Noncommutative Tate curves

Igor Nikolaev *

Abstract

It is proved, that the homology group of the Tate curve is the Pontryagin dual to the K-theory of the UHF-algebras.

Key words and phrases: Tate curves, UHF-algebras

AMS (MOS) Subj. Class.: 11G07 (elliptic curves over local fields); 46L85 (noncommutative topology)

1 Introduction

A. The Pontryagin duality establishes a canonical isomorphism between the locally compact abelian group G and the group **Char** (**Char** (G)), where **Char** is the group of characters of G, i.e. the homomorphisms $G \to S^1$ [4]; such a duality generalizes the correspondence between the periodic function and its Fourier series. The aim of the underlying note is the Pontryagin duality between a geometric object known as the Tate curve and a class of the operator algebras known as the Uniformly Hyper-Finite algebras (the UHF-algebras) [3]; such a duality provides a (little studied) link between algebraic geometry of elliptic curves and their noncommutative topology. Roughly speaking, our result says that the K-theory of a UHF-algebra is a "Fourier series" of the abelian variety over the field of p-adic numbers; the details of the construction are given below.

*Partially supported by NSERC.

B. The Tate curve. We shall work with a plane cubic $E_q : y^2 + xy = x^3 + a_4(q)x + a_6(q)$, such that

$$a_4(q) = -5 \sum_{n=1}^{\infty} \frac{n^3 q^n}{1-q^n}, \qquad a_6(q) = -\frac{1}{12} \sum_{n=1}^{\infty} \frac{(5n^3 + 7n^5)q^n}{1-q^n}, \tag{1}$$

where q is a p-adic number satisfying condition $0 < |q| < 1$. The series (1) are convergent and, therefore, E_q is an elliptic curve defined over the field of p-adic numbers $\mathbf{Q}_p$; it is called a *Tate curve* [5], p.190. There exists a remarkable uniformization of E_q by the lattice $q^{\mathbb{Z}} = \{q^n : n \in \mathbb{Z}\}$; an exact result is this. Let $\mathbf{Q}_p^*$ be the group of units of $\mathbf{Q}_p$ and consider an action $x \mapsto qx$ for $x \in \mathbf{Q}_p^*$; the action is discrete and, therefore, the quotient $\mathbf{Q}_p^*/q^{\mathbb{Z}}$ is a Hausdorff topological space. It was proved by Tate, that there exists an (analytic) isomorphism $\phi : \mathbf{Q}_p^*/q^{\mathbb{Z}} \to E_q$; it follows from the last formula, that $H_1(E_q; \mathbf{Z}_p) \cong \mathbf{Z}_p$ (see p.5).

C. The UHF-algebras. A *UHF-algebra* ("Uniformly Hyper-Finite C^*-algebra") is a C^*-algebra which is isomorphic to the inductive limit of the sequence

$$M_{k_1}(\mathbb{C}) \to M_{k_1}(\mathbb{C}) \otimes M_{k_2}(\mathbb{C}) \to M_{k_1}(\mathbb{C}) \otimes M_{k_2}(\mathbb{C}) \otimes M_{k_3}(\mathbb{C}) \to \dots, \tag{2}$$

where $M_{k_i}(\mathbb{C})$ is a matrix C^*-algebra and $k_i \in \{1, 2, 3, \dots\}$; we shall denote the UHF-algebra by $M_{\mathbf{k}}$, where $\mathbf{k} = (k_1, k_2, k_3, \dots)$. The UHF-algebras $M_{\mathbf{k}}$ and $M_{\mathbf{k}'}$ are said to be *stably isomorphic* (Morita equivalent), whenever $M_{\mathbf{k}} \otimes \mathcal{K} \cong M_{\mathbf{k}'} \otimes \mathcal{K}$, where $\mathcal{K}$ is the C^*-algebra of compact operators; such an isomorphism means, that from the standpoint of noncommutative topology $M_{\mathbf{k}}$ and $M_{\mathbf{k}'}$ are homeomorphic topological spaces. To classify the UHF-algebras up to the stable isomorphism, one needs the following construction. Let p be a prime number and $n = \sup \ \{0 \le j \le \infty : p^j \mid \prod_{i=1}^{\infty} k_i\}$; denote by $\mathbf{n} = (n_1, n_2, \dots)$ an infinite sequence of n_i as p_i runs the ordered set of all primes. By $\mathbb{Q}(\mathbf{n})$ we understand an additive subgroup of $\mathbb{Q}$ consisting of rational numbers, whose denominators divide the "supernatural number" $p_1^{n_1} p_2^{n_2} \dots$; the $\mathbb{Q}(\mathbf{n})$ is a dense subgroup of $\mathbb{Q}$ and every dense subgroup of $\mathbb{Q}$ containing $\mathbb{Z}$ is given by $\mathbb{Q}(\mathbf{n})$ for some $\mathbf{n}$. The UHF-algebra $M_{\mathbf{k}}$ and the group $\mathbb{Q}(\mathbf{n})$ are connected by the formula $K_0(M_{\mathbf{k}}) \cong \mathbb{Q}(\mathbf{n})$, where $K_0(M_{\mathbf{k}})$ is the K_0-group of the C^*-algebra $M_{\mathbf{k}}$. The UHF-algebras $M_{\mathbf{k}}$ and $M_{\mathbf{k}'}$ are stably isomorphic if and only if $r\mathbb{Q}(\mathbf{n}) = s\mathbb{Q}(\mathbf{n}')$ for some positive integers r and s [1], p.28.

D. The result. Denote by $\{a_n\}_{n=1}^{\infty}$ a *canonical sequence* of the p-adic number q, i.e. the sequence of integers $0 \le a_n \le p^n - 1$, such that $|q - a_n| \le p^n$; the sequence is unique and satisfies the equation $a_{n+1} \equiv a_n \ \mathbf{mod}\ p^n$. Consider the rational numbers $0 \le \gamma_n = \frac{a_n}{p^n} < 1$ and let

$$\Gamma_q := \sum_{n=1}^{\infty} \gamma_n \mathbb{Z} \tag{3}$$

be an additive subgroup of $\mathbb{Q}$ generated by γ_n; it is a dense subgroup of $\mathbb{Q}$ containing $\mathbb{Z}$ (lemma 1). Finally, let $M_q := M_{\mathbf{k}(q)}$ be a UHF-algebra, such that $K_0(M_q) \cong \Gamma_q$; our main result can be stated as follows.

Theorem 1 *The discrete group $K_0(M_q)$ is the Pontryagin dual of the continuous group $H_1(E_q; \mathbf{Z}_p)$.*

The note is organized as follows. Theorem 1 is proved in Section 2 and a numerical example of the duality is constructed in Section 3.

2 Proof

We split the proof in a series of lemmas; for the notation and preliminary facts, we refer the reader to [1]–[5].

Lemma 1 *Let $q \neq 0$. Then:*

(i) $\mathbb{Z} \subset \Gamma_q$;

(ii) $\overline{\Gamma}_q = \mathbb{Q}$.

Proof. Recall that every p-adic integer can be uniquely written as $q = \sum_{i=1}^{\infty} b_i p^i$, where $0 \le b_i \le p-1$; the integers b_i are related to the canonical sequence by the formulas:

$$\begin{cases} a_1 &= b_1 \\ a_2 &= b_1 + b_2 p \\ a_3 &= b_1 + b_2 p + b_3 p^2 \\ \vdots & \end{cases} \tag{4}$$

Note that $q = 0$ if and only if all $b_i = 0$. If $q \neq 0$, some $b_i \neq 0$; thus, there are infinitely many $a_i \neq 0$. Therefore, group Γ_q has an infinite number of the non-trivial generators.

(i) Let γ and γ' be a pair of non-trivial generators of Γ_q; clearly, their nominators a and a' are integers and belong to Γ_q. By the Euclidean algorithm, the equation $ra - sa' = 1$ has a solution in integers r and s; thus, $1 \in \Gamma_q$ and $\mathbb{Z} \subset \Gamma_q$. The first part of lemma 1 follows.

(ii) In view of formulas (4), we have

$$\gamma_n = \frac{a_n}{p^n} = \frac{b_1 + b_2 p + \ldots + b_n p^{n-1}}{p^n} \approx \frac{b_n}{p}, \tag{5}$$

where $\approx$ means the first approximation (the main part) of a rational number; thus, $\gamma_n \approx \frac{b_n}{p}$. Consider a pair of generators γ_n and $\gamma_{n'}$; then $p\gamma_n \approx b_n$ and $p\gamma_{n'} \approx b_{n'}$. Since $p\gamma_n \in \Gamma_q$ and $p\gamma_{n'} \in \Gamma_q$, the element $b_{n'}(p\gamma_n) - b_n(p\gamma_{n'})$ also belongs to Γ_q. But $pb_{n'}\gamma_n - pb_n\gamma_{n'} \approx 0$ and, therefore, there are elements of the group Γ_q, which are arbitrary close to zero. To prove part (ii), assume to the contrary that $\overline{\Gamma}_q \neq \mathbb{Q}$; then there exists $r/s \in \mathbb{Q}$ and the closest $\gamma \in \Gamma_q$, such that $|\gamma - \frac{r}{s}| = \varepsilon > 0$. Take $\gamma' \in \Gamma_q$ such that $|\gamma'| = \varepsilon_0 < \varepsilon$; then $\gamma - \gamma'$ lies between γ and r/s. Thus, γ is not the closest to r/s; this contradiction proves, that $\overline{\Gamma}_q = \mathbb{Q}$. Lemma 1 follows. $\square$

Recall that the abelian group

$$\mathbb{Z}(p^\infty) := \langle \gamma_1, \gamma_2, \ldots \mid p\gamma_1 = 0,\ p\gamma_2 = \gamma_1,\ p\gamma_3 = \gamma_2, \ldots \rangle \tag{6}$$

is called *quasicyclic* (or Prüfer) group [2], p.15; the following lemma clarifies the algebraic structure of Γ_q.

Lemma 2 $\Gamma_q/\mathbb{Z} \cong \mathbb{Z}(p^\infty)$ *whenever* $|q| < 1$.

Proof. Let us verify the condition $p\gamma_1 = 0$. Since $|q| < 1$, the p-adic number q is not a unit of the ring of p-adic integers $\mathbf{Z}_p$; therefore, in the canonical sequence for q the integer $a_1 = 0$. On the other hand, $p\gamma_1 = a_1$ and, thus, $p\gamma_1 = 0$.

Let us verify the condition $p\gamma_{n+1} = \gamma_n$ for $n \geq 1$; it follows from formulas (4), that:

$$\left\{ \begin{array}{lll} \gamma_n & = & \frac{b_1 + \ldots + b_n p^{n-1}}{p^n} \\ \gamma_{n+1} & = & \frac{b_1 + \ldots + b_n p^{n-1} + b_{n+1} p^n}{p^{n+1}}. \end{array} \right. \tag{7}$$

Since

$$p\gamma_{n+1} \quad = \quad \frac{b_1 + \ldots + b_n p^{n-1} + b_{n+1} p^n}{p^n} =$$

$$
\begin{aligned}
&= \frac{b_1 + \ldots + b_n p^{n-1}}{p^n} + b_{n+1} = \\
&= \gamma_n + b_{n+1},
\end{aligned}
$$

we have $p\gamma_{n+1} = \gamma_n + b_{n+1}$, where b_{n+1} is an integer; thus, $p\gamma_{n+1} = \gamma_n \textbf{ mod } 1$. Lemma 2 follows. □

Lemma 3 *Every $q \in \mathbf{Z}_p$ is a character of the abelian group $\mathbb{Z}(p^\infty)$.*

Proof. Since $\Gamma_q \subset \mathbb{R}$, by lemmas 1-2 there exists a map $i_q : \mathbb{Z}(p^\infty) \to \mathbb{R}/\mathbb{Z}$; note, that i_q is correctly defined for $0 < |q| < 1$ and extends to $q = 0$ and $q = 1$. Let us show, that i_q is a homomorphism. Indeed, if $\gamma, \gamma' \in \mathbb{Z}(p^\infty)$, then $i_q(\gamma + \gamma') = (\gamma + \gamma') \textbf{ mod } 1 = \gamma \textbf{ mod } 1 + \gamma' \textbf{ mod } 1 = i_q(\gamma) + i_q(\gamma')$. Thus, the map $i_q : \mathbb{Z}(p^\infty) \to \mathbb{R}/\mathbb{Z} \cong S^1$ is a homomorphism, i.e. i_q is a character of the group $\mathbb{Z}(p^\infty)$. □

In view of lemma 3, we have $\mathbf{Z}_p \cong \textbf{Char } (\mathbb{Z}(p^\infty))$, where **Char** is the group of characters of the abelian group. Note, that in the p-adic topology $\mathbf{Z}_p$ is a compact totally disconnected abelian group whose group operation is the addition of the p-adic numbers; likewise, $\mathbb{Z}(p^\infty)$ is a discrete abelian group endowed with the discrete topology. Since $\mathbf{Z}_p \cong \textbf{Char } (\mathbb{Z}(p^\infty))$, by the First Fundamental Theorem [4] there exists a canonical continuous isomorphism $\mathbb{Z}(p^\infty) \to \textbf{Char } (\textbf{Char } (\mathbb{Z}(p^\infty)))$; the isomorphism sends $\gamma \in \mathbb{Z}(p^\infty)$ into the character $x_\gamma : \textbf{Char } (\mathbb{Z}(p^\infty)) \to S^1$ defined by the formula:

$$
x_\gamma(y) = y(\gamma), \quad \forall y \in \textbf{Char } (\mathbb{Z}(p^\infty)). \tag{8}
$$

Thus, $\mathbf{Z}_p$ is the Pontryagin dual of the group $\Gamma_q \cong K_0(M_q)$.

Let us show, that $\mathbf{Z}_p \cong H_1(E_q; \mathbf{Z}_p)$. Indeed, each elliptic curve E is isomorphic to its own Jacobian, i.e. $E \cong \textbf{Jac } (E) := \Omega^1(E)/H_1(E)$, where $\Omega^1(E)$ is the vector space of analytic differentials on E. Since $\Omega^1(E_q) \cong \mathbf{Q}_p^*$ and $E_q \cong \mathbf{Q}_p^*/q^{\mathbb{Z}}$, we conclude that $H_1(E_q) \cong q^{\mathbb{Z}} \cong \mathbb{Z}$; then by the Universal Coefficient Formula one gets $H_1(E_q; \mathbf{Z}_p) \cong H_1(E_q) \otimes \mathbf{Z}_p \cong \mathbb{Z} \otimes \mathbf{Z}_p \cong \mathbf{Z}_p$. Theorem 1 is proved. □

3 Example

We shall consider an example illustrating theorem 1. Let p be a prime and consider the p-adic integer $q = p$; to obtain the canonical sequence for q, notice that:

$$\begin{cases} a_1 &= b_1 = 0 \\ a_2 &= b_1 + b_2 p = 0 + 1 \times p \\ a_3 &= b_1 + b_2 p + b_3 p^2 = 0 + 1 \times p + 0 \times p^2 \\ \vdots \end{cases} \tag{9}$$

Thus, $b_2 = 1$ and $b_1 = b_3 = \ldots = 0$; the canonical sequence $(a_1, a_2, a_3, \ldots)$ for $q = p$ takes the form $(0, p, p, \ldots)$ and, therefore, the generators $\gamma_1 = 0$ and $\gamma_n = \frac{a_n}{p^n} = \frac{p}{p^n} = \frac{1}{p^{n-1}}$ for $n \geq 2$. In this case one gets the following dense subgroup of $\mathbb{Q}$:

$$\Gamma_p = \sum_{n=1}^{\infty} \frac{1}{p^n} \mathbb{Z} = \mathbb{Z} \left[\frac{1}{p} \right]. \tag{10}$$

Thus $\Gamma_p \cong Q(\mathbf{n})$, where $\mathbf{n} = (0, \ldots, 0, \infty, 0, \ldots)$; therefore, $\Gamma_p \cong K_0(M_{\mathbf{k}})$, where $\mathbf{k} = (p, p, \ldots)$. In other words, the UHF-algebra corresponding to the Tate curve $E_p = \mathbf{Q}_p^* / p^{\mathbb{Z}}$ has the form:

$$M_{p^\infty} := M_p(\mathbb{C}) \otimes M_p(\mathbb{C}) \otimes \ldots \tag{11}$$

We conclude that the UHF-algebra M_{p^∞} is the "Fourier series" of the Tate curve E_p; in the particular case $p = 2$ one gets a duality between the Tate curve E_2 and the UHF-algebra M_{2^∞}, which is known as the Canonical Anti-commutation Relations C^*-algebra (the CAR or Fermion algebra) [1], p.13.

References

[1] E. G. Effros, Dimensions and C^*-Algebras, in: Conf. Board of the Math. Sciences No.46, AMS (1981).

[2] L. Fuchs, Infinite Abelian Groups, vol.1, Academic Press, 1970.

[3] J. G. Glimm, On a certain class of operator algebras, Trans. Amer. Math. Soc. 95 (1960), 318-340.

[4] L. S. Pontrjagin, The theory of topological commutative groups, Annals of Math. 35 (1934), 361-388.

[5] J. T. Tate, The arithmetic of elliptic curves, Inventiones Math. 23 (1974), 179-206.

The Fields Institute for Mathematical Sciences, Toronto, ON, Canada, E-mail: igor.v.nikolaev@gmail.com

Current address: 101-315 Holmwood Ave., Ottawa, ON, Canada, K1S 2R2