CRITERIA FOR PERIODICITY AND AN APPLICATION TO ELLIPTIC FUNCTIONS

EHUD DE SHALIT

Abstract. Let P and Q be relatively prime integers greater than 1, and f a real valued discretely supported function on a finite dimensional real vector space V. We prove that if $f_P(x) = f(Px) - f(x)$ and $f_Q(x) = f(Qx) - f(x)$ are both Λ-periodic for some lattice $\Lambda \subset V$, then so is f (up to a modification at 0). This result is used to prove a theorem on the arithmetic of elliptic function fields. In the last section we discuss the higher rank analogue of this theorem and explain why it fails in rank 2. A full discussion of the higher rank case will appear in a forthcoming work.

Introduction

Let V be an r-dimensional vector space over $\mathbb{R}$ and $\mathscr{D}$ the abelian group of *discretely supported* functions[1] $f : V \to \mathbb{R}$. If $P \geq 2$ is an integer and $f \in \mathscr{D}$ we let

$$f_P(x) = f(Px) - f(x) \in \mathscr{D}.$$

Note that f_P is insensitive to the value of f at 0, namely we may modify f at 0 without affecting f_P. We henceforth call f' a *modification of* f *at* 0 if $f'(x) = f(x)$ at every $x \neq 0$.

Let $\Lambda \subset V$ be a lattice. Our interest lies in the subgroup $\mathscr{P}$ of $f \in \mathscr{D}$ satisfying the periodicity condition

$$f(x + \lambda) = f(x) \ \ (\forall \lambda \in \Lambda).$$

If $f \in \mathscr{P}$ then clearly $f_P(0) = 0$ and $f_P \in \mathscr{P}$. The converse is false, even if we allow to modify f at 0. Indeed, let $V = \mathbb{R}$, $\Lambda = \mathbb{Z}$. Let f_P be any non-zero $\mathbb{Z}$-periodic function vanishing at 0 and

$$f(x) = \sum_{i=1}^{\infty} f_P(x/P^i).$$

Observe that for every x the sum is finite, and that $f \in \mathscr{D}$. Then $f(Px) - f(x) = f_P(x)$, but f need not be periodic. If $f_P \geq 0$ and is supported on non-integral rational numbers whose denominators are relatively prime to P, then f is even unbounded.

In the first part of this note we prove the following theorem.

Theorem 1. *Let P and Q be greater than 1 and relatively prime integers. If both f_P and f_Q are Λ-periodic, so is a suitable modification of f at 0.*

The proof is elementary, but somewhat tricky. It is possible that the theorem remains valid if P and Q are only multiplicatively independent ($P^a = Q^b$ for $a, b \in \mathbb{Z}$ if and only if $a = b = 0$). Our methods do not yield this generalization, although we do obtain a partial result along the way, see Proposition 6.

2000 *Mathematics Subject Classification.* 39A10, 12H10, 14H52.
The author was supported by ISF grant 276/17.

[1] We call f discretely supported if $\{x \in V | f(x) \neq 0\}$ has no accumulation points in V.

Taking $V=\mathbb{R}$, $\Lambda=\mathbb{Z}$ and $f(x)=1$ if $0\neq x\in\mathbb{Z}$ and 0 elsewhere, we get that f_p is $\mathbb{Z}$-periodic for any prime p. This shows that we can not forgo the modification at 0, even if we replace it by the condition $f(0)=0$.

In the second part of our note we derive from Theorem 1 a theorem on elliptic functions. Here we take, of course, $V=\mathbb{C}$. The relation with elliptic functions comes from the fact that the *divisor function* $e=div(f)$, (i.e. $e(z)=ord_z(f)$) of a Λ-elliptic function f lives in $\mathscr{P}$, and determines f up to a multiplicative constant. We refer to the text for the precise formulation of our main result, see Theorem 7. Besides Theorem 1, its proof uses only basic facts on elliptic functions (the Abel-Jacobi theorem). Here we mention an immediate corollary.

Theorem 2. *Let P and Q be greater than 1 and relatively prime integers. Let f be a meromorphic function on $\mathbb{C}$ for which $f_P(z)=f(Pz)/f(z)$ and $f_Q(z)=f(Qz)/f(z)$ are Λ-elliptic. Then there exists a lattice $\Lambda'\subset\Lambda$ and an integer m such that $z^m f(z)$ is Λ'-elliptic. If* $\gcd(P-1,Q-1)=D$ *we can take $\Lambda'=D\Lambda$.*

In the third and last section we discuss our motivation: an elliptic analogue of *a conjecture of Loxton and van der Poorten*, proved by Adamczewski and Bell in [2]. Again we refer to the text for details. The original proof of this celebrated conjecture relied on Cobham's theorem in the theory of automata, whose proof in [3] was notoriously long and complicated. Recently, Schäfke and Singer found an independent proof [7] that both clarified the ideas involved, and eliminated the dependence on Cobham's theorem. In fact, as was known to the experts, the latter *follows* in turn from the Loxton-van der Poorten conjecture, so [7] yields a conceptual and relatively short proof of Cobham's theorem as an added bonus. For more on this circle of ideas and related work, see the survey paper by Adamczewski [1].

Although not explicitly stated so in [7], the mechanism behind the proof of Schäfke and Singer is cohomological. Reformulating their work [4] lead us to a similar question in the elliptic set-up, involving a certain non-abelian cohomology of $\Gamma\simeq\mathbb{Z}^2$ with coefficients in $GL_d(K)$, where K is the maximal unramified extension of the field of Λ-elliptic functions. While theorem 2 amounts to a positive answer to the case $d=1$ of this question, we give an example showing that already for $d=2$ the answer is negative.

The complete solution of the question raised in the last part amounts to a classification of objects that we call, in a forthcoming paper [8], *elliptic (P,Q)-difference modules.* In that work we show how a generalization of the periodicity criterion of Theorem 1 leads to a connection between this classification problem and the classification of vector bundles on elliptic curves, a result of Atiyah from 1957. For $d=2$ this suffices to complete the classifictaion of rank-2 elliptic (P,Q)-difference modules and deduce that, "up to a twist", our counter-example is the only such counter-example. We hope to settle the higher rank question completely in [8].

1. The theorem on periodic functions

1.1. **A Lemma.** We begin with an elementary lemma. Fix an integer $N\geq 1$. If $0\neq x\in\mathbb{Z}$ and p is a prime number we write $v_p(x)$ for the power of p dividing x. If S is a set of primes we write

$$x'_S=\prod_{p\in S}p^{-v_p(x)}\cdot x,$$

for the "prime-to-S" part of x (retaining the sign).

For non-zero $x, y \in \mathbb{Z}$ we define $x \sim_S y$ to mean $v_p(x) = v_p(y)$ for every $p \in S$ and $x'_S \equiv y'_S \mod N$. This is clearly an equivalence relation on $\mathbb{Z}$ (where, by convention, the equivalence class of 0 is a singleton). For example, when $N = 10$ and $S = \{5\}$, $12 \sim_S 32$ and $15 \sim_S 65$ but $15 \nsim_S 35$.

Lemma 3. *Let $N \geq 1$. Let S and T be disjoint, non-empty finite sets of primes and define $\sim_S$ and $\sim_T$ as above. Let $\sim$ be the equivalence relation on $\mathbb{Z}$ generated by $\sim_S$ and $\sim_T$, namely $x \sim y$ if there exists a sequence $x = x^{(1)}, \ldots, x^{(K)} = y$ such that for every i, $x^{(i)} \sim_S x^{(i+1)}$ or $x^{(i)} \sim_T x^{(i+1)}$. Assume that $x, y \neq 0$. Then $x \sim y$ if and only if $x \equiv y \mod N$.*

Proof. Let $m_p = v_p(x) + 1$ $(p \in S)$ and $n_q = v_q(y) + 1$ $(q \in T)$. Let

$$P = \prod_{p \in S} p^{m_p}, \ \ Q = \prod_{q \in T} q^{n_q}.$$

Assume that $y = x + kN$ and let s and t satisfy

$$sP - tQ = k.$$

Then

$$z = x + sPN = y + tQN$$

and it is easily checked that $x \sim_S z$ and $z \sim_T y$. Thus $x \sim y$.

For the converse note that if $x \sim_S y$ then, letting $e_p = v_p(x) = v_p(y)$ for $p \in S$,

$$x = \prod_{p \in S} p^{e_p} x'_S \equiv \prod_{p \in S} p^{e_p} y'_S = y \mod N,$$

and similarly if $x \sim_T y$, so if $x \sim y$ we must have $x \equiv y \mod N$. □

1.2. **A Proposition.** We use the same notation as in the introduction. In particular V is a real r-dimensional vector space, and Λ is a lattice in V.

Proposition 4. *Let P and Q be greater than 1 and relatively prime integers. Let $f \in \mathscr{D}$ be a function supported on $PQ\Lambda$. Let*

$$f_P(x) = f(Px) - f(x), \ \ f_Q(x) = f(Qx) - f(x). \tag{1.1}$$

If both f_P and f_Q are $N\Lambda$-periodic then a certain modification of f at 0 is $N\Lambda$-periodic.

Proof. Observe first that f_P is supported on $Q\Lambda$ and f_Q is supported on $P\Lambda$. If $N\Lambda \nsubseteq Q\Lambda$, let $\omega \in N\Lambda$, $\omega \notin Q\Lambda$ and let x be any point where $f_P(x) \neq 0$. Then $x \in Q\Lambda$ but $x + \omega \notin Q\Lambda$, leading to the contradiction $0 = f_P(x + \omega) = f_P(x)$. Thus $N\Lambda \subset Q\Lambda$ and N is divisible by Q. Similarly N is divisible by P, so N is divisible by PQ.

For every $0 \neq x \in V$ equations (1.1) give the relations

$$f(x) = \sum_{i=1}^{\infty} f_P(x/P^i) = \sum_{j=1}^{\infty} f_Q(x/Q^j), \tag{1.2}$$

both sums being finite. Fix $0 \neq x, y \in \Lambda$ such that $x - y \in N\Lambda$. We shall show that $f(x) = f(y)$. In particular there will be a constant c such that $f(x) = c$ for every $0 \neq x \in N\Lambda$. Modifying f to obtain the value c at 0 too, we get an $N\Lambda$-periodic function.

Fix a basis of Λ over $\mathbb{Z}$ in which the coordinates of x and y are all non-zero. This is always possible, and we call such a basis *adapted* to x and y. Using this basis we identify Λ with $\mathbb{Z}^r$ and V with $\mathbb{R}^r$. Instead of congruences modulo $N\Lambda$ we write congruences modulo N.

Let S be the set of primes dividing P and T the set of primes dividing Q. For u and v in $\mathbb{Z}^r$ write $u \sim_S v$ if this equivalence relation holds coordinate-wise. In particular, if the ν-th coordinate of u vanishes, so must the ν-th coordinate of v.

Since $x \equiv y \mod N$ and none of the coordinates of x or y vanishes, there is a sequence

$$x = x^{(1)}, \ldots, x^{(K)} = y$$

of vectors in $\mathbb{Z}^r$ such that for each l we have $x^{(l)} \sim_S x^{(l+1)}$ or $x^{(l)} \sim_T x^{(l+1)}$. (In fact the proof of Lemma 3 shows that we can take $K = 3$.) It is therefore enough to show that if $x \sim_S y$ then $f(x) = f(y)$. Assume therefore that $x \sim_S y$.

Write $x = P^m x'$ and $y = P^m y'$ where x' and y' are in $\mathbb{Z}^r$ but not in $P\mathbb{Z}^r$. That the same m works for both x and y follows from the fact that for each $1 \le \nu \le r$, the p-adic valuations of the ν-th coordinates $v_p(x_\nu) = v_p(y_\nu)$ for every prime $p|P$. Since f_P is supported on $\mathbb{Z}^r$, equation (1.2) implies

$$f(x) = \sum_{i=0}^{m-1} f_P(P^i x').$$

But $x \sim_S y$ implies that $P^i x' \equiv P^i y' \mod N$. Since f_P is N-periodic we get that

$$f(x) = \sum_{i=0}^{m-1} f_P(P^i y') = f(y).$$

This concludes the proof of the Proposition. □

1.3. **The proof of Theorem 1.** Let $f \in \mathscr{D}$ be as in the Theorem, $P, Q \ge 2$. Let Λ be a lattice of periodicity for f_P and f_Q. Our goal is to show that if $(P, Q) = 1$ the function f, appropriately modified at 0, is also Λ-periodic.

Denote by $S_P, S_Q \subset V/\Lambda$ the supports of f_P and f_Q and by $\widetilde{S}_P$ and $\widetilde{S}_Q$ their pre-images in V. Let $\widetilde{S}$ be the support of f.

Lemma 5. *Assume that P and Q are multiplicatively independent. Then the projection $\widetilde{S} \mod \Lambda$ is finite.*

Proof. Equation (1.2) holds for every $x \in V$ and shows that $\widetilde{S}$ is contained in

$$\bigcup_{n=1}^{\infty} P^n \widetilde{S}_P \cap \bigcup_{m=1}^{\infty} Q^m \widetilde{S}_Q.$$

It is therefore enough to prove that $\bigcup_{n=1}^{\infty} P^n S_P \cap \bigcup_{m=1}^{\infty} Q^m S_Q$ is finite. The sets S_P and S_Q are of course finite. Let $\bar{z} = z \mod \Lambda \in S_P$ and $\bar{w} = w \mod \Lambda \in S_Q$, n and m be such that $P^n \bar{z} = Q^m \bar{w}$. If z (hence also w) lies in $M = \mathbb{Q}\Lambda$ then there are altogether only finitely many points of the form $P^n \bar{z}$ in V/Λ. It is therefore enough to assume that $z, w \notin M$ and prove that (n, m) are then uniquely determined by (z, w). But suppose $P^n z \equiv Q^m w \mod \Lambda$ and also $P^{n'} z \equiv Q^{m'} w \mod \Lambda$, where without loss of generality we may assume $n' > n$. Then

$$(P^{n'-n} Q^m - Q^{m'}) w \in \Lambda,$$

contradicting the assumption that $w \notin M$. In the last step we used the multiplicative independence of P and Q to guarantee that the coefficient of w is non-zero. □

We continue with the proof, assuming only that P and Q are multiplicatively independent. Let S be the projection of $\widetilde{S}$ modulo Λ. Pick $z \in \widetilde{S}_P$, $z \notin M = \mathbb{Q}\Lambda$. We call $\{z, Pz, P^2z, ...\} \cap \widetilde{S}_P$ the *P-chain through* z. Since $z \notin M$ all the $P^n z$ have distinct images modulo Λ, so only finitely many of them belong to $\widetilde{S}_P$. Let $P^{n(z)}z$ be the last one, and call $n(z) \geq 0$ the *exponent* of the P-chain through z. Call a P-chain *primitive* if it is not properly contained in any other P-chain, i.e. if none of the points $P^n z$, $n < 0$, belongs to $\widetilde{S}_P$. Since $\widetilde{S}_P$ is Λ-periodic, $n(z + \lambda) = n(z)$ for $\lambda \in \Lambda$. It follows from the discreteness of $\widetilde{S}_P$ that

$$n_P = 1 + \max_{z \in \widetilde{S}_P,\, z \notin M} n(z) < \infty.$$

Let $\{z, Pz, \ldots, P^{n(z)}z\} \cap \widetilde{S}_P$ be a primitive P-chain through $z \notin M$. We claim that

$$\sum_{i=0}^{n(z)} f_P(P^i z) = 0. \tag{1.3}$$

Indeed, for every $n > n(z)$

$$f(P^n z) = \sum_{i=1}^{\infty} f_P(P^{n-i} z) = \sum_{i=0}^{n(z)} f_P(P^i z)$$

so the assertion follows from Lemma 5, since otherwise all $P^n z$, $n > n(z)$, would lie in $\widetilde{S}$, and they are all distinct modulo Λ. It follows also that $f(P^n z) = 0$ if $n < 0$ or $n > n(z)$.

Let $\lambda \in \Lambda$. Assume $z \notin M$ and $f(z) \neq 0$. Then

$$f(z) = \sum_{i=1}^{n_P} f_P(P^{-i} z).$$

The reason we can stop at $i = n_P$ is that if i_0 is the largest index such that $f_P(P^{-i}z) \neq 0$ and $i_0 > n_P$ then $f(z) = \sum_{i=1}^{\infty} f_P(P^{-i}z) = 0$ by (1.3) applied to $P^{-i_0}z$ instead of z. Thus if $f(z) \neq 0$ we must have $i_0 \leq n_P$. By the periodicity of f_P we now have

$$f(z) = \sum_{i=1}^{n_P} f_P(P^{-i}(z + P^{2n_P}\lambda)).$$

The last sum is equal to $\sum_{i=1}^{2n_P} f_P(P^{-i}(z + P^{2n_P}\lambda))$ because the terms with $n_P < i \leq 2n_P$ all vanish as they are equal to $f(P^{-i}z)$, which, as we have just seen, vanish. Since one of the terms $f_P(P^{-i}(z + P^{2n_P}\lambda))$ with $i \leq n_P$ must not vanish, and the exponent of any primitive P-chain is less than n_P, the terms $f_P(P^{-i}(z + P^{2n_P}\lambda))$ with $i > 2n_P$ all vanish. We conclude that

$$f(z) = \sum_{i=1}^{\infty} f_P(P^{-i}(z + P^{2n_P}\lambda)) = f(z + P^{2n_P}\lambda).$$

To sum up, we have shown that if $z \notin M$ and $f(z) \neq 0$ then $f(z) = f(z + P^{2n_P}\lambda)$ for every $\lambda \in \Lambda$. This of course stays true if $f(z) = 0$, for if $f(z + P^{2n_P}\lambda) \neq 0$ switch the roles of z and $z + P^{2n_P}\lambda$ and replace λ by $-\lambda$.

Repeating the same arguments with Q replacing P we get that

$$f(z) = f(z + q^{2n_Q}\lambda)$$

for all $z \notin M$. If $\gcd(P,Q)=1$, the lattice generated by $P^{2n_P}\Lambda$ and $Q^{2n_Q}\Lambda$ is Λ. We therefore get the following conclusion:

Proposition 6. *Let $f \in \mathscr{D}$ and assume that P and Q are multiplicatively independent. If f_P and f_Q are Λ-periodic then there exists a lattice $\Lambda' \subset \Lambda$ (depending on f) such that for every $z \notin M = \mathbb{Q}\Lambda$ and $\lambda \in \Lambda'$*

$$f(z+\lambda) = f(z).$$

If furthermore $\gcd(P,Q)=1$, we may take $\Lambda' = \Lambda$.

It remains to examine periodicity of f at points $z \in M$. For that we must assume that P and Q are relatively prime, as in Theorem 1. By Lemma 5 the support of f is finite modulo Λ. Let N be an integer divisible by PQ such that, with $\Lambda' = N^{-1}\Lambda$, the function f is supported on $PQ\Lambda'$. Changing the lattice, we are reduced to the following.

Claim. Let $\Lambda' \subset V$ be a lattice, N an integer divisible by PQ and $f : PQ\Lambda' \to \mathbb{R}$ a function. Assume that f_P and f_Q, which are supported on Λ', are $N\Lambda'$-periodic for some integer N. Then a suitable modification of f at 0 is $N\Lambda'$-periodic.

This was proved in Proposition 4.

2. A theorem on elliptic functions

Let $\Lambda \subset \mathbb{C}$ be a lattice and $M = \mathbb{Q}\Lambda$. Let K be the field of meromorphic functions on $\mathbb{C}$ which are periodic with respect to *some* lattice $\Lambda' \subset M$. We call such functions *M-elliptic*. If K_Λ is the field of Λ-elliptic functions, then K is the maximal unramified extension of K_Λ.

Let p and q be multiplicatively independent natural numbers[2]. Consider the automorphisms

$$\sigma f(z) = f(pz), \quad \tau f(z) = f(qz)$$

of the field K. Let $\widehat{K} = \mathbb{C}((z))$ and embed K in $\widehat{K}$ assigning to any f its Laurent series at 0.

Let

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

be the group of automorphisms of K generated by σ and τ. As σ and τ commute, and p and q are multiplicatively independent, $\Gamma \simeq \mathbb{Z}^2$. The group Γ acts of course also on $\widehat{K}$. The goal of this section is to show how Theorem 1 can be used to prove the following.

Theorem 7. *Assume that p and q are relatively prime. Then the map*

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

is an isomorphism.

Proof. In this section we reserve the letter f to denote elliptic functions. Typically, if $f \in K^\times$,

$$e(z) = ord_z(f) \in \mathscr{D}$$

and is of course periodic.

The injectivity statement is trivial: if f is Λ-elliptic for some $\Lambda \subset M$ and $f(pz)/f(z)$ is constant then it is easily seen that f had to be constant to begin with.

For the surjectivity consider $\mathcal{D}$, the group of all the functions $d : \mathbb{C} \to \mathbb{Z}$ with discrete support, which are Λ-periodic for some lattice $\Lambda \subset M$. Let $\mathcal{D}^0$ be the subgroup of all $d \in \mathcal{D}$ which are

[2] For typographical reasons, we let p and q stand for what was denoted P and Q in the previous section. The primes dividing P or Q will not show up anymore.

of degree 0 on $\mathbb{C}/\Lambda$, for some (equivalently, any) lattice Λ modulo which they are periodic. Let $\mathcal{P} \subset \mathcal{D}^0$ be the subgroup of principal divisors, i.e. d for which there exists a function $f \in K$ with $ord_z(f) = d(z)$, or $d = div(f)$. By the Abel-Jacobi theorem a $d \in \mathcal{D}^0$ is principal if and only if for some (equivalently, any) lattice Λ modulo which d is periodic, $\sum_{z\in\mathbb{C}/\Lambda} zd(z) \in M$.

Let $\{f_\gamma\}$ be a 1-cocycle with values in $K^\times$, and choose a lattice Λ such that f_σ and f_τ are Λ-elliptic. From $\sigma\tau = \tau\sigma$ we get

$$f_\tau(pz)/f_\tau(z) = f_\sigma(qz)/f_\sigma(z).$$

If $\{d_\gamma\}$ is the 1-cocycle with values in $\mathcal{P}$ defined by $d_\gamma(z) = ord_z(f_\gamma)$ then, looking at the constant term on both sides of the last equation, we get

$$p^{d_\tau(0)} = q^{d_\sigma(0)},$$

hence $d_\tau(0) = d_\sigma(0) = 0$. This implies that $d_\gamma(0) = 0$ for every $\gamma \in \Gamma$. For lack of a better terminology we call such a 1-cocycle $\{d_\gamma\}$ *special.*

From the exactness of

$$0 \to \mathbb{C}^\times \to K^\times \to \mathcal{P} \to 0$$

we see that it is enough to prove that our special 1-cocycle $\{d_\gamma\}$ is a coboundary. As before, from $\sigma\tau = \tau\sigma$ we get

$$d_\tau(pz) - d_\tau(z) = d_\sigma(qz) - d_\sigma(z). \tag{2.1}$$

We have to show that there exists an $e \in \mathcal{P}$ with

$$d_\sigma(z) = e(pz) - e(z), \;\; d_\tau(z) = e(qz) - e(z). \tag{2.2}$$

From the equation (2.1) we get

$$\begin{gathered} d_\tau(z) = d_\tau(z/p) + d_\sigma(qz/p) - d_\sigma(z/p) = \\ d_\tau(z/p^2) + d_\sigma(qz/p^2) + d_\sigma(qz/p) - d_\sigma(z/p^2) - d_\sigma(z/p) = \cdots \\ = \sum_{n=1}^{\infty} (d_\sigma(qz/p^n) - d_\sigma(z/p^n)). \end{gathered}$$

The sum is finite by the assumption on the supports. Thus, by telescopy,

$$\tilde{e}(z) = \sum_{m=1}^{\infty} d_\tau(z/q^m) = \sum_{n=1}^{\infty} d_\sigma(z/p^n) \tag{2.3}$$

satisfies (2.2). Its support is discrete.

We are now in a position to apply Theorem 1. Suitably modifying $\tilde{e}$ at 0 we get a function $e \in \mathcal{D}$ satisfying (2.2), in fact of the same periodicity lattice Λ of d_σ and d_τ. It remains to show that $e \in \mathcal{P}$, i.e. that it satisfies the two conditions prescribed by the Abel-Jacobi theorem.

Let Π be a parllelogram which is a fundamental domain for $\mathbb{C}/\Lambda$. Since $d_\sigma \in \mathcal{D}^0$,

$$0 = \sum_{z\in\Pi} d_\sigma(z) = \sum_{z\in p\Pi} e(z) - \sum_{z\in\Pi} e(z) = (p^2 - 1) \sum_{z\in\Pi} e(z),$$

so $e \in \mathcal{D}^0$. Similarly

$$\sum_{z\in\Pi} zd_\sigma(z) = \sum_{z\in\Pi} z(e(pz) - e(z)) = p^{-1} \sum_{z\in p\Pi} ze(z) - \sum_{z\in\Pi} ze(z) = (p-1) \sum_{z\in\Pi} ze(z).$$

Since f_σ is Λ-elliptic, the left hand side lies in Λ. If $\Lambda' = (p-1)\Lambda$ and Π' is a fundamental domain for $\mathbb{C}/\Lambda'$ consisting of $(p-1)^2$ translates of Π then

$$\sum_{z\in\Pi'} ze(z) = (p-1)^2 \sum_{z\in\Pi} ze(z) = (p-1)\sum_{z\in\Pi} zd_\sigma(z) \in \Lambda'.$$

By Abel-Jacobi, e is the divisor of a Λ'-elliptic function.

We have found an $e \in \mathcal{P}$ such that $d_\gamma = \gamma(e) - e$ for every $\gamma \in \Gamma$. This concludes the proof of the theorem. □

Let us turn to the proof of Theorem 2. Let f be meromorphic in $\mathbb{C}$ and assume that

$$f_p(z) = f(pz)/f(z), \;\; f_q(z) = f(qz)/f(z)$$

are Λ-elliptic. Let

$$d_\sigma(z) = ord_z(f_p), \;\; d_\tau(z) = ord_z(f_q).$$

The relation

$$d_\sigma(qz) - d_\sigma(z) = d_\tau(pz) - d_\tau(z)$$

guarantees that we can extend d to a special 1-cocycle $\{d_\gamma\}$ of Γ in $\mathcal{P}$. The proof of Theorem 7 above yields an $e \in \mathcal{P}$ for which $d_\gamma = \gamma(e) - e$. Let $\tilde{f}$ be the Λ'-elliptic function whose divisor is e. Let $g = \tilde{f}/f$. Then $g(pz)/g(z)$ is periodic and has no poles or zeros, so must be constant. This immediately implies that $g(z) = cz^m$ for some c and m. The theorem follows.

The proof shows that $\tilde{f}$ is Λ'-periodic, where $\Lambda' = (p-1)\Lambda$. By the same token we can take $\Lambda' = (q-1)\Lambda$. It follows that we can take, as the periodicity lattice of $\tilde{f}$, the lattice $D\Lambda$, where D is the greatest common divisor of $p-1$ and $q-1$.

3. Higher rank analogues

Theorem 7 raises a question in non-abelian cohomology. Let $d \geq 1$. The group $\Gamma \subset Aut(K)$ acts on $GL_d(K)$ via its action on K.

Question: Assume that p and q are multiplicatively independent and $d \geq 1$. Is the map of pointed sets

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

bijective? If not, is it injective? Can we identify its image?

When $K = \bigcup \mathbb{C}(z^{1/n})$, $\sigma(f)(z) = f(z^p)$ and $\tau(f)(z) = f(z^q)$, the analogous map is bijective. This is due entirely to Schäfke and Singer, even if [7] falls short of formulating it in cohomological terms. See also [4].

In [8] we show that the answer to the above question is *negative* as soon as $d \geq 2$. The *reason* for the different behavior in the case of $\mathbb{G}_m = \mathbb{P}^1 - \{0, \infty\}$, the algebraic group underlying the rational case studied in [7], and the elliptic case, turns out to be that while every vector bundle on $\mathbb{G}_m$ is trivial, there are non-trivial vector bundles on elliptic curves which are *invariant under pull-back by all isogenies*. These vector bundles have been classified by Atiyah in 1957, and sometimes bear his name.

In [8] we prove a vast generalization of the periodicity criterion proved in Theorem 1. Using it, we associate to a given class in $H^1(\Gamma, GL_d(K))$ a vector bundle on $\mathbb{C}/\Lambda$, for all small enough Λ. It turns out that the map $H^1(\Gamma, GL_d(\mathbb{C})) \to H^1(\Gamma, GL_d(K))$ is injective, and its image consists of the classes whose associated vector bundle is trivial.

We end by giving an example of a cohomolgy class in $H^1(\Gamma, GL_2(K))$ that does not come from a similar class over $\mathbb{C}$ by base change. Let $\Lambda \subset \mathbb{C}$ be a lattice and let $\zeta(z) = \zeta(z, \Lambda)$ be the Weierstrass zeta function of Λ. Recall that

$$\zeta'(z, \Lambda) = \wp(z, \Lambda)$$

is the Weierstrass $\wp$-function, but for $0 \neq \omega \in \Lambda$

$$\zeta(z + \omega) - \zeta(z) = \eta(\omega, \Lambda)$$

is a non-zero constant. Let

$$\begin{cases} g_p(z) = p\zeta(qz) - \zeta(pqz) \\ g_q(z) = q\zeta(pz) - \zeta(pqz) \end{cases}.$$

Clearly, g_p, g_q are Λ-elliptic functions. Let

$$A = \begin{pmatrix} 1 & g_p(z) \\ 0 & p \end{pmatrix}, \quad B = \begin{pmatrix} 1 & g_q(z) \\ 0 & q \end{pmatrix}.$$

It can be checked that there is a cocycle of Γ in $GL_2(K)$ sending σ^{-1} to A and τ^{-1} to B. Since Γ is free abelian, this amounts to checking the *consistency equation*

$$A(z/q)B(z) = B(z/p)A(z)$$

which the reader may easily verify.

In [8] we show that this cocycle represents a cohomology class that does not arise form a similar class over $\mathbb{C}$. In the language of difference equations, the pair (A, B) is not guage-equivalent to a pair (A_0, B_0) of scalar matrices. In fact, the results of [8] show that every class in $H^1(\Gamma, GL_2(K))$ that is not in the image of $H^1(\Gamma, GL_2(\mathbb{C}))$ is represented by a pair of matrices (aA, bB) with A, B as above and $a, b \in \mathbb{C}^\times$. Similar, but more complicated, results hold in higher ranks.

References

[1] Adamczewski, B.: *Mahler's method*, in Documenta Mathematica Extra Volume: Mahler Selecta (2019), 95-122.

[2] Adamczewski, B., Bell, J.P.: *A problem about Mahler functions,* Ann. Sci. Norm. Super. Pisa **17** (2017), 1301-1355.

[3] Cobham, A.: *On the Hartmanis-Stearns problem for a class of tag machines,* Conference Record of 1968 Ninth Annual Symposium on Switching and Automata Theory, Schenectady, New York (1968), 51-60.

[4] de Shalit, E.: *Notes on the conjecture of Loxton and van der Poorten*, seminar notes, available at: http://www.ma.huji.ac.il/~deshalit/new_site/ln.htm

[5] van der Poorten, A.J.: *Remarks on automata, functional equations and transcendence*, Séminaire de Théorie des Nombres de Bordeaux (1986–1987), Exp. No. **27**, 11pp.

[6] van der Put, M., Singer, M.F.: *Galois theory of difference equations*, Lecture Notes in Mathematics **1666,** Springer-Verlag, 1997.

[7] Schäfke, R., Singer, M.F.: *Consistent systems of linear differential and difference equations,* J. Eur. Math. Soc. **21** (2019), 2751–2792.

[8] de Shalit, E.: *Elliptic (p, q)-difference modules,* arXiv:2007.09508.

EINSTEIN INSTITUTE OF MATHEMATICS, HEBREW UNIVERSITY OF JERUSALEM
E-mail address: ehud.deshalit@mail.huji.ac.il