# NOTES ON THE CONJECTURE OF LOXTON AND VAN DER POORTEN

EHUD DE SHALIT

These are notes for two talks in Kazhdan's "Basic Notions in Mathematics" seminar at the Hebrew University. They are based on the preprint [Sch-Si] from 2016, but the presentation is somewhat different. Except for Proposition 16, that mimics part of what is being done here in a different context (but is needed in the proof), the notes are self-contained.

## 1. The main results

Denote by $k = \mathbb{C}(x)$ and $\widehat{k} = \mathbb{C}((x))$.

**Theorem.** *(Ramis, 1992) Let $q \neq 0$ be a complex number which is not a root of unity. Consider the two operators*

$$\sigma f(x) = f(qx), \;\; \delta f(x) = x\frac{d}{dx}f(x)$$

*on $k$ and $\widehat{k}$. If $f \in \widehat{k}$ satisfies a linear homogeneous polynomial equation with coefficients from $k$ in each of the operators $\sigma$ and $\delta$, then $f \in k$.*

Here is another theorem of a similar nature.

**Theorem 1.** (Loxton - van der Poorten conjecture, proved by Adamczewski and Bell, 2013 [A-B]). *Let $p, q > 1$ be two natural numbers which are multiplicatively independent, i.e. $\log p / \log q \notin \mathbb{Q}$. Consider the operators $\sigma f(x) = f(x^p)$, $\tau f(x) = f(x^q)$ on $k$ and $\widehat{k}$. If $f \in \widehat{k}$ satisfies the two linear homogeneous polynomial equations*

$$\sum_{i=0}^{n} a_i \sigma^{n-i} f = 0, \;\; \sum_{j=0}^{m} b_j \tau^{m-j} f = 0 \tag{1.1}$$

*with coefficients $a_i, b_j \in k$, $a_0 = b_0 = 1$, then $f \in k$.*

**Remarks**

- The operators $\sigma$ and $\tau$ are called *Mahler operators* because Kurt Mahler was the first to study the consequences of equation (1.1).
- $\mathbb{C}$ can be any field of characteristic 0. It is an interesting question whether one can substitute for $\mathbb{C}$ a field of positive characteristic (prime to $pq$ ?) because the proof uses Riemann surface theory and analytic continuation, so is confined to characteristic 0.
- There are several more results of the same nature in the literature. Furstenberg's conjecture that if $p$ and $q$ are multiplicatively independent then the only Borel measure on the unit circle which is invariant under both $z \mapsto z^p$ and $z \mapsto z^q$ is the Lebesgue measure, is also of the same spirit, although seems to be much more difficult.

- Schäfke and Singer [?] gave a unified conceptual approach to the two theorems and many other results. Our goal is to describe their proof in the context of Theorem 1.
- Adamczewski and Bell deduced Theorem 1 from Cobham's theorem in the theory of automata, to be reviewed below. Cobham's proof (from 1969) is combinatorial, tricky and not transparent. On the other hand, Cobham's theorem can be deduced easily from Theorem 1, see section 2. Thus the work of Schäfke and Singer gives a new conceptual proof to Cobham's theorem.
- The theorem relates the algebraic group $\mathbb{G}_m$ and its formal counterpart $\widehat{\mathbb{G}}_m$. Indeed, the significance of $\sigma$ and $\tau$ is that they are endomorphisms of $\mathbb{G}_m$. Is there an analogue replacing $\mathbb{G}_m$ by an elliptic curve $E$? (Work of Eran Assaf).

We first replace $k$ and $\widehat{k}$ by

$$K = \bigcup_{s\in\mathbb{N}} \mathbb{C}(x^{1/s}), \quad \widehat{K} = \bigcup_{s\in\mathbb{N}} \mathbb{C}((x^{1/s})).$$

Here by $x^{1/s}$ we denote some $s$-th root of $x$ in a fixed algebraic closure, and for $s = rt$ we require $(x^{1/s})^r = x^{1/t}$. The field $\widehat{K}$, the field of Puiseaux series, is well-known to be *algebraically closed*. It carries the *valuation*

$$\omega(f) = ord_0 f$$

which is non-discrete (the value group is $\mathbb{Q}$), and normalized by $\omega(x) = 1$. We call the multiplicative subgroup $U(\widehat{K})$ of elements $f$ for which $\omega(f) = 0$ (i.e. Puiseaux series having neither a zero nor a pole at $x = 0$) the group of *units* of $\widehat{K}$. Every unit may be evaluated at $k = 0$ and the kernel of the evaluation homomorphism is the subgroup of *principal units* $U_1(\widehat{K})$. We have the short exact sequence

$$0 \to U_1(\widehat{K}) \to U(\widehat{K}) \to \mathbb{C}^\times \to 0.$$

Note that $\widehat{K}$ is *not* complete.

Theorem 1 remains valid with $(k, \widehat{k})$ replaced by $(K, \widehat{K})$ throughout. In fact, it is enough to prove it for $(K, \widehat{K})$ because if we know that $f \in \mathbb{C}((x))$ and also $f \in \mathbb{C}(x^{1/s})$ then $f$ is fixed under $Gal(\mathbb{C}(x^{1/s})/\mathbb{C}(x))$ so we conclude that it lies in $\mathbb{C}(x)$.

The advantage of $K$ and $\widehat{K}$ is that $\sigma$ and $\tau$ are *automorphisms* of these two fields, while they are only *endomorphisms* of $k$ or $\widehat{k}$. Observe that $\sigma$ and $\tau$ *commute*. The assumption that $p$ and $q$ are multiplicatively independent means that

$$\Gamma = \langle \sigma, \tau \rangle \subset Aut(K)$$

is *free abelian of rank* 2.

Suppose therefore that $f \in \widehat{K}$ satisfies (1.1) with $a_i, b_j \in K$. Let

$$W = Span_K\{\sigma^i \tau^j f \,|\, 0 \le i < n,\ 0 \le j < m\}.$$

Thanks to the fact that $\sigma, \tau$ commute, equation (1.1) shows that $W$ is a finite-dimensional $K$-vector space invariant under the semi-linear operators $\sigma$ and $\tau$. Let

$$d = \dim_K W.$$

Let $y = {}^t(y_1, \ldots, y_d) \in \widehat{K}^d$ be a column vector whose entries form a basis for $W$ over $K$. Then there are matrices $A, B \in GL_d(K)$ such that

$$\sigma(y) = Ay,\ \tau(y) = By. \tag{1.2}$$

The relation $\sigma\tau = \tau\sigma$ yields the *consistency equation*

$$\sigma(B) \cdot A = \tau(A) \cdot B. \tag{1.3}$$

If we make a change of basis

$$\widetilde{y} = Cy$$

with $C \in GL_d(K)$ then we find the equations $\sigma(\widetilde{y}) = \widetilde{A}\widetilde{y},\ \tau(\widetilde{y}) = \widetilde{B}\widetilde{y}$ with

$$\widetilde{A} = \sigma(C) \cdot A \cdot C^{-1},\quad \widetilde{B} = \tau(C) \cdot B \cdot C^{-1}. \tag{1.4}$$

We call a pair $(\widetilde{A}, \widetilde{B})$ related to $(A, B)$ by (1.4) an *equivalent* pair. Note that since $\sigma$ and $\tau$ are semi-linear, equivalence is expressed by *twisted conjugacy* and not by usual conjugacy.

**Theorem 2.** (Descent of coefficients) *Suppose $A, B \in GL_d(K)$ satisfy the consistency equation (1.3). Then they are equivalent to a pair $(\widetilde{A}, \widetilde{B})$ of commuting scalar ($\mathbb{C}$-valued) matrices.*

**Remarks**

- We shall later introduce a certain *non-abelian cohomology*. We shall then interpret the consistency equation as the equation defining a 1-cocycle, and the equivalence relation as the relation between two 1-cocycles being cohomologous.
- Theorem 2 "lives" entirely in $K$ and does not require the introduction of $\widehat{K}$ for its formulation. Its *proof*, however, will go through $\widehat{K}$.

*Claim.* Theorem 2 implies Theorem 1.

*Proof.* Let $f$ be as in Theorem 1, let $W$ and $d = \dim_K W$ be as above, choose a basis $y$ of $W$ over $K$ and let the matrices $A, B$ be defined via (1.2). Then they satisfy the consistency equation so we may find a matrix $C$ as in Theorem 2 and produce an equivalent *scalar* pair $(\widetilde{A}, \widetilde{B})$. Letting $\widetilde{y} = Cy$ we get the equations $\sigma(\widetilde{y}) = \widetilde{A}\widetilde{y},\ \tau(\widetilde{y}) = \widetilde{B}\widetilde{y}$. But then, since $\widetilde{A}$ is scalar,

$$\widetilde{y} = \widetilde{A}^{-1}\sigma(\widetilde{y}) = \widetilde{A}^{-2}\sigma^2(\widetilde{y}) = \cdots$$

(feed in the expression for $\widetilde{y}$ successively) so writing

$$\widetilde{y} = \sum c_n x^n$$

as a power series with coefficients from $\mathbb{C}^d$ we see that this is a power series in $x^{p^k}$ for every $k$, hence only $c_0 \neq 0$ and $\widetilde{y} \in \mathbb{C}^d$. But the $\widetilde{y}_i$ are linearly independent over $K$, so $d = 1$ and $W = K$. This implies $f \in K$ as desired. □

## 2. Application to the theory of automata

An automaton is a finite-state deterministic machine that gets as an input a natural number $x \in \mathbb{N} = \{0, 1, 2, ...\}$ and produces an output $y = \overline{T}(x)$ in a finite set of possible results. More precisely, a $p$-automaton ($p > 1$) consists of a finite set $S$ equipped with a base point $s_0$, and a function

$$T : \{0, 1, ..., p-1\} \times S \to S.$$

Here $\{0, 1, ..., p-1\}$ should be viewed as the set of digits in base $p$; $S$ is the set of *states*; $s_0$ is called the *initial* state, and $T(x, s) = s'$ means that upon reading the digit $x$, the machine moves from state $s$ to state $s'$. The input is a number $x \in \mathbb{N}$ given in base $p$ as

$$x = x_0 p^{k-1} + \cdots + x_{k-2} p + x_{k-1}$$

($0 \leq x_i \leq p-1$). The machine reads $x$ from left to right. Define successively (for $1 \leq i \leq k$)

$$s_i = T(x_{i-1}, s_{i-1}).$$

We say that $\overline{T}(x) = s_k$ or that $T$ computes $s_k$ on $x$.

A set $\mathcal{N} \subset \mathbb{N}$ is called $p$-automatic if there exists a $p$-automaton $T$ that decides if $x \in \mathcal{N}$. Without loss of generality we may require that $\overline{T}(x) = s_0$ (i.e. $T$ returns to its initial state) if $x \in \mathcal{N}$and $\overline{T}(x) \neq s_0$ otherwise.

It is easy to see that arithmetic progressions (including those of step 0, reduced to a point) are $p$-automatic for every $p > 1$. This is just a formalization of the "rules for divisibility" learned in school. So are finite unions of arithmetic progressions.

**Theorem 3.** *(Cobham, 1969). If $\mathcal{N}$ is $p$-automatic and also $q$-automatic for multiplicatively independent $p$ and $q$ then it is a finite union of arithmetic progressions.*

*Proof.* We deduce Theorem 3 from Theorem 1. For this it is enough to show: (1) If $\mathcal{N}$ is $p$-automatic then its characteristic power series

$$f_{\mathcal{N}} = \sum_{n \in \mathcal{N}} x^n$$

satisfies a $p$-Mahler equation (1.1) with the operator $\sigma$. (2) The set $\mathcal{N}$ is a finite union of arithmetic progressions if and only if $f_{\mathcal{N}}$ is the power-series expansion of a rational function.

We leave (2) as an easy exercise, and outline (1). It is clear that Theorem 1 then implies Cobham's theorem.

Number the states in $S$ by $1 \leq j \leq m$ and let $s_0$ be $j = 1$. For $k \in \{0, 1, \ldots, p-1\}$ let $v_{i,j,k} = 1$ if $T(k, j) = i$ and 0 otherwise. The $m \times m$ matrix

$$V_k = (v_{i,j,k})$$

is the *transition matrix* for digit $k$. For $n \in \mathbb{N}$ let $u_{i,n} = 1$ if $\overline{T}(n) = i$ and 0 otherwise. Let $u_n = {}^t(u_{1,n}, \ldots, u_{m,n})$. Clearly

$$u_{hp+k} = V_k u_h.$$

Consider the power series (with vector coefficients)

$$g(x) = \sum_{n=0}^{\infty} u_n x^n.$$

We have

$$g(x) = \sum_{h=0}^{\infty} \sum_{k=0}^{p-1} u_{hp+k} x^{hp+k} = \left( \sum_{k=0}^{p-1} V_k x^k \right) \sum_{h=0}^{\infty} u_h x^{hp} = C(x) g(x^p)$$

where the entries $c_{i,j}$ of $C(x)$ are polynomials. This is a matrix equation

$$g = C \cdot \sigma(g)$$

for $g = {}^t(g_1, \ldots, g_m)$. Alternatively, in $\widehat{K}$ we get

$$\sigma^{-1}(g) = A \cdot g$$

with $A = \sigma^{-1}(C) \in M_d(K)$. Inductively we get $\sigma^{-i}(g) = A_i \cdot g$. This gives a polynomial relation with coefficients from $K$ between the $\sigma^{-i}(g)$. Applying some high power of $\sigma$ to this relation gives such a relation for $\sigma^i(g)$ with coefficients from $k$. Since $f_{\mathcal{N}} = g_1$ we are done. □

Cobham's theorem is fundamental in the theory of automata. The original paper by Cobham was over 100 pages long and Samuel Eilenberg made a famous remark that his theorem called for a more conceptual proof. There have been many simplifications of the proof since it was first published in 1969, but none, to my understanding, is as elegant as the one resulting from the work of Schäfke and Singer. Automatic sequences have many relations to problems in ergodic theory, fractals and of course, computer science. See the book by J.-P. Allouche and J. Shallit, *Automatic sequences: Theory, applications, generalizations*, Cambridge University Press, Cambridge, 2003. The converse of (1) is false. Not every power series satisfying a $p$-Mahler equation is $p$-automatic. This led to the notion of $p$-regular sequences and more work which is outside my knowledge and the scope of the lectures.

## 3. Non-abelian cohomology and an analogue of Hilbert's theorem 90

Let $\Gamma$ be an abstract group acting via automorphism on a field $K$. We stress that $\Gamma$ need not be finite or profinite (acting through finite quotients), so we are not necessarily in the set-up for Galois theory. From now on write $G = GL_d$. Recall the definition of the pointed set $H^1(\Gamma, G(K))$. A 1-cocycle is a map $\Gamma \to G(K)$, denoted $\sigma \mapsto A_\sigma$, satisfying for any $\sigma, \tau \in \Gamma$

$$A_{\sigma\tau} = \sigma(A_\tau) \cdot A_\sigma.$$

If $C \in G(K)$ then

$$\widetilde{A}_\sigma = \sigma(C) \cdot A_\sigma \cdot C^{-1}$$

is another 1-cocycle, said to be cohomologous to $A$. The property of being cohomologous is an equivalence relation and $H^1(\Gamma, G(K))$ is the set of equivalence classes. If $d = 1$, it is even a *group,* under point-wise multiplication.

If $\Gamma$ acts trivially on $K$ then

$$H^1(\Gamma, G(K)) = Hom(\Gamma^{opp}, G(K))/\sim$$

is the set of anti-homomorphisms from $\Gamma$ to $G(K)$ up to conjugation by elements of $G(K)$. Any group is isomorphic, of course, to its opposite, so this may be identified also with $Hom(\Gamma, G(K))/\sim$.

If $F \subset K$ is a subfield preserved by $\Gamma$ then we get a map

$$H^1(\Gamma, G(F)) \to H^1(\Gamma, G(K)).$$

Suppose now that $\Gamma$ is finite, acting faithfully, and $F = K^\Gamma$. Then $K/F$ is a finite Galois extension, $\Gamma = Gal(K/F)$, and we have the following celebrated theorem.

**Theorem.** *(Hilbert's theorem 90) When* $\Gamma = Gal(K/F)$, $H^1(\Gamma, GL_d(K)) = 1$.

For the proof consult any text-book on algebra. Originally the name referred to the case $d = 1$, and even then Hilbert considered cyclic extensions only. But the proof for general $d$ and $\Gamma$ is not much different.

In our situation we let $K = \bigcup_{s\in\mathbb{N}} \mathbb{C}(x^{1/s})$ and $\Gamma = \langle\sigma, \tau\rangle \subset Aut(K)$ as in Theorem 1. As remarked above, the assumption that $p, q$ are multiplicatively independent translates into the fact that

$$(i, j) \mapsto \sigma^i\tau^j$$

is an isomorphism $\mathbb{Z}^2 \simeq \Gamma$.

**Lemma 4.** *Assume that $A, B$ satisfy the consistency equation (1.3). Then there exists a unique 1-cocycle $A_\bullet$ with $A_\sigma = A$ and $A_\tau = B$. Conversely, if these are the values of a 1-cocycle on the two generators of $\Gamma$, they satisfy the consistency equation.*

*Proof.* Since $\Gamma$ is free abelian we need only check the commutativity constraint and then the cocycle condition dictates the extension of $A_\bullet$ from the two generators to any element of $\Gamma$ uniquely. We leave out the easy computation. □

We now see that Theorem 2 is equivalent to the following.

**Theorem 5.** (Descent, cohomological formulation) *The map*

$$H^1(\Gamma, G(\mathbb{C})) \to H^1(\Gamma, G(K))$$

*is a bijection.*

## 4. Semilinear algebra

4.1. **Factorization in twisted polynomial rings.** Let $\widehat{K}$ and $\sigma$ be as above. We consider the twisted polynomial ring $\widehat{K}\left\langle\Phi, \Phi^{-1}\right\rangle$ consisting of Laurent polynomials

$$\sum a_i\Phi^i,$$

($a_i \in \widehat{K}$) where $\Phi a = \sigma(a)\Phi$.

**Lemma 6.** (Factorization) *Let $\sum_{i=0}^n a_i\Phi^{n-i} \in \widehat{K}\left\langle\Phi, \Phi^{-1}\right\rangle$, and assume $a_0 = 1$, $a_n \neq 0$. Then there exist $c \in \mathbb{C}^\times$, $\mu \in \mathbb{Q}$, $b_0, \ldots, b_{n-1} \in \widehat{K}$ such that $b_0 \in U_1(\widehat{K})$, $b_{n-1} \neq 0$ and*

$$\sum_{i=0}^{n} a_i\Phi^{n-i} = \sigma(b_0)^{-1}(\Phi - cx^\mu)\sum_{i=0}^{n-1} b_i\Phi^{n-1-i}.$$

[Compare Chapter IV, §4 Lemma 2 in Demazure's *Lectures on p-divisible groups* LNM 302 (1972) Springer-Verlag. That lemma is key to the Manin-Dieudonné classification of $F$-isocrystals over an algebraically closed field of characteristic $p$, or - what amounts to the same - the classification of $p$-divisible groups over such a field up to isogeny.]

*Proof.* To simplify the notation we write, in the proof of the lemma only, $a^{(n)} = \sigma^n(a)$. Write also $u = b_0^{(1)}$. We have to find $\mu, u, b_1, \ldots, b_{n-1}$ and $c$ as in the lemma satisfying the equations

$$ua_i = b_i^{(1)} - cx^\mu b_{i-1} \quad (0 \leq i \leq n) \tag{4.1}$$

($b_{-1} = b_n = 0$). Solving successively for $b_i$ we get the equation

$$(ua_0)c^n + (u^{(1)}a_1^{(1)}x^{-\mu p})c^{n-1} + \cdots + (u^{(n)}a_n^{(n)}x^{-\mu(p+\cdots+p^n)}) = 0, \tag{4.2}$$

which we have to solve for $u \in U_1(\widehat{K})$ and $c \in \mathbb{C}^\times$. Let

$$\mu = \min_{1\le i\le n}\left(\frac{1-1/p}{1-1/p^i}\right)\omega(a_i)$$

where $\omega$ is the valuation on $\widehat{K}$, normalized by $\omega(x) = 1$. Note that

$$\omega(a_i^{(i)}x^{-\mu(p+\cdots+p^i)}) = p^i\left(\omega(a_i) - \mu\left(\frac{1-1/p^i}{1-1/p}\right)\right) \ge 0$$

and there exists an index $i \ge 1$ for which this is 0. This means that the expression $a_i^{(i)}x^{-\mu(p+\cdots+p^i)}$, appearing together with $u^{(i)}$ as the coefficient of $c^{n-i}$, is integral, i.e. has no pole, and at least one such expression, besides the leading one, is a unit. Replacing $x$ by $\xi^k$ for a new variable $\xi$ and a suitable $k$, we may assume that all the exponents of $x$ appearing in (4.2) are integral. We solve (4.2) modulo higher and higher powers of $x$, setting

$$u = 1 + d_1x + d_2x^2 + \cdots$$

and choosing the $d_m$ successively. By what we have seen, there exists a $c \ne 0$ in $\mathbb{C}$ solving (4.2) modulo $x$ (i.e. substituting $x = 0$). Noting that

$$u^{(i)} = 1 + d_1x^{p^i} + d_2x^{2p^i} + \cdots$$

it is then an easy matter to solve successively for the $d_m$. □

**Corollary 7.** *Every polynomial from $\widehat{K}\langle\Phi, \Phi^{-1}\rangle$ factors as*

$$u_0(\Phi - c_1x^{\mu_1})u_1(\Phi - c_2x^{\mu_2})u_2\cdots u_{n-1}(\Phi - c_nx^{\mu_n})u_n$$

where the $\mu_j \in \mathbb{Q}$, $\mu_j \le p\mu_{j+1}$, $c_j \in \mathbb{C}^\times$ and $u_j \in U_1(\widehat{K})$.

*Proof.* Apply the lemma inductively. The relation $\mu_j \le p\mu_{j+1}$ follows from the inequality

$$p\omega(b_i) \ge \mu(1 + \frac{1}{p} + \cdots + \frac{1}{p^{i-1}})$$

which is proved by induction on $i$, based on (4.1). □

4.2. **Structure theorem for $\mathcal{D}$-modules.** We consider a finite dimensional vector space $M$ over $\widehat{K}$, equipped with an invertible $\sigma$-linear map $\Phi$. This is the same as a module of finite length over the twisted group ring $\widehat{K}\langle\Phi, \Phi^{-1}\rangle$. We call $\dim_{\widehat{K}} M$ the *rank* of $M$.

**Corollary 8.** (Existence of eigenvectors) *Let $M$ be as above Then there exists a non-zero $v \in M$ and $c \in \mathbb{C}^\times$ such that $\Phi v = cv$.*

*Proof.* Let $u$ be any non-zero vector from $M$, and $n$ the minimal number such that $u, \Phi u, \ldots, \Phi^n u$ are linearly dependent over $\widehat{K}$. Let $\sum_{i=0}^n a_i\Phi^{n-i}u = 0$ be a linear dependence and decompose the polynomial as in the lemma. Let $v = \sum_{i=0}^{n-1} b_i\Phi^{n-1-i}u$. Note that $v \ne 0$ by our assumption on $n$. Then $\Phi v = cx^\mu v$. If $\mu \ne 0$ replace $v$ by $x^{-\mu/(p-1)}v$. □

We now consider a *pair* of operators $\sigma$ and $\tau$ as above

$$\sigma f(x) = f(x^p), \quad \tau f(x) = f(x^q).$$

Let $\Gamma = \langle \sigma, \tau \rangle \subset Aut(\widehat{K})$. We do not make yet the assumption that $p$ and $q$ are multiplicatively independent. In fact, for the structure theorem below we may assume that $\Gamma$ is *any finitely generated abelian group* of automorphisms of $\widehat{K}$, containing $\sigma$. Let $\mathcal{D} = \widehat{K}\langle\Gamma\rangle$ be the twisted group ring. For a character $\chi : \Gamma \to \mathbb{C}^\times$ we denote by $\mathbb{C}_\chi$ the underlying one-dimensional complex representation and by

$$I_\chi = \widehat{K} \otimes_{\mathbb{C}} \mathbb{C}_\chi$$

the corresponding $\mathcal{D}$-module of rank 1, the group $\Gamma$ acting diagonally.

**Theorem 9.** (Structure theorem) *Let $M$ be a $\mathcal{D}$-module of finite rank $d$.*

*(1) There exists a filtration*

$$0 = M_0 \subset M_1 \subset \cdots \subset M_d = M$$

*by $\mathcal{D}$-submodules, and characters $\chi_i$ such that*

$$gr_i M = M_i/M_{i-1} \simeq I_{\chi_i}.$$

*(2) The characters $\chi_i$ (with their multiplicities) are uniquely determined by $M$ up to a permutation.*

*Proof.* Let $c \in \mathbb{C}^\times$ be such that

$$V_c = \{v \in M | \, \sigma v = cv\} \neq 0.$$

The existence of such a $c$ is guaranteed by Corollary 8. Clearly $V_c$ is a $\mathbb{C}$-vector space. We claim that if $v_1, \ldots, v_m \in V_c$ are linearly independent over $\mathbb{C}$ then they are also linearly independent over $\widehat{K}$. Indeed, assume that $\sum a_i v_i = 0$ is a shortest linear dependence with coefficients from $\widehat{K}$. We may assume $a_1 = 1$. Applying $\sigma$ and subtracting the original dependence we get a shorter dependence, unless all $a_i \in \mathbb{C}$. But this contradicts the linear dependence over $\mathbb{C}$. We conclude that $V_c$ is finite dimensional over $\mathbb{C}$. Since $\tau$ and $\sigma$ commute, $\tau$ preserves $V_c$, hence has an eigenvector there. Letting $v$ be such an eigenvector, $\tau v = dv$, we put $M_1 = \widehat{K}v$. Then $M_1$ is a $\mathcal{D}$-module of rank 1, isomorphic to $I_{\chi_1}$ where $\chi_1(\sigma) = c$ and $\chi_1(\tau) = d$. Part (1) now follows by induction. Part (2) (Jordan-Hölder) is standard and we omit it. □

**Corollary 10.** *Let $A, B \in G(\widehat{K})$ be two matrices satisfying the consistency equation (1.3). Then they are equivalent to a pair $(\widetilde{A}, \widetilde{B})$ of lower triangular matrices with non-zero scalars along their diagonals.*

*Proof.* Use $A$ and $B$ to define a $\mathcal{D}$-module structure on $\widehat{K}^d$, and let $C$ be the matrix changing the given basis to a basis as in Theorem 9. Then the matrices $\widetilde{A}$ and $\widetilde{B}$ (1.4) form an equivalent pair of the desired form. □

## 5. Proof of Theorem 5

We now assume, in addition, that $p$ and $q$ are multiplicatively independent. Consider the diagram of pointed sets

$$H^1(\Gamma, G(\mathbb{C})) \quad \stackrel{\alpha}{\to} \quad H^1(\Gamma, G(K)) \quad \stackrel{\beta}{\to} \quad H^1(\Gamma, G(\widehat{K})).$$

The strategy is to prove the following two claims.

(1) $\beta \circ \alpha$ is bijective [ = Proposition 23].
(2) $\beta$ is injective [ = Proposition 19 and Corollary 20].

This will prove Theorem 5, but also the following corollary.

**Corollary 11.** *The map $H^1(\Gamma, G(K)) \to H^1(\Gamma, G(\widehat{K}))$ is a bijection.*

Notice how far from true these claims are for $\Gamma$ which is of rank 1 (i.e. a single Mahler operator $\sigma$). The cohomology sets are then the $\sigma$-twisted conjugacy classes in $G(\mathbb{C})$, $G(K)$ and $G(\widehat{K})$, and there is no reason for the natural maps between them to be bijective.

The two claims are of a very different nature. Point (1) is algebraic, and will follow from Theorem 9. Point (2) requires complex function theory. Somehow we have to *descend* from formal power series to rational functions. We shall first show that we can pass from formal power series to convergent ones, then we shall use analytic continuation to continue these convergent power series meromorphically to the Riemann sphere $\widehat{\mathbb{C}}$, and finally we shall use the fact that an everywhere meromorphic function on the Riemann sphere is rational algebraic.

5.1. **Proof of Claim 1.** The injectivity of $\beta \circ \alpha$ is easy.

**Lemma 12.** *The map $\beta \circ \alpha$ is injective.*

*Proof.* A cohomology class $[A_\bullet]$ in $H^1(\Gamma, G(\mathbb{C}))$ is represented by a pair $(A, B) = (A_\sigma, A_\tau)$ of commuting matrices from $G(\mathbb{C})$. Suppose $(A', B')$ is another such pair and there exists a $C \in G(\widehat{K})$ such that

$$A' = \sigma(C) A C^{-1}, \;\; B' = \tau(C) B C^{-1}.$$

Then

$$C = A'^{-1} \sigma(C) A = A'^{-2} \sigma^2(C) A^2 = \cdots$$

so $C$ is constant, and the 1-cocycle represented by $(A', B')$ is cohomologous to the one represented by $(A, B)$ already in $H^1(\Gamma, G(\mathbb{C}))$. □

For the surjectivity of $\beta \circ \alpha$ we remark that it is enough to prove that if $(A, B)$ is a pair of matrices from $G(\widehat{K})$ satisfying the consistency equation, then they are equivalent to a pair where $A \in G(\mathbb{C})$. Indeed, if $A$ is scalar the consistency equation takes the from

$$B(x^p) A = A B(x). \tag{5.1}$$

As usual replacing $x$ by $\xi^m$ for a new variable $\xi$ and some $m$ we may assume that all the exponents of $x$ in $B$ are integral. As before this shows that

$$B(x) = A^{-1} B(x^p) A = A^{-2} B(x^{p^2}) A^2 = \cdots$$

so $B$, having its entries in $\mathbb{C}((x^{p^k}))$ for every $k$, is constant.

We argue by induction on $d$. The induction will in fact give us that the pair $(A, B)$ is equivalent to a pair of scalar *lower triangular* matrices. By Theorem 9 and its corollary we may assume that $A$ and $B$ are lower triangular with scalars along the diagonal. Write

$$A = \begin{pmatrix} A_{11} & 0 \\ A_{21} & A_{22} \end{pmatrix}, \;\; B = \begin{pmatrix} B_{11} & 0 \\ B_{21} & B_{22} \end{pmatrix}$$

where $A_{11} \in \mathbb{C}^\times$, $A_{22} \in GL_{d-1}(\widehat{K})$ and similarly for $B$. The consistency equation for $A$ and $B$ implies the same equation for $A_{22}$ and $B_{22}$. By the induction hypothesis we may therefore assume that $A_{22}$ and $B_{22}$ are scalar lower triangular. It remains to descend the constants in $A_{21}$ (and then $B_{21}$ will follow suit, as explained above).

The consistency equation now takes the form

$$A_{21}(x^q)B_{11} + A_{22}B_{21}(x) = B_{21}(x^p)A_{11} + B_{22}A_{21}(x). \tag{5.2}$$

Replacing $x$ by $\xi^m$ where $\xi$ is a new variable we may assume that all the exponents appearing in the equations are integers. For simplicity let us assume that $p$ and $q$ are not only multiplicatively independent but *relatively prime*. The modifications needed to treat the general case are minor, and will be explained below. We shall show that if $A_{21}(x)$ or $B_{21}(x)$ have a pole at 0, replacing the pair $(A, B)$ by an equivalent pair, we can reduce the order of the pole, until we get rid of the polar parts altogether. This we will do without affecting the diagonal blocks.

Let $Mx^{-m}$ be the lowest term in $A_{21}(x)$ and $Nx^{-n}$ the lowest term in $B_{21}(x)$ where $M, N \in M_{(d-1)\times 1}(\mathbb{C})$. Then looking at the lowest order terms in (5.2) gives $pn = qm$ and

$$MB_{11} = NA_{11}.$$

By our assumption $m/p$ and $n/q$ are integers. Let

$$C(x) = \begin{pmatrix} I & 0 \\ -MA_{11}^{-1}x^{-m/p} & I \end{pmatrix}.$$

Then $\sigma(C)AC^{-1} = \widetilde{A}$ is of the same shape as $A$ with

$$\widetilde{A}_{21}(x) = A_{21}(x) + C_{21}(x^p)A_{11} - A_{22}C_{21}(x). \tag{5.3}$$

Similarly $\tau(C)BC^{-1} = \widetilde{B}$ satisfies

$$\widetilde{B}_{21}(x) = B_{21}(x) + C_{21}(x^q)B_{11} - B_{22}C_{21}(x).$$

Thus the pair $(\widetilde{A}, \widetilde{B})$ is equivalent to $(A, B)$ but has a lower order pole at 0. Note that we have not introduced fractional powers of $x$ in the process. Continuing inductively we can eliminate the polar parts altogether.

If $p$ and $q$ are not relatively prime and $l = gcd(p, q)$ then a similar step would result in a new pair of matrices with entries which are power series in $x^{1/l}$. However, a careful analysis of the new fractional exponents reveals that when we substitute $x = \xi^l$ to switch back to integral exponents, the order of pole (in $\xi$) is still lower than the original order of pole (in $x$) so the induction can be carried out, in the new variable.

We may therefore assume that $A$ and $B$ have no poles. To conclude the proof of Claim 1 we must solve (5.3) for $C_{21}(x)$ so that the left hand side, $\widetilde{A}_{21}(x)$, is scalar. We take the LHS to be $A_{21}(0)$. Then we find $C_{21} \in M_{(d-1)\times 1}(x\mathbb{C}[[x]])$, by successively solving for the coefficients of $x^m$, $m \geq 1$. This completes the proof of Claim 1.

### 5.2. **Proof of Claim 2.**

5.2.1. *A reduction lemma.* Since we have already proved Claim 1, showing that $\beta$ is injective is the same as showing that $\alpha$ is surjective. Start with $(A, B)$ from $G(K)$ satisfying the consistency equation. Going over to $G(\widehat{K})$ we know that there exist a pair of commuting matrices $(A_0, B_0)$ in $G(\mathbb{C})$ and $C \in G(\widehat{K})$ such that

$$C(x^p)A(x)C(x)^{-1} = A_0, \quad C(x^q)B(x)C(x)^{-1} = B_0. \tag{5.4}$$

We have to show that $C$ in fact lies in $G(K)$.

**Lemma 13.** (Reduction Lemma) *It is enough to prove that if $A, B \in G(K)$ satisfy the consistency equation and the system*

$$g(x^p) = A(x)g(x), \quad g(x^q) = B(x)g(x) \tag{5.5}$$

*has a non-zero solution $g \in \widehat{K}^d$, then $g \in K^d$.*

Since $g_0 = C(x)g(x)$ satisfies the same system with $A_0$ and $B_0$ instead of $A(x)$ and $B(x)$, $g_0$ will lie in $\mathbb{C}^d$, and will be a fixed vector of both $A_0$ and $B_0$. The existence of a *full set of solutions* of (5.5), i.e. $d$ independent solutions, is equivalent to $A_0 = B_0 = I$, or to the cohomology class represented by $(A, B)$ in $H^1(\Gamma, G(\widehat{K}))$ being trivial. But this would be a too strong assumption to make.

*Proof.* We let $N = d^2$ and identify $V = End(K^d)$ with $K^N$ and similarly over $\widehat{K}$. Suppose $C(x) \in G(\widehat{K}) \subset V_{\widehat{K}} = \widehat{K}^N$ satisfies (5.4). Define $S, T \in GL(V) \simeq GL_N(K)$ as the linear transformation taking $Z \in V$ to

$$S(Z) = A_0 Z A(x)^{-1}, \quad T(Z) = B_0 Z B(x)^{-1}.$$

It is easy to see that $S, T$ satisfy the consistency equation $S(x^q) \circ T(x) = T(x^p) \circ S(x)$. The assumption (5.4) gets translated to $C(x^p) = S(x)(C(x))$ and $C(x^q) = T(x)(C(x))$. Thus we find ourselves in the set-up of the Lemma, with $d$ replaced by $N$, $A, B$ by $S, T$ respectively and $g$ by $C \in \widehat{K}^N$. We conclude that $C \in K^N$, hence $C(x) \in G(K)$. □

From now on we assume that $g(x) \in \widehat{K}^d$ is a non-zero solution of (5.5). The proof will be finished once we show that the entries of $g$ are rational.

5.2.2. *Convergence of $C(x)$ and $g(x)$.* We are allowed to replace $(A, B)$ by any $G(K)$-equivalent pair (and $g$ by the equivalent solution of the new system over $\widehat{K}$). Since $K$ is dense in $\widehat{K}$ we can approximate $C$ as well as we wish by a matrix $C'$ from $G(K)$. Applying twisted conjugation by $C'$ to the pair $(A, B)$ replaces $C$ by $CC'^{-1}$, which is close to $I$ in the topology of $\widehat{K}$. We may therefore assume (changing the variable $x$ if necessary to guarantee that all the exponents are integral) that

$$C \in I + xM_d(\mathbb{C}[[x]]).$$

It follows that $A(x)$ and $B(x)$ are regular at 0, and $A(0) = A_0$ as well as $B(0) = B_0$ are invertible.

**Lemma 14.** *There exists $0 < r < 1$ such that $C(x)$ and $g(x)$ converge for $|x| < r$.*

*Proof.* Take $r$ small enough so that $A(x)$ and $B(x)$ are regular for $|x| < r$. From the equation $C(x^p)A(x) = A_0 C(x)$ we get, iteratively,

$$C(x) = A_0^{-m} C(x^{p^m}) A(x^{p^{m-1}}) \cdots A(x^p) A(x).$$

This shows that as a formal power series

$$C(x) = \lim_{m\to\infty} A_0^{-m} A(x^{p^{m-1}}) \cdots A(x^p)A(x)$$

(the coefficient of $x^i$ in the RHS does not change as soon as $p^m > i$). However, it is an easy exercise to check that the power series in the RHS has a positive radius of convergence. This shows that $C(x)$ converges. As $C(x)g(x) = g_0$ is a scalar vector, $g(x)$ converges too. □

**Corollary 15.** *$C(x)$ and $g(x)$ have meromorphic continuation to $|x| < 1$.*

*Proof.* Equation (5.4) may be used to boost the radius of meromorphicity of $C(x)$ from $r$ to $r^{1/p}$, hence all the way up to 1. □

5.2.3. *Analytic continuation across the unit circle.* To bypass the natural boundary at $|x| = 1$ we have to use, for the first time in the proof of Claim 2, the assumption that $C$ satisfies both equations in (5.4), and that $p$ and $q$ are multiplicatively independent. We also use Lemma 13.

Making the change of variables $x = e^z$ we arrive at a pair of matrices $\overline{A}(z) = A(e^z)$ and $\overline{B}(z) = B(e^z)$ whose entries are everywhere meromorphic, with poles at a discrete set of points $\mathcal{M} \subset \mathbb{C}$, which is $2\pi i$ periodic, and contained in a vertical strip $-R_1 < Re(z) < R_1$. For the same price we include in $\mathcal{M}$ also the points $z$ for which $A(x)^{-1}$ or $B(x)^{-1}$ have a pole at $x = e^z$.

The two matrices satisfy

$$\overline{A}(qz)\overline{B}(z) = \overline{B}(pz)\overline{A}(z). \tag{5.6}$$

The vector $\overline{g}(z) = g(e^z)$, defined and meromorphic for $Re(z) < 0$, satisfies

$$\overline{g}(pz) = \overline{A}(z)\overline{g}(z), \quad \overline{g}(qz) = \overline{B}(z)\overline{g}(z).$$

Let $\widehat{E} = \mathbb{C}((z))$ and view (5.6) as a new type of a consistency equation in $G(\widehat{E})$.

**Proposition 16.** ("Claim 1 for case 2Q") *There exists a matrix $D(z) \in G(\widehat{E})$ such that*

$$D(pz)\overline{A}(z)D(z)^{-1} = A_1, \quad D(qz)\overline{B}(z)D(z)^{-1} = B_1$$

*are commuting scalar matrices. Moreover, as the entries of $\overline{A}(z)$ and $\overline{B}(z)$ are convergent in a punctured neighborhood of 0, so are the entries of $D(z)$.*

The proof of this Proposition is analogous to the proof of Claim 1 before, when we substitute for $\sigma$ and $\tau$ the operators

$$\overline{\sigma}(f)(z) = f(pz), \quad \overline{\tau}(f)(z) = f(qz).$$

This defines a group

$$\overline{\Gamma} = \langle \overline{\sigma}, \overline{\tau} \rangle \subset Aut(\widehat{E})$$

which is free abelian of rank 2, and the Proposition is the statement that

$$H^1(\overline{\Gamma}, G(\mathbb{C})) \to H^1(\overline{\Gamma}, G(\widehat{E}))$$

is bijective. Note that in the proof of Claim 1 the matrices satisfying the consistency equation could be taken to be any two matrices from $G(\widehat{K})$ (now from $G(\widehat{E})$) and the fact that they were rational (which no longer holds true after we substitute $x = e^z$) did not play a role. Of course, the analogous Claim 1 for the operators $\overline{\sigma}, \overline{\tau}$ does not *follow* from Claim 1 for $\sigma, \tau$, but the proof is similar and we shall skip

it. From one aspect the situation is even simpler, since the operators $\overline{\sigma}, \overline{\tau}$ do not require a passage to Puiseaux series.

**Lemma 17.** *The matrices $D(z)$ and $D(z)^{-1}$ can be continued to meromorphic functions everywhere in $z$, their poles are contained in $\bigcup_{n=0}^{\infty} p^n\mathcal{M}$, and there exists a $\delta > 0$ such that they are analytic in the sector $\overline{\Sigma}^{\pm} = \{z \in \mathbb{C}^{\times} | \, \delta < \arg(\pm z) < 2\delta\}$.*

*Proof.* By the equation $D(pz) = A_1 D(z)\overline{A}(z)^{-1}$ we extend $D(z)$ to a meromorphic function everywhere. Its poles, as well as the poles of $D(z)^{-1}$, are in $\bigcup_{n=0}^{\infty} p^n\mathcal{M}$. It is easily seen that the prescribed sector is disjoint from this set for a suitable $\delta$. □

Consider the vector-valued function

$$d(z) = D(z)\overline{g}(z).$$

Since (i) $g(x)$ is meromorphic for $|x| < 1$ and holomorphic in a punctured neighborhood of 0, and (ii) $D(z)$ is meromorphic everywhere and holomorphic in $\overline{\Sigma}^{-}$, we conclude that $d(z)$ is defined and meromorphic for $Re(z) < 0$ and holomorphic in

$$\overline{\Sigma}^{-}_{R} = \{z \in \mathbb{C}^{\times} | \, \pi + \delta < \arg(z) < \pi + 2\delta, \ |z| > R\}$$

for some $R > 0$. It satisfies there

$$d(pz) = A_1 d(z), \quad d(qz) = B_1 d(z).$$

This implies that $d(z)$ is in fact analytic on the whole of $\overline{\Sigma}^{-}$.

We now introduce a second change of variables

$$z = e^w$$

(so that $x = e^{e^w}$). The sector $\overline{\Sigma}^{\pm}$ is the biholomorphic image of the two infinite horizontal strips

$$\Sigma^{\pm} = \{\delta < Im(w) < 2\delta\} \cup \{\pi + \delta < Im(w) < \pi + 2\delta\}.$$

Let $L_1$ be a matrix such that $p^{L_1} = e^{\log p \cdot L_1} = A_1$. The vector-valued function

$$f(w) = e^{-wL_1} d(e^w) = e^{-wL_1} D(e^w)\overline{g}(e^w) \tag{5.7}$$

is holomorphic in $\Sigma^{-}$ and $\log p$-periodic. It has a Fourier expansion

$$f(w) = \sum_{l=-\infty}^{\infty} a_l e^{2\pi i l w/\log p}$$

convergent for $w \in \Sigma^{-}$. The second equation satisfied by $d(z)$ (with respect to $z \mapsto qz$) yields

$$f(w + \log q) = \widetilde{B}_1 f(w), \qquad \widetilde{B}_1 = e^{-\log q \cdot L_1} B_1$$

hence the Fourier coefficients satisfy

$$a_l e^{2\pi i l \cdot \log q/\log p} = \widetilde{B}_1 a_l.$$

Since the matrix $\widetilde{B}_1$ can have only finitely many eigenvalues and *since* $\log q/\log p$ *is irrational,* only finitely many Fourier coefficients are non-zero. This implies that $f(w)$ can be analytically continued to all $w \in \mathbb{C}$.

The function $\overline{g}(z) := g(e^z)$ is meromorphic in $Re(z) < 0$ and clearly $2\pi i$-periodic there. Let $w = \log(z)$ be the principal branch of the logarithm on the complement of the positive imaginary $z$-axis. Equation (5.7) defines a meromorphic continuation of $\overline{g}(z)$ to the complement of the positive imaginary $z$-axis. Since it is $2\pi i$ periodic for $Re(z) < 0$ it is $2\pi i$ periodic everywhere, but this gives now a $2\pi i$-periodic

meromorphic continuation of $\overline{g}(z)$ for every $z \in \mathbb{C}$. Moreover, the same equation shows that the poles of $\overline{g}(z)$, which can only come from the poles of $D(z)^{-1}$, hence lie in the set $\bigcup_{n=0}^{\infty} p^n \mathcal{M}$, are finite in number in any horizontal strip of width $2\pi i$.

We now conclude that $\overline{g}(z) = g(e^z)$ for a meromorphic function $g(x)$ which is everywhere defined in $\mathbb{C}$ and has finitely many poles.

5.2.4. *Growth at infinity.* To complete the proof of Claim 2, and with it the proof of the main theorem, it remains to show that $g(x)$ has polynomial growth as $x \to \infty$. This will establish that $g$ is meromorphic at $\infty$ too, hence rational. However, this polynomial growth is an immediate consequence of the functional equation

$$g(x^p) = A(x)g(x),$$

the fact that for $|x|$ large enough, $A$ and $g$ are analytic, and the fact that $||A(x)||$ grows polynomialy, as its entries are rational functions of $x$.

## References

[A-B] Boris Adamczewski, Jason P. Bell: A problem around Mahler functions, arXiv:1303.2019.

[Sch-Si] Reinhard Schäfke, Michael F. Singer: Consistent systems of linear differential and difference equations, arXiv:1605.02616.