Iterative q difference Galois theory

Charlotte Hardouin (IWR)

Leeds, June 2007

Iterative q-difference rings

Let C, be an algebraically closed field and let $q \neq 1$ be an element of C. Let $F = C(t)$ be the field of rational functions over C and let σ_q be the automorphism of F given by $\sigma_q(f)(t) = f(qt)$.

q-arithmetical properties

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

1. *Let us denote by $[k]_q!$ the element of C defined by $[k]_q[k-1]_q...[1]_q$. We will say that $[k]_q!$ is the q-factorial of k.*
2. *Let us denote by $\binom{r}{k}_q$ the element of C defined by $\frac{[r]_q!}{[k]_q![(r-k)]_q!}$. We will say that $\binom{r}{k}_q$ is the q-binomial coefficient of r to k.*

Iterative q-difference ring

Definition 2 *Let R be a q-difference ring extension of F and let $\delta_R^* := (\delta_R^{(k)})_{k\in\mathbb{N}}$ be a collection of maps from R to R. The family δ_R^* is called an* ***iterative q-difference*** *of R, if all the following properties are satisfied*

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

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

Iterative q-difference modules

For now on q denotes a n-th primitive root of unity.

Definition 3 *Let (R, δ_R^*) be an iterative q-difference ring. Let M be a free R-module of finite type over R. We will say that (M, δ_M^*) is an iterative q-difference module if there exists a family of map $\delta_M^* = (\delta_M^{(k)})_{k \in \mathbb{N}}$, such that for all $i, j, k \in \mathbb{N}$:*

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

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

Theorem 4 *Let (L, δ_L^*) be ID_q field. Then $IDM_q(L)$ is a neutral Tannakian category over L. The unit object is (L, δ_L^*).*

Iterative q-difference equation(ID_qE)

Notations 5 *Let (L, δ_L^*) be an iterative q-difference field. If,*

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

Proposition 6 *Let $M \in IDM_q(L)$ of dimension m and let $B_0 = \{b_1, ..., b_m\}$ be a basis of M. Then, there exist $\{A_k \in M_m(L)\}_{k\in\mathbb{N}}$ such that the following statements are equivalent :*

1. *For all $\mathbf{y} \in L^m$ s.t $B_0.\mathbf{y} = \sum_{i=1}^m y_i b_i \in V_M = \cap_{k\in\mathbb{N}^*} Ker(\delta_M^{(k)})$.*
2. *$\delta_L^{(k_C)}(\mathbf{y}) = A_k\mathbf{y},\ \forall k \in \mathbb{N}$.*

Definition 7 *The family of equations*

$$\{\delta_L^{(k_C)}(\mathbf{y}) = A_k\mathbf{y}\}_{k\in\mathbb{N}}$$

related to the IDM_q-module (M, δ_M^*) in proposition 6 is called an ***iterative q-difference equation****(ID_qE).*

Iterative q-difference Picard-Vessiot extensions

Definition 8 *Let (L, δ_L^*) be an iterative q-difference field, and let (M, δ_M^*) be an object of $IDM_q(L)$ and let $\{\delta_L^{(k_C)}(\mathbf{y}) = A_k\mathbf{y}\}_{k\in\mathbb{N}}$ be an **iterative q-difference equation** related to the IDM_q-module (M, δ_M^*), denoted by $IDE_q(M)$.*
*Let (R, δ_R^*) be an iterative q-difference extension of (L, δ_L^*). A matrix $Y \in Gl_n(R)$ is called a **fundamental solution matrix** for $ID_qE(M)$ if $\delta_R^{(k_C)}(Y) = A_kY,\ \forall k \in \mathbb{N}$.*

*The ring R is called an **iterative q-difference Picard-vessiot ring** for $IDqE(M)$ (IPV_q-ring) if it fulfills the following conditions :*

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

Existence of Picard-Vessiot Rings and Iterative Galois groups

Theorem 9 *Let (L, δ_L^*) be an ID_q field with $C := C(L)$ algebraically closed and $(M, \delta_M^*) \in IDM_q(L)$ with ID_qE : $\delta_L^{(k_C)}(\mathbf{y}) = A_k\mathbf{y}$. Then, there exists an iterative q-difference Picard-Vessiot ring for the iterative q-difference equation which is unique up to iterative q-difference isomorphism.*

Let F be an algebra over C and let (S, δ_S^*) be a q-iterative difference ring we define an iterative q-difference on $S \otimes_C F$ by setting $\delta_{S \otimes_C F}^{(k)}(s \otimes f) := \delta_S^{(k)}(s) \otimes f$ for all $k \in \mathbb{N}$. Till the end, every object of the previous kind will be endow with this iterative q-difference structure

Galois group scheme

Definition 10 (Definition proposition) *Let us define the functor*

$$\underline{Aut}(R/L): \qquad .$$

$$(Algebras/C) \longrightarrow (Groups)$$

$$F \longrightarrow Aut_{ID_q}(R \otimes_C F / L \otimes_C F)$$

The functor $\underline{Aut}(R/L)$ *is representable by a certain affine group-scheme of finite type over* C*. We call this affine group scheme* $\underline{Aut}(R/L)$ *the* ***Galois group scheme*** $\underline{Gal}(R/L)$ *of* R *over* L*.*

Proposition 11 *let* R/L *be an iterative* q*-difference Picard-Vessiot ring over* L *and* $\mathcal{G} := \underline{Gal}(R/L)$ *the Galois group scheme of* R*. Then* $Spec(R)$ *is a* $\mathcal{G}_L$*-torsor.*

Proposition 12 *Structure of the iterative q-difference ring*
Let R/L be an iterative q-difference Picard-Vessiot ring over L. Then, there exists idempotents $e_1, .., e_s \in R$ such that

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

Example of iterative q-difference Galois group

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

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

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

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

Theorem 13 *Let M be as above with its associated ID_qE. Let $\alpha = \sum_{l\geq 0} a_l p^l \in \mathbb{Q}_p$. Then for an iterative Picard-Vessiot extension R/F for M, we have*

Gal(R/F) $\simeq$ C$_r$ *the finite group of order r of $\mathbb{G}_a(K)$ if $\alpha \in \mathbb{Q}$ and* Gal(R/F) $\simeq \mathbb{G}_a$(K) *if $\alpha \notin \mathbb{Q}$*

Galois correspondence

Theorem 14 (Galois correspondence) *Let R/L be an iterative q-difference Picard-Vessiot ring over L, let E denotes its total iterative q-difference Picard-vessiot extension and let $\mathcal{G} := \underline{Gal}(R/L)$ be the Galois group scheme of R.*

1) Then there is an antiisomorphism of lattices between :

$\mathfrak{H} := \{\mathcal{H}|\mathcal{H} \subset \mathcal{G}$ *closed subgroup schemes of* $\mathcal{G}\}$

and

$\mathfrak{T} := \{T|L \subset T \subset E$ *intermediate IDq ring*

s.t any non zero divisor of T is a unit of T$\}$

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

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

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