Algebraic aspects of linear differential and difference equations
Hendriks, Peter Anne

IMPORTANT NOTE: You are advised to consult the publisher's version (publisher's PDF) if you wish to cite from it. Please check the document version below.

Document Version
Publisher's PDF, also known as Version of record

Publication date:
1996

Link to publication in University of Groningen/UMCG research database

Citation for published version (APA):

Copyright
Other than for strictly personal use, it is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license (like Creative Commons).

Take-down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Downloaded from the University of Groningen/UMCG research database (Pure): http://www.rug.nl/research/portal. For technical reasons the number of authors shown on this cover page is limited to 10 maximum.
Chapter 6

On the classification of a class of $q$-difference equations

6.1 Introduction

Let $q$ be an $m$ th root of unity. The aim of this article is to classify the $q$-difference equations over the field $K = \mathbb{C}(z)$. The classification is rather similar to the classification of differential and difference equations in characteristic $p$. See [Put95] and [PS96]. Further some Picard–Vessiot theory will be developed for these equations.

6.2 Picard–Vessiot Theory

Let $\phi : \mathbb{C}(z) \to \mathbb{C}(z)$ be an $\mathbb{C}$-linear automorphism given by $\phi(z) = qz$, where $q$ is an $m$ th root of unity. Consider the system of difference equation $(A) : \phi y = Ay$, where $A \in \text{Gl}(n, \mathbb{C}(z))$. (We restrict ourselves to equations with $A \in \text{Gl}(n, \mathbb{C}(z))$ in order to guarantee that we get $n$ independent solutions.

**Definition 6.2.1** A ring $R$ together with an automorphism $\phi_R : R \to R$ is called a Picard–Vessiot extension over $\mathbb{C}(z)$ associated with system $(A)$ if

1. $R$ is a commutative ring, $R \subseteq \mathbb{C}(z)$ and $\phi_R|_{\mathbb{C}(z)} = \phi$.

2. The only $\phi_R$–invariant ideals of $R$ are 0 and $R$

3. There exists a matrix $U \in \text{Gl}(n, R)$ such that $\phi_R(U) = AU$. (Such a matrix $U$ is called a fundamental matrix for the system $(A)$.)

4. $R$ is minimal with respect to the conditions 1, 2 and 3 or equivalently if $U = (u_{ij}) \in \text{Gl}(n, R)$ is a fundamental matrix for the matrix for the system $(A)$ then $R = \mathbb{C}(z)[u_{11}, \ldots, u_{nn}, \frac{1}{\det(U)}]$. 

91
From now on we will denote $\phi_R$ also by $\phi$. For a given system of $q$-difference equations $(A) : \phi y = Ay$ one can construct a Picard–Vessiot extension in the following way. Let $(x_{ij})$ denote a matrix of indeterminates and let $\det$ denote the determinant of this matrix. On the $C(z)$-algebra $C(z)[x_{ij}, \frac{1}{\det}]$ one extends the automorphism $\phi$ by setting $\phi(x_{ij}) = A(x_{ij})$. Let $I$ be an ideal of $C(z)[x_{ij}, \frac{1}{\det}]$, which is maximal among the proper $\phi$-invariant ideals. Then $C(z)[x_{ij}, \frac{1}{\det}]/I$ is a Picard–Vessiot ring for the system of equations $(A)$. Any Picard–Vessiot ring is of this form.

Unlike the case, where $q$ is not a root of unity, there is no uniqueness of Picard–Vessiot rings, due to the fact that in our case the field of constants $C(z^m) \subset C(z)$ is not algebraically closed. For instance assume that $q = 1$ and consider the first order equation $\phi(y) = -y$. Then $R_c := C(z)[u, u^{-1}]/(u^2 - c)$ is a Picard–Vessiot ring for all $c \in C(z)^*$, because if $c \in C(z)^*$ is a square then the only nontrivial ideals are generated by the cosets of $u - \sqrt{c}$ and $u + \sqrt{c}$ and these ideals are not $\phi$-invariant. We have $R_{c_1} \cong R_{c_2}$ if and only if $\frac{c_1}{c_2} \in C(z)^*$ is a square and this is not always the case.

If $q$ is not a root of unity, then there is a unique (up to $C$-linear isomorphisms commuting with $\phi$) Picard–Vessiot extension associated to every system of $q$-difference equations. See [PS96]. Then the $q$-difference Galois group of an equation is the group of $C$-linear automorphisms of the Picard–Vessiot ring commuting with $\phi$. Unfortunately in our case there is not a unique Picard–Vessiot ring for every system of $q$-difference equations. Hence it is not possible to define a $q$-difference Galois group of an equation in this way. However in section 4 we will use the theory of Tannakian categories for a suitable definition of the $q$-difference Galois group. The idea is to compare $q$-difference modules over $C(z)$ with modules over the ring $Z = L[t, t^{-1}]$, where $L$ is the field of constants $C(z^m)$, because modules over $Z = L[t, t^{-1}]$ are easier to understand.

To a system of $q$-difference equations one can associate a $q$-difference module. If a difference equation $\phi y = Ay$ with $A \in Gl(n, C(z))$ is given then one defines a $q$-difference module structure on $C(z)^n$ by setting $\Phi y = A^{-1} \phi y$. We have $\Phi a y = \phi(a) \Phi y$ if $a \in C(z)$. In the next section we will classify the $q$-difference modules over the field $C(z)$ if $q$ is a root of unity.

### 6.3 Classification of $q$-Difference Modules

Let $q$ be an $m$th root of unity and let $D$ be the skew Laurent polynomial ring $C(z)[\Phi, \Phi^{-1}]$, where the multiplication is fixed by the rule $\Phi z = qz\Phi$. In this section we will classify the left $D$-modules which have finite dimension over $C(z)$.

**Lemma 6.3.1** Let $Z$ be the center of $D$. Then

1. $Z = C(z^m)[\Phi^m, \Phi^{-m}]$ is a commutative Laurent polynomial ring.
2. $D$ is a free $Z$-module of rank $m^2$. 

92
3. Let $\text{Quot}(Z)$ denote the field of quotients of $Z$. Then $\text{Quot}(Z) \otimes_{Z} \mathcal{D}$ is a skew field with center $\text{Quot}(Z)$ and dimension $m^2$ over its center.

**Proof.**

1. For all integers $j \in \mathbb{Z}$ one has $\Phi^{j}z = q^{j}z\Phi^{j}$. This implies that $\Phi^{j} \in Z$ if and only if $j$ is a multiple of $m$. Further one has $\Phi^{j}z = q^{j}z\Phi$. Hence $z^{j} \in Z$ if and only if $j$ is a multiple of $m$. So we have $Z \supseteq C(z^{m})[\Phi^{m}, \Phi^{-m}]$. Any $f \in \mathcal{D}$ can be written uniquely as $f = \sum_{0 \leq i,j \leq m} f_{ij}z^{i}\Phi^{j}$ with all $f_{ij} \in C(z^{m})[\Phi^{m}, \Phi^{-m}]$. Suppose that $f \in Z$. Then $0 = zf - fz = \sum_{0 \leq i,j \leq m} (1 - q^{j})f_{ij}z^{i+1}\Phi^{j}$. Hence if $j \neq 0$ then $f_{ij} = 0$ and so $f = \sum_{0 \leq i \leq m} f_{i0}z^{i}$. And $0 = \Phi f - f\Phi = \sum_{0 \leq i \leq m} (q^{i} - 1)f_{i0}z^{i}\Phi$ implies $f = f_{00} \in C(z^{m})[\Phi^{m}, \Phi^{-m}]$. We conclude that $Z = C(z^{m})[\Phi^{m}, \Phi^{-m}]$

2. This is already shown in part 1 of the proof.

3. If $f \in \mathcal{D}$ then one can write $f = \sum_{i \in \mathbb{Z}} f_{i}\Phi^{i}$ with all $f_{i} \in C(z)$. We define the discrete valuation $v$ by $v(f) = \max\{k \mid f_{k} \neq 0\}$ and $v(0) = -\infty$. We have $v(fg) = v(f) + v(g)$. Hence $\mathcal{D}$ and $\text{Quot}(Z) \otimes_{Z} \mathcal{D}$ have no zero divisors and $\text{Quot}(Z) \otimes_{Z} \mathcal{D}$ must be a skew field with center $\text{Quot}(Z)$ and dimension $m^2$ over its center. □

**Lemma 6.3.2** Let $\mathfrak{m}$ denote a maximal ideal of $Z$ with residue field $L = Z/\mathfrak{m}$. Then $\mathcal{D}/\mathfrak{m}\mathcal{D} = L \otimes_{Z} \mathcal{D}$ is isomorphic to the matrix ring $M(m \times m, L)$.

**Proof.** First we will prove that $L \otimes_{Z} \mathcal{D}$ is a central simple algebra over $L$ with dimension $m^2$ over its center. Let $I \neq 0$ be a two-sided ideal of $L \otimes_{Z} \mathcal{D}$. We must show that $I$ is the unit ideal. Suppose $f \in I$ and $f \neq 0$. Then $f$ can be written uniquely in the form $f = \sum_{0 \leq i,j \leq m} f_{ij}z^{i}\Phi^{j}$, where $f_{ij} \in L$ for all $i,j$. Let $f_{1} = f - qz^{-1}fz \in I$. Then $f_{1} = \sum_{0 \leq j \leq m-1} f_{0j}(1 - q^{1+j})$. Note that the $m-1$ th coefficient of $f_{1}$ with respect to $\Phi$ is 0. We define recursively $f_{i} = f_{i+1} - q^{i}z^{-1}f_{i+1}z$. We have $f_{i} \in I$ for all $i$. Let $g_{0} = f_{m-1}$. Then we can write $g_{0} = \sum_{0 \leq i \leq m} a_{i}z^{i}$, where $a_{i} \in L$ for all $i$. We define recursively $g_{i} = g_{i-1} - q^{i}\Phi g_{i-1}\Phi^{-1}$. We have $g_{i} \in I$ for all $i$ and $g_{m-1} \in L$. Hence $I$ is the unit ideal. As in Lemma 6.3.1 one can easily verify that $L$ is the center of $L \otimes_{Z} \mathcal{D}$. The dimension of $L \otimes_{Z} \mathcal{D}$ over $L$ is $m^2$. The classification of central simple algebras tells us that $L \otimes_{Z} \mathcal{D}$ is isomorphic to a matrix algebra $M(d \times d, S)$ over a skew field $S$ containing $L$ with $[S : L] = e^2$ where $n = ed$. But $L$ is a $C_{1}$-field of characteristic 0. This implies that there does not exist such skew field extensions, that is $e = 1$. See [Gre69]. Hence $L \otimes_{Z} \mathcal{D}$ is isomorphic to the matrix ring $M(m \times m, L)$. □
**Theorem 6.3.3** (Classification of irreducible \( \mathcal{D} \)-modules) There is a bijective correspondence between the irreducible left \( \mathcal{D} \)-modules of finite dimension over \( K = \mathbb{C}(z) \) and the maximal ideals of \( Z \).

**Proof.** Suppose \( M \) is an irreducible left \( \mathcal{D} \)-module which has finite dimension over the field \( K \). Then the set \( \{ f \in Z \mid fM = 0 \} \) is a non-trivial ideal generated by some polynomial \( F \). Suppose that \( F \) has a non-trivial factorization \( F = F_1F_2 \). The submodule \( F_1M \) is nonzero and must then be equal to \( M \). Now \( F_2M = F_2F_1M = 0 \) contradicts the definition of \( F \). It follows that \( F \) is an irreducible polynomial. Let \( m \) be the ideal generated by \( F \) and let \( L \) denotes its residue field. We can consider \( M \) as an irreducible \( L \otimes Z \mathcal{D} \)-module and then \( M \) must be isomorphic to a vectorspace of dimension \( m \) with the natural action of the matrix algebra \( M(m \times m, L) \) on it. □

**Lemma 6.3.4** Let \( F \) be an irreducible element of \( Z \) and let \( m \) denote the maximal ideal generated by \( F \). Further let \( \hat{Z}_F \) denote the completion of the localization \( Z_m \). That is \( \hat{Z}_F \) is the projective limit of the rings \( Z/\mathfrak{m}^n \). Then the algebra \( \hat{Z}_F \otimes Z \mathcal{D} \) is isomorphic to \( M(m \times m, \hat{Z}_F) \).

**Proof.** We will denote the image of \( \Phi^n \) in \( Z/\mathfrak{m}^n \) by \( t_n \). By induction we will construct a sequence of elements \( c_n \in Z/\mathfrak{m}^n[\mathfrak{m}] \) such that \( \prod_{i=0}^{n-1} c_n(q^i) = t_n \) and \( c_{n+1} = c_n \mod F^n \) for all \( n \geq 1 \).

The norm map \( N: L[z] \to L \) given by \( c \mapsto \prod_{i=0}^{n-1} c(q^i) \) is surjective because \( L[z] \) is a finite cyclic field extension of \( L \) and \( L \) is a \( C_1 \)-field being a finite field extension of the field \( \mathbb{C}(z^m) \). Hence there exists an element \( c_1 \in Z/\mathfrak{m} \) such that \( N(c_1) = t_1 \). Note that \( c_1 \neq 0 \) because \( t_1 \neq 0 \).

Let \( c_n \in Z/\mathfrak{m}^n \) be constructed. Take some \( d \in Z/\mathfrak{m}^{n+1}[\mathfrak{m}] \) with image \( c_n \) and put \( c_{n+1} = d + F^n f \in Z/\mathfrak{m}^{n+1}[\mathfrak{m}] \). Then \( \prod_{i=0}^{n-1} c_{n+1}(q^i) = \prod_{i=0}^{n-1} d(q^i) + F^n \sum_{i=0}^{m-1} f(q^i) \prod_{j \neq i} d(q^j) \). Because the image of \( t_{n+1} \) in \( Z/\mathfrak{m}^n \) is equal to \( t_n \), we have \( t_{n+1} - \prod_{i=0}^{m-1} d(q^i) = gF^n \) in for a certain \( g \in Z/\mathfrak{m}^{n+1} \). Let \( \tilde{g} \) be the image of \( g \) in \( L \).

Then we want to find an element \( \tilde{f} \in L[z] \) such that \( \sum_{i=0}^{m-1} \tilde{f}(q^i) \prod_{j \neq i} c_i(q^j) = \tilde{g}(z) \). That is always possible. One can take \( \tilde{f} = \left( \prod_{i=0}^{m-1} c_i(q^i) \right)^{-\frac{q}{m}} \). Let \( f \in Z/\mathfrak{m}^{n+1}[\mathfrak{m}] \) be an element such that the image of \( f \) in \( L[z] \) is equal to \( \tilde{f} \). Then \( c_{m+1} = d + F^n f \) satisfies \( \prod_{i=0}^{m-1} c_{m+1}(q^i) = t_{n+1} \).

Let \( t_\infty \in \hat{Z}_F \) be the projective limit of the \( t_n \) and let \( c_\infty \in \hat{Z}_F[z] \) be the projective limit of the \( c_n \). Then \( c_\infty \) satisfies also \( \prod_{i=0}^{m-1} c_\infty(q^i) = t_\infty \). On the free
module $\hat{Z}_F[z]e$ over $\hat{Z}_F[z]$ of rank 1 one defines the operator $\Phi$ by $\Phi e = c_\infty e$. The equality $\prod_{i=0}^{m-1} c_\infty (q^i z) = t_\infty$ implies that $\hat{Z}_F[z]e$ is a left $\hat{Z}_F \otimes Z \mathcal{D}$–module. The natural map

$$\hat{Z}_F \otimes Z \mathcal{D} \to \text{End}_{\hat{Z}_F}(\hat{Z}_F[z]e) \cong M(m \times m, \hat{Z}_F)$$

is a homomorphism of $\hat{Z}_F$–algebras. It is an isomorphism because it is an isomorphism modulo the ideal $m = (F)$. □

**Theorem 6.3.5** (Classification of indecomposable $\mathcal{D}$–modules) There is a bijective correspondence between indecomposable left $\mathcal{D}$–modules of finite dimension over $K = \mathbb{C}(z)$ and the set of powers of the maximal ideals of $Z$.

**Proof.** Let $M$ be an indecomposable left $\mathcal{D}$–module of finite dimension over $K$. The set $\{f \in Z \mid fM = 0\}$ is a non-trivial ideal in $Z$ generated by some polynomial $F$. If $F$ factors as $F_1F_2$ with coprime $F_1$ and $F_2$ then one can write $1 = F_1G_1 + F_2G_2$ and any $m \in M$ can be written as $F_1G_1m + F_2G_2m$. Further $F_1M \cap F_2M = \{0\}$, because $m \in F_1M \cap F_2M$ implies that $m = (F_1G_1 + F_2G_2)m = 0$. Hence $M = F_1M + F_2M$. This contradicts the assumption that $M$ is indecomposable. Hence the annihilator of an indecomposable module must have the form $(F^m)$, where $(F)$ is a monic and irreducible element in $Z$. Therefore any indecomposable left $\mathcal{D}$–module can be identified with an indecomposable finitely generated module over $\hat{Z}_F \otimes \mathcal{D} \cong M(m \times m, \hat{Z}_F)$ (lemma 6.3.4), annihilated by some power of of a monic irreducible polynomial $F \in Z$.

Morita’s theorem gives an equivalence between $\hat{Z}_F$–modules and $M(m \times m, \hat{Z}_F)$–modules. (See [Ren75], theorem 1.3.16 and proposition 1.3.17.) In particular, every finitely generated indecomposable module has the form $I(F^m) := (\hat{Z}_F[z]e)/(F^m) \cong Z/(F^m)[z]e_n$. The structure as left $\mathcal{D}$–module is given by $\Phi(e) = c_\infty e$ and $\Phi(e_n) = c_ne_n$, where $c_n \in Z/(F^m)[z]$ is the image of $c_\infty$. (See the proof of lemma 6.3.4.) □

**Theorem 6.3.6** Every left $\mathcal{D}$–module of finite dimension over $K$ is a finite direct sum $\bigoplus_{F,m} I(F^m)e(F^m)$, where $F$ runs through a set of generators of the different maximal ideals of $Z$ and $m \geq 0$. The numbers $e(F, m)$ are uniquely determined by $M$.

**Proof.** The first statement is an immediate consequence of theorem 6.3.5. The numbers $e(F, m)$ are uniquely determined by $M$ since they can be computed in terms of the dimension over $K$ of the kernels of multiplication with $F^i$ on $M$. □
tensor product $M \otimes_K N$ with the operation of $\Phi$ given by $\Phi(m \otimes n) = \Phi(m) \otimes \Phi(n)$.

Let $L$ be any field and let $FMod_{L[t, t^{-1}]}$ denote the category of the modules over $L[t, t^{-1}]$, which have finite dimension over $L$. For this abelian category we define the tensor product of two monomials $M$ and $N$ as $M \otimes_L N$ with the operation of $t$ given by $t(m \otimes n) = (tm) \otimes (tn)$. This describes the tensor product for the category of $Z$-modules of finite dimension over $C(z^m)$.

**Theorem 6.3.7** (An equivalence of categories) There exists an equivalence $\mathcal{F}$ of the category of $Z$-modules of finite dimension over $C(z^m)$ onto the category of left $D$-modules of finite dimension over $K = C(z)$. Moreover $\mathcal{F}$ is exact, $C(z^m)$-linear and preserves tensor products.

**Proof.** First we define the functor $\mathcal{F}$. Let $\hat{Z}$ denote the completion of $Z$ with respect to the set of all nonzero ideals. Then $\hat{Z} = \prod F$, where the product is taken over a set of polynomials generating the different maximal ideals of $Z$. The modules over $Z$ of finite dimension over $C(z^m)$ coincide with the $\hat{Z}$-modules of finite dimension over $C(z^m)$. Let $D = \hat{Z} \otimes D$. The left $D$-modules of finite dimension over $K$ coincide with the left $D$-modules of finite dimension over $K$. Consider an irreducible polynomial $F \in Z$. By lemma 6.3.4 there exists a left $D$-module $Z_F[z] e_\infty$ with the action of $\Phi$ given by $\Phi e_\infty = e_\infty e_\infty$. We will denote this module by $Q_F$. Let the left $D$-module $\mathcal{Q}$ be the product of all the $Q_F$ where $F$ runs through a set of generators of all the different maximal ideals of $Z$. Then $\mathcal{Q} = \prod_{i=0}^{m-1} (q_i z)$ and the action of $\Phi$ on $\mathcal{Q}$ is given by $\Phi c = ce$ with $c \in \hat{Z}[z]$ satisfying $\prod_{i=0}^{m-1} (q_i z) = t$, where $t \in \hat{Z}$ denotes the image of $\Phi^m$.

For every $Z$-module $M$ of finite dimension over $C(z^m)$ one regards $M$ as a $\hat{Z}$-module and one defines a left $D$-module $\mathcal{F}(M) := M \otimes \mathcal{Q}$. This $D$-module has finite dimension and can also be considered as a left $D$-module of finite dimension. For morphisms $\phi : M \to N$ of $Z$-modules of finite dimension we define $\mathcal{F}(\phi) := \phi \otimes 1 : \mathcal{F}(M) \to \mathcal{F}(N)$. It is clear that $\mathcal{F}$ is a $C(z^m)$-linear functor. From theorem 6.3.6 it follows that $\mathcal{F}$ is bijective on isomorphy classes of objects. The map $\text{Hom}(M_1, M_2) \to \text{Hom}(\mathcal{F}(M_1), \mathcal{F}(M_2))$ is injective. By counting the dimensions of the two vector spaces over $C(z^m)$ one finds that the map is bijective.

We can describe the functor $\mathcal{F}$ in another more convenient way. Namely $\mathcal{F}M = M \otimes_{C(z^m)} C(z)$ with the obvious structure as $\hat{Z}[z]$-module. $\mathcal{F}M$ has finite dimension over $K$. Therefore $\mathcal{F}M$ is also a $\hat{Z}[z]$-module. The structure as left $D$-module is defined by $\Phi (m \otimes f e) = cm \otimes f(qz)e$. We will consider this module as a left $D$-module of finite dimension over $C(z)$. For two $Z$-modules $M_1, M_2$ of finite dimension one defines a $C(z)$-linear isomorphism

\[
(\mathcal{F}M_1) \otimes (\mathcal{F}M_2) = (M_1 \otimes_{C(z^m)} C(z)) \otimes (M_2 \otimes_{C(z^m)} C(z)) \cong (M_1 \otimes_{C(z^m)} M_2) \otimes_{C(z^m)} C(z)
\]

where $\mathcal{F}(M_1 \otimes_{C(z^m)} M_2) = \mathcal{F}(M_1) \otimes_{C(z^m)} \mathcal{F}(M_2)$.

96
by

\[(m_1 \otimes f_1e) \otimes (m_2 \otimes f_2e) \rightarrow (m_1 \otimes m_2) \otimes f_1f_2e.\]

Obviously this is an isomorphism of left \(D\)-modules of finite dimension over \(C(z)\).

\[\square\]

**Definition 6.3.8** The \(m\)-curvature of a \(D\)-module over \(C(z)\) is the \(C(z^m)\)-linear map \(\Phi^m\) on the module \(N\) with \(F(N) = M\). We will call the \(C(z)\)-linear map \(\Phi^m\) on \(M = N \otimes_{C(z^m)} C(z)\) also the \(m\)-curvature.

Consider the system of \(q\)-difference equations \(\phi(y) = Ay\), where \(A \in \text{Gl}(n, C(z))\). Let \(M\) be the \(q\)-difference module associated to this system of \(q\)-difference equations. Then the \(m\)-curvature as a \(C(z)\)-linear map on \(M\) has the matrix \(A^{-1}(q^{m-1}z) \cdots A^{-1}(qz) A^{-1}(z)\).

### 6.4 Tannakian Categories and the \(q\)-Difference Galois Group

In the previous section we have shown that the category \(\text{Diff}_{C(z)}\) of left \(D\)-modules of finite dimension over \(C(z)\) and the category \(\text{Mod}_Z\) of \(Z\)-modules of finite dimension over \(C(z^m)\) are equivalent. First we will take a closer look at the category \(\text{Mod}_Z\).

Now let \(L\) be any field. We want to describe the category \(\text{Mod}_{L[t, t^{-1}]}\) of all \(L[t, t^{-1}]\)-modules of finite dimension over \(L\) in more detail. A module is a finite dimensional vector space \(M\) over \(L\) together with an invertible linear map \(t\). For the terminology of Tannakian categories we refer to [DM82]. The tensor product is already defined in the previous section. The identity object \(1\) is the one dimensional module \(Le\) together with the invertible \(L\)-linear map \(t\) which is given by \(te = e\). The internal \(\text{Hom}\) is given as \(\text{Hom}(M, N) = \text{Hom}_L(M, N)\) with the \(L[t, t^{-1}]\)-structure given by \((tl)(m) = t^{-1}(l(tm))\) for \(l \in \text{Hom}_L(M, N)\) and \(m \in M\). The category \(\text{Mod}_{L[t, t^{-1}]}\) is a rigid, abelian, \(L\)-linear tensor category. Let \(\text{Vect}_L\) denote the category of finite dimensional vector spaces over \(L\) and let \(\omega : \text{Mod}_{L[t, t^{-1}]} \rightarrow \text{Vect}_L\) be the forgetful functor given by \(\omega(M) = M\). That is one forgets the action of \(t\) on \(M\). One can verify that \(\omega\) is a fibre functor. Hence \(\text{Mod}_{L[t, t^{-1}]}\) is a neutral Tannakian category over \(L\). Associated to this neutral Tannakian category there is an affine group scheme over \(L\), which represents the functor \(R \mapsto \text{Aut}^\circ(\omega)(R)\) defined on \(L\)-algebras.

For an object \(M \in \text{Mod}_{L[t, t^{-1}]}\) one can consider the full subcategory \(\{\{M\}\}\) of \(\text{Mod}_{L[t, t^{-1}]}\) generated by \(M\). The objects of this category are the subquotients of the tensor products \(M \otimes \cdots \otimes M \otimes M^* \otimes \cdots \otimes M^*\), where \(M^*\) denotes the dual of \(M\). The restriction of \(\omega\) to \(\{\{M\}\}\) is again a fibre functor. The affine linear group associated to this \(\{\{M\}\}\) is denoted by \(G_M\). In fact \(G_M\) is the smallest linear algebraic subgroup of \(\text{Gl}(M)\), which contains the action of \(t\) on \(M\). If
\text{char}(L) = 0$ and $L$ is algebraically closed then $G_M$ is a direct product of a torus, a finite cyclic group and if $t$ is not semisimple a $G_{a,L}$.

Now let $M$ be $D$-module over $C(z)$ and let $N$ be the $Z$-module with $\mathcal{F}(N) = M$. Let $\{\{M\}\}$ denote the full subcategory of $Diff_{C(z)}$ generated by $M$ then the functor $\mathcal{F} : FMod_Z \to Diff_{C(z)}$ induces an equivalence $\{\{N\}\} \to \{\{M\}\}$ of tensor categories. Hence $\{\{M\}\}$ is also a neutral Tannakian category. Its fibre functor is $\omega \circ \mathcal{F}^{-1} : \{\{M\}\} \to \text{Vect}_{C(z^m)}$.

**Definition 6.4.1** The difference Galois group $G$ of $M$ is the linear algebraic group over $C(z^m)$ associated to this fibre functor.

If $\mathcal{F}(N) = M$ then the difference Galois group $G$ of $M$ is isomorphic to the group $G_N$ as defined above. Hence the difference Galois group $G$ associated to a system of difference equations is the linear algebraic group generated by the $m$-curvature.

**Example.** Consider the first order equation $\phi(y) = ay$, where $a \in C(z)$. Then the $m$-curvature is equal to $\hat{a} = \frac{1}{a(q^m - 1) - a(q^m)_{\alpha}(z)}$. Hence the difference Galois group associated to this first order difference equation is finite cyclic of order $k$ if and only if $\hat{a}$ is a primitive $k$ th root of unity. Otherwise if $\hat{a}$ is not a root of unity then the difference Galois group is the group $G_{m,C(z^m)}$ i.e. the multiplicative group over the field $C(z^m)$.

**Example.** Consider the hypergeometric $q$-difference equation which is given by

$$\phi^2(y) + \frac{(-4 + q^\alpha + q^\beta)}{z - 1} z + 3 - q^{\gamma - 1} \phi(y) + \frac{(2 - q^\alpha)(2 - q^\beta)}{z - 1} y = 0.$$ 

We are interested in the case where $\alpha, \beta$ and $\gamma$ are integral parameters and $q$ is a root of unity. As usual we will identify the second order $q$-difference equation with the system $(A) : \phi y = \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix} y$, where $a = \frac{(-4 + q^\alpha + q^\beta)z + 3 - q^{\gamma - 1}}{z - 1}$ and $b = \frac{(2 - q^\alpha)(2 - q^\beta)z - 2 + q^{\gamma - 1}}{z - 1}$. Note that the hypergeometric equation is symmetric in the parameters $\alpha$ and $\beta$. This restricts the number of possibilities we have to consider.

If $q = 1$ then the system of $q$-difference equations $(A)$ simplifies to $\phi y = \begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix} y$. The $1$-curvature has the matrix $A^{-1} = \begin{pmatrix} 2 & -1 \\ 1 & 0 \end{pmatrix}$. Hence the $1$-curvature has two eigenvalues $1$ but is not semisimple. Therefore the $q$-difference Galois group $G$ is isomorphic to the additive group $G_{a}(C(z)) = \{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in C(z) \}$.

If $q = -1$ then the $2$-curvature has the matrix $A(-z)^{-1}A(z)^{-1}$. We distinguish six cases.
1. If \( \alpha \equiv 0 \mod 2, \beta \equiv 0 \mod 2 \) and \( \gamma \equiv 0 \mod 2 \) then the 2-curvature has eigenvalues 1 and \( \frac{\nu_{-1}}{2z} \). The \( q \)-difference Galois group \( G \) is isomorphic to the group \( \mathcal{C}(\nu_{-1})^* \).

2. If \( \alpha \equiv 1 \mod 2, \beta \equiv 0 \mod 2 \) and \( \gamma \equiv 0 \mod 2 \) or \( \alpha \equiv 0 \mod 2, \beta \equiv 1 \mod 2 \) and \( \gamma \equiv 0 \mod 2 \) then the 2-curvature has eigenvalues 1 and \( \frac{1}{2} \). The \( q \)-difference Galois group \( G \) is isomorphic to the group \( \mathcal{C}(\nu_{-1})^* \).

3. If \( \alpha \equiv 1 \mod 2, \beta \equiv 1 \mod 2 \) and \( \gamma \equiv 0 \mod 2 \) then the 2-curvature has eigenvalues \( \frac{1}{2} \) and \( \frac{\nu_{-1}}{2z} \). The \( q \)-difference Galois group \( G \) is isomorphic to the group \( \mathcal{C}(\nu_{-1})^* \).

4. If \( \alpha \equiv 0 \mod 2, \beta \equiv 0 \mod 2 \) and \( \gamma \equiv 1 \mod 2 \) then the 2-curvature has matrix \( \begin{pmatrix} 3 & -2 \\ 2 & -1 \end{pmatrix} \). Hence both eigenvalues of the 2-curvature are equal to 1 but the 2-curvature is not semisimple. The \( q \)-difference Galois group \( G \) is isomorphic to the additive group \( G_a = \mathcal{C}(\nu_{-1}) \).

5. If \( \alpha \equiv 1 \mod 2, \beta \equiv 0 \mod 2 \) and \( \gamma \equiv 1 \mod 2 \) or \( \alpha \equiv 0 \mod 2, \beta \equiv 1 \mod 2 \) and \( \gamma \equiv 1 \mod 2 \) then the 2-curvature has eigenvalues 1 and \( \frac{\nu_{-1}}{2z} \). The \( q \)-difference Galois group \( G \) is isomorphic to the group \( \mathcal{C}(\nu_{-1})^* \).

6. If \( \alpha \equiv 1 \mod 2, \beta \equiv 1 \mod 2 \) and \( \gamma \equiv 1 \mod 2 \) then the 2-curvature has eigenvalues \( \frac{\nu_{-1}}{2z} \) and \( \frac{\nu_{+1}}{2z} \). Note that also in this case the set of eigenvalues is invariant under the map \( z \mapsto -z \). The \( q \)-difference Galois group \( G \) is a non-split two dimensional torus which is isomorphic to two copies of the multiplicative group \( G_m \) after the field extension \( \mathcal{C}(\nu_{-1}) \supset \mathcal{C}(\nu_{-1}) \).