J. Noncommut. Geom. 8 (2014), 873–945
DOI 10.4171/JNCG/173

Journal of Noncommutative Geometry
© European Mathematical Society

On the arithmetic of the BC-system

Alain Connes and Caterina Consani*

Abstract. For each prime p and each embedding σ of the multiplicative group of an algebraic closure of $\mathbb{F}_p$ as complex roots of unity, we construct a p-adic indecomposable representation π_σ of the integral BC-system as additive endomorphisms of the big Witt ring of $\bar{\mathbb{F}}_p$. The obtained representations are the p-adic analogues of the complex, extremal KMS$_\infty$ states of the BC-system. The role of the Riemann zeta function, as partition function of the BC-system over $\mathbb{C}$ is replaced, in the p-adic case, by the p-adic L-functions and the polylogarithms whose values at roots of unity encode the KMS states. We use Iwasawa theory to extend the KMS theory to a covering of the completion $\mathbb{C}_p$ of an algebraic closure of $\mathbb{Q}_p$. We show that our previous work on the hyperring structure of the adèle class space, combines with p-adic analysis to refine the space of valuations on the cyclotomic extension of $\mathbb{Q}$ as a noncommutative space intimately related to the integral BC-system and whose arithmetic geometry comes close to fulfill the expectations of the "arithmetic site". Finally, we explain how the integral BC-system appears naturally also in de Smit and Lenstra construction of the standard model of $\bar{\mathbb{F}}_p$ which singles out the subsystem associated to the $\hat{\mathbb{Z}}$-extension of $\mathbb{Q}$.

Mathematics Subject Classification (2010). 11M55, 46L55, 58B34.
Keywords. Witt rings, finite fields, BC-system.

Contents

*The authors are partially supported by the NSF grant DMS-FRG-0652164. The first author is grateful to Yves André for a helpful suggestion. The second author would like to thank the Institut des Hautes Études Scientifiques and the Collège de France for some financial support.

1. Introduction

This paper describes several arithmetic properties of the BC-system, showing new and interesting connections with the theory of Witt vectors over the algebraic closure of finite fields and with p-adic analysis.

The BC-system is a system of quantum statistical mechanics defined by a noncommutative Hecke algebra of double classes in $P^+(\mathbb{Q})$ with respect to the subgroup $P^+(\mathbb{Z})$, where $P \subset \mathrm{GL}_2$ is the "$ax+b$" algebraic group (cf. [4], [10]). The complex Hecke algebra $\mathcal{H}_{\mathbb{C}}$ of the system has a highly non-trivial structure since its regular representation, in the Hilbert space of one sided classes, generates a factor of type III_1 and a canonical "time evolution" $\sigma_t \in \mathrm{Aut}(\mathcal{H}_{\mathbb{C}})$. The study of the KMS-equilibrium states at different temperatures has revealed the arithmetic nature of this dynamical system in view of the following facts.

- The partition function of the system is the Riemann zeta function.
- There is a phase transition with spontaneous symmetry breaking at the pole of zeta function.
- The zero temperature vacuum states implement the global class field isomorphism for $\mathbb{Q}$.

The study of the BC-system inaugurated the interplay between number-theory and noncommutative geometry. It is exactly the noncommutativity of the Hecke algebra of the system which generates its non-trivial dynamics. Moreover, on the noncommutative space of adèles classes $\mathbb{A}_{\mathbb{Q}}/\mathbb{Q}^*$, which is naturally associated to the type II dual of the BC-system, one obtains the spectral realization of zeros of L-functions and the trace formula interpretation of the Riemann-Weil explicit formulas (cf. [8]).

Further study (cf. [16]) has shown that the integral Hecke algebra $\mathcal{H}_{\mathbb{Z}} = \mathbb{Z}[\mathbb{Q}/\mathbb{Z}] \rtimes \mathbb{N}$ supplies an integral model to the BC-system. The endomorphisms $\sigma_n(e(r)) = e(nr)$, $n \in \mathbb{N}$, act on the canonical generators $e(r) \in \mathbb{Z}[\mathbb{Q}/\mathbb{Z}]$ for $r \in \mathbb{Q}/\mathbb{Z}$ and have natural linear quasi-inverses

$$\tilde{\rho}_n : \mathbb{Z}[\mathbb{Q}/\mathbb{Z}] \to \mathbb{Z}[\mathbb{Q}/\mathbb{Z}], \quad \tilde{\rho}_n(e(\gamma)) = \sum_{n\gamma'=\gamma} e(\gamma'),$$

which are used in the construction of the crossed product and in the presentation of the algebra.

In this paper we establish, for each prime p, a strong relation connecting the integral BC-system and the universal Witt ring $\mathbb{W}_0(\overline{\mathbb{F}}_p)$ of an algebraic closure of a prime field. The Witt construction is in fact considered in the following three different forms:

- as a K-theory endofunctor $A \mapsto \mathbb{W}_0(A) = K_0(\underline{\mathrm{End}}_A)/K_0(A)$ in the category of commutative rings (with unit);
- as the big Witt ring $\mathbb{W}(A)$;
- as the functor $A \mapsto \mathbb{W}_{p^\infty}(A)$ for A of characteristic p.

In the first two cases, the key structures are provided by the following operators:

- the Teichmüller multiplicative lift $\tau\colon A \to \mathbb{W}_0(A)$;
- the Frobenius endomorphisms $F_n\colon \mathbb{W}_0(A) \to \mathbb{W}_0(A)$, $n \in \mathbb{N}$;
- the Verschiebung (= shift), that is, additive functorial maps $V_n\colon \mathbb{W}_0(A) \to \mathbb{W}_0(A)$, $n \in \mathbb{N}$;
- the n-th ghost components $\mathrm{gh}_n\colon \mathbb{W}_0(A) \to A$, $n \in \mathbb{N}$.

These basic operators extend from the universal ring $\mathbb{W}_0(A)$ to its completion $\mathbb{W}(A)$ whose elements are expressed by Witt vectors, in terms of which all the algebraic operations can be defined in terms of polynomials with integral coefficients. This integrality property encodes a rich and deep arithmetical information. Moreover, the ring structure restricts to divisor stable subsets of $\mathbb{N}$ yielding, for the set of powers of a prime p, the functor $\mathbb{W}_{p^\infty}$.

In Proposition 4.4 and Theorem 4.5 we prove that the p-primary structure of the integral BC-system is completely encoded by the universal ring $\mathbb{W}_0(\bar{\mathbb{F}}_p)$, with a precise dictionary expressing the key operators σ_n and $\tilde{\rho}_n$ of the BC-system as respectively the Frobenius F_n and the Verschiebung V_n on $\mathbb{W}_0(\bar{\mathbb{F}}_p)$. The isomorphism connecting these algebraic structures depends upon the choice of a group isomorphism of the multiplicative group of $\bar{\mathbb{F}}_p$ with the group of *complex* roots of unity of order prime to p: the ambiguity inherent to this choice is the same as that pertaining to the construction of Brauer lift of characters.

The completion process associated to the inclusion $\mathbb{W}_0(A) \subset \mathbb{W}(A)$ with dense image, is then used in Theorem 6.4 to obtain, when $A = \bar{\mathbb{F}}_p$ and for each injective group homomorphism $\sigma\colon \bar{\mathbb{F}}_p^\times \to \mathbb{C}^\times$, a p-adic *indecomposable* representation π_σ of the integral BC-system as additive endomorphisms of the big Witt ring $\mathbb{W}(\bar{\mathbb{F}}_p)$. The construction uses the identification proven in Theorem 4.5 and the implementation of the Artin–Hasse exponentials. These representations are the p-adic analogues of the complex, extremal KMS_∞ states of the BC-system. In Section 7 this analogy is pursued much further. By implementing the theory of p-adic L-functions, we construct an analogue, in the p-adic case, of the partition function and of the KMS_β states. In particular, we show that the division relations for the p-adic polylogarithms at roots of unity correspond to the KMS condition. In §7.5 we prove that the definition of the functionals satisfying such condition extends from the standard "extended s-disk" to the natural multiplicative group covering of $\mathbb{C}_p$. These results are the p-adic counterparts of the statements proven in [17] for function fields. However, we also recognize an important difference with respect to the complex case, namely the presence of an added symmetry at non-zero temperature, due to the invariance of the states under the natural involution of $\mathbb{Q}^{\mathrm{cyc}}$ which replaces each root of unity by its inverse. This added symmetry is a consequence of the vanishing of the p-adic L-functions associated to odd Dirichlet characters.

In the second part of this paper we first recall known results of number theory on valuations of the cyclotomic field $\mathbb{Q}^{\mathrm{cyc}}$, abstractly defined in Definition 8.1 as the quotient of the group ring $\mathbb{Q}[\mathbb{Q}/\mathbb{Z}]$ by the cyclotomic ideal. We then relate these results to the first part, the parameter space X_p for the p-adic representations of the integral BC-system and the ongoing search of a geometric interpretation of the adèle class space. For p a prime number, the set X_p is, using the exponential $\mathbb{Q}/\mathbb{Z} \ni \gamma \mapsto e^{2\pi i\gamma}$ to embed $\mathbb{Q}^{\mathrm{cyc}} \subset \mathbb{C}$, the set of all injective group homomorphisms $\sigma\colon \bar{\mathbb{F}}_p^\times \to \mathbb{Q}/\mathbb{Z}$. In Section 8, we relate this set with the space $\mathrm{Val}_p(\mathbb{Q}^{\mathrm{cyc}})$ of extensions of the p-adic valuation to the maximal abelian field extension $\mathbb{Q}^{\mathrm{cyc}}$ of $\mathbb{Q}$. Let $(\mathbb{Q}/\mathbb{Z})^{(p)}$ be the subgroup of $\mathbb{Q}/\mathbb{Z}$ of fractions with denominator prime to p and let $\mathbb{Q}^{\mathrm{cyc,p}}$ be the subfield (i.e., the inertia subfield) of $\mathbb{Q}^{\mathrm{cyc}}$ generated by the group $\mu^{(p)} \sim (\mathbb{Q}/\mathbb{Z})^{(p)}$ of roots of unity of order prime to p. We describe canonical isomorphisms of $\mathrm{Val}_p(\mathbb{Q}^{\mathrm{cyc}})$ with each of the following spaces:

(1) The space of sequences of irreducible polynomials $P_n(T) \in \mathbb{F}_p[T]$, $n \in \mathbb{N}$, fulfilling the basic conditions of the Conway polynomials (cf. Theorem 8.7).

(2) The space Σ_p of bijections of the monoid $\mathcal{M}(p) = \mu^{(p)} \cup \{0\}$ commuting with their conjugates, as in Definition 8.5 (cf. Proposition 8.8).

(3) The space $\mathrm{Hom}(\mathbb{Q}_{\mathrm{Fr}}^{\mathrm{cycl,p}}, \mathbb{Q}_p)$ of field homomorphisms, where $\mathbb{Q}_{\mathrm{Fr}}^{\mathrm{cycl,p}} \subset \mathbb{Q}^{\mathrm{cyc,p}}$ is the decomposition subfield, i.e., the fixed field under the Frobenius automorphism (cf. Proposition 8.12).

(4) The quotient of the space X_p by the action of $\mathrm{Gal}(\bar{\mathbb{F}}_p)$ (cf. Proposition 8.14).

(5) The algebraic spectrum of the quotient algebra $\mathbb{F}_p[(\mathbb{Q}/\mathbb{Z})^{(p)}]/J_p$, where J_p is the reduction modulo p of the cyclotomic ideal (cf. Definition 8.1 and Proposition 8.16).

For a global field $\mathbb{K}$ of positive characteristic (i.e., a function field associated to a projective, non-singular curve over a finite field $\mathbb{F}_q$) it is a well-known fact that the space of valuations of the maximal abelian extension $\mathbb{K}^{\mathrm{ab}}$ of $\mathbb{K}$ has a geometric meaning. In fact, for each finite extension E of $\bar{\mathbb{F}}_q \otimes_{\mathbb{F}_q} \mathbb{K} \subset \mathbb{K}^{\mathrm{ab}}$, the space $\mathrm{Val}(E)$ of (discrete) valuations of E is an algebraic, one-dimensional scheme whose non-empty open sets are the complements of the finite subsets $F \subset \mathrm{Val}(E)$. The structure sheaf is locally defined by the intersection $\bigcap_F R$ of the valuation rings inside E. Then the space $\mathrm{Val}(\mathbb{K}^{\mathrm{ab}})$ is the projective limit of the schemes $\mathrm{Val}(E)$, $E \subset \mathbb{K}^{\mathrm{ab}}$.

For the global field $\mathbb{K} = \mathbb{Q}$ of rational numbers, one can consider its maximal abelian extension $\mathbb{Q}^{\mathrm{cyc}}$ as an abstract field and try to follow a similar idea. In Section 9, we show however that the space $\mathrm{Val}(\mathbb{Q}^{\mathrm{cyc}})$ provides only a rough analogue, in characteristic zero, of $\mathrm{Val}(\mathbb{K}^{\mathrm{ab}})$, more specifically the fiber $\mathrm{Val}_p(\mathbb{Q}^{\mathrm{cyc}})$ of $\mathrm{Val}(\mathbb{Q}^{\mathrm{cyc}})$ over a rational prime p does not give the sought for counterpart of the adelic description. Our approach to this problem is guided and motivated by the following three results contained in our previous work:

(a) The adelic interpretation of the loop groupoid $\Pi_1^{\mathrm{ab}}(X)'$ of the abelian cover of the algebraic curve X associated to a function field (cf. [15] and § 9.1).

(b) The determination of the counting function $N(q)$ (a distribution on $[1,\infty)$) which replaces, for $\mathbb{K} = \mathbb{Q}$, the classical Weil counting function for a function field (cf. [11] and § 9.4).

(c) The interpretation of the counting function $N(q)$ as an intersection number, using the action of the idèle class group on the adèle class space (cf. [12]).

By applying these results we find that the sought for geometric fiber over a non-archimedean, rational prime p is the total space of a principal bundle, with base $\mathrm{Val}_p(\mathbb{Q}^{\mathrm{cyc}})$ and structure group given by a connected, compact solenoid S whose definition is given in Proposition 9.2. Then, in Proposition 9.3, we derive a natural construction for the fiber as the mapping torus Y_p of the action of the Frobenius on the space X_p. In Section 9.3, we consider the fiber Y_∞ over the archimedean prime, with the implementation of the theory of multiplicative norms.

The interpretation given in (c) for the counting function as intersection number shows that the fibers Y_p should not be considered in isolation, but as being part of an ambient noncommutative space which is responsible for the transversality factors due to the archimedean contribution to the explicit formulas. This interpretation is explained in details in Section 9.4.

In Section 9.5, we show that the integral BC-system gives, for each p (including the archimedean prime), a natural embedding of the fiber Y_p into a noncommutative space constructed using the set $\mathcal{E}(\mathbb{C}_p)$ of the $\mathbb{C}_p$-rational points of the affine group scheme $\mathcal{E}$ which defines the abelian part of the system (cf. [16]). Here $\mathbb{C}_p$ denotes the p-adic completion of an algebraic closure of $\mathbb{Q}_p$. This result shows that the space

$$X(\mathbb{C}_p) := (\mathcal{E}(\mathbb{C}_p) \times (0, \infty))/(\mathbb{N} \times \{\pm 1\}) \tag{1}$$

matches, for any rational prime p including $p = \infty$, the definition of the adèle class space. In Proposition 9.5 we show, using the fact that $\mathcal{E}$ is a group scheme, that $X(\mathbb{C}_p)$ is a free module of rank one over the hyperring $\mathbb{H}_{\mathbb{Q}}$ of the adèle classes. The problem of a correct interpretation of the connected factor $(0, \infty)$ in (1) remains open.

It is a general principle that in our constructions the noncommutative spaces arise as $X(A)$ for a commutative ring A (cf. (1)), while the classical subspaces of $X(A)$ are defined as the support of the cyclotomic ideal (in the affine scheme $\mathcal{E} = \mathrm{Spec}(\mathbb{Z}[\mathbb{Q}/\mathbb{Z}])$).

We end the paper by showing in Section 10 the relevance of the recent work of B. de Smit and H. Lenstra (cf. [19]) on the "standard model" for the algebraic closure of a finite field. When $\mathbb{K}$ is a function field, the intermediate extension $\mathbb{K} \subset L = \overline{\mathbb{F}}_q \otimes_{\mathbb{F}_q} \mathbb{K} \subset \mathbb{K}^{\mathrm{ab}}$ plays an important geometric role, namely the extension of scalars to an algebraically closed field, for the algebraic curve associated to $\mathbb{K}$. When $\mathbb{K} = \mathbb{Q}$, we show that the intermediate extension $\mathbb{Q} \subset \mathbb{Q}_\Delta^{\mathrm{cycl}} \subset \mathbb{Q}^{\mathrm{cyc}}$ used by de Smit and Lenstra comes very close to fulfill the expected properties for a similar intermediate extension $\mathbb{Q} \subset L \subset \mathbb{Q}^{\mathrm{cyc}}$. Their construction provides a conceptual construction of the subfield of $\overline{\mathbb{F}}_p$ union of all extensions whose degree is prime to p. In the very last part of the paper we recall one of the first applications provided by E. Witt of his functor, which is a conceptual construction of the missing piece $\bigcup_n \mathbb{F}_{p^{p^n}} \subset \overline{\mathbb{F}}_p$, using the simple equation $X^p = X + 1$ in Witt vectors.

2. The functor $\mathbb{W}_0$

In this section we recall the definition and the main properties of the universal ring $\mathbb{W}_0(A)$, where A is any commutative ring with unit. We refer to [1] to read more details and also to [6], IX, Exercices 28–58, §1. The second part of the section describes $\mathbb{W}_0(k)$, for an algebraically closed field k.

One lets $\underline{\mathrm{End}}_A$ (or End $\mathcal{P}(A)$) be the category of endomorphisms of projective A-modules of finite rank. The objects are pairs (E, f) where E is a finite, projective A-module and $f \in \mathrm{End}_A(E)$. The morphisms in this category are required to commute with the endomorphisms f. The following operations of direct sum and tensor product,

$$(E_1, f_1) \oplus (E_2, f_2) = (E_1 \oplus E_2, f_1 \oplus f_2),$$
$$(E_1, f_1) \otimes (E_2, f_2) = (E_1 \otimes E_2, f_1 \otimes f_2),$$

turn the Grothendieck group $K_0(\underline{\mathrm{End}}_A)$ into a (commutative) ring. The pairs of the form $(E, f = 0)$ generate the ideal $K_0(A) \subset K_0(\underline{\mathrm{End}}_A)$. We denote the quotient ring, $\mathbb{W}_0(A)$, by

$$\mathbb{W}_0(A) = K_0(\underline{\mathrm{End}}_A)/K_0(A).$$

By construction, $\mathbb{W}_0$ is an endofunctor of the category $\mathfrak{Ring}$ of commutative rings with unit. Several key operators and maps act on $\mathbb{W}_0$, the following are the most relevant ones for our applications:

(1) The Teichmüller lift $\tau\colon A \to \mathbb{W}_0(A)$ which is a multiplicative map.

(2) For $n \in \mathbb{N}$, the Frobenius ring endomorphisms $F_n\colon \mathbb{W}_0(A) \to \mathbb{W}_0(A)$.

(3) For $n \in \mathbb{N}$, the Verschiebung (= shift), additive functorial maps $V_n\colon \mathbb{W}_0(A) \to \mathbb{W}_0(A)$.

(4) For $n \in \mathbb{N}$, the n-th ghost component homomorphisms $\mathrm{gh}_n\colon \mathbb{W}_0(A) \to A$.

We briefly recall their definitions.

(1) The Teichmüller lift $\tau = [\,\cdot\,]\colon A \to \mathbb{W}_0(A)$ is defined by $f \mapsto \tau(f) = [f] = (A, f)$.

(2) For $n \in \mathbb{N}$, the operations in $\underline{\mathrm{End}}_A$ of raising an endomorphism f to the n-th power induce the Frobenius ring endomorphims in $\mathbb{W}_0(A)$:

$$F_n\colon \mathbb{W}_0(A) \to \mathbb{W}_0(A), \quad F_n(E, f) = (E, f^n). \tag{2}$$

(3) For $n \in \mathbb{N}$, the Verschiebung maps are defined by the following operations on matrices:

$$V_n \colon \mathbb{W}_0(A) \to \mathbb{W}_0(A), \quad V_n(E,f) = \left(E^{\oplus n}, \begin{bmatrix} 0 & 0 & \dots & \dots & f \\ 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}\right). \tag{3}$$

(4) For $n \in \mathbb{N}$, the ghost components are given by

$$\mathrm{gh}_n \colon \mathbb{W}_0(A) \to A, \quad \mathrm{gh}_n(E,f) = \mathrm{Trace}(f^n).$$

Let $\Lambda(A) := 1 + tA[[t]]$ be the multiplicative abelian group of formal power series with constant term 1. The (inverse of the) characteristic polynomial defines a homomorphism of abelian groups

$$L \colon \mathbb{W}_0(A) \to \Lambda(A), \quad L(E,f) = \det(1 - tM(f))^{-1}, \tag{4}$$

where $M(f) = (a_{ij})$ is a matrix associated to $f \colon E \to E$ (i.e., $f \longleftrightarrow \sum_i x_i^* \otimes x_i$, $x_i^* \in E^*$, $x_i \in E$, $a_{ij} = \langle x_i^*, x_j \rangle$). By a fundamental result of G. Almkvist ([1], Theorem 6.4, or [2], Main Theorem), one has

Theorem 2.1. *The map L is injective and its image is the subgroup*

$$\mathrm{Range}(L) = \{(1 + a_1 t + \cdots + a_n t^n)/(1 + b_1 t + \cdots + b_n t^n) \mid a_j, b_j \in A\}$$

of $\Lambda(A)$.

Note in particular that for E a finite, projective A-module and $f, g \in \mathrm{End}_A(E)$ one has

$$(E, fg) = (E, gf) \in \mathbb{W}_0(A). \tag{5}$$

One also has

$$V_{nm} = V_n \circ V_m = V_m \circ V_n, \quad F_{nm} = F_n \circ F_m = F_m \circ F_n. \tag{6}$$

The following proposition collects together several standard equations connecting these operators

Proposition 2.2. *Let A be a commutative ring and $x, y \in \mathbb{W}_0(A)$. The following hold:*

(1) $F_n \circ V_n(x) = nx$.

(2) $V_n(F_n(x)y) = xV_n(y)$.

(3) *If* $(m,n) = 1$, *then* $V_m \circ F_n = F_n \circ V_m$.

(4) *For* $n \in \mathbb{N}$, $V_n(x)V_n(y) = nV_n(xy)$.

(5) *For* $n \in \mathbb{N}$, $F_n(\tau(f)) = \tau(f^n)$.

(6) *For* $n, m \in \mathbb{N}$, $\mathrm{gh}_n(F_m(f)) = \mathrm{gh}_{nm}(f)$.

(7) $\mathrm{gh}_n(V_m(f)) = \begin{cases} m\,\mathrm{gh}_{n/m}(f) & \text{if } m \mid n, \\ 0 & \text{otherwise.} \end{cases}$

Proof. All proofs are straightforward, we just check (4) as an example. For $x \in \mathrm{End}_A(E)$, the action of $X = V_n(E, x)$ on vectors $\xi = (\xi_1, \ldots, \xi_n) \in E^{\oplus n}$ is given by

$$(X\xi)_1 = x\xi_n, \quad (X\xi)_j = \xi_{j-1} \quad \text{for all } j \text{ with } 2 \le j \le n.$$

Similar formulas hold for $Y = V_n(F, y)$ with $y \in \mathrm{End}_A(F)$. By definition, $V_n(x)V_n(y)$ corresponds to $X \otimes Y \in \mathrm{End}_A(E^{\oplus n} \otimes F^{\oplus n})$. This endomorphism decomposes into the direct sum of n endomorphisms of $(E \otimes F)^{\oplus n}$, each of these is of the form

$$\begin{bmatrix} 0 & 0 & \ldots & \ldots & x \otimes 1 \\ 1 & 0 & 0 & \ldots & 0 \\ 0 & 1 \otimes y & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} 0 & 0 & \ldots & \ldots & x \otimes y \\ 1 & 0 & 0 & \ldots & 0 \\ 0 & 1 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

By applying (5), one checks that each of the above endomorphisms is equivalent to $V_n(x \otimes y)$. The equality $V_n(x)V_n(y) = nV_n(xy)$ follows. □

We shall apply the following proposition to the case $A = k = \bar{\mathbb{F}}_p$ an algebraic closure of $\mathbb{F}_p$.

Proposition 2.3. *Let k be an algebraically closed field. Then the map which associates to $(E, f) \in \underline{\mathrm{End}}_k$ the divisor $\delta(f)$ of non-zero eigenvalues of f (with multiplicity taken into account) extends to a ring isomorphism*

$$\delta\colon \mathbb{W}_0(k) \xrightarrow{\sim} \mathbb{Z}[k^\times]. \tag{7}$$

Under the above isomorphism, the Frobenius F_n on $\mathbb{W}_0(k)$ is given on $\mathbb{Z}[k^\times]$ by the natural linearization of the group endomorphism $k^\times \to k^\times$, $g \mapsto g^n$.

Proof. By applying Theorem 2.1, the characteristic polynomial extends to a complete invariant on $K_0(\underline{\mathrm{End}}_k)$ and to an isomorphism of $K_0(\underline{\mathrm{End}}_k)$ with the ring of quotients of monic polynomials in $k[t]$. Moding out this ring by $K_0(k)$ means that one removes the powers of the variable. Thus the divisor of non-zero eigenvalues of f extends to define a bijection of sets $\mathbb{W}_0(k) \simeq \mathbb{Z}[k^\times]$.

It remains to check that this bijection preserves the ring operations. For addition, the set underlying the divisor $\delta(f_1 + f_2)$ is the disjoint union of the two sets of roots of f_j and hence $\delta(f_1 + f_2) = \delta(f_1) + \delta(f_2)$. For the product, it is enough and easy to check that the tensor product of two rank one elements $(k, a) \otimes (k, b)$ is given by (k, ab) for non-zero elements of k. The statement about F_n is checked in the same way using (2) on elements (k, a). □

Recall the following formula for $L(f)$ in terms of the divisor $\delta(f) = \sum n(\alpha)[\alpha] \in \mathbb{Z}[k^\times]$:

$$L(f) = \prod (1 - \alpha\, t)^{-n(\alpha)}. \tag{8}$$

Corollary 2.4. *For any given isomorphism* $\sigma\colon \bar{\mathbb{F}}_p^\times \xrightarrow{\sim} (\mathbb{Q}/\mathbb{Z})^{(p)}$ *of the multiplicative group of the algebraic closure* $\bar{\mathbb{F}}_p$ *with the subgroup* $(\mathbb{Q}/\mathbb{Z})^{(p)} \subset \mathbb{Q}/\mathbb{Z}$ *of fractions with denominator prime to* p*, one derives an isomorphism*

$$\tilde{\sigma}\colon \mathbb{W}_0(\bar{\mathbb{F}}_p) \xrightarrow{\sim} \mathbb{Z}[(\mathbb{Q}/\mathbb{Z})^{(p)}].$$

Under the isomorphism $\tilde{\sigma}$*, the Frobenius* F_n *of* $\mathbb{W}_0(\bar{\mathbb{F}}_p)$ *is given on* $\mathbb{Z}[(\mathbb{Q}/\mathbb{Z})^{(p)}]$ *by the natural linearization of the group endomorphism* $(\mathbb{Q}/\mathbb{Z})^{(p)} \to (\mathbb{Q}/\mathbb{Z})^{(p)}$*,* $g \mapsto g^n$ *(i.e.,* $\gamma \mapsto n\gamma$ *in additive notation).*

3. The integral BC-system

For each $n \in \mathbb{N}$, one defines group ring endomorphisms

$$\sigma_n\colon \mathbb{Z}[\mathbb{Q}/\mathbb{Z}] \to \mathbb{Z}[\mathbb{Q}/\mathbb{Z}], \quad \sigma_n(e(\gamma)) = e(n\gamma),$$

and additive maps

$$\tilde{\rho}_n\colon \mathbb{Z}[\mathbb{Q}/\mathbb{Z}] \to \mathbb{Z}[\mathbb{Q}/\mathbb{Z}], \quad \tilde{\rho}_n(e(\gamma)) = \sum_{n\gamma'=\gamma} e(\gamma'). \tag{9}$$

We recall from [16], Proposition 4.4, the following result.

Proposition 3.1. *The endomorphisms* σ_n *and the maps* $\tilde{\rho}_m$ *fulfill the relations*

$$\sigma_{nm} = \sigma_n\sigma_m, \quad \tilde{\rho}_{mn} = \tilde{\rho}_m\tilde{\rho}_n \quad \textit{for all } m, n \in \mathbb{N}, \tag{10}$$

$$\tilde{\rho}_m(\sigma_m(x)y) = x\tilde{\rho}_m(y) \quad \textit{for all } x, y \in \mathbb{Z}[\mathbb{Q}/\mathbb{Z}], \tag{11}$$

and

$$\sigma_c(\tilde{\rho}_b(x)) = (b,c)\,\tilde{\rho}_{b'}(\sigma_{c'}(x)), \quad b' = b/(b,c), \quad c' = c/(b,c), \tag{12}$$

where $(b,c) = \gcd(b,c)$*.*

Note that taking $b = c = n$ in (12) gives

$$\sigma_n(\tilde{\rho}_n(x)) = nx \quad \text{for all } x \in \mathbb{Z}[\mathbb{Q}/\mathbb{Z}]. \tag{13}$$

On the contrary, if we take $b = n$ and $c = m$ to be relatively prime we get

$$\sigma_n \circ \tilde{\rho}_m = \tilde{\rho}_m \circ \sigma_n. \tag{14}$$

We recall from [16] (Definition 4.7 and §4.2) the following facts. The integral BC-algebra is the algebra $\mathcal{H}_{\mathbb{Z}} = \mathbb{Z}[\mathbb{Q}/\mathbb{Z}] \rtimes_{\tilde{\rho}} \mathbb{N}$ generated by the group ring $\mathbb{Z}[\mathbb{Q}/\mathbb{Z}]$ and by the elements $\tilde{\mu}_n$ and μ_n^*, with $n \in \mathbb{N}$, which satisfy the relations

$$\begin{aligned} \tilde{\mu}_n x \mu_n^* &= \tilde{\rho}_n(x), \\ \mu_n^* x &= \sigma_n(x)\mu_n^*, \\ x\tilde{\mu}_n &= \tilde{\mu}_n \sigma_n(x), \end{aligned} \tag{15}$$

where $\tilde{\rho}_m$, $m \in \mathbb{N}$, is defined in (9), as well as the relations

$$\begin{aligned} \tilde{\mu}_{nm} &= \tilde{\mu}_n\tilde{\mu}_m \quad \text{for all } n, m \in \mathbb{N}, \\ \mu_{nm}^* &= \mu_n^*\mu_m^* \quad \text{for all } n, m, \\ \mu_n^*\tilde{\mu}_n &= n, \\ \tilde{\mu}_n\mu_m^* &= \mu_m^*\tilde{\mu}_n, \quad (n,m) = 1. \end{aligned} \tag{16}$$

After tensoring by $\mathbb{Q}$, the Hecke algebra $\mathcal{H}_{\mathbb{Q}} = \mathcal{H}_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q}$ has a simpler explicit presentation with generators μ_n $(= \frac{1}{n}\tilde{\mu}_n)$, μ_n^*, $n \in \mathbb{N}$, and $e(r)$, for $r \in \mathbb{Q}/\mathbb{Z}$, satisfying the relations

- $\mu_n^*\mu_n = 1$ for all $n \in \mathbb{N}$,
- $\mu_m\mu_n = \mu_{mn}$, $\mu_m^*\mu_n^* = \mu_{mn}^*$ for all $m, n \in \mathbb{N}$,
- $\mu_n\mu_m^* = \mu_m^*\mu_n$ if $(n,m) = 1$,
- $e(0) = 1$, $e(r)^* = e(-r)$ and $e(r)e(s) = e(r+s)$ for all $r, s \in \mathbb{Q}/\mathbb{Z}$,
- for all $n \in \mathbb{N}$ and all $r \in \mathbb{Q}/\mathbb{Z}$,

$$\mu_n\, e(r)\, \mu_n^* = \frac{1}{n}\sum_{ns=r} e(s).$$

After tensoring by $\mathbb{C}$ and completion one gets a C*-algebra with a natural time evolution σ_t ([4], [18], Chapter III). The extremal KMS states below critical temperature vanish on the monomials $\mu_n x \mu_m^*$ for $n \neq m$ and $x \in \mathbb{Q}[\mathbb{Q}/\mathbb{Z}]$, and their value on $\mathbb{Q}[\mathbb{Q}/\mathbb{Z}]$ is given by

$$\varphi_{\beta,\rho}(e(a/b)) = \frac{1}{\zeta(\beta)}\sum_{n=1}^{\infty} n^{-\beta}\rho(\zeta_{a/b}^n), \tag{17}$$

where $\rho \in \hat{\mathbb{Z}}^*$ determines an embedding in $\mathbb{C}$ of the cyclotomic field $\mathbb{Q}^{\text{cyc}}$ generated by the abstract roots of unity.

4. $\mathbb{W}_0(\bar{\mathbb{F}}_p)$ and the BC-system

In [30] Quillen makes use of the choice of an embedding

$$\sigma : \bar{\mathbb{F}}_p^\times \to \mathbb{C}^\times$$

in the study of the algebraic K-theory of the general linear group over a finite field. In this section we compare the description of the universal Witt ring $\mathbb{W}_0(\bar{\mathbb{F}}_p)$, endowed with the structure given by the Frobenius endomorphisms F_n and the Verschiebung maps V_n with the integral BC-algebra $\mathcal{H}_{\mathbb{Z}}$.

By a simple comparison process we notice that the relations (10), (11), (12) holding on $\mathcal{H}_{\mathbb{Z}}$ are the same as those fulfilled by the Frobenius endomorphisms F_n and the Verschiebung maps V_n on $\mathbb{W}_0(\bar{\mathbb{F}}_p)$. More precisely, under the correspondences $\sigma_n \to F_n$, $\tilde{\rho}_n \to V_n$ the two relations of (6) correspond to (10), and the first three relations of Proposition 2.2 correspond respectively to (13), (11) and (14). These results evidently point out to the existence of a strong relation between the (λ)-ring $\mathbb{W}_0(\bar{\mathbb{F}}_p)$ and the group ring $\mathbb{Z}[\mathbb{Q}/\mathbb{Z}]$ endowed with the aforementioned operators.

Next, we compare the two groups rings: $\mathbb{Z}[(\mathbb{Q}/\mathbb{Z})^{(p)}]$ and $\mathbb{Z}[\mathbb{Q}/\mathbb{Z}]$ which arise in the description of $\mathbb{W}_0(\bar{\mathbb{F}}_p)$ and in the construction of the BC-algebra respectively. One has a surjective group homomorphism: $\mathbb{Q}/\mathbb{Z} \to (\mathbb{Q}/\mathbb{Z})^{(p)}$ induced by the canonical factorization of the groups

$$\mathbb{Q}/\mathbb{Z} = (\mathbb{Q}/\mathbb{Z})^{(p)} \times \mu_{p^\infty}, \tag{18}$$

where μ_{p^∞} is the group of fractions whose denominator is a power of p. Thus one obtains a corresponding factorization of the rings

$$\mathbb{Z}[\mathbb{Q}/\mathbb{Z}] = \mathbb{Z}[(\mathbb{Q}/\mathbb{Z})^{(p)}] \otimes_{\mathbb{Z}} \mathbb{Z}[\mu_{p^\infty}].$$

By using the trivial representation of μ_{p^∞} (i.e., the augmentation ϵ of $\mathbb{Z}[\mu_{p^\infty}]$), one gets a retraction $r = \mathrm{id} \otimes \epsilon$ producing the splitting

$$\mathbb{Z}[(\mathbb{Q}/\mathbb{Z})^{(p)}] \xrightarrow{j_p} \mathbb{Z}[\mathbb{Q}/\mathbb{Z}] \xrightarrow{\mathrm{id}\otimes\epsilon} \mathbb{Z}[(\mathbb{Q}/\mathbb{Z})^{(p)}]. \tag{19}$$

Notice that $(\mathbb{Q}/\mathbb{Z})^{(p)}$ is preserved by the action of the map $\gamma \mapsto n\gamma$, $\gamma \in (\mathbb{Q}/\mathbb{Z})^{(p)})$. This implies that the endomorphisms σ_n acting on the BC-algebra restrict naturally to determine endomorphisms $\sigma_n : \mathbb{Z}[(\mathbb{Q}/\mathbb{Z})^{(p)}] \to \mathbb{Z}[(\mathbb{Q}/\mathbb{Z})^{(p)}]$.

Let us denote by $I(p) \subset \mathbb{N}$ the set of integers which are prime to p. The following lemma describes the projection of the operators $\tilde{\rho}_n$ of the BC-algebra on the group ring $\mathbb{Z}[(\mathbb{Q}/\mathbb{Z})^{(p)}]$

Proposition 4.1. *Let $n = p^k m$ with $m \in I(p)$. For $\gamma \in \mathbb{Q}/\mathbb{Z}$, we write modulo* 1

$$\gamma = \frac{a}{b} + \frac{c}{p^s}, \quad b \in I(p),\ a, b, c, s \in \mathbb{N}. \tag{20}$$

Then, with $\tilde{\rho}_n$ as in (9)*, we have*

$$r \circ \tilde{\rho}_n(e(\gamma)) = p^k \sum_{w=0}^{m-1} e\left(\frac{f + wb}{bm}\right), \tag{21}$$

where $y = \frac{f}{bm}$*,* $f \in \mathbb{Z}/bm\mathbb{Z}$*, is the unique solution in* $\mathbb{Q}/\mathbb{Z}$ *with denominator prime to* p *of the equation*

$$p^k y = \frac{a}{bm} \in \mathbb{Q}/\mathbb{Z}. \tag{22}$$

Proof. The existence and uniqueness of the decomposition (20) derives from the factorization (18). For $d \in I(p)$, the endomorphism of $\mathbb{Q}/\mathbb{Z}$: $x \mapsto px$ restricts to an automorphism on the subgroup $G_d = \{\frac{a}{d} \in \mathbb{Q}/\mathbb{Z} \mid a \in \mathbb{Z}\} \subset \mathbb{Q}/\mathbb{Z}$. For $d = bm$, this fact shows the existence and uniqueness of the solution $y = \frac{f}{bm}$ of (22). One has $p^k y = \frac{a}{bm} + j$ for some integer $j \in \mathbb{Z}$, thus

$$y = \frac{a}{bmp^k} + \frac{j}{p^k} = \frac{a}{bn} + \frac{j}{p^k}, \qquad ny = \frac{a}{b} + jm.$$

By applying (18), one also has a decomposition of the form

$$\frac{c}{np^s} = \frac{c}{mp^{s+k}} = \frac{d}{m} + \frac{e}{p^{s+k}}. \tag{23}$$

One has $ny = \frac{a}{b}$ modulo 1, $n\frac{c}{np^s} = \frac{c}{p^s}$, thus the solutions of the equation $n\gamma' = \gamma$ in $\mathbb{Q}/\mathbb{Z}$ which enter in (9) are of the form

$$\gamma' = y + \frac{c}{np^s} + \frac{u}{m} + \frac{v}{p^k}, \qquad u \in \{0, \dots, m-1\},\ v \in \{0, \dots, p^k - 1\}.$$

By using (23) one derives

$$\gamma' = y + \frac{u}{m} + \frac{d}{m} + \frac{v}{p^k} + \frac{e}{p^{s+k}}, \qquad u \in \{0, \dots, m-1\},\ v \in \{0, \dots, p^k - 1\}.$$

For the projection $r(e(\gamma')) \in \mathbb{Z}[(\mathbb{Q}/\mathbb{Z})^{(p)}]$ one thus gets that

$$r(e(\gamma')) = e\left(y + \frac{w}{m}\right) = e\left(\frac{f + wb}{bm}\right), \qquad w \in \{0, \dots, m-1\},$$

which is repeated with multiplicity p^k. Equation (21) follows. □

Corollary 4.2. *One has*

$$r \circ \tilde{\rho}_n(x) = r \circ \tilde{\rho}_n(r(x)) \quad \textit{for all } x \in \mathbb{Z}[\mathbb{Q}/\mathbb{Z}],\ n \in \mathbb{N}, \tag{24}$$

and

$$r \circ \tilde{\rho}_{p^k}(x) = p^k \sigma_{p^k}^{-1}(r(x)) \quad \textit{for all } x \in \mathbb{Z}[\mathbb{Q}/\mathbb{Z}],\ k \in \mathbb{N}.$$

Proof. The two statements follow from (21). □

Definition 4.3. For p a prime number, we denote by X_p the space of all injective group homomorphisms $\sigma : \bar{\mathbb{F}}_p^\times \to \mathbb{Q}/\mathbb{Z}$.

The relation between $\mathbb{W}_0(\bar{\mathbb{F}}_p)$ and the abelian part $\mathbb{Z}[\mathbb{Q}/\mathbb{Z}]$ of the integral BC-algebra $\mathcal{H}_{\mathbb{Z}}$ is described by the following lemma

Proposition 4.4. *Let $\sigma \in X_p$ and let $\tilde{\sigma}$ be the associated ring isomorphism*

$$\tilde{\sigma} : \mathbb{W}_0(\bar{\mathbb{F}}_p) \xrightarrow{\sim} \mathbb{Z}[(\mathbb{Q}/\mathbb{Z})^{(p)}] \subset \mathbb{Z}[\mathbb{Q}/\mathbb{Z}].$$

Then the Frobenius F_n and Verschiebung maps V_n on $\mathbb{W}_0(\bar{\mathbb{F}}_p)$ are obtained by restriction of the ring endomorphisms σ_n and the maps $\tilde{\rho}_n$ on $\mathbb{Z}[\mathbb{Q}/\mathbb{Z}]$ by the formulas

$$\tilde{\sigma} \circ F_n = \sigma_n \circ \tilde{\sigma}, \quad \tilde{\sigma} \circ V_n = r \circ \tilde{\rho}_n \circ \tilde{\sigma}. \tag{25}$$

Proof. In Section 2 we recalled (cf. [20] for details) that the Frobenius F_n on $\mathbb{W}_0(A)$ is given by $F_n(E, f) = (E, f^n)$. At the level of the divisor of the eigenvalues of f (it is a divisor in the virtual case), i.e., at the level of the associated element in $\mathbb{Z}[k^\times]$, $A = k = \bar{\mathbb{F}}_p$, the Frobenius F_n corresponds to the group homomorphism $g \mapsto g^n$ (cf. Proposition 2.3). The Verschiebung maps V_n are described by the operation (3) on matrices. The maps V_n are additive and hence determined by the elements $V_n([\alpha])$ where $\alpha \in k^\times$. They correspond to the n eigenvalues of the following matrix

$$V_n(\alpha) = \begin{bmatrix} 0 & 0 & \dots & \dots & \alpha \\ 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

Since the n-th power of the above matrix is the multiplication by α, all its eigenvalues fulfill the equation $\beta^n = \alpha$. In fact the characteristic polynomial of the above matrix is $P(X) = X^n - \alpha$. Let $n = p^k m$, where m is prime to p. Since $\bar{\mathbb{F}}_p$ is a perfect field, the root $\alpha^{p^{-k}} \in \bar{\mathbb{F}}_p$ of $X^{p^k} - \alpha$ is unique and it admits m distinct roots of order m: $\beta^m = \alpha^{p^{-k}}$, which are the m roots of $P(X)$. They take the form $\xi\beta_0$, with $\xi^m = 1$. Thus the corresponding divisor is

$$\delta = \sum_{\xi^m=1} p^k[\xi\beta_0].$$

We now compare the above description of the divisor associated to $V_n(E, f)$ with $r \circ \tilde{\rho}_n(e(\gamma))$, where $\gamma = \sigma(\alpha) = \frac{a}{b} \in (\mathbb{Q}/\mathbb{Z})^{(p)} \subset \mathbb{Q}/\mathbb{Z}$. The elements $\xi\beta_0 \in \bar{\mathbb{F}}_p$ are the m distinct roots of the equation $X^n = \alpha$. Similarly, with the notations of (21), the elements

$$\frac{f + wb}{bm} \in (\mathbb{Q}/\mathbb{Z})^{(p)} \subset \mathbb{Q}/\mathbb{Z}, \quad w \in \{0, \dots, m-1\},$$

are the m solutions in $(\mathbb{Q}/\mathbb{Z})^{(p)}$ of the equation $nz = \gamma$. One thus gets

$$\tilde{\sigma}(\delta) = p^k \sum_{w=0}^{m-1} e\left(\frac{f + wb}{bm}\right).$$

Thus (21) shows that

$$\tilde{\sigma}(V_n([\alpha])) = \tilde{\sigma}(\delta) = r \circ \tilde{\rho}_n(e(\gamma)) = r \circ \tilde{\rho}_n \circ \tilde{\sigma}([\alpha]). \qquad \square$$

Theorem 4.5. *Let $\sigma \in X_p$. The following formulas define a representation π_σ of the integral BC-system $\mathcal{H}_{\mathbb{Z}}$ as additive endomorphisms of $\mathbb{W}_0(\bar{\mathbb{F}}_p)$:*

$$\pi_\sigma(x)\xi = \tilde{\sigma}^{-1}(r(x))\,\xi, \quad \pi_\sigma(\mu_n^*) = F_n, \quad \pi_\sigma(\tilde{\mu}_n) = V_n \tag{26}$$

for all $\xi \in \mathbb{W}_0(\bar{\mathbb{F}}_p)$, $x \in \mathbb{Z}[\mathbb{Q}/\mathbb{Z}]$ and $n \in \mathbb{N}$.

Proof. By construction $x \mapsto \tilde{\sigma}^{-1}(r(x))$ is a homomorphism of the group ring $\mathbb{Z}[\mathbb{Q}/\mathbb{Z}]$ to $\mathbb{W}_0(\bar{\mathbb{F}}_p)$ and hence, by composition with the left regular representation, π_σ gives a representation of $\mathbb{Z}[\mathbb{Q}/\mathbb{Z}]$. The F_n and V_n are additive. It remains to check the relations (15) and (16). The latter ones follow from (6) for the first two, and from (1) and (3) of Proposition 2.2 for the last two. To check the first relation of (15) one needs to show that

$$V_n \pi_\sigma(x) F_n = \pi_\sigma(\tilde{\rho}_n(x)). \tag{27}$$

One has $\pi_\sigma(x) = \pi_\sigma(r(x))$ for all $x \in \mathbb{Z}[\mathbb{Q}/\mathbb{Z}]$. Thus, by applying (24), one can replace x by $r(x)$ without changing both sides of the equation. Thus we can assume that $x = \tilde{\sigma}(z)$ for some $z \in \mathbb{W}_0(\bar{\mathbb{F}}_p)$. Then $\pi_\sigma(x)$ is just the multiplication by z. By (25) one has

$$r \circ \tilde{\rho}_n(x) = r \circ \tilde{\rho}_n(\tilde{\sigma}(z)) = \tilde{\sigma} \circ V_n(z).$$

Thus $\pi_\sigma(\tilde{\rho}_n(x))$ is the multiplication by $V_n(z)$ and (27) follows from

$$V_n(zF_n(\xi)) = V_n(z)\xi \quad \text{for all } \xi \in \mathbb{W}_0(\bar{\mathbb{F}}_p),$$

which is statement (2) of Proposition 2.2. Let us check the other two relations of (15). The second one means

$$F_n \pi_\sigma(x) = \pi_\sigma(\sigma_n(x)) F_n,$$

and since $r \circ \sigma_n = \sigma_n \circ r$, we can assume as before that $x = \tilde{\sigma}(z)$ for some $z \in \mathbb{W}_0(\bar{\mathbb{F}}_p)$. Then $\pi_\sigma(x)$ is the multiplication by z and, by (25), $\pi_\sigma(\sigma_n(x))$ is the multiplication by $F_n(z)$. The required equality then follows since F_n is multiplicative. The last relation of (15) means

$$\pi_\sigma(x) V_n = V_n \pi_\sigma(\sigma_n(x)),$$

and assuming $x = \tilde{\sigma}(z)$ it reduces to

$$zV_n(\xi) = V_n(F_n(z)\xi) \quad \text{for all } \xi \in \mathbb{W}_0(\bar{\mathbb{F}}_p),$$

which in turn follows from statement (2) of Proposition 2.2. □

5. The Witt vectors functor and the truncation quotients

In this section we provide a short overview on the construction of the universal Witt scheme in the form that is most suitable to the applications contained in this paper, for more details we refer to [40], [29], [7], [24], [3], [34], [25]. In the second part of the section we connect the universal ring $\mathbb{W}_0(A)$ with $\mathbb{W}(A)$.

The construction of the ring of big Witt vectors (or generalized Witt vectors) is described by a covariant endofunctor $\mathbb{W}\colon \mathfrak{Ring} \to \mathfrak{Ring}$ in the category of commutative rings (with unit). For $A \in \mathrm{obj}(\mathfrak{Ring})$, and as a functor to the category of sets, one defines

$$\mathbb{W}(A) = A^{\mathbb{N}} = \{(x_1, x_2, x_3, \dots) \mid x_i \in A\}.$$

To a truncation set $N \subseteq \mathbb{N}$ (i.e., a subset of $\mathbb{N}$ which contains every positive divisor of each of its elements), one associates the truncated functor

$$\mathbb{W}_N\colon \mathfrak{Ring} \to \mathfrak{Sets}, \quad \mathbb{W}_N(A) = A^N.$$

As a functor to the category of sets, $\mathbb{W}_N$ is left represented by the polynomial ring $R_N = \mathbb{Z}[x_n | n \in N]$. Then it follows that the big Witt vectors functor $\mathbb{W} = \mathbb{W}_{\mathbb{N}}$ is left represented by the symmetric algebra $\mathrm{Symm} = \mathbb{Z}[x_1, x_2, x_3, \dots]$

$$\mathbb{W}(A) = \mathrm{Hom}_{\mathfrak{Ring}}(\mathrm{Symm}, A) \quad \text{for all } A \in \mathrm{obj}(\mathfrak{Ring}). \tag{28}$$

As an endofunctor in the category of commutative rings, $\mathbb{W}_N\colon \mathfrak{Ring} \to \mathfrak{Ring}$ is *uniquely* determined by requiring that for any commutative ring A and for any $n \in N$, the map

$$\mathrm{gh}_n\colon \mathbb{W}_N(A) \to A, \quad \mathrm{gh}_n(x) = \sum_{d|n} d x_d^{n/d},$$

called the n-th ghost component, is a ring homomorphism.

For t a variable, the functorial bijection of sets

$$\varphi_A\colon \mathbb{W}(A) \to \Lambda(A) = 1 + tA[[t]], \quad x = (x_n)_{n\in\mathbb{N}} \mapsto f_x(t) = \prod_{n\in\mathbb{N}} (1 - x_n t^n)^{-1}, \tag{29}$$

transports the ring structure from $\mathbb{W}(A)$ to the multiplicative abelian group $\Lambda(A)$ of power series over A with constant term 1, under the usual multiplication of power series (the power series 1 acts as the identity element). In other words, one has

$$\varphi_A(x + y) = \varphi_A(x)\varphi_A(y) \quad \text{for all } x, y \in \mathbb{W}(A).$$

To make the description of the corresponding product $\star$ on $\Lambda(A)$ more explicit, one introduces first the n-ghost components $w_n\colon \Lambda(A) \to A$, $n \in \mathbb{N}$, which are defined by the formula

$$w(f) = w(1 + a_1 t + a_2 t^2 + a_3 t^3 + \cdots) = w_1 t + w_2 t^2 + \cdots = t\tfrac{d}{dt}(\log(f(t))).$$

For example, the first three ghost components are given by the universal formulas

$$w_1(f) = a_1, \quad w_2(f) = -a_1^2 + 2a_2, \quad w_3(f) = a_1^3 - 3a_1a_2 + 3a_3.$$

For products of the form $\prod_{k=1}^m (1 - \xi_k t)^{-1} = 1 + a_1 t + a_2 t^2 + \cdots = f(t)$ this means that

$$\begin{aligned} w_1 t + w_2 t^2 + w_3 t^3 + \cdots &= t\tfrac{d}{dt}(\log(f(t))) \\ &= t\tfrac{d}{dt}\sum_{k=1}^m \log((1-\xi_k t)^{-1}) \\ &= \sum_{i=1}^\infty (\xi_1^i + \xi_2^i + \cdots + \xi_m^i) t^i \\ &= \sum_{i=1}^\infty p_i(\xi) t^i. \end{aligned}$$

Thus the ghost components are given by the power sums in the ξ_k's. Then the product $\star$ on $\Lambda(A)$ is *uniquely* determined by requiring that these ghost components are (functorial) ring homomorphisms. In fact, distributivity and functoriality together force the multiplication of power series in $\Lambda(A)$ to be expressed by the rule

$$f(t) = \prod_i (1-\xi_i t)^{-1},\ g(t) = \prod_i (1-\eta_i t)^{-1} \implies (f \star g)(t) = \prod_{i,j}(1 - \xi_i \eta_j t)^{-1}, \tag{30}$$

where

$$t\tfrac{d}{dt}(\log(\prod_{i,j}(1-\xi_i\eta_j t)^{-1})) = \sum_{n=1}^\infty p_n(\xi) p_n(\eta) t^n.$$

It follows that multiplication according to (30) translates into component-wise multiplication for the ghost components on $\Lambda(A)$. It is expressed by explicit polynomials with integral coefficients of the form

$$\begin{aligned} &(1 + \textstyle\sum a_n t^n) \star (1 + \sum b_n t^n) \\ &\quad = 1 + a_1 b_1 t + (a_1^2 b_1^2 - a_2 b_1^2 - a_1^2 b_2 + 2a_2 b_2) t^2 + (a_1^3 b_1^3 - 2a_1 a_2 b_1^3 + a_3 b_1^3 \\ &\qquad - 2a_1^3 b_1 b_2 + 5a_1 a_2 b_1 b_2 - 3a_3 b_1 b_2 + a_1^3 b_3 - 3a_1 a_2 b_3 + 3a_3 b_3) t^3 + \cdots . \end{aligned}$$

The ghost components $\mathrm{gh}_n(x)$ of a Witt vector $x = (x_1, x_2, x_3, \dots) \in \mathbb{W}(A)$ become the ghost components of $\varphi_A(x)$, i.e.,

$$\mathrm{gh}_n \colon \mathbb{W}(A) \to A, \quad \mathrm{gh}_n(x) = w_n(\varphi_A(x)).$$

It follows that the bijection $\varphi_A \colon \mathbb{W}(A) \to \Lambda(A)$ becomes a ring isomorphism.

Note moreover that the homomorphism of abelian groups $L \colon \mathbb{W}_0(A) \to \Lambda(A)$ of (4), preserves the product, i.e.,

$$L((E, f) \otimes (F, g)) = L((E, f)) \star L((F, g)),$$

so that it defines an injective ring homomorphism.

Two Witt vectors $x, y \in \mathbb{W}(A)$ are added and multiplied by means of universal polynomials with integer coefficients

$$\begin{aligned} x +_{\mathbb{W}} y &= (\mu_{S,1}(x,y), \mu_{S,2}(x,y), \dots), \\ x \times_{\mathbb{W}} y &= (\mu_{P,1}(x,y), \mu_{P,2}(x,y), \dots). \end{aligned}$$

The polynomials $\mu_{S,i}$, $\mu_{P,j}$ are recursively computed using the ghost components by the formulas

$$\begin{aligned} \mathrm{gh}_n(\mu_{S,1}(x,y), \mu_{S,2}(x,y), \dots) &= \mathrm{gh}_n(x) + \mathrm{gh}_n(y), \\ \mathrm{gh}_n(\mu_{P,1}(x,y), \mu_{P,2}(x,y), \dots) &= \mathrm{gh}_n(x)\,\mathrm{gh}_n(y). \end{aligned}$$

Notice that the polynomials $\mathrm{gh}_n(x)$ depend only on the x_d for d a divisor of n, hence the n-th addition and multiplication polynomials $\mu_{S,n}$, $\mu_{P,n}$ are polynomials that only involve the x_d and y_d with d a divisor of n. Thus, for a truncation set $N \subseteq \mathbb{N}$, the polynomial ring $R_N = \mathbb{Z}[x_n \mid n \in N]$ is a sub Hopf algebra and a sub co-ring object of Symm, this means that it defines a quotient functor, which coincides with $\mathbb{W}_N$. This result applies in particular to the truncation set $N = \{p^n \mid n \geq 0\}$, where p is a prime number. Thus the p-adic Witt vectors $\mathbb{W}_{p^\infty}(A)$ can be interpreted as a functorial quotient of the big Witt vectors (similarly one obtains $\mathbb{W}_{p^n}(A)$ as the p-adic Witt vectors of length $n+1$).

The Teichmüller representative is a multiplicative map which defines a section to the ghost map gh_1. If $N \subset \mathbb{N}$ is a truncation set, the Teichmüller representative is defined as

$$[\cdot]_N \colon A \to \mathbb{W}_N(A), \quad a \mapsto [a]_N = ([a]_N)_{n \in N}, \quad [a]_{N,n} = \begin{cases} a & \text{if } n = 1, \\ 0 & \text{if } n > 1. \end{cases}$$

One has $\mathrm{gh}_n([a]_N) = a^n$ for all $n \in N$.

On the functorial ring $\mathbb{W}(A)$ one can introduce several functorial operations which derive from (the large number of) ring endomorphisms of Symm and by applying the representability property (28). For instance, the Verschiebung, additive functorial endomorphisms on $\mathbb{W}$ and its quotients arise from the ring endomorphism

$$\mathbf{V}_n \colon \mathrm{Symm} \to \mathrm{Symm}, \quad x_i \mapsto \begin{cases} x_{i/n} & \text{if } i \text{ is divisible by } n, \\ 0 & \text{otherwise,} \end{cases}$$

which corresponds to the map $f(t) \mapsto f(t^n)$ in $\Lambda(A)$.

For $N \subset \mathbb{N}$ a truncation set, the shift is the additive map given by

$$V_n \colon \mathbb{W}_{N/n}(A) \to \mathbb{W}_N(A), \quad V_n((a_d \mid d \in N/n)) = (a'_m \mid m \in N),$$

where $a'_m = \begin{cases} a_d & \text{if } m = nd, \\ 0 & \text{otherwise,} \end{cases}$ and $N/n = \{d \in \mathbb{N} \mid nd \in N\}$. This means that the composite with the ghost components is given by

$$\mathrm{gh}_m V_n = \begin{cases} n\,\mathrm{gh}_{m/n} & \text{if } n \text{ divides } m, \\ 0 & \text{otherwise.} \end{cases}$$

The n-th Frobenius is the (unique) natural ring homomorphism

$$F_n \colon \mathbb{W}_N(A) \to \mathbb{W}_{N/n}(A)$$

which is defined on the ghost components by the formula $\mathrm{gh}_r F_n = \mathrm{gh}_{rn}$. Thus by definition the n-th Frobenius map makes the diagram

$$\begin{tikzcd}
\mathbb{W}_N(A) \arrow[r, "\mathrm{gh}"] \arrow[d, "F_n"'] & A^N \arrow[d, "F_n^{\mathrm{gh}}"] \\
\mathbb{W}_{N/n}(A) \arrow[r, "\mathrm{gh}"] & A^{N/n}
\end{tikzcd}$$

commute, where F_n^{gh} takes a sequence $(a_m \mid m \in N)$ to the sequence whose d-th component is a_{dn}. At the level of the components x_j of a Witt vector $x \in \mathbb{W}_N(A)$, the Frobenius F_n is given by polynomials with integral coefficients. For instance, the following are the first 5 components of $F_3(x)$:

$$\begin{aligned}
F_3(x)_1 &= x_1^3 + 3x_3, \\
F_3(x)_2 &= x_2^3 - 3x_1^3x_3 - 3x_3^2 + 3x_6, \\
F_3(x)_3 &= -3x_1^6x_3 - 9x_1^3x_3^2 - 8x_3^3 + 3x_9, \\
F_3(x)_4 &= -3x_1^9x_3 + 3x_1^3x_2^3x_3 - 18x_1^6x_3^2 + 3x_2^3x_3^2 - 36x_1^3x_3^3, \\
&\qquad - 24x_3^4 + x_4^3 - 3x_2^3x_6 + 9x_1^3x_3x_6 + 9x_3^2x_6 - 3x_6^2 + 3x_{12}, \\
F_3(x)_5 &= -3x_1^{12}x_3 - 18x_1^9x_3^2 - 54x_1^6x_3^3 - 81x_1^3x_3^4 - 48x_3^5 + x_5^3 + 3x_{15}.
\end{aligned}$$

Note that when p is a rational prime one has (cf. [31] Proposition 5.12)

$$F_p(x)_m \equiv x_m^p \pmod{pA}. \tag{31}$$

One also has (cf. [31], Proposition 5.9)

$$V_{nm} = V_n \circ V_m = V_m \circ V_n, \quad F_{nm} = F_n \circ F_m = F_m \circ F_n,$$

where for the maps F_n one assumes $nN \subset N$ and $mN \subset N$.

Proposition 2.2 extends without change (cf., e.g., [6], IX, Exercice 47, [31] Proposition 5.10).

Proposition 5.1. *Let $N \subset \mathbb{N}$ be a truncation set and $n \in N$ with $nN \subset N$. Let A be a commutative ring and $x, y \in \mathbb{W}_N(A)$. Then:*

(1) $F_n \circ V_n(x) = nx$.

(2) $V_n(F_n(x)y) = xV_n(y)$.

(3) *If m is prime to n, one has $V_m \circ F_n = F_n \circ V_m$.*

(4) $V_n(x)V_n(y) = nV_n(xy)$.

Proof. We refer to [31], Proposition 5.10. The statement (4) differs slightly from this reference, it can be checked directly using Proposition 2.2. It implies that when n is invertible in $\mathbb{W}_N(A)$, then $\frac{1}{n}V_n$ defines a ring endomorphism. □

It is important to see how the description of the universal ring $\mathbb{W}_0(A)$ fits with the definition of $\mathbb{W}(A)$. There is a canonical ring monomorphism $\mathbb{W}_0(A) \hookrightarrow \mathbb{W}(A)$, which is given as the composite of the injective ring homomorphism $L\colon \mathbb{W}_0(A) \to \Lambda(A)$ as in (4) and of the ring isomorphism $\varphi_A^{-1}\colon \Lambda(A) \xrightarrow{\sim} \mathbb{W}(A)$ (cf. (29)):

$$\mathbb{W}_0(A) \to \Lambda(A) \simeq \mathbb{W}(A), \quad (E, f) \mapsto \det(1 - tM(f))^{-1}. \tag{32}$$

This ring monomorphism has dense range when one endows $\mathbb{W}(A) \simeq \Lambda(A)$ with the topology of formal power series with coefficients in A, using the valuation on $\Lambda(A)$ (and the discrete topology on A). In the case $A = \bar{\mathbb{F}}_p$ the characteristic polynomial $\det(1 - tM(f)) = \det(1 - tf)$ factorizes as a product of terms $(1 - t\alpha_j)$ of degree one, where the $\alpha_j \in \bar{\mathbb{F}}_p$ are the eigenvalues of f (cf. (8)).

Lemma 5.2. *Let $[\cdot]\colon \bar{\mathbb{F}}_p \to \mathbb{W}(\bar{\mathbb{F}}_p)$, $x \mapsto \tau(x) := [x]$, be the Teichmüller lift, and let $\delta\colon \mathbb{W}_0(\bar{\mathbb{F}}_p) \to \mathbb{Z}[\bar{\mathbb{F}}_p^\times]$ be the isomorphism of (7). Then the canonical map (32) is given explicitly by*

$$j\colon \mathbb{W}_0(\bar{\mathbb{F}}_p) \to \mathbb{W}(\bar{\mathbb{F}}_p), \quad j \circ \delta^{-1}\colon \mathbb{Z}[\bar{\mathbb{F}}_p^\times] \ni \sum n_j\alpha_j \mapsto \sum n_j\tau(\alpha_j) \in \mathbb{W}(\bar{\mathbb{F}}_p).$$

This lemma together with Theorem 2.1 shows that the subring $\mathbb{W}_0(\bar{\mathbb{F}}_p) \subset \mathbb{W}(\bar{\mathbb{F}}_p)$ is just the group ring $\mathbb{Z}[\bar{\mathbb{F}}_p^\times]$ and is freely generated over $\mathbb{Z}$ by the Teichmüller lifts.

6. The p-adic representations π_σ of the BC-system

In this section we shall implement the results of [7], [34], [3] to describe the ring $\mathbb{W}(\bar{\mathbb{F}}_p)$, then using the embedding with dense image $\mathbb{W}_0(\bar{\mathbb{F}}_p) \hookrightarrow \mathbb{W}(\bar{\mathbb{F}}_p)$ we will extend the representation π_σ of $\mathcal{H}_\mathbb{Z}$ on $\mathbb{W}_0(\bar{\mathbb{F}}_p)$ (Theorem 4.5) to a representation of the integral BC-system on $\mathbb{W}(\bar{\mathbb{F}}_p)$. Such representation is the p-adic analogue of the irreducible complex representation (48).

We begin by recalling the definition of the isomorphism

$$\mathbb{W}(\bar{\mathbb{F}}_p) \simeq \mathbb{W}_{p^\infty}(\bar{\mathbb{F}}_p)^{I(p)},$$

where $I(p) \subset \mathbb{N}$ is the set of positive integers which are prime to p and p^∞ is the set of integer powers of p. At the conceptual level, this isomorphism is a special case of the general functorial isomorphism holding for any commutative ring A with unit ([3], Theorem 1):

$$\mathbb{W}(A) = \mathbb{W}_{I(p)}(\mathbb{W}_{p^\infty}(A)).$$

When A is an $\mathbb{F}_p$-algebra, every element of $I(p)$ is invertible in $B = \mathbb{W}_{p^\infty}(A)$, thus one derives a canonical isomorphism $\mathbb{W}_{I(p)}(B) \simeq B^{I(p)}$ which is defined in terms of the ghost components. Let $\mathbb{Z}_{(p)}$ be the ring $\mathbb{Z}$ localized at the prime ideal $p\mathbb{Z}$ so that every element of $I(p)$ is invertible in $\mathbb{Z}_{(p)}$. A central role, in the ring $\Lambda(\mathbb{Z}_{(p)})$, is played by the Artin–Hasse exponential, which is the power series

$$E_p(t) = \operatorname{hexp}(t) = \exp\left(t + \frac{t^p}{p} + \frac{t^{p^2}}{p^2} + \cdots\right) \in \Lambda(\mathbb{Z}_{(p)}).$$

The following properties are well known (cf. [3], [34]).

Proposition 6.1. (1) *$E_p(t)$ is an idempotent of $\Lambda(\mathbb{Z}_{(p)})$.*

(2) *For $n \in I(p)$, the series $E_p(n)(t) := \frac{1}{n} V_n(E_p)(t) \in \Lambda(\mathbb{Z}_{(p)})$ determine an idempotent. As n varies in $I(p)$, the $E_p(n)$ form a partition of unity by idempotents.*

(3) *For $n \notin p^{\mathbb{N}}$, $F_n(E_p)(t) = 1\ (= 0_\Lambda)$ and $F_{p^k}(E_p)(t) = E_p(t)$ for all $k \in \mathbb{N}$.*

To check (1) directly, one shows that there exists a unique sequence $(x_n)_{n\in\mathbb{N}} \in \mathbb{W}(\mathbb{Z}_{(p)})$ such that

- $x_1 = 1$,
- $x_{p^k} = 0$ for all $k > 0$,
- $F_m(x)_{p^k} = 0$ for all $m \in I(p)$ and $k \geq 0$.

This follows by noticing that the coefficient of x_{mp^k} in $F_m(x)_{p^k}$ is $m \in I(p)$ which is invertible in $\mathbb{Z}_{(p)}$, so that one determines the x_n inductively. One then checks that the ghost components of $(x_n)_{n\in\mathbb{N}} \in \mathbb{W}(\mathbb{Z}_{(p)})$ are the same as those of $E_p(t)$, i.e., $gh_n(x)$ is equal to 1 if $n \in p^{\mathbb{N}}$ and is zero otherwise.

Note that any $n \in I(p)$ is invertible in $\Lambda(\mathbb{Z}_{(p)})$. Division by n corresponds to the extraction of the n-th root of the power series $f(t) = 1 + g(t)$. Formally, this is given by the binomial formula

$$f^{\frac{1}{n}} = (1+g)^{\frac{1}{n}} = 1 + \frac{1}{n} g + \cdots + \frac{\frac{1}{n}(\frac{1}{n}-1)\dots(\frac{1}{n}-k+1)}{k!} g^k + \cdots.$$

The p-adic valuation of the rational coefficient of g^k is positive because $\frac{1}{n} \in \mathbb{Z}_p$, thus this coefficient can be approximated arbitrarily by a binomial coefficient. It follows from Proposition 2.2 (4) that $\frac{1}{n} V_n$ is an endomorphism of $\Lambda(\overline{\mathbb{F}}_p)$ and also a right inverse of F_n.

One easily derives from [7], [3], [34] the following result.

Proposition 6.2. *Let A be an $\mathbb{F}_p$-algebra.*

(a) *The map*

$$\psi_A\colon \mathbb{W}_{p^\infty}(A) \to \Lambda(A)_{E_p}, \quad \psi_A(x)(t) := h_x(t) = \prod_{\mathbb{N}} E_p(x_{p^n} t^{p^n}),\ x = (x_{p^n})_{n\in\mathbb{N}},$$

is an isomorphism onto the reduced ring $\Lambda(A)_{E_p} = \{x \in \Lambda(A) \mid x \star E_p = x\}$.

(b) *For $n \in I(p)$, the composite $\psi_A^{-1} \circ F_n$ is an isomorphism of the reduced algebra $\Lambda(A)_{E_p(n)}$ with $\mathbb{W}_{p^\infty}(A)$.*

(c) *The composite*

$$\theta_A(x) = (\theta_A(x))_n = \psi_A^{-1} \circ F_n(x \star E_p(n)), \quad n \in I(p),\ x \in \Lambda(A), \tag{33}$$

is a canonical isomorphism $\theta_A\colon \Lambda(A) \to \mathbb{W}_{p^\infty}(A)^{I(p)} = \mathbb{W}(A)$.

(d) *The composite isomorphism $\Theta_A := \theta_A \circ \varphi_A\colon \mathbb{W}(A) \to \mathbb{W}_{p^\infty}(A)^{I(p)}$ is given explicitly on the components by*

$$(\Theta_A(x)_n)_{p^k} = F_n(x)_{p^k} \quad \textit{for all } x \in \mathbb{W}(A) \textit{ and } n \in I(p). \tag{34}$$

Proof. The first three statements follow from [7], §3.b, [3], Thm. 1 and Prop. 1, [34], Thm. 9.15. We prove (d). Since the Frobenius F_n is an endomorphism and $F_n(x \star E_p(n)) = F_n(x) \star E_p$, one can rewrite (33) as

$$(\theta_A(x))_n = \psi_A^{-1}(E_p \star F_n(x)) \quad \text{for all } n \in I(p).$$

Thus, to show (34) it is enough to prove it for $n = 1$. One needs to check that for all $x \in \mathbb{W}(A)$, one has

$$E_p \star \varphi_A(x) = \prod_{\mathbb{N}} E_p(x_{p^n} t^{p^n}).$$

Indeed, this follows from distributivity and the identity

$$E_p \star (1 - xt^n)^{-1} = \begin{cases} 1 & \text{if } n \notin p^{\mathbb{N}}, \\ E_p(xt^{p^k}) & \text{if } n = p^k. \end{cases}$$

The above identity can be checked directly knowing that $(1 - xt^n)^{-1} = V_n(\tau(x))$ and by applying the equality

$$E_p \star (1 - xt^n)^{-1} = E_p \star V_n(\tau(x)) = V_n(F_n(E_p) \star \tau(x))$$

together with Proposition 6.1 (3) and the equality

$$\tau(y) \star f(t) = (1 - yt)^{-1} \star f(t) = f(yt),$$

which holds for any element $f(t) \in \Lambda(A)$. In particular, for the Teichmüller lift $\tau(y) = [y]$ of an element $y \in A$ one gets

$$\theta_A(\tau(y))_n = \tau(y^n) \quad \text{for all } n \in I(p) \tag{35}$$

where, on the right-hand side, τ denotes the original Teichmüller lift $\tau\colon A \to \mathbb{W}_{p^\infty}(A)$. Indeed one has $F_n(\tau(y)) = \tau(y^n)$. □

Corollary 6.3. *Let A be an $\mathbb{F}_p$-algebra. Then the common fixed points of the endomorphisms $F_n\colon \mathbb{W}(A) \to \mathbb{W}(A)$ for $n \in I(p)$ are the elements of the form*

$$L(\lambda) = \sum_{m \in I(p)} \frac{1}{m} V_m(E_p \star \lambda), \quad \lambda \in \mathbb{W}_{p^\infty}(A). \tag{36}$$

One also has

$$\varphi_A(L(\lambda)) = \prod_{n \in I(p)} h_\lambda(t^n)^{\frac{1}{n}}.$$

Proof. Let $x \in \mathbb{W}(A)$ with $F_n(x) = x$ for all $n \in I(p)$. Then it follows from (34) and (33) that all the components $(\theta_A(x))_n$ are equal, so that for some $\lambda \in \mathbb{W}_{p^\infty}(A)$ one has

$$E_p(n) \star x = \frac{1}{n} V_n(E_p \star \lambda)$$

and x is of the required form. Conversely, by Proposition 6.1 (3), one has $F_a(E_p) = 0_\Lambda$ for all $a \in I(p)$, $a \neq 1$. Thus when one applies F_k to $\frac{1}{n} V_n(E_p \star \lambda)$, one gets 1 $(= 0_\Lambda)$ unless $k|n$ using Proposition 5.1 (2), (3). When $k|n$ one obtains $\frac{1}{m} V_m(E_p \star \lambda)$, with $m = n/k$. Thus the elements of the form (36) are fixed under all F_k. □

We now apply these results to the case $A = \bar{\mathbb{F}}_p$. We identify $\mathbb{W}_{p^\infty}(\bar{\mathbb{F}}_p)$ with a subring of $\mathbb{C}_p$ (the p-adic completion of an algebraic closure of $\mathbb{Q}_p$). Let $\widehat{\mathbb{Q}_p^{\mathrm{un}}} \subset \mathbb{C}_p$ be the completion of the maximal unramified extension of $\mathbb{Q}_p$. Then one knows that $\mathbb{W}_{p^\infty}(\bar{\mathbb{F}}_p) = \mathcal{O}_{\widehat{\mathbb{Q}_p^{\mathrm{un}}}}$ is the ring of integers of $\widehat{\mathbb{Q}_p^{\mathrm{un}}}$. With Θ the isomorphism of (34), we have

$$\Theta\colon \mathbb{W}(\bar{\mathbb{F}}_p) \xrightarrow{\sim} (\mathcal{O}_{\widehat{\mathbb{Q}_p^{\mathrm{un}}}})^{I(p)}, \quad (\Theta(x)_n)_{p^k} = F_n(x)_{p^k},$$

for all $n \in I(p)$ and all $x \in \mathbb{W}(\bar{\mathbb{F}}_p)$. Thus Θ makes $\mathbb{W}(\bar{\mathbb{F}}_p)$ a module over $\mathcal{O}_{\widehat{\mathbb{Q}_p^{\mathrm{un}}}}$.

To the Frobenius automorphism of $\bar{\mathbb{F}}_p$ corresponds, by functoriality, a canonical automorphism Fr of $\mathcal{O}_{\widehat{\mathbb{Q}_p^{\mathrm{un}}}}$ which extends to a continuous automorphism

$$\mathrm{Fr} \in \mathrm{Aut}(\widehat{\mathbb{Q}_p^{\mathrm{un}}}).$$

We can now describe the p-adic analogues of the complex irreducible representations of the BC-system (cf. (48)). We recall that X_p denotes the space of all injective group homomorphisms $\sigma\colon \bar{\mathbb{F}}_p^\times \to \mathbb{C}^\times$. Using the embedding (84) of the abstract cyclotomic field $\mathbb{Q}^{\mathrm{cyc}} \subset \mathbb{C}$, and Proposition 8.16, the choice of $\sigma \in X_p$ determines an embedding $\rho\colon \mathbb{Q}^{\mathrm{cyc,p}} \to \mathbb{C}_p$ of the cyclotomic field generated by the abstract roots of unity of order prime to p inside $\mathbb{C}_p$.

In the following we shall use the simplified notation $\mathcal{O} = \mathcal{O}_{\widehat{\mathbb{Q}_p^{\mathrm{un}}}}$. For $m \in I(p)$, we let ϵ_m be the vector in $\mathbb{W}(\bar{\mathbb{F}}_p)$ with only one non-zero component: $\epsilon_m(m) = 1$.

Theorem 6.4. *Let $\sigma \in X_p$. The representation π_σ as in Theorem 4.5 extends by continuity to a representation of the integral BC-algebra $\mathcal{H}_\mathbb{Z}$ on $\mathbb{W}(\bar{\mathbb{F}}_p)$. For $n \in I(p)$ and for $x \in \mathbb{Z}[\mathbb{Q}/\mathbb{Z}]$, $\pi_\sigma(\mu_n)$, $\pi_\sigma(x)$ and $\pi_\sigma(\mu_n^*)$ are $\mathcal{O}$-linear operators on $\mathbb{W}(\bar{\mathbb{F}}_p)$ and we have*

$$\pi_\sigma(\mu_n)\epsilon_m = \epsilon_{nm}, \quad \pi_\sigma(e(a/b))\epsilon_m = \rho(\zeta_{a/b}^m)\epsilon_m \tag{37}$$

for all $a \in \mathbb{Z}$ and all $b, m \in I(p)$,

$$\pi_\sigma(\mu_n^*)\epsilon_k = \begin{cases} 0 & \text{if } k \notin n\mathbb{N}, \\ \epsilon_{k/n} & \text{if } k \in n\mathbb{N}. \end{cases} \tag{38}$$

One has $\pi_\sigma(x) = \pi_\sigma(r(x))$ for all $x \in \mathbb{Z}[\mathbb{Q}/\mathbb{Z}]$ ($r\colon \mathbb{Z}[\mathbb{Q}/\mathbb{Z}] \to \mathbb{Z}[(\mathbb{Q}/\mathbb{Z})^{(p)}]$ the retraction as in (19)) and

$$\pi_\sigma(\mu_p) = \mathrm{Fr}^{-1}, \quad \pi_\sigma(\mu_p^*) = \mathrm{Fr}, \tag{39}$$

where Fr *is the Frobenius automorphism acting componentwise as a skew-linear operator.*

Proof. Theorem 4.5 and the density of $\mathbb{W}_0(\bar{\mathbb{F}}_p)$ in $\mathbb{W}(\bar{\mathbb{F}}_p)$ (cf., e.g., [23], 1.8) show that π_σ extends by continuity to a representation of the integral BC-algebra $\mathcal{H}_\mathbb{Z}$ on $\mathbb{W}(\bar{\mathbb{F}}_p)$. In view of the invertibility of the elements $n \in I(p)$ in $\mathbb{W}(\bar{\mathbb{F}}_p)$, the description of the representation π_σ is simplified by using the elements $\mu_n = \frac{1}{n}\tilde{\mu}_n$, to stress the analogy with the complex case. It follows from Corollary 6.3 that the subring $\mathcal{O}$ of $\mathbb{W}(\bar{\mathbb{F}}_p)$ is the fixed subring for the action of the operators F_n for all $n \in I(p)$. For $n \in I(p)$, the operators F_n are $\mathcal{O}$-linear likewise the V_n (cf. Proposition 2.2 (2) which correspond to the $\tilde{\mu}_n$ by means of the representation π_σ. Thus we obtain the first equality in (37). The operators $\pi_\sigma(e(a/b))$ are the multiplication operators (cf. Corollary 2.4) by $\tau(e(a/b))$, thus they are $\mathcal{O}$-linear and the second equation in (37) follows from (35). By applying (26) one has $\pi_\sigma(\mu_n^*) = F_n$ for all n. Taking $n = p$, one gets that $\pi_\sigma(\mu_p^*) = F_p$, which coincides with Fr acting componentwise, as it follows from the commutation $F_p \circ \frac{1}{n}V_n = \frac{1}{n}V_n \circ F_p$ for $n \in I(p)$ and (31). Since $\mu_p^*\mu_p = 1$ and Fr is invertible, one gets (39). □

Definition 6.5. We denote by $\mathcal{J}_p \subset \mathcal{H}_\mathbb{Z}$ the two-sided ideal generated by the elements

$$1 - e(p^{-k}) \quad \text{for all } k \in \mathbb{N}. \tag{40}$$

Proposition 6.6. *One has $\mathcal{J}_p = \operatorname{Ker}\pi_\sigma$ (cf. (37)), and the intersection $\mathbb{Z}[\mathbb{Q}/\mathbb{Z}] \cap \mathcal{J}_p$ is the ideal $\mathcal{J}_p^0$ of $\mathbb{Z}[\mathbb{Q}/\mathbb{Z}]$ generated by the elements as in (40).*

The sequence of commutative algebras

$$0 \to \mathcal{J}_p^0 \to \mathbb{Z}[\mathbb{Q}/\mathbb{Z}] \xrightarrow{r} \mathbb{Z}[(\mathbb{Q}/\mathbb{Z})^{(p)}] \to 0$$

is exact.

Proof. Let $r = \mathrm{id}_{\mathbb{Z}[(\mathbb{Q}/\mathbb{Z})^{(p)}]} \otimes \epsilon \colon \mathbb{Z}[\mathbb{Q}/\mathbb{Z}] \to \mathbb{Z}[(\mathbb{Q}/\mathbb{Z})^{(p)}]$ be the retraction map introduced in (19). By construction, one has

$$\mathcal{J}_p^0 = \mathrm{Ker}(r).$$

Since $\pi_\sigma(e(a/b))$ only depends upon $r(e(a/b))$ it follows that $\mathcal{J}_p \subset \mathrm{Ker}\,\pi_\sigma$. One knows (cf. [16], Lemma 4.8) that any element of the algebra $\mathcal{H}_\mathbb{Z}$ can be written as a finite sum of monomials of the form

$$\sum_{\substack{\{a,b\}\in\mathbb{N}^2\\(a,b)=1}} \tilde{\mu}_a\, x_{\{a,b\}}\, \mu_b^*, \quad x_{\{a,b\}} \in \mathbb{Z}[\mathbb{Q}/\mathbb{Z}]. \tag{41}$$

We show that for any finite sum X as in (41) we have

$$\pi_\sigma(X) = 0 \implies x_{\{a,b\}} \in \mathcal{J}_p^0. \tag{42}$$

It is enough to prove that $r(x_{\{a,b\}}) = 0$ for all $a, b \in \mathbb{N}$, and since $\mathbb{Z}[(\mathbb{Q}/\mathbb{Z})^{(p)}]$ is torsion-free, it suffices to show that $ar(x_{\{a,b\}}) = 0$ for all $a, b \in \mathbb{N}$. Let $y\colon \mathbb{Q}_+^* \to \mathbb{Z}[(\mathbb{Q}/\mathbb{Z})^{(p)}]$, $y(\frac{a}{b}) := a\,r(x_{\{a,b\}})$; then y has finite support. For any group homomorphism

$$\chi\colon (\mathbb{Q}/\mathbb{Z})^{(p)} \to \mathcal{O}^\times$$

there is a unique ring homomorphism h_χ with

$$h_\chi\colon \mathbb{Z}[(\mathbb{Q}/\mathbb{Z})^{(p)}] \to \mathcal{O}, \quad h_\chi(e(\gamma)) = \chi(\gamma) \quad \text{for all } \gamma \in (\mathbb{Q}/\mathbb{Z})^{(p)}.$$

This applies in particular, for any integer j, to $\chi = \rho^j$ where we view $\rho\colon \mathbb{Q}^{\mathrm{cyc,p}} \to \mathbb{C}_p$ as a group homomorphism $\rho\colon (\mathbb{Q}/\mathbb{Z})^{(p)} \to \mathcal{O}^\times$. One has

$$\bigcap_{j\in\mathbb{Z}} \mathrm{Ker}\, h_{\rho^j} = \{0\} \tag{43}$$

since an injective character of a finite cyclic group generates the dual group. Let $n, m \in I(p)$ be relatively prime. Then one has

$$(\pi_\sigma(X) z \epsilon_{jm})_{jn} = \sum_{k\in\mathbb{Z}} h_{\rho^j}(y(p^{-k}\tfrac{n}{m}))\, \mathrm{Fr}^k(z).$$

for any $j \in I(p)$ and $z \in \mathcal{O}$. Thus if $\pi_\sigma(X) = 0$ one has for all j and m, n as above

$$\sum_{k\in\mathbb{Z}} h_{\rho^j}(y(p^{-k}\tfrac{n}{m}))\, \mathrm{Fr}^k(z) = 0 \quad \text{for all } z \in \mathcal{O}.$$

For z a root of unity one has $\mathrm{Fr}^k(z) = z^{p^k}$. Thus the polynomial

$$\sum_{k\in\mathbb{Z}} h_{\rho^j}(y(p^{-k}\tfrac{n}{m}))\, Z^{p^{k+n}}$$

vanishes, for n large enough, on all roots of unity, thus it is identically zero, hence all its coefficients must vanish, i.e.,

$$h_{\rho^j}(y(p^{-k}\tfrac{n}{m})) = 0 \quad \text{for all } k \in \mathbb{Z},\ j \in \mathbb{N}.$$

It then follows from (43) that $y(\frac{a}{b}) = y(p^{-k}\frac{n}{m}) = 0$, hence (42) holds, and the proof that any element of $\operatorname{Ker}\pi_\sigma$ is in $\mathcal{J}_p$ is complete. Finally, if $x \in \mathbb{Z}[\mathbb{Q}/\mathbb{Z}]$ belongs to $\operatorname{Ker}\pi_\sigma$, one has $x \in \mathcal{J}_p^0$ by (42), and thus the intersection $\mathbb{Z}[\mathbb{Q}/\mathbb{Z}] \cap \mathcal{J}_p$ is the ideal $\mathcal{J}_p^0$. □

Definition 6.7. We denote by $\mathcal{H}_{\mathbb{Z}}^{(p)}$ the quotient by $\mathcal{J}_p$ of the subalgebra of $\mathcal{H}_{\mathbb{Z}}$ generated by $\mathbb{Z}[\mathbb{Q}/\mathbb{Z}]$, $\tilde{\mu}_n$, μ_n^* for $n \in I(p)$.

The algebra $\mathcal{H}_{\mathbb{Z}}^{(p)}$ is generated by $\mathbb{Z}[(\mathbb{Q}/\mathbb{Z})^{(p)}]$, the operators $\tilde{\mu}_n$ and μ_n^* for $n \in I(p)$, and its presentation is similar to the presentation of $\mathcal{H}_{\mathbb{Z}}$. The relations are

$$\begin{aligned} \tilde{\mu}_{nm} &= \tilde{\mu}_n\tilde{\mu}_m, \quad \mu_{nm}^* = \mu_n^*\mu_m^* \quad \text{for all } n, m \in I(p),\\ \mu_n^*\tilde{\mu}_n &= n \quad \text{for all } n \in I(p),\\ \tilde{\mu}_n\mu_m^* &= \mu_m^*\tilde{\mu}_n \quad \text{for all } n, m \in I(p) \text{ with } (n,m) = 1, \end{aligned}$$

as well as the relations

$$\tilde{\mu}_n x \mu_n^* = \tilde{\rho}_n(x), \quad \mu_n^* x = \sigma_n(x)\mu_n^*, \quad x\tilde{\mu}_n = \tilde{\mu}_n\sigma_n(x), \tag{44}$$

where $\tilde{\rho}_n$, $n \in I(p)$, is defined by

$$\tilde{\rho}_n(e(\gamma)) = \sum_{n\gamma'=\gamma} e(\gamma') \quad \text{for all } \gamma \in (\mathbb{Q}/\mathbb{Z})^{(p)}. \tag{45}$$

Given an algebra $\mathcal{A}$, an automorphism $\theta \in \operatorname{Aut}(\mathcal{A})$ and an integer p we let $\mathcal{A} \rtimes_{\theta,p} \mathbb{Z}$ be the subalgebra of the algebraic cross product $\{\sum_{n\in\mathbb{Z}} a_n V^n \mid a_n \in \mathcal{A}\}$ determined by the condition

$$a_{-n} \in p^n\mathcal{A} \quad \text{for all } n \in \mathbb{N}.$$

Lemma 6.8. *Let $V = U^*$ and $pV^{-1} = \widetilde{U}$, then $\mathcal{A} \rtimes_{\theta,p} \mathbb{Z}$ is generated by $\mathcal{A}$, $\widetilde{U}$, U^* with the relations*

$$U^*\widetilde{U} = p, \quad \widetilde{U}xU^* = p\theta^{-1}(x), \quad U^*x = \theta(x)U^*, \quad x\widetilde{U} = \widetilde{U}\theta(x) \tag{46}$$

for all $x \in \mathcal{A}$.

Proof. By construction all elements of $\mathcal{A} \rtimes_{\theta,p} \mathbb{Z}$ are linear combinations of monomials in $\mathcal{A}$, $\widetilde{U}$, U^*. Moreover, the relations are sufficient to recover the cross product rules. □

Proposition 6.9. *There exists a unique automorphism* $\mathrm{Fr} \in \mathrm{Aut}(\mathcal{H}_{\mathbb{Z}}^{(p)})$ *such that*

$$\mathrm{Fr}(e(\gamma)) = e(\gamma)^p \quad \textit{for all } \gamma \in (\mathbb{Q}/\mathbb{Z})^{(p)},$$
$$\mathrm{Fr}(\tilde{\mu}_n) = \tilde{\mu}_n, \quad \mathrm{Fr}(\mu_n^*) = \mu_n^* \quad \textit{for all } n \in I(p).$$

One derives an isomorphism

$$\mathcal{H}_{\mathbb{Z}}/\mathcal{J}_p = \mathcal{H}_{\mathbb{Z}}^{(p)} \rtimes_{\mathrm{Fr},p} \mathbb{Z}.$$

Proof. The map $\gamma \to p\gamma$ defines an automorphism of $(\mathbb{Q}/\mathbb{Z})^{(p)}$. Its linearization Fr acts on $\mathbb{Z}[(\mathbb{Q}/\mathbb{Z})^{(p)}]$ and commutes with the endomorphisms σ_n and $\tilde{\rho}_n$. In fact by applying the isomorphism of Proposition 4.4, Fr corresponds to the Frobenius automorphism of $\bar{\mathbb{F}}_p$. Thus it extends to an automorphism $\mathrm{Fr} \in \mathrm{Aut}(\mathcal{H}_{\mathbb{Z}}^{(p)})$.

The second statement follows by comparing the presentation of $\mathcal{H}_{\mathbb{Z}}/\mathcal{J}_p$ with that of the crossed product $\mathcal{H}_{\mathbb{Z}}^{(p)} \rtimes_{\mathrm{Fr},p} \mathbb{Z}$ as in (46). □

Proposition 6.10. *Let* $\sigma \in X_p$.

(1) *The restriction* $\pi_\sigma|_{\mathcal{H}_{\mathbb{Z}}^{(p)}}$ *of the representation* π_σ (*as in Theorem* 6.4) *to* $\mathcal{H}_{\mathbb{Z}}^{(p)}$ *is* $\mathcal{O}$*-linear and indecomposable over* $\mathcal{O}$.

(2) *The representations* $\pi_\sigma|_{\mathcal{H}_{\mathbb{Z}}^{(p)}}$ *are pairwise inequivalent.*

(3) *The representation* π_σ *is linear and indecomposable over* $\mathbb{Z}_p$.

(4) *Two representations* π_σ *and* $\pi_{\sigma'}$ *are equivalent over* $\mathbb{Z}_p$ *if and only if there exists* $\alpha \in \mathrm{Aut}(\bar{\mathbb{F}}_p)$ *such that* $\sigma' = \sigma \circ \alpha$.

Proof. (1) The $\mathcal{O}$-linearity property is checked directly on the generators using Theorem 6.4. It follows from (37) that the vector ϵ_1 is cyclic for $\mathcal{H}_{\mathbb{Z}}^{(p)}$, i.e., $\pi_\sigma(\mathcal{H}_{\mathbb{Z}}^{(p)})\epsilon_1$ is dense in $\mathbb{W}(\bar{\mathbb{F}}_p) = \mathcal{O}^{I(p)}$. One has

$$\mathcal{O}\epsilon_1 = \{\xi \in \mathbb{W}(\bar{\mathbb{F}}_p) \mid \pi_\sigma(\mu_n^*)(\xi) = 0 \text{ for all } n \neq 1,\ n \in I(p)\}. \tag{47}$$

For any $\mathcal{O}$-linear continuous operator T in the commutant of $\mathcal{H}_{\mathbb{Z}}^{(p)}$ one has $\pi_\sigma(\mu_n^*)T\epsilon_1 = T\pi_\sigma(\mu_n^*)\epsilon_1 = 0$ for all $n > 1$, and by (47) there exists $\lambda \in \mathcal{O}$ such that $T\epsilon_1 = \lambda\epsilon_1$. Thus, since ϵ_1 is cyclic, T is given by the module action of $\lambda \in \mathcal{O}$.

(2) By (37), the action of $\pi_\sigma(e(\gamma))$ for $\gamma \in (\mathbb{Q}/\mathbb{Z})^{(p)}$ on the subspace (47) is given by the multiplication by $\rho(\gamma) \in \mathcal{O}^\times$. Thus, ρ is an invariant of the representation.

(3) Any element of the commutant of the action of $\mathcal{H}_{\mathbb{Z}}$ is given by the module action of $\lambda \in \mathcal{O}$, where λ is fixed for the action of the Frobenius on $\mathcal{O}$, i.e., $\lambda \in \mathbb{Z}_p$. This shows that π_σ is indecomposable.

(4) We show first that if there exists $\alpha \in \mathrm{Aut}(\bar{\mathbb{F}}_p)$ such that $\sigma' = \sigma \circ \alpha^{-1}$, the representations π_σ and $\pi_{\sigma'}$ are equivalent over $\mathbb{Z}_p$. Let $\tilde{\alpha} = \mathbb{W}_{p^\infty}(\alpha) \in \mathrm{Aut}(\mathbb{W}_{p^\infty}(\bar{\mathbb{F}}_p)) = \mathrm{Aut}(\mathcal{O})$ and define $U\colon \mathcal{O}^{I(p)} \to \mathcal{O}^{I(p)}$, $(U\xi)_n = \tilde{\alpha}(\xi_n)$, for

all $n \in I(p)$. One has $U\epsilon_n = \epsilon_n$ for all $n \in I(p)$, and if T is an $\mathcal{O}$-linear operator so is UTU^{-1}. It thus follows from (37) and (38) that $U\pi_\sigma(\mu_n)U^{-1} = \pi_\sigma(\mu_n)$ and $U\pi_\sigma(\mu_n^*)U^{-1} = \pi_\sigma(\mu_n^*)$. For $x \in \mathbb{Z}[\mathbb{Q}/\mathbb{Z}]$, $U\pi_\sigma(x)U^{-1}$ only depends on $r(x)$ and for $x = e(a/b)$, $b \in I(p)$, one has $U\pi_\sigma(e(a/b))U^{-1}\epsilon_m = \tilde{\alpha}(\rho(\zeta_{a/b}^m))\epsilon_m = \rho'(\zeta_{a/b}^m)\epsilon_m = \pi_{\sigma'}(e(a/b))$.

Moreover, since $\tilde{\alpha}$ commutes with Fr, it follows from (39) that $U\pi_\sigma(\mu_p)U^{-1} = \pi_\sigma(\mu_p)$ and $U\pi_\sigma(\mu_p^*)U^{-1} = \pi_\sigma(\mu_p^*)$. Thus one gets the required equivalence.

Conversely, assume that two representations π_σ and $\pi_{\sigma'}$ are equivalent over $\mathbb{Z}_p$. By (47) the $\mathbb{Z}_p$-linear representation π_σ (and similarly $\pi_{\sigma'}$) determines uniquely the representation

$$\beta_\sigma(e(a/b))\xi = \rho(\zeta_{a/b})\xi, \quad \text{for all } \xi \in \mathcal{O},$$

of $\mathbb{Z}[(\mathbb{Q}/\mathbb{Z})^{(p)}]$ in the $\mathbb{Z}_p$-module $\mathcal{O}$. In turn, this determines an extension of the p-adic valuation to the subfield $\mathbb{Q}^{\mathrm{cyc,p}} \subset \mathbb{Q}^{\mathrm{cyc}}$ generated over $\mathbb{Q}$ by $\mu^{(p)}$. Indeed the formula

$$\mathrm{val}(x) = \inf\{k \geq 0 \mid \beta_\sigma(x)\mathcal{O} \subset p^k\mathcal{O}\} \quad \text{for all } x \in \mathbb{Z}[(\mathbb{Q}/\mathbb{Z})^{(p)}]$$

only depends on the class of x in $\mathbb{Q}^{\mathrm{cyc,p}}$ and extends uniquely to a valuation on $\mathbb{Q}^{\mathrm{cyc,p}}$. The conclusion then follows from Proposition 8.14. □

7. The KMS theory of the BC-system at a prime p

In [4] it was shown that the extremal, complex KMS states below critical temperature of the BC-system (cf. (17)) are of the form

$$\varphi_{\beta,\rho}(X) = \frac{\mathrm{Tr}(\pi_\rho(X)e^{-\beta H})}{\mathrm{Tr}(e^{-\beta H})} \quad \text{for all } X \in \mathcal{H}_{\mathbb{Z}},$$

where H is the Hamiltonian operator of multiplication by $\log n$ in the canonical basis ϵ_n of the Hilbert space $\ell^2(\mathbb{N})$ and π_ρ is the irreducible representation of the algebra $\mathcal{H}_{\mathbb{Q}}$ given by

$$\pi_\rho(\mu_n)\epsilon_m = \epsilon_{nm}, \quad \pi_\rho(\mu_n^*) = \pi_\rho(\mu_n)^*, \quad \pi_\rho(e(a/b))\epsilon_m = \rho(\zeta_{a/b}^m)\epsilon_m, \tag{48}$$

where $\rho \in \hat{\mathbb{Z}}^*$ determines an embedding in $\mathbb{C}$ of the cyclotomic field $\mathbb{Q}^{\mathrm{cyc}}$ generated by the abstract roots of unity. Thus the extremal KMS states $\varphi_{\beta,\rho}$ are directly computable using the representation π_ρ and the explicit description of the Hamiltonian.

In Section 6 we have described the p-adic analogue of the representation π_ρ. In this section, our goal is to obtain the p-adic analogue of the KMS states $\varphi_{\beta,\rho}$. The guiding equation is provided by the general algebraic formulation of the KMS condition which is described by the equality

$$\varphi(x\sigma(y)) = \varphi(y\,x) \quad \text{for all } x, y \in \mathcal{A},$$

where φ is a linear form on an algebra $\mathcal{A}$ endowed with an automorphism $\sigma \in \mathrm{Aut}(\mathcal{A})$. In our case the algebra is

$$\mathcal{A} = \mathcal{H}^{(p)}_{\mathbb{C}_p} = \mathcal{H}^{(p)}_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{C}_p.$$

In §7.1 we introduce, using the Iwasawa logarithm as a substitute for the above complex Hamiltonian H, the automorphisms $\sigma^{(\beta)} \in \mathrm{Aut}(\mathcal{H}^{(p)}_{\mathbb{C}_p})$. These automorphisms are defined for β in the "extended s-disk" D_p (cf. (50) below). In §7.5 we shall show how to extend their definition from the domain D_p to a covering M of $\mathbb{C}_p$. The construction of the KMS states is based on the classical construction of the p-adic L-functions and p-adic polylogarithm and many properties that we obtain rely on the simplifications which occur when $\beta = 1 - k(p-1)$ $(k \in \mathbb{Z})$. In §7.2 we prove the identities in the cyclotomic field, involving Bernoulli polynomials, which are behind the verification of the KMS condition. In §7.3 we provide the construction of the linear forms $\varphi_{\beta,\rho}$ using some of the results from [38] (cf. Chapter V). In §7.4 we prove that the functionals $\varphi_{\beta,\rho}$ fulfill the KMS condition with respect to the automorphism $\sigma^{(\beta)} \in \mathrm{Aut}(\mathcal{H}^{(p)}_{\mathbb{C}_p})$. Unlike the complex case, this construction exhibits the (new) phenomenon of the invariance of the linear forms $\varphi_{\beta,\rho}$ under the symmetry of $\mathcal{H}^{(p)}_{\mathbb{C}_p}$ given by the automorphism $e(\gamma) \mapsto e(-\gamma)$.

Throughout this section we fix a finite, rational prime p and an algebraic closure $\bar{\mathbb{Q}}_p$ whose completion is denoted $\mathbb{C}_p$. We also use the notation

$$q = 4 \text{ if } p = 2, \qquad q = p \text{ if } p \neq 2, \tag{49}$$

and

$$\varphi(q) = 2 \text{ if } p = 2, \quad \varphi(q) = p - 1 \text{ if } p \neq 2.$$

One has $qp^{-1/(p-1)} > 1$. We consider the "extended s-disk",

$$D_p := \{\beta \in \mathbb{C}_p \mid |\beta|_p < qp^{-1/(p-1)}\}, \tag{50}$$

and first develop the theory for $\beta \in D_p$. In §7.5 we shall explain how the Iwasawa construction of p-adic L-functions allows one to extend the whole theory from the domain D_p to the covering of $\mathbb{C}_p$ given by the multiplicative group M which is the open disk of radius one and center 1 in $\mathbb{C}_p$.

7.1. The automorphisms $\sigma^{(\beta)} \in \mathrm{Aut}(\mathcal{H}^{(p)}_{\mathbb{C}_p})$.

Let $\mathbb{Z}^{\times}_{(p)} \subset \mathbb{Q}^{\times}$ be the multiplicative group of rational fractions whose numerator and denominator are prime to p. We use throughout the same notion of analyticity as in [38].

Lemma 7.1. *Let $r \in \mathbb{Z}^{\times}_{(p)}$. There exists a unique analytic function*

$$D_p \to \mathbb{C}_p, \quad \beta \mapsto r^{(\beta)},$$

such that

$$r^{(\beta)} = r^{\beta} \quad \textit{for all } \beta \in 1 - \varphi(q)\mathbb{Z}. \tag{51}$$

Proof. We recall that the Iwasawa logarithm $\log_p$ is the unique extension of the function defined in the open unit disk centered at 1 by

$$-\log_p(1-x) = \sum_{n=1}^{\infty} \frac{x^n}{n} \quad \text{for all } x \in \mathbb{C}_p,\ |x|_p < 1,$$

to a map $\log_p : \mathbb{C}_p^\times \to \mathbb{C}_p$ such that

$$\log_p(xy) = \log_p(x) + \log_p(y) \quad \text{for all } x, y \in \mathbb{C}_p,\ \log_p(p) = 0. \tag{52}$$

One has $\log_p(-1) = 0$ since -1 is a root of unity, and

$$|\log_p(r)|_p \leq q^{-1} \quad \text{for all } r \in \mathbb{Z}_{(p)}^\times. \tag{53}$$

Moreover, the exponential function is defined by the series

$$\exp(x) = \sum_{n=1}^{\infty} \frac{x^n}{n!} \quad \text{for all } x \in \mathbb{C}_p,\ |x|_p < r_p = p^{-\frac{1}{p-1}}.$$

We define

$$r^{(\beta)} := r \exp((\beta - 1)\log_p(r)) \quad \text{for all } \beta \in D_p. \tag{54}$$

This is a well-defined, analytic function of $\beta \in D_p$ since $\beta - 1 \in D_p$, and thus $|(\beta - 1)\log_p(r)|_p < r_p$ by (53). We show that (51) holds. This follows from the equality

$$\exp(k\varphi(q)\log_p(r)) = r^{k\varphi(q)} \quad \text{for all } r \in \mathbb{Z}_{(p)}^\times,\ k \in \mathbb{Z},$$

which holds for $r = -1$ since $\varphi(q)$ is even. In general, (51) follows from the formula

$$\exp(n \log_p(a)) = a^n \quad \text{for all } a \in \mathbb{Z}_p^*,\ n \in \varphi(q)\mathbb{Z},$$

as shown in [38] (Chapter 5, p. 52), where the notation

$$\langle a \rangle = \exp(\log_p(a)) \tag{55}$$

is introduced. The uniqueness follows from the discreteness of the set of zeros of analytic functions (cf. [38]). □

Lemma 7.2. *Let $\beta \in D_p$. Then*

$$\mathbb{Z}_{(p)}^\times \ni r \mapsto r^{(\beta)} \in \mathbb{C}_p^\times$$

is a group homomorphism. Moreover, for $r \in \mathbb{Z}_{(p)}^\times$,

$$r^{(\beta_1)} r^{(\beta_2)} = r^{(\beta_1+\beta_2)} r^{(0)} \quad \textit{for all } \beta_j \in D_p. \tag{56}$$

Proof. This follows from (52) and the equality (cf. [33])

$$\exp(x_1 + x_2) = \exp(x_1)\exp(x_2) \quad \text{for all } x_j,\ |x_j|_p < r_p. \qquad \square$$

The standard notation for $r^{(0)}$ is $\omega(r)$: it is the unique $\varphi(q)$ root of unity which is congruent to r modulo q. In particular one has

$$(r^{(0)})^{\varphi(q)} = 1 \quad \text{for all } r \in \mathbb{Z}_{(p)}^{\times}. \tag{57}$$

Proposition 7.3. (1) *For $\beta \in D_p$ there exists a unique automorphism $\sigma^{(\beta)} \in \mathrm{Aut}(\mathcal{H}_{\mathbb{C}_p}^{(p)})$ such that*

$$\sigma^{(\beta)}(\tilde{\mu}_a e(\gamma)\mu_b^*) = \left(\frac{b}{a}\right)^{(\beta)} \tilde{\mu}_a e(\gamma)\mu_b^* \quad \textit{for all } a, b \in I(p),\ \gamma \in (\mathbb{Q}/\mathbb{Z})^{(p)}.$$

(2) *One has*

$$\sigma^{(\beta_1)} \circ \sigma^{(\beta_2)} = \sigma^{(\beta_1+\beta_2)} \circ \sigma^{(0)} \quad \textit{for all } \beta_j \in D_p, \tag{58}$$

and $\sigma^{(0)}$ is an automorphism of order $\varphi(q)$.

Proof. It suffices to check that $\sigma^{(\beta)}$ preserves the presentation given by the relations (44) and (44). This follows from the multiplicativity shown in Lemma 7.2. Similarly (58) follows from (56). The last statement follows from (57). □

7.2. Cyclotomic identities for the polylogarithm. We recall that the Bernoulli polynomials $B_n(u)$ are defined inductively as follows

$$B_0(x) = 1, \qquad B_n'(x) = nB_{n-1}(x), \qquad \int_0^1 B_n(x)dx = 0.$$

Equivalently, these polynomials can be introduced using the generating function

$$F(u,t) = \frac{te^{ut}}{e^t - 1} = \sum_{n=0}^{\infty} B_n(u)\frac{t^n}{n!}. \tag{59}$$

The first few are

$$\begin{aligned}
B_0(u) &= 1,\\
B_1(u) &= -\frac{1}{2} + u,\\
B_2(u) &= \frac{1}{6} - u + u^2,\\
B_3(u) &= \frac{u}{2} - \frac{3u^2}{2} + u^3,\\
B_4(u) &= -\frac{1}{30} + u^2 - 2u^3 + u^4,\\
B_5(u) &= -\frac{u}{6} + \frac{5u^3}{3} - \frac{5u^4}{2} + u^5.
\end{aligned}$$

These polynomials fulfill the equation $B_n(1-u) = (-1)^n B_n(u)$. The Bernoulli numbers are $B_n = B_n(0)$. Using (59), one checks the identity (cf. [38], Chapter 4, Proposition 4.1)

$$g^{n-1}\sum_{j=0}^{g-1} B_n\left(\frac{x+j}{g}\right) = B_n(x). \tag{60}$$

We also introduce inductively the rational fractions $\ell_\beta(z)$ for $\beta \in -\mathbb{N}$ as follows:

$$z\partial_z \ell_\beta(z) = \ell_{\beta-1}(z), \quad \ell_0(z) = \frac{z}{1-z}.$$

For $\alpha \in \mathbb{Q}/\mathbb{Z}$ we denote by $\zeta_\alpha \in \mathbb{Q}^{\mathrm{cyc}}$ the class of $e(\alpha) \in \mathbb{Q}[\mathbb{Q}/\mathbb{Z}]$ modulo the cyclotomic ideal (cf. Definition 8.1). It is a root of unity whose order is the denominator of α.

Lemma 7.4. *Let $n > 1$, $a, b \in \mathbb{N}$. Then*

$$b^{n-1}\sum_{j=0}^{b-1} \zeta_{a/b}^j B_n\left(\frac{j}{b}\right) = \begin{cases} -n\ell_{1-n}(\zeta_{a/b}) & \text{if } \zeta_{a/b} \neq 1, \\ B_n, & \text{if } \zeta_{a/b} = 1. \end{cases} \tag{61}$$

Proof. The equality (61) for $\zeta_{a/b} = 1$ follows from (60). Thus we can assume that $z = \zeta_{a/b} \neq 1$. The Taylor expansion at $t = 0$ of $(ze^t - 1)^{-1}$ is given by

$$(ze^t - 1)^{-1} = (z-1)^{-1} - \sum_{n=1}^{\infty} \ell_{-n}(z)\frac{t^n}{n!} \tag{62}$$

since $(z-1)^{-1} = -1 - \ell_0(z)$ and ∂_t agrees with $z\partial_z$. Then for $b \in \mathbb{N}$ and t such that $ze^{\frac{t}{b}} \neq 1$ one has

$$\sum_{j=0}^{b-1} z^j e^{\frac{j}{b}t} = \frac{z^b e^t - 1}{ze^{\frac{t}{b}} - 1}.$$

Since $z^b = 1$, one derives

$$\sum_{n=0}^{\infty}\left(\sum_{j=0}^{b-1} z^j B_n\left(\frac{j}{b}\right)\right)\frac{t^n}{n!} = \sum_{j=0}^{b-1} z^j F\left(\frac{j}{b}, t\right) = \frac{t}{ze^{\frac{t}{b}} - 1}.$$

Since $z \neq 1$, taking the Taylor expansion at $t = 0$ using (62) gives the equality

$$\sum_{j=0}^{b-1} z^j B_n\left(\frac{j}{b}\right) = -\frac{n}{b^{n-1}}\ell_{1-n}(z) \quad \text{for all } n > 1. \qquad \square$$

Proposition 7.5. *Let $n > 1$, $a, b \in \mathbb{N}$.*

(1) *The sum*

$$Y_n(a/b) = f^{n-1} \sum_{j=0}^{f-1} \zeta_{a/b}^{j} B_n\left(\frac{j}{f}\right) \quad \text{for all } f \in b\mathbb{N},\ f \neq 0 \tag{63}$$

only depends upon n and $\frac{a}{b} \in \mathbb{Q}/\mathbb{Z}$.

(2) *One has*

$$\frac{1}{b} \sum_{a=0}^{b-1} Y_n(a/b) = b^{n-1} B_n = b^{n-1} Y_n(0). \tag{64}$$

(3) *For $g \geq 1$, $x^g \neq 1$ one has*

$$\frac{1}{g} \sum_{j=0}^{g-1} \ell_{1-n}(\zeta_{j/g} x) = g^{n-1} \ell_{1-n}(x^g). \tag{65}$$

Proof. (1) Follows from (61). To obtain (2), note that

$$\frac{1}{b} \sum_{a=0}^{b-1} \zeta_{a/b}^{j} = 0 \quad \text{for all } j \neq 0 \ (\mathrm{mod}\ b), \qquad \frac{1}{b} \sum_{a=0}^{b-1} \zeta_{a/b}^{j} = 1 \quad \text{for all } j = 0 \ (\mathrm{mod}\ b).$$

(3) One checks (65) as an identity between rational fractions by induction on $n \in \mathbb{N}$. It holds for $n = 1$ by applying the operation $-z\partial_z \log()$ to both sides of the identity

$$\prod_{j=0}^{g-1} (1 - \zeta_{j/g} z) = 1 - z^g.$$

To obtain (65) for n assuming it for $n-1$ one applies the operation $z\partial_z$ to both sides of the identity for $n-1$. □

Combining (65) with (61) we obtain, using (64) when $\alpha \in \mathbb{Z}$,

$$\frac{1}{b} \sum_{j=0}^{b-1} Y_n\left(\frac{\alpha + j}{b}\right) = b^{n-1} Y_n(\alpha) \quad \text{for all } \alpha \in \mathbb{Q}/\mathbb{Z}. \tag{66}$$

7.3. The linear forms $\varphi_{\beta,\rho}$. In this section we shall provide a meaning to expressions of the form

$$Z_\rho(\tfrac{a}{b}, \beta) = \sum_{m \in I(p)} \rho(\zeta_{a/b}^{m}) m^{-\beta}, \quad \beta \in D_p, \tag{67}$$

where $\frac{a}{b} \in \mathbb{Q}$, $b \in I(p)$ is an integer prime to p and $\rho\colon \mathbb{Q}^{\mathrm{cyc}} \hookrightarrow \mathbb{C}_p$. Note that as a function of $m \in I(p)$, $\rho(\zeta_{a/b}^{m})$ only depends on the residue of m modulo b. We let $f = bp$ and decompose the sum (67) according to the residue α of m modulo f. One has $\mathbb{Z}/f\mathbb{Z} = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$. The elements of $I(p)$ are characterized by the fact that their residues mod. f are given by pairs $\alpha = (\alpha_1, \alpha_2) \in \mathbb{Z}/f\mathbb{Z}$, with $\alpha_1 \neq 0$. For $\alpha \in (\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}/b\mathbb{Z}$, we let $\tilde{\alpha} \in \mathbb{N}$ be the smallest integer with residue modulo f equal to α. Then the sum (67) can be written as

$$Z_\rho(\tfrac{a}{b}, \beta) = \sum_{\alpha} \rho(\zeta^{\alpha}_{a/b}) \sum_{n \geq 0} (\tilde{\alpha} + fn)^{-\beta}, \quad \beta \in D_p. \tag{68}$$

Notice that the first sum (over α) in (68) only involves finitely many terms. Each infinite sum in (68) is of the form (with $z = \tilde{\alpha}/f$)

$$\sum_{n \in \mathbb{N}} (\tilde{\alpha} + fn)^{-\beta} = f^{-\beta} \sum_{n \in \mathbb{N}} (z + n)^{-\beta}, \quad \beta \in D_p,$$

and it is well known that this expression retains a meaning in the p-adic context (cf. [38], Chapter V). More precisely, the asymptotic expansion in the complex case, for $z \to \infty$ (this process goes back to Euler's computation of $\sum_1^\infty n^{-2}$),

$$\sum_{n=0}^{\infty} (z+n)^{-\beta} \sim \frac{z^{1-\beta}}{\beta - 1} \sum_0^\infty \binom{1-\beta}{j} B_j z^{-j}$$

motivates the following precise formula, where we prefer to leave some freedom in the choice of the multiple f of bq.

Lemma 7.6. *With q as in (50) and $f \in \mathbb{N}$, $f \neq 0$, a multiple of bq, the expression*

$$Z_\rho(\tfrac{a}{b}, \beta, f) := \frac{1}{f} \sum_{\substack{1 \leq c < f \\ c \notin p\mathbb{N}}} \rho(\zeta^{c}_{a/b}) \frac{\langle c \rangle^{1-\beta}}{\beta - 1} \sum_{j=0}^{\infty} \binom{1-\beta}{j} \left(\frac{f}{c}\right)^j B_j, \quad \beta \in D_p, \tag{69}$$

defines a meromorphic function of $\beta \in D_p$ with at most a single pole at $\beta = 1$.

Proof. It follows from [38] (Proposition 5.8) and the inequality (cf. [38], Theorem 5.10)

$$\left| \left(\frac{f}{c}\right)^j B_j \right|_p \leq p |f|_p^j$$

that the series

$$\sum_{j=0}^{\infty} \binom{1-\beta}{j} \left(\frac{f}{c}\right)^j B_j$$

converges for $|\beta|_p < |f|_p^{-1} p^{-\frac{1}{p-1}}$ and $|f|_p^{-1} p^{-\frac{1}{p-1}} \geq q p^{-\frac{1}{p-1}} > 1$. □

Lemma 7.7. *For β a negative odd integer of the form $\beta = 1 - m = 1 - k\varphi(q)$ and $f \in \mathbb{N}$, $f \neq 0$, f a multiple of bq, one has*

$$Z_\rho(\tfrac{a}{b}, \beta, f) = -\frac{1}{m}\rho\left(Y_m\left(\frac{a}{b}\right) - p^{m-1}Y_m\left(\frac{pa}{b}\right)\right), \tag{70}$$

with Y_m defined by (63).

Proof. For $1 \leq c < f$, $c \notin p\mathbb{N}$, one has $\langle c\rangle^{1-\beta} = c^m$. The binomial coefficients $\binom{1-\beta}{j}$ in (69) all vanish for $j > m$ and the sum defining $Z(\frac{a}{b}, \beta, f)$ is therefore finite. One has

$$\frac{\langle c\rangle^{1-\beta}}{\beta - 1}\sum_{j=0}^{\infty}\binom{1-\beta}{j}\left(\frac{f}{c}\right)^j B_j = -\frac{c^m}{m}\sum_{j=0}^{m}\binom{m}{j}\left(\frac{f}{c}\right)^j B_j.$$

Moreover for any integer $m > 0$, the Bernoulli polynomials fulfill the equation

$$\sum_{j=0}^{m}\binom{m}{j}z^{-j}B_j = z^{-m}B_m(z).$$

For $1 \leq c < f$, $c \notin p\mathbb{N}$, one thus gets, taking $z = \frac{c}{f}$,

$$\frac{1}{f}\frac{\langle c\rangle^{1-\beta}}{\beta - 1}\sum_{j=0}^{\infty}\binom{1-\beta}{j}\left(\frac{f}{c}\right)^j B_j = -\frac{f^{m-1}}{m}B_m\left(\frac{c}{f}\right).$$

For any $c \in \mathbb{N}$ one defines

$$T(c) := -\frac{f^{m-1}}{m}B_m\left(\frac{c}{f}\right).$$

One has

$$Z_\rho(\tfrac{a}{b}, \beta, f) = \sum_{\substack{1\leq c<f\\ c\notin p\mathbb{N}}} T(c)\rho(\zeta_{a/b}^c) = \sum_{0\leq c<f} T(c)\rho(\zeta_{a/b}^c) - \sum_{\substack{c=jp\\ 0\leq j<f/p}} T(c)\rho(\zeta_{a/b}^c).$$

Since b divides f, one derives

$$\sum_{0\leq c<f} T(c)\rho(\zeta_{a/b}^c) = -\frac{f^{m-1}}{m}\sum_{0\leq c<f}\rho(\zeta_{a/b}^c)B_m\left(\frac{c}{f}\right) = -\frac{1}{m}\rho(Y_m(\zeta_{a/b})),$$

while, since b divides $f/p = f'$, one gets

$$\sum_{\substack{c=jp\\ 0\leq j<f/p}} T(c)\rho(\zeta_{a/b}^c) = -\frac{f^{m-1}}{m}\sum_{0\leq j<f/p}\rho(\zeta_{a/b}^{jp})B_m\left(\frac{j}{f'}\right) = -\frac{p^{m-1}}{m}\rho(Y_m(\zeta_{a/b}^p)).$$

The equality (70) follows. □

Corollary 7.8. *The function*

$$Z_\rho(\tfrac{a}{b},\beta) := Z_\rho(\tfrac{a}{b},\beta,f)$$

is independent of the choice of $f \in bq\mathbb{N}$, $f \neq 0$.

Proof. For two choices f, f' the analytic function of $\beta \in D_p$

$$(\beta-1)(Z_\rho(\tfrac{a}{b},\beta,f) - Z_\rho(\tfrac{a}{b},\beta,f'))$$

vanishes at all negative integers $1-k\varphi(q)$ by the equality (70). Therefore it is identically 0. □

Definition 7.9. The equation

$$\varphi_{\beta,\rho}(\tilde{\mu}_n e(\tfrac{a}{b})\mu_m^*) = \begin{cases} Z_\rho(\tfrac{a}{b},\beta) & \text{if } n=m=1, \\ 0 & \text{otherwise,} \end{cases} \tag{71}$$

defines a linear form $\varphi_{\beta,\rho}$ on $\mathcal{H}_{\mathbb{Z}}^{(p)}$ for any $\beta \in D_p$, where $n, m \in I(p)$ are relatively prime.

The next lemma will play an important role in the proof (cf. next section) that $\varphi_{\beta,\rho}$ fulfills the KMS condition.

Lemma 7.10. *For any $n \in I(p)$ and $\beta \in D_p$, $\beta \neq 1$, one has*

$$\varphi_{\beta,\rho}(\tilde{\rho}_n(X)) = \langle n\rangle^{1-\beta}\varphi_{\beta,\rho}(X) \quad \textit{for all } X \in \mathbb{Z}[(\mathbb{Q}/\mathbb{Z})^{(p)}] \tag{72}$$

(*cf.* (45) *for the definition of $\tilde{\rho}_n$*).

Proof. After multiplication by $\beta-1$, both sides of (72) are analytic functions of $\beta \in D_p$. Thus it is enough to show that (72) holds for $\beta = 1-k\varphi(q) = 1-m$. In this case one has $\langle n\rangle^{1-\beta} = n^m$ and, from (70) one gets

$$\varphi_{\beta,\rho}(e(\gamma)) = -\frac{1}{m}\rho(Y_m(\gamma) - p^{m-1}Y_m(p\gamma)) \quad \text{for all } \gamma \in (\mathbb{Q}/\mathbb{Z})^{(p)}.$$

To prove the equality (72) we can assume that $X = e(\alpha)$ for $\alpha \in (\mathbb{Q}/\mathbb{Z})^{(p)}$. One has

$$\tilde{\rho}_n(X) = \sum_{j=0}^{n-1} e\Big(\frac{\alpha+j}{n}\Big)$$

so that

$$\varphi_{\beta,\rho}(\tilde{\rho}_n(X)) = -\frac{1}{m}\sum_{j=0}^{n-1}\rho\Big(Y_m\Big(\frac{\alpha+j}{n}\Big) - p^{m-1}Y_m\Big(p\frac{\alpha+j}{n}\Big)\Big).$$

Then (72) follows from (66). Since p is prime to n and the rational numbers $p\frac{\alpha+j}{n} \in \mathbb{Q}/\mathbb{Z}$ form the same subset as the set made by the $\frac{p\alpha+j}{n}$, we derive

$$\sum_{j=0}^{n-1} Y_m\left(\frac{\alpha+j}{n}\right) = n^m Y_m(\alpha), \quad \sum_{j=0}^{n-1} Y_m\left(p\frac{\alpha+j}{n}\right) = n^m Y_m(p\alpha). \qquad \square$$

7.4. The KMS$_\beta$ condition. The main result of this section is the following

Theorem 7.11. *For any $\beta \in D_p$, $\beta \neq 1$ and $\rho\colon \mathbb{Q}^{\mathrm{cyc,p}} \hookrightarrow \mathbb{C}_p$, the linear form $\varphi_{\beta,\rho}$ fulfills the KMS$_\beta$ condition*

$$\varphi_{\beta,\rho}(x\sigma^{(\beta)}(y)) = \varphi_{\beta,\rho}(y\,x) \quad \textit{for all } x, y \in \mathcal{H}^{(p)}_{\mathbb{C}_p}. \tag{73}$$

Moreover, the partition function is the p-adic L-function

$$Z(\beta) := \varphi_{\beta,\rho}(1) = L_p(\beta, 1),$$

which does not vanish for $\beta \in D_p$.

Proof. We fix $x, y \in \mathcal{H}^{(p)}_{\mathbb{C}_p}$. Then after multiplication by $\beta - 1$ both sides of (73) are analytic functions of $\beta \in D_p$. We first assume that $\beta \neq 1$; we shall consider the case $\beta = 1$ separately later. Since any element of the algebra $\mathcal{H}^{(p)}_{\mathbb{C}_p}$ can be written as a finite linear combination of $\tilde\mu_n X \mu_m^*$ for $X \in \mathbb{Z}[\mathbb{Q}/\mathbb{Z}]$, we may assume that

$$x = \tilde\mu_n X \mu_m^*, \quad y = \tilde\mu_s Y \mu_t^*,$$

where $n, m \in I(p)$, $(n, m) = 1$, $s, t \in I(p)$, $(s, t) = 1$ and $X, Y \in \mathbb{Z}[\mathbb{Q}/\mathbb{Z}]$. Then we use the presentation of $\mathcal{H}^{(p)}_{\mathbb{C}_p}$ to compute $xy = \tilde\mu_n X \mu_m^* \tilde\mu_s Y \mu_t^*$. Let u be the gcd of $m = um'$ and $s = us'$. One has

$$\mu_m^* \tilde\mu_s = \mu_{m'}^* \mu_u^* \tilde\mu_u \tilde\mu_{s'} = u \mu_{m'}^* \tilde\mu_{s'} = u \tilde\mu_{s'} \mu_{m'}^*,$$
$$\tilde\mu_n X \mu_m^* \tilde\mu_s Y \mu_t^* = u \tilde\mu_n X \tilde\mu_{s'} \mu_{m'}^* Y \mu_t^* = u \tilde\mu_n \tilde\mu_{s'} \sigma_{s'}(X) \sigma_{m'}(Y) \mu_{m'}^* \mu_t^*.$$

Let v be the gcd of $ns' = vw$ and $m't = vz$. One has

$$\tilde\mu_n \tilde\mu_{s'} = \tilde\mu_w \tilde\mu_v, \quad \mu_{m'}^* \mu_t^* = \mu_v^* \mu_z^*,$$
$$\tilde\mu_n X \mu_m^* \tilde\mu_s Y \mu_t^* = u \tilde\mu_w \tilde\mu_v \sigma_{s'}(X) \sigma_{m'}(y) \mu_v^* \mu_z^* = u \tilde\mu_w \tilde\rho_v(\sigma_{s'}(X)\sigma_{m'}(Y)) \mu_z^*.$$

We obtain

$$\tilde\mu_n X \mu_m^* \tilde\mu_s Y \mu_t^* = u \tilde\mu_w \tilde\rho_v(\sigma_{s'}(X)\sigma_{m'}(Y)) \mu_z^*, \quad \frac{w}{z} = \frac{n}{m}\frac{s}{t}.$$

It follows that unless $s = m$ and $t = n$ one has $\frac{w}{z} \neq 1$ and

$$\varphi_{\beta,\rho}(x\sigma^{(\beta)}(y)) = \varphi_{\beta,\rho}(y\,x) = 0.$$

Thus we can assume that $s = m$ and $t = n$. Then we have

$$x\sigma^{(\beta)}(y) = m\left(\frac{n}{m}\right)^{(\beta)} \tilde{\mu}_n\, XY\, \mu_n^* = m\left(\frac{n}{m}\right)^{(\beta)} \tilde{\rho}_n(XY)$$

so that, by (72), one derives

$$\varphi_{\beta,\rho}(x\sigma^{(\beta)}(y)) = m\left(\frac{n}{m}\right)^{(\beta)} \langle n\rangle^{1-\beta}\varphi_{\beta,\rho}(XY).$$

Similarly, by applying again (72), one has

$$yx = n\tilde{\mu}_m YX\mu_m^*, \quad \varphi_{\beta,\rho}(y\,x) = n\langle m\rangle^{1-\beta}\varphi_{\beta,\rho}(XY).$$

Thus (73) follows from the equality

$$m\left(\frac{n}{m}\right)^{(\beta)} \langle n\rangle^{1-\beta} = n\langle m\rangle^{1-\beta},$$

which in turn derives from (54) and (55).

Now we turn to the normalization factor (i.e., partition function) in (71), which is given by

$$Z(\beta) := \varphi_{\beta,\rho}(1) = \frac{1}{q}\sum_{\substack{1\le c<q\\ c\notin p\mathbb{N}}} \frac{\langle c\rangle^{1-\beta}}{\beta-1}\sum_{j=0}^{\infty}\binom{1-\beta}{j}\left(\frac{q}{c}\right)^j B_j.$$

This is the p-adic L-function for the character $\chi = 1$ (cf. [38], Chapter 5, Theorem 5.11):

$$Z(\beta) = L_p(\beta, 1).$$

Moreover, notice that the Iwasawa construction of L-functions (cf. [38], Chapter 7, Theorem 7.10) yields a formal power series $\frac{1}{2}g(T) \in \mathbb{Z}_p[[T]]^\times$ such that (with q as in (49)) the following equality holds:

$$L_p(\beta, 1) = g((1+q)^\beta - 1)/(1-(1+q)^{1-\beta}) \quad \text{for all } \beta \in D_p. \tag{74}$$

Since $\frac{1}{2}g(T) \in \mathbb{Z}_p[[T]]^\times$ is invertible (cf. [38], Lemma 7.12), this gives the required result. □

Note that $Z(\beta)$ has a pole at $\beta = 1$, with residue given by

$$\frac{1}{q}\sum_{\substack{1\le c<q\\ c\notin p\mathbb{N}}} 1 = \frac{\varphi(q)}{q} = \frac{p-1}{p}.$$

Proposition 7.12. *When $\beta \to 1$ one has*

$$\lim_{\beta\to 1} Z(\beta)^{-1} Z_\rho(\tfrac{a}{b}, \beta) = \begin{cases} 1 & \text{if } \frac{a}{b} \in \mathbb{Z},\\ 0 & \text{otherwise.}\end{cases}$$

Proof. Assume first that $\frac{a}{b} \notin \mathbb{Z}$. Then $\xi = \rho(\zeta_{a/b})$ is a non-trivial root of unity, whose order $m > 1$ divides b which is prime to p and hence prime to q. Thus using the decomposition $\mathbb{Z}/bq\mathbb{Z} = \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ we get

$$\sum_{\substack{1 \le c < bq \\ c \notin p\mathbb{N}}} \xi^c = \varphi(q) \sum_{n \in \mathbb{Z}/b\mathbb{Z}} \xi^n = 0.$$

If $\frac{a}{b} \in \mathbb{Z}$, the result follows from the above discussion. □

Notice in particular that the limit of the functional values $Z(\beta)^{-1}Z(\frac{a}{b}, \beta)$ as $\beta \to 1$ is independent of values of ρ (i.e., independent of the choice of $\sigma \in X_p$). In the complex case, the functional values for $\beta > 1$, are given by the formula (17). In that case, we shall now check directly that for $\beta \in \mathbb{C}$, $\mathrm{Re}(\beta) > 1$, the functional values determine $\rho\colon \mathbb{Q}^{\mathrm{cyc}} \to \mathbb{C}$ as an embedding of the abstract cyclotomic field $\mathbb{Q}^{\mathrm{cyc}}$ in $\mathbb{C}$.

Lemma 7.13. (1) *Let $\lambda \in \hat{\mathbb{Z}}^*$, $\lambda \neq \pm 1$. Then the graph of the multiplication by λ in $\mathbb{Q}/\mathbb{Z}$ is a dense subset of $\mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$.*

(2) *Let $\theta \in \mathrm{Aut}((\mathbb{Q}/\mathbb{Z})^{(p)})$. Assume that $\theta \notin \{\pm p^{\mathbb{Z}}\}$. Then the graph of θ is dense in $\mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$.*

Proof. (1) The set $G = \{(\alpha, \lambda\alpha) \mid \alpha \in \mathbb{Q}/\mathbb{Z}\}$ is a subgroup of $\mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$ and so is its closure $\bar{G}$. If G were not dense, then there would exist a non-trivial character χ of the compact group $\mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$ whose kernel contains $\bar{G}$. Thus there would exist a non-zero pair $(n, m) \in \mathbb{Z}^2$ such that $n\alpha + m\lambda\alpha \in \mathbb{Z}$ for all $\alpha \in \mathbb{Q}/\mathbb{Z}$. This would imply that the multiplication by $\lambda \in \hat{\mathbb{Z}}^*$ in the group $\mathbb{Q}/\mathbb{Z} = \mathbb{A}_{\mathbb{Q},f}/\hat{\mathbb{Z}}$ ($\mathbb{A}_{\mathbb{Q},f}$ are the finite adèles) ought to fulfill $n\alpha + m\lambda\alpha \in \hat{\mathbb{Z}}$ for all $\alpha \in \mathbb{A}_{\mathbb{Q},f}$. This implies that $(n + m\lambda_p)\alpha \in \mathbb{Z}_p$ for all $\alpha \in \mathbb{Q}_p$ and hence $n + m\lambda_p = 0$ for all primes p. If $n/m \notin \{\pm 1\}$, this contradicts the fact that $\lambda \in \hat{\mathbb{Z}}^*$, i.e., $\lambda_p \in \hat{\mathbb{Z}}_p^*$ for all p.

(2) The group $G_p = \prod_{\ell \neq p} \mathbb{Z}_\ell^*$ is the group of automorphisms of the group $(\mathbb{Q}/\mathbb{Z})^{(p)}$ viewed as the additive group $\Gamma = \bigoplus_{\ell \neq p} \mathbb{Q}_\ell/\mathbb{Z}_\ell$ (cf. Lemma 8.6). Let $\lambda \in G_p$ represent $\theta \in \mathrm{Aut}((\mathbb{Q}/\mathbb{Z})^{(p)})$. Then the same proof as in (1) shows that if the graph of θ is not dense, there exists a non-zero pair $(n, m) \in \mathbb{Z}^2$ such that $n + m\lambda_\ell = 0$ for all primes $\ell \neq p$. It follows that $-n/m \in \{\pm p^{\mathbb{Z}}\}$ and $\theta \in \{\pm p^{\mathbb{Z}}\}$. □

From Lemma 7.13 we derive that if $f : \{z \in \mathbb{C} \mid |z| = 1\} \to \mathbb{C}$ is a continuous non-constant function and $\rho_j : \mathbb{Q}^{\mathrm{cyc}} \to \mathbb{C}$ are injective, an equality of the form

$$f(\rho_1(\zeta_{a/b})) = f(\rho_2(\zeta_{a/b})) \quad \text{for all } a/b \in \mathbb{Q}/\mathbb{Z}$$

necessarily implies that $\rho_2 = \rho_1$ or $\rho_2 = \bar{\rho}_1$. In the latter case one also gets

$$f(\bar{z}) = f(z) \quad \text{for all } z,\ |z| = 1.$$

By uniqueness of the Fourier decomposition, however, this case cannot occur if $f(z) = \sum_{n=1}^{\infty} n^{-\beta} z^n$ for $\mathrm{Re}(\beta) > 1$.

Next we fix an integer $\beta = 1 - m = 1 - k\varphi(q)$, $k > 0$, and we investigate the dependence on ρ in the expressions (70).

For a chosen pair of embeddings ρ, ρ', assume that $Z_\rho(\frac{a}{b}, \beta) = Z_{\rho'}(\frac{a}{b}, \beta)$ holds for all $a/b \in (\mathbb{Q}/\mathbb{Z})^{(p)}$, i.e., the equality holds for all fractions with denominator b prime to p. It follows from (70) that one has (with Fr the Frobenius automorphism of $\widehat{\mathbb{Q}_p^{\mathrm{un}}}$)

$$(1 - p^{m-1}\mathrm{Fr})^{-1} Z_\rho(\tfrac{a}{b}, \beta) = -\frac{b^{m-1}}{m} \sum_{1 \le c \le b} \rho(\zeta_{a/b}^c) B_m\left(\frac{c}{b}\right) \in \widehat{\mathbb{Q}_p^{\mathrm{un}}}.$$

Thus we get, extending the Bernoulli polynomials from the unit interval by periodicity,

$$\sum_{1 \le c \le b} \rho(\zeta_{a/b}^c) B_m(\tfrac{c}{b}) = \sum_{1 \le c \le b} \rho'(\zeta_{a/b}^c)\, B_m(\tfrac{c}{b}) \quad \text{for all } a/b \in (\mathbb{Q}/\mathbb{Z})^{(p)}. \tag{75}$$

Since both ρ and ρ' are isomorphisms of the group of roots of unity in $\mathbb{Q}^{\mathrm{cyc},\mathrm{p}}$ with the group of roots of unity in $\mathbb{C}_p$ of order prime to p, there exists an automorphism $\theta \in \mathrm{Aut}((\mathbb{Q}/\mathbb{Z})^{(p)})$ such that $\rho'(\zeta_{a/b}) = \rho(\zeta_{\theta(a/b)})$ for all $a/b \in (\mathbb{Q}/\mathbb{Z})^{(p)}$. One has

$$\sum_{1 \le c \le b} \rho'(\zeta_{a/b}^c) B_m(\tfrac{c}{b}) = \sum_{1 \le c \le b} \rho(\zeta_{\theta(c/b)}^a) B_m(\tfrac{c}{b}) = \sum_{1 \le c \le b} \rho(\zeta_{a/b}^c) B_m(\theta^{-1}(\tfrac{c}{b})).$$

By uniqueness of the Fourier transform for the finite group $\mathbb{Z}/b\mathbb{Z}$, (75) yields the equality

$$B_m(\theta^{-1}(\tfrac{c}{b})) = B_m(\tfrac{c}{b}) \quad \text{for all } c/b \in (\mathbb{Q}/\mathbb{Z})^{(p)}. \tag{76}$$

Lemma 7.14. *Let $p > 2$ and let $\theta \in \mathrm{Aut}((\mathbb{Q}/\mathbb{Z})^{(p)})$. If $\theta \in \{\pm 1\}$, one has*

$$Z_\rho(\tfrac{a}{b}, \beta) = Z_{\theta \circ \rho}(\tfrac{a}{b}, \beta) \quad \textit{for all } a/b \in (\mathbb{Q}/\mathbb{Z})^{(p)},\ \beta \in D_p. \tag{77}$$

If $\theta \notin \{\pm 1\}$ and $\beta = 1 - m = 1 - k\varphi(q)$, $k > 0$, then the functionals $Z_\rho(\,\cdot\,, \beta)$ and $Z_{\theta \circ \rho}(\,\cdot\,, \beta)$ are distinct.

Proof. To prove (77) we can assume that $\theta = -1$, i.e., that $\theta(\zeta_{a/b}) = \zeta_{a/b}^{-1}$ for all $a/b \in (\mathbb{Q}/\mathbb{Z})^{(p)}$. Then we have $\rho'(\zeta_{a/b}^c) = \rho(\zeta_{a/b}^{b-c})$ with $\rho' = \theta \circ \rho$. Let first $\beta = 1 - m = 1 - k\varphi(q)$. One has

$$\sum_{1 \le c \le b} \rho'(\zeta_{a/b}^c) B_m\left(\frac{c}{b}\right) = \sum_{0 \le c \le b-1} \rho(\zeta_{a/b}^c) B_m\left(\frac{b-c}{b}\right).$$

Since $m = k\varphi(q)$ is even, the Bernoulli polynomial B_m fulfills the equality

$$B_m(1 - x) = B_m(x) \quad \text{for all } m \in 2\mathbb{N}.$$

Thus (77) follows for all values $\beta = 1 - m = 1 - k\varphi(q)$. Since these values admit 0 as an accumulation point, one derives the equality of the analytic functions on their domain D_p.

Now we assume that $\theta \notin \{\pm p^{\mathbb{Z}}\}$. Then it follows from Lemma 7.13 that the graph of θ is dense in $\mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$. Thus (76) implies that $B_m(x)$ is constant, which is a contradiction. It remains to show that for non-zero powers p^a of p one cannot have an equality of the form

$$B_m(x) = B_m(p^a x - [p^a x]) \quad \text{for all } x \in [0, 1],$$

where $[p^a x]$ is the integral part of $p^a x$. In fact, this would imply that $B_m(x) - B_m(p^a x)$ has infinitely many zeros, thus $B_m(x) = B_m(p^a x)$, which is a contradiction. □

7.5. Extension of the KMS$_\beta$ theory to the covering of $\mathbb{C}_p$. In this section we show that the construction of the KMS$_\beta$ states $\varphi_{\beta,\rho}$ for $\beta \in D_p$ extends naturally to the covering of $\mathbb{C}_p$ defined by the group homomorphism

$$M = D(1, 1^-) \ni \lambda \mapsto \beta = \ell(\lambda) = \frac{\log_p \lambda}{\log_p(1+q)} \in \mathbb{C}_p,$$

where $M = D(1, 1^-)$ is the open unit disk in $\mathbb{C}_p$ with radius 1, viewed as a multiplicative group. Up to the normalization factor $\log_p(1+q)$, this group homomorphism coincides with the definition of the Iwasawa logarithm, it is surjective with kernel the subgroup of roots of unity of order a p-power (cf. [33], Theorem on p. 257) and it defines by restriction a bijection

$$\ell\colon \{\lambda \in M \mid |\lambda - 1|_p < p^{-1/(p-1)}\} \xrightarrow{\sim} D_p$$

whose inverse is given by the map

$$D_p \ni \beta \mapsto \psi(\beta) = (1+q)^\beta = \exp(\beta \log_p(1+q)).$$

By construction, this local section is a group homomorphism which allows one to view the additive group D_p as a subgroup of M.

We start by extending the definition of the functions $r^{(\beta)}$, as in (54), which were implemented in the construction of the automorphisms $\sigma^{(\beta)} \in \mathrm{Aut}(\mathcal{H}^{(p)}_{\mathbb{C}_p})$ (cf. Proposition 7.3). For $r \in \mathbb{Z}^\times_{(p)}$ the equality

$$i_p(r) = \frac{\log_p(r)}{\log_p(1+q)} \in \mathbb{Z}_p \tag{78}$$

defines a group homomorphism from $\mathbb{Z}^\times_{(p)}$ to the additive group $\mathbb{Z}_p$.

Lemma 7.15. *For $\beta \in D_p$, $r \in \mathbb{Z}_{(p)}^{\times}$ and $\lambda = (1+q)^{\beta}$ one has*

$$\langle r\rangle^{\beta} = \lambda^{i_p(r)}, \quad r^{(\beta)} = \omega(r)\lambda^{i_p(r)}.$$

Proof. One has $\log_p(r) = i_p(r)\log_p(1+q) \in q\mathbb{Z}_p$. Thus $|\beta \log_p(r)|_p < p^{-1/(p-1)}$ and

$$\langle r\rangle^{\beta} = \exp(\beta \log_p(r)) = \exp(\beta i_p(r)\log_p(1+q)) = (1+q)^{\beta i_p(r)} = \lambda^{i_p(r)}.$$

The second equality follows from the definition (54). □

Proposition 7.3 and its proof thus extend from D_p to M. This means that for $\lambda \in M$ there exists a unique automorphism $\sigma[\lambda] \in \mathrm{Aut}(\mathcal{H}_{\mathbb{C}_p}^{(p)})$ such that

$$\sigma[\lambda](\tilde{\mu}_a e(\gamma)\mu_b^*) = \omega(b/a)\lambda^{i_p(b/a)}\tilde{\mu}_a e(\gamma)\mu_b^* \quad \text{for all } a,b \in I(p),\ \gamma \in (\mathbb{Q}/\mathbb{Z})^{(p)}.$$

Next we extend the construction of the linear forms $\varphi_{\beta,\rho}$ given in §7.3. It is sufficient to extend the definition of the functions

$$Z_\rho(\tfrac{a}{b},\beta) := \frac{1}{f}\sum_{\substack{1\le c<f\\ c\notin p\mathbb{N}}} \rho(\zeta_{a/b}^{c})\frac{\langle c\rangle^{1-\beta}}{\beta-1}\sum_{j=0}^{\infty}\binom{1-\beta}{j}\left(\frac{f}{c}\right)^{j}B_j, \quad \beta \in D_p, \tag{79}$$

of Lemma 7.6 (which we proved to be independent of the choice of $f \neq 0$ multiple of bq). To define the sought for extension it is convenient to express the above function in terms of the p-adic L-functions $L_p(\beta,\chi)$ associated to even Dirichlet characters of conductor f_χ prime to p. By definition, a Dirichlet character χ is a character of the multiplicative group $\hat{\mathbb{Z}}^*$ and its conductor f_χ is the integer such that the kernel of χ is the kernel of the projection $\hat{\mathbb{Z}}^* \to (\mathbb{Z}/f_\chi\mathbb{Z})^*$. The definition of $L_p(\beta,\chi)$ is similar to (79), precisely as follows

$$L_p(\beta,\chi) := \frac{1}{f}\sum_{\substack{1\le c<f\\ c\notin p\mathbb{N}}} \chi(c)\frac{\langle c\rangle^{1-\beta}}{\beta-1}\sum_{j=0}^{\infty}\binom{1-\beta}{j}\left(\frac{f}{c}\right)^{j}B_j, \tag{80}$$

where f is any multiple of pf_χ and where χ has been extended to a periodic function of period f_χ vanishing outside $(\mathbb{Z}/f_\chi\mathbb{Z})^*$. We recall that the L-function $L_p(\beta,\chi)$ is identically zero when the character χ is odd, i.e., when $\chi(-1) = -1$ (cf. [38] Remarks p. 57). Moreover when χ is even, non-trivial, and its conductor is prime to p, there exists an analytic function H_χ on M such that (cf. [38], Theorem 7.10)

$$L_p(\beta,\chi) = H_\chi((1+q)^{\beta}) \quad \text{for all } \beta \in D_p\,. \tag{81}$$

The extension of the functions $Z_\rho(\frac{a}{b},\beta)$ to M is a consequence of the following

Lemma 7.16. *For any $a/b \in (\mathbb{Q}/\mathbb{Z})^{(p)}$ there exists coefficients $c(d,\chi) \in \mathbb{C}_p$ such that*

$$Z_\rho(\tfrac{a}{b},\beta) = \sum_{d|b,\chi} c(d,\chi)L_p(\beta,\chi)d^{-1}\langle d\rangle^{1-\beta}\prod(1-\chi(\ell)\ell^{-1}\langle \ell\rangle^{1-\beta}),$$

where d varies among the divisors of b and, for fixed d, χ varies among the set of Dirichlet characters whose conductor f_χ divides $m = b/d$. The integers ℓ are the primes which divide m/f_χ but not f_χ.

Proof. Let b be an integer prime to p, and $g \in C(\mathbb{Z}/b\mathbb{Z},\mathbb{C}_p)$. The expression

$$Y(g,\beta) := \frac{1}{f}\sum_{\substack{1\le c<f\\ c\notin p\mathbb{N}}} g(c)\frac{\langle c\rangle^{1-\beta}}{\beta-1}\sum_{j=0}^{\infty}\binom{1-\beta}{j}\left(\frac{f}{c}\right)^j B_j, \quad \beta \in D_p,$$

is independent of the choice of the multiple $f \neq 0$ of bq. Let χ be a Dirichlet character (with values in $\mathbb{C}_p$) with conductor f_χ and let m be a multiple of f_χ. Then

$$z(\chi,m)(c) = \begin{cases}\chi(c) & \text{if } c \in (\mathbb{Z}/m\mathbb{Z})^*,\\ 0 & \text{otherwise,}\end{cases}$$

defines a multiplicative map from $\mathbb{Z}/m\mathbb{Z}$ to $\mathbb{C}_p$. If m divides b and one replaces χ with $z(\chi,m)$ in (80), one obtains instead of $L_p(\beta,\chi)$ the function

$$Y(z(\chi,m),\beta) = L_p(\beta,\chi)\prod(1-\chi(\ell)\ell^{-1}\langle \ell\rangle^{1-\beta}), \tag{82}$$

where the integers ℓ are the primes which divide m/f_χ without dividing f_χ. Next define for any divisor d of b and any function $h \in C(\mathbb{Z}/m\mathbb{Z},\mathbb{C}_p)$, $m = b/d$,

$$e_d(h)(a) = \begin{cases}h(a/d) & \text{if } d\,|\,a,\\ 0 & \text{otherwise.}\end{cases}$$

One then gets

$$Y(e_d(h),\beta) = d^{-1}\langle d\rangle^{1-\beta}Y(h,\beta). \tag{83}$$

Thus using (82) and (83) it is enough to prove that for any function $g \in C(\mathbb{Z}/b\mathbb{Z},\mathbb{C}_p)$ there exists coefficients $c(d,\chi) \in \mathbb{C}_p$ such that

$$g(c) = \sum_{d|b,\chi} c(d,\chi)e_d(z(\chi,b/d)).$$

It is in fact enough to check this for $g = \delta_a$ where $a \in \mathbb{Z}/b\mathbb{Z}$. Let then d be the gcd of a and b. One has $\delta_a = e_d(\delta_c)$ where $c = a/d$ is prime to $m = b/d$. Moreover, for any element $c \in (\mathbb{Z}/m\mathbb{Z})^*$ one has

$$\delta_c(x) = \frac{1}{\varphi(m)}\sum_{\chi,f_\chi|m}\chi(c)^{-1}z(\chi,m)(x) \quad \text{for all } x \in \mathbb{Z}/m\mathbb{Z},$$

which gives the required equality. □

We thus obtain the following extension of Theorem 7.11, referring to [38] for the precise meaning of analyticity in this context.

Theorem 7.17. *There exists an analytic family of functionals $\psi_{\lambda,\rho}$, $\lambda \in M$, on $\mathcal{H}_{\mathbb{Z}}^{(p)}$ such that*

- $\psi_{\lambda,\rho}(1) = 1$;
- $\psi_{\lambda,\rho}$ *fulfills the KMS condition*

$$\psi_{\lambda,\rho}(x\sigma[\lambda](y)) = \psi_{\lambda,\rho}(y\,x) \quad \textit{for all } x, y \in \mathcal{H}_{\mathbb{C}_p}^{(p)};$$

- *For $\beta \in D_p$ and $\lambda = (1+q)^\beta$ one has*

$$\psi_{\lambda,\rho} = Z(\beta)^{-1}\varphi_{\beta,\rho}.$$

Proof. It follows from (74) that there exists an analytic function $z(\lambda)$ of $\lambda \in M$ such that

$$Z(\beta)^{-1} = (1+q-\lambda)z(\lambda), \quad \lambda = (1+q)^\beta.$$

By applying (81), Lemma 7.15 and Lemma 7.16, we see that there exists, for $b \in I(p)$ and $a/b \notin \mathbb{Z}$, an analytic function $H_{a,b}(\lambda)$ of $\lambda \in M$ such that

$$Z_\rho(\frac{a}{b}, \beta) = H_{a,b}(\lambda), \quad \lambda = (1+q)^\beta.$$

This proves the existence of the analytic family of functionals $\psi_{\lambda,\rho}$ fulfilling the required conditions. □

8. Extension of the p-adic valuation to $\mathbb{Q}^{\mathrm{cyc}}$

For a global field $\mathbb{K}$ of positive characteristic (i.e., a function field associated to a projective, geometrically connected non-singular curve C over a finite field $\mathbb{F}_q$) it is a well-known fact that the space of valuations of the maximal abelian extension $\mathbb{K}^{\mathrm{ab}}$ of $\mathbb{K}$ has a geometric meaning. In fact, for each finite extension E of $\overline{\mathbb{F}}_q \otimes_{\mathbb{F}_q} \mathbb{K} \subset \mathbb{K}^{\mathrm{ab}}$ the space $\mathrm{Val}(E)$ of (discrete) valuations of E is turned into an algebraic, one-dimensional scheme whose non-empty open sets are the complements of finite subsets $F \subset \mathrm{Val}(E)$. The structure sheaf is locally defined by the intersection $\bigcap_F R$ of the valuation rings inside E. Then the space $\mathrm{Val}(\mathbb{K}^{\mathrm{ab}})$ is the projective limit of the schemes $\mathrm{Val}(E)$, $E \subset \mathbb{K}^{\mathrm{ab}}$.

For the global field $\mathbb{K} = \mathbb{Q}$ of rational numbers, one can consider its maximal abelian extension $\mathbb{Q}^{\mathrm{cyc}}$ as an abstract field (cf. Definition 8.1) and try to follow a similar idea. In Section 9, we will see however that the space $\mathrm{Val}(\mathbb{Q}^{\mathrm{cyc}})$ provides only a rough analogue, in characteristic zero, of $\mathrm{Val}(\mathbb{K}^{\mathrm{ab}})$. This section develops the preliminary step of presenting five different but equivalent descriptions of the space

$\mathrm{Val}_p(\mathbb{Q}^{\mathrm{cyc}})$ of extensions of the p-adic valuation of $\mathbb{Q}$ to the abstract cyclotomic field $\mathbb{Q}^{\mathrm{cyc}}$. The field $\mathbb{Q}^{\mathrm{cyc}}$ is the composite of the field generated by roots of unity of order a p-power and the field $\mathbb{Q}^{\mathrm{cyc,p}}$ generated by the roots of unity of order prime to p. We describe canonical isomorphisms of $\mathrm{Val}_p(\mathbb{Q}^{\mathrm{cyc}})$ with[1]

(1) the space of sequences of irreducible polynomials $P_n(T) \in \mathbb{F}_p[T]$, $n \in \mathbb{N}$, fulfilling the basic conditions of the Conway polynomials (cf. Theorem 8.7);

(2) the space Σ_p of bijections of the monoid $\mathcal{M}(p) = \mu^{(p)} \cup \{0\}$ of roots of unity of order prime to p which commute with their conjugates, as in Definition 8.5 (cf. Proposition 8.8);

(3) the space $\mathrm{Hom}(\mathbb{Q}^{\mathrm{cycl,p}}_{\mathrm{Fr}}, \mathbb{Q}_p)$ of field homomorphisms, where $\mathbb{Q}^{\mathrm{cycl,p}}_{\mathrm{Fr}} \subset \mathbb{Q}^{\mathrm{cyc,p}}$ is the fixed field under the Frobenius automorphism (cf. Proposition 8.12);

(4) the quotient of the space X_p of Definition 4.3 by the action of $\mathrm{Gal}(\bar{\mathbb{F}}_p)$ (cf. Proposition 8.14);

(5) the algebraic spectrum of the quotient algebra $\mathbb{F}_p[(\mathbb{Q}/\mathbb{Z})^{(p)}]/J_p$, where J_p is the reduction modulo p of the cyclotomic ideal (cf. Definition 8.1 and Proposition 8.16).

Incidentally, we notice that (1) describes the link between $\mathrm{Val}_p(\mathbb{Q}^{\mathrm{cyc}})$ and the explicit construction of an algebraic closure $\bar{\mathbb{F}}_p$ of $\mathbb{F}_p$ by means of a sequence of irreducible polynomials over $\mathbb{F}_p$ fulfilling the basic conditions of the Conway polynomials.[2] Theorem 8.7 states that the map which associates to a valuation $v \in \mathrm{Val}_p(\mathbb{Q}^{\mathrm{cyc}})$ the sequence $\{P_n\}$ of characteristic polynomials for the action (by multiplication) of the primitive root $\xi_{\frac{1}{p^n-1}} \in \mathbb{Q}^{\mathrm{cyc,p}}$ on the residue field of the restriction of v to $\mathbb{Q}^{\mathrm{cyc,p}}$, determines a bijection between $\mathrm{Val}_p(\mathbb{Q}^{\mathrm{cyc}})$ and sequences of polynomials in $\mathbb{F}_p[T]$ fulfilling the basic conditions of the Conway polynomials.

Definition 8.1. The abstract cyclotomic field $\mathbb{Q}^{\mathrm{cyc}}$ is the quotient of the group ring $\mathbb{Q}[\mathbb{Q}/\mathbb{Z}]$ by the ideal J generated by the idempotents

$$\pi_n = \frac{1}{n}\sum_{j=0}^{n-1} e\left(\frac{j}{n}\right), \quad n \geq 2.$$

where $e(\frac{j}{n})$ is the canonical element associated to $\frac{j}{n} \in \mathbb{Q}/\mathbb{Z}$.

In general, if we let

$$\sigma_k(x) = \sum_{j=0}^{k-1} x^j,$$

[1] While we believe these results may be known, we give the complete proofs for completeness.

[2] Conway polynomials provide a particular example of such sequence, they are selected using a lexicographic ordering.

then one knows that the n-th cyclotomic polynomial $\Phi_n(x)$ is the gcd of the polynomials $\sigma_m(x^d)$ for $m > 1$, $m|n$ and $d = n/m$. For $x = e(1/n)$, and $n = md$ one has

$$\sigma_m(x^d) = \sum_{j=0}^{m-1} e(j/m) = m\pi_m \in J,$$

thus $\Phi_n(e(1/n)) \in J$. It follows that the homomorphism

$$\rho_0 \colon \mathbb{Q}[\mathbb{Q}/\mathbb{Z}]/J \to \mathbb{C}, \quad \rho_0(e(\gamma)) = e^{2\pi i\gamma}, \tag{84}$$

induces an isomorphism of $\mathbb{Q}^{\text{cyc}}$ with the subfield of $\mathbb{C}$ generated by roots of unity.

Using the identification $\mathbb{Q}/\mathbb{Z} = \mathbb{A}^f_{\mathbb{Q}}/\hat{\mathbb{Z}}$ the group $\hat{\mathbb{Z}}^*$ acts by automorphisms of $\mathbb{Q}/\mathbb{Z}$ and hence by automorphisms of the group ring $\mathbb{Q}[\mathbb{Q}/\mathbb{Z}]$. This action preserves globally the n-torsion in $\mathbb{Q}/\mathbb{Z}$ and hence fixes each of the projection π_n. It follows that it leaves the ideal J globally invariant and hence it induces an action on the quotient field $\mathbb{Q}^{\text{cyc}}$. This action gives the Galois group $G = \text{Gal}(\mathbb{Q}^{\text{cyc}} : \mathbb{Q}) \simeq \hat{\mathbb{Z}}^*$, which acts on roots of unity as it acts on $\mathbb{Q}/\mathbb{Z}$. For each prime p, one has ($\ell =$ rational prime)

$$G = \prod_{\ell} \mathbb{Z}_\ell^* = \mathbb{Z}_p^* \times \prod_{\ell \neq p} \mathbb{Z}_\ell^* = \mathbb{Z}_p^* \times G_p.$$

One lifts $\mathbb{Z}_p^*$ to the subgroup $\mathbb{Z}_p^* \times 1 \subset G$, with all components equal to 1 except at p. This subgroup acts trivially on $(\mathbb{Q}/\mathbb{Z})^{(p)}$. Its fixed subfield $\mathbb{Q}^{\text{cyc,p}} \subset \mathbb{Q}^{\text{cyc}}$ is the subfield of $\mathbb{Q}^{\text{cyc}}$ generated over $\mathbb{Q}$ by the group $\mu^{(p)} \subset \mathbb{Q}^{\text{cyc}}$ of roots of unity of order prime to p. It coincides with the *inertia subfield*

$$\mathbb{Q}^{\text{cyc}} \cap \mathbb{Q}_p^{\text{ur}} \subset \mathbb{Q}^{\text{cyc}}$$

for any extension $v \in \text{Val}_p(\mathbb{Q}^{\text{cyc}})$ of the p-adic valuation to $\mathbb{Q}^{\text{cyc}}$. More precisely, let $(\mathbb{Q}^{\text{cyc}})_v$ be the completion of $\mathbb{Q}^{\text{cyc}}$ for the valuation v. Then one knows that the composite subfield $\mathbb{Q}_p \cdot \mathbb{Q}^{\text{cyc}} \subset (\mathbb{Q}^{\text{cyc}})_v$ is the maximal abelian extension $\mathbb{Q}_p^{\text{ab}}$ of $\mathbb{Q}_p$. This extension is the composite (cf. [35])

$$\mathbb{Q}_p^{\text{ab}} = \mathbb{Q}_p^{\text{ur}} \cdot \mathbb{Q}_{p^\infty},$$

where $\mathbb{Q}_p^{\text{ur}}$ denotes the maximal unramified extension of $\mathbb{Q}_p$ and $\mathbb{Q}_{p^\infty}$ is obtained by adjoining to $\mathbb{Q}_p$ all roots of unity of order a p-power. The translation Theorem of Galois theory gives a canonical isomorphism (by restriction) of Galois groups

$$\text{Gal}(\mathbb{Q}_p^{\text{ab}} : \mathbb{Q}_p) \xrightarrow{\sim} \text{Gal}(\mathbb{Q}^{\text{cyc}} : \mathbb{Q}^{\text{cyc}} \cap \mathbb{Q}_p), \quad \alpha \mapsto \alpha|_{\mathbb{Q}}^{\text{cyc}}. \tag{85}$$

The *decomposition subfield*, $\mathbb{Q}^{\text{cyc}} \cap \mathbb{Q}_p$, is independent of the choice of the valuation $v \in \text{Val}_p(\mathbb{Q}^{\text{cyc}})$ since G is abelian and acts transitively on $\text{Val}_p(\mathbb{Q}^{\text{cyc}})$. More precisely, one has the following classical result.

Proposition 8.2. (1) *The group $G_p = \prod_{\ell \neq p} \mathbb{Z}_\ell^*$ is the group of automorphisms of the group $(\mathbb{Q}/\mathbb{Z})^{(p)}$.*

(2) *The inertia subfield $\mathbb{Q}^{\mathrm{cyc,p}}$ is the fixed subfield of $\mathbb{Z}_p^* \subset G$ and its Galois group is canonically isomorphic to G_p acting on $\mu^{(p)} \subset \mathbb{Q}^{\mathrm{cyc,p}}$ as it acts on $(\mathbb{Q}/\mathbb{Z})^{(p)}$.*

(3) *Let $f_p \in G_p$ be the element of $G_p = \prod_{\ell \neq p} \mathbb{Z}_\ell^*$ with all components equal to p. Then the associated automorphism $\mathrm{Fr} \in \mathrm{Aut}(\mathbb{Q}^{\mathrm{cyc,p}})$ is the unique automorphism which acts by $x \mapsto x^p$ on the multiplicative group $\mu^{(p)} \subset \mathbb{Q}^{\mathrm{cyc,p}}$.*

(4) *The fixed subfield $\mathbb{Q}_{\mathrm{Fr}}^{\mathrm{cycl,p}} \subset \mathbb{Q}^{\mathrm{cyc,p}}$ of Fr is the decomposition subfield $\mathbb{Q}^{\mathrm{cyc}} \cap \mathbb{Q}_p$.*

(5) *The group $G = \mathrm{Gal}(\mathbb{Q}^{\mathrm{cyc}} : \mathbb{Q})$ acts transitively on $\mathrm{Val}_p(\mathbb{Q}^{\mathrm{cyc}})$ with isotropy $\mathbb{Z}_p^* \times f_p^{\hat{\mathbb{Z}}}$, where $f_p^{\hat{\mathbb{Z}}} \subset G_p$ is the closure of $f_p^{\mathbb{Z}}$.*

Proof. (1) Let $\Gamma = (\mathbb{Q}/\mathbb{Z})^{(p)}$ viewed as a discrete group. The Pontrjagin dual $\hat{\Gamma}$ is the product $\prod_{\ell \neq p} \mathbb{Z}_\ell$. We claim that the group of automorphisms of Γ is

$$\mathrm{Aut}(\Gamma) = \prod_{\ell \neq p} \mathbb{Z}_\ell^*. \tag{86}$$

Indeed, one has $\Gamma = \bigoplus_{\ell \neq p} \mathbb{Q}_\ell/\mathbb{Z}_\ell$, so that the dual of Γ is $\prod_{\ell \neq p} \mathbb{Z}_\ell$. This is a compact ring which contains $\mathbb{Z}$ as a dense subring. Thus an automorphism θ of the additive group is characterized by the assignment $a = \theta(1)$ and is given by multiplication by a. Invertibility shows that $a \in \prod_{\ell \neq p} \mathbb{Z}_\ell^*$. This proves (86).

(2) Under the isomorphism (85) the Galois group $\mathrm{Gal}(\mathbb{Q}_{p^\infty} : \mathbb{Q}_p) \simeq \mathbb{Z}_p^*$ becomes the subgroup $\mathbb{Z}_p^* \times 1 \subset G$. The fixed subfield of this subgroup is $\mathbb{Q}^{\mathrm{cyc,p}} \subset \mathbb{Q}^{\mathrm{cyc}}$ and is the inertia subfield of $\mathbb{Q}^{\mathrm{cyc}}$. The quotient $G/\mathbb{Z}_p^*$ is canonically isomorphic to G_p.

(3) Under the isomorphism $\mathrm{Gal}(\mathbb{Q}^{\mathrm{cyc,p}} : \mathbb{Q}) = G_p$ the action of Fr on $\mu^{(p)}$ corresponds to the multiplication by p in $(\mathbb{Q}/\mathbb{Z})^{(p)}$.

(4) The Galois group $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ur}} : \mathbb{Q}_p) \simeq \hat{\mathbb{Z}}$ is topologically generated by the Frobenius automorphism Fr_p whose action on the roots of unity of order prime to p is given by $\mathrm{Fr}_p(\xi) = \xi^p$. Under the isomorphism (85) this automorphism restricts to the automorphism $\mathrm{Fr} \in \mathrm{Aut}(\mathbb{Q}^{\mathrm{cyc,p}})$. Notice that the fields $\mathbb{Q}^{\mathrm{cyc,p}}$ and $\mathbb{Q}_p$ are linearly disjoint over their intersection

$$K = \mathbb{Q}^{\mathrm{cyc,p}} \cap \mathbb{Q}_p = \mathbb{Q}^{\mathrm{cyc}} \cap \mathbb{Q}_p. \tag{87}$$

Then the translation theorem in Galois theory shows that, by restriction to $\mathbb{Q}^{\mathrm{cyc,p}}$, one has an isomorphism

$$\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ur}} : \mathbb{Q}_p) \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}^{\mathrm{cyc,p}} : K), \quad \mathrm{Fr}_p \mapsto \mathrm{Fr}.$$

This shows that K is the fixed subfield $\mathbb{Q}_{\mathrm{Fr}}^{\mathrm{cycl,p}} \subset \mathbb{Q}^{\mathrm{cyc,p}}$ of Fr.

(5) It is well known that the Galois group acts transitively on extensions of a valuation. Moreover the isotropy subgroup is the subgroup of the Galois group corresponding to the decomposition subfield and is hence given by $\mathbb{Z}_p^* \times f_p^{\hat{\mathbb{Z}}}$. □

Corollary 8.3. *The natural map* $\mathrm{Val}_p(\mathbb{Q}^{\mathrm{cyc}}) \to \mathrm{Val}_p(\mathbb{Q}^{\mathrm{cyc,p}})$ *given by restriction of valuations is equivariant and bijective.*

Proof. The restriction map is equivariant for the action of G on both spaces, these actions are transitive and have the same isotropy group so the restriction map is bijective. □

In fact it is worth giving explicitly the unique extension of a valuation $v \in \mathrm{Val}_p(\mathbb{Q}^{\mathrm{cyc,p}})$ to $\mathbb{Q}^{\mathrm{cyc}}$. The latter field is obtained by adjoining to $\mathbb{Q}^{\mathrm{cyc,p}}$ primitive roots of unity of order a power of p, i.e., a solution z of an equation of the form

$$z^{(p-1)p^{m-1}} + z^{(p-2)p^{m-1}} + \cdots + 1 = 0.$$

One writes $z = 1 + \pi$ and finds that the equation fulfilled by π is of Eisenstein type, the constant term being equal to p, and reduces to $\pi^{\varphi(n)} = 0$, modulo p. This shows that

$$v(\pi) = \frac{v(p)}{\varphi(n)}, \quad \varphi(n) = (p-1)p^{m-1}.$$

Then the valuation v, normalized so that $v(p) = 1$, extends uniquely to elements of the extension $\mathbb{Q}^{\mathrm{cyc,p}}[z]$ by setting

$$v(a_0 + a_1\pi + \cdots + a_{\varphi(n)-1}\pi^{\varphi(n)-1}) = \inf_{0\le j<\varphi(n)} \{v(a_j) + \tfrac{j}{\varphi(n)}\}. \tag{88}$$

Remark 8.4. The decomposition subfield $\mathbb{Q}_p \cap \mathbb{Q}^{\mathrm{cyc}}$ is an infinite extension of $\mathbb{Q}$ which contains for instance $\sqrt{n}$ for n a quadratic residue modulo p. Its Galois group $\mathrm{Gal}(\mathbb{Q}_p \cap \mathbb{Q}^{\mathrm{cyc}} : \mathbb{Q})$ is the quotient of G_p by the closure of the group of powers of f_p and is a compact group which contains for each prime $\ell \neq p$ the cyclic group of order $\ell - 1$ coming from the torsion part of $\mathbb{Z}_\ell^*$.

Definition 8.5. Let $\mathcal{M}(p) = \{0\} \cup \mu^{(p)}$ be the monoid obtained by adjoining a zero element to the multiplicative group $\mu^{(p)}$. We denote by Σ_p the set of bijections $s\colon \mathcal{M}(p) \to \mathcal{M}(p)$ which commute with all their conjugates $R \circ s \circ R^{-1}$ under rotations R by elements of $\mu^{(p)}$ and fulfill the relations $s(0) = 1$, $s^p = s \circ s \circ \cdots \circ s =$ id.

The maps s encode the addition of 1 on $\mathcal{M}(p)$ when one enriches the multiplicative structure of the monoid $\mathcal{M}(p)$ with an additive structure turning it to a field of characteristic p (i.e., an algebraic closure of $\mathbb{F}_p$). Notice that using distributivity the addition of 1 encodes the full additive structure (cf. [14]).

Lemma 8.6. *The group* $G_p = \prod_{\ell\neq p} \mathbb{Z}_\ell^*$ *acts transitively on* Σ_p *with isotropy* $f_p^{\hat{\mathbb{Z}}} \subset G_p$.

Proof. We check that G_p acts transitively on Σ_p. Let $s_j \in \Sigma_p$, for $j = 1, 2$ and let $\mathbb{K}(s_j)$ be the two corresponding field structures on $\mathcal{M}(p)$. Then the two fields $\mathbb{K}(s_j)$ are algebraic closures of $\mathbb{F}_p$ and hence they are isomorphic. We let $\theta\colon \mathbb{K}(s_1) \to \mathbb{K}(s_2)$ be such an isomorphism. By construction θ is an automorphism of the multiplicative group $\mu^{(p)}$ and it transports the operation s_1 of addition of 1 in $\mathbb{K}(s_1)$ into the operation s_2 of addition of 1 in $\mathbb{K}(s_2)$. Since the Galois group of $\overline{\mathbb{F}}_p$ is topologically generated by the Frobenius $x \mapsto x^p$ one gets, using Galois theory, that the isotropy of any $s \in \Sigma_p$ is the closure of the group of powers of f_p, i.e., the subgroup $f_p^{\hat{\mathbb{Z}}} \subset G_p$. □

We are now ready to state the main result of this section.

Theorem 8.7. *There is a canonical bijection between* $\mathrm{Val}_p(\mathbb{Q}^{\mathrm{cyc}})$ *and sequences of polynomials* $P_n(T) \in \mathbb{F}_p[T]$ *of degree* $n \geq 1$ *such that*

- *each* $P_n(T)$ *is monic and irreducible,*
- $T \in \mathbb{F}_p[T]/(P_n(T))$ *is a generator of the multiplicative group of the quotient field,*
- $P_m(T^d)$ *is a multiple of* $P_n(T)$ *for any integer* $m|n$ *and* $d = (p^n - 1)/(p^m - 1)$.

Proof. The first step in the proof is to construct a natural map $\mathrm{Val}_p(\mathbb{Q}^{\mathrm{cyc}}) \ni v \mapsto s_v \in \Sigma_p$. We know that $\mathbb{Q}_p \subset (\mathbb{Q}^{\mathrm{cyc}})_v$ and that $\mu^{(p)} \cup \{0\} \subset \mathbb{Q}^{\mathrm{cyc}}$, thus we consider the valuation ring $\mathbb{Z}_p^{\mathrm{ur}} \subset (\mathbb{Q}^{\mathrm{cyc}})_v$ of $\mathbb{Q}_p^{\mathrm{ur}}$. It contains $\mathbb{Z}_p$ and $\mu^{(p)}$. Note that the ring generated by $\mathbb{Z}$ and $\mu^{(p)}$ is the ring of integers of the subfield $\mathbb{Q}^{\mathrm{cyc,p}} \subset \mathbb{Q}^{\mathrm{cyc}}$ generated over $\mathbb{Q}$ by $\mu^{(p)}$. One has the diagram of inclusions

$$\begin{tikzcd}
& (\mathbb{Q}^{\mathrm{cyc}})_v & \mathbb{Q}^{\mathrm{cyc}} \arrow[l] & \\
\overline{\mathbb{F}}_p & \mathbb{Z}_p^{\mathrm{ur}} \arrow[l, "\epsilon"] \arrow[u] & \mathbb{Z}_p^{\mathrm{ur}} \cap \mathbb{Q}^{\mathrm{cyc}} \arrow[l] \arrow[u] & \mu^{(p)} \cup \{0\} \arrow[l] \\
\mathbb{F}_p \arrow[u] & \mathbb{Z}_p \arrow[l, "\epsilon"] \arrow[u] & \mathbb{Z}_p \cap \mathbb{Q}^{\mathrm{cyc}} \arrow[l] \arrow[u] & \tau(\mathbb{F}_p), \arrow[l] \arrow[u]
\end{tikzcd}$$

where $\tau\colon \mathbb{F}_p \to \mathbb{Z}_p$ is the Teichmüller lift. Note that $\tau(\mathbb{F}_p) \subset \mathbb{Z}_p \cap \mathbb{Q}^{\mathrm{cyc}}$ since this lift is formed of roots of unity (of order $p-1$). In the middle line of the above diagram, the composite map ϵ from $\mu^{(p)} \cup \{0\}$ to $\overline{\mathbb{F}}_p$ is an isomorphism of multiplicative monoids. Indeed, the Teichmüller lift $\overline{\mathbb{F}}_p \ni x \mapsto \tau(x) \in \mathbb{Z}_p^{\mathrm{ur}}$ gives the inverse map. Since $\overline{\mathbb{F}}_p$ is a field one can transport its additive structure using ϵ and one obtains a unique element $s_v \in \Sigma_p$ by transporting the operation of addition of 1.

Proposition 8.8. *The map* $\mathrm{Val}_p(\mathbb{Q}^{\mathrm{cyc}}) \ni v \mapsto s_v \in \Sigma_p$ *is a bijection and is equivariant for the action of* $G_p = \mathrm{Gal}(\mathbb{Q}^{\mathrm{cyc,p}} : \mathbb{Q})$.

Proof. The action of G_p on the subset $\mu^{(p)}$ is the one described in Lemma 8.6. This shows that the map $v \mapsto s_v$ is equivariant. Since both spaces $\mathrm{Val}_p(\mathbb{Q}^{\mathrm{cyc}})$ and Σ_p are homogeneous spaces over G_p with the same isotropy groups $p^{\hat{\mathbb{Z}}} \subset G_p$ as follows from Lemmas 8.2 and 8.6, the map $v \mapsto s_v$ is bijective. □

We can produce a concrete construction of the valuation v associated to the map s_v. One first determines v on the subfield $\mathbb{Q}^{\mathrm{cyc,p}} \subset \mathbb{Q}^{\mathrm{cyc}}$. It is enough to determine the valuation v on elements of the form

$$x = \sum n_j \xi_j, \quad n_j \in \mathbb{Z},\ \xi_j \in \mu^{(p)} \subset \mathbb{Q}^{\mathrm{cyc}}.$$

Let $K = \bar{\mathbb{F}}_p$ be the algebraic closure of $\mathbb{F}_p$ obtained by endowing the multiplicative monoid $\mu^{(p)} \cup \{0\}$ with the addition associated to s_v. One then has

$$v(x) = w_p\big(\sum n_j \tau(\xi_j)\big),$$

where w_p is the p-adic valuation in the Witt ring $\mathbb{W}_{p^\infty}(K)$ and τ the Teichmüller lift. Finally since the field $\mathbb{Q}^{\mathrm{cyc}}$ is the composite of the subfields $\mathbb{Q}^{\mathrm{cyc,p}}$ and the fixed field of the action of $G_p \subset \hat{\mathbb{Z}}^* = \mathrm{Gal}(\mathbb{Q}^{\mathrm{cyc}} : \mathbb{Q})$, which is generated by roots of unity of order a p-power, one can use (88) to extend the valuation v uniquely to $\mathbb{Q}^{\mathrm{cyc}}$.

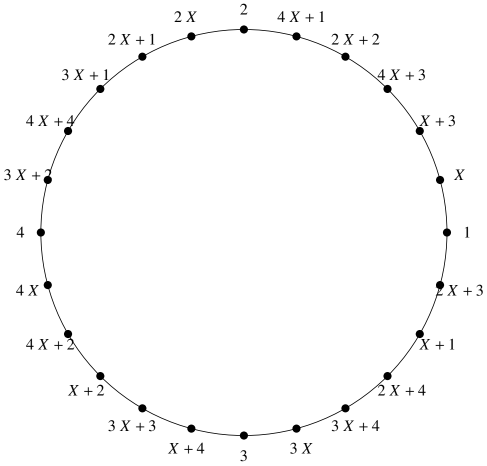

Figure 1. The elements of $\mathbb{F}_{25}$ and roots of unity.

We are now ready to complete the proof of Theorem 8.7, i.e., we prove the following:

Lemma 8.9. *An element $s \in \Sigma_p$ is entirely characterized by a sequence $P_n(T)$ of polynomials of $\mathbb{F}_p[T]$ fulfilling the Conway conditions as in Theorem 8.7.*

Proof. Let $s \in \Sigma_p$. For each $n \in \mathbb{N}$, let $\mathbb{K}_n(s)$ be the corresponding field structure on the union $\{0\} \cup \mu^{(p)}(n)$, where $\mu^{(p)}(n)$ is the group of roots of unity of order $p^n - 1$ in $\mathbb{Q}^{\text{cyc}}$ generated by $\xi = e(\frac{1}{p^n-1})$. The $\mathbb{F}_p$ vector space $\mathbb{K}_n(s)$ is of dimension n since its cardinality is p^n. The canonical generator ξ of $\mu^{(p)}(n)$ acts on the $\mathbb{F}_p$ vector space $\mathbb{K}_n(s)$ by the multiplication M_ξ. We let $P_n(T)$ be its characteristic polynomial, i.e., the determinant $P_n(T) = \det(T - M_\xi)$. It is a monic polynomial of degree n with coefficients in $\mathbb{F}_p$. In the field $\mathbb{K}_n(s)$ one has $P_n(\xi) = 0$, since M_ξ fulfills its characteristic equation. Thus we derive a homomorphism of algebras $\rho\colon \mathbb{F}_p[T]/(P_n(T)) \to \mathbb{K}_n(s)$ which sends $T \mapsto \xi$. It is surjective since any non-zero element of $\mathbb{K}_n(s)$ is a power of ξ. Since $P_n(T)$ has degree n, the two algebras have the same dimension over $\mathbb{F}_p$ and thus ρ is an isomorphism. It follows that $P_n(T)$ is irreducible over $\mathbb{F}_p$. The second property of $P_n(T)$ also follows since ξ is a generator of the multiplicative group. Now let $m \,|\, n$ be a divisor of n. Then $r = p^m - 1$ divides $k = p^n - 1$ and the group $\mu^{(p)}(m)$ is a subgroup of $\mu^{(p)}(n)$. Thus one has a field inclusion $\mathbb{K}_m(s) \subset \mathbb{K}_n(s)$, where the canonical generator $\xi_m = e(\frac{1}{p^m-1})$ of $\mathbb{K}_m(s)$ is sent to ξ_n^d, with ξ_n the canonical generator $\xi_n = e(\frac{1}{p^n-1})$ of $\mathbb{K}_n(s)$ and $d = (p^n - 1)/(p^m - 1)$. One has $P_m(\xi_m) = 0$ and hence $P_m(\xi_n^d) = 0$ so that, using the above isomorphism ρ, it follows that the polynomial $P_m(T^d)$ is a multiple of $P_n(T)$.

Conversely, given a sequence $P_n(T)$ of polynomials fulfilling the conditions of the theorem, one constructs an algebraic closure $\overline{\mathbb{F}}_p$ and an isomorphism

$$\overline{\mathbb{F}}_p^* \xrightarrow{j} \mu^{(p)}$$

as follows. One lets for each n, $\mathbb{K}_n = \mathbb{F}_p[T]/(P_n(T))$ and one gets an inductive system using for $m|n$ the field homomorphism which sends the generator T_m of $\mathbb{K}_m$ to T_n^d, $d = (p^n - 1)/(p^m - 1)$. The inductive limit $\mathbb{K} = \varinjlim \mathbb{K}_n$ is an algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$ and the map $T_n \mapsto e^{2\pi i/k}$, $k = p^n - 1$, defines an isomorphism j of $\overline{\mathbb{F}}_p^*$ with $\mu^{(p)}$. Note that this construction makes sense also for $n = 1$ and that the first polynomial is of degree one and thus picks a specific generator of the multiplicative group of $\mathbb{F}_p$. One checks that the sequence of polynomials associated to the pair $(\overline{\mathbb{F}}_p, j)$ is the sequence $P_n(T)$. Thus there is a complete equivalence between elements $s \in \Sigma_p$ and sequences of polynomials fulfilling the Conway conditions of the theorem. □

To make the above map from Σ_p to sequences of polynomials more explicit we introduce the "trace invariant" of an element $s \in \Sigma_p$. We continue to denote by $\mathbb{K}_n(s)$ the field structure on the union $\{0\} \cup \mu^{(p)}(n)$, where $\mu^{(p)}(n)$ is the group of roots of unity generated by $\xi = e(\frac{1}{p^n-1})$. In particular, $\mathbb{K}_1(s)$ is a field uniquely isomorphic to $\mathbb{F}_p$. Let $\eta \in \mu^{(p)}$. Then the orbit $\mathcal{O} = \{\mathrm{Fr}^k(\eta) \mid k \in \mathbb{N}\}$ of the map $x \mapsto \mathrm{Fr}(x) = x^p$ is a finite set, let $|\mathcal{O}|$ be its cardinality. Then the sum

$$\mathrm{tr}_s(\mathcal{O}) = \sum_{\mathcal{O}} \eta$$

computed in any $\mathbb{K}_n(s)$, for $|\mathcal{O}| \mid n$ is the same and it determines an element of $\mathbb{K}_1(s) = \mathbb{F}_p$.

Definition 8.10. Let $\mathbb{O}(p)$ be the space of orbits of the map $x \mapsto \mathrm{Fr}(x) = x^p$ acting on $\mu^{(p)}$. Let $s \in \Sigma_p$. We call the map

$$\mathrm{tr}_s : \mathbb{O}(p) \to \mathbb{F}_p, \quad \mathcal{O} \mapsto \mathrm{tr}_s(\mathcal{O}),$$

the trace invariant of s.

The trace invariant characterizes s as shown by the next proposition.

Proposition 8.11. *Let $s \in \Sigma_p$. Then for each $n \in \mathbb{N}$ the polynomial $P_n(T) \in \mathbb{F}_p[T]$ associated to s by Lemma 8.9 is given by*

$$P_n(T) = T^n + \sum_{k=1}^{n-1} (-1)^k \sigma_k T^{n-k}$$

for

$$\sigma_k = \sum_{\mathcal{O} \subset D_k} \mathrm{tr}_s(\mathcal{O}), \tag{89}$$

where $D_k \subset (\mathbb{Q}/\mathbb{Z})^{(p)}$ is the set of fractions $\frac{a}{p^n-1}$ where $1 \le a \le p^n - 1$ and the digits of a in base p are all zeros except for k of them which are equal to 1.

Proof. In the field $\mathbb{K}_n(s)$ the n roots of the polynomial $P_n(T)$ are the elements $e(\frac{p^j}{p^n-1})$, for $j = 0, \dots, n-1$. For each $k = 1, \dots, n$, the set of products of k distinct roots is the set of elements of the form

$$e\Big(\sum_{j \in Y} \frac{p^j}{p^n - 1}\Big), \quad Y \subset \{0, 1, \dots, n-1\},\ |Y| = k.$$

One thus gets that the k-th symmetric function σ_k of the roots of $P_n(T)$ is given by the sum (89), over orbits $\mathcal{O}$ satisfying the prescribed condition $\mathcal{O} \subset D_k$. □

We now give a third equivalent description of the space $\mathrm{Val}_p(\mathbb{Q}^{\mathrm{cyc}})$. We recall that the decomposition subfield $\mathbb{Q}_p \cap \mathbb{Q}^{\mathrm{cyc}}$ is independent of the choice of $v \in \mathrm{Val}_p(\mathbb{Q}^{\mathrm{cyc}})$ and is equal to $\mathbb{Q}_{\mathrm{Fr}}^{\mathrm{cycl,p}} \subset \mathbb{Q}^{\mathrm{cyc}}$.

Proposition 8.12. *The map*

$$\beta\colon \mathrm{Val}_p(\mathbb{Q}^{\mathrm{cyc}}) \to \mathrm{Hom}(\mathbb{Q}_{\mathrm{Fr}}^{\mathrm{cycl,p}}, \mathbb{Q}_p), \quad \beta(v) = \beta_v \colon \mathbb{Q}_{\mathrm{Fr}}^{\mathrm{cycl,p}} \subset \mathbb{Q}_p,$$

where the fields inclusion β_v derives from (87), determines a canonical and G_p-equivariant isomorphism of sets.

Proof. Notice that the inclusion $\beta_v : \mathbb{Q}_{\mathrm{Fr}}^{\mathrm{cycl,p}} \subset \mathbb{Q}_p$ depends upon the choice of the valuation v. One has $\beta_v \in \mathrm{Hom}(\mathbb{Q}_{\mathrm{Fr}}^{\mathrm{cycl,p}}, \mathbb{Q}_p)$, and the map $v \mapsto \beta_v$ is equivariant for the action of $G_p/f_p^{\hat{\mathbb{Z}}}$ on $\mathrm{Val}_p(\mathbb{Q}^{\mathrm{cyc}})$ and on the space $\mathrm{Hom}(\mathbb{Q}_{\mathrm{Fr}}^{\mathrm{cycl,p}}, \mathbb{Q}_p)$ by

$$\mathrm{Hom}(\mathbb{Q}_{\mathrm{Fr}}^{\mathrm{cycl,p}}, \mathbb{Q}_p) \ni \beta \mapsto \beta \circ \gamma \quad \text{for all } \gamma \in G_p = \mathrm{Gal}(\mathbb{Q}^{\mathrm{cyc,p}} : \mathbb{Q}).$$

Since for both spaces the action of $G_p/f_p^{\hat{\mathbb{Z}}}$ is free and transitive, it follows that the map β is bijective. □

We let $\mathbb{Z}[(\mathbb{Q}/\mathbb{Z})^{(p)}]$ be the group ring of $(\mathbb{Q}/\mathbb{Z})^{(p)}$ and let $\mathrm{Fr} \in \mathrm{Aut}(\mathbb{Z}[(\mathbb{Q}/\mathbb{Z})^{(p)}])$ be the Frobenius automorphism given by the natural linearization of the group automorphism $(\mathbb{Q}/\mathbb{Z})^{(p)} \to (\mathbb{Q}/\mathbb{Z})^{(p)}$, of multiplication by p (cf. Corollary 2.4). The natural ring homomorphism

$$\delta \colon \mathbb{Z}[(\mathbb{Q}/\mathbb{Z})^{(p)}] \to \mathbb{Q}^{\mathrm{cyc,p}} \tag{90}$$

is equivariant for the action of Fr, its image is the subring of integers of $\mathbb{Q}^{\mathrm{cyc,p}}$ while the kernel is described by the intersection $\mathbb{Z}[(\mathbb{Q}/\mathbb{Z})^{(p)}] \cap J$, where J is the ideal of Definition 8.1. The $\mathbb{F}_p$-algebra

$$\mathbb{Z}[(\mathbb{Q}/\mathbb{Z})^{(p)}] \otimes_{\mathbb{Z}} \mathbb{F}_p = \mathbb{F}_p[(\mathbb{Q}/\mathbb{Z})^{(p)}]$$

is perfect since the group $(\mathbb{Q}/\mathbb{Z})^{(p)}$ is uniquely p-divisible. By restriction to the fixed points of Fr and composition with the residue map $\epsilon \colon \mathbb{Z}_p \to \mathbb{F}_p$, one obtains the map

$$\mathrm{Hom}(\mathbb{Q}_{\mathrm{Fr}}^{\mathrm{cycl,p}}, \mathbb{Q}_p) \to \mathrm{Hom}(\mathbb{F}_p[(\mathbb{Q}/\mathbb{Z})^{(p)}]^{\mathrm{Fr}}, \mathbb{F}_p), \quad \alpha \mapsto \mathrm{res}(\alpha) = \epsilon \circ \alpha \circ \delta. \tag{91}$$

Note that elements of $\mathrm{Hom}(\mathbb{F}_p[(\mathbb{Q}/\mathbb{Z})^{(p)}]^{\mathrm{Fr}}, \mathbb{F}_p)$ are finitely supported maps from $\mathbb{O}(p)$ to $\mathbb{F}_p$, thus they can be lifted to elements of $\mathbb{Z}[(\mathbb{Q}/\mathbb{Z})^{(p)}]^{\mathrm{Fr}}$. One derives

$$\mathbb{F}_p[(\mathbb{Q}/\mathbb{Z})^{(p)}]^{\mathrm{Fr}} = \mathbb{Z}[(\mathbb{Q}/\mathbb{Z})^{(p)}]^{\mathrm{Fr}} \otimes_{\mathbb{Z}} \mathbb{F}_p.$$

Next we show that the map res as in (91) is injective.

Proposition 8.13. *Let $v \in \mathrm{Val}_p(\mathbb{Q}^{\mathrm{cyc}})$. We denote by $s_v \in \Sigma_p$ and $\beta_v \colon \mathbb{Q}_{\mathrm{Fr}}^{\mathrm{cycl,p}} \to \mathbb{Q}_p$ the corresponding elements as in Lemma 8.8 and Proposition 8.12. Then the trace invariant map of s_v has the description*

$$\mathrm{tr}_{s_v} = \mathrm{res}(\beta_v). \tag{92}$$

The map res *as in* (91) *is injective.*

Proof. The additive structure s_v on $\mathcal{M}(p) = \{0\} \cup \mu^{(p)}$ is the same as that of the residue field of the completion $\mathbb{Q}^{\mathrm{cyc,p}}$ for the restriction of v. It follows that on each orbit $\mathcal{O}$ of the action of Fr on $(\mathbb{Q}/\mathbb{Z})^{(p)}$ the sum $\mathrm{tr}_{s_v}(\mathcal{O})$ coincides with the residue

$$\epsilon(\beta_v(u)), \quad u = \sum_{\mathcal{O}} \xi \in \mathbb{Q}_{\mathrm{Fr}}^{\mathrm{cycl,p}}.$$

Since $u = \delta(w)$, where $w = \sum_{\mathcal{O}} \xi \in \mathbb{Z}[(\mathbb{Q}/\mathbb{Z})^{(p)}]^{\mathrm{Fr}}$, one gets (92). Then it follows from Proposition 8.11 that the map res is injective. □

We now briefly explain how one can reconstruct $\alpha \in \mathrm{Hom}(\mathbb{Q}_{\mathrm{Fr}}^{\mathrm{cycl,p}}, \mathbb{Q}_p)$ from its residue $\mathrm{res}(\alpha)$, using the Witt functor $\mathbb{W}_{p^\infty}$. Given $\varsigma \in \mathrm{Hom}(\mathbb{F}_p[(\mathbb{Q}/\mathbb{Z})^{(p)}]^{\mathrm{Fr}}, \mathbb{F}_p)$, the Witt functor $\mathbb{W}_{p^\infty}$ yields a homomorphism

$$\mathbb{W}_{p^\infty}(\varsigma) \in \mathrm{Hom}(\mathbb{W}_{p^\infty}(\mathbb{F}_p[(\mathbb{Q}/\mathbb{Z})^{(p)}]^{\mathrm{Fr}}), \mathbb{Z}_p).$$

If $\varsigma = \mathrm{res}(\alpha)$, one can reconstruct α directly using $\mathbb{W}_{p^\infty}(\varsigma)$. This gives a direct proof of the injectivity of the map res. Indeed, for an orbit $\mathcal{O}$ of the action of Fr on $(\mathbb{Q}/\mathbb{Z})^{(p)}$, the element ($\tau$ = Teichmüller lift)

$$\nu(\mathcal{O}) = \sum_{\mathcal{O}} \tau(\upsilon) \in \mathbb{W}_{p^\infty}(\mathbb{F}_p[(\mathbb{Q}/\mathbb{Z})^{(p)}])$$

is fixed by the Frobenius, i.e., $\nu(\mathcal{O}) \in \mathbb{W}_{p^\infty}(\mathbb{F}_p[(\mathbb{Q}/\mathbb{Z})^{(p)}]^{\mathrm{Fr}})$. One then sees that

$$\alpha(\sum_{\mathcal{O}} \upsilon) = \mathbb{W}_{p^\infty}(\varsigma)(\nu(\mathcal{O})).$$

We end this section by giving the relation between $\Sigma_p = \mathrm{Val}_p(\mathbb{Q}^{\mathrm{cyc}})$ and the space X_p of all injective group homomorphisms $\sigma\colon \bar{\mathbb{F}}_p^\times \to (\mathbb{Q}^{\mathrm{cyc}})^\times$ (cf. Definition 4.3).

We recall that the Galois group $\mathrm{Aut}(\bar{\mathbb{F}}_p)$ is the closure $f_p^{\hat{\mathbb{Z}}}$ of the group generated by the Frobenius f_p.

Proposition 8.14. *Let $\bar{\mathbb{F}}_p$ be a fixed algebraic closure of $\mathbb{F}_p$. Then*

(1) *G_p acts freely and transitively on X_p;*

(2) *the quotient of X_p by $f_p^{\hat{\mathbb{Z}}}$ is isomorphic to $\Sigma_p = \mathrm{Val}_p(\mathbb{Q}^{\mathrm{cyc}})$.*

Proof. Let $\sigma \in X_p$. The range of σ is the group $\mu^{(p)}$ of all roots of unity in $\mathbb{Q}^{\mathrm{cyc}}$ of order prime to p. Thus for a pair $\sigma_j \in X_p$, $j = 1,2$, one has $\sigma_1 \circ \sigma_2^{-1} \in \mathrm{Aut}((\mathbb{Q}/\mathbb{Z})^{(p)}) = G_p$. This proves the first statement.

For any isomorphism $\sigma\colon \bar{\mathbb{F}}_p^* \to (\mathbb{Q}^{\mathrm{cyc}})^\times$ of the multiplicative group of the algebraic closure $\bar{\mathbb{F}}_p$ with the group $(\mathbb{Q}/\mathbb{Z})^{(p)}$, the following defines an element $s \in \Sigma_p$:

$$s(x) = \sigma(\sigma^{-1}(x) + 1) \quad \text{for all } x \neq -1,\ s(-1) = 0.$$

All elements of Σ_p arise this way. Two pairs $(\bar{\mathbb{F}}_p, \sigma_j)$, $j = 1,2$ whose associated $s_j \in \Sigma_p$ are the same are easily seen to be related by an automorphism $\theta \in \mathrm{Aut}(\bar{\mathbb{F}}_p)$, i.e., $\sigma_2 = \sigma_1 \circ \theta$. The second statement thus follows. □

Proposition 8.12 suggests a more appropriate equivalent description of X_p using a chosen algebraic closure $\bar{\mathbb{Q}}_p$ of the p-adic field and its completion $\mathbb{C}_p$.

Corollary 8.15. *The map*

$$i: X_p \to \mathrm{Hom}(\mathbb{Q}^{\mathrm{cyc,p}}, \mathbb{C}_p), \quad \sigma \mapsto \tau \circ \sigma^{-1}, \tag{93}$$

where σ^{-1} is composed with the Teichmüller lift to determine a field homomorphism from $\mathbb{Q}^{\mathrm{cyc,p}}$ to $\mathbb{C}_p$, is a bijection of sets.

The canonical surjection $X_p \to \Sigma_p$ of Proposition 8.14 (2) is the restriction map

$$\mathrm{Hom}(\mathbb{Q}^{\mathrm{cyc,p}}, \mathbb{C}_p) \to \mathrm{Hom}(\mathbb{Q}^{\mathrm{cycl,p}}_{\mathrm{Fr}}, \mathbb{Q}_p). \tag{94}$$

Proof. Let $\sigma \in X_p$, then $\sigma^{-1}: (\mathbb{Q}/\mathbb{Z})^{(p)} \to \bar{\mathbb{F}}_p^{\times}$ composed with the Teichmüller lift $\tau: \bar{\mathbb{F}}_p^{\times} \to \mathcal{O}_{\widehat{\mathbb{Q}_p^{\mathrm{un}}}} \subset \mathbb{C}_p$ extends to a unique homomorphism $i(\sigma) \in \mathrm{Hom}(\mathbb{Q}^{\mathrm{cyc,p}}, \mathbb{C}_p)$. The map i is equivariant for the action of G_p on X_p as in Proposition 8.14 and on $\mathrm{Hom}(\mathbb{Q}^{\mathrm{cyc,p}}, \mathbb{C}_p)$ by composition with elements of $G_p = \mathrm{Gal}(\mathbb{Q}^{\mathrm{cyc,p}} : \mathbb{Q})$. Since both actions are free and transitive, i is bijective.

For any $\gamma \in \mathrm{Hom}(\mathbb{Q}^{\mathrm{cyc,p}}, \mathbb{C}_p)$, the range of γ is the subfield of the maximal unramified extension $\mathbb{Q}_p^{\mathrm{ur}} \subset \mathbb{C}_p$ generated over $\mathbb{Q}$ by roots of unity of order prime to p. One has by construction $\gamma \circ \mathrm{Fr} = \mathrm{Fr}_p \circ \gamma$. Thus the image $\gamma(\mathbb{Q}^{\mathrm{cycl,p}}_{\mathrm{Fr}})$ is contained in the fixed subfield $\mathbb{Q}_p$ for the action of Fr_p on $\mathbb{Q}_p^{\mathrm{ur}}$. This shows that the restriction map (94) is well defined. For $j = 1, 2$, let $\gamma_j \in \mathrm{Hom}(\mathbb{Q}^{\mathrm{cyc,p}}, \mathbb{C}_p)$. Then $\gamma_2^{-1} \circ \gamma_1 \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{cyc,p}} : \mathbb{Q})$ and this automorphism fixes $\mathbb{Q}^{\mathrm{cycl,p}}_{\mathrm{Fr}}$ pointwise if and only the restrictions $\gamma_j|_{\mathbb{Q}^{\mathrm{cycl,p}}_{\mathrm{Fr}}}$ are equal. Since $\mathrm{Gal}(\mathbb{Q}^{\mathrm{cyc,p}} : \mathbb{Q}^{\mathrm{cycl,p}}_{\mathrm{Fr}})$ is topologically generated by Fr, this happens if and only if the γ_j are the same in the quotient of X_p by $f_p^{\hat{\mathbb{Z}}}$. □

We implement the homomorphism $\delta: \mathbb{Z}[(\mathbb{Q}/\mathbb{Z})^{(p)}] \to \mathbb{Q}^{\mathrm{cyc,p}}$ of (90) to associate to an element $\rho \in \mathrm{Hom}(\mathbb{Q}^{\mathrm{cyc,p}}, \mathbb{C}_p)$ its residue

$$\mathrm{res}(\rho) = \epsilon \circ \rho \circ \delta \in \mathrm{Hom}(\mathbb{F}_p[(\mathbb{Q}/\mathbb{Z})^{(p)}], \bar{\mathbb{F}}_p).$$

The image of δ is the ring of integers of $\mathbb{Q}^{\mathrm{cyc,p}}$; thus the image of $\rho \circ \delta$ in $\mathbb{C}_p$ is contained in $\mathcal{O}_{\widehat{\mathbb{Q}_p^{\mathrm{un}}}}$ and the composite $\epsilon \circ \rho \circ \delta$ is well defined. Moreover, since $\mathrm{Ker}(\delta) = J \cap \mathbb{Z}[(\mathbb{Q}/\mathbb{Z})^{(p)}]$, it follows that $\mathrm{Ker}(\mathrm{res}(\rho))$ contains the ideal J_p reduction of $\mathrm{Ker}(\delta)$ modulo p.

Proposition 8.16. *Let $\mathcal{A}$ be the quotient algebra $\mathbb{F}_p[(\mathbb{Q}/\mathbb{Z})^{(p)}]/J_p$. Then*

(1) *the map*

$$\mathrm{res}: \mathrm{Hom}(\mathbb{Q}^{\mathrm{cyc,p}}, \mathbb{C}_p) \to \mathrm{Hom}(\mathcal{A}, \bar{\mathbb{F}}_p), \quad \mathrm{res}(\rho) = \epsilon \circ \rho \circ \delta,$$

is a bijection of sets;

(2) *the algebraic spectrum* $\mathrm{Spec}(\mathcal{A})$ *is in canonical bijection with the set* Σ_p;

(3) *the canonical surjection* $X_p \to \Sigma_p$ *of Proposition* 8.14 (2) *corresponds to the natural map*

$$\mathrm{Hom}(\mathcal{A}, \bar{\mathbb{F}}_p) \to \mathrm{Spec}(\mathcal{A}).$$

Proof. (1) For any integer m prime to p, the ideal J_p contains the projection (cf. Definition 8.1) $\pi_m = \frac{1}{m}\sum_{j=0}^{m-1} e(\frac{j}{m})$. Thus an element $\rho \in \mathrm{Hom}(\mathcal{A}, \bar{\mathbb{F}}_p)$ is given by a group homomorphism $\rho\colon (\mathbb{Q}/\mathbb{Z})^{(p)} \to \bar{\mathbb{F}}_p^{\times}$ such that (for $m > 1$ prime to p) $\sum_{j=0}^{m-1} \rho(e(\frac{j}{m})) = 0$. Notice that this equality holds if and only if ρ is injective and hence, by restriction to the finite level subgroups in the projective limit $(\mathbb{Q}/\mathbb{Z})^{(p)}$, if and only if it is bijective. Thus (1) follows from the first statement of Corollary 8.15.

(2) Consider the finite field $\mathbb{F}_{p^n}$. Two generators of the multiplicative group $\mathbb{F}_{p^n}^{\times}$ have the same characteristic polynomial if and only if they are conjugate under the action of the Galois group $\mathrm{Gal}(\mathbb{F}_{p^n} : \mathbb{F}_p)$. This shows that the cardinality of the set I_n of irreducible monic polynomials of degree n over $\mathbb{F}_p$, whose roots are generators of the multiplicative group, is $\varphi(p^n - 1)/n$, where φ is the Euler totient function. Each of these polynomials $P(X)$ divides the reduction modulo p of the cyclotomic polynomial $\Phi_{p^n-1}(X)$, thus one derives, modulo p, the equality

$$\Phi_{p^n-1}(X) = \prod_{I_n} P(X)$$

since the degrees of the polynomials are the same and the right-hand side divides the left one. Moreover one also has

$$\Phi_{p^n-1}(e(\tfrac{1}{p^n-1})) \in J_p.$$

This determines a canonical isomorphism

$$\mathcal{A}_n = \mathbb{F}_p[\mu^{(p)}(n)]/(J_p \cap \mathbb{F}_p[\mu^{(p)}(n)]) \to \prod_{I_n} \mathbb{F}_{p^n}$$

and thus a canonical bijection of sets $\mathrm{Spec}(\mathcal{A}_n) \to I_n$. Since $\mathcal{A}$ is the inductive limit of the $\mathcal{A}_n$, $\mathrm{Spec}(\mathcal{A})$ is the projective limit of the I_n, i.e., the space of sequences of Conway polynomials as in Theorem 8.7. This space is in canonical bijection with Σ_p.

(3) follows from the proof of (2). □

The restriction to the fixed points of the Frobenius automorphism $\mathrm{Fr} \in \mathrm{Aut}(\mathcal{A})$ does not change the algebraic spectrum as a set, thus we derive a canonical bijection of sets

$$\mathrm{Spec}(\mathcal{A}) \xrightarrow{\sim} \mathrm{Spec}(\mathcal{A}^{\mathrm{Fr}}). \tag{95}$$

Finally, we characterize the image of the map res as in (91).

Corollary 8.17. *Let* $\varsigma \in \mathrm{Hom}(\mathbb{F}_p[(\mathbb{Q}/\mathbb{Z})^{(p)}]^{\mathrm{Fr}}, \mathbb{F}_p)$. *Then* ς *belongs to the image of the map* res *as in* (91) *if and only if* $\mathrm{Ker}(\varsigma)$ *contains* $\mathbb{F}_p[(\mathbb{Q}/\mathbb{Z})^{(p)}]^{\mathrm{Fr}} \cap J_p$.

Proof. By (95) and Proposition 8.16 (2), one has natural bijections of sets

$$\Sigma_p \simeq \mathrm{Spec}(\mathcal{A}) \simeq \mathrm{Spec}(\mathcal{A}^{\mathrm{Fr}}) \simeq \mathrm{Hom}(\mathcal{A}^{\mathrm{Fr}}, \mathbb{F}_p).$$

Then the statement follows by noticing that the elements of $\mathrm{Hom}(\mathcal{A}^{\mathrm{Fr}}, \mathbb{F}_p)$ are the elements of $\mathrm{Hom}(\mathbb{F}_p[(\mathbb{Q}/\mathbb{Z})^{(p)}]^{\mathrm{Fr}}, \mathbb{F}_p)$ whose kernel contains $\mathbb{F}_p[(\mathbb{Q}/\mathbb{Z})^{(p)}]^{\mathrm{Fr}} \cap J_p$. □

9. The base point problem and the "curve" for the global field $\mathbb{Q}$

In this section we compare the space $\mathrm{Val}_p(\mathbb{Q}^{\mathrm{cyc}})$ of extensions of the p-adic valuation to $\mathbb{Q}^{\mathrm{cyc}}$ (studied at length in Section 8), with the fiber over a prime p of a space Y which represents, in this set-up, the analogue of the curve that, for function fields, plays a fundamental role in A. Weil's proof of the Riemann Hypothesis. Our results show that for each place $v \in \Sigma(\mathbb{Q})$, there is a natural model Y_v for the fiber over v and an embedding of this model in a noncommutative space $X(\mathbb{C}_v)$ which is a v-adic avatar of the adèle class space $\mathbb{H}_{\mathbb{Q}} = \mathbb{A}_{\mathbb{Q}}/\mathbb{Q}^*$.

We shall denote by $\mathbb{K}$ a global field. To motivate our constructions we first recall a few relevant facts holding for function fields.

9.1. Adelic interpretation of the loop groupoid $\Pi_1^{\mathrm{ab}}(X)'$ for function fields.

In this subsection we assume that $\mathbb{K}$ is a function field. We let $\mathbb{F}_q \subset \mathbb{K}$ be the field of constants. Let $\bar{\mathbb{K}}$ be a fixed separable closure of $\mathbb{K}$ and let $\mathbb{K}^{\mathrm{ab}} \subset \bar{\mathbb{K}}$ be the maximal abelian extension of $\mathbb{K}$. We denote by $\overline{\mathbb{F}}_q$ the algebraic closure of the finite field $\mathbb{F}_q$ inside $\mathbb{K}^{\mathrm{ab}}$.

A main result holding for function fields is that for each finite field extension E of $\overline{\mathbb{F}}_q \otimes_{\mathbb{F}_q} \mathbb{K}$ the space of (discrete) valuations $\mathrm{Val}(E)$ inherits the structure of an algebraic, one-dimensional scheme X_E whose non-empty open sets are the complements of the finite subsets and whose structure sheaf is defined by considering the intersection of the valuation rings inside E. More precisely, $\mathrm{Val}(E)$ coincides with the set of (closed) points of the unique projective, non-singular algebraic curve X_E over $\overline{\mathbb{F}}_q$ with function field E.

We recall (cf. Corollary 6.12 of [22]) that the category of non-singular, projective algebraic curves over $\overline{\mathbb{F}}_q$ and dominant morphisms is equivalent to the category of function fields of dimension one over $\overline{\mathbb{F}}_q$. Thus, one associates (uniquely) to $\mathbb{K}^{\mathrm{ab}} = \varinjlim_E E$ the projective limit $X^{\mathrm{ab}} = \varprojlim_E X_E$ which is the abelian cover $X^{\mathrm{ab}} \to X$ of the non-singular projective curve X over $\mathbb{F}_q$ with function field $\mathbb{K}$. By restricting valuations, one also derives a natural projection map

$$\pi : X^{\mathrm{ab}} = \mathrm{Val}(\mathbb{K}^{\mathrm{ab}}) \to \Sigma(\mathbb{K})$$

onto the space $\Sigma(\mathbb{K})$ of valuations of $\mathbb{K}$. Thus, in the function field case one derives a geometric interpretation for the natural fibration associated to the space of valuations of the field extension $\mathbb{K}^{\mathrm{ab}} \supset \mathbb{K}$.

In [15] we have given an adelic description of the loop groupoid $\Pi_1^{\mathrm{ab}}(X)'$ of the abelian cover $X^{\mathrm{ab}} \to X$. We recall that the adèle class space $\mathbb{A}_{\mathbb{K}}/\mathbb{K}^*$ of any global field $\mathbb{K}$ has a natural structure of hyperring $\mathbb{H}_{\mathbb{K}}$ (cf. [15]) and that the prime elements $P(\mathbb{H}_{\mathbb{K}})$ of this hyperring determine a groupoid. The units of this groupoid form the set $\Sigma(\mathbb{K})$ of places of $\mathbb{K}$, and the source and range maps coincide with the map

$$s\colon P(\mathbb{H}_{\mathbb{K}}) \to \Sigma(\mathbb{K})$$

which associates to a prime element of $\mathbb{H}_{\mathbb{K}}$ the principal prime ideal of $\mathbb{H}_{\mathbb{K}}$ it generates (and thus the associated place). When $\mathbb{K}$ is a function field, the groupoid $P(\mathbb{H}_{\mathbb{K}})$ is canonically isomorphic to the loop groupoid $\Pi_1^{\mathrm{ab}}(X)'$ of the abelian cover $X^{\mathrm{ab}} \to X$, and the isomorphism is equivariant for the respective actions of the abelianized Weil group $\mathcal{W}^{\mathrm{ab}}$ (i.e., the subgroup of elements of $\mathrm{Gal}(\mathbb{K}^{\mathrm{ab}} : \mathbb{K})$ whose restriction to $\overline{\mathbb{F}}_q$ is an integral power of the Frobenius), and of the idèle class group $C_{\mathbb{K}} = \mathbb{A}_{\mathbb{K}}^*/\mathbb{K}^*$.

It follows that, as a group action on a set, the action of $\mathcal{W}^{\mathrm{ab}}$ on $\mathrm{Val}(\mathbb{K}^{\mathrm{ab}})$ is isomorphic to the action of the idèle class group $C_{\mathbb{K}}$ on $P(\mathbb{H}_{\mathbb{K}})$. In other words, by choosing a set-theoretic section ξ of the projection

$$\pi\colon\ \mathrm{Val}(\mathbb{K}^{\mathrm{ab}}) \to \Sigma(\mathbb{K}), \quad \pi(v) = v|_{\mathbb{K}},$$

one obtains an equivariant set-theoretic bijection $P(\mathbb{H}_{\mathbb{K}}) \simeq_\xi \mathrm{Val}(\mathbb{K}^{\mathrm{ab}})$ which depends though, in a crucial manner, on the choice of the base point $\xi(w)$, for each place $w \in \Sigma(\mathbb{K})$. This dependence prevents one from transporting the algebraic geometric structure of X^{ab} onto $P(\mathbb{H}_{\mathbb{K}})$, and it also shows that the adelic space $P(\mathbb{H}_{\mathbb{K}})$ carries only the information on the curve X^{ab} given in terms of a set with a group action.

9.2. Fiber over a finite place of $\mathbb{Q}$. Now we turn to the global field $\mathbb{K} = \mathbb{Q}$. A natural starting point for the construction of a replacement of the covering X^{ab} in this number field case is to consider the maximal abelian extension of $\mathbb{Q}$, i.e., the cyclotomic field $\mathbb{Q}^{\mathrm{cyc}}$ as analogue of $\mathbb{K}^{\mathrm{ab}}$. Then the space $\mathrm{Val}_p(\mathbb{Q}^{\mathrm{cyc}})$ of extensions of the p-adic valuation to $\mathbb{Q}^{\mathrm{cyc}}$ appears as the first candidate for the analogue of the fiber, over a finite place, of the abelian cover $X^{\mathrm{ab}} \to X$. Thus, the first step is evidently that to compare $\mathrm{Val}_p(\mathbb{Q}^{\mathrm{cyc}})$ with the fiber $P_p(\mathbb{H}_{\mathbb{Q}})$ of the fibration $s\colon P(\mathbb{H}_{\mathbb{Q}}) \to \Sigma(\mathbb{Q})$ over a rational prime $p \in \Sigma(\mathbb{Q})$. At the level of sets with group actions, this process shows that $\mathrm{Val}_p(\mathbb{Q}^{\mathrm{cyc}})$ is not yet the correct fiber. The following discussion indicates that one should consider instead the total space of a principal bundle, with base $\mathrm{Val}_p(\mathbb{Q}^{\mathrm{cyc}})$ and structure group a connected compact solenoid S whose definition is given in Proposition 9.2. Then a natural construction of the fiber is provided by the mapping torus Y_p of the action of the Frobenius on the space X_p of Definition 4.3.

Proposition 9.1. *Let $P_p(\mathbb{H}_{\mathbb{Q}})$ be the fiber of the groupoid $P(\mathbb{H}_{\mathbb{Q}})$ over a non-archimedean, rational prime $p \in \Sigma_{\mathbb{Q}}$. Then the following results hold.*

(1) *The idèle class group $C_{\mathbb{Q}} = \mathbb{A}_{\mathbb{Q}}^*/\mathbb{Q}^*$ acts transitively on $P_p(\mathbb{H}_{\mathbb{Q}})$. The isotropy group of any element of $P_p(\mathbb{H}_{\mathbb{Q}})$ is the cocompact subgroup $W_p = \mathbb{Q}_p^* \subset C_{\mathbb{Q}}$ of classes of idèles (j_v) such that $j_v = 1$ for all $v \neq p$.*

(2) *Under the class field theory isomorphism*

$$\mathrm{Gal}(\mathbb{Q}^{\mathrm{cyc}} : \mathbb{Q}) \simeq C_{\mathbb{Q}}/D_{\mathbb{Q}},$$

where $D_{\mathbb{Q}}$ = *connected component of* 1, $C_{\mathbb{Q}}$ *acts transitively on* $\mathrm{Val}_p(\mathbb{Q}^{\mathrm{cyc}})$ *and the isotropy group of any element of* $\mathrm{Val}_p(\mathbb{Q}^{\mathrm{cyc}})$ *is*

$$I_p = \mathbb{Z}_p^* \times H \times \mathbb{R}_+^* \subset \hat{\mathbb{Z}}^* \times \mathbb{R}_+^* = C_{\mathbb{Q}}.$$

$H \subset G_p = \prod_{\ell \neq p} \mathbb{Z}_\ell^*$ *is the closed subgroup* $p^{\hat{\mathbb{Z}}} \subset G_p$ *generated by* p *in* $G_p = \prod_{\ell \neq p} \mathbb{Z}_\ell^*$.

Proof. (1) follows from Theorem 7.10 of [15]. (2) follows from Lemma 8.2. □

Notice that if $\mathbb{K}$ is a function field and v is a valuation of $\mathbb{K}^{\mathrm{ab}}$ extending the valuation w of $\mathbb{K}$, any $g \in \mathcal{W}^{\mathrm{ab}} \subset \mathrm{Gal}(\mathbb{K}^{\mathrm{ab}} : \mathbb{K})$ such that $g(v) = v$, belongs to the local Weil group $\mathcal{W}_w^{\mathrm{ab}} \subset \mathcal{W}^{\mathrm{ab}}$. This is due to the fact that the restriction of g to an automorphism of $\overline{\mathbb{F}}_q$ is an integral power of the Frobenius.

When $\mathbb{K} = \mathbb{Q}$, the isotropy group of the valuation v is instead larger than the local Weil group W_p. The difference is determined by the presence of the quotient I_p/W_p of the isotropy group I_p by the local Weil group $W_p = \mathbb{Q}_p^* = \mathbb{Z}_p^* \times (\tilde{p})^{\mathbb{Z}}$. Here, $\tilde{p}$ is represented by the idèle all of whose components are 1 except at the place p where it is equal to p^{-1}. By multiplying with the principal idèle p, one gets the same class as the element of $\hat{\mathbb{Z}}^* \times \mathbb{R}_+^*$ which is equal to p everywhere except at the place p where it is equal to 1. Thus, its image in $G_p = \prod_{\ell \neq p} \mathbb{Z}_\ell^*$ is p. The quotient group

$$I_p/W_p = (H \times \mathbb{R}_+^*)/(\tilde{p})^{\mathbb{Z}} \simeq (\hat{\mathbb{Z}} \times \mathbb{R})/\mathbb{Z} = S$$

is a compact connected solenoid which is described in the following Proposition 9.2. The presence of the connected piece S is due to the fact that the connected component of the identity in the idèle class group acts trivially, at the Galois level, on $\mathbb{Q}^{\mathrm{cyc}}$.

Proposition 9.2. *The group* S *is compact and connected and is canonically isomorphic to the projective limit of the compact groups* $\mathbb{R}/n\mathbb{Z}$, *under divisibility of the labels* n.

Proof. We consider first the factor

$$S_n = ((\mathbb{Z}/n\mathbb{Z}) \times \mathbb{R})/\mathbb{Z}$$

of the projective limit S, where $\mathbb{Z}$ acts diagonally, i.e., by the element $(1, 1)$, on $(\mathbb{Z}/n\mathbb{Z}) \times \mathbb{R}$. One has a natural map $p_n : S_n \to \mathbb{R}/n\mathbb{Z}$ given by

$$p_n(j, s) = s - j \quad \text{for all } s \in \mathbb{R},\ j \in \mathbb{Z}/n\mathbb{Z},$$

where one views $\mathbb{Z}/n\mathbb{Z}$ as a subgroup of $\mathbb{R}/n\mathbb{Z}$. The map p_n is an isomorphism of groups. When n divides m, the subgroup $m\mathbb{Z} \subset \mathbb{Z}$ is contained in $n\mathbb{Z} \subset \mathbb{Z}$ and this inclusion corresponds to the projection $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. Under the isomorphisms p_n, this corresponds to the projection $\mathbb{R}/m\mathbb{Z} \to \mathbb{R}/n\mathbb{Z}$. Thus the projective system defining S is isomorphic to the projective system of the projections $\mathbb{R}/m\mathbb{Z} \to \mathbb{R}/n\mathbb{Z}$ and the projective limits are isomorphic. □

Next we describe a general construction of mapping torus which yields, when applied to the groups

$$X = G_p, \quad Z = G_p/p^{\hat{\mathbb{Z}}}, \tag{96}$$

the fiber $P_p(\mathbb{H}_\mathbb{Q})$ of the groupoid $P(\mathbb{H}_\mathbb{Q})$ over a finite, rational prime $p \in \Sigma(\mathbb{Q})$.

Proposition 9.3. *Let $G_p = \prod_{\ell \neq p} \mathbb{Z}_\ell^*$ be the group of automorphisms of the multiplicative group $\mu^{(p)}$ of roots of unity in $\mathbb{Q}^{\mathrm{cyc}}$ of order prime to p and let $f_p \in G_p$ be the element $\xi \mapsto \xi^p$. Let G_p act freely and transitively on a compact space X. Let Y be the quotient space*

$$Y = (X \times (0,1))/\sigma^{\mathbb{Z}},$$

where $\sigma^{\mathbb{Z}}$ acts on the product $X \times (0,1)$ by

$$\sigma(x,\rho) = (f_p x, \rho^p) \quad \textit{for all } x \in X,\ \rho \in (0,1). \tag{97}$$

Then the following results hold.

(1) *The space Y is compact and is an S-principal bundle over the quotient Z of X by $f_p^{\hat{\mathbb{Z}}} \subset G_p$, where S is the solenoid group of Proposition 9.2.*

(2) *Let X and Z be as in (96). Then Y is canonically isomorphic to the fiber $P_p(\mathbb{H}_\mathbb{Q})$.*

Proof. (1) We first look at the action of $\mathbb{Z}$ on the open interval $(0,1)$ given by $\rho \mapsto \rho^p$. We consider the map $\psi\colon (0,1) \to \mathbb{R}$ given by

$$\psi(\rho) = \log(-\log(\rho)) \quad \text{for all } \rho \in (0,1). \tag{98}$$

One has

$$\begin{aligned}\psi(\rho^p) &= \log(-\log(\rho^p))\\ &= \log(-p\log(\rho)) = \log(-\log(\rho)) + \log(p) = \psi(\rho) + \log(p),\end{aligned}$$

which shows that the action of $\mathbb{Z}$ on $(0,1)$ given by $\rho \mapsto \rho^p$ is isomorphic to the action of $\mathbb{Z}$ on $\mathbb{R}$ given by translation by $\log(p)$.

By construction $G_p = \prod_{\ell \neq p} \mathbb{Z}_\ell^*$ is a compact, totally disconnected group. Next we show that the map which associates to $n \in \mathbb{Z}$ the element $f_p^n \in G_p$ extends to a bijection of $\hat{\mathbb{Z}}$ with the closed subgroup of G_p generated by f_p. In fact, the isomorphism follows from the isomorphism between G_p and $\mathrm{Gal}(\bar{\mathbb{F}}_p : \mathbb{F}_p)$, with f_p being the Frobenius. The result follows by applying e.g. [5] (Chapitre V, Appendice II, Exercice 5). This gives a natural inclusion $\hat{\mathbb{Z}} \subset G_p$, $a \mapsto f_p^a$, as a closed subgroup. We now consider the action of the product group $\hat{\mathbb{Z}} \times \mathbb{R}_+^*$ on $X \times (0,1)$ given by

$$(a, \lambda) \cdot (x, \rho) = (f_p^a\, x, \rho^\lambda).$$

By construction the element $(1, p) \in \hat{\mathbb{Z}} \times \mathbb{R}_+^*$ acts as σ (cf. (97)). The quotient group

$$(\hat{\mathbb{Z}} \times \mathbb{R}_+^*)/s^{\mathbb{Z}}, \quad s = (1, p),$$

is isomorphic to the solenoid S by using the isomorphism of the group $\mathbb{R}_+^*$ with $\mathbb{R}$ given by the logarithm in base p. To see that Y is a principal bundle over S one uses the map ψ of (98) to check that S acts freely on Y. The quotient of Y by the action of S is the quotient of X by the action of $\hat{\mathbb{Z}}$.

(2) The fiber $P_p(\mathbb{H}_{\mathbb{Q}})$ has a canonical base point given by the idempotent $u \in P_p(\mathbb{H}_{\mathbb{Q}}), u^2 = u$. Hence by applying Proposition 9.1, this fiber is canonically isomorphic to the quotient $C_{\mathbb{Q}}/W_p$. By identifying $C_{\mathbb{Q}}$ with $\hat{\mathbb{Z}}^* \times \mathbb{R}_+^*$, this quotient coincides with the quotient of $G_p \times \mathbb{R}_+^*$ by the powers of the element $(p, p) \in G_p \times \mathbb{R}_+^*$. Under the bijection $\rho \mapsto -\log(\rho)$ from $(0,1)$ to $\mathbb{R}_+^*$, one obtains the same action as in (97) and hence the desired isomorphism. □

In order to obtain the analogue, for the global field $\mathbb{K} = \mathbb{Q}$, of the fiber of the algebraic curve X^{ab}, we should apply the construction of Proposition 9.3 to a compact space X_p so that the following requirements are satisfied:

(1) G_p acts freely and transitively on X_p.

(2) The quotient of X_p by $f_p^{\hat{\mathbb{Z}}}$ is canonically isomorphic to $\mathrm{Val}_p(\mathbb{Q}^{\mathrm{cyc}})$.

Proposition 8.14 provides a natural candidate for X_p. Moreover, equation (93) shows that one can equivalently describe X_p as the space $\mathrm{Hom}(\mathbb{Q}^{\mathrm{cyc,p}}, \mathbb{C}_p)$ and that the canonical identification of $X_p/f_p^{\hat{\mathbb{Z}}}$ with $\mathrm{Val}_p(\mathbb{Q}^{\mathrm{cyc}})$ is given by the restriction map to the fixed points of Fr as in (94). We derive the definition of the following model for the fiber Y_p over a finite prime p

$$Y_p = (\mathrm{Hom}(\mathbb{Q}^{\mathrm{cyc,p}}, \mathbb{C}_p) \times (0,1))/\sigma^{\mathbb{Z}}. \tag{99}$$

9.3. Fiber over the archimedean place of $\mathbb{Q}$. We move now to the discussion of the analogues of the spaces $\mathrm{Val}_p(\mathbb{Q}^{\mathrm{cyc}})$, X_p and Y_p, when p is the archimedean prime $p = \infty$ (i.e., the archimedean valuation). The space $\mathrm{Val}_\infty(\mathbb{Q}^{\mathrm{cyc}})$ is the space of multiplicative norms on $\mathbb{Q}^{\mathrm{cyc}}$ whose restriction to $\mathbb{Q}$ is the usual absolute value. For $v \in \mathrm{Val}_\infty(\mathbb{Q}^{\mathrm{cyc}})$, the field completion $(\mathbb{Q}^{\mathrm{cyc}})_v$ is isomorphic to $\mathbb{C}$, thus one derives

$$\mathrm{Val}_\infty(\mathbb{Q}^{\mathrm{cyc}}) = \mathrm{Hom}(\mathbb{Q}^{\mathrm{cyc}}, \mathbb{C})/\{\pm 1\},$$

where $\{\pm 1\} \subset \hat{\mathbb{Z}}^* = \mathrm{Gal}(\mathbb{Q}^{\mathrm{cyc}} : \mathbb{Q})$ corresponds to complex conjugation. It follows that for $p = \infty$ the space X_p is simply

$$X_\infty = \mathrm{Hom}(\mathbb{Q}^{\mathrm{cyc}}, \mathbb{C}).$$

On the other hand, the fiber $P_\infty(\mathbb{H}_\mathbb{Q})$ is the quotient $C_\mathbb{Q}/W_\infty$, where $W_\infty = \mathbb{R}^*$ is the cocompact subgroup of $C_\mathbb{Q}$ given by classes of idèles whose components are all 1 except at the archimedean place. Then we derive that

$$P_\infty(\mathbb{H}_\mathbb{Q}) = \hat{\mathbb{Z}}^*/\{\pm 1\}.$$

This discussion shows that at $p = \infty$ there is no need for a mapping torus, and that the expected fiber is simply given by

$$Y_\infty = \mathrm{Val}_\infty(\mathbb{Q}^{\mathrm{cyc}}) = \mathrm{Hom}(\mathbb{Q}^{\mathrm{cyc}}, \mathbb{C})/\{\pm 1\} = X_\infty/\{\pm 1\}. \tag{100}$$

9.4. Ambient noncommutative space. The model (99) for the fiber over a rational prime p is only a preliminary step toward the global construction of the "curve" which we expect to replace, when $\mathbb{K} = \mathbb{Q}$, the geometric cover X^{ab}. In fact, one still needs to suitably combine these models into a noncommutative space to account for the presence of transversality factors in the explicit formulas. We explain why in some details below.

In [11] we showed how to determine the counting function $N(q)$ (a distribution on $[1,\infty)$) which replaces, for $\mathbb{K} = \mathbb{Q}$, the classical Weil counting function for a field $\mathbb{K}$ of functions of an algebraic curve Y over $\mathbb{F}_p$ (cf. [28], [36]). The Weil counting function determines the number of rational points on the curve Y defined over field extensions $\mathbb{F}_q$ of $\mathbb{F}_p$

$$\#Y(\mathbb{F}_q) = N(q) = q - \sum_\alpha \alpha^r + 1, \quad q = p^r.$$

The numbers α's are the complex roots of the characteristic polynomial of the Frobenius endomorphism acting on the étale cohomology $H^1(Y \otimes \bar{\mathbb{F}}_p, \mathbb{Q}_\ell)$, for $\ell \neq p$. In [11] we have shown that the distribution $N(q)$ associated to the (complete) Riemann zeta function is described by the similar formula

$$N(u) = u - \frac{d}{du}\Big(\sum_{\rho \in Z} \mathrm{order}(\rho)\frac{u^{\rho+1}}{\rho+1}\Big) + 1,$$

where Z is the set of non-trivial zeros of the Riemann zeta function. This distribution is positive on $(1,\infty)$ and fulfills all the expected properties of a counting function. In particular, it takes the correct value $N(1) = -\infty$ in agreement with the (expected) value of the Euler characteristic. In [12] we pushed these ideas further and we explained how to implement the trace formula understanding of the explicit formulas in number-theory, to express the distribution $N(q)$ as an *intersection number* involving the scaling action of the idèle class group on the adèle class space. This development involves a Lefschetz formula whose geometric side corresponds to the following expression of the counting distribution $N(u)$:

$$N(u)=\frac{d}{du}\varphi(u)+\kappa(u), \quad \varphi(u)=\sum_{n<u} n\,\Lambda(n). \tag{101}$$

Here, $\Lambda(n)$ is the von Mangoldt function taking the value $\log p$ at prime powers p^ℓ and zero otherwise and $\kappa(u)$ is the distribution defined, for any test function f, by

$$\int_1^\infty \kappa(u)f(u)d^*u=\int_1^\infty \frac{u^2f(u)-f(1)}{u^2-1}d^*u+cf(1), \quad c=\frac{1}{2}(\log\pi+\gamma),$$

where $\gamma=-\Gamma'(1)$ is the Euler constant. The distribution $\kappa(u)$ is positive on $(1,\infty)$ and in this domain it is equal to the function $\kappa(u)=\frac{u^2}{u^2-1}$. The contribution in the counting distribution $N(u)$ coming from the term $\frac{d}{du}\varphi(u)$ in (101) can be understood geometrically as arising from a counting process performed on the fibers Y_p (each of them accounting for the delta functions located on the powers of p). The value $\log(p)$ coming from the von Mangoldt function $\Lambda(n)$ corresponds to the length of the orbit in the mapping torus (cf. [12], §2.2). On the other hand, as explained in [12], the contribution of the archimedean place cannot be understood in a naive manner as a simple counting process of points and its expression involves a transversality factor measuring the transversality of the action of the idèle class group with respect to periodic orbits. This shows that the periodic orbits cannot be considered in isolation and must be thought of as (suitably) embedded in the ambient adèle class space. This development supplies a precious hint toward the final construction of the “curve” and shows that the role of ergodic theory and noncommutative geometry is indispensable.

9.5. The BC-system over $\mathbb{Z}$ and $\mathbb{F}_{1^\infty}\otimes_{\mathbb{F}_1}\mathbb{Z}$. Next we shall explain how the BC-system over $\mathbb{Z}$ gives, for each p, a natural embedding of the fiber Y_p (cf. (100)) into a noncommutative space constructed using the set $\mathcal{E}(\mathbb{C}_p)$ of the $\mathbb{C}_p$-rational points of the affine group scheme $\mathcal{E}$ which describes the abelian part of the system (cf. [16]). Since the fields $\mathbb{C}_p$ are abstractly pairwise isomorphic the obtained spaces are also abstractly isomorphic, but in a non-canonical manner. In [16], following a proposal of C. Soulé for the meaning of the ring $\mathbb{F}_{1^n}\otimes_{\mathbb{F}_1}\mathbb{Z}$, we noted that the inductive limit

$$\mathbb{F}_{1^\infty}\otimes_{\mathbb{F}_1}\mathbb{Z}:=\varinjlim_n \mathbb{F}_{1^n}\otimes_{\mathbb{F}_1}\mathbb{Z}=\mathbb{Z}[\mathbb{Q}/\mathbb{Z}]$$

coincides with the abelian part of the algebra defining the integral BC-system. The description given in that paper of the BC-system as an affine pro-group scheme $\mathcal{E}$ over $\mathbb{Z}$, together with the dynamic of the action of a semigroup of endomorphisms, allows one to consider its rational points over any ring, A

$$\mathcal{E}(A)=\mathrm{Hom}(\mathbb{Z}[\mathbb{Q}/\mathbb{Z}],A)\,.$$

Then one can implement, for each rational prime p, the canonical inclusion

$$X_p = \mathrm{Hom}(\mathbb{Q}^{\mathrm{cyc,p}}, \mathbb{C}_p) \subset \mathrm{Hom}(\mathbb{Z}[\mathbb{Q}/\mathbb{Z}], \mathbb{C}_p) = \mathcal{E}(\mathbb{C}_p). \tag{102}$$

The next result shows that the space

$$X(\mathbb{C}_p) := (\mathcal{E}(\mathbb{C}_p) \times (0,\infty))/(\mathbb{N} \times \{\pm 1\}) \tag{103}$$

matches, for any p including $p = \infty$, the definition of the adèle class space $\mathbb{H}_{\mathbb{Q}}$. The action of $m = \pm n$ (in the semigroup $\mathbb{N} \times \{\pm 1\}$) is the product of the linearization of the action $e(\gamma) \mapsto e(m\gamma)$ on the ($\mathbb{C}_p$-rational points of the) scheme $\mathcal{E}$, with the action on $(0,\infty)$ given by the map $x \mapsto x^m$.

Proposition 9.4. (1) *The space $X(\mathbb{C})$ is canonically isomorphic to the adèle class space $\mathbb{H}_{\mathbb{Q}}$.*

(2) *The subspace of the adèle class space made by classes whose archimedean component vanishes corresponds to the quotient*

$$\mathcal{E}(\mathbb{C})/(\mathbb{N} \times \{\pm 1\}) = \hat{\mathbb{Z}}/(\mathbb{N} \times \{\pm 1\}).$$

Proof. (1) The space $\mathcal{E}(\mathbb{C})$ is the space of complex characters of the abelian group $\mathbb{Q}/\mathbb{Z}$ and is canonically isomorphic to $\hat{\mathbb{Z}}$. We use the map $\rho \mapsto -\log(\rho)$ to map the interval $(0,\infty)$ to $\mathbb{R}$. Under this map the transformation $x \mapsto x^m$ becomes the multiplication by m. The action $e(\gamma) \mapsto e(m\gamma)$ on the scheme $\mathcal{E}$ corresponds to the multiplication by m in $\hat{\mathbb{Z}}$. Since any adèle class is equivalent to an element of $\hat{\mathbb{Z}} \times \mathbb{R}$, (103) gives, for $p = \infty$,

$$X(\mathbb{C}) = (\hat{\mathbb{Z}} \times \mathbb{R})/(\mathbb{N} \times \{\pm 1\}) = \mathbb{A}_{\mathbb{Q}}/\mathbb{Q}^* = \mathbb{H}_{\mathbb{Q}}. \tag{104}$$

(2) follows from the identification (104). □

Note that by using the inclusion $(0,1) \subset (0,\infty)$, one derives a natural inclusion

$$Y_p = (\mathrm{Hom}(\mathbb{Q}^{\mathrm{cyc,p}}, \mathbb{C}_p) \times (0,1))/\sigma^{\mathbb{Z}} \to (\mathcal{E}(\mathbb{C}_p) \times (0,\infty))/(\mathbb{N} \times \{\pm 1\}) = X(\mathbb{C}_p).$$

For $p = \infty$ one has the natural inclusion

$$Y_\infty = \mathrm{Hom}(\mathbb{Q}^{\mathrm{cyc}}, \mathbb{C})/\{\pm 1\} \to (\mathcal{E}(\mathbb{C}) \times (0,\infty))/(\mathbb{N} \times \{\pm 1\}) = X(\mathbb{C}),$$

which is obtained by using the canonical inclusion (102) for $p = \infty$ and the fixed point $1 \in (0,\infty)$.

The group ring $\mathbb{Z}[\mathbb{Q}/\mathbb{Z}]$ is a Hopf algebra for the coproduct,

$$\Delta(e(\gamma)) = e(\gamma) \otimes e(\gamma) \quad \text{for all } \gamma \in \mathbb{Q}/\mathbb{Z},$$

and the antipode $e(\gamma) \mapsto e(-\gamma)$, thus $\mathcal{E}$ is a group scheme.

Proposition 9.5. *Let A be a commutative ring.*

(1) *The abelian group $\mathcal{E}(A)$ is torsion-free.*

(2) *The space*

$$X(A) = (\mathcal{E}(A) \times (0,\infty))/(\mathbb{N} \times \{\pm 1\}) \tag{105}$$

is a module over the hyperring $\mathbb{H}_{\mathbb{Q}}$.

(3) *For any rational prime p, $X(\mathbb{C}_p)$ is a free module of rank one over $\mathbb{H}_{\mathbb{Q}}$.*

Proof. (1) One has

$$\mathcal{E}(A) = \operatorname{Hom}(\mathbb{Z}[\mathbb{Q}/\mathbb{Z}], A) = \operatorname{Hom}(\mathbb{Q}/\mathbb{Z}, A^\times),$$

where the second Hom is taken in the category of abelian groups. Since the group $\mathbb{Q}/\mathbb{Z}$ is divisible, the group $\operatorname{Hom}(\mathbb{Q}/\mathbb{Z}, H)$ has no torsion for any abelian group H.

(2) We first show that $X(A)$ is a hypergroup and in fact a vector space over the Krasner hyperfield $\mathbf{K} = \{0,1\}$ (cf. [15]). The two abelian groups $\mathcal{E}(A)$ and $(0,\infty)$ are both torsion-free, thus one gets

$$(\mathcal{E}(A) \times (0,\infty))/(\mathbb{N} \times \{\pm 1\}) = ((\mathcal{E}(A) \times (0,\infty)) \otimes_{\mathbb{Z}} \mathbb{Q})/\mathbb{Q}^\times, \tag{106}$$

which is a projective space, hence a vector space over $\mathbf{K}$ (cf. [15]). Next we show that $X(A)$ is a module over $\mathbb{H}_{\mathbb{Q}}$. We use the canonical ring isomorphism $\hat{\mathbb{Z}} = \operatorname{End}_{\mathbb{Z}}(\mathbb{Q}/\mathbb{Z})$ to define the ring homomorphism

$$c_A\colon \hat{\mathbb{Z}} \to \operatorname{End}_{\mathbb{Z}}(\mathcal{E}(A)), \quad c_A(\alpha)\xi = \xi \circ \alpha \quad \text{for all } \xi \in \operatorname{Hom}(\mathbb{Q}/\mathbb{Z}, A^\times),$$

from $\hat{\mathbb{Z}}$ to the ring $\operatorname{End}_{\mathbb{Z}}(\mathcal{E}(A))$. The map

$$p\colon \mathbb{R} \to \operatorname{End}_{\mathbb{Z}}(\mathbb{R}_+^*), \quad p(\lambda)x = x^\lambda,$$

is a ring homomorphism, thus $c_A \times p$ defines a ring homomorphism from $\hat{\mathbb{Z}} \times \mathbb{R}$ to the endomorphisms of the abelian group $\mathcal{E}(A) \times (0,\infty)$. For any $m \in \mathbb{Z} \subset \hat{\mathbb{Z}} \times \mathbb{R}$, one has

$$(c_A \times p)(m)((e(\gamma), x)) = (e(m\gamma), x^m),$$

thus the restriction of $c_A \times p$ to the monoid of non-zero elements of $\mathbb{Z}$ gives the equivalence relation which defines $X(A)$ as in (105). It follows an action of the hyperring

$$((\hat{\mathbb{Z}} \times \mathbb{R}) \otimes_{\mathbb{Z}} \mathbb{Q})/\mathbb{Q}^\times = \mathbb{A}_{\mathbb{Q}}/\mathbb{Q}^\times = \mathbb{H}_{\mathbb{Q}}$$

on the hypergroup (106).

(3)It is easy to see that, once one fixes an embedding $\rho\colon \mathbb{Q}^{\mathrm{cyc}} \to \mathbb{C}_p$ and an $x \in (0,\infty)$ and a real number $x \neq 1$, the element $(\rho, x) \in X(\mathbb{C}_p)$ is a generator of $X(\mathbb{C}_p)$ as a free module over $\mathbb{H}_{\mathbb{Q}}$. □

The next lemma provides some simple arithmetic-geometric properties of the scheme $\mathcal{E}$.

Lemma 9.6. (1) *Let $\mathbb{Q}_p^{\mathrm{ab}} \subset \mathbb{C}_p$ be the maximal abelian extension of $\mathbb{Q}_p$. Then the natural map $\mathcal{E}(\mathbb{Q}_p^{\mathrm{ab}}) \to \mathcal{E}(\mathbb{C}_p)$ is a bijection of sets.*

(2) *Let $\mathbb{Q}_p^{\mathrm{ur}} \subset \mathbb{Q}_p^{\mathrm{ab}}$ be the maximal unramified extension of $\mathbb{Q}_p$ and $\mathbb{Z}_p^{\mathrm{ur}} \subset \mathbb{Q}_p^{\mathrm{ur}}$ the valuation ring of the p-adic valuation. Then the natural map $\mathcal{E}(\mathbb{Z}_p^{\mathrm{ur}}) \to \mathcal{E}(\mathbb{Q}_p^{\mathrm{ur}})$ is a bijection of sets.*

(3) *Let $\epsilon\colon \mathbb{Z}_p^{\mathrm{ur}} \to \bar{\mathbb{F}}_p$ be the residue homomorphism. Then the associated map $\mathcal{E}(\mathbb{Z}_p^{\mathrm{ur}}) \to \mathcal{E}(\bar{\mathbb{F}}_p)$ is a bijection.*

Proof. (1) Let $\rho \in \mathcal{E}(\mathbb{C}_p) = \mathrm{Hom}(\mathbb{Z}[\mathbb{Q}/\mathbb{Z}], \mathbb{C}_p)$. Then the image of ρ is contained in the subfield of $\mathbb{C}_p$ generated over $\mathbb{Q}$ by roots of unity, which is contained in $\mathbb{Q}_p^{\mathrm{ab}}$.

(2) Let $\rho \in \mathcal{E}(\mathbb{Q}_p^{\mathrm{ur}}) = \mathrm{Hom}(\mathbb{Z}[\mathbb{Q}/\mathbb{Z}], \mathbb{Q}_p^{\mathrm{ur}})$. Then the image of ρ is contained in the subring of $\mathbb{Q}_p^{\mathrm{ur}}$ generated over $\mathbb{Z}$ by roots of unity (of order prime to p), which is contained in $\mathbb{Z}_p^{\mathrm{ur}}$.

(3) Let $\rho \in \mathcal{E}(\mathbb{Z}_p^{\mathrm{ur}}) = \mathrm{Hom}(\mathbb{Z}[\mathbb{Q}/\mathbb{Z}], \mathbb{Z}_p^{\mathrm{ur}})$. Then ρ is entirely characterized by the group homomorphism

$$\rho\colon \mathbb{Q}/\mathbb{Z} \to G,$$

where G is the group of roots of unity in $\mathbb{Z}_p^{\mathrm{ur}}$, which is non-canonically isomorphic to the group $\mu^{(p)}$ of abstract roots of unity of order prime to p. Similarly an element of $\mathcal{E}(\bar{\mathbb{F}}_p) = \mathrm{Hom}(\mathbb{Z}[\mathbb{Q}/\mathbb{Z}], \bar{\mathbb{F}}_p)$ is entirely characterized by the associated group homomorphism from $\mathbb{Q}/\mathbb{Z}$ to $\bar{\mathbb{F}}_p^*$. Since the residue morphism ϵ gives an isomorphism $G \xrightarrow{\simeq} \bar{\mathbb{F}}_p^*$, one obtains the conclusion. □

We can now describe the structure of the $\mathbb{H}_{\mathbb{Q}}$-module $X(\bar{\mathbb{F}}_p)$.

Proposition 9.7. (4) *The $\mathbb{H}_{\mathbb{Q}}$-module*

$$X(\bar{\mathbb{F}}_p) \simeq X(\mathbb{Z}_p^{\mathrm{ur}}) \simeq X(\mathbb{Q}_p^{\mathrm{ur}}) \subset X(\mathbb{Q}_p^{\mathrm{ab}}) \simeq X(\mathbb{C}_p)$$

is described by

$$X(\bar{\mathbb{F}}_p) = \mathfrak{p}_p X(\mathbb{C}_p),$$

where $\mathfrak{p}_p \in \mathrm{Spec}(\mathbb{H}_{\mathbb{Q}})$ is the prime ideal of adèle classes whose p-component vanishes.

Proof. One has $\hat{\mathbb{Z}} = \mathrm{Hom}(\mathbb{Q}/\mathbb{Z}, \mathbb{Q}/\mathbb{Z})$. Let, as above, $(\mathbb{Q}/\mathbb{Z})^{(p)} \subset \mathbb{Q}/\mathbb{Z}$ be the subgroup of elements of denominator prime to p. Then $\mathrm{Hom}(\mathbb{Q}/\mathbb{Z}, (\mathbb{Q}/\mathbb{Z})^{(p)}) \subset \mathrm{Hom}(\mathbb{Q}/\mathbb{Z}, \mathbb{Q}/\mathbb{Z})$ is given by

$$\big\{(a_\ell) \in \prod \mathbb{Z}_\ell = \hat{\mathbb{Z}} \mid a_p = 0\big\},$$

which corresponds to the prime, principal ideal $\mathfrak{p}_p$ of the hyperring structure $\mathbb{H}_{\mathbb{Q}}$ inherent to the adèle class space (cf. [15]). □

10. The standard model of $\overline{\mathbb{F}}_p$ and the BC-system

As shown in Section 8, the space $\mathrm{Val}_p(\mathbb{Q}^{\mathrm{cyc}})$ is intimately related to the space of sequences of irreducible polynomials $P_n(T) \in \mathbb{F}_p[T]$, $n \in \mathbb{N}$, fulfilling the basic conditions of the Conway polynomials (cf. Theorem 8.7) and hence to the explicit construction of an algebraic closure of $\mathbb{F}_p$. The normalization condition using the lexicographic ordering just specifies a particular element v_c of $\mathrm{Val}_p(\mathbb{Q}^{\mathrm{cyc}})$. Since the explicit computation of the sequence $P_n(T) \in \mathbb{F}_p[T]$, $n \in \mathbb{N}$, associated to v_c has been proven to be completely untractable, B. de Smit and H. Lenstra have recently devised a more efficient construction of $\overline{\mathbb{F}}_p$ (cf. [19]). Our goal in this section is to make explicit the relation between their construction, the BC-system and the sought for "curve".

When $\mathbb{K}$ is a global field of positive characteristic, i.e., the function field of an algebraic curve over a finite field $\mathbb{F}_q$, the intermediate extension $\mathbb{K} \subset \overline{\mathbb{F}}_q \otimes_{\mathbb{F}_q} \mathbb{K} \subset \mathbb{K}^{\mathrm{ab}}$ plays an important geometric role since it corresponds to working over an algebraically closed field. For $\mathbb{K} = \mathbb{Q}$, it is therefore natural to ask for an intermediate extension $\mathbb{Q} \subset L \subset \mathbb{Q}^{\mathrm{cyc}}$ playing a similar role. One feature of the former extension is that the residue fields are algebraically closed.

In their construction, de Smit and Lenstra use the intermediate extension $\mathbb{Q} \subset \mathbb{Q}_\Delta^{\mathrm{cycl}} \subset \mathbb{Q}^{\mathrm{cyc}}$ which comes very close to fulfill the expected properties. For each prime ℓ, let us denote by $\Delta_\ell \subset \mathbb{Z}_\ell^*$ the torsion subgroup. For $\ell = 2$ one has $\Delta_2 = \{\pm 1\}$, while for $\ell \neq 2$ one gets $\Delta_\ell = \tau(\mathbb{F}_\ell^*)$, where $\tau \colon \mathbb{F}_\ell \to \mathbb{Z}_\ell$ is the Teichmüller lift. The product

$$\Delta := \prod_\ell \Delta_\ell \subset \prod_\ell \mathbb{Z}_\ell^*$$

is a compact group and a subgroup of the Galois group $\hat{\mathbb{Z}}^* = \mathrm{Gal}(\mathbb{Q}^{\mathrm{cyc}} : \mathbb{Q})$. By Galois theory, one can thus associate to Δ a (fixed) field extension

$$L = \mathbb{Q}_\Delta^{\mathrm{cycl}} \subset \mathbb{Q}^{\mathrm{cyc}}.$$

Notice that one derives a subsystem of the BC-system given by the fixed points of the action of Δ. At the rational level and by implementing the cyclotomic ideal J of Definition 8.1, one obtains the exact sequence of algebras

$$0 \to J \cap \mathbb{Q}[\mathbb{Q}/\mathbb{Z}]^\Delta \to \mathbb{Q}[\mathbb{Q}/\mathbb{Z}]^\Delta \xrightarrow{q} \mathbb{Q}_\Delta^{\mathrm{cycl}} \to 0.$$

The image of the restriction to $\mathbb{Z}[\mathbb{Q}/\mathbb{Z}]^\Delta$ of the homomorphism q is contained in the integers of $\mathbb{Q}_\Delta^{\mathrm{cycl}}$ and one has

$$\mathrm{Gal}(\mathbb{Q}_\Delta^{\mathrm{cycl}} : \mathbb{Q}) \simeq \hat{\mathbb{Z}}^*/\Delta \simeq \prod_\ell \mathbb{Z}_\ell^*/\Delta_\ell.$$

The space $\mathrm{Val}_p(\mathbb{Q}^{\mathrm{cyc}})$ is the total space of a principal bundle whose base is the space $\mathrm{Val}_p(\mathbb{Q}_\Delta^{\mathrm{cycl}})$ of valuations on $\mathbb{Q}_\Delta^{\mathrm{cycl}}$ extending the p-adic valuation. The group of the principal bundle is the quotient of Δ by its intersection Δ_p with the isotropy group of elements of $\mathrm{Val}_p(\mathbb{Q}^{\mathrm{cyc}})$. The projection $\mathrm{Val}_p(\mathbb{Q}^{\mathrm{cyc}}) \to \mathrm{Val}_p(\mathbb{Q}_\Delta^{\mathrm{cycl}})$ is given by restriction of valuations from $\mathbb{Q}^{\mathrm{cyc}}$ to $\mathbb{Q}_\Delta^{\mathrm{cycl}}$. For $w \in \mathrm{Val}_p(\mathbb{Q}_\Delta^{\mathrm{cycl}})$, the isotropy group Π_p of w for the action of $\mathrm{Gal}(\mathbb{Q}_\Delta^{\mathrm{cycl}} : \mathbb{Q})$ is the image of the isotropy group of v in $\mathrm{Gal}(\mathbb{Q}^{\mathrm{cyc}} : \mathbb{Q})$ for any extension v of w to $\mathbb{Q}^{\mathrm{cyc}}$. It follows from Lemma 8.2 that the isotropy subgroup of v is $\mathbb{Z}_p^* \times f_p^{\hat{\mathbb{Z}}} \subset \mathbb{Z}_p^* \times G_p$, thus one gets

$$\Pi_p \simeq \mathbb{Z}_p^*/\Delta_p \times \overline{f_p^{\mathbb{Z}}}, \quad \overline{f_p^{\mathbb{Z}}} \subset \prod_{\ell \neq p} \mathbb{Z}_\ell^*/\Delta_\ell.$$

Lemma 10.1. *For each prime ℓ the group $\mathbb{Z}_\ell^*/\Delta_\ell$ is canonically isomorphic to the additive group $\mathbb{Z}_\ell$. Moreover, for each prime $p \neq \ell$, the closed subgroup of $\mathbb{Z}_\ell^*/\Delta_\ell$ generated by p is open and of finite index $\ell^{u(p,\ell)}$, where*

$$u(p,\ell) = \begin{cases} v_\ell(p^{\ell-1} - 1) - 1 & \text{for } \ell > 2, \\ v_2(p^2 - 1) - 3 & \text{for } \ell = 2. \end{cases}$$

Proof. For each prime ℓ there is a canonical isomorphism of groups

$$\mathbb{Z}_\ell^* \xrightarrow{\sim} \Delta_\ell \times \mathbb{Z}_\ell, \quad x \mapsto (\omega(x), i_\ell(x)),$$

where the group $\mathbb{Z}_\ell$ is viewed as an additive group. For ℓ odd, $\omega(x)$ is the unique $\ell - 1$ root of unity which is congruent to x modulo ℓ and $i_\ell(x)$, as in (78), is the ratio $\log_\ell x / \log_\ell(1 + \ell)$. For $\ell = 2$, $\omega(x) = \pm 1$ is congruent to x modulo 4 and $i_2(x) = \log_2 x / \log_2(1 + 4)$. The first statement thus follows. The second statement follows since one has

$$v_\ell(i_\ell(p)) = u(p,\ell)$$

and the closed subgroup of $\mathbb{Z}_\ell$ generated by $i_\ell(p)$ is $\ell^{u(p,\ell)}\mathbb{Z}_\ell$. □

Under the isomorphisms

$$\mathrm{Gal}(\mathbb{Q}_\Delta^{\mathrm{cycl}} : \mathbb{Q}) \simeq \prod_\ell \mathbb{Z}_\ell^*/\Delta_\ell \simeq \prod_\ell \mathbb{Z}_\ell \simeq \hat{\mathbb{Z}} \tag{107}$$

one gets, by the Chinese remainder theorem,

$$\Pi_p \simeq \mathbb{Z}_p \times \prod_{\ell \neq p} \ell^{u(p,\ell)}\mathbb{Z}_\ell \subset \hat{\mathbb{Z}}. \tag{108}$$

Notice the independence of the places ℓ in the above formula which makes the group Π_p a cartesian product and allows one to express $\mathrm{Val}_p(\mathbb{Q}_\Delta^{\mathrm{cycl}})$ as an infinite product of finite sets.

To label concretely these finite sets consider, for each prime ℓ the $\mathbb{Z}_\ell$-extension $\mathbb{B}_\infty(\ell)$ of $\mathbb{Q}$. One has $\mathbb{B}_\infty(\ell) = \bigcup_k \mathbb{B}_k(\ell))$ where, for $k \in \mathbb{N}$, the finite extension

$\mathbb{B}_k(\ell)$ of $\mathbb{Q}$ is associated to $\ell^{-k} \in \mathbb{Q}/\mathbb{Z}$ viewed as a character of $\hat{\mathbb{Z}} \simeq \mathrm{Gal}(\mathbb{Q}_\Delta^{\mathrm{cycl}} : \mathbb{Q})$. For ℓ odd, $\mathbb{B}_k(\ell)$ is the fixed subfield for the action of Δ_ℓ on the extension of $\mathbb{Q}$ generated by a primitive root of unity of order ℓ^{k+1}. For $\ell = 2$ one uses a primitive root of unity of order 2^{k+2}. We denote by $\mathbb{B}(\ell, p) = \mathbb{B}_{u(p,\ell)}(\ell)$: this is a cyclic extension of $\mathbb{Q}$ of degree $\ell^{u(p,\ell)}$. The Artin reciprocity law shows that, for p a prime $p \neq \ell$, the reduction modulo p of the integers of $\mathbb{B}(\ell, p)$ decomposes into a product of $\ell^{u(p,\ell)}$ copies of $\mathbb{F}_p$, parameterized by the set $\mathrm{Val}_p(\mathbb{B}(\ell, p))$ of extensions of the p-adic valuation to $\mathbb{B}(\ell, p)$, which is a finite set of cardinality $\ell^{u(p,\ell)}$.

The following result is a consequence of the construction of the "standard model" of de Smit and Lenstra for the algebraic closure of a finite field.

Theorem 10.2. *Let p be a rational prime.*

(1) *For $\ell \neq p$ a prime, the restriction map $\mathrm{Val}_p(\mathbb{B}_\infty(\ell)) \to \mathrm{Val}_p(\mathbb{B}(\ell, p))$ is bijective.*

(2) *The restriction maps from $\mathbb{Q}_\Delta^{\mathrm{cycl}}$ to $\mathbb{B}_\infty(\ell)$ give a bijection*

$$\mathrm{Val}_p(\mathbb{Q}_\Delta^{\mathrm{cycl}}) = \prod_{\ell \neq p} \mathrm{Val}_p(\mathbb{B}_\infty(\ell)).$$

(3) *The restriction of $v \in \mathrm{Val}_p(\mathbb{Q}_\Delta^{\mathrm{cycl}})$ to $\mathbb{Q}_\Delta^{\mathrm{cyc,p}}$ is unramified and the residue field is isomorphic to*

$$\bigcup_{n \in I(p)} \mathbb{F}_{p^n} \subset \bar{\mathbb{F}}_p,$$

where $I(p) \subset \mathbb{N}$ denotes the subset of positive integers which are prime to p.

Proof. (1) It is enough to show that the image of the isotropy group $\mathbb{Z}_p^* \times p^{\hat{\mathbb{Z}}} \subset \mathbb{Z}_p^* \times G_p$ of Lemma 8.2 maps surjectively onto the Galois group $\mathrm{Gal}(\mathbb{B}_\infty(\ell) : \mathbb{B}(\ell, p))$. This follows from Lemma 10.1.

(2) The restriction maps determine an equivariant map

$$\mathrm{Val}_p(\mathbb{Q}_\Delta^{\mathrm{cycl}}) \to \prod_{\ell \neq p} \mathrm{Val}_p(\mathbb{B}_\infty(\ell)) \tag{109}$$

for the action of the Galois group $\mathrm{Gal}(\mathbb{Q}_\Delta^{\mathrm{cycl}} : \mathbb{Q})$. By (107) and (108), the isotropy groups are the same so that the map (109) is bijective.

(3) By extending v to an element of $\mathrm{Val}_p(\mathbb{Q}^{\mathrm{cyc}})$ one gets that the restriction to $\mathbb{Q}^{\mathrm{cyc,p}}$ and hence to $\mathbb{Q}_\Delta^{\mathrm{cyc,p}}$ is unramified. Moreover, the residue field is determined by the topology on the closure set of the action of the Frobenius, i.e., on $\prod_{\ell \neq p} \mathbb{Z}_\ell$. The result follows. □

Next we shall explain the link with the notations used by de Smit and Lenstra and their construction. First, we recall that the additive group $\mathbb{Q}/\mathbb{Z}$ is the direct sum of its ℓ-torsion components

$$H_\ell = \{\alpha \in \mathbb{Q}/\mathbb{Z} \mid \text{there is } n \text{ such that } \ell^n \alpha = 0\} \simeq \mathbb{Q}_\ell/\mathbb{Z}_\ell.$$

Thus the group ring $\mathbb{Z}[\mathbb{Q}/\mathbb{Z}]$ can be written as a tensor product

$$\mathbb{Z}[\mathbb{Q}/\mathbb{Z}] = \bigotimes_{\ell \text{ prime}} \mathbb{Z}[H_\ell].$$

The natural action of $\hat{\mathbb{Z}}^*$ on $\mathbb{Z}[\mathbb{Q}/\mathbb{Z}]$ by automorphisms of the group $\mathbb{Q}/\mathbb{Z}$ factorizes in the individual actions of $\mathbb{Z}_\ell^* = \mathrm{Aut}(H_\ell)$.

One lets A_ℓ be the ring $\mathbb{Z}[X_0, X_1, \dots]$ modulo the ideal generated by

$$\sum_{j=0}^{\ell-1} X_0^j, \quad X_{k+1}^\ell - X_k \quad \text{for all } k \geq 0. \tag{110}$$

Thus one has $X_0^\ell = 1$ in A_ℓ and $X_{k+1}^\ell = X_k$ for all $k \geq 0$. The algebra B_ℓ of de Smit and Lenstra is defined as $B_\ell = A_\ell^{\Delta_\ell}$. The next lemma shows that the algebra B_ℓ is intimately related to the fixed point algebra $\mathbb{Z}[H_\ell]^{\Delta_\ell}$.

Lemma 10.3. *One has*

$$B_\ell \simeq (\mathbb{Z}[H_\ell]/J)^{\Delta_\ell}, \tag{111}$$

where J is the ideal generated by the relations $\sum_{\ell\gamma=0} e(\gamma) \in \mathbb{Z}[H_\ell]$.

Proof. It follows from the relations (110) that $X_k^{\ell^{k+1}} = 1$ for all k. Moreover, the map $\theta(e(\ell^{-k})) = X_{k-1}$ extends to a surjective homomorphism $\mathbb{Z}[H_\ell] \to A_\ell$ with kernel J, one thus gets (111). □

One has the trace map

$$\Sigma\colon A_\ell \to B_\ell, \quad \Sigma(x) = \sum_{\sigma\in\Delta_\ell} \sigma(x),$$

and natural ring homomorphisms $B_\ell \to E(\ell)$. De Smit and Lenstra (cf. [19]) lift the natural generator of $E_k(\ell)$ as an extension of $E_{k-1}(\ell)$, and the Galois conjugates under $\mathrm{Gal}(E_k(\ell) : E_{k-1}(\ell))$ as the following elements of B_ℓ

$$\eta_{\ell,k,i} = \Sigma(e(\tfrac{1}{\ell^{k+1}} + \tfrac{i}{\ell})), \quad i = 0, \dots \ell - 1.$$

When $\ell = 2$, one has simply $\Delta_2 = \{\pm 1\} \subset \mathbb{Z}_2^*$, and in this case the above list of elements reduces to

$$\eta_{2,k} = \Sigma\big(e\big(\tfrac{1}{2^{k+2}}\big)\big).$$

The two authors show that the prime ideals $\mathfrak{p}$ of B_ℓ that contain p are uniquely specified by a finite system of elements $a(\mathfrak{p}, j) \in \mathbb{F}_p$, $0 \leq j < \ell u(p,\ell)$. More precisely, $\mathfrak{p}$ is generated by p and by the $\eta_{\ell,k+1,i} - a(\mathfrak{p}, i + k\ell)$ for $0 \leq k < u(p,\ell)$ and $0 \leq i < \ell$.

To complete the dictionary with the notations of de Smit and Lenstra, we leave to the reader as an exercise to show that

- the prime ideals $\mathfrak{p}$ of B_ℓ that contain p correspond to the valuations $\mathrm{Val}_p(\mathbb{B}_\infty(\ell))$;
- the subfield $\mathbb{Q}_p \cap \mathbb{B}_\infty(\ell) \subset \mathbb{B}_\infty(\ell)_v$ is equal to $\mathbb{B}(\ell, p)$;
- the system of elements $a(\mathfrak{p}, j) \in \mathbb{F}_p$ corresponds, as in Proposition 8.13, to the residue of the inclusion $\gamma_v : \mathbb{B}(\ell, p) \to \mathbb{Q}_p$, defined as in Proposition 8.12.

Theorem 10.2 does not yield the full algebraic closure of $\mathbb{F}_p$ but only the subfield

$$\bigcup_{n \in I(p)} \mathbb{F}_{p^n} \subset \bar{\mathbb{F}}_p.$$

Thus it remains to understand how to produce naturally the missing part

$$\bigcup_n \mathbb{F}_{p^{p^n}} \subset \bar{\mathbb{F}}_p$$

in such a way that the tensor product over $\mathbb{F}_p$ yields $\bar{\mathbb{F}}_p$.

De Smit and Lenstra construction of $\mathbb{F}_{p^{p^\infty}} = \varinjlim_n \mathbb{F}_{p^{p^n}}$ is performed using the Artin–Schreier equations

$$y_0^p - y_0 = 1, \quad y_{n+1}^p - y_{n+1} + \frac{y_n}{y_n + 1} = 0 \quad \text{for all } n \geq 0,$$

which have the advantage of simplicity. E. Witt gave in [39] a conceptual construction of $\mathbb{F}_{p^{p^\infty}}$ based on the Witt functor $\mathbb{W}_{p^\infty}$ and its finite truncations $\mathbb{W}_{p^n}$. The addition of two Witt vectors $x = (x_j)$ and $y = (y_j)$ is a vector whose components $S_j(x, y)$ were proven by Witt to be polynomials with integer coefficients. Note also that for $p \neq 2$ the Witt components of $-x$ (the additive inverse of x) are simply $-x_j$, but this result does not hold for $p = 2$. Recall also that in terms of Witt vectors the Frobenius F is given in characteristic p by $(F(x))_j = x_j^p$ for all j.

From [39], one derives the following result.

Theorem 10.4. *Let $n \in \mathbb{N}$. Let $R_n = \mathbb{F}_p[x_0, x_1, \ldots, x_{n-1}]$ be the ring of polynomials in n variables and $J_n \subset R_n$ the ideal generated by the components of the Witt vector $F(x) - x - 1$, where $x \in \mathbb{W}_{p^{n-1}}(R)$ is the Witt vector with components x_j. Then J_n is a prime ideal and the quotient field of the integral ring R_n/J_n defines the field extension $E_n \simeq \mathbb{F}_{p^{p^n}}$.*

As an extension of E_{n-1}, E_n is given by an Artin–Schreier equation of the form

$$X^p = X + \alpha, \quad \alpha \in E_{n-1}.$$

One derives, for instance, that the first extensions for $p = 2$ are given by the equations with coefficients in $\mathbb{F}_2$:

$$\begin{aligned}
x_0^2 &= 1 + x_0,\\
x_1^2 &= x_0 + x_1,\\
x_2^2 &= x_0 + x_0^3 + x_0 x_1 + x_2,
\end{aligned}$$

and

$$\begin{aligned}x_3^2 &= x_0 + x_0^3 + x_0^5 + x_0^7 + x_0^2 x_1 + x_0^3 x_1 + x_0^4 x_1 \\ &\quad + x_0 x_1^3 + x_0 x_2 + x_0^3 x_2 + x_0 x_1 x_2 + x_3.\end{aligned}$$

For $p = 3$ one gets the following equations with coefficients in $\mathbb{F}_3$

$$\begin{aligned}x_0^3 &= 1 + x_0, \\ x_1^3 &= 2x_0 + 2x_0^2 + x_1, \\ x_2^3 &= 2x_0 + 2x_0^2 + 2x_0^4 + 2x_0^5 + 2x_0^7 + 2x_0^8 + 2x_0^2 x_1 \\ &\quad + x_0^3 x_1 + 2x_0^4 x_1 + x_0 x_1^2 + x_0^2 x_1^2 + x_2.\end{aligned}$$

In this way one obtains a completely canonical construction of the field $\mathbb{F}_{p^{p^\infty}}$ by simply writing the equation $F(X) = X + 1$ in the ring of Witt vectors $\mathbb{W}_{p^\infty}$.

References

[1] G. Almkvist, Endomorphisms of finitely generated projective modules over a commutative ring. *Ark. Mat.* **11** (1973), 263–301. Zbl 0278.13005 MR 0424786

[2] G. Almkvist, The Grothendieck ring of the category of endomorphisms. *J. Algebra* **28** (1974), 375–388. Zbl 0281.18012 MR 0432738

[3] R. Auer, A functorial property of nested Witt vectors. *J. Algebra* **252** (2002), 293–299. Zbl 1011.13013 MR 1925139

[4] J.-B. Bost and A. Connes, Hecke algebras, type III factors and phase transitions with spontaneous symmetry breaking in number theory. *Selecta Math.* (*N.S.*) **1** (1995), 411–457. Zbl 0842.46040 MR 1366621

[5] N. Bourbaki, *Algebra. II. Chapters 4–7*. Springer-Verlag, Berlin 2003. Zbl 1017.12001 MR 1994218

[6] N. Bourbaki, *Algèbre commutative. Chapitres 8 et 9*. Springer, Berlin 2006. Zbl 1103.13003 MR 2284892

[7] P. Cartier, Groupes formels associés aux anneaux de Witt généralisés. *C. R. Acad. Sci. Paris Sér. A* **265** (1967), 49–52. Zbl 0168.27501 MR 0218361

[8] A. Connes, Trace formula in noncommutative geometry and the zeros of the Riemann zeta function. *Selecta Math.* (*N.S.*) **5** (1999), 29–106. Zbl 0945.11015 MR 1694895

[9] A. Connes, The Witt construction in characteristic one and quantization. In *Noncommutative geometry and global analysis*, Contemp. Math. 546, Amer. Math. Soc., Providence, RI, 2011, 83–113. Zbl 1245.13015 MR 2815131

[10] A. Connes, The BC-system and L-functions. *Jpn. J. Math.* **6** (2011), 1–44. Zbl 1276.14002 MR 2835360

[11] A. Connes and C. Consani, Schemes over $\mathbb{F}_1$ and zeta functions. *Compos. Math.* **146** (2010), 1383–1415. Zbl 1201.14001 MR 2735370

[12] A. Connes and C. Consani From monoids to hyperstructures: in search of an absolute arithmetic. In *Casimir force, Casimir operators and the Riemann hypothesis*, Walter de Gruyter, Berlin 2010, 147–198. Zbl 1234.14002 MR 2777715

[13] A. Connes and C. Consani On the notion of geometry over $\mathbb{F}_1$. *J. Algebraic Geom.* **20** (2011), 525–557. Zbl 1227.14006 MR 2786665

[14] A. Connes and C. Consani Characteristic 1, entropy and the absolute point. In *Noncommutative geometry, arithmetic, and related topics*, Johns Hopkins University Press, Baltimore 2011, 75-–139. Zbl 1273.11140 MR 2907005

[15] A. Connes and C. Consani, The hyperring of adèle classes. *J. Number Theory* **131** (2011), 159–194. Zbl 1221.14002 MR 2736850

[16] A. Connes, C. Consani, and M. Marcolli, Fun with $\mathbb{F}_1$. *J. Number Theory* **129** (2009), 1532–1561. Zbl 1228.11143 MR 2521492

[17] C. Consani and M. Marcolli, Quantum statistical mechanics over function fields. *J. Number Theory* **123** (2007), 487–528. Zbl 1160.11043 MR 2301227

[18] A. Connes and M. Marcolli, *Noncommutative geometry, quantum fields and motives*. Amer. Math. Soc. Colloq. Publ. 55, Amer. Math. Soc., Providence, RI, 2008. Zbl 1209.58007 MR 2371808

[19] B. de Smit and H. W. Lenstra, Standard models for finite fields: the definition. Intercity Seminar Standard models of finite fields, Nijmegen, September 26, 2008. http://www.math.leidenuniv.nl/~desmit/papers/standard_models.pdf

[20] D. R. Grayson, Grothendieck rings and Witt vectors. *Comm. Algebra* **6** (1978), 249–255. Zbl 0383.13009 MR 484183

[21] A. Grothendieck, La théorie des classes de Chern. *Bull. Soc. Math. France* **86** (1958), 137–154. Zbl 0091.33201 MR 0116023

[22] R. Hartshorne, *Algebraic geometry*. Graduate Texts in Math. 52, Springer-Verlag, New York 1977. Zbl 0367.14001 MR 0463157

[23] M. Hazewinkel, Operations in the K-theory of endomorphisms. *J. Algebra* **84** (1983), 285–304. Zbl 0534.13010 MR 723394

[24] M. Hazewinkel M. Hazewinkel, Witt vectors. I. In *Handbook of algebra*. Vol. 6, Handb. Algebr. 6, Elsevier, Amsterdam 2009, 319–472. Zbl 1221.13036 MR 2553661

[25] L. Hesselholt, The big De Rham–Witt complex. Preprint 2010. arXiv:1006.3125

[26] J. L. Kelley and E. H. Spanier, Euler characteristics. *Pacific J. Math.* **26** (1968), 317—339. Zbl 0164.33401 MR 0260842

[27] H. W. Lenstra, Jr., Finding isomorphisms between finite fields. *Math. Comp.* **56** (1991), 329–347. Zbl 0709.11072 MR 1052099

[28] Yu. I. Manin, Lectures on zeta functions and motives (according to Deninger and Kurokawa). *Astérisque* **228** (1995), 121–163. Zbl 00772545 MR 1330931

[29] D. Mumford, *Lectures on curves on an algebraic surface*. Ann. of Math. Stud. 59, Princeton University Press, Princeton, N.J., 1966. Zbl 0187.42701 MR 0209285

[30] D. Quillen, On the cohomology and K-theory of the general linear groups over a finite field. *Ann. of Math.* (2) **96** (1972), 552–586. Zbl 0249.18022 MR 0315016

[31] J. Rabinoff, The theory of Witt vectors.
Notes available at www.math.harvard.edu/~rabinoff/misc/witt.pdf

[32] J.-P. Ramis, *Séries divergentes et théories asymptotiques*. Bull. Soc. Math. France 121, Panoramas et Synthèses, suppl., Soc. Math. France, Paris 1993. Zbl 0830.34045 MR 1272100

[33] A. M. Robert, *A course in p-adic analysis*. Graduate Texts in Math. 198, Springer-Verlag, New York 2000. Zbl 0947.11035 MR 1760253

[34] L. G. Roberts, The ring of Witt vectors. In *The Curves Seminar at Queen's*, Vol. XI (Kingston, ON, 1997) , Queen's Papers in Pure and Appl. Math. 105, Queen's University, Kingston, ON, 1997, 2–36. Zbl 1032.13013 MR 1464698

[35] J.-P. Serre, *Corps locaux*. Deuxième édition, Publications de l'Université de Nancago, No. VIII, Hermann, Paris 1968. Zbl 0137.02601 MR 0354618

[36] C. Soulé, Les variétés sur le corps à un élément. *Moscow Math. J.* **4** (2004), 217–244. Zbl 1103.14003 MR 2074990

[37] O. Teichmüller, Über die Struktur diskret bewerteter perfekter Körper. *Nachr. Ges. Wiss. Göttingen* **1936**, Math.-Phys. Kl. I, N. F. 1, 151–161; also in *Gesammelte Abhandlungen/Collected Papers*, Springer-Verlag, Belin 1982, 53–63. JFM 62.0110.01 Zbl 0013.29301

[38] L. C. Washington, *Introduction to cyclotomic fields*. 2nd ed., Graduate Texts in Math. 83, 2nd ed., Springer-Verlag, New York 1997. Zbl 0966.11047 MR 1421575

[39] E. Witt, Zyklische Körper und Algebren der Charakteristik p vom Grad p^n. *J. Reine Angew. Math.* **176** (1936), 126–140. JFM 62.1112.03 Zbl 0016.05101 http://gdz.sub.uni-goettingen.de/dms/load/toc/?PPN=PPN243919689_0176

[40] E. Witt, Vektorkalkül und Endomorphismen der Einspotenzreihengruppe. Unpublished 1969. In: Ernst Witt, *Collected Papers/Gesammelte Abhandlungen*, Springer-Verlag, Berlin 1998, 157–163.

Received April 12, 2011; revised November 20, 2012

A. Connes, Collège de France, 3 rue d'Ulm, Paris 75005, France
I.H.E.S. and The Ohio State University, U.S.A.
E-mail: alain@connes.org

C. Consani, Department of Mathematics, The Johns Hopkins University, Baltimore,
MD 21218, U.S.A.
E-mail: kc@math.jhu.edu