COMPOSITIO MATHEMATICA

On classical irregular *q*-difference equations

Julien Roques

Compositio Math. **148** (2012), 1624–1644.

doi:10.1112/S0010437X12000292

https://doi.org/10.1112/S0010437X12000292 Published online by Cambridge University Press

Compositio Math. 148 (2012) 1624–1644
doi:10.1112/S0010437X12000292

On classical irregular q-difference equations

Julien Roques

Abstract

The primary aim of this paper is to (provide tools to) compute Galois groups of classical irregular q-difference equations. We are particularly interested in quantizations of certain differential equations that arise frequently in the mathematical and physical literature, namely confluent generalized q-hypergeometric equations and q-Kloosterman equations.

1. Introduction

Throughout this paper, q is a nonzero complex number such that $|q|<1$. For all $\alpha \in \mathbb{C}$, we set $q^{\alpha}=e^{\alpha \log(q)}$ where $\log(q)$ is a fixed logarithm of q. We denote by $\mathbb{C}(z)\langle \sigma_q, \sigma_q^{-1}\rangle$ the noncommutative algebra of noncommutative Laurent polynomials with coefficients in $\mathbb{C}(z)$ such that $\sigma_q z = qz\sigma_q$.

1.1 Motivation

Here are some examples of computations of q-difference Galois groups derived from the main results of this paper.

The generalized q-hypergeometric operator $\mathcal{L}_q(\underline{a};\underline{b};\lambda)$ with parameters $\underline{a}=(a_1,\dots,a_r)\in (q^{\mathbb{R}})^r$ $(r\in\mathbb{N})$, $\underline{b}=(b_1,\dots,b_s)\in (q^{\mathbb{R}})^s$ $(s\in\mathbb{N})$ and $\lambda\in\mathbb{C}^*$ is given by

$$\mathcal{L}_q(\underline{a};\underline{b};\lambda)=\prod_{j=1}^{s}\left(\frac{b_j}{q}\sigma_q-1\right)-z\lambda\prod_{i=1}^{r}(a_i\sigma_q-1).$$

We assume that $r\neq s$ (see [Roq11] for the case where $r=s$). By replacing z with $1/z$ if necessary, we can assume that $r>s$. For all $(i,j)\in\{1,\dots,r\}\times\{1,\dots,s\}$, we let $\alpha_i,\beta_j\in\mathbb{R}$ be such that $a_i=q^{\alpha_i}$ and $b_j=q^{\beta_j}$.

Theorem. *Assume that $\beta_j-\alpha_i\notin\mathbb{Z}$ for all $(i,j)\in\{1,\dots,r\}\times\{1,\dots,s\}$ (this condition is empty if $s=0$) and that the algebraic group generated by $\mathrm{diag}(e^{2\pi i\alpha_1},\dots,e^{2\pi i\alpha_r})$ is connected. Then the Galois group of $\mathcal{L}_q(\underline{a};\underline{b};\lambda)$ is $\mathrm{GL}(\mathbb{C}^r)$.*

Example. The Galois group of $(q^{1/2}\sigma_q-1)^s-z(\sigma_q-1)^r$ is $\mathrm{GL}(\mathbb{C}^r)$.

The q-Kloosterman operator $\mathrm{Kl}_q(U,V)$ associated to a pair (U,V) of elements of $\mathbb{C}[X]$ such that $U(0)=0$ and $V(0)\neq 0$ is given by

$$\mathrm{Kl}_q(U,V)=U(\sigma_q)+V(z^{-1}).$$

Received 2 June 2011, accepted in final form 17 January 2012, published online 25 July 2012.
2010 Mathematics Subject Classification 39A13 (primary).
Keywords: q-difference equations, difference Galois theory.

We let $c_1, \ldots, c_{\deg U}$ be the complex roots of $X^{\deg U}(U(X^{-1}) + V(0)) \in \mathbb{C}[X]$ and, for all $i \in \{1, \ldots, \deg U\}$, we denote by (u_i, α_i) the unique element of $\mathbb{U} \times \mathbb{R}$ such that $c_i = u_i q^{\alpha_i}$ ($\mathbb{U} \subset \mathbb{C}$ denotes the unit circle).

Theorem. *Assume that* $\deg U$ *and* $\deg V$ *are relatively prime, that the algebraic group generated by* $\operatorname{diag}(u_1, \ldots, u_{\deg U})$ *and* $\operatorname{diag}(e^{2\pi i\alpha_1}, \ldots, e^{2\pi i\alpha_{\deg U}})$ *is connected, and that there exists* $z_0 \in \mathbb{C}^*$ *such that* $V(z_0) = 0$ *and* $V(q^k z_0) \neq 0$ *for all* $k \in \mathbb{Z}^*$*. Then the Galois group of* $\mathrm{Kl}_q(U, V)$ *is* $\mathrm{GL}(\mathbb{C}^{\deg U})$.

Example. For relatively prime integers m and n, the Galois group of $(1 - \sigma_q)^n + (1 - z^{-1})^m - 1$ is $\mathrm{GL}(\mathbb{C}^n)$.

Proposition. *Let us consider* $V \in q + X\mathbb{C}[X]$*. Then, for any odd integer* $n \geqslant 2$ *coprime to* $\deg V$*, the Galois group of* $\mathrm{Kl}_q((q^{1/2} - X)^2(1 - X)^{n-2} - q, V)$ *is* $\mathrm{GL}(\mathbb{C}^n)$.

In order to achieve these goals, we present our results in two parts.

Part I is devoted to the following problem: *find simple and relevant characterizations of the classical linear algebraic groups.*

Part II is a Galoisian study of q-difference operators $L \in \mathbb{C}(z)\langle \sigma_q, \sigma_q^{-1}\rangle$ of rank n satisfying one of the following properties (see § 4.2 for the notion of slope).

($\mathscr{H}1$) At 0, L is isoclinic and its slope is of the form m/n with $m \in \mathbb{Z}^*$ coprime to n.

($\mathscr{H}2$) At 0, L has two slopes, 0 and μ. Denoting by r the multiplicity of μ, we have $\mu = m/r$ for some $m \in \mathbb{Z}^*$ coprime to r. The exponents attached to the slope 0 belong to $q^{\mathbb{R}}$.

For instance, the generalized q-hypergeometric operators with $s > 0$ considered above satisfy ($\mathscr{H}2$), whereas the generalized q-hypergeometric operators with $s = 0$ and the q-Kloosterman operators $\mathrm{Kl}_q(U, V)$ with $\deg U$ coprime to $\deg V$ satisfy ($\mathscr{H}1$).

Our starting point originates from the work of Katz [Kat87]: we exploit the structure of the local formal Galois groups. However, the q-difference and differential cases are rather different; in particular, the 'theta torus' is 'poorer' than its differential analogue, Ramis's exponential torus. We make essential use of works by van der Put and Reversat [vdPR07], van der Put and Singer [vdPS97] and Sauloy [Sau04]. In the theory of (irregular) linear differential equations, another way of computing Galois groups was explored: the use of Ramis's 'wild fundamental group' (see [DM89, Mit96]). It would be interesting to compute q-difference Galois groups using the q-analogue of the wild fundamental group introduced by Ramis and Sauloy in [RS07, RS09]. The crucial difference lies in the presence of a unipotent Stokes component (and hence in the *analytic* properties of the slopes filtration).

In some cases, the classical equations studied in this paper can be seen as q-deformations of certain classical differential equations (this is exploited by André in [And01]; see also [Sau00, §§ 3–5]), namely the confluent generalized hypergeometric equations and the Kloosterman equations. These differential equations were studied by Katz, with contributions from Gabber, in [Kat87, Kat90], by Katz and Pink in [KP87], by Beukers *et al.* in [BBH88], by Duval and Mitschi in [DM89] and by Mitschi in [Mit96].

The original interest of the author in the classical equations studied in the present paper comes from the discrete Morales–Ramis theory developed in [CR08, CR11] for deriving the nonintegrability of classical nonlinear q-difference equations, such as discrete Painlevé equations.

1.2 Organization of the paper

Part I essentially provides 'easily checkable' characterizations of the classical linear algebraic groups. In § 2 we give a new characterization relying on pairs of semisimple elements with special spectra. In § 3 we give consequences of results established by Katz and Kostant. Part II considers applications of these purely representation-theoretic results to the Galois theory of irregular q-difference equations. In § 4 we present the elements of slopes theory and some useful Galoisian results. In §§ 5 and 6 we show that the connected algebraic groups occurring as Galois groups of irreducible equations that satisfy either $(\mathscr{H}1)$ or $(\mathscr{H}2)$ belong to a very short list of linear algebraic groups. In § 7 we compute Galois groups of q-Kloosterman equations and of generalized q-hypergeometric equations. In § 8 we give a $\otimes$-indecomposability criterion, which we apply to the calculation of q-difference Galois groups. In § 9, combining several results of this paper, we give additional computations of Galois groups.

Part I. Characterizations of the classical linear algebraic groups

2. A characterization of the classical linear algebraic groups

Let E be a $\mathbb{C}$-vector space of finite dimension $n \geqslant 3$. Let us consider α and β in $\mathbb{N}$ such that $\alpha \geqslant 1$, $\beta \geqslant 2$ and $n = \alpha + \beta$.

Definition 1 (Property $(\mathcal{P})$). A pair f, g of semisimple elements of $\mathrm{GL}(E)$ satisfies property $(\mathcal{P})$ if:

- the list of eigenvalues of f is of the form (a repeated α times, b repeated β times) where $a, b \in \mathbb{C}^*$ are such that $a \neq \pm b$;
- the list of eigenvalues of g is of the form (c repeated $\alpha + 1$ times, $d_1, \ldots, d_{\beta-1}$) where $c, d_1, \ldots, d_{\beta-1}$ are pairwise distinct nonzero complex numbers.

This section is devoted to the proof of the following result.

Theorem 2. *Let G be a connected algebraic subgroup of $\mathrm{GL}(E)$ which acts irreducibly on E. If G contains a pair of semisimple elements f, g satisfying $(\mathcal{P})$, then the derived subgroup G' of G is $\mathrm{SL}(E)$, $\mathrm{SO}(E)$ or (if $n = \dim(E)$ is even) $\mathrm{Sp}(E)$. Furthermore, $G' \subset G \subset \mathbb{C}^* G'$.*

Proposition 3. *Let G be a connected semisimple algebraic subgroup of $\mathrm{GL}(E)$ which acts irreducibly on E. If G contains a semisimple element f whose list of eigenvalues is of the form (a repeated α times, b repeated β times) for some $a, b \in \mathbb{C}^*$ such that $a \neq \pm b$, then its Lie algebra $\mathfrak{g}$ contains a semisimple element whose list of eigenvalues is (β repeated α times, $-\alpha$ repeated β times).*

Proof. Gabber's theorem [Kat90, Theorem 1.0] applied to the Lie subalgebra $\mathfrak{g}$ of $\mathrm{End}(E)$ and the subgroup H of G generated by f ensures that, for any x, y in $\mathbb{C}$ such that $\alpha x + \beta y = 0$, $\mathfrak{g}$ contains a semisimple element whose list of eigenvalues is (x repeated α times, y repeated β times). □

Proposition 4. *Let G be a connected semisimple algebraic subgroup of $\mathrm{SL}(E)$ which acts irreducibly on E. If G contains a pair of semisimple elements f, g satisfying $(\mathcal{P})$, then G is simple (in the sense that its Lie algebra is simple).*

Proof. Let $\rho : G \hookrightarrow \mathrm{GL}(E)$ be the standard representation of G, which is irreducible by hypothesis. It comes from an irreducible representation $\widetilde{\rho} : \widetilde{G} \twoheadrightarrow G \hookrightarrow \mathrm{GL}(E)$ of the universal covering $\widetilde{G}$ of G. We want to prove that G is simple, i.e. that its Lie algebra $\mathrm{Lie}(G) = \mathrm{Lie}(\widetilde{G}) = \mathfrak{g}$ is simple.

Assume to the contrary that $\mathfrak{g}$ is not simple. Then it splits into a direct sum $\mathfrak{g} = \mathfrak{g}_1 \oplus \mathfrak{g}_2$ of nontrivial semisimple Lie algebras $\mathfrak{g}_1$ and $\mathfrak{g}_2$ in such a way that the irreducible representation $\mathrm{Lie}(\widetilde{\rho}) : \mathfrak{g} \hookrightarrow \mathrm{End}(E)$ is (irreducible representation $\mathfrak{g}_1 \to \mathrm{End}(E_1)$) $\otimes$ (irreducible representation $\mathfrak{g}_2 \to \mathrm{End}(E_2)$) with $n_1 = \dim(E_1) \geqslant 2$ and $n_2 = \dim(E_2) \geqslant 2$. Denoting by $\widetilde{G}_1$ and $\widetilde{G}_2$ the connected and simply connected semisimple Lie groups with respective Lie algebras $\mathfrak{g}_1$ and $\mathfrak{g}_2$ and integrating the above representations of $\mathfrak{g}_1$ and $\mathfrak{g}_2$ into representations $\widetilde{\rho}_1 : \widetilde{G}_1 \to \mathrm{GL}(E_1)$ and $\widetilde{\rho}_2 : \widetilde{G}_2 \to \mathrm{GL}(E_2)$, we get that $\widetilde{G}$ is $\widetilde{G_1} \times \widetilde{G_2}$ and $\widetilde{\rho}$ is $\widetilde{\rho}_1 \otimes \widetilde{\rho}_2$. So the list of eigenvalues of any element of $G = \mathrm{Im}(\widetilde{\rho})$ is of the form $\{\lambda_i \mu_j \,;\, 1 \leqslant i \leqslant n_1, 1 \leqslant j \leqslant n_2\}$.

Since f belongs to G, its list of eigenvalues (a repeated α times, b repeated β times) is of the form $(\lambda_i \mu_j \,;\, 1 \leqslant i \leqslant n_1, 1 \leqslant j \leqslant n_2)$.

Note that either $\mathrm{card}\{\lambda_i \mid 1 \leqslant i \leqslant n_1\} = 1$ or $\mathrm{card}\{\mu_j \mid 1 \leqslant j \leqslant n_2\} = 1$. Otherwise, there would exist $t, u \in \{\lambda_i \mid 1 \leqslant i \leqslant n_1\}$ and $v, w \in \{\mu_j \mid 1 \leqslant j \leqslant n_2\}$ such that $t \neq u$ and $v \neq w$. The sublist (tv, tw, uv, uw) of $(\lambda_i \mu_j \,;\, 1 \leqslant i \leqslant n_1, 1 \leqslant j \leqslant n_2)$ would be made up of at least three distinct numbers (otherwise, since $\{tv, uw\} \cap \{tw, uv\} = \emptyset$, we would have $tv = uw$ and $tw = uv$ so that $v/w = (tv)/(tw) = (uw)/(uv) = w/v$ and hence $v = -w$ and $t = -u$; therefore the inclusion $\{tv, -tv\} = \{tv, tw, uv, uw\} \subset \{\lambda_i \mu_j \mid 1 \leqslant i \leqslant n_1, 1 \leqslant j \leqslant n_2\} = \{a, b\}$ would be an equality, and so $a = -b$, which is a contradiction). This contradicts the fact that f has two eigenvalues.

Up to relabeling, we can assume that $\mathrm{card}\{\lambda_i \mid 1 \leqslant i \leqslant n_1\} = 1$ and $\mathrm{card}\{\mu_j \mid 1 \leqslant j \leqslant n_2\} = 2$. Hence α and β are nonzero integral multiples of n_1; in particular, $n_1 \leqslant \alpha$ and $n_1 \leqslant \beta$.

Since g belongs to G, its list of eigenvalues (c repeated $\alpha + 1$ times, $d_1, \ldots, d_{\beta-1}$) is of the form $(\lambda'_i \mu'_j \,;\, 1 \leqslant i \leqslant n_1, 1 \leqslant j \leqslant n_2)$. So there exist $\alpha + 1$ distinct indices $(i_1, j_1), \ldots, (i_{\alpha+1}, j_{\alpha+1})$ in $\{1, \ldots, n_1\} \times \{1, \ldots, n_2\}$ such that $c = \lambda'_{i_1} \mu'_{j_1} = \cdots = \lambda'_{i_{\alpha+1}} \mu'_{j_{\alpha+1}}$. Since $n_1 < \alpha + 1$, we get that there exist $1 \leqslant k \neq k' \leqslant \alpha + 1$ such that $i_k = i_{k'}$. Hence $j_k \neq j_{k'}$ and $\lambda'_{i_k} \mu'_{j_k} = \lambda'_{i_{k'}} \mu'_{j_{k'}}$, so $\mu'_{j_k} = \mu'_{j_{k'}}$. Therefore, for all $1 \leqslant i \leqslant n_1$, $\lambda'_i \mu'_{j_k} = \lambda'_i \mu'_{j_{k'}}$ and so $\lambda'_i \mu'_{j_k} = c$ (because c is the unique eigenvalue of g with multiplicity greater than 1). Thus, $\lambda'_1 = \cdots = \lambda'_{n_1}$. So any element of $(\lambda'_i \mu'_j \,;\, 1 \leqslant i \leqslant n_1, 1 \leqslant j \leqslant n_2)$ occurs at least $n_1 > 1$ times. But this is a contradiction (since g has at least one eigenvalue with multiplicity 1), so $\mathfrak{g}$ is simple. $\square$

We have proved that any connected semisimple algebraic subgroup of $\mathrm{GL}(E)$ that acts irreducibly on E and which contains a pair of semisimple elements f, g satisfying $(\mathcal{P})$ is simple and that its Lie algebra contains a morphism with exactly two eigenvalues. This restricts the possibilities for G by virtue of the following result of Serre. For the notion of minuscule representations, we refer to Bourbaki [Bou75].

Theorem 5 (Serre [Ser79, § 3]). *If a simple Lie subalgebra $\mathfrak{g}$ of $\mathrm{End}(E)$ which acts irreducibly on E contains a morphism with exactly two eigenvalues, then $\mathfrak{g}$ is a classical Lie algebra (A_m, B_m, C_m or D_m) and its weights in E are minuscule.*

It is proved in [Bou75, ch. 8, § 7.3] that the minuscule representations of classical Lie algebras are

$$\begin{aligned}
&A_m,\ m \geqslant 1;\ \omega_1, \ldots, \omega_m \\
&B_m,\ m \geqslant 3;\ \omega_m \\
&C_m,\ m \geqslant 2;\ \omega_1 \\
&D_m,\ m \geqslant 4;\ \omega_1, \omega_{m-1}, \omega_m.
\end{aligned}$$

Remark 1. This list is slightly different from the one given in [Bou75] because (we are only interested in classical Lie algebras and) we have taken into consideration accidental isomorphisms.

The corresponding representations of connected Lie groups are conjugated to a factor of one of the following representations:

$$\begin{aligned} \mathrm{SL}_{m+1}(\mathbb{C}),\ m \geqslant 1;&\ \mathrm{std},\ \Lambda^2(\mathrm{std})\ldots,\ \Lambda^m(\mathrm{std}) \\ \mathrm{Spin}_{2m+1}(\mathbb{C}),\ m \geqslant 3;&\ \text{spin representation} \\ \mathrm{Sp}_{2m}(\mathbb{C}),\ m \geqslant 2;&\ \mathrm{std} \\ \mathrm{Spin}_{2m}(\mathbb{C}),\ m \geqslant 4;&\ \text{half-spin representations or 'std representation of } \mathrm{SO}_{2m}(\mathbb{C})\text{'}. \end{aligned}$$

For any subgroup G of $\mathrm{GL}(E)$, we denote by std the standard representation of G, i.e. the inclusion $G \hookrightarrow \mathrm{GL}(E)$.

In what follows, we shall prove that among the above representations, the only ones whose image contains a pair of semisimple elements satisfying $(\mathcal{P})$ are $\mathrm{SL}_{m+1}(\mathbb{C})$ in std or in $\Lambda^m(\mathrm{std})$, $\mathrm{Sp}_{2m}(\mathbb{C})$ in std, and $\mathrm{Spin}_{2m}(\mathbb{C})$ in the standard representation of $\mathrm{SO}_{2m}(\mathbb{C})$.

Proposition 6. *For $1 < k < m$ (so $m \geqslant 3$), the image of $\mathrm{SL}_{m+1}(\mathbb{C})$ in $\Lambda^k(\mathrm{std})$ does not contain a pair of semisimple elements satisfying $(\mathcal{P})$.*

Proof. By duality, i.e. the fact that $\Lambda^k(\mathrm{std}) \cong (\Lambda^{m+1-k}(\mathrm{std}))^*$, it is sufficient to consider the case where $1 < k \leqslant (m+1)/2$.

Assume to the contrary that the image of $\mathrm{SL}_{m+1}(\mathbb{C})$ in $\Lambda^k(\mathrm{std})$ contains a pair of semisimple elements f, g satisfying $(\mathcal{P})$.

Then, the list of eigenvalues (a repeated α times, b repeated β times) of f is of the form

$$(u_{i_1,\ldots,i_k} = u_{i_1} \cdots u_{i_k}\,;\ 1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant m+1).$$

We have $\mathrm{card}\{u_i \mid 1 \leqslant i \leqslant m+1\} \geqslant 2$ because $a \neq b$. We claim that $\mathrm{card}\{u_i \mid 1 \leqslant i \leqslant m+1\} = 2$. Assume to the contrary that $\mathrm{card}\{u_i \mid 1 \leqslant i \leqslant m+1\} > 2$. Up to renumbering, we can assume that u_1, u_2 and u_3 are pairwise distinct. Then $u_{3,\ldots,k+2}$, $u_{2,4,\ldots,k+2}$ and $u_{1,4,\ldots,k+2}$ (note that $k+2 \leqslant (m+1)/2+2 \leqslant m+1$ because $m \geqslant 3$) would be pairwise distinct, and therefore $\mathrm{card}\{u_{i_1,\ldots,i_k} \mid 1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant m+1\} > 3$: this is a contradiction.

So, up to renumbering, we can assume that there exists $i \in \{1, \ldots, m\}$ such that $u := u_1 = \cdots = u_i \neq u_{i+1} = \cdots = u_{m+1} =: v$.

We claim that $i = 1$ or $i = m$. Indeed, assume to the contrary that $2 \leqslant i \leqslant m-1$ (recall that $m \geqslant 3$) and denote by l the smallest nonnegative integer such that $i \leqslant l+k$ (so $l = 0$ if $i \leqslant k$ and $l = i-k$ if $i > k$). Then $u_{l+1,\ldots,l+k}$, $u_{l+2,\ldots,l+k+1}$ and $u_{l+3,\ldots,l+k+2}$ would be pairwise distinct (indeed, there exists $t \in \mathbb{C}^*$ such that $u_{l+1,\ldots,l+k} = u^2 t$, $u_{l+2,\ldots,l+k+1} = uvt$ and $u_{l+3,\ldots,l+k+2} = v^2 t$, and these three numbers are pairwise distinct because $u \neq \pm v$), so $\mathrm{card}\{u_{i_1,\ldots,i_k} \mid 1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant m+1\} > 3$: this is a contradiction.

Consequently, we have that either $u_1 \neq u_2 = \cdots = u_{m+1}$ or $u_1 = \cdots = u_m \neq u_{m+1}$, so we have either $(\alpha, \beta) = \big(\binom{m}{k-1}, \binom{m}{k}\big)$ or $(\alpha, \beta) = \big(\binom{m}{k}, \binom{m}{k-1}\big)$. In any case, we have $\alpha \geqslant \min\big\{\binom{m}{k-1}, \binom{m}{k}\big\} = \binom{m}{k-1}$ (the last equality holds because $k \leqslant (m+1)/2$).

On the other hand, the list of eigenvalues (c repeated $\alpha+1$ times, $d_1, \ldots, d_{\beta-1}$) of g is of the form

$$(v_{i_1,\ldots,i_k} = v_{i_1} \cdots v_{i_k}\,;\ 1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant m+1).$$

https://doi.org/10.1112/S0010437X12000292 Published online by Cambridge University Press

This list is the concatenation of the $\binom{m}{k-1}$ lists of the form

$$(v_{i_1,\ldots,i_{k-1},j} = v_{i_1} \cdots v_{i_{k-1}} v_j \; ; \; i_{k-1} < j \leqslant m+1)$$

indexed by $1 \leqslant i_1 < i_2 < \cdots < i_{k-1} \leqslant m$.

Since $\alpha + 1 > \binom{m}{k-1}$, we get that there exist $1 \leqslant i_1 < i_2 < \cdots < i_{k-1} \leqslant m$ and $i_{k-1} < j, j' \leqslant m+1$ with $j \neq j'$ such that $c = v_{i_1,\ldots,i_{k-1},j} = v_{i_1,\ldots,i_{k-1},j'}$. So $v_j = v_{j'}$. Up to renumbering, we can assume that $v_1 = v_2$.

For all $3 \leqslant i_2 < \cdots < i_k \leqslant m+1$, we obviously have $v_1 v_{i_2} \cdots v_{i_k} = v_2 v_{i_2} \cdots v_{i_k}$. Since c is the only eigenvalue of g with multiplicity greater than 1, we necessary have, for all $3 \leqslant i_2 < \cdots < i_k \leqslant m+1$, $c = v_1 v_{i_2} \cdots v_{i_k}$. Therefore, $v_3 = \cdots = v_{m+1}$.

If $k > 2$, then it is clear that any element of the list $(v_{i_1,\ldots,i_k} \; ; \; 1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant m+1)$ occurs with multiplicity at least 2: this is a contradiction.

If $k = 2$, then any element of the list $(v_{i_1,i_2} \; ; \; 1 \leqslant i_1 < i_2 \leqslant m+1)$ occurs with multiplicity at least 2 except, possibly, the term corresponding to $i_1 = 1$ and $i_2 = 2$. In particular, $c = v_1 v_3 = v_3 v_4 = v_3^2$ and so $v_1 = v_3$, giving $v_1 = \cdots = v_{m+1}$ and hence $\operatorname{card}\{v_{i_1,\ldots,i_k} \mid 1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant m+1\} = 1$: this is a contradiction. □

PROPOSITION 7. *The image of* $\mathrm{Spin}_{2m}(\mathbb{C})$ *with* $m \geqslant 4$ *in any of its* $1/2$*-spin representations does not contain a pair of semisimple elements satisfying* $(\mathcal{P})$.

Proof. Assume to the contrary that the image G of $\mathrm{Spin}_{2m}(\mathbb{C})$ in one of its 1/2-spin representations contains a pair of semisimple elements f, g satisfying $(\mathcal{P})$.

Let us first treat the case of the 1/2-spin representation ρ_- whose weights have an odd number of minus signs.

Proposition 3 ensures that $\mathrm{Lie}(G) = \mathfrak{g}$ contains an element u whose list of eigenvalues is $E_u = (\beta$ repeated α times, $-\alpha$ repeated β times). There exist $\lambda_1, \ldots, \lambda_m$ in $\mathbb{C}$ such that

$$E_u = (\epsilon_1 \lambda_1 + \cdots + \epsilon_m \lambda_m \; ; \; (\epsilon_1, \ldots, \epsilon_m) \in \{-1, 1\}^m \text{ such that } \epsilon_1 \cdots \epsilon_m = -1).$$

Since $(\lambda_1 + \cdots + \lambda_m - 2\lambda_1, \lambda_1 + \cdots + \lambda_m - 2\lambda_2, \ldots, \lambda_1 + \cdots + \lambda_m - 2\lambda_m)$ is a sublist of E_u, we get that $\operatorname{card}\{\lambda_i \mid 1 \leqslant i \leqslant m\} \leqslant 2$.

Assume that $\operatorname{card}\{\lambda_i \mid 1 \leqslant i \leqslant m\} = 1$, i.e. that $\lambda := \lambda_1 = \cdots = \lambda_m$. Note that $\lambda \neq 0$. If $m \geqslant 5$, then

$$\begin{aligned}(\lambda_1 + \cdots + \lambda_m - 2\lambda_1,\ &\lambda_1 + \cdots + \lambda_m - 2\lambda_1 - 2\lambda_2 - 2\lambda_3, \\ &\lambda_1 + \cdots + \lambda_m - 2\lambda_1 - 2\lambda_2 - 2\lambda_3 - 2\lambda_4 - 2\lambda_5) \\ &= ((m-2)\lambda,\ (m-6)\lambda,\ (m-10)\lambda)\end{aligned}$$

is a sublist of E_u made up of three distinct numbers, which is a contradiction. If $m = 4$, then E_u is (2λ repeated 4 times, -2λ repeated 4 times). In particular, $\alpha = \beta = 2^{m-2}$.

Assume that $\operatorname{card}\{\lambda_i \mid 1 \leqslant i \leqslant m\} = 2$, i.e. that $\lambda := \lambda_1 = \cdots = \lambda_i$ and $\lambda_{i+1} = \cdots = \lambda_m =: \mu$ for some $1 \leqslant i < m$ and some distinct complex numbers λ and μ. Since $m \geqslant 4$, up to relabeling we can assume that $i \geqslant 2$. Then

$$\begin{aligned}&(\lambda_1 + \cdots + \lambda_m - 2\lambda_1,\ \lambda_1 + \cdots + \lambda_m - 2\lambda_m,\ \lambda_1 + \cdots + \lambda_m - 2\lambda_1 - 2\lambda_2 - 2\lambda_m) \\ &\quad = (\lambda_1 + \cdots + \lambda_m - 2\lambda,\ \lambda_1 + \cdots + \lambda_m - 2\mu,\ \lambda_1 + \cdots + \lambda_m - 2(2\lambda + \mu))\end{aligned}$$

is a sublist of E_u. Since $\lambda \neq \mu$, we have $\lambda_1 + \cdots + \lambda_m - 2\lambda \neq \lambda_1 + \cdots + \lambda_m - 2\mu$; so, since E_u is composed of two elements, $\lambda_1 + \cdots + \lambda_m - 2(2\lambda + \mu)$ is equal to either $\lambda_1 + \cdots + \lambda_m - 2\lambda$

or $\lambda_1+\cdots+\lambda_m-2\mu$, that is, $\lambda=0$ or $\mu=-\lambda$. If $\lambda=0$ and $i<m-1$, then

$$\begin{aligned}&(\lambda_1+\cdots+\lambda_m-2\lambda_1,\ \lambda_1+\cdots+\lambda_m-2\lambda_1-2\lambda_2-2\lambda_m,\ \lambda_1+\cdots+\lambda_m-2\lambda_1-2\lambda_{m-1}-2\lambda_m)\\&\quad=((m-i)\mu,\ (m-i-2)\mu,\ (m-i-4)\mu)\end{aligned}$$

is a sublist of E_u made up of three pairwise distinct complex numbers (because $\mu\neq\lambda=0$); but this is impossible. If $\lambda=0$ and $i=m-1$, then E_u has the form (μ repeated 2^{m-2} times, $-\mu$ repeated 2^{m-2} times) and hence $\alpha=\beta=2^{m-2}$. If $\mu=-\lambda$ and $i\geqslant 3$, then

$$\begin{aligned}&(\lambda_1+\cdots+\lambda_m-2\lambda_1,\ \lambda_1+\cdots+\lambda_m-2\lambda_1-2\lambda_2-2\lambda_3,\ \lambda_1+\cdots+\lambda_m-2\lambda_m)\\&\quad=(\lambda_1+\cdots+\lambda_m-2\lambda,\ \lambda_1+\cdots+\lambda_m-6\lambda,\ \lambda_1+\cdots+\lambda_m+2\lambda)\end{aligned}$$

is a sublist of E_u made up of three pairwise distinct complex numbers, which is impossible. Similarly, the case where $\lambda=-\mu$ and $m-i\geqslant 3$ is impossible. So, since $m\geqslant 4$, the only possibility that is compatible with $\lambda=-\mu$ is $m=4$ and $i=2$, in which case E_u is of the form (2λ repeated 4 times, -2λ repeated 4 times); thus, in particular, $\alpha=\beta=2^{m-2}$.

Therefore, in any possible case, we have $\alpha=\beta=2^{m-2}$.

On the other hand, since g belongs to G, its list of eigenvalues $E_g=$ (c repeated $\alpha+1$ times, $d_1,\ldots,d_{\beta-1}$) has the form

$$E_g=(\mu_1^{\epsilon_1}\cdots\mu_m^{\epsilon_m}\ ;\ (\epsilon_1,\ldots,\epsilon_n)\in\{-1,1\}^m \text{ such that } \epsilon_1\cdots\epsilon_m=-1).$$

This list is the concatenation of the 2^{m-2} lists of the form

$$\Bigg(\prod_{i\in\{1,\ldots,m\}\setminus\{i_1,\ldots,i_{p-1},i_p\}}\mu_i\cdot\prod_{i\in\{i_1,\ldots,i_{p-1},i_p\}}\mu_i^{-1}\ ;\ i_{p-1}<i_p\leqslant m\Bigg)$$

indexed by $1\leqslant i_1<\cdots<i_{p-1}\leqslant m-1$ with $1\leqslant p\leqslant m$ an odd number. Since $\alpha+1>2^{m-2}$, we see that there exist $1\leqslant i_1<\cdots<i_{p-1}\leqslant m-1$ and $i_{p-1}<j,j'\leqslant m$ with $j\neq j'$ such that

$$c=\prod_{i\in\{1,\ldots,m\}\setminus\{i_1,\ldots,i_{p-1},j\}}\mu_i\cdot\prod_{i\in\{i_1,\ldots,i_{p-1},j\}}\mu_i^{-1}=\prod_{i\in\{1,\ldots,m\}\setminus\{i_1,\ldots,i_{p-1},j'\}}\mu_i\cdot\prod_{i\in\{i_1,\ldots,i_{p-1},j'\}}\mu_i^{-1}$$

and so $\mu_j^2=\mu_{j'}^2$, i.e. $\mu_j=\pm\mu_{j'}$. Up to renumbering, we can assume that $\mu_1=\pm\mu_2$. So, for all $3\leqslant k,l\leqslant m$ with $k\neq l$ (recall that $m\geqslant 4$), we have

$$\mu_1\mu_2^{-1}\mu_k^{-1}\mu_l^{-1}\prod_{i\in\{1,\ldots,m\}\setminus\{1,2,k,l\}}\mu_i=\mu_1^{-1}\mu_2\mu_k^{-1}\mu_l^{-1}\prod_{i\in\{1,\ldots,m\}\setminus\{1,2,k,l\}}\mu_i.$$

Thus $\mu_1\mu_2^{-1}\mu_k^{-1}\mu_l^{-1}\prod_{i\in\{1,\ldots,m\}\setminus\{1,2,k,l\}}\mu_i$ occurs with multiplicity greater than 1 in E_g, and hence

$$c=\mu_1\mu_2^{-1}\mu_k^{-1}\mu_l^{-1}\prod_{i\in\{1,\ldots,m\}\setminus\{1,2,k,l\}}\mu_i.$$

Similarly, for all $3\leqslant k,l\leqslant m$ with $k\neq l$,

$$c=\mu_1\mu_2^{-1}\mu_k\mu_l\prod_{i\in\{1,\ldots,m\}\setminus\{1,2,k,l\}}\mu_i.$$

So, for all $3\leqslant k,l\leqslant m$ with $k\neq l$, we have $\mu_k^2\mu_l^2=1$. If $m\geqslant 5$, then for all $3\leqslant k,l\leqslant m$ there exists $3\leqslant k'\leqslant m$ such that $k'\neq k,l$; so $\mu_k^2/\mu_l^2=(\mu_k^2\mu_{k'}^2)/(\mu_l^2\mu_{k'}^2)=1/1=1$, i.e. $\mu_k^2=\mu_l^2$. Therefore, we get $\mu_3^2=\cdots=\mu_m^2=\pm 1$. This implies that any element of

$$E_g=(\mu_1^{\epsilon_1}\cdots\mu_m^{\epsilon_m}\ ;\ (\epsilon_1,\ldots,\epsilon_n)\in\{-1,1\}^m \text{ such that } \epsilon_1\cdots\epsilon_m=-1)$$

https://doi.org/10.1112/S0010437X12000292 Published online by Cambridge University Press

has multiplicity at least 2 because $\mu_1^{\epsilon_1}\cdots\mu_m^{\epsilon_m}=\mu_1^{\epsilon_1}\cdots\mu_{m-2}^{\epsilon_{m-2}}\mu_{m-1}^{-\epsilon_{m-1}}\mu_m^{-\epsilon_m}$; this is a contradiction. If $m=4$, then it is easily seen that E_g is of the form $(\nu_1,\nu_1^{-1},\ldots,\nu_{2^{m-2}},\nu_{2^{m-2}}^{-1})$ (this is more generally true if m is even). If $m=4$ and $c^{-1}=c$, then $\alpha+1$ would be an even number (because if $c\in\{\nu_i,\nu_i^{-1}\}$, then $\{\nu_i,\nu_i^{-1}\}=\{c\}$ and so the number $\alpha+1$ of occurrences of c in $E_g=(\nu_1,\nu_1^{-1},\ldots,\nu_{2^{m-2}},\nu_{2^{m-2}}^{-1})$ must be even); so α would be an odd number and hence would not be an integral power of 2, which is a contradiction. If $m=4$ and $c^{-1}\neq c$, then the fact that c occurs with multiplicity $\alpha+1$ in $E_g=(\nu_1,\nu_1^{-1},\ldots,\nu_{2^{m-2}},\nu_{2^{m-2}}^{-1})$ implies that c^{-1} occurs with multiplicity $\alpha+1>1$ in E_g, so $c=c^{-1}$ (because c is the unique eigenvalue of g with multiplicity greater than 1); this is again a contradiction.

Let us now treat the case of the 1/2-spin representation ρ_+ whose weights have an even number of minus signs.

Since ρ_+ is dual to ρ_- when m is odd, it is sufficient to consider the case where m is even. As mentioned above, the fact that m is even implies that the list $E_f=(a$ repeated α times, b repeated β times) of eigenvalues of f is of the form $E_f=(\nu_1,\nu_1^{-1},\ldots,\nu_{2^{m-2}},\nu_{2^{m-2}}^{-1})$. We claim that $\alpha=\beta=2^{m-2}$. Indeed, assume first that $a=a^{-1}$, i.e. that $a=\pm 1$. This implies that $b^{-1}\neq b$ and $b^{-1}\neq a$, because $b\neq\pm a=\pm 1$. So b^{-1} does not belong to $E_f=(a$ repeated α times, b repeated β times), and hence b itself does not belong to $E_f=(\nu_1,\nu_1^{-1},\ldots,\nu_{2^{m-2}},\nu_{2^{m-2}}^{-1})$, which is a contradiction. A similar argument shows that $b\neq b^{-1}$. Therefore $a\neq a^{-1}$ and $b\neq b^{-1}$. Since b belongs to $E_f=(\nu_1,\nu_1^{-1},\ldots,\nu_{2^{m-2}},\nu_{2^{m-2}}^{-1})$, b^{-1} belongs to E_f. Since $b^{-1}\neq b$, the only possibility is that $a=b^{-1}$, and hence the number of occurrences of a and of b in $E_f=(\nu_1,\nu_1^{-1},\ldots,\nu_{2^{m-2}},\nu_{2^{m-2}}^{-1})$ are the same. Thus $\alpha=\beta=2^{m-2}$. Now, the same argument as for the $m=4$ case treated above allows us to conclude the proof. □

Proposition 8. *The image of* $\mathrm{Spin}_{2m+1}(\mathbb{C})$ *in its spin representation does not contain a pair of semisimple elements satisfying* $(\mathcal{P})$.

Proof. Assume that the image G of $\mathrm{Spin}_{2m+1}(\mathbb{C})$ in its spin representation contains a pair of semisimple elements f,g satisfying $(\mathcal{P})$.

Proposition 3 ensures that $\mathrm{Lie}(G)=\mathfrak{g}$ contains an element u whose list of eigenvalues is $E_u=(\beta$ repeated α times, $-\alpha$ repeated β times). So there exist $\lambda_1,\ldots,\lambda_m$ in $\mathbb{C}$ such that

$$E_u=(\epsilon_1\lambda_1+\cdots+\epsilon_m\lambda_m\,;\ (\epsilon_1,\ldots,\epsilon_m)\in\{-1,1\}^m).$$

Since $(\lambda_1+\cdots+\lambda_m-2\lambda_1,\lambda_1+\cdots+\lambda_m-2\lambda_2,\ldots,\lambda_1+\cdots+\lambda_m-2\lambda_m)$ is a sublist of E_u, we get that $\mathrm{card}\{\lambda_i\mid 1\leqslant i\leqslant m\}\leqslant 2$.

Assume that $\mathrm{card}\{\lambda_i\mid 1\leqslant i\leqslant m\}=1$, i.e. that $\lambda:=\lambda_1=\cdots=\lambda_m$. We have $\lambda\neq 0$. Then

$$\begin{aligned}(\lambda_1+\cdots+\lambda_m,\ \lambda_1+\cdots+\lambda_m-2\lambda_1,\ \lambda_1+\cdots+\lambda_m-2\lambda_1-2\lambda_2,\ldots,\\ \lambda_1+\cdots+\lambda_m-2\lambda_1-\cdots-2\lambda_m)\\ =((m-2j)\lambda\,;\ 0\leqslant j\leqslant m)\end{aligned}$$

is a sublist of E_u made of $m+1>2$ mutually distinct numbers, and this is a contradiction.

Assume that $\mathrm{card}\{\lambda_i\mid 1\leqslant i\leqslant m\}=2$, i.e. that $\lambda:=\lambda_1=\cdots=\lambda_i$ and $\lambda_{i+1}=\cdots=\lambda_m=:\mu$ for some $1\leqslant i<m$ and some distinct complex numbers λ and μ. Up to renumbering, we can assume that $i\geqslant 2$. Using the fact that $(\pm\lambda\pm\lambda+\lambda_3+\cdots+\lambda_m)$ is a sublist of E_u, we see that $\lambda=0$. Moreover, $i=m-1$, because otherwise $(\lambda_1+\cdots+\lambda_{m-2}\pm\mu\pm\mu)$ would be a sublist of E_u made up of four distinct elements (as $\mu\neq\lambda=0$), which is impossible. So E_u has the form $(\mu$ repeated 2^{m-1} times, $-\mu$ repeated 2^{m-1} times), hence $\alpha=\beta=2^{m-1}$.

On the other hand, since g belongs to G, its list of eigenvalues $E_g = (c$ repeated $\alpha+1$ times, $d_1, \ldots, d_{\beta-1})$ is of the form $E_g = (\mu_1^{\epsilon_1} \cdots \mu_m^{\epsilon_m}\,;(\epsilon_1, \ldots, \epsilon_n) \in \{-1,1\}^m)$. This list is the concatenation of the 2^{m-1} lists

$$\left(\prod_{i\in\{1,\ldots,m\}\setminus\{i_1,\ldots,i_{p-1},i_p\}} \mu_i \cdot \prod_{i\in\{i_1,\ldots,i_{p-1},i_p\}} \mu_i^{-1}\,;\; i_{p-1} < i_p \leqslant m \right)$$

indexed by $1 \leqslant i_1 < \cdots < i_{p-1} \leqslant m-1$ with $0 \leqslant p \leqslant m$. Since $\alpha + 1 > 2^{m-1}$, we see that there exist $1 \leqslant i_1 < \cdots < i_{p-1} \leqslant m-1$ and $i_{p-1} < j, j' \leqslant m$ with $j \neq j'$ such that

$$\prod_{i\in\{1,\ldots,m\}\setminus\{i_1,\ldots,i_{p-1},j\}} \mu_i \cdot \prod_{i\in\{i_1,\ldots,i_{p-1},j\}} \mu_i^{-1} = \prod_{i\in\{1,\ldots,m\}\setminus\{i_1,\ldots,i_{p-1},j'\}} \mu_i \cdot \prod_{i\in\{i_1,\ldots,i_{p-1},j'\}} \mu_i^{-1}$$

and so $\mu_j^2 = \mu_{j'}^2$. Up to renumbering, we can assume that $\mu_1^2 = \mu_2^2$. So, for all $3 \leqslant k \leqslant m$, we have

$$\mu_1 \mu_2^{-1} \mu_k^{-1} \prod_{i\in\{1,\ldots,m\}\setminus\{1,2,k\}} \mu_i = \mu_1^{-1} \mu_2 \mu_k^{-1} \prod_{i\in\{1,\ldots,m\}\setminus\{1,2,k\}} \mu_i.$$

Therefore $\mu_1 \mu_2^{-1} \mu_k^{-1} \prod_{i\in\{1,\ldots,m\}\setminus\{1,2,k\}} \mu_i$ occurs with multiplicity greater than 1 in E_g, and hence

$$c = \mu_1 \mu_2^{-1} \mu_k^{-1} \prod_{i\in\{1,\ldots,m\}\setminus\{1,2,k\}} \mu_i.$$

Similarly, we have, for all $3 \leqslant k \leqslant m$,

$$c = \mu_1 \mu_2^{-1} \prod_{i\in\{1,\ldots,m\}\setminus\{1,2\}} \mu_i.$$

Therefore, for all $3 \leqslant k \leqslant m$, $\mu_k^2 = 1$, i.e. $\mu_k = \pm 1$. This clearly implies that any element of $E_g = (\mu_1^{\epsilon_1} \cdots \mu_m^{\epsilon_m}\,;\,(\epsilon_1, \ldots, \epsilon_n) \in \{-1,1\}^m)$ occurs with multiplicity at least 2, which is a contradiction. □

Proof of Theorem 2. Since G acts irreducibly on E, we have $G = Z(G)^\circ G'$ where $Z(G)^\circ$ denotes the connected center of G and G' the derived subgroup of G. Moreover, $Z(G)^\circ$ is included in the scalars, so $G' \subset G \subset \mathbb{C}^* G'$ and G' is a connected semisimple algebraic subgroup of $\mathrm{SL}(E)$ which acts irreducibly on E. Let f, g be a pair of semisimple elements of G satisfying $(\mathcal{P})$. Then there exist $t_f, t_g \in \mathbb{C}^*$ such that $f' = t_f f$ and $g' = t_g g$ belong to G'. It is clear that f', g' is a pair of semisimple elements of G' satisfying $(\mathcal{P})$. Proposition 4 ensures that G' is simple. Proposition 3 and Theorem 5 ensure that G' is classical and that, as a representation of G', E is minuscule. In view of the classification of minuscule representations given after Theorem 5, the result follows from Propositions 6, 7 and 8. □

3. Additional results

We let E be a $\mathbb{C}$-vector space of finite dimension $n \geqslant 2$.

Theorem 9. *Let G be a connected algebraic subgroup of $\mathrm{GL}(E)$. Assume that G contains a semisimple element u having n distinct eigenvalues and an element v which permutes cyclically the n eigenspaces of u. Then the derived subgroup G' of G is either the image of $\prod_{i=1}^{l} \mathrm{SL}(\mathbb{C}^{n_i})$ in $\bigotimes_{i=1}^{l}$ std for some $l \in \mathbb{N}^*$ and some pairwise coprime numbers $n_1, n_2, \ldots, n_l > 1$ or the image of $\mathrm{Sp}(\mathbb{C}^{n_1}) \times \prod_{i=2}^{l} \mathrm{SL}(\mathbb{C}^{n_i})$ in $\bigotimes_{i=1}^{l}$ std for some $l \in \mathbb{N}^*$ and some pairwise coprime numbers $n_1 \geqslant 4$ even and $n_2, \ldots, n_l > 1$. Moreover, $G' \subset G \subset \mathbb{C}^* G'$.*

https://doi.org/10.1112/S0010437X12000292 Published online by Cambridge University Press

Proof. The fact that G contains a semisimple element u having n distinct eigenvalues and an element v which permutes cyclically the corresponding eigenspaces implies that G acts irreducibly on E. So $G' \subset G \subset \mathbb{C}^* G'$ and G' is a connected semisimple algebraic subgroup of $\mathrm{SL}(E)$ which acts irreducibly on E (see the beginning of the proof of Theorem 2 for details) and contains an element u' $(= \xi u$ for some $\xi \in \mathbb{C}^*)$ with n distinct eigenvalues and an element v' $(= \zeta v$ for some $\zeta \in \mathbb{C}^*)$ that permutes cyclically the corresponding eigenspaces.

By virtue of [Kat87, Corollary 3.2.8], to conclude the proof it suffices to find a maximal torus $\mathcal{T}$ in G' and an element w in the normalizer $N(\mathcal{T})$ of $\mathcal{T}$ such that, as a representation of $\mathcal{T}$, E is the direct sum of n distinct characters which are cyclically permuted by the conjugation action of w. But since u' is a semisimple element of G', it is contained in a maximal torus $\mathcal{T}$ of G'. By commutativity, this maximal torus leaves invariant the n eigenspaces of u'. It is now clear that $\mathcal{T}$ and $w = v' \in N(\mathcal{T})$ have the required properties. □

Theorem 10. *Let G be a connected algebraic subgroup of $\mathrm{GL}(E)$ which acts irreducibly on E. If G contains a semisimple element f whose list of eigenvalues is of the form $(a$, b repeated $n-1$ times$)$ for some $a, b \in \mathbb{C}^*$ such that $a \neq \pm b$, then the derived subgroup G' of G is $\mathrm{SL}(E)$. Furthermore, $G' \subset G \subset \mathbb{C}^* G'$.*

Proof. Since G acts irreducibly on E, $G' \subset G \subset \mathbb{C}^* G'$ and G' is a connected semisimple algebraic subgroup of $\mathrm{SL}(E)$ which acts irreducibly on E (see the beginning of the proof of Theorem 2 for details) and contains $f' = tf$ for some $t \in \mathbb{C}^*$. Proposition 3 ensures that the semisimple Lie algebra $\mathfrak{g}'$ of G' contains a semisimple morphism whose list of eigenvalues is $(n-1,\ -1$ repeated $n-1$ times$)$. Since G' acts irreducibly on E, so does $\mathfrak{g}'$. Kostant's characterization of $\mathfrak{sl}(E)$ given in [Kos58] then ensures that $\mathfrak{g}' = \mathfrak{sl}(E)$ and hence that $G' = \mathrm{SL}(E)$. □

Part II. Applications to q-difference Galois theory

4. Review of useful facts and results

4.1 q-difference modules and systems

Let (K, σ) be a difference field and let $\mathcal{D}_{(K,\sigma)}$ be the noncommutative algebra $K\langle \sigma, \sigma^{-1}\rangle$ of noncommutative Laurent polynomials with coefficients in K satisfying the relation $\sigma a = \sigma(a)\sigma$ for any $a \in K$. The full subcategory of the category of $\mathcal{D}_{(K,\sigma)}$-modules whose objects are the $\mathcal{D}_{(K,\sigma)}$-modules of finite length is denoted by $\mathcal{E}_{(K,\sigma)}$. It is a K^σ-linear abelian tensor category, where $K^\sigma = \{a \in K \mid \sigma(a) = a\}$ is the subfield of constants of (K, σ).

It will sometimes be convenient to choose specific bases. We introduce the category $\mathcal{E}'_{(K,\sigma)}$, which is tensor-equivalent to $\mathcal{E}_{(K,\sigma)}$, described as follows: its objects are difference systems $(\sigma Y = AY)$ where $A \in \mathrm{GL}_n(K)$, and its morphisms from $(\sigma Y = AY)$, $A \in \mathrm{GL}_n(K)$, to $(\sigma Y = BY)$, $B \in \mathrm{GL}_m(K)$, are the matrices $F \in M_{m,n}(K)$ such that $BF = \sigma(F)A$.

We refer to [vdPS97, Chapter 1, especially § 1.4] or to [Sau04, § 1.1] for details. In particular, the tensor product, denoted by $\otimes$, and the dual, denoted by $\cdot^\vee$, are defined there.

We denote by $\mathbb{C}\{z\}$ the local ring of germs of analytic functions at 0 and by $\mathbb{C}(\{z\})$ its field of fractions; we denote by $\mathbb{C}[[z]]$ the local ring of formal series in z and by $\mathbb{C}((z))$ its field of fractions.

For $K = \mathbb{C}(z)$, $\mathbb{C}(\{z\})$ or $\mathbb{C}((z))$, we denote by σ_q the automorphism of K defined by $\sigma_q(a(z)) = a(qz)$. Then (K, σ_q) is a difference field with field of constants $\mathbb{C}$.

https://doi.org/10.1112/S0010437X12000292 Published online by Cambridge University Press

For any $N \in \mathbb{N}^*$, we set $q_N = q^{1/N}$ and denote by $[N] : \mathbb{C}^* \to \mathbb{C}^*$ the étale morphism $z \mapsto z^N$ and by $[N]^* : \mathcal{E}_{(\mathbb{C}((z)),\sigma_q)} \to \mathcal{E}_{(\mathbb{C}((z_N)),\sigma_{q_N})}$ the corresponding ramification functor (explicitly defined in [DiV02, § 1.4], for instance).

4.2 Slopes

Our main reference for slopes theory is [Sau04], where it is assumed that $|q| > 1$ (in opposition to our hypothesis of $|q| < 1$). The slopes defined in this paper are thus the opposite of those defined in [Sau04]; but since we use only the formal part of [Sau04], this has no impact on what follows.

The Newton polygon $\mathcal{N}(L)$ of $L = \sum_i a_i \sigma_q^i \in \mathcal{D}_{(\mathbb{C}((z)),\sigma_q)}$ is the convex hull in $\mathbb{R}^2$ of $\{(i,j) \mid i \in \mathbb{Z} \text{ and } j \geqslant v_z(a_i)\}$ where v_z denotes the z-adic valuation on $\mathbb{C}((z))$. This polygon is made up of two vertical half-lines and k vectors $(r_1, d_1), \ldots, (r_k, d_k) \in \mathbb{N}^* \times \mathbb{Z}$ having pairwise distinct slopes, called the slopes of L. For any $i \in \{1, \ldots, k\}$, r_i is called the multiplicity of the slope d_i/r_i.

Let M be an object of $\mathcal{E}_{(\mathbb{C}((z)),\sigma_q)}$. The cyclic vector lemma [DiV02, Lemma 1.3.1] ensures that there exists $L \in \mathcal{D}_{(\mathbb{C}((z)),\sigma_q)}$ such that $M \cong \mathcal{D}_{(\mathbb{C}((z)),\sigma_q)}/\mathcal{D}_{(\mathbb{C}((z)),\sigma_q)}L$. One can define the slopes of M to be the slopes of L and the multiplicity of a slope λ of M to be the multiplicity of λ as a slope of L. This definition is independent of the chosen L (see [Sau04, Théorème et définition 2.2.5]). An object M of $\mathcal{E}_{(\mathbb{C}((z)),\sigma_q)}$ is pure isoclinic if it has a unique slope.

For instance, for $a \in \mathbb{C}((z))^\times$, the Newton polygon of $M = \mathcal{D}_{(\mathbb{C}((z)),\sigma_q)}/\mathcal{D}_{(\mathbb{C}((z)),\sigma_q)}(\sigma_q - a)$ is the convex subset of $\mathbb{R}^2$ delimited by the vertical half-lines $\{0\} \times \mathbb{R}^+$ and $\{1\} \times [v_z(a), +\infty[$ together with the segment from $(0,0)$ to $(1, v_z(a))$. So M is pure isoclinic with slope $v_z(a)$. To give another example, $M = \mathcal{D}_{(\mathbb{C}((z)),\sigma_q)}/\mathcal{D}_{(\mathbb{C}((z)),\sigma_q)}(qz\sigma_q^2 - (1+z)\sigma_q + 1)$ has two slopes, namely 0 and 1, both with multiplicity 1.

4.3 Galois groups

Let $\mathcal{E}$ be a tannakian category over $\mathbb{C}$, and let ω be a $\mathbb{C}$-fiber functor on $\mathcal{E}$. For any object M of $\mathcal{E}$, we let $\langle M \rangle$ denote the tannakian category generated by M in $\mathcal{E}$ and let $\mathrm{Gal}(M, \omega)$ denote the complex linear algebraic group $\mathrm{Aut}^{\otimes}(\omega_{|\langle M \rangle})$. The choice of a specific fiber functor is of no consequence: since $\mathbb{C}$ is algebraically closed, any two $\mathbb{C}$-fiber functors on $\mathcal{E}$ are isomorphic. For the theory of tannakian categories, we refer to Deligne and Milne's paper [DM81].

4.3.1 *Connectedness.* Let M be an object of $\mathcal{E}_{(\mathbb{C}(z),\sigma_q)}$.

The categories $\mathcal{E}_{(\mathbb{C}((z)),\sigma_q)}$ and $\mathcal{E}_{(\mathbb{C}(z),\sigma_q)}$ are neutral tannakian over $\mathbb{C}$ (see [vdPS97, § 1.4]). Let $\widehat{\omega}$ be a $\mathbb{C}$-fiber functor on $\mathcal{E}_{(\mathbb{C}((z)),\sigma_q)}$. The formalization functor $\widehat{\cdot} : \mathcal{E}_{(\mathbb{C}(z),\sigma_q)} \to \mathcal{E}_{(\mathbb{C}((z)),\sigma_q)}$ being an exact and faithful $\otimes$-functor, $\omega = \widehat{\omega} \circ \widehat{\cdot}$ is a $\mathbb{C}$-fiber functor on $\mathcal{E}_{(\mathbb{C}(z),\sigma_q)}$.

The following result is [vdPS97, Proposition 12.2] (compare with Gabber's result [Kat87, Proposition 1.2.5]).

Proposition 11. *The natural closed immersion* $\mathrm{Gal}(\widehat{M}, \widehat{\omega}) \hookrightarrow \mathrm{Gal}(M, \omega)$ *of the local formal Galois group* $\mathrm{Gal}(\widehat{M}, \widehat{\omega})$ *of* M *at* 0 *into the Galois group* $\mathrm{Gal}(M, \omega)$ *of* M *induces a surjective morphism* $\mathrm{Gal}(\widehat{M}, \widehat{\omega})/\mathrm{Gal}(\widehat{M}, \widehat{\omega})^\circ \twoheadrightarrow \mathrm{Gal}(M, \omega)/\mathrm{Gal}(M, \omega)^\circ$.

Corollary 12. *If* $\mathrm{Gal}(\widehat{M}, \widehat{\omega})$ *is connected, then* $\mathrm{Gal}(M, \omega)$ *is connected.*

We give an additional corollary for later use.

Corollary 13. *Assume that M satisfies ($\mathscr{H}1$) and is regular singular at ∞ with exponents in $\{c \in \mathbb{C}^* \mid c^{n'} \in q^{\mathbb{Z}}\}$ for some $n' \in \mathbb{Z}^*$ coprime to the rank n of M. Then $\mathrm{Gal}(M, \omega)$ is connected.*

Proof. We set $G = \mathrm{Gal}(M, \omega)$ and denote by G_0 and G_∞ the local formal Galois groups of M at 0 and ∞, respectively. Proposition 16 below and [vdPR07, Example 5.6 in § 5.2] ensure that $G_0/G_0^\circ \cong (\mathbb{Z}/n^2\mathbb{Z})$. Proposition 11 implies that the order of any element of G/G° divides n^2. Moreover, using [vdPS97, ch. 12] or [Sau03, § 2.2], we see that the order of any element of G_∞/G_∞° divides n'. Proposition 11 ensures that the same property holds for the elements of G/G°. Therefore, G/G° is trivial. □

4.3.2 *Lie-irreducibility.*

Definition 14. We say that a list $c_1, \ldots, c_n$ of nonzero complex numbers is q-Kummer induced if there exist a divisor $d \geqslant 2$ of n and a permutation ν of $\{1, \ldots, n\}$ such that, for all $i \in \{1, \ldots, n\}$, $c_i = q^{1/d} c_{\nu(i)} \bmod q^{\mathbb{Z}}$.

Proposition 15. *If M is an irreducible object of $\mathcal{E}_{(\mathbb{C}(z),\sigma_q)}$ which is of rank n and regular singular at ∞ with non-q-Kummer-induced exponents $c_1, \ldots, c_n \in q^{\mathbb{R}}$, then M is Lie-irreducible, i.e. the action of $\mathrm{Gal}(M, \omega)^\circ$ on $\omega(M)$ is irreducible.*

Proof. For all $i \in \{1, \ldots, n\}$, let $\gamma_i \in \mathbb{R}$ be such that $c_i = q^{\gamma_i}$. It follows from [vdPS97, ch. 12] or [Sau03, § 2.2] that the local formal Galois group of M at ∞ is generated, as an algebraic group, by its neutral component and by a semisimple morphism f with list of eigenvalues $e^{2\pi i \gamma_1}, \ldots, e^{2\pi i \gamma_n}$. Proposition 11 implies that $G = \mathrm{Gal}(M, \omega)$ is generated, as an algebraic group, by G° and f. So, since the action of G on $\omega(M)$ is irreducible, its restriction to the abstract group H generated by G° and f is still irreducible. Assume that M is not Lie-irreducible and let $V \neq \{0\}, \omega(M)$ be a minimal invariant subspace of $\omega(M)$ for the action of G°. For all $k \in \mathbb{Z}$, $f^k V$ is an invariant subspace of $\omega(M)$ for the action of G°, because G° is a normal subgroup of G. Therefore $\sum_{k \in \mathbb{Z}} f^k V$ is an invariant subspace of $\omega(M)$ for the action of H and hence $\omega(M) = \sum_{k \in \mathbb{Z}} f^k V$. Let d be the smallest integer greater than 1 such that $\omega(M) = \sum_{k=0}^{d-1} f^k V$. It is easily seen that $\omega(M) = \bigoplus_{k=0}^{d-1} f^k V$. This implies that f and $e^{2\pi i/d} f$ are conjugate. Considering the eigenvalues of f, we see that there exists a permutation ν of $\{1, \ldots, n\}$ such that, for all $i \in \{1, \ldots, n\}$, $e^{2\pi i \gamma_i} = e^{2\pi i/d} e^{2\pi i \gamma_{\nu(i)}}$, i.e. $c_i = q^{1/d} c_{\nu(i)} \bmod q^{\mathbb{Z}}$. Since $n = d \dim V$, d divides n. □

5. Main theorem in the one-slope case

Proposition 16 (Reformulation of ($\mathscr{H}1$)). *Let $\widehat{M}$ be an object of $\mathcal{E}_{(\mathbb{C}((z)),\sigma_q)}$ of rank $n \geqslant 2$. The following properties are equivalent:*

(a) *$\widehat{M}$ is irreducible (i.e. simple);*

(b) *$\widehat{M} \cong \widehat{M}_q(n, m, a) := \mathcal{D}_{(\mathbb{C}((z)),\sigma_q)}/\mathcal{D}_{(\mathbb{C}((z)),\sigma_q)}(\sigma_q^n - q_n^{mn(n-1)/2} a z^m)$ for some $m \in \mathbb{Z}^*$ coprime to n and some $a \in \mathbb{C}^*$;*

(c) *$\widehat{M}$ satisfies ($\mathscr{H}1$).*

Proof. The equivalence (a) ⇔ (b) is [vdPR07, Proposition 1.3], and (b) ⇒ (c) is obvious. It remains to prove (c) ⇒ (a). Assume that $\widehat{M}$ satisfies ($\mathscr{H}1$). Let $\widehat{M}'$ be a nonzero subobject of $\widehat{M}$. Then $\widehat{M}'$ is pure isoclinic with slope μ (see [Sau04, Théorème 2.3.1]). In order to prove that $\widehat{M} = \widehat{M}'$, it is sufficient to prove that the rank n' of $\widehat{M}'$ is greater than or equal to n.

This is indeed the case as $n'\mu$ has to be a relative integer (immediate from the definition of the slopes of $\widehat{M}'$). $\square$

Lemma 17. *If $M_1, \dots, M_l$ are objects of $\mathcal{E}_{(\mathbb{C}(z),\sigma_q)}$ of rank greater than 1 such that $M = M_1 \otimes \cdots \otimes M_l$ satisfies $(\mathscr{H}1)$, then $M_1, \dots, M_l$ satisfy $(\mathscr{H}1)$.*

Proof. Let $n, n_1, \dots, n_l$ be the respective ranks of $M, M_1, \dots, M_l$. Note that $n = n_1 \cdots n_l$. Since $M = M_1 \otimes \cdots \otimes M_l$ is pure isoclinic at 0 with slope $\mu = m/n$, $M_1, \dots, M_l$ are pure isoclinic at 0 with respective slopes $\mu_1, \dots, \mu_l$ such that $\mu = \mu_1 + \cdots + \mu_l$ (see [Sau04, Théorème 2.3.1]). For any $i \in \{1, \dots, l\}$, μ_i has the form m_i/n_i for some $m_i \in \mathbb{Z}$. The equalities $m/n = \mu = \mu_1 + \cdots + \mu_l = m_1/n_1 + \cdots + m_l/n_l$ and $n = n_1 \cdots n_l$, together with the fact that m is coprime to n, imply that for any $i \in \{1, \dots, l\}$, m_i is coprime to n_i. $\square$

Lemma 18. *Let M be an object of $\mathcal{E}_{(\mathbb{C}(z),\sigma_q)}$ which is of rank n and satisfies $(\mathscr{H}1)$. Assume that $M \cong M_1 \otimes M_2$ for some objects M_1 and M_2 of $\mathcal{E}_{(\mathbb{C}(z),\sigma_q)}$ with respective ranks $n_1 > 1$ and n_2. If $M_1^\vee \cong U_1 \otimes M_1$ for some rank-one object U_1 of $\mathcal{E}_{(\mathbb{C}(z),\sigma_q)}$, then $n_1 = 2$.*

Proof. We have $M^\vee \cong M_1^\vee \otimes M_2^\vee \cong U_1 \otimes M_1 \otimes M_2^\vee$. Lemma 17 ensures that both M_1 and M_2 satisfy $(\mathscr{H}1)$. Denoting by μ_1, μ_2 and ν the respective slopes of M_1, M_2 and U_1 at 0, we get that the unique slope $-\mu_1 - \mu_2$ of $M^\vee$ at 0 is equal to the unique slope $\nu + \mu_1 - \mu_2$ of $U_1 \otimes M_1 \otimes M_2^\vee$ at 0. So $2\mu_1 = -\nu \in \mathbb{Z}$ (because U_1 has rank one). Since M_1 satisfies $(\mathscr{H}1)$, we get $n_1 = 2$. $\square$

This following result was (essentially) proved by van der Put and Singer in [vdPS97, § 1.2]. Following the referees' suggestion, we shall give a sketch of the proof here.

Proposition 19. *If $(\sigma_q Y = AY)$ is an object of $\mathcal{E}'_{(\mathbb{C}(z),\sigma_q)}$ which is of rank n and has a connected Galois group G, then there exists an object $(\sigma_q Y = BY)$ of $\mathcal{E}'_{(\mathbb{C}(z),\sigma_q)}$ isomorphic to $(\sigma_q Y = AY)$ such that B belongs to $G(\mathbb{C}(z))$.*

Proof. We keep, and specialize to our situation, the notation of [vdPS97, § 1.2]: let $k = \mathbb{C}(z)$, $\phi = \sigma_q$ and $C = \mathbb{C}$. The Galois group G can be seen as the group of k-automorphisms which commute with ϕ of some Picard–Vessiot ring R over k of $(\sigma_q Y = AY)$. We consider the algebraic group $G_k = G \otimes_{\mathbb{C}} k$ in $\mathrm{GL}_{n;k}$. Also, we consider the reduced algebraic subset Z of $\mathrm{GL}_{n;k}$ corresponding to R. From [vdPS97, Theorem 1.13] it follows that Z/k has a natural structure of G-torsor: the morphism $Z \times_k G_k \to G_k \times_k G_k$ given by $(z, g) \mapsto (zg, g)$ is an isomorphism. But $k = \mathbb{C}(z)$ is a $\mathcal{C}^1$-field and G is connected, so [vdPS97, Corollary 1.18] and the discussion following it ensure that Z/k is a trivial G-torsor. Therefore $Z(k)$ is nonempty, and for $U \in Z(k)$ we have $Z(\overline{k}) = UG(\overline{k})$. We now use the τ-invariance of Z (the map τ is defined at the beginning of [vdPS97, § 1.2] and the τ-invariance property is [vdPS97, Lemma 1.10]): since $\tau Z(\overline{k}) = Z(\overline{k})$, we have $\tau(UG(\overline{k})) = UG(\overline{k})$, i.e. $A^{-1}\phi(U)G(\overline{k}) = UG(\overline{k})$ (where we have used the fact that $\tau(UG(\overline{k})) = A^{-1}\phi(U)\phi G(\overline{k}) = A^{-1}\phi(U)G(\overline{k})$). Hence $\phi(U)^{-1}AU \in G(k)$. $\square$

Theorem 20 (Main theorem in the one-slope case). *Let M be an object of $\mathcal{E}_{(\mathbb{C}(z),\sigma_q)}$ which is of rank n, has a connected Galois group and satisfies $(\mathscr{H}1)$. Then $\mathrm{Gal}(M, \omega)$ is the image of $\prod_{i=1}^l \mathrm{GL}(\mathbb{C}^{n_i})$ in $\bigotimes_{i=1}^l \mathrm{std}$ for some $l \in \mathbb{N}^*$ and some pairwise coprime numbers $n_1, \dots, n_l > 1$ such that $n = n_1 \cdots n_l$.*

Proof. We set $G = \mathrm{Gal}(M, \omega)$. Proposition 16 and [vdPR07, Example 5.6 in § 5.2] show that the hypotheses of Theorem 9 are satisfied by G and hence that the derived subgroup G'

of G is either the image of $\prod_{i=1}^{l}\mathrm{SL}(\mathbb{C}^{n_i})$ in $\bigotimes_{i=1}^{l}\mathrm{std}$ for some $l\in\mathbb{N}^*$ and some pairwise coprime numbers $n_1,n_2,\ldots,n_l>1$ or the image of $\mathrm{Sp}(\mathbb{C}^{n_1})\times\prod_{i=2}^{l}\mathrm{SL}(\mathbb{C}^{n_i})$ in $\bigotimes_{i=1}^{l}\mathrm{std}$ for some $l\in\mathbb{N}^*$ and some pairwise coprime numbers $n_1\geqslant 4$ even and $n_2,\ldots,n_l>1$ and that $G'\subset G\subset\mathbb{C}^*G'$. Since $\det(M)$ is a rank-one irregular object of $\mathcal{E}_{(\mathbb{C}(z),\sigma_q)}$, its Galois group is $\mathbb{C}^*$, so $G=\mathbb{C}^*G'$. Therefore, G is either the image of $\prod_{i=1}^{l}\mathrm{GL}(\mathbb{C}^{n_i})$ in $\bigotimes_{i=1}^{l}\mathrm{std}$ or the image of $\mathbb{C}^*\,\mathrm{Sp}(\mathbb{C}^{n_1})\times\prod_{i=2}^{l}\mathrm{GL}(\mathbb{C}^{n_i})$ in $\bigotimes_{i=1}^{l}\mathrm{std}$. It remains to exclude the second case. Assume to the contrary that G is $\mathbb{C}^*\,\mathrm{Sp}(\mathbb{C}^{n_1})\times\prod_{i=2}^{l}\mathrm{GL}(\mathbb{C}^{n_i})$ in $\bigotimes_{i=1}^{l}\mathrm{std}$. Using Proposition 19, we would get $M\cong M_1\otimes\cdots\otimes M_l$ for some objects $M_1,\ldots,M_l$ of $\mathcal{E}_{(\mathbb{C}(z),\sigma_q)}$, where M_1 is such that $M_1^\vee\cong U_1\otimes M_1$ for some rank-one object U_1 of $\mathcal{E}_{(\mathbb{C}(z),\sigma_q)}$. Lemma 18 would then imply that $n_1=2$. This is a contradiction. □

Definition 21. An object M of $\mathcal{E}_{(\mathbb{C}(z),\sigma_q)}$ is $\otimes$-decomposable if there exist two objects M_1 and M_2 of $\mathcal{E}_{(\mathbb{C}(z),\sigma_q)}$ of rank at least 2 such that $M\cong M_1\otimes M_2$.

Corollary 22. *Let M be an object of $\mathcal{E}_{(\mathbb{C}(z),\sigma_q)}$ which is of rank n, has a connected Galois group and satisfies ($\mathscr{H}1$). If M is $\otimes$-indecomposable, then $\mathrm{Gal}(M,\omega)$ is $\mathrm{GL}(\omega(M))$.*

Proof. This is a direct consequence of Theorem 20 and Proposition 19. □

6. Main theorem in the two-slopes case

Lemma 23. *Let M be an object of $\mathcal{E}_{(\mathbb{C}(z),\sigma_q)}$ of rank $n\geqslant 3$ satisfying ($\mathscr{H}2$). Then $\mathrm{Gal}(M,\omega)$ is neither a subgroup of $\mathbb{C}^*\mathrm{SO}(\omega(M))$ nor a subgroup of $\mathbb{C}^*\mathrm{Sp}(\omega(M))$ (for some bilinear forms).*

Proof. Let H be either $\mathrm{SO}(\omega(M))$ or $\mathrm{Sp}(\omega(M))$ and set $G=\mathbb{C}^*H$. Assume that $\mathrm{Gal}(M,\omega)$ is a subgroup of G. Let ρ be the representation of $\mathrm{Gal}(M,\omega)$ corresponding to M by tannakian duality. Let χ be the character of G defined, for any $t\in\mathbb{C}^*$ and any $A\in H$, by $\chi(tA)=t^2$. The dual $\rho^\vee$ of ρ is conjugated to $\rho\otimes(\chi^{-1}\circ\rho)$. Therefore, there exists a rank-one object U of $\langle M\rangle$ such that $M^\vee\cong U\otimes M$. But at 0 (see [Sau04, Théorème 2.3.1]), $M^\vee$ has two slopes, namely 0 with multiplicity $n-r$ and $-\mu$ with multiplicity r, while $U\otimes M$ has two slopes, namely ν with multiplicity $n-r$ and $\mu+\nu$ with multiplicity r where $\nu\in\mathbb{Z}$ denotes the unique slope of U. The only possibility is $\mu=0$, which gives a contradiction. □

Theorem 24 (Main theorem in the two-slopes case). *Let M be an irreducible object of $\mathcal{E}_{(\mathbb{C}(z),\sigma_q)}$ which is of rank n, has a connected Galois group and satisfies ($\mathscr{H}2$). Then $\mathrm{Gal}(M,\omega)=\mathrm{GL}(\omega(M))$.*

Proof. The formal slopes decomposition [Sau04, Théorème 3.1.7] ensures that $\widehat{M}\cong\widehat{M}_0\oplus\widehat{M}_\mu$, where $\widehat{M}_0$ is a regular singular object of $\mathcal{E}_{(\mathbb{C}((z)),\sigma_q)}$ with exponents in $q^{\mathbb{R}}$ and $\widehat{M}_\mu$ is a pure isoclinic object of $\mathcal{E}_{(\mathbb{C}((z)),\sigma_q)}$ of slope μ and rank r. Proposition 16 ensures that $\widehat{M}_\mu\cong\widehat{M}_q(r,m,a)$ for some $a\in\mathbb{C}^*$, so $\widehat{M}\cong\widehat{M}_0\oplus\widehat{M}_q(r,m,a)$. Thus $\mathrm{Gal}(M,\omega)$ contains, with respect to a suitable basis, $I_{n-r}\oplus\mathbb{C}^*I_r$ and $I_{n-r}\oplus\mathrm{diag}(1,\zeta,\ldots,\zeta^{r-1})$ where ζ is a primitive rth root of 1 (a consequence of applying [vdPR07, § 5] or [RS07, § 3.2] to $[r]^*\widehat{M}\cong[r]^*\widehat{M}_0\bigoplus_{c^r=a}\widehat{M}_{q_r}(1,0,c)\otimes\widehat{M}_{q_r}(1,m,1)$). If $r\geqslant 2$, Theorem 2 implies that $G\subset\mathrm{Gal}(M,\omega)\subset\mathbb{C}^*G$ with $G=\mathrm{SL}(\omega(M))$, $\mathrm{SO}(\omega(M))$ or $\mathrm{Sp}(\omega(M))$. Note that the Galois group of $\det(M)$ is $\mathbb{C}^*$ because $\det(M)$ is irregular of rank one, so $\mathrm{Gal}(M,\omega)$ is $\mathbb{C}^*G$. Lemma 23 leads to the conclusion. If $r=1$, the result follows from Theorem 10. □

7. Some computations of Galois groups

7.1 Generalized q-hypergeometric equations with two slopes

We keep the notation of § 1 (and the hypothesis that $r>s$) for the generalized q-hypergeometric operator with parameters $\underline{a}=(a_1,\dots,a_r)\in(q^{\mathbb{R}})^r$, $\underline{b}=(b_1,\dots,b_s)\in(q^{\mathbb{R}})^s$ and $\lambda\in\mathbb{C}^*$, and we set

$$\mathcal{H}_q(\underline{a};\underline{b};\lambda)=\mathcal{D}_{(\mathbb{C}(z),\sigma_q)}/\mathcal{D}_{(\mathbb{C}(z),\sigma_q)}\mathcal{L}_q(\underline{a};\underline{b};\lambda).$$

If $s>0$, then $\mathcal{H}_q(\underline{a};\underline{b};\lambda)$ satisfies $(\mathscr{H}2)$ (its slopes at 0 are 0 with multiplicity s and $1/(r-s)$ with multiplicity $r-s$). Theorem 24 leads to the following.

Theorem 25. *The general linear group $\mathrm{GL}(\mathbb{C}^r)$ is the unique connected algebraic group occurring as the Galois group of some irreducible generalized q-hypergeometric module $\mathcal{H}_q(\underline{a};\underline{b};\lambda)$ with parameters $\underline{a}=(a_1,\dots,a_r)\in(q^{\mathbb{R}})^r$ and $\underline{b}=(b_1,\dots,b_s)\in(q^{\mathbb{R}})^s$ with $r>s>0$.*

We now turn to explicit computations of q-hypergeometric Galois groups. For all $i\in\{1,\dots,r\}$, we denote by α_i the unique element of $\mathbb{R}$ such that $a_i=q^{\alpha_i}$.

Theorem 26. *Assume that $s>0$, that $\beta_j-\alpha_i\notin\mathbb{Z}$ for all $(i,j)\in\{1,\dots,r\}\times\{1,\dots,s\}$, and that the algebraic group generated by $\mathrm{diag}(e^{2\pi i\alpha_1},\dots,e^{2\pi i\alpha_r})$ is connected. Then $\mathrm{Gal}(\mathcal{H}_q(\underline{a};\underline{b};\lambda),\omega)=\mathrm{GL}(\mathbb{C}^r)$.*

Proof. Since, for all $(i,j)\in\{1,\dots,r\}\times\{1,\dots,s\}$, $\beta_j-\alpha_i\notin\mathbb{Z}$, we have that $\mathcal{H}_q(\underline{a};\underline{b};\lambda)$ is irreducible (using the same arguments as in [Roq11, § 5.1]). Moreover, $\mathcal{H}_q(\underline{a};\underline{b};\lambda)$ is regular singular at ∞ with exponents $a_1,\dots,a_r$. It follows easily from [vdPS97, ch. 12] or [Sau03, § 2.2] that if the algebraic group generated by $\mathrm{diag}(e^{2\pi i\alpha_1},\dots,e^{2\pi i\alpha_r})$ is connected, then the local formal Galois group of $\mathcal{H}_q(\underline{a};\underline{b};\lambda)$ at ∞ is connected; hence, by virtue of (the variant at ∞ of) Corollary 12, $\mathrm{Gal}(\mathcal{H}_q(\underline{a};\underline{b};\lambda),\omega)$ is connected. Theorem 25 leads to the desired result. □

For instance, the algebraic group generated by $\mathrm{diag}(e^{2\pi i\alpha_1},\dots,e^{2\pi i\alpha_r})$ is connected if $\underline{a}\in\left(q^{\mathbb{Z}}\right)^r$ or if $\alpha_1,\dots,\alpha_r$ are $\mathbb{Z}$-linearly independent.

7.2 q-Kloosterman equations

We retain the notation of § 1 for the q-Kloosterman operators and set

$$\mathcal{K}l_q(U,V)=\mathcal{D}_{(\mathbb{C}(z),\sigma_q)}/\mathcal{D}_{(\mathbb{C}(z),\sigma_q)}\,\mathrm{Kl}_q(U,V).$$

Note that $\mathcal{K}l_q(U,V)$ is pure isoclinic at 0 with slope $\deg V/\deg U$. In particular, if $\deg U$ is coprime to $\deg V$, then $\mathcal{K}l_q(U,V)$ satisfies $(\mathscr{H}1)$. Theorem 20 and Corollary 22 lead to the following result.

Theorem 27. *Let G be a connected algebraic group occurring as the Galois group of some q-Kloosterman module $\mathcal{K}l_q(U,V)$ such that $\deg U$ is coprime to $\deg V$. Then G is the image of $\prod_{i=1}^{l}\mathrm{GL}(\mathbb{C}^{n_i})$ in $\bigotimes_{i=1}^{l}\mathrm{std}$ for some $l\in\mathbb{N}^*$ and some pairwise coprime numbers $n_1,\dots,n_l>1$ such that $\deg U=n_1\cdots n_l$. If, moreover, $\mathcal{K}l_q(U,V)$ is $\otimes$-indecomposable, then G is $\mathrm{GL}(\mathbb{C}^{\deg U})$.*

We denote by $c_1,\dots,c_{\deg U}$ the roots of $X^u(U(X^{-1})+V(0))\in\mathbb{C}[X]$. For all $i\in\{1,\dots,\deg U\}$, we denote by (u_i,α_i) the unique element of $\mathbb{U}\times\mathbb{R}$ such that $c_i=u_iq^{\alpha_i}$.

Theorem 28. *If* $\deg U$ *is coprime to* $\deg V$ *and if the algebraic group generated by* $\mathrm{diag}(u_1,\dots,u_{\deg U})$ *and* $\mathrm{diag}(e^{2\pi i\alpha_1},\dots,e^{2\pi i\alpha_{\deg U}})$ *is connected, then* $\mathrm{Gal}(\mathcal{K}l_q(U,V),\omega)$ *is the image of* $\prod_{i=1}^{l}\mathrm{GL}(\mathbb{C}^{n_i})$ *in* $\bigotimes_{i=1}^{l}\mathrm{std}$ *for some* $l\in\mathbb{N}^*$ *and some pairwise coprime numbers* $n_1,\dots,n_l>1$ *such that* $\deg U=n_1\cdots n_l$. *If, moreover,* $\mathcal{K}l_q(U,V)$ *is* $\otimes$*-indecomposable, then* $\mathrm{Gal}(\mathcal{K}l_q(U,V),\omega)$ *is* $\mathrm{GL}(\mathbb{C}^{\deg U})$.

Proof. Note that $\mathcal{K}l_q(U,V)$ is regular singular at ∞ with exponents $c_1,\dots,c_{\deg U}$. It follows easily from [vdPS97, ch. 12] or [Sau03, § 2.2] that if the algebraic group generated by $\mathrm{diag}(u_1,\dots,u_{\deg U})$ and $\mathrm{diag}(e^{2\pi i\alpha_1},\dots,e^{2\pi i\alpha_{\deg U}})$ is connected, then the local formal Galois group of $\mathcal{K}l_q(U,V)$ at ∞ is connected and hence, by virtue of (the variant at ∞ of) Corollary 12, $\mathrm{Gal}(\mathcal{K}l_q(U,V),\omega)$ is connected. Theorem 27 leads to the desired result. □

Note that a q-Kloosterman module $\mathcal{K}l_q(U,V)$ with $\deg U$ coprime to $\deg V$ is not necessarily $\otimes$-indecomposable. For instance,

$$\begin{aligned}&\mathcal{K}l_q(X^6,-(1+q^{-4}X)(1+q^{-3}X)(1+q^{-2}X)(1+X)^2)\\ &\quad\cong\mathcal{K}l_q(X^2,-(1+X))\otimes\mathcal{K}l_q(X^3,-(1+X)).\end{aligned}$$

8. A $\otimes$-indecomposability criterion and application to q-Kloosterman operators (including $\mathcal{H}_q(\underline{a};\emptyset;\lambda)$)

8.1 A $\otimes$-indecomposability criterion

Slopes theory leads to a simple proof of the $\otimes$-indecomposability of the Kloosterman differential modules with bidegree (u,v) such that u is coprime to v; see [Kat87]. In contrast, we gave at the end of § 7.2 an example of $\otimes$-decomposable q-Kloosterman module $\mathcal{K}l_q(U,V)$ with $\deg U$ coprime to $\deg V$. In this section, we propose an obstruction to $\otimes$-decomposability (Theorem 31 below) coming from residues at points in $\mathbb{C}^*$ of intrinsic Birkhoff matrices. In [Roq11], we used related ideas to obtain an analogue of the usual notion of monodromy for the generalized q-hypergeometric equations.

We first work with q-difference systems.

Definition 29 (Property (H_q)). We say that an object $(\sigma_qY=AY)$ of $\mathcal{E}'_{(\mathbb{C}(z),\sigma_q)}$ of rank n satisfies the condition (H_q) if:

(1) there exists $z_0\in\mathbb{C}^*$ such that A is analytic at any point of $q^{\mathbb{Z}}z_0$, $A(z_0)$ has rank $n-1$ and, for all $k\in\mathbb{Z}^*$, $A(q^kz_0)\in\mathrm{GL}_n(\mathbb{C})$;

(2) $(\sigma_qY=AY)$ is pure isoclinic at both 0 and ∞.

Lemma 30. *Let* $(\sigma_qY=AY)$ *be an object of* $\mathcal{E}'_{(\mathbb{C}(z),\sigma_q)}$ *of rank* n. *If* $(\sigma_qY=AY)$ *is pure isoclinic at* 0 *and* ∞ *with integral slopes denoted, respectively, by* μ_0 *and* μ_∞, *then:*

(i) *there exist* $A^{(0)}\in\mathrm{GL}_n(\mathbb{C})$ *and* $F^{(0)}\in\mathrm{GL}_n(\mathbb{C}(\{z\}))$ *such that* $F^{(0)}$ *is an isomorphism in* $\mathcal{E}'_{(\mathbb{C}((z)),\sigma_q)}$ *from* $(\sigma_qY=z^{\mu_0}A^{(0)}Y)$ *to* $(\sigma_qY=AY)$. *Similarly, there exist* $A^{(\infty)}\in\mathrm{GL}_n(\mathbb{C})$ *and* $F^{(\infty)}\in\mathrm{GL}_n(\mathbb{C}(\{z^{-1}\}))$ *such that* $F^{(\infty)}$ *is an isomorphism in* $\mathcal{E}'_{(\mathbb{C}((z^{-1})),\sigma_{q_r})}$ *from* $(\sigma_qY=z^{\mu_\infty}A^{(\infty)}Y)$ *to* $(\sigma_qY=AY)$.

If, moreover, $(\sigma_qY=AY)$ *satisfies* (H_q), *then:*

(ii) *for any* $A^{(0)}$, $F^{(0)}$, $A^{(\infty)}$ *and* $F^{(\infty)}$ *satisfying the conditions of* (i), *we have, for* z *near* z_0, $(F^{(0)})^{-1}F^{(\infty)}(z)=H \bmod (z-z_0)M_n(\mathbb{C}\{z-z_0\})$ *for some* $H\in M_n(\mathbb{C})$ *with rank* $n-1$.

https://doi.org/10.1112/S0010437X12000292 Published online by Cambridge University Press

Proof. For (i), we refer to [RS07, § 2.2] and the references therein. We now prove that (ii) holds. Since $F^{(0)}$ is an isomorphism from $(\sigma_q Y = z^{\mu_0} A^{(0)} Y)$ to $(\sigma_q Y = AY)$, we have, for z near 0, $F^{(0)}(qz) z^{\mu_0} A^{(0)} = A(z) F^{(0)}(z)$. Similarly, for z near ∞, $F^{(\infty)}(qz) z^{\mu_\infty} A^{(\infty)} = A(z) F^{(\infty)}(z)$. These equations, together with the fact that $F^{(0)} \in \mathrm{GL}_n(\mathbb{C}(\{z\}))$ and $F^{(\infty)} \in \mathrm{GL}_n(\mathbb{C}(\{z^{-1}\}))$, show that $F^{(0)}$ and $F^{(\infty)}$ can be extended meromorphically to $\mathbb{C}$ and $\mathbb{C}^*$, respectively, and that for all $m \in \mathbb{N}^*$ we have, over $\mathbb{C}^*$,

$$(F^{(0)})^{-1} F^{(\infty)}(z) = z^{-m\mu_0} q^{-(m(m-1)/2)\mu_0} (A^{(0)})^{-m} (F^{(0)})^{-1}(q^m z) A(q^{m-1} z) \cdots A(z) \cdot A(q^{-1} z) \cdots A(q^{-m} z) F^{(\infty)}(q^{-m} z) (A^{(\infty)})^{-m} z^{-m\mu_\infty} q^{(m(m+1)/2)\mu_\infty}.$$

Now the result follows easily from the facts that $(F^{(0)})^{-1} \in \mathrm{GL}_n(\mathbb{C}(\{z\}))$, $F^{(\infty)} \in \mathrm{GL}_n(\mathbb{C}(\{z^{-1}\}))$, $A(z) = A(z_0) \bmod (z - z_0) M_n(\mathbb{C}\{z - z_0\})$ and, for any $k \in \mathbb{Z}^*$, $A(q^k z) \in \mathrm{GL}_n(\mathbb{C}) + (z - z_0) M_n(\mathbb{C}\{z - z_0\})$. □

Theorem 31 ($\otimes$-indecomposability criterion for systems). *Let $(\sigma_q Y = AY)$ be an object of $\mathcal{E}'_{(\mathbb{C}(z),\sigma_q)}$ which satisfies (H_q). Then $(\sigma_q Y = AY)$ is $\otimes$-indecomposable.*

Proof. Assume to the contrary that $(\sigma_q Y = AY)$ is $\otimes$-decomposable. Then there exist $A_1 \in \mathrm{GL}_{n_1}(\mathbb{C}(z))$ and $A_2 \in \mathrm{GL}_{n_2}(\mathbb{C}(z))$ $(n_1, n_2 > 1)$ such that $(\sigma_q Y = AY) \cong (\sigma_q Y = A_1 Y) \otimes (\sigma_q Y = A_2 Y)$. For further use, we denote by $R \in \mathrm{GL}_n(\mathbb{C}(z))$ an isomorphism from $(\sigma_q Y = A_1 Y) \otimes (\sigma_q Y = A_2 Y)$ to $(\sigma_q Y = AY)$. Since $(\sigma_q Y = AY) \cong (\sigma_q Y = A_1 Y) \otimes (\sigma_q Y = A_2 Y)$ is pure isoclinic, both $(\sigma_q Y = A_1 Y)$ and $(\sigma_q Y = A_2 Y)$ are pure isoclinic (see [Sau04, Théorème 2.3.1]). Let $N \in \mathbb{N}^*$ be such that $[N]^*(\sigma_q Y = A_1 Y) \cong (\sigma_q Y = [N]^* A_1 Y)$, $[N]^*(\sigma_q Y = A_2 Y) \cong (\sigma_q Y = [N]^* A_1 Y)$ and $[N]^*(\sigma_q Y = AY) \cong (\sigma_q Y = [N]^* A_1 Y) \otimes (\sigma_q Y = [N]^* A_2 Y)$ are all pure isoclinic with integral slopes. Lemma 30 ensures that there are $\mu_{1;0}, \mu_{1;\infty}, \mu_{2;0}, \mu_{1;\infty} \in \mathbb{Z}$ such that there exist:

- $A_1^{(0)} \in \mathrm{GL}_{n_1}(\mathbb{C})$ and $F_1^{(0)} \in \mathrm{GL}_{n_1}(\mathbb{C}(\{z_N\}))$ such that $F_1^{(0)}$ is an isomorphism from $\sigma_{q_N} Y = z_N^{\mu_{1;0}} A_1^{(0)} Y$ to $\sigma_{q_N} Y = [N]^* A_1 Y$;
- $A_1^{(\infty)} \in \mathrm{GL}_{n_1}(\mathbb{C})$ and $F_1^{(\infty)} \in \mathrm{GL}_{n_1}(\mathbb{C}(\{z_N^{-1}\}))$ such that $F_1^{(\infty)}$ is an isomorphism from $\sigma_{q_N} Y = z_N^{\mu_{1;\infty}} A_1^{(\infty)} Y$ to $\sigma_{q_N} Y = [N]^* A_1 Y$;
- $A_2^{(0)} \in \mathrm{GL}_{n_2}(\mathbb{C})$ and $F_2^{(0)} \in \mathrm{GL}_{n_2}(\mathbb{C}(\{z_N\}))$ such that $F_2^{(0)}$ is an isomorphism from $\sigma_{q_N} Y = z_N^{\mu_{2;0}} A_2^{(0)} Y$ to $\sigma_{q_N} Y = [N]^* A_2 Y$;
- $A_2^{(\infty)} \in \mathrm{GL}_{n_2}(\mathbb{C})$ and $F_2^{(\infty)} \in \mathrm{GL}_{n_2}(\mathbb{C}(\{z_N^{-1}\}))$ such that $F_2^{(\infty)}$ is an isomorphism from $\sigma_{q_N} Y = z_N^{\mu_{2;\infty}} A_2^{(\infty)} Y$ to $\sigma_{q_N} Y = [N]^* A_2 Y$.

So $F^{(0)} = ([N]^* R)(F_1^{(0)} \otimes F_2^{(0)}) \in \mathrm{GL}_n(\mathbb{C}(\{z_N\}))$ is an isomorphism from $(\sigma_{q_N} Y = z_N^{\mu_{1;0}} A_1^{(0)} Y) \otimes (\sigma_{q_N} Y = z_N^{\mu_{2;0}} A_2^{(0)} Y)$ to $(\sigma_{q_N} Y = [N]^* AY)$ and $F^{(\infty)} = ([N]^* R)(F_1^{(\infty)} \otimes F_2^{(\infty)}) \in \mathrm{GL}_n(\mathbb{C}(\{z_N^{-1}\}))$ is an isomorphism from $(\sigma_{q_N} Y = z_N^{\mu_{1;\infty}} A_1^{(\infty)} Y) \otimes (\sigma_{q_N} Y = z_N^{\mu_{2;\infty}} A_2^{(\infty)} Y)$ to $(\sigma_{q_N} Y = [N]^* AY)$. It is easily seen that $(\sigma_{q_N} Y = [N]^* AY)$ satisfies (H_{q_N}). So Lemma 30 ensures that, near some $z_0 \in \mathbb{C}^*$, $(F^{(0)})^{-1} F^{(\infty)}(z_N) = H \bmod (z_N - z_0) M_n(\mathbb{C}\{z_N - z_0\})$ for some $H \in M_n(\mathbb{C})$ with rank $n - 1$. Since $(F^{(0)})^{-1} F^{(\infty)} = (F_1^{(0)})^{-1} F_1^{(\infty)} \otimes (F_2^{(0)})^{-1} F_2^{(\infty)}$, H has the form $H_1 \otimes H_2$ for some $H_1 \in M_{n_1}(\mathbb{C})$ and $H_2 \in M_{n_2}(\mathbb{C})$. Therefore the rank of H is the product of the ranks of H_1 and H_2. This implies that either $n_1 = 1$ or $n_2 = 1$, which is a contradiction. □

Let us now switch to operators. Recall that the q-difference system $(\sigma_q Y = AY)$ associated to $L = \sum_{k=0}^{n} a_{n-k}\sigma_q^k \in \mathcal{D}_{(\mathbb{C}(z),\sigma_q)}$ with $a_0 a_n \neq 0$ is given by:

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ -\dfrac{a_n}{a_0} & -\dfrac{a_{n-1}}{a_0} & -\dfrac{a_{n-2}}{a_0} & \cdots & -\dfrac{a_2}{a_0} & -\dfrac{a_1}{a_0} \end{pmatrix} \in \mathrm{GL}_n(\mathbb{C}(z)).$$

THEOREM 32 ($\otimes$-indecomposability criterion for operators). *Assume that* $L = \sum_{k=0}^{n} a_{n-k}\sigma_q^k \in \mathcal{D}_{(\mathbb{C}(z),\sigma_q)}$ *with* $a_0 a_n \neq 0$ *is such that:*

(1) *there exists* $z_0 \in \mathbb{C}^*$ *such that* $a_n/a_0, \ldots, a_1/a_0$ *are analytic at any point of* $q^{\mathbb{Z}} z_0$, $a_n/a_0(z_0) = 0$ *and, for all* $k \in \mathbb{Z}^*$, $a_n/a_0(q^k z_0) \neq 0$;

(2) L *is pure isoclinic at both* 0 *and* ∞.

Then L *is* $\otimes$*-indecomposable.*

Proof. Since L is $\otimes$-indecomposable if and only if the associated q-difference system $(\sigma_q Y = AY)$ is $\otimes$-indecomposable, the result is an immediate consequence of Theorem 31. □

8.2 Application to q-Kloosterman operators (including $\mathcal{H}_q(\underline{a}; \emptyset; \lambda)$)

We keep the notation of § 7.2.

THEOREM 33. *The general linear group* $\mathrm{GL}(\mathbb{C}^{\deg U})$ *is the unique connected algebraic group occurring as the Galois group of some* q*-Kloosterman module* $\mathcal{K}l_q(U, V)$ *such that* $\deg U$ *is coprime to* $\deg V$ *and such that there exists* $z_0 \in \mathbb{C}^*$ *satisfying* $V(z_0) = 0$ *and, for all* $k \in \mathbb{Z}^*$, $V(q^k z_0) \neq 0$.

Proof. This is an immediate consequence of Theorems 32 and 27. □

COROLLARY 34. *The general linear group* $\mathrm{GL}(\mathbb{C}^r)$ *is the unique connected algebraic group occurring as the Galois group of some confluent generalized* q*-hypergeometric module* $\mathcal{H}_q(\underline{a}; \emptyset; \lambda)$.

Proof. This is a special case of Theorem 33, since $\mathcal{L}_q(\underline{a}; \emptyset; \lambda) = z\,\mathrm{Kl}_q(-\lambda \prod_{i=1}^{r}(a_i X - 1) + (-1)^r \lambda, -(-1)^r \lambda + X)$. □

In the following result, $c_1, \ldots, c_{\deg U}$ denote the complex roots of $X^{\deg U}(U(X^{-1}) + V(0)) \in \mathbb{C}[X]$ and, for all $i \in \{1, \ldots, \deg U\}$, (u_i, α_i) denotes the unique element of $\mathbb{U} \times \mathbb{R}$ such that $c_i = u_i q^{\alpha_i}$.

THEOREM 35. *Assume that* $\deg U$ *is coprime to* $\deg V$, *that the algebraic group generated by* $\mathrm{diag}(u_1, \ldots, u_{\deg U})$ *and* $\mathrm{diag}(e^{2\pi i \alpha_1}, \ldots, e^{2\pi i \alpha_{\deg U}})$ *is connected, and that there exists* $z_0 \in \mathbb{C}^*$ *such that* $V(z_0) = 0$ *and, for all* $k \in \mathbb{Z}^*$, $V(q^k z_0) \neq 0$. *Then,* $\mathrm{Gal}(\mathcal{K}l_q(U, V), \omega)$ *is* $\mathrm{GL}(\mathbb{C}^{\deg U})$.

Proof. This is an immediate consequence of Theorems 32 and 28. □

In the following result, for all $i \in \{1, \ldots, r\}$, (u_i, α_i) denotes the unique element of $\mathbb{U} \times \mathbb{R}$ such that $a_i = u_i q^{\alpha_i}$.

Theorem 36. *If the algebraic group generated by* $\mathrm{diag}(u_1, \ldots, u_n)$ *and* $\mathrm{diag}(e^{2\pi i\alpha_1}, \ldots, e^{2\pi i\alpha_r})$ *is connected, then* $\mathrm{Gal}(\mathcal{H}_q(\underline{a}; \emptyset; \lambda), \omega)$ *is* $\mathrm{GL}(\mathbb{C}^r)$.

Proof. This is a special case of Theorem 35, since $\mathcal{L}_q(\underline{a}; \emptyset; \lambda) = z\,\mathrm{Kl}_q(-\lambda \prod_{i=1}^r (a_i X - 1) + (-1)^r \lambda, -(-1)^r \lambda + X)$. □

8.3 Equations satisfying ($\mathscr{H}1$) with Galois group $\bigotimes_{i=1}^l \mathrm{GL}(\mathbb{C}^{n_i})$

Theorem 37. *For any* $l \in \mathbb{N}^*$, *given any pairwise coprime numbers* $n_1, \ldots, n_l > 1$, *the image of* $\prod_{i=1}^l \mathrm{GL}(\mathbb{C}^{n_i})$ *in* $\bigotimes_{i=1}^l \mathrm{std}$ *occurs as the Galois group of some object of* $\mathcal{E}_{(\mathbb{C}(z),\sigma_q)}$ *which is of rank* $n = n_1 \cdots n_l$ *and satisfies* ($\mathscr{H}1$).

Proof. Theorem 36 ensures that, for any $i \in \{1, \ldots, l\}$, there exists an object M_i of $\mathcal{E}_{(\mathbb{C}(z),\sigma_q)}$ of rank n_i which satisfies ($\mathscr{H}1$) and whose Galois group is $\mathrm{GL}(\mathbb{C}^{n_i})$. It is easily seen that $\bigotimes_{i=1}^l M_i$ satisfies ($\mathscr{H}1$). For any $i \in \{1, \ldots, l\}$, let ρ_i be the representation of $\mathrm{Gal}(\bigoplus_{i=1}^l M_i, \omega)$ corresponding to M_i by tannakian duality. Then, for any $i \in \{1, \ldots, l\}$, the image of ρ_i is $\mathrm{GL}(\mathbb{C}^{n_i})$ and $\bigoplus_{i=1}^l \rho_i$ is a faithful representation (because it is the representation of $\mathrm{Gal}(\bigoplus_{i=1}^l M_i, \omega)$ corresponding to $\bigoplus_{i=1}^l M_i$ itself). So the image of $\bigotimes_{i=1}^l \rho_i$ coincides with the image of $\prod_{i=1}^l \mathrm{GL}(\mathbb{C}^{n_i})$ in $\bigotimes_{i=1}^l \mathrm{std}$, by virtue of the Goursat–Kolchin–Ribet theorem [Kat90, Proposition 1.8.2]. □

9. More computations

9.1 Non-q-Kummer-induced equations in the two-slopes case

Theorem 38. *Let* M *be an irreducible object of* $\mathcal{E}_{(\mathbb{C}(z),\sigma_q)}$ *which is of rank* n *and satisfies* ($\mathscr{H}2$) *with* r *coprime to* n. *Assume that* M *is regular singular at* ∞ *with exponents* $c_1, \ldots, c_n \in q^{\mathbb{R}}$. *If the list* $c_1, \ldots, c_n$ *is not* q*-Kummer induced, then* $\mathrm{Gal}(M, \omega) = \mathrm{GL}(\omega(M))$.

Proof. We let $G = \mathrm{Gal}(M, \omega)$. Proposition 15 ensures that G°, and hence its Lie algebra $\mathfrak{g}$, acts irreducibly on $\omega(M)$. Moreover, the proof of Theorem 24 shows that G° contains, with respect to some basis, $I_{n-r} \oplus \mathbb{C}^* I_r$. So $\mathfrak{g}$ contains, with respect to some basis, $0_{n-r} \oplus \mathbb{C} I_r$ and hence contains an element having two eigenvalues with relatively prime multiplicities. According to Serre [Ser67, § 4], this implies that $\mathfrak{g}$ is either $\mathfrak{sl}(\omega(M))$ or $\mathfrak{gl}(\omega(M))$. Since $\det(M)$ is irregular of rank one, its Galois group is $\mathbb{C}^*$. So $G = \mathrm{GL}(\omega(M))$. □

An immediate application is the following (see § 7.1 for $\mathcal{H}_q(\underline{a}; \underline{b}; \lambda)$).

Theorem 39. *If* $a_1, \ldots, a_r \in q^{\mathbb{R}}$ *is not* q*-Kummer induced and if* r *is coprime to* $s > 0$, *then* $\mathrm{Gal}(\mathcal{H}_q(\underline{a}; \underline{b}; \lambda), \omega) = \mathrm{GL}(\mathbb{C}^r)$.

9.2 Another example of a q-Kloosterman equation

The proof of the following $\otimes$-indecomposability criterion is left to the reader.

Proposition 40. *Let* M *be an object of* $\mathcal{E}_{(\mathbb{C}(z),\sigma_q)}$ *of rank* n. *Assume that* M *is regular singular at* ∞ *with exponents* $c_1, \ldots, c_n$ *in* $q^{\mathbb{R}}$. *If* M *is* $\otimes$*-decomposable, then there exists a divisor* $1 < d < n$ *of* n *such that* $c_1, \ldots, c_n \bmod q^{\mathbb{Z}}$ *is of the form* $(c'_i c''_j\,; 1 \leqslant i \leqslant d, 1 \leqslant j \leqslant n/d) \bmod q^{\mathbb{Z}}$ *for some* $c'_1, \ldots, c'_d \in \mathbb{C}^*$ *and some* $c''_1, \ldots, c''_{n/d} \in \mathbb{C}^*$.

We now give an illustration of the previous result. Note that we cannot apply Theorem 35 to $\mathcal{K}l_q((q^{1/2} - X)^2 (1 - X)^{n-2} - q, V)$ where $V \in \mathbb{C}[X]$ is such that $V(0) = q$. However, we can obtain the following result.

PROPOSITION 41. *Let us consider $V \in q + X\mathbb{C}[X]$. Then, for any odd integer $n \geqslant 2$ coprime to* $\deg V$*, the Galois group of* $\mathcal{K}l_q((q^{1/2}-X)^2(1-X)^{n-2}-q, V)$ *is* $\mathrm{GL}(\mathbb{C}^n)$.

Proof. Recall (see § 7.2) that $M = \mathcal{K}l_q((q^{1/2}-X)^2(1-X)^{n-2}-q, V)$ is pure isoclinic at 0 with slope $\deg V/n$ and is regular singular at ∞, having exponents $q^{1/2}$ with multiplicity 2 and 1 with multiplicity $n-2$. Since n is odd, Corollary 13 ensures that the Galois group of M is connected. It is easily seen that M is $\otimes$-indecomposable by using Proposition 40. Theorem 27 leads to the conclusion. □

REFERENCES

And01 Y. André, *Différentielles non commutatives et théorie de Galois différentielle ou aux différences*, Ann. Sci. Éc. Norm. Supér (4) **34** (2001), 685–739.

BBH88 F. Beukers, W. D. Brownawell and G. Heckman, *Siegel normality*, Ann. of Math. (2) **127** (1988), 279–308.

Bou75 N. Bourbaki, *Groupes et algèbres de Lie: Chapitres 7 et 8* (Hermann, Paris, 1975).

CR08 G. Casale and J. Roques, *Dynamics of rational symplectic mappings and difference Galois theory*, Int. Math. Res. Not. IMRN (2008), Art. ID rnn 103.

CR11 G. Casale and J. Roques, *Nonintegrability by discrete quadratures*, Preprint (2011), available at http://www-fourier.ujf-grenoble.fr/∼jroques/.

DM81 P. Deligne and J. S. Milne, *Tannakian categories in Hodge cycles, motives, and Shimura varieties*, Lecture Notes in Mathematics, vol. 900 (Springer, Berlin, 1981).

DiV02 L. Di Vizio, *Arithmetic theory of q-difference equations: the q-analogue of Grothendieck-Katz's conjecture on p-curvatures*, Invent. Math. **150** (2002), 517–578.

DM89 A. Duval and C. Mitschi, *Matrices de Stokes et groupe de Galois des équations hypergéométriques confluentes généralisées*, Pacific J. Math. **138** (1989), 25–56.

Kat87 N. M. Katz, *On the calculation of some differential Galois groups*, Invent. Math. **87** (1987), 13–61.

Kat90 N. M. Katz, *Exponential sums and differential equations*, Annals of Mathematics Studies, vol. 124 (Princeton University Press, Princeton, NJ, 1990).

KP87 N. M. Katz and R. Pink, *A note on pseudo-CM representations and differential Galois groups*, Duke Math. J. **54** (1987), 57–65.

Kos58 B. Kostant, *A characterization of the classical groups*, Duke Math. J. **25** (1958), 107–123.

Mit96 C. Mitschi, *Differential Galois groups of confluent generalized hypergeometric equations: an approach using Stokes multipliers*, Pacific J. Math. **176** (1996), 365–405.

RS07 J.-P. Ramis and J. Sauloy, *The q-analogue of the wild fundamental group. I*, in *Algebraic, analytic and geometric aspects of complex differential equations and their deformations. Painlevé hierarchies*, RIMS Kôkyûroku Bessatsu, vol. B2 (Research Institute for Mathematical Sciences (RIMS), Kyoto, 2007), 167–193.

RS09 J. -P. Ramis and J. Sauloy, *The q-analogue of the wild fundamental group. II*, Astérisque **323** (2009), 301–324.

Roq11 J. Roques, *Generalized basic hypergeometric equations*, Invent. Math. **184** (2011), 499–528.

Sau00 J. Sauloy, *Systèmes aux q-différences singuliers réguliers: classification, matrice de connexion et monodromie*, Ann. Inst. Fourier (Grenoble) **50** (2000), 1021–1071.

Sau03 J. Sauloy, *Galois theory of Fuchsian q-difference equations*, Ann. Sci. Éc. Norm. Supér. (4) **36** (2003), 925–968.

Sau04 J. Sauloy, *La filtration canonique par les pentes d'un module aux q-différences et le gradué associé*, Ann. Inst. Fourier (Grenoble) **54** (2004), 181–210.

Ser67 J.-P. Serre, *Sur les groupes de Galois attachés aux groupes p-divisibles*, in *Proceedings of a conference on local fields (Driebergen, 1966)* (Springer, Berlin, 1967), 118–131.

Ser79 J.-P. Serre, *Groupes algébriques associés aux modules de Hodge-Tate*, Astérisque **65** (1979), 155–188 Journées de Géométrie Algébrique de Rennes (Rennes, 1978), vol. III.

vdPR07 M. van der Put and M. Reversat, *Galois theory of q-difference equations*, Ann. Fac. Sci. Toulouse Math. (6) **16** (2007), 665–718.

vdPS97 M. van der Put and M. F. Singer, *Galois theory of difference equations*, Lecture Notes in Mathematics, vol. 1666 (Springer, Berlin, 1997).

Julien Roques Julien.Roques@ujf-grenoble.fr
Institut Fourier, Université Grenoble 1, UMR CNRS 5582,
100 rue des Maths, BP 74, 38402 St Martin d'Hères, France

https://doi.org/10.1112/S0010437X12000292 Published online by Cambridge University Press