ELECTRONIC RESEARCH ANNOUNCEMENTS
OF THE AMERICAN MATHEMATICAL SOCIETY
Volume 1, Issue 1, 1995

GALOIS GROUPS AND CONNECTION MATRICES OF q-DIFFERENCE EQUATIONS

PAVEL I. ETINGOF

(Communicated by David Kazhdan)

Abstract. We study the Galois group of a matrix q-difference equation with rational coefficients which is regular at 0 and ∞, in the sense of (difference) Picard-Vessiot theory, and show that it coincides with the algebraic group generated by matrices $C(u)C(w)^{-1}$ $u, w \in \mathbb{C}^*$, where $C(z)$ is the Birkhoff connection matrix of the equation.

1. Differential algebra

The notion of the Galois group of a linear ordinary differential equation or a holonomic system of such equations is well known. For example, consider the differential equation

$$\frac{df(z)}{dz} = a(z)f(z), \tag{1.1}$$

where a is an $N \times N$-matrix valued function and f is an unknown $\mathbb{C}^N$-valued function of one complex variable z (both are assumed holomorphic in z in a certain region). To define the Galois group, one fixes a field of functions F containing the coefficients of the equation and invariant under d/dz. Let L be the field generated over F by all solutions of the system. This field is invariant under d/dz. The Galois group G of the system is, by definition, the group of all automorphisms g of the field L such that g fixes all elements of F and $[g, d/dz] = 0$.

The group G is naturally isomorphic to a linear algebraic group over $\mathbb{C}$. Indeed, let $f_1, ..., f_N \in L$ be a basis of the space of solutions of the system. Then for any $g \in G$, $g(f_i)$ are also solutions of the system, so $g(f_i) = \sum_j g_{ij} f_j$. Moreover, g is uniquely determined by the matrix g_{ij}. Thus we get an embedding of G into $GL_N(\mathbb{C})$, given by $g \to \{g_{ij}\}^t$ (superscript t means transposition). It can be shown that the image of this map is a closed subgroup. If we replace the basis $f_1, ..., f_N$ by another basis, this embedding will be conjugated by the corresponding transformation matrix.

The properties of group G are the subject of Picard-Vessiot (or differential Galois) theory, and are described in [Ko,R,Ka]. This theory allows to prove that certain linear differential equations of second and higher order cannot be reduced

Received by the editors April 6, 1995.
1991 *Mathematics Subject Classification.* 12H10;39A10.

to a sequence of first order equations, by showing that their Galois groups are not solvable.

Computation of the Galois group of a given system of differential equations is, in general, a nontrivial problem, like in the usual Galois theory. However, in some cases, this group is easily computable. One of the most interesting cases is the following.

Let X be a smooth projective algebraic variety over $\mathbb{C}$. Let S be a hypersurface on X. Let D be an N-dimensional holonomic system of linear differential equations over X with rational coefficients which are regular outside S. Assume that the system has regular singularities at S. Then the Galois group of D over the field $F = \mathbb{C}(X)$ coincides with the Zariski closure $\bar{\Gamma}$ of the monodromy group Γ of D in $GL_N(\mathbb{C})$.

This well known theorem is proved, roughly, as follows. Assume for simplicity that X is a curve, S is a finite set. We assume that we fixed a base point $x \in X \setminus S$ and a basis of solutions of the system near this point. Let G be the Galois group. It is clear that $\Gamma \subset G$, since analytic continuation along a nontrivial loop starting and ending at x clearly defines an automorphism of the solution field F fixing rational functions and d/dz. Therefore, $\bar{\Gamma} \subset G$. Now assume that $\bar{\Gamma}$ is a proper closed subgroup in G. Then, by the main theorem of the differential Galois theory ([Ka], Theorem 5.9) $\mathbb{C}(X) = L^G \subset L^{\bar{\Gamma}}$ is a proper subfield, where L^H is the field of H-invariants in L. But it is easy to see that $L^{\bar{\Gamma}} = \mathbb{C}(X)$. It is even true that $L^{\Gamma} = \mathbb{C}(X)$. Indeed, let $f \in L^{\Gamma}$. Let $\tilde{X}$ be the universal cover of $X \setminus S$. Then f is meromorphic on $\tilde{X}$. Because f is invariant under the monodromy group, it is meromorphic on $X \setminus S$. Since our equation has regular singularities, f has to have polynomial growth near S. Thus, f is meromorphic at S too, so $f \in \mathbb{C}(X)$.

Among other things, this theorem implies the following. Assume that our variety X, hypersurface S, and system D are defined over the field $\bar{\mathbb{Q}}$ of algebraic numbers. Then the group $\bar{\Gamma}$ is defined over algebraic numbers; that is, we can find a basis of solutions of D in which $\bar{\Gamma} = H(\mathbb{C})$, where H is an affine algebraic group over $\bar{\mathbb{Q}}$. Indeed, the definition of the Galois group is purely algebraic, so it is defined over $\bar{\mathbb{Q}}$ automatically. Therefore, so is $\bar{\Gamma}$. More generally, one can see that if the data X, S, D are defined over any subfield $K \subset \mathbb{C}$, the group $\bar{\Gamma}$ is defined over some finite extension M of K ($\bar{\Gamma} = H(\mathbb{C})$, H is defined over M; however, note that H is not unique). This is true because G has the same property (this is also discussed in [De]). In contrast to this, note that Γ itself usually contains transcendental points of $\bar{\Gamma}$, i.e. points which are not defined over $\bar{\mathbb{Q}}$.

In the next sections we describe difference counterparts of these statements. For simplicity we restrict ourselves to the case of equations with one independent variable.

2. Difference algebra.

The following notions of difference algebra can be found in [Co],[Fr], and references therein.

Let F be a field of characteristic 0. We say that F is an (inversive) difference field if it is equipped with an automorphism $T : F \to F$. For example, if M is the field of meromorphic functions in $\mathbb{C}^*$, and $Tf(z) = f(qz)$, where $q \in \mathbb{C}^*$ is a fixed number, then (M, T) is a difference field. Also, any T-invariant subfield of M is a difference field with the same T.

Let (F,T) be a difference field. An element $f \in F$ is called a constant if $Tf = f$. Constants in F form a field which we denote by C_F.

We say that L is a difference field extension of F if L is a difference field and F is a difference subfield of L (with the same T).

Let F be a difference field, and L be a difference field extension of F. Consider a system of difference equations

$$Tf = af, \quad a \in GL_N(F) \tag{2.1}$$

with respect to $f \in GL_N(L)$. We say that L is a solution field of (2.1) over F if there exists a solution $f \in GL_N(L)$ of (2.1), and $L = F(f)$ (by $F(f)$ we mean the field obtained by adding all entries of f to F; it is clearly closed under T because of (2.1)). If $f' \in GL_N(L)$ is any other solution of (2.1) then $f' = fR$, $R \in GL_N(C_L)$. Thus solutions of (2.1) in $GL_N(L)$ form a principal homogeneous space of $GL_N(C_L)$.

We say that a solution field L is a Picard-Vessiot extension of F if C_F is algebraically closed, and $C_L = C_F$.

Note that if $F \subset K \subset L$ is any intermediate field and L is a Picard-Vessiot extension of F, it is also a Picard-Vessiot extension of K.

Remark. Strictly speaking, our definition of a Picard-Vessiot extension is a little more general than in [Co],[Fr], where the authors considered extensions generated by scalar, higher order difference equations, of the form $T^n f + a_1 T^{n-1} f + ... + a_n f = 0$, $a_i \in F$, $f \in L$. However, the theory of matrix equations (2.1) is completely analogous to the theory of scalar equations of higher order, so we make no distinction between them.

Let $F \subset L$ be a Picard-Vessiot extension associated to (2.1). The Galois group of L over F, $G = \mathrm{Gal}(L/F)$ is, by definition, the group of all automorphisms of L fixing all elements of F and commuting with T.

Let f be a solution of (2.1) in $GL_N(L)$. For any $g \in G$, $g(f)$ is another solution. So there exists a unique matrix $R_g \in GL_N(C_F)$ such that $g(f) = fR_g$. Thus the assignment $g \to R_g$ defines an embedding $G \to GL_N(C_F)$. The image of this embedding is a closed subgroup, because it can be described as follows.

Let I be the set of all polynomials P of N^2 variables over F such that $P(f) = 0$. It is clear that I is a radical ideal, and $F[f]$ is isomorphic to $F[X]/I$, $X = \{x_{ij}\}$, $i, j = 1, ..., N$, via the map $f \to X$. Let Y be the spectrum of the ring $F[X]/I$. It is an affine algebraic variety defined over F. We call this variety the variety of relations for L and call the ideal I the ideal of relations. We have $L = F(f) = F(Y)$. It is clear that the image of G in $GL_N(C_F)$ coincides with the set of those $R_g \in GL_N(C_F)$ whose right action maps Y to itself. So it is a Zariski closed matrix group.

For Picard-Vessiot extensions, one has the following main theorem of Galois theory.

Theorem 2.1. ([Fr]) *If $F \subset L$ is a Picard-Vessiot extension then there exists a 1-1 correspondence between intermediate difference fields K, $F \subset K \subset L$, which are relatively algebraically closed in L, and connected closed subgroups K' in Gal(L/F). This correspondence is given by the formulas $K = L^{K'}$, $K' = $ Gal(L/K). The transcendency degree of L over K equals the dimension of K'.*

3. q-Difference equations

From now on we will assume that the field F is the field $\mathbb{C}(z)$ of rational functions in one variable, and T acts by $Tf(z) = f(qz)$, where $q \in \mathbb{C}^*$ is a fixed number with $|q| < 1$. Let M be the field of all meromorphic functions in $\mathbb{C}^*$. This is a difference field, with the same T. We call a Picard-Vessiot extension of $\mathbb{C}(z)$ meromorphic if it can be embedded into M consistently with T. Since $\mathbb{C}(z)$ is algebraically closed in M (a single-valued algebraic function is rational), the Galois group of any meromorphic Picard-Vessiot extension is connected. Also, it is known [Fr] that if two Picard-Vessiot extensions of the same difference field can be placed inside of a common difference field, then they are isomorphic to each other as difference field extensions. This shows that if there exists at least one meromorphic Picard-Vessiot extension of $\mathbb{C}(z)$ corresponding to a given system of equations, then the Galois group depends only on the system and not on the choice of such extension.

We will also assume that the element a used in (2.1) (which is now a rational matrix function) is such that $a(0) = a(\infty) = 1$. Then it is easy to construct two meromorphic Picard-Vessiot extensions of $\mathbb{C}(z)$ corresponding to (2.1) as follows.

1. Let

$$f_0(z) = \prod_{j=0}^{\infty} a(q^j z)^{-1} = a(z)^{-1} a(qz)^{-1} ... \tag{3.1}$$

Then f_0 is a solution of (2.1), as a meromorphic function. Let $L_0 = \mathbb{C}(z, f_0)$.

2. Let

$$f_\infty(z) = \prod_{j=1}^{\infty} a(q^{-j} z) = a(q^{-1}z)a(q^{-2}z)... \tag{3.2}$$

Then f_∞ is a solution of (2.1). Let $L_\infty = \mathbb{C}(z, f_\infty)$.

Then L_0, L_∞ are Picard-Vessiot extensions of $\mathbb{C}(z)$ (the constant field is $\mathbb{C}$). This follows from the fact that all elements of L_0 (L_∞) are meromorphic at 0 (∞), so if we have an element that is periodic: $h(z) = h(qz)$, in either of them, this element has to be constant.

We know that these extensions should be identical. But how to identify them? This is done as follows.

Consider the Birkhoff connection matrix of (2.1):

$$C(z) = f_0(z)^{-1} f_\infty(z) = \prod_{j=-\infty}^{\infty} a(q^{-j}z) = ...a(qz)a(z)a(q^{-1}z)... \tag{3.3}$$

This is an elliptic function with values in $N \times N$ matrices: it is meromorphic in $\mathbb{C}^*$ and $C(qz) = C(z)$.

Theorem 3.1. *Let $w \in \mathbb{C}^*$ be such that $C(w)$ is finite and invertible. Then the map $f_\infty \to f_0 C(w)$ defines an isomorphism of Picard-Vessiot extensions $\tau_w : L_\infty \to L_0$.*

Proof. The proof relies on the following simple but crucial analytic lemma.

Lemma. *Assume that we have an identity*

$$\sum_{j=1}^{n} m_j(z)p_j(z) = 0, \tag{3.4}$$

where m_j are meromorphic functions in $\mathbb{C}$, and p_j are periodic meromorphic functions in $\mathbb{C}^*$: $p_j(qz) = p_j(z)$. Then

$$\sum_{j=1}^{n} m_j(z)p_j(w) = 0, \tag{3.5}$$

for generic z, w.

Proof of the Lemma. Fix $w \in \mathbb{C}^*$ such that p_j are nonsingular at w. Using (3.4) and periodicity of p_j, for sufficiently large k (so that $m_j(q^k w)$ are defined) we get

$$\sum_{j=1}^{n} m_j(q^k w)p_j(w) = 0. \tag{3.6}$$

Consider the function $h(z) = \sum_{j=1}^{n} m_j(z)p_j(w)$. We have: $h(q^k w) = 0$ for big k. Also, h is meromorphic at 0. Therefore, $h = 0$, as desired. □

Proof of the theorem. Let I_0, I_∞ be the ideals of relations of L_0, L_∞, and let Y_0, Y_∞ be the corresponding varieties of relations. Let $P \in I_\infty$. Then we have $P(z, f_\infty(z)) = 0$. We can rewrite it as $P(z, f_0(z)C(z)) = 0$. This relation is exactly of the type (3.4), because f_0, z are meromorphic at 0, and C is periodic. Therefore, by the Lemma $P(z, f_0(z)C(w)) = 0$ for generic z, w.

Now consider the map $\tau_w : \mathbb{C}(z)[X] \to \mathbb{C}(z)[X]$ $(X = \{x_{ij}\})$ given by $\tau_w(X) = XC(w)$. I claim that this homomorphism maps I_∞ to I_0. Indeed, we just showed that if $P \in I_\infty$ then $\tau_w(P) \in I_0$, since $\tau_w(P)(z, f_0(z)) = P(z, f_0(z)C(w)) = 0$. Therefore, τ_w descends to a morphism of algebraic varieties $Y_0 \to Y_\infty$. This morphism is an isomorphism – the inverse to τ_w is constructed analogously to τ_w. In particular, we get an isomorphism of the fields of rational functions on these varieties, i.e. a difference field isomorphism $L_\infty \to L_0$, which is identity on $\mathbb{C}(z)$, as desired. □

Now choose $u, w \in \mathbb{C}^*$ and consider the composition $\tau_w^{-1}\tau_u : L_\infty \to L_\infty$. This composition acts by $f_\infty \to f_\infty C(u)C(w)^{-1}$ and defines an element of the Galois group $\mathrm{Gal}(L_\infty/F)$. Thus, we proved

Corollary. *The matrix $C(u)C(w)^{-1}$, for all values of u, w for which it is defined and nondegenerate, belongs to $G = Gal(L_\infty/F)$ (where G is regarded as a closed subgroup in $GL_N(\mathbb{C})$).*

Let Γ be the group generated by the matrices $C(u)C(w)^{-1}$.

Proposition 3.2. *Γ is a closed connected subgroup of $GL_N(\mathbb{C})$.*

Proof. Connectedness is obvious, because the set of matrices $C(u)C(w)^{-1}$ is connected. Let us show that Γ is closed.

Let E be the elliptic curve $\mathbb{C}^*/q^{\mathbb{Z}}$. Let $E_0 \subset E$ be the open set consisting of all points w such that $C(w)$ is defined and invertible. We have a regular map of algebraic varieties: $\mu_1 : E_0^2 \to GL_N(\mathbb{C})$ defined by $\mu_1(u,w) = C(u)C(w)^{-1}$. Consider the regular map $\mu_k : E_0^{2k} \to GL_N(\mathbb{C})$ defined by

$$\mu_k(u_1, w_1, ..., u_k, w_k) = \mu_1(u_1, w_1)...\mu_1(u_k, w_k). \tag{3.7}$$

Let X_k be the image of μ_k, and let $\bar{X}_k$ be the closure of X_k. It is clear that $\bar{X}_k$ are irreducible (because of irreducibility of E_0^{2k}), and $\bar{X}_k \subset \bar{X}_{k+1}$. This means that they must stabilize: there exists m such that $\bar{X}_m = \cup_{k\geq 1}\bar{X}_k$. Observe that $\Gamma = \cup_{k\geq 0} X_k$. Therefore, $\bar{\Gamma} = \bar{X}_m$. But a standard theorem of algebraic geometry claims that if $f : X \to Y$ is a morphism of quasiprojective varieties, and $f(X)$ is dense in Y then $f(X)$ contains an open subset of Y. Applying this to $\mu_m : E_0^{2m} \to \bar{X}_m$, we can let $X_m^0 \subset X_m \subset \Gamma$ be an open subset of $\bar{X}_m = \bar{\Gamma}$. Thus, we have a connected affine algebraic group $\bar{\Gamma}$ and a subgroup Γ containing an open subset of $\bar{\Gamma}$. This implies that $\Gamma = \bar{\Gamma}$.□

Theorem 3.3. *$Gal(L_\infty/F) = \Gamma$.*

Proof. Let $h \in L_\infty$, and assume that h is fixed by all matrices $C(u)C(w)^{-1}$. We have $h(z) = P(z, f_\infty(z))$, where P is some rational function. In particular, h is meromorphic at infinity. By the invariance property, we get $h(z) = P(z, f_\infty(z)C(u)C(w)^{-1})$ for such u, w that $C(u), C(w)$ are nondegenerate. In particular, for $u = z$ we get $h(z) = P(z, f_0(z)C(w)^{-1})$. This shows that h is meromorphic at the origin. Thus, h is meromorphic on the whole Riemann sphere, i.e. rational. This proves:

$$L_\infty^\Gamma = F = \mathbb{C}(z). \tag{3.8}$$

So, by Theorem 2.1, it follows that Γ is the whole Galois group, as desired. □

Remark. Informally speaking, the matrices $C(u)C(w)^{-1}$ play the role of monodromy matrices in the difference case, and the group Γ plays the role of the monodromy group. Taking the product $C(u)C(w)^{-1}$, $u \neq w$ corresponds (in the differential setting) to moving from ∞ to 0 along one path, and returning along another, to obtain a nontrivial loop from $\pi_1(\mathbb{C}P^1 \setminus S, \infty)$ (assuming $0, \infty$ are regular points). The regularity of the points $0, \infty$ is expressed in the difference case by the identities $a(0) = a(\infty) = 1$.

Corollary. *Let K be any subfield of $\mathbb{C}$. Assume that $a \in K(z)$, $q \in K^*$. Then the group Γ generated by the matrices $C(u)C(w)^{-1}$ is of the form $H(\mathbb{C})$, where H is an affine algebraic group defined over K.*

Remarks. 1. Note that even if the equations have rational coefficients, the monodromy matrices $C(u)C(w)^{-1}$ will be generally transcendental, since they are given by infinite products. Still, the group generated by them in this case will be defined over rational numbers.

2. Note that the claim is that the two groups (the span of $C(u)C(w)^{-1}$ and $H(\mathbb{C})$) are *literally* the same, not only up to conjugation.

Proof. By Theorem 3.3, it is enough to prove this for the Galois group. To do this, it is enough to prove that the variety of relations Y_∞ of the field L_∞ over F is defined over $K(z)$. Let us write the function f_∞ as a series in powers of $1/z$ near $z = \infty$. It is easy to see from (3.2), that the coefficients of this series are rational functions in q with coefficients in K. For example, the coefficient to $1/z$ is $a_{-1}q/(1-q)$, where $a = 1 + a_{-1}/z + \dots$. Thus, if $q \in K^*$, these coefficients are automatically in K. Any relation $P(z, f_\infty) = 0$ can therefore be regarded as a relation in $\mathbb{C}((1/z))$. Therefore, one can find a basis of the ideal I_∞ which is defined over $K(z)$, i.e. Y_∞ is defined over $K(z)$, as desired. $\square$

Theorem 3.3 allows to obtain an easy solution of the inverse problem of Galois theory for difference equations over $\mathbb{C}(z)$:

Proposition 3.4. *Let G be any connected affine algebraic group over $\mathbb{C}$. Then there exists a Picard-Vessiot extension of $\mathbb{C}(z)$ (in the sense of Section 2) whose Galois group is G.*

Sketch of Proof. Pick $a \in G(\mathbb{C}(z))$ in such a way that $a(0) = a(\infty) = 1$, and the elements $a(u)a(w)^{-1}$, taken for all u, w where a is regular, generate G. This will be so "for most elements" of $G(\mathbb{C}()$. Consider now equation (2.1) with q very close to 0. Since $C(z)$ is approximately equal to $a(z)$, $C(u)C(w)^{-1}$ generate G. Therefore, by Theorem 3.3, G is the Galois group of the Picard-Vessiot extension associated to (2.1). $\square$

Remark. This proof shows that if the group G is defined over a field $K \subset \mathbb{C}$, then it is possible to find a system of the form (2.1) with $a \in GL_N(K(z))$ and $q \in K^*$ and a meromorphic Picard-Vessiot extension of $\mathbb{C}(z)$ associated to it, whose Galois group is G.

Finally, let us discuss solvability of difference equations. First, let us consider some simple difference equations.

1. Suppose we have an equation

$$f(qz) = a(z)f(z), \tag{3.9}$$

where $a(z)$ is a meromorphic scalar-valued function in $\mathbb{C}^*$.

Let $r \in \mathbb{R}^+$ be such that a has no zeros or poles on $|z| = r$. Then a can be uniquely written as a product $a = a_+a_-a_0$, where $a_0 = Cz^m$, a_+ is holomorphic in $|z| \le r$, a_- is holomorphic in $|z| \ge r$, and $a_+(0) = a_-(\infty) = 1$. This is done with the help of Cauchy integral. Now we set

$$\begin{aligned} f_+(z) &= \prod_{m=0}^{\infty} a_+(q^m z)^{-1}, \\ f_-(z) &= \prod_{m=1}^{\infty} a_-(q^{-m} z), \\ f_0(z) &= (-1)^m \Theta(Cz)^{-1}\Theta(z)^{-m+1}, \end{aligned} \tag{3.10}$$

where

$$\Theta(z) = \prod_{m\ge 0} (1-q^{m+1})(1-q^m z)(1-q^{m+1}z^{-1}) \tag{3.11}$$

is the theta-function.

It is easy to check that $f_j(qz) = a_j(z)f_j(z)$, $j = +, -, 0$. Therefore, $f = f_+f_-f_0$ is a meromorphic solution of (3.9). Also, any other meromorphic solution of (3.9) has the form $f(z)\varepsilon(z)$, where $\varepsilon(z)$ is an elliptic function, i.e. a meromorphic function in $\mathbb{C}^*$ such that $\varepsilon(qz)=\varepsilon(z)$.

2. Suppose we have a system of the form

$$f_1(qz)=f_1(z)+a(z)f_2(z), \quad f_2(qz)=f_2(z), \tag{3.12}$$

where a is a scalar meromorphic function. Setting $f_2=1$, we reduce it to the equation $f(qz)=f(z)+a(z)$. Let $r\in\mathbb{R}^+$ be such that a has no zeros or poles on $|z|=r$. Then a can be uniquely written as a sum $a=a_++a_-+a_0$, where $a_0=C$, a_+ is holomorphic in $|z|\le r$, a_- is holomorphic in $|z|\ge r$, and $a_+(0)=a_-(\infty)=0$. This is done by using the Cauchy integral. Now we set

$$\begin{aligned} f_+(z) &= -\sum_{m=0}^{\infty} a_+(q^m z), \\ f_-(z) &= \sum_{m=1}^{\infty} a_-(q^{-m} z), \\ f_0(z) &= -Cz\Theta'(z)/\Theta(z). \end{aligned} \tag{3.13}$$

It is easy to check that $f_j(qz)=f_j(z)+a_j(z)$, $j=+,-,0$. Therefore, if $h=f_++f_-+f_0$ then the matrix $f=\begin{pmatrix}1 & h\\ 0 & 1\end{pmatrix}$ is a meromorphic solution of (3.12). Moreover, any nondegenerate meromorphic matrix solution of (3.12) is of the form $f(z)\varepsilon(z)$, where ε is a nondegenerate 2×2 matrix whose entries are elliptic functions.

Let K be a difference field extension of $F=\mathbb{C}(z)$, $F\subset K\subset M$. After [Fr], we call K a Liouville extension if there exists a tower of difference fields of the form $F=F_0\subset F_1\subset ...\subset F_n=K$ such that for each j, $F_{j+1}=F_j(f)$, where f is a nondegenerate solution of (3.9) or (3.12), with $a\in F_j$. We call a difference field extension K_0 a generalized Liouville extension if $K_0\subset K$, where K is Liouville.

So, the property of an extension K to be generalized Liouville is equivalent to the possibility of computing any element of K via infinite sums and products, starting with rational functions (note that we don't allow nonabelian products of the form (3.1), (3.2) – since any equation we are considering admits a solution of such form). Therefore, if a meromorphic Picard-Vessiot extension of $\mathbb{C}(z)$ associated to an equation of the form (2.1) is generalized Liouville, we will say that this equation can be solved in q-quadratures.

The following theorem is a special case of a more general statement which can be found in [Fr]:

Theorem 3.5. *A meromorphic Picard-Vessiot extension of $\mathbb{C}(z)$ is generalized Liouville if and only if its Galois group is solvable.*

This implies:

Proposition 3.6. *An equation of the form (2.1) with $a(0)=a(\infty)=1$ can be solved in q-quadratures if and only if the group generated by the matrices $C(u)C(w)^{-1}$ (where $C(z)$ is the Birkhoff connection matrix (3.3)), is solvable.*

Final remark. We have been considering the case of difference equations in one variable regular at $0,\infty$ ($a(0)=a(\infty)=1$). This was done for the sake of brevity. The above theory carries over, with minor modifications, to a larger class of equations

– such that $a(0), a(\infty)$ are arbitrary invertible matrices, and to analogous systems of difference equations with several variables. In particular, it can be applied to q-hypergeometric systems and their generalizations.

Acknowledgements.

I would like to thank Maxim Kontsevich and Misha Verbitsky for inspiring me to write this note, and David Kazhdan for useful discussions.

References

[Co] Cohn, R.M., *Difference algebra*, Interscience Publ., New York, 1965.
[De] Deligne P., *Catégories Tannakiennes*, Grothendieck Festschrift **2** (1991), Birkhäuser, Boston, 111-195.
[Fr] Franke, C.H., *Picard-Vessiot theory of linear homogeneous difference equations*, Trans. of AMS **108** (1963), 491-515.
[Ka] Kaplansky, I., *An introduction to differential algebra*, Hermann, Paris, 1957.
[Ko] Kolchin, E.R., *Differential algebra and algebraic groups*, Acad. Press, New York, 1973.
[R] Ritt, J.F., *Differential algebra*, vol. XXXIII, Colloquium publ. of AMS, 1950.

Department of Mathematics, Harvard University, Cambridge, MA 02138, USA.
E-mail address: etingof@math.harvard.edu