset M_1 = \iota^{-1}(\widetilde{M}_1) \subset \ldots \subset M_l = \iota^{-1}(\widetilde{M}_l) = M$$

satisfies the conditions:
1) for all $i = -1, 0, \dots, l$ the sub-vector space M_i is stable under the operator induced by Δ_q;
2) for all $i = 0, \dots, l$ the quotient module $M_i/M_{i-1} \cong \widetilde{M}_i/\widetilde{M}_{i-1}$ equipped with its natural structure of q-difference module is trivial over $\mathcal{F}$. ■

Remark 3.2.2. In [H, Ch. 6] we can find a classification of q-difference modules over $R(x)$ when q is a root of unity and R is a field of zero characteristic. The author defines the Galois group associated to a linear q-difference module and proves that it is the smallest algebraic group over $R(x^\kappa)$ containing Φ_q^κ.

4. Introduction to p-adic q-difference modules.

Let K_v be a field of characteristic zero, complete with respect to a non-archimedean norm $|\ |_v$. Let $\mathcal{V}_v$ be the ring of integers of K_v, ϖ_v the uniformizer of $\mathcal{V}_v$, k_v its residue field of characteristic $p > 0$.

We fix a non-zero element $q \in K_v$, such that q is not a root of unity and $|q|_v = 1$. Let $\overline{q}$ be the image of q in k_v; we suppose that $\overline{q}$ is algebraic over the prime field $\mathbb{F}_p$ and we set

$$\kappa_v = \min\{m \in \mathbb{Z} : m > 0,\ \overline{q}^m = 1\} \geq 1 .$$

We notice that $\overline{q} \in k_v$ satisfies the assumption of the previous section.

In addition, we assume that

$$|1 - q^{\kappa_v}|_v < |p|_v^{1/(p-1)} .$$

(If q is an element of $\mathbb{Q}_p \subset K_v$ this holds automatically).

4.1. p-adic estimates of q-binomials.

Lemma 4.1.1. *Let $n \geq i \geq 0$ be two integers. We have*

$$|(n)_q!|_v = |(\kappa_v)_q|_v^{\left[\frac{n}{\kappa_v}\right]} \left|\left[\frac{n}{\kappa_v}\right]!\right|_v , \tag{4.1.1.1}$$

where $[x]$ is the integer part of $x \in \mathbb{R}$, and

$$\left|\binom{n}{i}_q\right|_v \leq 1 . \tag{4.1.1.2}$$

Proof.
1) By the definition of κ_v, if κ_v does not divide n, $|1-q^n|_v = 1$. Since $|1-q^{n\kappa_v}|_v \leq |1-q^{\kappa_v}|_v < |p|_v^{1/(p-1)}$ for all $n \in \mathbb{Z}$, $n \geq 1$, we have (*cf.* for instance [DGS, II, 1.1])

$$|1 - q^{n\kappa_v}|_v = |\log q^{n\kappa_v}|_v = |n \log q^{\kappa_v}|_v = |n|_v |1 - q^{\kappa_v}|_v , \tag{4.1.1.3}$$

so $|(n\kappa_v)_q|_v = \left|\frac{1-q^{n\kappa_v}}{1-q}\right|_v = |n|_v|(\kappa_v)_q|_v$. We obtain

$$|[n]!_q|_v = |(\kappa_v)_q|_v^{\left[\frac{n}{\kappa_v}\right]} \prod_{\substack{i\le n\\ \kappa_v|i}} |i|_v$$
$$= |(\kappa_v)_q|_v^{\left[\frac{n}{\kappa_v}\right]} |\kappa_v|_v^{\left[\frac{n}{\kappa_v}\right]} \left|\left[\frac{n}{\kappa_v}\right]!\right|_v .$$

Since κ_v is a divisor of $p^s - 1$ for a suitable integer $s \ge 1$, we have $(\kappa_v, p) = 1$, which implies that $|\kappa_v|_v = 1$.

2) Since q is an invertible element of the ring of integers $\mathcal{V}_v$, we draw the inequality $\left|\binom{n}{i}_q\right|_v \le 1$ using the relation

$$(1-x)_n = \sum_{j=0}^{n} (-1)^j \binom{n}{j}_q q^{j(j-1)/2} x^j \in \mathcal{V}_v[x] .$$

■

4.2. The Gauss norm and the invariant $\chi_v(\mathcal{M})$.

By the Gauss lemma, one can extends the norm $|\ |_v$ to the so-called Gauss norm $|\ |_{v,Gauss}$ over $K_v(x)$ by setting

$$\left|\frac{\sum_{i=0}^{n} a_i x^i}{\sum_{j=0}^{m} b_j x^j}\right|_{v,Gauss} = \frac{\sup_{i=0,\dots,n} |a_i|_v}{\sup_{j=0,\dots,m} |b_j|_v} .$$

Lemma 4.2.1. *For any $f(x) \in K_v(x)$ and any positive integer n, we have*

$$\left|\frac{d_q^n}{[n]!_q} f(x)\right|_{v,Gauss} \le |f(x)|_{v,Gauss} .$$

Proof. By (2.1.9) and (4.1.1) the inequality holds for all $f(x) \in K_v[x]$. Furthermore we have

$$\left|d_q\left(\frac{1}{f(x)}\right)\right|_{v,Gauss} = \left|\frac{d_q f(x)}{f(x)f(qx)}\right|_{v,Gauss} \le \left|\frac{1}{f(x)}\right|_{v,Gauss} .$$

By the q-analogue of the Leibniz formula (2.1.10.2) we have

$$\frac{d_q^n}{[n]!_q}\left(\frac{1}{f(x)}\right) = -\frac{1}{f(q^n x)} \sum_{i=0}^{n-1} \frac{d_q^i}{[i]!_q}(f)(q^{n-i}x) \frac{d_q^{n-i}}{[n-i]!_q}\left(\frac{1}{f(x)}\right) ;$$

and therefore by induction

$$\left|\frac{d_q^n}{[n]!_q}\left(\frac{1}{f(x)}\right)\right|_{v,Gauss} \le \left|\frac{1}{f(x)}\right|_{v,Gauss} .$$

Finally, if $g(x) \in K_v[x]$ we obtain

$$\left| \frac{d_q^n}{[n]!_q} \left(\frac{g(x)}{f(x)} \right) \right|_{v,Gauss} = \left| \sum_{i=0}^{n} \frac{d_q^i}{[i]!_q}(g)(q^{n-i}x) \frac{d_q^{n-i}}{[n-i]!_q} \left(\frac{1}{f(x)} \right) \right|_{v,Gauss} \leq \left| \frac{g(x)}{f(x)} \right|_{v,Gauss} .$$

■

Let $\mathcal{M} = (M, \Phi_q)$ be a q-difference module over $K_v(x)$. Since K_v is a field, we have well defined operators

$$d_q = \frac{\varphi_q - 1}{(q-1)x} \text{ and } \Delta_q = \frac{\Phi_q - 1}{(q-1)x}$$

acting over $K_v(x)$ and M, respectively (*cf.* (2.1.8)).

We fix a basis $\underline{e}$ of M over $K_v(x)$ and define a sequence of matrices $G_n(x) \in M_{\mu\times\mu}(K_v(x))$ for any integer $n \geq 0$, with $G_0(x) = \mathbb{I}_\mu$, by setting

$$\Delta_q^n(\underline{e}) = \underline{e}G_n(x) . \tag{4.2.1.1}$$

The matrices $G_n(x)$ satisfy the inductive relation

$$G_0(x) = \mathbb{I}_\mu,\ G(x) = G_1(x),\ G_{n+1}(x) = G_1(x)G_n(qx) + d_qG_n(x) . \tag{4.2.1.2}$$

We call

$$d_qY = YG(x) \tag{$\mathscr{S}$}$$

the *q-difference system associated to* $\mathcal{M}$ *with respect to the basis* $\underline{e}$. If zero is not a pole of $G_1(x)$, we obtain a formal solution of $(\mathscr{S})$: $\sum_{n=1}^{\infty} \frac{G_n(0)}{[n]!_q} x^n$. More generally, if $q^n a$ is not a pole of $G_1(x)$ for all positive integers n, the matrix

$$\sum_{n=1}^{\infty} \frac{G_n(a)}{[n]!_q}(x-a)_n \in M_{\mu\times\mu}(K_v[\![x-a]\!]_q)$$

is a formal solution of $(\mathscr{S})$.

One can easily check that if $\mathcal{Y}$ is a fundamental matrix for $(\mathscr{S})$ with coefficients in some fixed q-difference algebra $\mathcal{F}$ (*i.e.* an invertible matrix solution of $(\mathscr{S})$ with coefficients in $\mathcal{F}$), any other fundamental matrix of $(\mathscr{S})$ in $Gl_\mu(\mathcal{F})$ is of the form $\mathcal{Y}F$, where F is an invertible matrix with coefficients in the subring of constant of $\mathcal{F}$.

In the following definition, the sup-norm of a matrix is the maximum of the norms of its entries:

Definition 4.2.2. $\chi_v(\mathcal{M}) = \inf\left(1, \liminf_{n\to\infty} \left| \frac{G_n(x)}{[n]!_q} \right|_{v,Gauss}^{-1/n}\right)$.

Lemma 4.2.3. *Let*

$$h(n) = \sup_{s\leq n} \log^+ \left| \frac{G_s(x)}{[s]!_q} \right|_{v,Gauss} = \sup_{s\leq n} \log \left| \frac{G_s(x)}{[s]!_q} \right|_{v,Gauss} ,$$

with $\log^+ x = \log \sup(x, 1)$, *for all* $x \in \mathbb{R}$. *Then*

$$\limsup_{n\to\infty} \frac{h(n)}{n} = \log \frac{1}{\chi_v(\mathcal{M})} \ .$$

Moreover, $\chi_v(\mathcal{M})$ *is independent of the choice of the* $K_v(x)$*-basis* $\underline{e}$ *of* M.

Proof. We recall that $G_0(x) = \mathbb{I}_\mu$ and that therefore the two definition of $h(x)$ are equivalent.

Let $\underline{f} = \underline{e}F(x)$ be another $K_v(x)$-basis of M, with $F(x) \in Gl_\mu(K_v(x))$. For any integer $n \geq 0$, we set:

$$\begin{cases} \Delta_q^n(\underline{e}) = \underline{e}G_n(x), \quad h_{\underline{e}}(n) = \sup\limits_{s\leq n} \log \left| \dfrac{G_s(x)}{[s]!_q} \right|_{v,Gauss} ; \\ \Delta_q^n(\underline{f}) = \underline{f}H_n(x), \quad h_{\underline{f}}(n) = \sup\limits_{s\leq n} \log \left| \dfrac{H_s(x)}{[s]!_q} \right|_{v,Gauss} . \end{cases}$$

By (2.1.10.2) we have

$$\begin{aligned} \underline{f}\frac{H_n(x)}{[n]!_q} = \frac{\Delta_q^n}{[n]!_q}(\underline{f}) &= \frac{\Delta_q^n}{[n]!_q}(\underline{e}F(x)) \\ &= \underline{f}F(x)^{-1} \sum_{i=0}^{n} \frac{G_i(x)}{[i]!_q} \frac{d_q^{n-i}(F)}{[n-i]!_q}(q^i x) \ , \end{aligned}$$

and hence it follows

$$h_{\underline{f}}(n) \leq \log |F(x)^{-1}|_{v,Gauss} + \log |F(x)|_{v,Gauss} + h_{\underline{e}}(n) \ . \tag{4.2.3.1}$$

By symmetry, we deduce that

$$\limsup_{n\to\infty} \frac{h_{\underline{e}}(n)}{n} = \limsup_{n\to\infty} \frac{h_{\underline{f}}(n)}{n} \ .$$

Let $h(n) = h_{\underline{e}}(n)$. It is a general fact (*cf.* for instance the proof of [DGS, VII, Lemma 4.1]) that

$$\limsup_{n\to\infty} \frac{h(n)}{n} = \log \frac{1}{\chi_v(\mathcal{M})} \ .$$

■

Let a be an element of K_v such that $q^n a$ is not a pole of $G_1(x)$ for any $n \geq 1$. We want to relate $\chi_v(\mathcal{M})$ and the radius of convergence of the matrix $\sum_{n=1}^{\infty} \frac{G_n(a)}{[n]!_q}(x-a)_n$, solution of the linear q-difference system associated to $\mathcal{M}$, with respect to the basis $\underline{e}$. First of all, we notice that if $|a|_v \leq 1$ we have

$$\left| \frac{G_n(x)}{[n]!_q} \right|_{v,Gauss} \geq \left| \frac{G_n(a)}{[n]!_q} \right|_v \ ,$$

and therefore we obtain

$$\chi_v(\mathcal{M}) \leq \liminf_{n\to\infty} \left| \frac{G_n(a)}{[n]!_q} \right|_v^{-1/n} \ .$$

Hence, if zero is not a pole of $G_1(x)$, the matrix $\sum_{n=1}^{\infty} \frac{G_n(0)}{[n]!_q} x^n$ converges at least for $|x|_v < \chi_v(\mathcal{M})$. If $a \neq 0$ the situation is slightly more complicated:

Lemma 4.2.4. *Let $\sum_{n=0}^{\infty} a_n(x-a)_n \in K_v[\![x-a]\!]_q$ and let $\varrho \in (0,1]$ be a real number. Then if*

$$\sup(\varrho, |a|_v)^{1-\frac{1}{\kappa_v}} \sup(\varrho, |a|_v|(\kappa_v)_q|_v)^{\frac{1}{\kappa_v}} < \liminf_{n\to\infty} |a_n|_v^{-1/n}$$

(in particular, if $\sup(\varrho, |a|_v) < \liminf_{n\to\infty} |a_n|_v^{-1/n}$)

the series $\sum_{n=0}^{\infty} a_n(x-a)_n$ converges in the disk $\{x \in K_v : |x-a|_v < \varrho\}$.

Corollary 4.2.5. *Let $a \in \mathcal{V}_v$ such that $|a|_v \leq \chi_v(\mathcal{M})$, then $\sum_{n=1}^{\infty} \frac{G_n(a)}{[n]!_q}(x-a)_n$ converges in the open disk $\{x \in K_v : |x-a|_v < \chi_v(\mathcal{M})\}$.*

Example 4.2.6. Let us consider the analogue of the exponential series

$$\exp_q(x) = \sum_{n=0}^{\infty} \frac{x^n}{[n]!_q} .$$

Obviously $\exp_q(x)$ is the solution at zero of the q-difference equation $d_q y = y$, which is the system associated to the q-difference module $(K_v(x), \Delta_q)$, with $\Delta_q(f(x)) = d_q f(x) + f(qx)$ for all $f(x) \in K_v(x)$. Then $\chi_v(K_v(x), \Delta_q)$ coincides with the radius of convergence of $\exp_q(x)$, that is $|(\kappa_v)_q|_v^{1/\kappa_v} |p|_v^{1/\kappa_v(p-1)}$, by (4.1.1.1).

Proof of lemma 4.2.4. By the Maximum Modulus Principle [DGS, VI, 1.1] and (4.1.1.3) we have

$$\begin{aligned}
\sup_{|x-a|_v<\varrho} |(x-a)_n|_v &= \sup_{|x-a|_v<\varrho} \left|(x-a)\left(x-a+a(1-q)\right)\cdots\left(x-a+a\left(1-q^{n-1}\right)\right)\right|_v \\
&= \varrho \sup(\varrho, |a|_v)^{(n-1)-\left[\frac{n-1}{\kappa_v}\right]} \prod_{i=1}^{\left[\frac{n-1}{\kappa_v}\right]} \sup(\varrho, |ai|_v|(\kappa_v)_q|_v) \\
&\leq \varrho \sup(\varrho, |a|_v)^{(n-1)-\left[\frac{n-1}{\kappa_v}\right]} \sup(\varrho, |a|_v|(\kappa_v)_q)|_v)^{\left[\frac{n-1}{\kappa_v}\right]}
\end{aligned}$$

Finally, $\sum_{n=0}^{\infty} a_n(x-a)_n$ converges if

$$\sup(\varrho, |a|_v)^{1-\frac{1}{\kappa_v}} \sup(\varrho, |a|_v|(\kappa_v)_q|_v)^{\frac{1}{\kappa_v}} < \liminf_{n\to\infty} |a_n|_v^{-1/n} .$$

■

The following characterization of $\chi_v(\mathcal{M})$ is the q-analogue of a result by André (*cf.* [A, IV, §5]):

Proposition 4.2.7. *The sequence $\left(\frac{h(n)}{n}\right)_{n\in\mathbb{N}}$ defined in (4.2.3) is convergent:*

$$\lim_{n\to\infty} \frac{h(n)}{n} = \log \frac{1}{\chi_v(\mathcal{M})} . \tag{4.2.7.1}$$

Proof. By (4.2.3) it is enough to prove the existence of the limit. Let s, n be two positive integers; we have

$$\begin{aligned}\frac{\Delta_q^{s+n}}{[s+n]!_q}(\underline{e}) &= \frac{\Delta_q^n}{[s+n]!_q}\left(\Delta_q^s \underline{e}\right) = \frac{\Delta_q^n}{[s+n]!_q}\left(\underline{e} G_s(x)\right) \\ &= \underline{e}\frac{1}{[s+n]!_q}\sum_{i=0}^{n}\binom{n}{i}_q G_i(x) d_q^{n-i}(G_s)(q^i x) \\ &= \underline{e}\sum_{i+j=n}\frac{[n]!_q[s]!_q}{[s+n]!_q}\frac{G_i(x)}{[i]!_q}\frac{d_q^j}{[j]!_q}\left(\frac{G_s(q^i x)}{[s]!_q}\right)\end{aligned}$$

It follows that

$$\frac{G_{s+n}(x)}{[s+n]!_q} = \sum_{i+j=n}\frac{[n]!_q[s]!_q}{[s+n]!_q}\frac{G_i(x)}{[i]!_q}\frac{d_q^j}{[j]!_q}\left(\frac{G_s(q^i x)}{[s]!_q}\right)$$

and hence

$$\log\left|\frac{G_{s+n}(x)}{[s+n]!_q}\right|_{v,Gauss} \leq \log\left|\frac{G_s(x)}{[s]!_q}\right|_{v,Gauss} + h(n) - \log\left|\binom{n+s}{s}_q\right|_v .$$

For all $k \in \mathbb{N}$ and $n \geq s$, by induction we obtain

$$\begin{aligned}\log\left|\frac{G_{s+kn}(x)}{[s+kn]!_q}\right|_{v,Gauss} &\leq \log\left|\frac{G_{s+(k-1)n}(x)}{[s+(k-1)n]!_q}\right|_{v,Gauss} + h(n) - \log\left|\binom{s+kn}{s+(k-1)n}_q\right|_v \\ &\leq \log\left|\frac{G_s(x)}{[s]!_q}\right|_{v,Gauss} + kh(n) - \log\left|\prod_{i=1}^{k}\binom{s+in}{s+(i-1)n}_q\right|_v .\end{aligned}$$

Let $N \in \mathbb{N}$, $N \geq n$; then $N = \left[\frac{N}{n}\right] n + s$, with $0 \leq s < n$, and the previous inequality becomes

$$\log\left|\frac{G_N(x)}{[N]!_q}\right|_{v,Gauss} \leq \left(\left[\frac{N}{n}\right]+1\right)h(n) - \log\left|\prod_{i=1}^{\left[\frac{N}{n}\right]}\binom{s+in}{s+(i-1)n}_q\right|_v .$$

Since $\log\left|\prod_{i=1}^{\left[\frac{N}{n}\right]}\binom{s+in}{s+(i-1)n}_q\right|_v \leq 0$ is a decreasing function of N we obtain:

$$\begin{aligned}\frac{h(N)}{N} &\leq \left(\frac{1}{n}+\frac{1}{N}\right)h(n) - \log\left|\prod_{i=1}^{\left[\frac{N}{n}\right]}\binom{s+in}{s+(i-1)n}_q\right|_v \\ &\leq \left(\frac{1}{n}+\frac{1}{N}\right)h(n) - \log\left|\frac{[N]!_q}{([n]!_q)^{\left[\frac{N}{n}\right]}[s]!_q}\right|_v .\end{aligned}$$

Finally we deduce by (4.1.1.1) that

$$\limsup_{N\to\infty}\frac{h(N)}{N}\leq\limsup_{N\to\infty}\left(\left(\frac{1}{n}+\frac{1}{N}\right)h(n)-\log\left|\frac{[N]!_q}{([n]!_q)^{\left[\frac{N}{n}\right]}\,[s]!_q}\right|_v^{\frac{1}{N}}\right)$$
$$\leq\frac{h(n)}{n}-\log\left(\frac{|(\kappa_v)_q|_v^{1/\kappa_v}|p|_v^{1/\kappa_v(p-1)}}{|[n]!_q|_v^{1/n}}\right)$$

and therefore

$$\limsup_{N\to\infty}\frac{h(N)}{N}\leq\liminf_{n\to\infty}\frac{h(n)}{n}$$

From which it follows that the sequence $\left(\frac{h(n)}{n}\right)_{n\in\mathbb{N}}$ is convergent. ■

Now we prove a first estimate for $\chi_v(\mathcal{M})$. In the following sections we will prove more precise estimate linked to the notion of unipotent reduction.

Proposition 4.2.8. *We have:*

$$\chi_v(\mathcal{M})\geq\frac{|(\kappa_v)_q|_v^{1/\kappa_v}|p|_v^{1/\kappa_v(p-1)}}{\sup\left(|G(x)|_{v,Gauss},1\right)}\ .$$

Proof. By induction, we get

$$\left|\frac{G_n(x)}{[n]!_q}\right|_{v,Gauss}\leq\frac{\sup\left(|G(x)|_{v,Gauss},1\right)^n}{|[n]!_q|_v}$$

and the conclusion follows by lemma (4.1.1.1). ■

Remark 4.2.9. We notice that if $|q|_v>1$ then $|[n]!_q|_v=|q|_v^{\frac{n(n-1)}{2}}$ for all $n\geq 0$, and therefore

$$\chi_v(\mathcal{M})^{-1}=\limsup_{n\to\infty}\left|\frac{G_n(x)}{[n]!_q}\right|_{v,Gauss}^{1/n}=\limsup_{n\to\infty}\frac{|G_n(x)|_{v,Gauss}^{1/n}}{|q|_v^{\frac{n-1}{2}}}\ .$$

This limit can be zero as well as ∞ or a finite value. On the other hand, if $|q|_v<1$ then $|[n]!_q|=1$ for any $n\geq 0$, and therefore

$$\chi_v(\mathcal{M})^{-1}=\limsup_{n\to\infty}\left|\frac{G_n(x)}{[n]!_q}\right|_{v,Gauss}^{1/n}=\limsup_{n\to\infty}|G_n(x)|_{v,Gauss}^{1/n}\leq\sup\left(|G(x)|_{v,Gauss},1\right)\ .$$

Proposition 4.2.10. *If $|q|_v=1$ and $|1-q^{\kappa_v}|_v\geq|p|_v^{1/(p-1)}$ then*

$$\frac{\sup\left(|G(x)|_{v,Gauss},1\right)}{|p|_v^{1/\kappa_v(p-1)}|1-q^{e\kappa_v}|_v^{1/e\kappa_v}}\geq\chi_v(\mathcal{M})^{-1}\geq\frac{\sup\left(|G(x)|_{v,Gauss},1\right)}{|(\kappa_v)_q|_v^{1/\kappa_v}}\ .$$

Proof. Obviously we have: $|[n]!_q|_v \leq |(\kappa_v)_q|_v^{\left[\frac{n}{\kappa_v}\right]}$. Let

$$e = \inf\{m \in \mathbb{Z} : m > 0, |1 - q^{e\kappa_v}|_v < |p|_v^{1/(p-1)}\} \ .$$

For any positive integer n, there exist two positive integers $r, s < e$, such that $n = se + r$. We obtain

$$|1 - q^{n\kappa_v}|_v = |1 - q^{(se+r)\kappa_v}|_v = |1 - q^{se\kappa_v} + q^{se\kappa_v}(1 - q^{r\kappa_v})|_v \begin{cases} \geq |p|_v^{1/(p-1)} & \text{if } r \neq 0 \\ = |s|_v |1 - q^{e\kappa_v}|_v & \text{otherwise} \end{cases} ;$$

from which we infer that

$$\begin{aligned} |(\kappa_v)_q|_v^{1/\kappa_v} &\geq \limsup_{n\to\infty} |[n]!_q|_v^{1/n} \\ &\geq \liminf_{n\to\infty} |[n]!_q|_v^{1/n} \\ &\geq \liminf_{n\to\infty} \left(|p|_v^{\left(\left[\frac{n}{\kappa_v}\right] - \left[\frac{n}{e\kappa_v}\right]\right)\frac{1}{p-1}} |1 - q^{e\kappa_v}|_v^{\left[\frac{n}{e\kappa_v}\right]} \left| \left[\frac{n}{e\kappa_v}\right]! \right|_v \right)^{1/n} \\ &\geq |p|_v^{1/\kappa_v(p-1)} |1 - q^{e\kappa_v}|_v^{1/e\kappa_v} \ . \end{aligned}$$

Finally we have:

$$\frac{\sup\left(|G(x)|_{v,Gauss}, 1\right)}{|p|_v^{1/\kappa_v(p-1)} |1 - q^{e\kappa_v}|_v^{1/e\kappa_v}} \geq \chi_v(\mathcal{M})^{-1} \geq \frac{\sup\left(|G(x)|_{v,Gauss}, 1\right)}{|(\kappa_v)_q|_v^{1/\kappa_v}} \ .$$

■

4.3. q-analogue of the Dwork-Frobenius Theorem.

The next proposition is the q-analogue of the Dwork-Frobenius-Young Theorem [DGS, VI, 2.1], which establishes a relation between $\chi_v(\mathcal{M})$ and the coefficients of the q-difference matrix associated to $\mathcal{M} = (M, \Phi_q)$ with respect to a cyclic basis, when $\kappa_v = 1$:

Proposition 4.3.1. *We suppose that $\kappa_v = 1$. Let $\mathcal{M}$ be a q-difference module over $K_v(x)$ of rank μ, $m \in M$ a cyclic vector (cf. (2.3.1)) such that*

$$\Delta_q(m, \Delta_q(m), \ldots, \Delta_q^{\mu-1}(m)) = (m, \Delta_q(m), \ldots, \Delta_q^{\mu-1}(m)) \left(\begin{array}{ccc|c} 0 & \ldots & 0 & a_0(x) \\ \hline & & & a_1(x) \\ & \mathbb{I}_{\mu-1} & & \vdots \\ & & & a_{\mu-1}(x) \end{array} \right) .$$

If $\sup_{i=0,\ldots,\mu-1} |a_i(x)|_{v,Gauss} > 1$ then

$$\chi_v(\mathcal{M}) = \frac{|p|_v^{1/(p-1)}}{\sup_{i=0,\ldots,\mu-1} |a_i(x)|_{v,Gauss}^{1/(\mu-i)}} \ .$$

It follows immediately by (4.2.8) that:

Corollary 4.3.2. $\chi_v(\mathcal{M}) \geq |p|_v^{1/(p-1)}$ *if and only if* $\sup_{i=0,\dots,\mu-1} |a_i(x)|_{v,Gauss} \leq 1$.

Proof of proposition 4.3.1. We recall that $\chi_v(\mathcal{M})$ is independent of the choice of the basis of M over $K_v(x)$.

Let $\gamma \in K_v$ such that $|\gamma|_v = \sup_{i=0,\dots,\mu-1} |a_i(x)|_{v,Gauss}^{1/(\mu-i)}$, $\underline{e} = (m, \Delta_q(m), \dots, \Delta_q^{\mu-1}(m))$ and

$$H = \begin{pmatrix} \gamma^{\mu-1} & & & 0 \\ & \gamma^{\mu-2} & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix} .$$

We set $\underline{f} = \underline{e}H$. By a direct calculation we obtain

$$\Delta_q(\underline{f}) = H^{-1}\Delta_q(\underline{e})H = \underline{f}\gamma W(x) \text{ , with } W(x) = \left(\begin{array}{ccc|c} 0 & \dots & 0 & a_0(x)/\gamma^{\mu} \\ \hline & & & a_1(x)/\gamma^{\mu-1} \\ & \mathbb{I}_{\mu-1} & & \vdots \\ & & & a_{\mu-1}(x)/\gamma \end{array}\right) .$$

We set $\Delta_q^n(\underline{f}) = \underline{f}H_n(x)$, with $H_1(x) = \gamma W(x)$. We want to prove by induction on n that $H_n(x) \equiv \gamma^n W(x)\cdots W(q^{n-1}x) \bmod \gamma^{n-1}$. We remark that $H_n(x) \equiv \gamma^n W(x)\cdots W(q^{n-1}x) \bmod \gamma^{n-1}$ implies that $|H_n(x)|_{v,Gauss} \leq |\gamma|_v^n$, therefore $|d_q H_n(x)|_{v,Gauss} \leq |\gamma|_v^n$ (*cf.* (4.2.1)). Then we have

$$\begin{aligned} H_{n+1}(x) &= H_1(x)H_n(qx) + d_q H_n(x) \\ &\equiv \gamma^{n+1} W(x)\cdots W(q^n x) \bmod \gamma^n. \end{aligned}$$

We deduce that $|H_n(x)|_{v,Gauss} \leq |\gamma|_v^n$, for all $n \geq 1$, and hence that

$$\chi_v(\mathcal{M}) \geq \frac{|p|_v^{1/(p-1)}}{\sup_{i=0,\dots,\mu-1} |a_i(x)|_{v,Gauss}^{1/(\mu-i)}} .$$

Let us prove the opposite inequality. By induction on μ one prove that the characteristic polynomial of $W(x)$ is

$$X^{\mu} - \frac{a_{\mu-1}(x)}{\gamma}X^{\mu-1} - \frac{a_{\mu-2}(x)}{\gamma^2}X^{\mu-2} - \dots - \frac{a_0(x)}{\gamma^{\mu}} . \tag{4.3.2.1}$$

By our choice of γ the reduction modulo ϖ of (4.3.2.1) has a non zero root, hence $W(x)$ has an eigenvalue of norm 1. Then there exist

- an extension L of $K_v(x)$ equipped with an extension of $|\ |_{v,Gauss}$, still denoted by $|\ |_{v,Gauss}$,
- $\Lambda \in L$, such that $|\Lambda|_{v,Gauss} = 1$,
- $\vec{V} \in L^{\mu}$, such that $|\vec{V}|_{v,Gauss} = 1$,

satisfying the relation

$W(x)\cdots W(q^{n-1}x)\overrightarrow{V} \equiv W(x)^n\overrightarrow{V} \equiv \Lambda^n\overrightarrow{V}$ in the residue field of L with respect to $|\ |_{v,Gauss}$.

We deduce that

$$\gamma^{-n}H_n(x)\overrightarrow{V} \equiv \Lambda^n\overrightarrow{V} \text{ in the residue field of } L \text{ with respect to } |\ |_{v,Gauss}.$$

Finally we obtain

$$\left|\gamma^{-n}\frac{H_n(x)}{[n]!_q}\right|_{v,Gauss} \geq \left|\frac{\gamma^{-n}}{[n]!_q}H_n(x)\overrightarrow{V}\right|_{v,Gauss} = \left|\frac{\Lambda^n\overrightarrow{V}}{[n]!_q}\right|_{v,Gauss} = \left|\frac{1}{[n]!_q}\right|_v$$

and hence

$$\begin{aligned}\chi_v(\mathcal{M})^{-1} &= \sup\left(1, \limsup_{n\to\infty}\left|\frac{H_n(x)}{[n]!_q}\right|^{1/n}_{v,Gauss}\right)\\ &\geq \limsup_{n\to\infty}\left|\frac{\gamma^n}{[n]!_q}\right|^{1/n}_v\\ &= \frac{\sup_{i=0,\dots,\mu-1}|a_i(x)|^{1/(\mu-i)}_{v,Gauss}}{|p|_v^{1/(p-1)}}\ .\end{aligned}$$

■

In the previous proposition we have supposed that $\kappa_v = 1$. If $\kappa_v > 1$ we have:

Proposition 4.3.3. *The q-difference module (M, Φ_q) equipped with the operator $\Phi_q^{\kappa_v}$ (and consequently with $\Delta_{q^{\kappa_v}} = (\Phi_q^{\kappa_v} - \mathbb{I}_\mu)/(q^{\kappa_v}-1)x$) is a q^{κ_v}-difference module and*

$$\chi_v(M, \Phi_q) \leq \chi_v(M, \Phi_q^{\kappa_v})^{1/\kappa_v}\ .$$

Proof. Applying successively (2.1.11.1) and (2.1.11.2), we obtain

(4.3.3.1)

$$\Delta^n_{q^{\kappa_v}} = \frac{(-1)^n}{(q^{\kappa_v}-1)^n x^n}\sum_{\substack{i=0,\dots,n\\ j=0,\dots,i\kappa_v}}\left((-1)^i\binom{n}{i}_{q^{-\kappa_v}} q^{-\kappa_v\frac{i(i-1)}{2}}\binom{i\kappa_v}{j}_q (q-1)^j q^{\frac{j(j-1)}{2}}x^j\right)\Delta_q^j\ .$$

Let $\underline{f}$ be a basis of M over $K_v(x)$ such that $\Delta^n_{q^{\kappa_v}}\underline{f} = \underline{f}H_n(x)$ and $\Delta^n_q\underline{f} = \underline{f}G_n(x)$. We deduce by (4.3.3.1) that

$$|H_n(x)|_{v,Gauss} \leq \frac{1}{|q^{\kappa_v}-1|_v^n}\left(\sup_{s\leq n\kappa_v}|G_s(x)|_{v,Gauss}\right)\ .$$

Recalling the estimations in (4.1.1) and same general property of lim sup (*cf.* [AB, II, 1.8]) we obtain

$$\begin{aligned}\frac{1}{\chi_v(M,\Phi_{q^{\kappa_v}})} &= \limsup_{n\to\infty}\left|\frac{H_n(x)}{n_{q^{\kappa_v}}!}\right|^{1/n}_{v,Gauss}\\ &\leq \frac{\limsup_{n\to\infty}\left(\sup_{s\leq n\kappa_v}|G_s(x)|_{v,Gauss}\right)^{1/n}}{|q^{\kappa_v}-1|_v|p|_v^{1/(p-1)}}\\ &= \frac{1}{\chi_v(M,\Phi_q)^{\kappa_v}}\end{aligned}$$

■

5. *p*-adic criteria of unipotent reduction.

We recall that K_v is a field complete with respect to the norm $|\ |_v$ and that $\mathcal{V}_v$ is its ring of integers, ϖ_v its uniformizer and k_v the residue field.

Let q be an element of K_v such that $|q|_v = 1$, q is not a root of unity and that the order κ_v of its image in the multiplicative group $k_v^\times$ is finite.

Let $\mathcal{F} \subset K_v(x)$ be a q-difference algebra essentially of finite type over $\mathcal{V}_v$ (*cf.* (2.1.2)). Let $\mathfrak{a}$ be an ideal of $\mathcal{V}_v$ and $\overline{q}$ the image of q in $\mathcal{V}_v/\mathfrak{a}$. The algebra $\mathcal{F} \otimes_{\mathcal{V}_v} \mathcal{V}_v/\mathfrak{a}$ has a natural structure of $\overline{q}$-difference algebra. Let $\mathcal{M} = (M, \Phi_q)$ be a q-difference module over $\mathcal{F}$. We consider the free $\mathcal{F} \otimes_{\mathcal{V}_v} \mathcal{V}_v/\mathfrak{a}$-module $M \otimes_{\mathcal{V}_v} \mathcal{V}_v/\mathfrak{a}$ equipped with the morphism $\Phi_{\overline{q}}$ induced by Φ_q: it is a $\overline{q}$-difference module over $\mathcal{F} \otimes_{\mathcal{V}_v} \mathcal{V}_v/\mathfrak{a}$, which satisfies the assumptions of §3.

We are especially interested in the following two cases:

- $\mathfrak{a}$ is the maximal ideal of $\mathcal{V}_v$, generated by ϖ_v. We will refer to $(M \otimes_{\mathcal{V}_v} \mathcal{V}_v/\varpi_v\mathcal{V}_v, \Phi_{\overline{q}})$ as the *reduction of $\mathcal{M}$ modulo ϖ_v or over k.*

- $\mathfrak{a}$ is the ideal of $\mathcal{V}_v$ generated by $1 - q^{\kappa_v}$. We will refer to $(M \otimes_{\mathcal{V}_v} \mathcal{V}_v/(1-q^{\kappa_v})\mathcal{V}_v, \Phi_{\overline{q}})$ as the *reduction modulo* $1 - q^{\kappa_v}$.

Remark 5.0.4. We notice that $|p!|_v = |p|_v$, therefore both reductions are q-analogues of the reduction modulo p in the differential case (*cf.* §1) and both of them are interesting. In (§6) we analyses the reduction modulo ϖ_v, while in our main theorem (7.1.1) we consider the reduction modulo $1 - q^{\kappa_v}$.

Motivated by §3, we are particularly interested in q-difference modules $\mathcal{M}$ over $\mathcal{F}$ such that the reduction modulo ϖ_v (resp. $1 - q^{\kappa_v}$) of the operator $\Phi_q^{\kappa_v}$ is unipotent. We will briefly say that $\mathcal{M}$ has *unipotent reduction of order n modulo ϖ_v (resp. $1 - q^{\kappa_v}$)* if the reduction of $\Phi_q^{\kappa_v}$ modulo ϖ_v (resp. $1 - q^{\kappa_v}$) is an unipotent morphism of order n.

The following example shows that $\mathcal{M}$ can have unipotent reduction modulo ϖ_v without having unipotent reduction modulo $1 - q^{\kappa_v}$:

Example. Let us consider the q-difference module over $\mathbb{Q}_p(x)$ associated to the q-difference system

$$\begin{pmatrix} y_1(qx) \\ y_2(qx) \end{pmatrix} = \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix} \begin{pmatrix} y_1(x) \\ y_2(x) \end{pmatrix} . \tag{5.0.4.1}$$

Then

$$\begin{pmatrix} y_1(q^{\kappa_p}x) \\ y_2(q^{\kappa_p}x) \end{pmatrix} = \begin{pmatrix} 1 & \kappa_p p \\ 0 & 1 \end{pmatrix} \begin{pmatrix} y_1(x) \\ y_2(x) \end{pmatrix} ,$$

from which it follows

$$\left| \begin{pmatrix} 1 & \kappa_p p \\ 0 & 1 \end{pmatrix} - \mathbb{I}_2 \right|_p = |\kappa_p p|_p = |p|_p .$$

If we choose $q = 8$ and $p = 3$ then $\kappa_p = 2$ and $|1 - q^{\kappa_p}|_p = |1 - 8^2|_p = |3^2|_p < |3|_p$, and therefore $\begin{pmatrix} 1 & \kappa_p p \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 6 \\ 0 & 1 \end{pmatrix} \equiv \mathbb{I}_2 \bmod 3$, but $\begin{pmatrix} 1 & 6 \\ 0 & 1 \end{pmatrix} \not\equiv \mathbb{I}_2 \bmod 3^2$. Then by (3.1.2) the q-difference module associated to (5.0.4.1) has trivial reduction modulo $\varpi = 3$, but not modulo $1 - q^{\kappa_p} = (-7)3^2$.

We want to relate the property of having unipotent reduction modulo ϖ_v (resp. $1 - q^{\kappa_v}$) to an estimate of the invariant $\chi_v(\mathcal{M}) = \chi_v(\mathcal{M}_{K_v(x)})$.

5.1. q-difference modules having unipotent reduction modulo ϖ_v.

First we consider q-difference modules having unipotent reduction modulo ϖ. The following proposition is a q-analogue of a classical estimate for p-adic differential modules [DGS, page 96]:

Proposition 5.1.1. *If $\mathcal{M}$ has unipotent reduction modulo ϖ of order n then*

$$\chi_v(\mathcal{M}) \geq |\varpi|_v^{-1/\kappa_v n} |(\kappa_v)_q|_v^{1/\kappa_v} |p|_v^{1/\kappa_v(p-1)} \ . \tag{5.1.1.1}$$

The proof of (5.1.1) relies on the following lemma:

Lemma 5.1.2. *Let us assume that that $\mathcal{M}$ has unipotent reduction of order n modulo ϖ. Let $\underline{e}$ be a basis of M over $\mathcal{F}$ and let $\Delta_q^m \underline{e} = \underline{e} G_m(x)$, for any $m \geq 1$, with $G_n(x) \in M_{\mu\times\mu}(K_v(x))$. Then*

$$|G_{sn\kappa_v}(x)|_{v,Gauss} \leq |\varpi|_v^s \ ,$$

for every integer $s \geq 1$.

Proof. By (2.1.10.2), for all $s \in \mathbb{N}$, $s > 1$ we have

$$\begin{aligned} \Delta_q^{(s+1)n\kappa_v}(\underline{e}) &= \underline{e} G_{(s+1)n\kappa_v}(x) \\ &= \Delta_q^{n\kappa_v}(\underline{e} G_{sn\kappa_v}(x)) \\ &= \sum_{i=0}^{n\kappa_v} \binom{n\kappa_v}{i}_q \Delta_q^{n\kappa_v - i}(\underline{e}) d_q^i (G_{sn\kappa_v})(q^{n\kappa_v - i} x) \\ &= \underline{e} \sum_{i=0}^{n\kappa_v} \binom{n\kappa_v}{i}_q G_{n\kappa_v - i}(x) d_q^{n\kappa_v - i}(G_{sn\kappa_v})(q^{n\kappa_v - i} x) \ , \end{aligned}$$

and hence

$$G_{(s+1)n\kappa_v}(x) = \sum_{i=0}^{n\kappa_v} \binom{n\kappa_v}{i}_q G_{n\kappa_v - i}(x) d_q^i (G_{sn\kappa_v})(q^{n\kappa_v - i} x) \tag{5.1.2.1}$$

By (3.1.3), the definition of unipotent reduction modulo ϖ is equivalent to the condition

$$|G_{n\kappa_v}(x)|_{v,Gauss} \leq |\varpi|_v \ .$$

We shall prove the statement by induction, using (5.1.2.1). We suppose that

$$|G_{sn\kappa_v}(x)|_{v,Gauss} \leq |\varpi|_v^s \ .$$

Then all the terms occurring in the sum (5.1.2.1) are bounded by $|\varpi|_v^{s+1}$, in fact:
1) If $(\kappa_v, i) = 1$, then

$$\left| \binom{n\kappa_v}{i}_q \right|_v = \left| \frac{(n\kappa_v)_q}{(i)_q} \binom{n\kappa_v - 1}{i-1}_q \right|_v \leq |(\kappa_v)_q|_v \leq |\varpi|_v$$

and the absolute value of the corresponding term in sum (5.1.2.1) is bounded by $|\varpi|_v^{s+1}$.
2) For all $i = 1, \ldots, n$, we have $|d_q^{i\kappa_v} f(x)|_{v,Gauss} \leq |(\kappa_v)_q|_v |f(x)|_{v,Gauss}$ and therefore

$$\left| \binom{n\kappa_v}{i\kappa_v}_q G_{n\kappa_v - i\kappa_v}(x) d_q^{i\kappa_v} \left(G_{sn\kappa_v}\right)(q^{n\kappa_v - i\kappa_v} x) \right|_{v,Gauss} \leq |(\kappa_v)_q|_v |\varpi|_v^s \leq |\varpi|_v^{s+1} \ ,$$

for all $i = 1, \ldots, n$.
3) The term of (5.1.2.1) corresponding to $i = 0$ is $G_{n\kappa_v}(x) G_{sn\kappa_v}(q^{n\kappa_v} x)$, and therefore it is bounded by $|\varpi|_v^{s+1}$, by induction. Thus we have proved that $|G_{(s+1)n\kappa_v}(x)|_{v,Gauss} \leq |\varpi|_v^{s+1}$.
■

Proof of proposition 5.1.1. By the recursive formula (4.2.1.2) we have

$$|G_m(x)|_{v,Gauss} \leq \left| G_{[\frac{m}{n\kappa_v}]n\kappa_v}(x) \right|_{v,Gauss} \ .$$

The estimate (5.1.1.1) follows from previous lemma, since

$$\begin{aligned} \chi_v(\mathcal{M}) &\geq \inf \left(1, \liminf_{m\to\infty} \frac{|G_{[\frac{m}{n\kappa_v}]n\kappa_v}(x)|_{v,Gauss}^{-1/m}}{|[m]!_q|_v^{-1/m}} \right) \\ &\geq \liminf_{m\to\infty} |\varpi|_v^{-\left[\frac{m}{n\kappa_v}\right]\frac{1}{m}} |m_q!|_v^{1/m} \\ &= |\varpi|_v^{-1/n\kappa_v} |(\kappa_v)_q|_v^{1/\kappa_v} |p|_v^{1/\kappa_v(p-1)} \ . \end{aligned}$$

■

Corollary 5.1.3. *The q-difference module $\mathcal{M}$ has unipotent reduction modulo ϖ if and only if*

$$\chi_v(\mathcal{M}) > |(\kappa_v)_q|_v^{1/\kappa_v} |p|_v^{1/\kappa_v(p-1)} \ .$$

Proof. If $\mathcal{M}$ has unipotent reduction modulo ϖ, we immediately deduce by (5.1.1) that $\chi_v(\mathcal{M}) > |(\kappa_v)_q|_v^{1/\kappa_v} |p|_v^{1/\kappa_v(p-1)}$.

On the other hand, by hypothesis we have

$$\begin{aligned}|(\kappa_v)_q|_v^{1/\kappa_v}|p|_v^{1/\kappa_v(p-1)} &< \chi_v(\mathcal{M}) \\ &= \inf\left(1, \liminf_{n\to\infty}\left|\frac{G_n(x)}{[n]!_q}\right|_{v,Gauss}^{-1/n}\right) \\ &= \inf\left(1, |(\kappa_v)_q|_v^{1/\kappa_v}|p|_v^{1/\kappa_v(p-1)}\liminf_{n\to\infty}|G_n(x)|_{v,Gauss}^{-1/n}\right) .\end{aligned}$$

We deduce that

$$\limsup_{n\to\infty}|G_n(x)|_{v,Gauss}^{1/n} < 1 .$$

We conclude that there exists $N \in \mathbb{N}$ such that $|G_n(x)|_{v,Gauss} < 1$ for all $n > N$, which implies that $\mathcal{M}$ has unipotent reduction modulo ϖ. ■

5.2. q-difference modules having unipotent reduction modulo $1 - q^{\kappa_v}$.

Under the hypothesis of unipotent reduction modulo $1-q^{\kappa_v}$, we obtain a slight but crucial improvement of (5.1.1), that will be fundamental in the proof of the main result (7.1.1) below:

Proposition 5.2.1. *Let $\mathcal{M}$ be a q-difference module over $K_v(x)$, with unipotent reduction modulo $1 - q^{\kappa_v}$ of order n. Then*

$$\chi_v(\mathcal{M}) \geq |(\kappa_v)_q|_v^{(n-1)/n\kappa_v}|p|_v^{1/\kappa_v(p-1)} .$$

Proof. Let $\underline{e}$ be the basis of M such that $\Delta_q^m\underline{e} = \underline{e}G_m(x)$, for all $m \geq 1$. Then

$$|G_{n\kappa_v}(x)|_{v,Gauss} \leq |(\kappa_v)_q|_v .$$

The estimates in (5.1.2) show that

$$|G_{sn\kappa_v}(x)|_{v,Gauss} \leq |(\kappa_v)_q|_v^s , \ \forall\ s \geq 1, \tag{5.2.1.1}$$

therefore we conclude that

$$\chi_v(\mathcal{M}) \geq |(\kappa_v)_q|_v^{(n-1)/n\kappa_v}|p|_v^{1/\kappa_v(p-1)} .$$

■

Corollary 5.2.2. *The following assertions are equivalent:*
1) $\chi_v(\mathcal{M}) \geq |p|_v^{1/\kappa_v(p-1)}$.
2) $\Phi_q^{\kappa_v}$ induces the identity on the reduction of $\mathcal{M}$ modulo $1 - q^{\kappa_v}$.

Proof. The implication "*2)⇒1)*" is a consequence of the previous proposition.

We prove "*1)⇒2)*". The $\mathcal{F}$-module M equipped with the operators $\Phi_q^{\kappa_v}$ is a q^{κ_v}-difference module. It follows by (4.3.3) that $\chi_v(M, \Phi_q^{\kappa_v}) \geq |p|_v^{1/(p-1)}$. We know by (2.3.1) that $(M, \Phi_q^{\kappa_v})$

admits a cyclic basis $\underline{e}$ over $\mathcal{F}$. Let $\Phi_q^{\kappa_v}\underline{e} = \underline{e}A_{\kappa_v}(x)$. We deduce by (4.3.1) that $|A_{\kappa_v}(x) - \mathbb{I}_\mu|_{v,Gauss} \leq |1-q^{\kappa_v}|_v$. ■

6. Arithmetic q-difference modules and regularity.

We fix some notation that will be maintained until the end of the paper:
$K=$ a number field.
$\mathcal{V}_K=$ the ring of integers of K.
$|\ |_v=$ a v-adic absolute value of K. In the non-archimedean case we normalize $|\ |_v$ as follow:

$$|p|_v = p^{-[K_v:\mathbb{Q}_p]/[K:\mathbb{Q}]},$$

where K_v is the v-adic completion of K and $v|p$. Similarly, in the archimedean case we normalize $|\ |_v$ setting

$$|x|_v = \begin{cases} |x|_{\mathbb{R}}^{1/[K:\mathbb{Q}]} & \text{if } K_v = \mathbb{R} \\ |x|_{\mathbb{C}}^{2/[K:\mathbb{Q}]} & \text{if } K_v = \mathbb{C} \end{cases},$$

where $|\ |_{\mathbb{R}}$ and $|\ |_{\mathbb{C}}$ are the usual absolute values of $\mathbb{R}$ and and of $\mathbb{C}$ respectively.
$\Sigma_f=$ the set of finite places v of K.
$\varpi_v=$ uniformizer $\in \mathcal{V}_k$ associated to the finite place v.
$k_v=$ residue field of K with respect to a finite place v.
$\Sigma_\infty=$the set of archimedean places of K.

6.1. On cyclic subgroups of $\overline{\mathbb{Q}}^\times$ and their reduction modulo almost every prime.

We fix an element q of K which is not zero and not a root of unity. For each $v \in \Sigma_f$ such that $|q|_v = 1$, we define κ_v to be the multiplicative order of the image of q in the residue field of K with respect to v. We notice that for any integer $n \geq 1$ the set of places $v \in \Sigma_f$, for which $\kappa_v = n$, is finite.

We recall that the *Dirichlet density $d(S)$ of a set S* of finite places of a number field K(*cf.* for instance [N, VII, §13]) is defined by

$$d(S) = \limsup_{s \to 1^+} \frac{\sum_{v \in S} p^{-sf_v}}{\sum_{v \in \Sigma_f} p^{-sf_v}},$$

where $f_v = [k_v : \mathbb{F}_p]$, if $v|p$.

The proposition below is a particular case of a theorem by Schinzel [Sc, Th. 2]. We prefer to give here a direct proof.

Proposition 6.1.1. *Let $S \subset \Sigma_f$ a set of finite places of K of Dirichlet density 1 and let a, b be two elements of $K^\times = K \smallsetminus \{0\}$ such that for all $v \in S$, the reduction of b modulo ϖ_v belongs to the cyclic group generated by the reduction of a modulo ϖ_v. Then $b \in a^{\mathbb{Z}}$.*

Corollary 6.1.2. *Let a, b be two elements of K, which are not roots of unity, such that for almost all $v \in \Sigma_f$ the order of a modulo ϖ_v and the order of b modulo ϖ_v coincide. Then either $a = b$ or $a = b^{-1}$.*

Remark 6.1.3. This shows that $\{q, q^{-1}\}$ is uniquely determined by the family of integers $(\kappa_v)_v$.

Proof of corollary 6.1.2. We recall that $k_v^\times$ is a cyclic group and that, therefore, its subgroups are determined by their order. By the previous proposition, we know that $b = a^n$ and $a = b^m$ for some integers n and m. We deduce that $a^{nm} = a$. Since a is not a root of unity, we have $mn = 1$ and hence either $m = n = 1$ or $m = n = -1$. ■

Proof of proposition 6.1.1 (following an argument of P. Colmez). We fix a rational prime ℓ. Let ζ_ℓ a ℓ-th root of unity. We consider the following Galois extensions of K: $K_1 = K(a^{1/\ell}, \zeta_\ell)$, $K_2 = K(b^{1/\ell}, \zeta_\ell)$ and $K_{12} = K(a^{1/\ell}, b^{1/\ell}, \zeta_\ell)$. We will prove that $K_1 = K_{12}$, and hence that $K_2 \subset K_1$, by applying the following corollary of the Čebotarev Density Theorem:

> **[N, VII, (13.6)]** *Let $\widetilde{K}$ be a Galois extension of the number field K and let $P(\widetilde{K}/K)$ be the set of primes of K that split totally in $\widetilde{K}$. Then the Dirichlet density of $P(\widetilde{K}/K)$ is*
>
> $$d(P(\widetilde{K}/K)) = \frac{1}{[\widetilde{K} : K]} .$$

Let $v \in \Sigma_f$ be a prime of K and let $\{w_1, \ldots, w_r\} \subset \Sigma_f$ be the set of all primes w of K_1 such that $w|v$. Let e_i be the ramification index of $w_i|v$ and f_i be the residue degree. Since K_1/K is a Galois extension we have: $e = e_1 = \ldots = e_r$ and $f = f_1 = \ldots = f_r$ (*cf.* [N, IV, page 55]). Therefore, $e = f = 1$ if and only if we have $[K_1 : K] = \sum_{i=1}^r e_i f_i = r$: so v split totally in K_1 if and only if $e = f = 1$. Then $P(K_1/K)$ is the set of all primes $v \in \Sigma_f$ of K such that:

- $v|p$ and $p \equiv 1 \bmod \ell$;
- there exists $a' \in k_v$ such that $a'^\ell \equiv a$ in k_v;
- v is not ramified in K_1.

For the same reason, $P(K_{12}/K)$ is the set of all the primes $v \in \Sigma_f$ such that:

- $v|p$ and $p \equiv 1 \bmod \ell$;
- there exists $a' \in k_v$ such that $a'^\ell \equiv a$ in k_v;
- there exists $b' \in k_v$ such that $b'^\ell \equiv b$ in k_v;
- v is not ramified in K_{12}.

Let $v \in P(K_1/K) \cap S$ and let $a' \in k_v$ be such that $a \equiv a'^{\ell}$ in k_v. By hypothesis there exists a positive integer $n(v)$ such that $b \equiv a^{n(v)}$ in k_v and hence $b \equiv (a'^{n(v)})^{\ell}$. If v is not ramified in K_{12} then $v \in P(K_{12}/K)$. Since S has density 1 and there are only a finitely many $v \in \Sigma_f$ which ramify in K_{12} we have

$$d(P(K_{12}/K)) = \frac{1}{[K_{12} : K]} \geq d(P(K_1/K)) = \frac{1}{[K_1 : K]} \ .$$

We conclude that $K_{12} = K_1$ and therefore $K_2 \subset K_1$.

We recall the following fact from Kummer theory:

[**N, VII, (3.6)**] *Let n be a positive integer which is relatively prime to the characteristic of the field K, and assume that K contains the group of n-th roots of unity. Then the abelian extensions $\widetilde{K}/K$ of exponents n are in one-to-one correspondence with the subgroups $\Gamma \subset K^{\times} = K \smallsetminus \{0\}$, which contain $K^{\times n}$, via the rule $\Gamma \longmapsto \widetilde{K} = K(\sqrt[n]{\Gamma})$.*

This statement applied to $K_2 \subset K_1 = K_{12}$ and $n = \ell$, says that

$$b^{\mathbb{Z}} K^{\times \ell} \subset a^{\mathbb{Z}} K^{\times \ell} \Rightarrow b \in a^{\mathbb{Z}} K^{\times \ell} \ .$$

Since ℓ was arbitrary, we conclude that $b \in a^{\mathbb{Z}}$. ■

6.2. Unipotent reduction and regularity.

Let $\mathcal{M} = (M, \Phi_q)$ be a q-difference module over a q-difference algebra $\mathcal{F} \subset K(x)$ essentially of finite type over $\mathcal{V}_K$ (*cf.* (2.1.2)).

Definition 6.2.1. *The q-difference module $\mathcal{M}$ over $\mathcal{F}$ is regular singular if both $\mathcal{M}_{K((x))}$ and $\mathcal{M}_{K((1/x))}$ are regular singular singular q-difference modules.*

Let Σ_{nilp} be the set of finite place v of K such that the $\mathcal{M}$ has unipotent reduction modulo ϖ_v.

The following result is a q-analogue of a well known result due to Katz (*cf.* [K1, 13.0]).

Theorem 6.2.2.
1) If Σ_{nilp} is infinite, then $\mathcal{M}$ is regular singular.
2) If moreover Σ_{nilp} has Dirichlet density 1, the exponents of $K((x)) \otimes_{\mathcal{F}} M$ with respect to same basis $\underline{e}$ (and hence to any basis) over $K((x))$ coincide with $q^{\mathbb{Z}}$.

Proof.
1) It is enough to prove the statement at zero. Let $\underline{e}$ be a basis of M over $\mathcal{F}$, such that $\Phi_q \underline{e} = \underline{e} A(x)$, with $A(x) \in Gl_{\mu}(\mathcal{F})$. Then $A(x)$ can be regarded as an element of $Gl_{\mu}(K((x)))$:

$$A(x) = \frac{1}{x^l} \sum_{i \geq 0} A_i x^i \in \frac{1}{x^l} Gl_{\mu}(K[\![x]\!]) \ ,$$

for some $l \in \mathbb{Z}$ and $l \geq 0$. For all positive integers m, we have

$$\Phi_q^m(\underline{e}) = \underline{e}A(x)A(qx)\cdots A(q^{m-1}x) = \underline{e}\left(\frac{A_0^m}{q^{\frac{lm(m-1)}{2}}x^{ml}} + h.o.t.\right)$$

For any $v \in \Sigma_{nilp}$, there exist a positive integer $n(v) \geq 1$ such that we have

$$\big(A(x)A(qx)\cdots A(q^{\kappa_v-1}x) - 1\big)^{n(v)} \equiv 0 \bmod \varpi_v;$$

we deduce that $A_0^{\kappa_v} \equiv 0$ modulo ϖ_v and hence that A_0 is a nilpotent matrix.

We suppose that zero is not a regular singularity. By (2.4.4), there exists an extension $L((t))$ of $K((x))$, with $t^d = x$, such that we can find a basis $\underline{f}$ of $L((t)) \otimes_{\mathcal{F}} M$ over $L((t))$ with the following properties:

$$\Phi_{\widetilde{q}}(\underline{f}) = \underline{f}B(t)$$

and

$$B(t) = \frac{B_k}{t^k} + \frac{B_{k-1}}{t^{k-1}} + \cdots + \frac{B_1}{t^1} + \widetilde{B}_0(t)\ ,$$

with $\widetilde{B}_0(t) \in M_{\mu\times\mu}(L[\![t]\!])$, $k \geq 1$ and $B_k \in Gl_\mu(L)$ *non* nilpotent and in Jordan normal form. Let $F(t) = \frac{F}{t^m} + h.o.t \in Gl_\mu(L((t)))$ such that $\underline{e} = \underline{f}F(t)$. This implies that $A(x) = F(t)^{-1}B(t)F(\widetilde{q}t)$. We get a contradiction since the matrix $F \in Gl_\mu(L)$ verifies $A_0 = F^{-1}B_kF$. *2)* We know by *1)* that $\mathcal{M}$ has a regular singularity at zero. Then there exists a $K((x))$-basis $\underline{e}$ of $K((x)) \otimes_{\mathcal{F}} M$ such that $\Phi_q(\underline{e}) = \underline{e}A$, with $A \in Gl_\mu(K)$ in Jordan normal form. By the remark (2.4.2), we can chose $\underline{e}$ such that for all $v \in \Sigma_{nilp}$ there exists $n(v) \geq 1$ satisfying the equivalence

$$(A^{\kappa_v} - 1)^{n(v)} \equiv 0 \bmod \varpi_v.$$

Therefore the matrix A^{κ_v} is unipotent modulo ϖ_v for all $v \in \Sigma_{nilp}$. We deduce that the reduction modulo ϖ_v of the eigenvalues of A are κ_v-th roots of unity for all $v \in \Sigma_{nilp}$. This means that the reduction modulo ϖ_v of the eigenvalues of A is an element of the cyclic group generated by the reduction of q, for all $v \in \Sigma_{nilp}$. The conclusion follows by applying lemma (6.1.1). ■

Proposition 6.2.3. *Let us assume that the q-difference module $\mathcal{M}$ over $\mathcal{F}$ has the property that for almost all finite places v of K the morphism $\Phi_q^{\kappa_v}$ induces the identity on the reduction of $\mathcal{M}$ modulo ϖ_v. Then $\mathcal{M}$ becomes trivial over $K((x))$.*

Remark. The q-difference module $\mathcal{M}$ becomes trivial over $K((x))$ if and only if there exists a basis $\underline{e}$ of $\mathcal{M}_{K(x)}$ over $K(x)$ such that the associated q-difference system has a fundamental matrix of solutions with coefficients in $K[\![x]\!]$ and the matrix $G(x)$ defined by $\Delta_q(\underline{e}) = \underline{e}G(x)$ has no pole at zero

Proof. By the theorem (6.2.2) we know that $\mathcal{M}$ is a regular singular q-difference module. By the formal classification (2.4.4) there exists a $K((x))$-basis $\underline{f}$ of $K((x)) \otimes_{\mathcal{F}} M$ such that

$\Phi_q(\underline{f}) = \underline{f}A$, with $A \in Gl_\mu(K)$ in the Jordan normal form. By (2.4.2), we can choose $\underline{e}$ such that for almost all $v \in \Sigma_f$ we have

$$A^{\kappa_v} - 1 \equiv 0 \bmod \varpi_v.$$

We deduce that A is actually a diagonal matrix and that the eigenvalues of A are in $q^{\mathbb{Z}}$. We can assume $A = \mathbb{I}_\mu$ by applying a "shearing transformation" (*cf.* [PS, page 154]), *i.e.* a basis change of the form

$$\begin{pmatrix} x^{n_1}\mathbb{I}_{\nu_1} & & \\ & \ddots & \\ & & x^{n_r}\mathbb{I}_{\nu_r} \end{pmatrix},$$

where $\nu_1, \ldots, \nu_r$ are positive integers such that $\sum \nu_i = \mu$ and $n_1, \ldots, n_r \in \mathbb{Z}$. Let $\underline{e}$ be a basis of M over $\mathcal{F}$. Then there exists $F(x) \in Gl_\mu(K((x)))$ such that $\underline{e} = \underline{f}F(x)$. It follows that

$$\Phi_q\underline{e} = \underline{f}F(qx) = \underline{e}F(x)^{-1}F(qx) \ .$$

Then $F(x)$ is a fundamental matrix of solutions for the q-difference system associated to $\mathcal{M}$ with respect to the basis $\underline{e}$. After a change of basis of the form $\underline{e}' = x^m C\underline{e}$, where $m \in \mathbb{Z}$ and C is a constant invertible matrix, we obtain a q-difference system having a solution $Y(x) = \mathbb{I}_\mu + \sum_{m\geq 1} Y_m x^m \in Gl_\mu(K[\![x]\!])$. Then $Y(x)^{-1} = \mathbb{I}_\mu + \sum_{m\geq 1} \widetilde{Y}_m x^m \in Gl_\mu(K[\![x]\!])$ and

$$G(x) = Y(x)^{-1} d_q(Y)(x) = \left(\mathbb{I}_\mu + \sum_{m\geq 1} \widetilde{Y}_m x^m\right)\left(\sum_{m\geq 1} (m)_q Y_m x^{m-1}\right)$$

has no poles at zero. ■

7. Statement of the q-analogue of Grothendieck's conjecture on p-curvatures.

7.1. Statement of the main theorem.

We recall that K is a number field, $\mathcal{V}_K$ its ring of integers, v is a finite or an infinite place of K and q an element of K, which is not a root of unity. The uniformizer of the finite place v is denoted by ϖ_v. For almost all finite places v, let κ_v be the the multiplicative order of the image of q in the residue field of M modulo ϖ_v. Let $\varpi_{q,v}$ be the integer power of ϖ_v such that $|\varpi_{q,v}|_v = |1 - q^{\kappa_v}|_v$.

We consider a q-difference algebra $\mathcal{F} \subset K(x)$ essentially of finite type over $\mathcal{V}_K$ and a q-difference module $\mathcal{M} = (M, \Phi_q)$ over $\mathcal{F}$.

We want to prove the following theorem, which we consider as the q-analogue of the Grothendieck conjecture for differential equations with p-curvatures zero for almost all finite places:

Main Theorem 7.1.1. *Let $\mathcal{M} = (M, \Phi_q)$ be a q-difference module over $\mathcal{F}$, such that*

(*) *the operator $\Phi_q^{\kappa_v}$ induces the identity on the reduction of $\mathcal{M}$ modulo $\varpi_{q,v}$ for almost all finite places v.*

Then $\mathcal{M}$ becomes trivial over $K(x)$.

Remark 7.1.2. We recall that the q-difference module $\mathcal{M}$ over $K(x)$ is trivial if and only if the following equivalent conditions are satisfied:
1) there exists an isomorphism of q-difference modules $M^{\Phi_q} \otimes_K K(x) \cong M$;
2) there exists a $K(x)$-vector space isomorphism $\psi : M \longrightarrow K(x)^\mu$ such that for all $m \in M$ we have: $\psi(\Phi_q(m)) = \varphi_q(\psi(m))$, where φ_q is defined componentwise on $K(x)^\mu$.
3) there exists a basis $\underline{e}$ of M over $K(x)$ such that, if $\Delta_q \underline{e} = \underline{e} G(x)$, we can find $Y(x) \in Gl(K(x))$ satisfying the q-difference linear system $d_q Y(x) = Y(x)G(x)$.

It is clear that if a q difference module $\mathcal{M}$ over $\mathcal{F}$ becomes trivial over $K(x)$, the hypothesis of the theorem above is satisfied.

By (3.1.2) we immediately obtain:

Corollary 7.1.3. *Let $\mathcal{M} = (M, \Phi_q)$ be a q-difference module over $\mathcal{F}$, such that the reduction of $\mathcal{M}$ modulo $\varpi_{q,v}$ is trivial for almost all v. Then (M, Φ_q) is trivial over $K(x)$.*

In (7.1.1) we have assumed that q is not a root of unity: if q is a root of unity, theorem (7.1.1) is an easy consequence of the results in (§3). We notice that in this particular case, we just need the hypothesis of trivial reduction modulo ϖ_v:

Proposition 7.1.4. *Let q be a primitive κ-root of unity, with $\kappa \geq 1$. Then the q-difference module $\mathcal{M} = (M, \Phi_q)$ over $\mathcal{F}$ becomes trivial over $K(x)$ if and only if $\mathcal{M}$ has trivial reduction modulo ϖ_v for an infinite number of $v \in \Sigma_f$.*

Proof. Let $\underline{e}$ be a basis of M over $\mathcal{F}$ and let $\Phi_q^m(\underline{e}) = \underline{e} A_n(x)$, for all $m \geq 1$. By (3.1.2) it is enough to prove that

$$A_\kappa(x) = \mathbb{I}_\mu \Leftrightarrow A_{\kappa_v}(x) \equiv \mathbb{I}_\mu \text{ modulo } \varpi_v, \text{ for all } v \in S.$$

To conclude it is enough to notice that $\kappa_v = \kappa$ for almost all $v \in \Sigma_f$. ∎

7.2. Idea of the proof.

The proof of (7.1.1) is inspired by the theory of G-functions, from which we derive the definitions below. In the q-difference case they are not as interesting as in the differential one, in fact, as we will see later, the two invariants that we are going to define are finite only in the trivial case. In any case they will be useful in some intermediate steps of the proof.

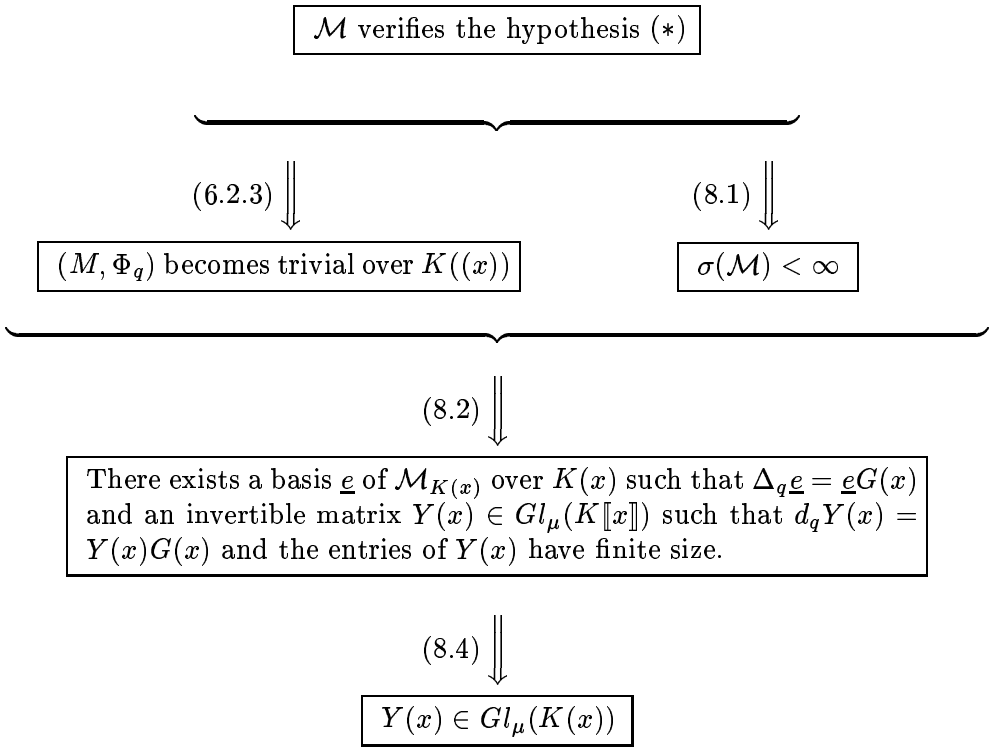
Definition 7.2.1. *Let $y = \sum_{n=0}^{\infty} a_n x^n \in K[\![x]\!]$. We set $h(y, n, v) = \sup_{|\underline{\alpha}| \leq n} \left(\log^+ |a_{\underline{\alpha}}|_v\right)$ and we call size of y (cf.* [A1, I, 1.3]*) the number*

$$\sigma(y) = \limsup_{n \to \infty} \frac{1}{n} \sum_{v \in \Sigma_f \cup \Sigma_\infty} h(y, n, v) \ .$$

Let $\mathcal{M} = (M, \Phi_q)$ be a q-difference module over a q-difference algebra $\mathcal{F} \subset K(x)$. We fix a basis $\underline{e}$ of $\mathcal{M}_{K(x)}$ over $K(x)$ and we set as usual $\Delta_q^n \underline{e} = \underline{e} G_n(x)$ and $h(M, n, v) = \sup_{0 \leq s \leq n} \log \left| \frac{G_s(x)}{[s]!_q} \right|_{v,Gauss}$. We define the size of $\mathcal{M}$ to be

$$\sigma(\mathcal{M}) = \limsup_{n \to \infty} \frac{1}{n} \sum_{\substack{v \in \Sigma_f \\ |1 - q^{\kappa} v|_v < |p|_v^{1/(p-1)}}} h(M, n, v) \ .$$

The proof, that will be detailed in the next section, is organized as follows:



8. Proof of (7.1.1).

8.1. Finiteness of the size of $\mathcal{M}$.

Proposition 8.1.1. *Let $\mathcal{M}$ be a q-difference module over $\mathcal{F} \subset K(x)$ satisfing (∗). Then*

$$\sigma(\mathcal{M}) < +\infty \ .$$

Proof. By assumption there exists a basis $\underline{e}$ of M over $\mathcal{F}$ such that $\Delta_q^m \underline{e} = \underline{e} G_m(x)$ and $|G_{\kappa_v}(x)|_{v,Gauss} \leq |(\kappa_v)_q|_v$ for almost all $v \in \Sigma_f$. For such a v by (5.2.1.1) we have

$$\left| \frac{G_n(x)}{[n]!_q} \right|_{v,Gauss} \leq \left| \frac{G_{[\frac{n}{\kappa_v}]\kappa_v}(x)}{[n]!_q} \right|_{v,Gauss} \leq \frac{|(\kappa_v)_q|_v^{[\frac{n}{\kappa_v}]}}{|[n]!_q|_v} \leq |p|_v^{-n/\kappa_v(p-1)} ,$$

from which we obtain

$$h(M,n,v) \leq n \frac{\log |p|_v^{-1}}{\kappa_v(p-1)} .$$

Let

$$T_1 = \{v \in \Sigma_f : |1-q^{\kappa_v}|_v < |p|_v^{1/(p-1)},\ |G_{\kappa_v}(x)|_{v,Gauss} \leq |(\kappa_v)_q|\}$$

and

$$T_2 = \{|1-q^{\kappa_v}|_v < |p|_v^{1/(p-1)},\ |G_{\kappa_v}(x)|_{v,Gauss} > |(\kappa_v)_q|\} .$$

By (4.2.7.1) we deduce that

$$\sigma(\mathcal{M}) \leq \sum_{v \in T_1} \frac{\log |p|_v^{-1}}{\kappa_v(p-1)} + \sum_{v \in T_2} \log^+ \frac{1}{\chi_v(M)} .$$

We recall that $\Phi_q^{\kappa_v}$ induces the identity on the reduction of $\mathcal{M}$ modulo $\varpi_{q,v}$ if and only if $|G_{\kappa_v}(x)|_{v,Gauss} \leq |(\kappa_v)_q|_v$, so the assumption $(*)$ implies that T_2 is finite.

Let us consider the set $\widetilde{\Sigma}$ of all finite places v of K such that $|q|_v = 1$. Then T_1 is cofinite in $\widetilde{\Sigma}$, hence, to conclude that $\sigma(\mathcal{M})$ is finite, it is enough to prove the lemma:

Lemma 8.1.2. *Let $q \neq 0$ be an element of K which is not a root of unity, $\widetilde{\Sigma}$ be the set of all finite places v of K such that $|q|_v = 1$ and κ_v be the multiplicative order of the image of q in the residue field of K with respect to $v \in \widetilde{\Sigma}$. Then*

$$\sum_{v \in \widetilde{\Sigma}} \frac{\log |p|_v^{-1}}{\kappa_v(p-1)} < \infty .$$

Proof. Let $0 < \varepsilon < 1$. We consider the sets:

$$S_0 = \{v \in \widetilde{\Sigma},\ \kappa_v \geq p-1\} ,$$
$$S_1 = \{v \in \widetilde{\Sigma},\ \kappa_v < p-1 \ , \kappa_v^2 \geq p^{1+\varepsilon}\} ,$$
$$S_2 = \{v \in \widetilde{\Sigma},\ \kappa_v < p-1 \ , \kappa_v^2 < p^{1+\varepsilon}\} .$$

Then, for $\eta = (1-\varepsilon)/(1+\varepsilon)$ and $v \in S_2$, we have

$$p > \kappa_v^{2/(1+\varepsilon)} \ \Rightarrow p-1 \geq \kappa_v^{2/(1+\varepsilon)} = \kappa_v^{1+\eta} ,$$

and hence we obtain

$$\sum_{v \in \widetilde{\Sigma}} \frac{\log |p|_v^{-1}}{\kappa_v(p-1)} \leq \sum_{v \in S_0} \frac{\log |p|_v^{-1}}{(p-1)^2} + \sum_{v \in S_1} \frac{\log |p|_v^{-1}}{p^{1+\varepsilon}} + \sum_{v \in S_2} \frac{\log |p|_v^{-1}}{\kappa_v^{2+\eta}} .$$

The sums over S_0 and S_1 are clearly convergent. To conclude that the sum over S_2 is convergent it is enough to prove that $\sum_{v\in\widetilde{\Sigma}} \frac{\log|1-q^{\kappa_v}|_v^{-1}}{\kappa_v^{2+\eta}}$ is convergent for all $\eta > 0$, since for almost all $v \in \widetilde{\Sigma}$ we have $|1-q^{\kappa_v}|_v^{-1} \geq |p|_v^{-1}$. We recall that $\widetilde{\Sigma}$ is cofinite in Σ_f and that for all integers $n \geq 1$ there exist only a finite number of $v \in \Sigma_f$ such that $\kappa_v = n$ (since $|1-q^n|_v = 1$ for almost every $v \in \Sigma_f$). Therefore by the Product Formula, we get

$$\sum_{v\in\widetilde{\Sigma}} \frac{\log|1-q^{\kappa_v}|_v^{-1}}{\kappa_v^{2+\eta}} = \sum_{n=1}^{\infty} \sum_{\substack{v\in\widetilde{\Sigma} \\ \kappa_v=n}} \frac{\log|1-q^n|_v^{-1}}{n^{2+\eta}}$$
$$= \sum_{n=1}^{\infty} \sum_{\substack{v\in\widetilde{\Sigma},\ \kappa_v\neq n \\ \text{or } v\in(\Sigma_f\cup\Sigma_\infty)\smallsetminus\widetilde{\Sigma}}} \frac{\log|1-q^n|_v}{n^{2+\eta}} .$$

For every $v \in \Sigma_f$ such that $|q|_v \leq 1$ we have $|1-q^n|_v \leq 1$. In particular $|1-q^n|_v = 1$ for almost all $v \in \Sigma_f$. Therefore we obtain

$$\sum_{v\in\widetilde{\Sigma}} \frac{\log|1-q^{\kappa_v}|_v^{-1}}{\kappa_v^{2+\eta}} \leq \sum_{n=1}^{\infty} \sum_{\substack{v\in\Sigma_f,\ |q|_v>1 \\ \text{or } v\in\Sigma_\infty}} \frac{\log|1-q^n|_v}{n^{2+\eta}}$$
$$\leq \sum_{n=1}^{\infty} \left(\sum_{v\in\Sigma_\infty,\ |q|_v\leq 1} \frac{\log 2}{n^{2+\eta}} + \sum_{\substack{v\in\Sigma_f\cup\Sigma_\infty \\ |q|_v>1}} \frac{\log(1+|q|_v)}{n^{1+\eta}} \right) < \infty . \tag{8.1.2.1}$$

■

8.2. Finiteness of the size of a fundamental matrix of solutions.

We have already proven that a q-difference module $\mathcal{M}$ satisfying $(*)$ becomes trivial over $K((x))$ (*cf.* (6.2.3)) and that it has finite size (*cf.* (8.1.1)).

Proposition 8.2.1. *There exists a basis $\underline{e}$ of $(M \otimes_{\mathcal{F}} K(x), \Phi_q \otimes \varphi_q$ over $K(x)$ such that the q-difference system associated to $\mathcal{M}_{K(x)}$ with respect to $\underline{e}$ has an invertible matrix of solution $Y(x) \in Gl_\mu(K[\![x]\!])$, whose entries have finite size.*

Remark 8.2.2. We recall a property of the size of a formal power series, that we will use in the proof below. We know (*cf.* for example [DGS, VI, 4.1]) that

$$\limsup_{n\to\infty} \frac{1}{n} h(n,v,y) = \log^+ \frac{1}{r_v(y)} ,$$

where $r_v(y)$ is the v-adic radius of convergence of y. Then $\sigma(y) < \infty$ if and only if there exists finite set $S \subset \Sigma_f \cup \Sigma_\infty$ such that y has non zero radius of convergence for all $v \in S$ and

$$\limsup_{n\to\infty} \frac{1}{n} \sum_{v\in\Sigma_f\cup\Sigma_\infty\smallsetminus S} h(n,v,y) < \infty .$$

Proof. As in (6.2.3) we can find a basis $\underline{e}$ of $\mathcal{M}_{K(x)}$ such that the associated q-difference system has a solution $Y(x) \in Gl_\mu(K[\![x]\!])$ such that $Y(0) = \mathbb{I}_\mu$. Let $\Delta_q^n \underline{e} = \underline{e} G_n(x)$. Since $G_0 = Y(0) = \mathbb{I}_\mu$, we conclude that $Y(x) = \sum_{n \geq 0} \frac{G_n(0)}{[n]!_q} x^n$.

We want to prove that the entries of $Y(x)$ have finite size. By (4.2.3) and (4.2.10), we deduce that

$$\limsup_{n \to \infty} \frac{1}{n} \sum_{\substack{v \in \Sigma_f \\ |q|_v \leq 1}} \sup_{0 \leq s \leq n} \log^+ |Y_n|_v \leq \sigma(\mathcal{M}) + \sum_{\substack{v \in \Sigma_f, |q|_v < 1 \\ \text{or } 1 > |1-q^\kappa|_v \geq |p|_v^{1/(p-1)}}} \log^+ \frac{1}{\chi_v(M)} < \infty \ .$$

By the previous remark it is enough to prove that the entries of $Y(x)$ have non zero radius of convergence for all $v \in \Sigma_\infty$ and for all $v \in \Sigma_f$ such that $|q|_v > 1$. Since $\mathcal{M}$ is a regular q-difference module over $K(x)$ each entry of $Y(x)$ is solution of a regular singular q-difference equation, by (2.4.5). It follows by [Be, IV] and [BB, IV][(1)] that the entries of $Y(x)$ have non zero radius of convergence for all $v \in \Sigma_\infty$ such that $|q|_v \neq 1$ and for all $v \in \Sigma_f$ such that $|q|_v > 1$.

The conclusion of the proof of (8.2.1) is the object of the next section.

8.3. How to deal with the problem of archimedean small divisors.

To conclude that the entries of $Y(x)$ have finite radius of convergence for all infinite place v such that $|q|_v = 1$ we recall the following result:

[Be, 6.1] *Let $\mathcal{L} = \sum_{i=0}^{\mu} \sum_{j=0}^{\nu} a_{i,j} x^j \varphi_q^i \in \mathbb{C}[x, \varphi_q]$ be a q-difference operator and let $Q(x) = \sum_{i=0}^{\mu} a_{i,j_0} x^i$ be a polynomial such that $j_0 = \min\{j = 0, \ldots, \nu : a_{i,j} \neq 0\}$. We suppose that $|q|_{\mathbb{C}} = 1$ and that there exist two positive real constants c_1 and c_2 such that all the roots u of the polynomial $(x-1)Q(x)$ satisfy the inequality $|q^n - u|_v \geq c_1 n^{-c_2}$ for $n >> 0$. Then a formal power series $y \in \mathbb{C}[\![x]\!]$ solution of $\mathcal{L}y = 0$ is convergent.*

It is enough to prove that for any finite place v such that $|q|_v = 1$, there exist two positive real constant $c_{1,v}$ and $c_{2,v}$ such that

$$|q^n - u|_v \geq c_{1,v} n^{-c_{2,v}} \tag{8.3.0.1}$$

for $n >> 0$. To verify (8.3.0.1) we will use the following theorem by Baker[(2)]:

---

(1) In [Be] and [BB] the authors assume $|q| < 1$. It is only a problem of convention and their results translate to our situation.

(2) We can find a proof of the additive version of this theorem in [B], but we prefer to cite the version in [Se], which is more suitable to our situation.

[Se, 8.2, Corollary] *Let K be a number field, $\alpha_1, \dots, \alpha_l \in K$, $\beta_1, \dots, \beta_l \in \mathbb{Z}$ and v a place of K. If $\alpha_1^{\beta_1} \cdots \alpha_l^{\beta_l} \neq 1$ then*

$$\left|\alpha_1^{\beta_1} \cdots \alpha_l^{\beta_l} - 1\right|_v \geq \sup(4, \beta_1, \dots, \beta_l)^{-const} ,$$

where the constant depends only on v and on $\alpha_1, \dots, \alpha_l \in K$.

Let $l = 2$, $\alpha_1 = q$, $\alpha_2 = u$, $\beta_1 = n$ and $\beta_2 = -1$. Since for $n >> 0$ we have $q^n u^{-1} \neq 1$, we obtain $|q^n - u|_v \geq |u|_v n^{-c(u)}$. Here $c(u)$ is a constant depending on u, q and v. We set

$$c_{1,v} = \sup\left(\{|u|_v : \text{such that } Q(u) = 0\} \cup \{1\}\right)$$

and

$$c_{2,v} = \sup\{c(u) : u \text{ such that } Q(u) = 0 \text{ or } u = 1\} ;$$

then we obtain the desired inequality. This concludes the proof of (8.2.1). ■

8.4. Conclusion of the proof: a criterion of rationality.

We conclude the proof of (7.1.1) by applying the following proposition:

Proposition 8.4.1. (Y. André) *Let $y(x) \in K[\![x]\!]$ be a formal power series solution of a q-difference equation*

$$a_\mu(x) d_q^\mu(y)(x) + a_{\mu-1}(x) d_q^{\mu-1}(y)(x) + \cdots + a_0(x) y(x) = 0 ,$$

with $a_i(x) \in K(x)$ for all $i = 0, \dots, \mu$. If $\sigma(y) < \infty$ then $y(x)$ is the Taylor expansion of a rational function $\in K(x)$.

Proof. It is a general property of q-difference equations that for all $v \in \Sigma_f \cup \Sigma_\infty$ such that $|q|_v \neq 1$ the series $y(x)$ with non zero radius of convergence has infinite radius of meromorphy (*cf.* [BB, 7.2]). We remark that we can always find such a v since q is not a root of unity. To conclude that $y(x)$ is a rational function it is enough to apply the more general result [A1, VIII, 1.1, Th.], but we prefer to sketch the proof, since it simplifies under the present assumptions. First we prove that $y(x)$ is an algebraic function following the proof of [A2, 2.3.1] adapted to this particular case.

Step 1. We fix $\eta \in (0, 1]$ and an integer $\nu > 1$. Let

$$\vec{Y} = {}^t(1, y(x), \dots, y(x)^{\nu-1}) = \sum_{m \geq 0} \vec{Y}_m x^m \in K[\![x]\!]^\nu .$$

Using the Siegel's Lemma we can construct a polynomial vector

$$\vec{P_N}(x) = (P_{N,0}(x), \dots, P_{N,\nu-1}(x)) = \sum_{m \geq 0} \vec{P}_N^{(m)} x^m \in K[x]^\nu ,$$

for all $N \in \mathbb{N}$, such that

$i)$ $$\mathrm{ord}_0(\overrightarrow{P_N} \cdot \overrightarrow{Y}) = M \geq N \ ;$$

$ii)$ $$\deg_x \overrightarrow{P_N} = \sup_{i=0,\ldots,\nu-1} (\deg_x P_{N,i}(x)) \leq \frac{1}{\nu}\left(1+\frac{1}{\eta}\right) N + o(N) \ ;$$

$iii)$ $$h(\overrightarrow{P_N}) = \limsup_{m\to\infty} \frac{1}{m} \sum_{v\in\Sigma_f\cup\Sigma_\infty} \log^+ \left(\sup_{m\geq 0} |\overrightarrow{P_N}^{(m)}|_v \right) \leq \eta N \sigma(\overrightarrow{Y}) + o(N) \ .$$

Step 2. Let us suppose that $y(x)$ is *not* algebraic; then $\overrightarrow{P_N} \cdot \overrightarrow{Y} \neq 0$ for all $N \geq 1$ and hence $M < \infty$. We set

$$\alpha = \frac{1}{M!}\frac{d^M}{dx^M}(\overrightarrow{P_N}\overrightarrow{Y})(0) \neq 0 \ .$$

For all $v \in \Sigma_f$ we have

(8.4.1.1) $$\log|\alpha|_v \leq \log^+ |\overrightarrow{P_N}(x)|_{v,Gauss} + \sup_{m\leq M} \log^+ |\overrightarrow{Y}_m|_v \ .$$

Step 3. Let V a finite subset of $\Sigma_f \cup \Sigma_\infty$ containing Σ_∞. Then V contains at least one place v such that the radius of meromorphy $M_v(y)$ is infinite, since q is not a root of unity. For all $v \in V$ the formal power series $y(x)$ is the germ at zero of a meromorphic function, therefore we can write $y(x) = f_v(x)/g_v(x)$, where $f_v(x)$ and $g_v(x)$ are v-adic analytic functions converging for $|x|_v < M_v(y)$. We can suppose that $g_v(0) = 1$. We set:

$$\overrightarrow{Z}_v(x) = (g_v(x)^{\nu-1}, g_v(x)^{\nu-2} f_v(x), \ldots, f_v(x)^{\nu-1}),$$
$$\psi_v(x) = \overrightarrow{P_N}(x) \cdot \overrightarrow{Z}_v(x);$$

from which follows

$$\overrightarrow{P_N}(x) \cdot \overrightarrow{Y}(x) = \frac{1}{g_v(x)^{\nu-1}} \psi_v(x) \ .$$

We deduce that:

$$\alpha = \frac{1}{M!}\frac{d^M}{dx^M}(\psi_v)(0) \ .$$

Step 4. Let us fix $m_v < M_v(y)$ for all $v \in V$. By Cauchy's estimates we obtain

(8.4.1.2)
$$\begin{aligned} \log|\alpha|_v &\leq -M \log m_v + \log\left(\sup_{|x|_v = m_v} |\psi_v(x)|_v \right) \\ &\leq -M \log m_v + \log^+ \left(\sup_{m\leq N} |\overrightarrow{P_N}^{(m)}|_v \right) + m_v \deg_x \overrightarrow{P_N} + o(N) \ . \end{aligned}$$

Step 5. Summing (8.4.1.1) for $v \in (\Sigma_\infty \cup \Sigma_f) \smallsetminus V$ and (8.4.1.2) for $v \in V$, by the Product Formula we obtain

$$M \sum_{v \in V} \log m_v \leq \sum_{v \in \Sigma_f \cup \Sigma_\infty} \log^+ \left(\sup_{m \leq N} |\overrightarrow{P_N}^{(m)}|_v \right) + \sum_{v \notin V} \sup_{m \leq M} \log^+ |\overrightarrow{Y}_m|_v + \deg_x \overrightarrow{P_N} \sum_{v \in V} m_v + o(N) \ ;$$

dividing by $M \geq N$ and taking the lim sup for $N \to \infty$ we have

$$\sum_{v \in V} \log m_v \leq (\eta + 1)\sigma(y) + \frac{1}{\nu}\left(1 + \frac{1}{\eta}\right) \sum_{v \in V} m_v \ .$$

Finally we can take the limit for $\nu \to \infty$ and $\eta \to 0$ and obtain:

$$\sum_{v \in V} \log m_v \leq \sigma(y) \ .$$

Since $\sigma(y) < \infty$, we get a contradiction by letting $m_v \to M_v(y)$.

Then we have proved that $y(x)$ is an algebraic function. Let us fix $v \in \Sigma_\infty$ such that $|q|_v \neq 1$, hence such that $y(x)$ has infinite v-adic radius of meromorphy. By choosing the place v, we have fixed an isometry $K \hookrightarrow \mathbb{C}_v$. The field $\mathbb{C}_v(x,y)$ is the field of meromorphic functions over a surface E. The immersion $\mathbb{C}_v(x) \hookrightarrow \mathbb{C}_v(x,y)$ determines an algebraic covering $p : E \longrightarrow \mathbb{A}^1_{\mathbb{C}_v}$. Since $y(x)$ is a meromorphic function over E, p is an étale covering of $\mathbb{A}^1_{\mathbb{C}_v}$. Such a covering is necessarily trivial, hence $\mathbb{C}_v(x,y) = \mathbb{C}_v(x)$. ∎

This achieves the proof of the main theorem (7.1.1).

8.5. A corollary.

We point out that we can deduce the following corollary by the proof of (7.1.1):

Corollary 8.5.1. *Let S be a subset of Σ_f having Dirichlet density 1 and $\mathcal{M}$ a q-difference module over a q-difference algebra $\mathcal{F} \subset K(x)$ essentially of finite type over $\mathcal{V}_v$. We assume that for all $v \in S$ the operator $\Phi_q^{\kappa_v}$ induces the identity over the reduction of $\mathcal{M}$ modulo $\varpi_{q,v}$. We assume moreover that:*

$$\sum_{\substack{v \in \Sigma_f \smallsetminus S \\ |1-q^{\kappa_v}|_v < |p|_v^{1/(p-1)}}} \log \frac{1}{\chi_v(M)} < \infty \ .$$

Then $\mathcal{M}$ becomes trivial over $K(x)$.

Proof. We notice that in the proof of (8.1.1) we have actually shown that:

$$\limsup_{n \to \infty} \frac{1}{n} \sum_{\substack{v \in S \\ |1-q^{\kappa_v}|_v \leq |p|_v^{1/(p-1)}}} h(M,n,v) < \infty \ .$$

Let

$$T = \{v \in \Sigma_f \smallsetminus S : |G(x)|_{v,Gauss} \leq 1 \text{ and } |1 - q^{\kappa_v}|_v < |p|_v^{1/(p-1)}\} .$$

If we prove that

$$\limsup_{n\to\infty} \frac{1}{n} \sum_{v\in T} h(M,n,v) \leq \sum_{v\in T} \log \frac{1}{\chi_v(M)} \tag{8.5.1.1}$$

then we obtain that $\sigma(\mathcal{M}) < \infty$, since $\chi_v(M) \geq |\kappa_v|_v^{1/\kappa} |p|_v^{1/\kappa_v(p-1)}$ and $|G(x)|_{v,Gauss} \leq 1$ for almost all $v \in \Sigma_f$. Then we can conclude the proof as the proof of (7.1.1).

To prove (8.5.1.1) we just need to notice that for all $v \in \Sigma_f \smallsetminus S$ such that $|1 - q^{\kappa_v}|_v < |p|_v^{1/(p-1)}$ and $|G(x)|_{v,Gauss} \leq 1$ and for all $n \geq 1$ we have

$$h(M,n,v) \leq \log \left(|(\kappa_v)_q|_v^{\left[\frac{n}{\kappa_v}\right]} |p|_v^{\left[\frac{n}{\kappa_v}\right]\frac{1}{p-1}} \right) \leq n \log \frac{1}{\chi_v(M)} .$$

■

References.

[A1] André Y.: "*G-functions and Geometry*", Aspects of Mathematics E13, Vieweg, Braunschweig/Wiesbaden, 1989.

[A2] André Y.: "Sur la conjecture des p-courbures de Grothendieck-Katz", Institut de Mathématiques de Jussieu, preprint 134, octobre 1997.

[A3] André Y.: "Séries Gevrey de type arithmétique. II. Transcendance sans transcendance", Annals of Math, 151, 2 (2000), 741-756.

[A4] André Y.: "Différentielles non-commutatives et théorie de Galois différentielle ou aux différences", to appear in Annals Scient. Éc. Norm. Sup..

[AB] André Y., Baldassarri F.: "*De Rham Cohomology of Differential Modules on Algebraic Varieties*", Prépublication de l'Institut de Mathématiques de Jussieu 184, Septembre 1998.

[B] Baker A.: "The theory of linear forms in logarithms", Transcendence theory: advances and applications (Proc. Conf., Univ. Cambridge, Cambridge, 1976), pp. 1–27. Academic Press, London, 1977.

[Be] Bézivin J.P.: "Sur les équations fonctionnelles aux q-différences", Aequationes math. 43, (1992).

[BB] Bézivin J.P., Boutabaa A.: "Sur les équations fonctionnelles p-adique aux q-différences", Collect. Math. 43, 2 (1992).

[Bo] Bost J.B.: "Algebraic leaves of algebraic foliations over number fields", Université d'Orsay, preprint 2000-60.

[CC] Chudnovsky D.V., Chudnovsky G.V.: "Applications of Padé approximations to the Grothendieck conjecture on linear differential equations", Lect. Notes Math. 1135 (1985), 52-100.

[Ch] Cohen P.: "*Skew field constructions*", Cambridge Univ. Press, 1977.

[DV] Di Vizio L.: "Arithmetic theory of q-difference equations II. The q-analogue of Katz's conjectural description of differential Galois groups", (Section IV).

[Du] Duval A.: "Lemmes de Hensel et Factorisation Formelle pour les Opérateurs aux Différences", Funkcialaj Ekvacioj, 26 (1983), 349-368.

[D] Dwork B.: "On the size of differential modules", Duke Math. J. 96 (1999), no. 2, 225–239.

[DGS] Dwork B., Gerotto G., Sullivan F.: "*An Introduction to* G*-functions*", Annals of Mathematical Studies 133, Princeton University Press, Princeton N.J., 1994.

[GR] Gasper G., Rahman M.: "*Basic hypergeometric series*", Cambridge Univ. Press, Cambridge, 1990.

[H] Hendriks P. A.: "Algebraic Aspects of Linear Differential and Difference Equations", Ph. D. thesis, University of Groningen, 1996.

[Ho] Honda T.: "Algebraic differential equations", I.N.D.A.M. Symp. Math. XXIV (1981), 169-204.

[K1] Katz N. M.: "Nilpotent connections and the monodromy theorem. Applications of a result of Turrittin", Publ. Math. IHES 39 (1970), 175-232.

[K2] Katz N. M.: "Algebraic solution of differential equations (p-curvature and Hodge Filtration)", Invent. Math. 18, (1972), 1-118.

[K3] Katz N. M.: "A conjecture in the arithmetic theory of differential equations", Bull. S.M.F. 110, (1982), 203-239, and Bull. S.M.F. 111, (1982), 347-348.

[K4] Katz N. M.: "On the calculation of some differential Galois groups", Invent. math. 87, 13-61 (1987).

[N] Neukirch J.: "*Algebraic number theory*", Grundlehren der math. Wissenschaften 322, Springer-Verlag, 1999.

[P] Praagman C.: "The formal classification of linear difference equation", Proc. Kon. Ned. Ac. Wet. Ser. A, 86, 1983.

[PS] van der Put M., Singer M. F.: "*Galois Theory of Difference Equations*", Lecture Notes in Mathematics 1666, Springer, 1997.

[S] Sauloy J.: "*Théorie de Galois des équations aux q-différences fuchsiennes*", Thèse doctorale de l'Université Paul Sabatier de Toulouse.

[Se] Serre J.P.: "*Lectures on the Mordell-Weil theorem*", Aspects of Mathematics E15, Vieweg, Braunschweig/Wiesbaden, 1989.

[Sc] Schinzel A.: "Abelians binomials, power residues and exponential congruences", Acta Arithmetica, 27, 1975, 397-420.

Section IV.
The q-analogue of Katz's conjectural description of differential Galois group

Introduction.

In the introduction of [K3], N. Katz asks the following question:

> *"if one is explicitly given an n'th order differential equation, how can one "tell at a glance" what its differential Galois group G_{gal} is?"*

This question is said to be the starting point for the articles [K1], [K2] and [K3] and it still has not received a satisfactory answer.

In this paper we prove an analogue for q-difference equations of the conjectural description of the Lie algebra of the generic Galois group in [K2]. In some cases, this q-analogue turns out to be an effective instrument to "tell at a glance" what the differential Galois group of a q-difference equation is.

Let us recall the conjecture in [K2]. Let $\mathbb{Q}$ be the field of rational numbers, $\mathbb{Q}(x)$ be the field of rational functions with coefficients in $\mathbb{Q}$ and $\mathcal{M} = (M, \nabla)$ be $\mathbb{Q}(x)$-vector space with a $\mathbb{Q}(x)/\mathbb{Q}$-connection. We define the generic Galois group $Gal(\mathcal{M})$ of $\mathcal{M}$ to be the algebraic subgroup of $GL(M)$ stabilizing all the sub-subspaces in the mixed tensor spaces $\oplus_{i,j}(M^{\otimes^i} \otimes_{\mathbb{Q}(x)} (M^*)^{\otimes^j})$. We can consider a lattice $\widetilde{M}$ of M over a finite type algebra over $\mathbb{Z}$, stable under the connection, and we can reduce $\widetilde{M}$ modulo p, for almost all primes p. The operator $\psi_p = \nabla\left(\frac{d}{dx}\right)^p$ acting over $\widetilde{M} \otimes_{\mathbb{Z}} \mathbb{F}_p$, is called the *$p$-curvature*. Beside it makes sense to consider the reduction modulo p for almost all p of $Gal(M)$ and its Lie algebra. The Katz conjecture says:

Katz's conjecture. *The Lie algebra of $Gal(M)$ is the smallest algebraic Lie sub-algebra of $\mathrm{End}_{\mathbb{Q}(x)}(M)$ whose reduction modulo p contains ψ_p for almost all p.*

It is proved in [K2] that this conjecture is equivalent to Grothendieck's conjecture on p-curva-

tures:

Grothendieck's conjecture. *The differential module (M, ∇) becomes trivial over a finite extension of $\mathbb{Q}(x)$ if and only if the p-curvatures ψ_p are zero for almost all p.*

We recall that for a differential module over $\mathbb{F}_p(x)$ the condition $\psi_p = 0$ is equivalent to the triviality.

We consider now the q-difference case. Let $q \neq 0, 1, -1$ be a rational number and

$$\begin{array}{rccc} \varphi_q : & \mathbb{Q}(x) & \longrightarrow & \mathbb{Q}(x) \\ & f(x) & \longmapsto & f(qx) \end{array}$$

a q-difference operator. Let M be a finite dimensional $\mathbb{Q}(x)$-vector space equipped with a q-difference operator $\Phi_q : M \longrightarrow M$, *i.e.* with a $\mathbb{Q}$-linear invertible morphism such that $\Phi_q(fm) = \varphi_q(f)\Phi_q(m)$ for all $f \in \mathbb{Q}(x)$ and all $m \in M$. As in the differential module theory, we can attach to $\mathcal{M} = (M, \Phi_q)$ an algebraic closed subgroup $Gal(\mathcal{M})$ of $GL(M)$, that we call q-difference generic Galois group. It is the stabilizer of all q-difference sub-modules of all finite sums of the form $\oplus_{i,j}(M^{\otimes^i} \otimes_{\mathbb{Q}(x)} (M^*)^{\otimes^j})$, equipped with the operator induced by Φ_q.

For almost every prime p we can define a non negative integer κ_p by setting:

$$\kappa_p = \min\{n \in \mathbb{Z} : n > 0,\ q^n \equiv 1 \bmod p\} .$$

We define ℓ_p to be the positive integer such that

$$1 - q^{\kappa_p} = p^{\ell_p}\frac{h}{g}, \text{ with } h, g \in \mathbb{Z} \text{ primes to } p.$$

We can consider the reduction modulo p^{ℓ_p} of M for almost all p, by reducing a lattice $\widetilde{M}$ of M defined over a $\mathbb{Z}$-algebra of finite type and stable by Φ_q. Also the algebraic group $Gal(\mathcal{M})$ can be reduced modulo p^{ℓ_p} for almost all p. Then our description of $Gal(\mathcal{M})$ is the following:

Main theorem. *The algebraic group $Gal(\mathcal{M})$ is the smallest algebraic subgroup of $GL(M)$ whose reduction modulo p^{ℓ_p} contains the reduction of $\Phi_q^{\kappa_p}$ modulo p^{ℓ_p} for almost all p.*

Taking into account the fact that Φ_q is a φ_q-linear endomorphism (which is easier to handle than the higher derivations occurring in the differential case), sometimes it happens that one can calculate all Φ_q^n at once and therefore determines the generic Galois group.

The proof of the theorem relies on the q-analogue of Grothendieck's conjecture on p-curvatures proved in [DVIII, (7.1)]:

Theorem. *The q-difference module (M, Φ_q) is trivial over $\mathbb{Q}(x)$ if and only if $\Phi_q^{\kappa_p}$ is the identity modulo p^{ℓ_p} for almost all p.*

To solve this technical problem we exploit a specific property of q-difference modules. One can attached to $\mathcal{M}$ a q^r-difference module $\mathcal{M}_r$, replacing Φ_q by Φ_q^r: it follows that instead of a

single Galois group attached to M, we have a family of algebraic group $Gal\mathcal{M}_r$ for all integers $r \geq 1$, partially ordered by inclusion.

Table of contents

1. Definition of the generic Galois group associated to a q-difference module.

1.1. q-difference modules.

Let R be a commutative ring. We fix a *unit q in R*. We shall informally refer to a R-algebra $\mathcal{F}$ of functions of the variable x endowed with the operator φ_q, such that $\varphi_q(f(x)) = f(qx)$, as a *q-difference algebra over R*. A *morphism $\mathcal{F} \longrightarrow \mathcal{F}'$ of q-difference algebras* is a morphism of R-algebra commuting to the action of φ_q.

We shall say that a q-difference algebra $\mathcal{F}$ over R is *essentially of finite type* if there exist $P_1, \ldots, P_n \in \mathcal{F}$ such that $\mathcal{F} = R[P_1(q^i x), \ldots, P_n(q^i x); i \geq 0]$.

We denote by $C = \{f \in \mathcal{F} : \varphi_q(f) = f\}$ the *subring of constants of $\mathcal{F}$*.

Example 1.1.1. We are particularly interested in the following two cases:
i) $R = K$ is a field and q *is a non zero element of* K, *which is not a root of unity.* Then $K(x)$ is a q-difference algebra with respect to $\varphi_q(f(x)) = f(qx)$. It is easy to verify that the subfield of constants of $K(x)$ is:

$$K(x)^{\varphi_q} = \{f \in K(x) : \varphi_q(f) = f\} = K \ .$$

ii) Let R be a sub-ring of the field K and and $P_1(x), \ldots, P_n(x) \in K(x)$. Then

$$R\left[x, \frac{1}{P_1(q^i x)}, \ldots, \frac{1}{P_n(q^i x)}; i \geq 0\right] \ ,$$

endowed with the restriction of φ_q, is a q-difference algebra essentially of finite type over R.

Definition 1.1.2. *A q-difference module $\mathcal{M} = (M, \Phi_q)$ over $\mathcal{F}$ is a free $\mathcal{F}$-module M of finite rank equipped with a φ_q-semilinear automorphism Φ_q, i.e. a C-linear automorphism of M, such that $\Phi_q(f(x)m) = f(qx)\Phi_q(m)$, for any $m \in M$ and any $f(x) \in \mathcal{F}$.*

Definition 1.1.3. *A morphism $\psi : (M, \Phi_q) \longrightarrow (M', \Phi'_q)$ of q-difference modules a C-linear morphism $\psi : M \longrightarrow M'$ commuting with the action of Φ_q and Φ'_q.*

Definition 1.1.4. *A q-difference module $\mathcal{M} = (M, \Phi_q)$ over $\mathcal{F}$ is trivial if there exists a free C-module N such that $\mathcal{M}$ is isomorphic to $(N \otimes_C \mathcal{F}, id_N \otimes \varphi_q)$ as a q-difference module.*

Let us consider a morphism $\mathcal{F} \longrightarrow \mathcal{F}'$ of q-difference algebras and a q-difference module $\mathcal{M} = (M, \Phi_q)$ over $\mathcal{F}$.

Definition 1.1.5. *The q-difference module $\mathcal{M}_{\mathcal{F}'}$ obtained from $\mathcal{M}$ by extension of coefficients from $\mathcal{F}$ to $\mathcal{F}'$ is the $\mathcal{F}'$-module $M \otimes_{\mathcal{F}} \mathcal{F}'$ equipped with the operator $\Phi_q \otimes \varphi_q$.*

1.2. Some algebraic constructions.

We consider the following algebraic constructions on the category of q-difference modules over a fixed q-difference algebra $\mathcal{F}$:

Dual q-difference module. Let $\mathcal{M} = (M, \Phi_q)$ be a q-difference module over $\mathcal{F}$. Let us consider the dual $\mathcal{F}$-module $\check{M} = Hom_{\mathcal{F}}(M, \mathcal{F})$ of M: $\check{M}$ is naturally a q-difference module equipped with the q-difference operator $\check{\Phi}_q = {}^t\Phi_q^{-1}$, defined by

$$< \check{\Phi}_q(\check{m}), m >=< \check{m}, \Phi_q^{-1}(m) > \text{ , for all } \check{m} \in \check{M} \text{ and } m \in M.$$

The q-difference module $\check{\mathcal{M}} = (\check{M}, \check{\Phi}_q)$ over $\mathcal{F}$ is the dual q-difference module of $\mathcal{M}$.

Tensor product of q-difference modules. Let $\mathcal{M}' = (M', \Phi'_q)$ and $\mathcal{M}'' = (M'', \Phi''_q)$ be two q-difference modules of finite rank over $\mathcal{F}$. The tensor product $M' \otimes_{\mathcal{F}} M''$ has a natural structure of q-difference module defined by:

$$\Phi_q(m' \otimes m'') = \Phi'_q(m') \otimes \Phi''_q(m'') \text{ , for all } m' \in M' \text{ and } m'' \in M''.$$

The q-difference module $\mathcal{M}' \otimes_{\mathcal{F}} \mathcal{M}'' = (M' \otimes_{\mathcal{F}} M'', \Phi'_q \otimes \Phi''_q)$ over $\mathcal{F}$ is the tensor product of $\mathcal{M}'$ and $\mathcal{M}''$.

We denote by $<\mathcal{M}>^{\otimes}$ the full subcategory of the category of the q-difference modules over $\mathcal{F}$ containing all the subquotients of the q-difference modules obtained as finite sums of the form $\oplus_{i,j} T^{i,j}(\mathcal{M})$, where $T^{i,j}(\mathcal{M}) = \mathcal{M}^{\otimes^i} \otimes \check{\mathcal{M}}^{\otimes^j}$.

1.3. Definition of the Galois group of a q-difference module.

Let K be a field and q be a non zero element of K which is not a root of unity. Let $\mathcal{M} = (M, \Phi_q)$ be a q-difference module over $K(x)$.

Sometimes, the tensor category $<\mathcal{M}>^{\otimes}$ comes equipped with a K-linear fiber functor

$$\omega : <\mathcal{M}>^{\otimes} \longrightarrow \{\text{finite dimensional } K\text{-vector spaces}\} .$$

In fact, such a fiber functor always exists after replacing K by some finite extension. Here is an explicit construction. The q-difference module $\mathcal{M}$ admits a "model" $\widetilde{\mathcal{M}}$ over some q-difference algebra $\mathcal{F} \subset K(x)$ essentially of finite type over $\mathcal{V}_K$. This provides a corresponding "model" $\widetilde{\mathcal{N}}$ for any $\mathcal{N}$ in $<\mathcal{M}>^{\otimes}$. Consider a K-valued point x of $\mathcal{F}$ (which exists after passing to a finite extension of K). Then the fiber at x provides a "fiber functor". The corresponding tannakian group may be interpreted as Picard-Vessiot group of a q-difference systems, as considered in [PS] (this interpretation is not used in the sequel).

It follows (*cf.* [DM, 2.11] and [A2, III, 2.1.1]) that there exists an algebraic closed subgroup $Gal(\mathcal{M}, \omega)$ of $GL(\omega(\mathcal{M}))$, such that ω induces a tensor equivalence of categories between $<\mathcal{M}>^{\otimes}$ and the category of of finite type representations of $Gal(\mathcal{M}, \omega)$ over K.

Definition 1.3.1. *The algebraic group $Gal(\mathcal{M}, \omega)$ is the Galois group of $\mathcal{M}$ pointed at ω.*

We recall the following results:

Lemma 1.3.2. [A2, III, 2.1.1] *The algebraic group $Gal(\mathcal{M}, \omega)$ is the subgroup of $Gl(\omega(\mathcal{M}))$ which stabilizes $\omega(\mathcal{N})$ for all sub-object $\mathcal{N}$ of a finite sum $T^{i,j}(\mathcal{M}) = \mathcal{M}^{\otimes^i} \otimes \check{\mathcal{M}}^{\otimes^j}$.*

Remark 1.3.3. We notice that $Gal(\mathcal{M}, \omega)$ is a stabilizer in the sense of algebraic groups.

Lemma 1.3.4. [A2, III, 2.1.4] *The group $Gal(\mathcal{M}, \omega)$ is trivial if and only if $\mathcal{M}$ is a trivial q-difference module over $K(x)$ (cf. (1.1.4)).*

1.4. Definition of the generic Galois group of a q-difference module.

Let $\mathcal{M} = (M, \Phi_q)$ be a q-difference module over $K(x)$. Let us consider the forgetful fiber functor "underlying vector space"

$$\eta : <\mathcal{M}>^{\otimes} \longrightarrow \{K(x)\text{-vector spaces}\} .$$

The functor $\underline{Aut}^{\otimes}(\eta)$ defined on the category of commutative $K(x)$-algebras is representable by an algebraic group $Gal(\mathcal{M}, \eta)$ over $K(x)$.

Definition 1.4.1. *The algebraic group $Gal(\mathcal{M}, \eta)$ is the generic Galois group of $\mathcal{M}$.*

Remark 1.4.2. The generic Galois group $Gal(\mathcal{M}, \eta)$ admits the following concrete description: it is the closed subgroup of $GL(M)$ which stabilizes all the q-difference sub-modules in finite sums $\oplus_{i,j} T^{i,j}(\mathcal{M})$ (*cf.* [A2, §III, 2.2]), in the sense of algebraic groups. Since $GL(M)$

is a noetherian algebraic variety, $Gal(\mathcal{M},\eta)$ is defined as the stabilizer of a finite number of q-difference sub-modules $\mathcal{N}_1,\dots,\mathcal{N}_r$ of some finite sums $\oplus_{i,j}T^{i,j}(\mathcal{M})$: this is equivalent to ask that $Gal(\mathcal{M},\eta)$ is the stabilizer of the maximal exterior power of $\oplus_{i=1}^r\mathcal{N}_i$ (*cf.* [W, A.2]). This shows that $Gal(\mathcal{M},\eta)$ can be define as the stabilizer of a q-difference sub-module of rank 1 of a finite sum $\oplus_h T^{i_h,j_h}(\mathcal{M})$.

Warning. A sub-$K(x)$-vector space of a finite sum $\oplus_{i,j}T^{i,j}(M)$ stabilized by the generic Galois group $Gal(\mathcal{M},\eta)$ is not necessarily a q-difference module.

Remark 1.4.3. If ω is a fiber functor over $<\mathcal{M}>^{\otimes}$, with values in K-spaces, the functor $\underline{Isom}^{\otimes}(\omega\otimes_K 1_{K(x)},\eta)$ is representable by a $K(x)$-group scheme $\Sigma(\mathcal{M},\omega)$, which is a torsor over $Gal(\mathcal{M},\omega)\otimes_K K(x)$ (*cf.* [DM, 3.2] and [A2, III, 2.2]), such that $Gal(\mathcal{M},\eta) = Aut_{Gal(\mathcal{M},\omega)\otimes_K K(x)}\Sigma(\mathcal{M},\omega)$.

Lemma 1.4.4. *A q-difference module $\mathcal{M}$ over $K(x)$ is trivial if and only if $Gal(\mathcal{M},\eta)$ is the trivial group.*

Proof. If a fiber functor exists, this follows from the previous remark and (1.3.4). In general, ω exists after replacing K by a finite extension, and the result follows by an easy Galois descent. ■

2. An arithmetic description of the generic Galois group.

Let K be a number field and $\mathcal{V}_K$ the ring of integers of K. We denote by Σ_f the set of all finite places v of K, by $\varpi_v\in\mathcal{V}_K$ the uniformizer associated to v, and by $\mathcal{V}_v$ the discrete valuation ring of K associated to v.

We choose an element $q\in K$ which is *not* a root of unity. For every finite place v such that q is a unit of $\mathcal{V}_v$ we denote by κ_v the order of the cyclic group generated by the image of q in the residue field of $\mathcal{V}_v$, *i.e.*:

$$\kappa_v = \min\{m\in\mathbb{Z}:\ m>0 \text{ and } 1-q^m\in\varpi_v\mathcal{V}_v\}\ .$$

Let $\varpi_{q,v}$ be the power of ϖ_v satisfying $1-q^{\kappa_v}\in\varpi_{v,q}\mathcal{V}_v$ and $1-q^{\kappa_v}\notin\varpi_v\varpi_{v,q}\mathcal{V}_v$. We set $k_{q,v}=\mathcal{V}_K/\varpi_{q,v}\mathcal{V}_K$.

2.1. Algebraic groups "containing $\Phi_q^{\kappa_v}$ for almost all v".

Let $\mathcal{M}=(M,\Phi_q)$ be a q-difference module over $K(x)$. One can always find a q-difference algebra $\mathcal{F}\subset K(x)$ essentially of finite type over the ring of integers $\mathcal{V}_K$ of K and a q-difference module $\widetilde{\mathcal{M}}=(\widetilde{M},\widetilde{\Phi}_q)$ over $\mathcal{F}$ such that $\mathcal{M}$ is isomorphic to $\widetilde{\mathcal{M}}_{K(x)}$.

Remark. Since $q^{\kappa_v}\equiv 1$ modulo $\pi_{q,v}$, $\Phi_q^{\kappa_v}$ induces a $(\mathcal{F}\otimes_{\mathcal{V}_K}k_{q,v})$-linear morphism on $\widetilde{M}\otimes_{\mathcal{V}_K}k_{q,v}$.

Let G be a closed algebraic subgroup of $GL(M)$. By Chevalley's theorem, G is the stabilizer of a one dimensional sub-$K(x)$-vector space L in a finite sum $\oplus_h T^{i_h,j_h}(M)$. Up to enlarging $\mathcal{F}$ a little, there exists an $\mathcal{F}$-free module $\widetilde{L}$, such that $L \cong \widetilde{L} \otimes_{\mathcal{F}} K(x)$.

Definition 2.1.1. *The closed algebraic subgroup G of $GL(M)$ contains $\Phi_q^{\kappa_v}$ for almost all $v \in \Sigma_f$ if, for almost every finite place v, $\widetilde{L} \otimes_{\mathcal{V}_K} k_{v,q}$ is stable by $\Phi_q^{\kappa_v}$ in $\oplus_h T^{i_h,j_h}(\widetilde{M}) \otimes_{\mathcal{V}_K} k_{v,q}$.*

Remark 2.1.2. We notice that the notion of an algebraic group over $K(x)$ containing $\Phi_q^{\kappa_v}$ for almost all $v \in \Sigma_f$ is well defined:

Independence of the choice of $\mathcal{F}$ and $\widetilde{L}$: let $\widetilde{L}'$ and $\mathcal{F}'$ be a different choice for $\widetilde{L}$ and $\mathcal{F}$ in the previous definition. Then there exists a third $\mathcal{V}_K$-algebra $\mathcal{F}''$ of the same form with $\mathcal{F}, \mathcal{F}' \subset \mathcal{F}''$. So by extension of scalars, we may suppose that $\mathcal{F} = \mathcal{F}'$ and that $\widetilde{L}$ and $\widetilde{L}'$ are two different $\mathcal{F}$-lattices of L. By enlarging $\mathcal{F}$, we may suppose that there exists an $\mathcal{F}$-linear isomorphism $\psi : \widetilde{L} \longrightarrow \widetilde{L}'$. For almost all $v \in \Sigma_f$ the morphism ψ induces a $(\mathcal{F} \otimes_{\mathcal{V}_K} k_{q,v})$-linear isomorphism $\widetilde{L} \otimes_{\mathcal{V}_K} k_{q,v} \longrightarrow \widetilde{L}' \otimes_{\mathcal{V}_K} k_{q,v}$ commuting to the action of $\Phi_q^{\kappa_v}$.

Independence of the choice of L: it follows by the fact that $\widetilde{L}$ is a direct factor of a $\mathcal{F}$-lattice of $\oplus_h T^{i_h,j_h}(M)$, hence any $\mathcal{F} \otimes_{\mathcal{V}_K} k_{q,v}$-linear automorphism $\oplus_h T^{i_h,j_h}(\widetilde{M}) \otimes_{\mathcal{V}_K} k_{v,q}$ stabilizing $\widetilde{L} \otimes_{\mathcal{V}_K} k_{q,v}$ comes from an $\mathcal{F}$-linear automorphism of $\oplus_h T^{i_h,j_h}(\widetilde{M})$ stabilizing $\widetilde{L}$.

Lemma 2.1.3. *The smallest closed algebraic subgroup G_{Φ^κ} of $GL(M)$ which contains $\Phi_q^{\kappa_v}$ for almost all $v \in \Sigma_f$ exists.*

Proof. Let G_1 and G_2 be two closed algebraic subgroup of $GL(M)$ containing $\Phi_q^{\kappa_v}$ for almost all v. Let G_1 (resp. G_2) be defined as the stabilizer of a line L_1 (resp. L_2) in some $\oplus_h T^{i_h,j_h}(M)$. Then the intersection of G_1 and G_2 is the algebraic group stabilizing the lines L_1 and L_2, or equivalently the line $\wedge^2(L_1 \oplus L_2)$ (*cf.* [W, A2]). This implies that the intersection of two algebraic subgroups of $GL(M)$ containing the $\Phi_q^{\kappa_v}$ for almost all $v \in \Sigma_f$ is still an algebraic subgroup of $GL(M)$ containing the κ_v-curvature for almost all $v \in \Sigma_f$, in the sense of definition (2.1.1).

Moreover $GL(M)$ is an algebraic variety of finite dimension, hence any descending chain of closed algebraic subgroups containing the $\Phi_q^{\kappa_v}$ for almost all $v \in \Sigma_f$ is stationary. ∎

Lemma 2.1.4. *Let $\mathcal{N} = (N, \Phi_q)$ be an object of $<\mathcal{M}>^{\otimes}$. Then the natural morphism*

$$\Omega_{\Phi^\kappa} : G_{\Phi^\kappa}(\mathcal{M}) \longrightarrow G_{\Phi^\kappa}(\mathcal{N})$$

is surjective.

Proof. Since the action of Φ_q on $\mathcal{N}$ is induced by the action of Φ_q on $\mathcal{M}$, the image of natural morphism $\Omega_{\Phi^\kappa} : G_{\Phi^\kappa}(\mathcal{M}) \longrightarrow GL(\mathcal{N})$ contains $\Phi_q^{\kappa_v}$ for almost all v, hence contains $G_{\Phi^\kappa}(\mathcal{N})$.

Let us choose a line L in some finite sum $\oplus_h T^{i_h,j_h}(N)$, such that $G_{\Phi^\kappa}(\mathcal{N})$ is the stabilizer of L. Let $\widetilde{L}$ be an $\mathcal{F}$-lattice of L, defined over a q-difference algebra $\mathcal{F} \subset K(x)$ essentially of finite type over $\mathcal{V}_K$. Since $\mathcal{N}$ is an object of $<\mathcal{M}>^{\otimes}$, L is a line in a suitable subquotient of a finite sum $\oplus_l T^{i_l,j_l}(M)$. Since $\widetilde{L} \otimes_{\mathcal{V}_K} k_{v,q}$ is stable by $\Phi_q^{\kappa_v}$ for almost all v, L is stabilized by

$G_{\Phi^\kappa}(\mathcal{M})$, by construction of $G_{\Phi^\kappa}(\mathcal{M})$. It follows that the image of Ω_{Φ^κ} is precisely $G_{\Phi^\kappa}(\mathcal{N})$. ■

2.2. Statement of the main theorem.

Main theorem 2.2.1. *The algebraic group $Gal(\mathcal{M},\eta)$ is the smallest closed subgroup of $GL(M)$ containing $\Phi_q^{\kappa_v}$ for almost all $v \in \Sigma_f$.*

Example. Let us consider the q-difference equation $y(qx) = q^{1/2}y(x)$, associated to the q-difference module:

$$\begin{array}{rccc} \Phi_q : & K(x) & \longrightarrow & K(x) \\ & f(x) & \longmapsto & q^{1/2}f(qx) \end{array} .$$

The q-difference module $(K(x),\Phi_q)$ is trivial over $K(x^{1/2})$, hence the generic Galois group of $(K(x),\Phi_q)$ is the group $\mu_2 = \{1,-1\}$. For all v such that $|q|_v = 1$ and that the image of $q^{1/2}$ is an element of the cyclic group generated by the image of q in $k_{q,v}$, the module $(K(x),\Phi_q)$ has κ_v-curvature zero. For every other v such that $|q|_v = 1$, we have $\phi_q^{2\kappa_v} \equiv 1$ over $k_{q,v}$, which means that $\phi_q^{\kappa_v} = \pm 1$. So the Galois group is the smallest algebraic subgroup of the multiplicative group $K(x)^\times \cong GL(K(x))$ containing $\Phi_q^{\kappa_v}$ for almost all v.

The proof of the last statement relies on the q-analogue of Grothendieck's conjecture on p-curvatures proved in [DVIII], that we are going to recall in the following section.

A part of the statement is very easy to prove:

Proposition 2.2.2. *The algebraic group $Gal(\mathcal{M},\eta)$ contains the $\Phi_q^{\kappa_v}$ for almost all $v \in \Sigma_f$.*

Proof. The algebraic group $Gal(\mathcal{M},\eta)$ is defined as the stabilizer of a q-difference module L of rank one over $K(x)$. The choice of an $\mathcal{F}$-lattice $\widetilde{M}$ of M determines an $\mathcal{F}$-lattice $\widetilde{L}$ of L of rank one. The reduction over $k_{q,v}$ of $\widetilde{L}$ is stable by the morphism induced by $\Phi_q^{\kappa_v}$ since $\widetilde{L}$ is a q-difference module, hence stable under Φ_q. ■

3. The q-analogue of Grothendieck's conjecture on p-curvatures.

We recall that K is a number field, $\mathcal{V}_K$ its ring of integers, q a non zero element of K which is not a root of unity and that, for almost every v, κ_v is the order of the image of q in the residue field of K with respect to v.

We consider a q-difference module $\widetilde{\mathcal{M}} = (\widetilde{M},\widetilde{\Phi}_q)$ over a q-difference algebra $\mathcal{F} \subset K(x)$ essentially of finite type over $\mathcal{V}_K$, and we denote $\mathcal{M} = \widetilde{\mathcal{M}}_{K(x)}$ the q-difference module obtained by $\widetilde{\mathcal{M}}_{K(x)}$ by extension of coefficients from $\mathcal{F}$ to $K(x)$.

Theorem 3.0.3. [DVIII, (7.1)] *The q-difference module $\mathcal{M}$ is trivial if and only if $\Phi_q^{\kappa_v}$ induces the identity on $\widetilde{M} \otimes_{\mathcal{V}_K} k_{v,q}$.*

4. Proof of the main theorem.

Let $\mathcal{M} = (M, \Phi_q)$ be a q-difference module over $K(x)$ and let $Gal(\mathcal{M}, \eta)$ be its generic Galois group. We denote by $G_{\Phi^\kappa}(\mathcal{M})$ the smallest algebraic subgroup of $GL(M)$ containing $\Phi_q^{\kappa_v}$ for almost all v. Our purpose is to prove that $Gal(\mathcal{M}, \eta) = G_{\Phi^\kappa}(\mathcal{M})$ (*cf.* (2.2.1)).

We recall that we have already proved that $G_{\Phi^\kappa} \subset Gal(\mathcal{M}, \eta)$ in (2.2.2).

We choose a $K(x)$-vector space L of dimension 1 in a finite sum of the form $\oplus_h T^{i_h, j_h}(M)$, such that $G_{\Phi^\kappa}(\mathcal{M})$ is the stabilizer of L.

We denote by $\mathcal{W} = (W, \Phi_q)$ the smallest q-difference sub-module of $\oplus_h T^{i_h, j_h}(M)$ containing L.

Let $\mathcal{F} \subset K(x)$ be a q-difference algebra essentially of finite type and $\widetilde{M}$ an $\mathcal{F}$-lattice of M, stable by Φ_q. Let m be a basis of the $\mathcal{F}$-lattice $\widetilde{L}$ of L determined by $\widetilde{M}$. Then m is a cyclic vector for a suitable $\mathcal{F}$-lattice $\widetilde{W}$ of W. For almost all $v \in \Sigma_f$, $\widetilde{L} \otimes_{\mathcal{V}_K} k_{q,v}$ is stable with respect to the morphism induced by $\Phi_q^{\kappa_v}$, which means that:

$$\Phi_q^{\kappa_v}(m) \equiv \alpha_v(x) m \text{ in } \widetilde{L} \otimes_{\mathcal{V}_K} k_{q,v}, \text{ with } \alpha_v(x) \in \mathcal{F} \otimes_{\mathcal{V}_K} k_{q,v}.$$

If ν is the rank of W, we obtain:

$$\Phi_q^{\kappa_v}(m, \Phi_q(m), \ldots, \Phi_q^{\nu-1}(m)) \equiv (m, \Phi_q(m), \ldots, \Phi_q^{\nu-1}(m)) \begin{pmatrix} \alpha_v(x) & & 0 \\ & \ddots & \\ 0 & & \alpha_v(q^{\nu-1}x) \end{pmatrix} \text{ in } \widetilde{W} \otimes_{\mathcal{V}_K} k_{q,v}.$$

We deduce that the reduction modulo $\varpi_{v,q}$ of the sub-$\mathcal{F}$-module of $\widetilde{W}$ generated by $\Phi_q^i(m)$, for any $i = 0, \ldots, \nu - 1$, is stable by $\Phi_q^{\kappa_v}$, for almost all v. This implies that the $K(x)$-vector space generated by $\Phi_q^i(m)$, for any $i = 0, \ldots, \nu - 1$, is stable by $G_{\Phi^\kappa}(\mathcal{M})$. Let us call U the sub-$K(x)$-vector space of W generated by $(\Phi_q(m), \ldots, \Phi_q^{\nu-1}(m))$. Then $W = L \oplus U$ is a decomposition of W in subspaces stable by $G_{\Phi^\kappa}(\mathcal{M})$. Let us consider the dual decomposition of $\check{W}$: $\check{W} = \check{L} \oplus \check{U}$. It follows that $G_{\phi^\kappa}(\mathcal{M})$ is the group fixing the line $L \otimes \check{L}$ in $W \otimes \check{W}$ (*cf.* for instance the proof of theorem [D, 3.1]).

Let us consider the line $L \otimes \check{L}$ instead of the line L to define $G_{\phi^\kappa}(\mathcal{M})$ as a stabilizer. Then we are in the following situation: $G_{\phi^\kappa}(\mathcal{M})$ is the group fixing the line L and $\mathcal{W} = (W, \Phi_q)$ is the smallest q-difference module containing L. The $\mathcal{F}$-lattice $\widetilde{L}$ of L is direct factor in a suitable $\mathcal{F}$-lattice of $\oplus_h T^{i_h, j_h}(M)$, hence $\widetilde{L} \otimes_{\mathcal{V}_K} k_{v,q}$ is fixed by $\Phi_q^{\kappa_v}$, for almost all $v \in \Sigma_f$:

$$\Phi_q^{\kappa_v}(m) \equiv m \text{ in } \widetilde{L} \otimes_{\mathcal{V}_K} k_{q,v}, \text{ for all } m \in \widetilde{L}.$$

Let us fix a cyclic vector $m \in \widetilde{L}$ for $\widetilde{W}$. Then we have:

$$\Phi_q^{\kappa_v}(m, \Phi_q(m), \ldots, \Phi_q^{\nu-1}(m)) \equiv (m, \Phi_q(m), \ldots, \Phi_q^{\nu-1}(m)) \mathbb{I}_\nu \text{ in } \widetilde{W} \otimes_{\mathcal{V}_K} k_{q,v}.$$

By (3.0.3), the q-difference module $\mathcal{W}$ is trivial and hence $Gal(\mathcal{W},\eta)=1$. Since $\mathcal{W}\in<\mathcal{M}>^{\otimes}$, we have a natural morphism

$$Gal(\mathcal{M},\eta)\longrightarrow Gal(\mathcal{W},\eta)=1\ ,$$

which prove that $Gal(\mathcal{M},\eta)$ stabilizes each line of W. In particular $Gal(\mathcal{M},\eta)$ stabilizes L, hence $Gal(\mathcal{M},\eta)=G_{\phi^\kappa}(\mathcal{M})$. This achieves the proof.

5. Examples of calculation of generic Galois groups.

We conclude by some examples of arithmetic calculations of the generic Galois group.

Example 5.0.4. Let us consider the q-difference equation

$$\begin{pmatrix} y_1(qx)\\ y_2(qx)\end{pmatrix}=\begin{pmatrix}1 & a(x)\\ 0 & b(x)\end{pmatrix}\begin{pmatrix} y_1(x)\\ y_2(x)\end{pmatrix}\ , \tag{5.0.4.1}$$

with $a(x)\neq 0$. Then for all positive integers n we obtain:

$$\begin{pmatrix} y_1(q^nx)\\ y_2(q^nx)\end{pmatrix}=\begin{pmatrix}1 & *\\ 0 & b(q^{n-1}x)\cdots b(x)\end{pmatrix}\begin{pmatrix} y_1(x)\\ y_2(x)\end{pmatrix}\ .$$

Let us consider the q-difference modules $\mathcal{M}$ generated by (e_1,e_2) with

$$\Phi_q(e_1,e_2)=(e_1,e_2)\begin{pmatrix}1 & 0\\ a(x) & b(x)\end{pmatrix}\ .$$

Then the q-difference linear system (5.0.4.1) is associated to $\mathcal{M}$ with respect to the basis $\underline{e}$. We can distinguish several cases:
1) *$y(qx)=b(x)y(x)$ has a solution in $K(x)$*
Then the generic Galois group of $\mathcal{M}$ is:

$$Gal(\mathcal{M},\eta)=\left\{\begin{pmatrix}1 & 0\\ c(x) & 1\end{pmatrix}\ :\ c(x)\in K(x)\right\}\ .$$

2) *the equation $y(qx)=b(x)y(x)$ has a solution in an extension $K(q^{1/d})(x^{1/d})$ of $K(x)$*,
for a suitable integer $d>1$. We choose d minimal with respect this property. We obtain:

$$Gal(\mathcal{M},\eta)=\left\{\begin{pmatrix}1 & 0\\ c(x) & \zeta\end{pmatrix}\ :\ c(x)\in K(x),\zeta\in\mu_d\right\}\ .$$

3) *none of the previous conditions is satisfied*.

We find the algebraic group:

$$Gal(\mathcal{M},\eta)=\left\{\begin{pmatrix}1 & 0\\ c(x) & d(x)\end{pmatrix}\ :\ c(x),d(x)\in K(x),d(x)\neq 0\right\}\ .$$

Example 5.0.5.
Let us consider the q-difference linear system of order two:

$$\begin{pmatrix} y_1(qx) \\ y_2(qx) \end{pmatrix} = \begin{pmatrix} 0 & r(x) \\ 1 & 0 \end{pmatrix} \begin{pmatrix} y_1(x) \\ y_2(x) \end{pmatrix} ,$$

with $r(x) \in K(x)$ and $r(x) \neq 0$. We can easily calculate by induction that for all positive integers n we have:

$$\begin{pmatrix} y_1(q^{2n}x) \\ y_2(q^{2n}x) \end{pmatrix} = \begin{pmatrix} r(q^{2n-1}x)\cdots r(q^3x)r(qx) & 0 \\ 0 & r(q^{2n-2}x)\cdots r(q^2x)r(x) \end{pmatrix} \begin{pmatrix} y_1(x) \\ y_2(x) \end{pmatrix}$$

and

$$\begin{pmatrix} y_1(q^{2n+1}x) \\ y_2(q^{2n+1}x) \end{pmatrix} = \begin{pmatrix} 0 & r(q^{2n}x)\cdots r(q^2x)r(x) \\ r(q^{2n-1}x)\cdots r(q^3x)r(qx) & 0 \end{pmatrix} \begin{pmatrix} y_1(x) \\ y_2(x) \end{pmatrix} .$$

It follows that for the generic Galois group of the q-difference module $\mathcal{M}$ of rank 2 such that for a fixed basis (e_1, e_2) we have:

$$\Phi_q(e_1, e_2) = (e_1, e_2) \begin{pmatrix} 0 & 1 \\ r(x) & 0 \end{pmatrix}$$

there are two possibilities:
1) *$y(q^2x) = r(x)y(x)$ has a solution in $K(x)$*
Then $\Phi_q^{2\kappa_v} \equiv 1$ modulo $\varpi_{q,v}$ for almost all v and the generic Galois group of $\mathcal{M}$ is represented as the algebraic linear subgroup $Gl_2(K(x))$ of the form:

$$Gal(\mathcal{M}, \eta) = \left\{ \mathbb{I}_2, -\mathbb{I}_2, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \right\} .$$

2) *$y(q^2x) = r(x)y(x)$ has a solution in an extension $K(q^{2/d})(x^{1/d})$ of $K(x)$*,
for a suitable integer $d > 1$. We choose d minimal with respect this property. Then:

$$Gal(\mathcal{M}, \eta) = \left\{ \begin{pmatrix} \zeta_1 & 0 \\ 0 & \zeta_2 \end{pmatrix} \ : \ \zeta_1, \zeta_2 \in \mu_d \right\} \cup \left\{ \begin{pmatrix} 0 & \zeta_3 \\ \zeta_4 & 0 \end{pmatrix} \ : \ \zeta_3, \zeta_4 \in \mu_d \right\} .$$

3) *none of the previous conditions is satisfied.*

then the generic Galois group of $\mathcal{M}$ is represented as the infinite algebraic linear subgroup $Gl_2(K(x))$ of the form:

$$Gal(\mathcal{M}, \eta) = \left\{ \begin{pmatrix} a(x) & 0 \\ 0 & b(x) \end{pmatrix} \ : \ a(x), b(x) \in K(x), a(x)b(x) \neq 0 \right\}$$
$$\cup \left\{ \begin{pmatrix} 0 & c(x) \\ d(x) & 0 \end{pmatrix} \ : \ c(x), d(x) \in K(x), c(x)d(x) \neq 0 \right\} .$$

Moreover this example shows that we can have $Gal(\mathcal{M}_2) \neq Gal(\mathcal{M}, \eta)$, since $Gal(\mathcal{M}_2)$ is represented as a diagonal matrix.

References.

[A1] André Y.: "Sur la conjecture des p-courbures de Grothendieck-Katz", Institut de Mathématiques de Jussieu, preprint 134, octobre 1997.

[A4] André Y.: "Différentielles non-commutatives et théorie de Galois différentielle ou aux différences", to appear in Annals Scient. Éc. Norm. Sup..

[DVIII] Di Vizio L.: "Arithmetic theory of q-difference equations I. The q-analogue of Grothendieck's conjecture on p-curvatures. ", in preparation.

[D] Deligne P.: "Hodge cycles on abelian variety", Springer Lecture Notes 900 (1982), 9-100.

[DM] Deligne P., Milne J.: "Tannakian categories", Springer Lecture Notes 900 (1982), 101-228.

[GR] Gasper G., Rahman M.: "*Basic hypergeometric series*", Cambridge Univ. Press, Cambridge, 1990.

[H] Hendriks P. A.: "Algebraic Aspects of Linear Differential and Difference Equations", Ph. D. thesis, University of Groningen, 1996.

[K1] Katz N. M.: "Algebraic solution of differential equations (p-curvature and Hodge Filtration)", Invent. Math. 18, (1972), 1-118.

[K2] Katz N. M.: "A conjecture in the arithmetic theory of differential equations", Bull. S.M.F. 110, (1982), 203-239, and Bull. S.M.F. 111, (1982), 347-348.

[K3] Katz N. M.: "On the calculation of some differential Galois groups", Invent. math. 87, 13-61 (1987).

[PS] van der Put M., Singer M. F.: "*Galois Theory of Difference Equations*", Lecture Notes in Mathematics 1666, Springer, 1997.

[W] Waterhouse W.C.: "*Introduction to Affine Group Schemes*", Springer, Graduate Texts in Mathematics 66, 1979.