Iwasawa Algebras and p-adic Measures

Leonardo Colò

October 11th, 2016

1 Iwasawa Algebras

First of all we want to recall some definitions and to fix the notation. We will write $\mathcal{G}$ to indicate the Galois Group of the extension $\mathbb{Q}(\mu_{p^\infty})$ over $\mathbb{Q}$:

$$\mathcal{G} = Gal(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$$

The Iwasawa algebra will play a fundamental role in this seminar: in general, let $\mathfrak{G}$ be a profinite abelian group. This means that $\mathfrak{G}$ is a topological group which is obtained as the projective limit of a discrete collection of finite groups, each given the discrete topology.

$$\mathfrak{G} = \lim_{\leftarrow} \mathfrak{F}_n$$

where $(\mathfrak{F}_n, \pi_n)$ is a projective system and $\mathfrak{F}_n$ is a finite topological group for all n. The topology on $\mathfrak{G}$ is the topology originated by the projections

$$p_n : \mathfrak{G} \to \mathfrak{F}_n$$

A basis for the topology is the set of all the preimages of open subsets in $\mathfrak{F}_n$ with respect to p_n.
A neighbourhood basis for 0 is given by the set of $\ker(p_n)$.
Let $\mathcal{T}_{\mathfrak{G}}$ be the set of all open subgroups of $\mathfrak{G}$.

Theorem. *A topological group is profinite if and only if it is Hausdorff, compact, and totally disconnected.*

We recall that a topological space is totally disconnected if the only (non-empty) connected subsets are one-point subsets, or equivalently, if for any two points there is an open and closed subset containing one but not the other.

Proposition. *Let $\mathfrak{G}$ be a compact group, and $\mathfrak{H} \subseteq \mathfrak{G}$ a subgroup. Then $\mathfrak{H}$ is open if and only if $\mathfrak{H}$ is closed and of finite index.*

Proof. Suppose $\mathfrak{H}$ is open. Then $\mathfrak{H}$ has finite index, since $\mathfrak{G}$ is compact and every coset of an open subgroup is open. $\mathfrak{H}$ is then also closed, since its complement is a union of cosets, each of which is open. Conversely, if $\mathfrak{H}$ is closed and has finite index, then its complement is a finite union of closed cosets, and hence closed, so $\mathfrak{H}$ is open. □

Corollary. *Let $\mathfrak{G}$ be a profinite group, and $\mathfrak{H} \subseteq \mathfrak{G}$ a subgroup. Then $\mathfrak{H}$ is open if and only if $\mathfrak{H}$ is closed and has finite index.*

We conclude that every element in $\mathcal{T}_{\mathfrak{G}}$ has finite index in $\mathfrak{G}$. This means that for all $\mathfrak{H}$ open subgroup of $\mathfrak{G}$, the quotient $\mathfrak{G}/\mathfrak{H}$ is a finite group.

Definition. *Given a profinite abelian group $\mathfrak{G}$, we define the Iwasawa algebra to be*

$$\Lambda(\mathfrak{G}) = \lim_{\leftarrow} \mathbb{Z}_p[\mathfrak{G}/\mathfrak{H}]$$

where $\mathfrak{H}$ runs over $\mathcal{T}_{\mathfrak{G}}$, and $\mathbb{Z}_p[\mathfrak{G}/\mathfrak{H}]$ denotes the ordinary group ring over $\mathbb{Z}_p$.

The topology on $\Lambda(\mathfrak{G})$ is given by the projection maps

$$\pi_{\mathfrak{H}} : \Lambda(\mathfrak{G}) = \lim_{\leftarrow} \mathbb{Z}_p[\mathfrak{G}/\mathfrak{H}] \to \mathbb{Z}_p[\mathfrak{G}/\mathfrak{H}]$$

Hence the open subsets of $\Lambda(\mathfrak{G})$ are the preimages of open subsets in $\mathbb{Z}_p[\mathfrak{G}/\mathfrak{H}]$.

Lemma. *For all $\mathcal{U} \in \mathcal{T}_{\mathfrak{G}}$, we can write $\mathcal{U}$ ha a disjoint union:*

$$\mathcal{U} = \coprod_{i=1}^{n} (q_i + \mathfrak{H})$$

Where q_i are representants of the elements of $\mathcal{U}/\mathfrak{H}$.

Example. We know that $\frac{p\mathbb{Z}_p}{p^2\mathbb{Z}_p} \simeq \frac{\mathbb{Z}}{p\mathbb{Z}}$

$1+p\mathbb{Z}_p = (1+p^2\mathbb{Z}_p)+((1+p)+p^2\mathbb{Z}_p)+((1+2p)+p^2\mathbb{Z}_p)+\ldots+((1+(p-1)p)+p^2\mathbb{Z}_p)$

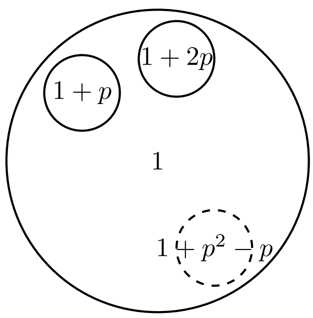
We obtain

$$(1 + p\mathbb{Z}_p) = \coprod_{n=0}^{p-1} ((1 + np) + p^2\mathbb{Z}_p)$$

we recall that

$$(1 + p\mathbb{Z}_p) = \{x \in \mathbb{Z}_p \mid \nu(x - 1) \geq 1\}$$

And so we have the following representation:



The small open disks cover the big disk and they are disjoint.

Recall. If we have two disks $D_1; D_2$ in $\mathbb{Q}_p$ we only have two possibilities:

- $D_1 \cap D_2 = \emptyset$
- $D_1 \subset D_2$ or $D_2 \subset D_1$

The main goal of this work is to build a bijection

$$\Lambda(\mathfrak{G}) \longleftrightarrow Meas(\mathfrak{G}, \mathbb{Z}_p)$$
$$\lambda \longleftrightarrow \mu_\lambda$$

associating to every element of the Iwasawa algebra a p-adic measure valued in $\mathbb{Z}_p$.

Definition. *A p-adic distribution is a map*

$$\mu : \mathcal{T} = \{open\ and\ compact\ subsets\ of\ \Lambda(\mathfrak{G})\} \to \mathbb{C}_p$$

which is additive. This means that if we consider a disjoint family $\{\mathcal{U}_n\}_{n=1}^N$ of elements of $\mathcal{T}$, where $\mathcal{U}_n \cap \mathcal{U}_m = \emptyset$ for all $n \neq m$, then

$$\mu(\coprod_{n=1}^N \mathcal{U}_n) = \sum_{n=1}^N \mu(\mathcal{U}_n)$$

Definition. *A p-adic measure is a bounded p-adic distribution.*
A p-adic distribution is bounded if there exists $B \in \mathbb{R}$ such that $||\mu(\mathcal{U})|| < B$ for all $\mathcal{U}$. Equivalently, working with the p-adic valuation, if there exists $C \in \mathbb{R}$ such that $|\mu(\mathcal{U})|_p > C$ for all $\mathcal{U}$.

Remark. If our measure takes values in $\mathbb{Z}_p$ we do not need the condition $||\mu(\mathcal{U})|| < B$ for all $\mathcal{U}$ since $|x|_p \leq 1$ for all $x \in \mathbb{Z}_p$.

Let $\mathbb{C}_p$ be the completion of the algebraic closure of the field of p-adic numbers $\mathbb{Q}_p$, and write $|\cdot|_p$ for its p-adic norm.

Definition. *We write $\mathscr{C}(\mathfrak{G}, \mathbb{C}_p) = \{Continuous\ functions\ from\ \mathfrak{G}\ to\ \mathbb{C}_p\}$ for the $\mathbb{C}_p$-algebra of continuous functions from $\mathfrak{G}$ to $\mathbb{C}_p$.*

We can define a norm on $\mathscr{C}(\mathfrak{G}, \mathbb{C}_p)$ by

$$||f|| = \sup_{g \in \mathfrak{G}} |f(g)|_p$$

Observation. $||f||$ is well defined as $\sup_{g \in \mathfrak{G}} |f(g)|_p$ is finite: indeed, $\mathfrak{G}$ is compact and so f is bounded $\Longrightarrow \sup_{g \in \mathfrak{G}} |f(g)|_p$ is bounded.

This norm makes $\mathscr{C}(\mathfrak{G}, \mathbb{C}_p)$ into a $\mathbb{C}_p$ Banach space.

Definition. *A function $f : \mathfrak{G} \to \mathbb{C}_p$ is said to be locally constant if, for all $a \in \mathfrak{G}$, there exist an open subgroup $\mathfrak{H} \subseteq \mathfrak{G}$ such that $f_{|a+\mathfrak{H}}$ is constant, i.e. $f(a + \mathfrak{h}) = f(a)$, for all $\mathfrak{h} \in \mathfrak{H}$*

In other words, a function f in $\mathscr{C}(\mathfrak{G}, \mathbb{C}_p)$ is defined to be locally constant if there exists an open subgroup $\mathfrak{H}$ of $\mathfrak{G}$ such that f is constant modulo $\mathfrak{H}$, i.e. gives a function from $\mathfrak{G}/\mathfrak{H}$ to $\mathbb{C}_p$.

Definition. *We write $Step(\mathfrak{G})$ for the sub-algebra of locally constant functions.*

Let f be constant modulo $\mathfrak{H}$.

$$\mathfrak{G} = (a_1 + \mathfrak{H}) \amalg \ldots \amalg (a_n + \mathfrak{H})$$

with a_i representants of $\mathfrak{G}/\mathfrak{H}$. Then we can write

$$f = \sum_{i=1}^n \alpha_i \chi_{a_i+\mathfrak{H}} \qquad \alpha_i \in \mathbb{C}_p$$

$\mathfrak{H}$ is an open and compact set $\Longrightarrow \mathfrak{H}$ is open and closed $\Longrightarrow \chi_{a_i+\mathfrak{H}}$ is continuous.

We have the following lemma:

Lemma. *$Step(\mathfrak{G})$ is dense in $\mathscr{C}(\mathfrak{G}, \mathbb{C}_p)$.*

Proof. $Step(\mathfrak{G}) \subseteq \mathscr{C}(\mathfrak{G}, \mathbb{C}_p)$ and $||f|| = \sup_{\mathfrak{g}\in\mathfrak{G}} |f(\mathfrak{g})|$.
Let $f \in \mathscr{C}(\mathfrak{G}, \mathbb{C}_p)$; $f : \mathfrak{G} \to \mathbb{C}_p$. Since $\mathfrak{G}$ is compact, we have that f is uniformly continuous:

$\forall \epsilon > 0$, $\exists \mathfrak{H}_\epsilon \subseteq \mathfrak{G}$ *open subset such that* $\forall x, y \in \mathfrak{G}$ *with* $x - y \in \mathfrak{H}_\epsilon \Rightarrow |f(x) - f(y)| < \epsilon$

Let $\mathfrak{G}/\mathfrak{H}_\epsilon = \{a_1; \dots; a_n\}$. We set

$$g = \sum_{i=1}^{n} f(a_i)\chi_{a_i+\mathfrak{H}_\epsilon} \in Step(\mathfrak{G})$$

For all $x \in \mathfrak{G}$ there exists i_0 such that $x \in a_{i_0} + \mathfrak{H}_\epsilon$.

$$|f(x) - g(x)| = |f(x) - f(a_{i_0})| < \epsilon$$

since $x - a_{i_0} \in \mathfrak{H}_\epsilon$ and f is uniformly continuous.
Hence

$$||f(x) - g(x)|| = \sup_{x\in\mathfrak{G}} |f(x) - g(x)| \leq \epsilon$$

We conclude that $Step(\mathfrak{G})$ is dense in $\mathscr{C}(\mathfrak{G}, \mathbb{C}_p)$. □

Definition. *If $f = \sum_{i=1}^{n} \alpha_i \chi_{a_i+\mathfrak{H}} \in Step(\mathfrak{G})$ we set*

$$\int_{\mathfrak{G}} f d\mu = \sum_{i=1}^{n} \alpha_i \mu(a_i + \mathfrak{H})$$

Lemma. *The definition above is independent on the choice of $\mathfrak{H}$.*

Since $Step(\mathfrak{G})$ si dense in $\mathscr{C}(\mathfrak{G}, \mathbb{C}_p)$, then for all f continuous function we have a sequence $\{h_n\}_{n\in\mathbb{N}}$ of locally constant functions converging to f.

Definition. *We set*

$$\int_{\mathfrak{G}} f d\mu = \lim_{n\to\infty} \int_{\mathfrak{G}} h_n d\mu$$

This is a good definition since we have the following

Theorem. *Let $\{g_n\}_{n\in\mathbb{N}}$ be a sequence of locally constant functions such that*

$$\lim_{n\to\infty} g_n = f$$

then we have

i. *The sequence $\{\int_{\mathfrak{G}} g_n d\mu\}_{n\in\mathbb{N}}$ is Cauchy.*

ii. *The quantity*

$$\lim_{n\to\infty} \int_{\mathfrak{G}} g_n d\mu$$

does not depends on the choice of $\{g_n\}_{n\in\mathbb{N}}$ but only on f.

Proof. **i.** $\lim_{n\to\infty} g_n = f$ and $\{g_n\}_{n\in\mathbb{N}}$ is Cauchy.

Then $(g_{n+1} - g_n) \to 0$ as $n \to \infty$ and $||g_{n+1} - g_n|| \to 0$ as $n \to \infty$.

$$\int_{\mathfrak{G}} (g_{n+1} - g_n) d\mu = \int_{\mathfrak{G}} g_{n+1} d\mu - \int_{\mathfrak{G}} g_n d\mu$$

$$|\int_{\mathfrak{G}} (g_{n+1} - g_n) d\mu| \leq ||g_{n+1} - g_n|| \cdot ||\mu||$$

where $||\mu|| = \sup_{\mathcal{U}} |\mu(\mathcal{U})|$. Since $||\mu||$ is bounded and $||g_{n+1} - g_n|| \to 0$ we have

$$|\int_{\mathfrak{G}} (g_{n+1} - g_n) d\mu| = |\int_{\mathfrak{G}} g_{n+1} d\mu - \int_{\mathfrak{G}} g_n d\mu| \leq ||g_{n+1} - g_n|| \cdot ||\mu|| \to 0.$$

ii. Suppose we have $\{g_n\}_{n\in\mathbb{N}}$ and $\{h_n\}_{n\in\mathbb{N}}$ two sequences converging to f.

$$|\int_{\mathfrak{G}} h_n d\mu - \int_{\mathfrak{G}} g_n d\mu| = |\int_{\mathfrak{G}} (h_n - g_n) d\mu| \leq ||h_n - g_n|| ||\mu|| =$$
$$= ||h_n - f + f - g_n|| ||\mu|| \leq \max\{||h_n - f||; ||f - g_n||\} ||\mu||$$

but $||h_n - f|| \to 0$ as $n \to \infty$ and $||f - g_n|| \to 0$ as $n \to \infty$. Moreover μ is bounded. So we have

$$|\int_{\mathfrak{G}} h_n d\mu - \int_{\mathfrak{G}} g_n d\mu| \to 0 \qquad as\ n \to \infty$$

□

Definition. *We define the convolution product in $Meas(\mathfrak{G}, \mathbb{Z}_p)$ as $\mu_1 * \mu_2$ in this way:*

$$\int_{\mathfrak{G}} f(x) d(\mu_1 * \mu_2)(x) = \int_{\mathfrak{G}} (\int_{\mathfrak{G}} f(x + y) d\mu_1(x)) d\mu_2(y)$$

With this definition we know the behaviour of $\mu_1 * \mu_2$ on all subsets $A \subset \mathfrak{G}$:

$$\mu_1 * \mu_2(A) = \int_{\mathfrak{G}} \chi_A d(\mu_1 * \mu_2)$$

Theorem. *$\Lambda(\mathfrak{G})$ and $Meas(\mathfrak{G}, \mathbb{Z}_p)$ are isomorphic.*

Proof. We want to find an isomorphism

$$\Psi : \Lambda(\mathfrak{G}) \to Meas(\mathfrak{G}, \mathbb{Z}_p)$$

Let's consider $\lambda \in \Lambda(\mathfrak{G})$. $\lambda = (\lambda_{\mathfrak{H}})_{\mathfrak{H}}$. We want to find $\mu_\lambda \in Meas(\mathfrak{G}, \mathbb{Z}_p)$. We only need to describe what is $\mu_\lambda(a + \Gamma)$. Indeed, every compact subset of $\mathfrak{G}$ is union of elements of this form: $a + \Gamma$ where $a \in \mathfrak{G}$ and $\Gamma \subseteq \mathfrak{G}$ is in $\mathcal{T}_{\mathfrak{G}}$.

$$\lambda_\Gamma = \sum_{\sigma \in \mathfrak{G}/\Gamma} a_\sigma \sigma \qquad\qquad a_\sigma \in \mathbb{Z}_p$$

Let be $\overline{\gamma} \in \mathfrak{G}/\Gamma$. $\overline{\gamma}$ is one of the σ and $a_{\overline{\gamma}} \in \mathbb{Z}_p$. We set

$$\mu_\lambda(\gamma + \Gamma) = a_{\overline{\gamma}}$$

Clearly μ_λ is bounded since $a_{\overline{\gamma}}$ si in $\mathbb{Z}_p$.
We now want to check the additivity of μ: if $\gamma + \Gamma = \amalg_{i=1}^n (a_i + \mathfrak{H})$ with $\mathfrak{H} \subseteq \Gamma \subseteq \mathfrak{G}$ and a_i are the representatives of all the elements in $\alpha_i \in \mathfrak{G}/\mathfrak{H}$ such that $\alpha_i = \gamma \mod \Gamma$, then we claim that

$$\mu_\lambda(\gamma + \Gamma) = \mu_\lambda(\amalg_{i=1}^n (a_1 + \mathfrak{H})) = \sum_{i=1}^n \mu_\lambda(a_i + \mathfrak{H})$$

But this is plain from the compatibility of the family $\lambda = (\lambda_{\mathfrak{K}})_{\mathfrak{K}}$. Indeed, if

$$\lambda_\Gamma = \sum_{\sigma \in \mathfrak{G}/\Gamma} a_\sigma \sigma \qquad \textit{and} \qquad \lambda_{\mathfrak{H}} = \sum_{\tau \in \mathfrak{G}/\mathfrak{H}} b_\tau \tau$$

then

$$\mu_\lambda(\gamma + \Gamma) = a_{\sigma_0} \qquad \textit{where } \gamma = \sigma_0 \mod \Gamma$$
$$\sum_{i=1}^n \mu_\lambda(a_i + \mathfrak{H}) = \sum_{i=1}^n b_{\tau_i} \qquad \textit{where } a_i = \tau_i \mod \mathfrak{H}$$

Since

$$\pi : \mathbb{Z}[\mathfrak{G}/\mathfrak{H}] \to \mathbb{Z}[\mathfrak{G}/\Gamma]$$
$$\lambda_{\mathfrak{H}} \to \lambda_\Gamma$$
$$\sum_{\tau \in \mathfrak{G}/\mathfrak{H}} b_\tau \tau \to \sum_{\sigma \in \mathfrak{G}/\Gamma} a_\sigma \sigma$$

then

$$\sum_{\sigma \in \mathfrak{G}/\Gamma} a_\sigma \sigma = \pi(\sum_{\tau \in \mathfrak{G}/\mathfrak{H}} b_\tau \tau) = \sum_{\sigma \in \mathfrak{G}/\Gamma} (\sum_{\tau \equiv_\Gamma \sigma} b_\tau)\sigma$$

and we conclude that $a_{\sigma_0} = \sum_{\tau \equiv_\Gamma \sigma_0} b_\tau = \sum_{i=1}^n b_{\tau_i}$.
It can be shown that the product in $\Lambda(\mathfrak{G})$ gives the convolution product in $Meas(\mathfrak{G}, \mathbb{Z}_p)$ and so Ψ is a $\mathbb{Z}_p$-algebras homomorphism.
Ψ is injective since $\ker(\Psi) = \{0\}$. Indeed, if $\Psi(\lambda) = 0 \in Meas(\mathfrak{G}, \mathbb{Z}_p)$ then $0(A) = 0$ for all $A \subset \mathfrak{G}$. Then every component of λ is 0 and so $\lambda = 0$.
Finally Ψ is surjective: given a measure $\mu \in Meas(\mathfrak{G}, \mathbb{Z}_p)$ then we can construct a sequence $(\lambda_{\mathfrak{H}})_{\mathfrak{H}}$ where $\lambda_{\mathfrak{H}} = \sum_{\sigma \in \mathfrak{G}/\mathfrak{h}} \mu(\sigma + \mathfrak{H})\sigma$. The only thing we have to check is that $(\lambda_{\mathfrak{H}})_{\mathfrak{H}} \in \Lambda(\mathfrak{G})$ i.e. that $(\lambda_{\mathfrak{H}})_{\mathfrak{H}}$ is a compatible system.
Suppose we have $\mathfrak{H} \subset \Gamma \subset \mathfrak{G}$ then $\Gamma = \amalg(a_i + \mathfrak{H})$ then

$$\lambda_\Gamma = \sum_{\sigma \in \mathfrak{G}/\Gamma} \mu(\sigma + \Gamma)\sigma$$
$$\lambda_{\mathfrak{H}} = \sum_{\tau \in \mathfrak{G}/\mathfrak{H}} \mu(\tau + \mathfrak{H})\tau$$

Now we use the additivity of the measure μ to prove the compatibility of $(\lambda_{\mathfrak{H}})_{\mathfrak{H}}$

$$\pi(\lambda_{\mathfrak{H}}) = \pi(\sum_{\tau \in \mathfrak{G}/\mathfrak{H}} \mu(\tau + \mathfrak{H})\tau) = \sum_{\sigma \in \mathfrak{G}/\Gamma} (\sum_{\tau \equiv_\Gamma \sigma} \mu(\tau + \mathfrak{H}))\sigma =$$
$$= \sum_{\sigma \in \mathfrak{G}/\Gamma} \mu(\coprod_{\tau \equiv_\Gamma \sigma} (\tau + \mathfrak{H}))\sigma = \sum_{\sigma \in \mathfrak{G}/\Gamma} \mu(\sigma + \Gamma)\sigma = \lambda_\Gamma$$

□

The isomorphism we built allows us to speak about integration of continuous functions against an element $\lambda \in \Lambda(\mathfrak{G})$: setting $\lambda = (\lambda_{\mathfrak{K}})_{\mathfrak{K}} = (\sum_{x \in \mathfrak{B}/\mathfrak{K}} c_{\mathfrak{K}}(x)x)$ with $c_{\mathfrak{H}}(x) \in \mathbb{Z}_p$, we define the integral of a function f locally constant on $\mathfrak{H}$ as

$$\int_{\mathfrak{G}} f d\lambda = \sum_{x \in \mathfrak{B}/\mathfrak{H}} f(x) c_{\mathfrak{H}}(x)$$

Observation. Since the $c_{\mathfrak{H}}$ lie in $\mathbb{Z}_p$ we have

$$|\int_{\mathfrak{G}} f d\lambda|_p \leq ||f||$$

Indeed $|\int_{\mathfrak{G}} f d\lambda|_p = |\sum_{x \in \mathfrak{B}/\mathfrak{H}} f(x) c_{\mathfrak{H}}(x)| \leq \max\{|f(x) c_{\mathfrak{H}}(x)|\}$ and, since $c_{\mathfrak{H}}(x) \in \mathbb{Z}_p$, then $|c_{\mathfrak{H}}(x)| \leq 1$. We conclude that

$$|\int_{\mathfrak{G}} f d\lambda|_p \leq \max\{|f(x)| \cdot |c_{\mathfrak{H}}(x)|\} \leq ||f|| \cdot 1 = ||f||$$

If f is any continuous function and $\{f_n\}_{n \in \mathbb{N}}$ is a sequence converging to f, then

$$\int_{\mathfrak{G}} f d\lambda = \lim_{n \to \infty} \int_{\mathfrak{G}} f_n d\lambda$$

We have a linear functional

$$\begin{aligned} M_\lambda : \mathscr{C}(\mathfrak{G}, \mathbb{C}_p) &\longrightarrow \mathbb{C}_p \\ f &\longrightarrow \int_{\mathfrak{G}} f d\lambda \end{aligned}$$

satisfying $|M_\lambda(f)| \leq ||f||$.
It is clear that if $M_{\lambda_1} = M_{\lambda_2}$, then $\lambda_1 = \lambda_2$. Finally, $M_\lambda(f)$ belongs to $\mathbb{Q}_p$ when f takes values in $\mathbb{Q}_p$. Conversely we have the following lemma

Lemma. *Every linear functional $\mathcal{L}$ on $\mathscr{C}(\mathfrak{G}, \mathbb{C}_p)$ satisfying $|\mathcal{L}(f)|_p \leq ||f||$ for all continuous functions f and $\mathcal{L}(f)$ belongs to $\mathbb{Q}_p$ when f takes values in $\mathbb{Q}_p$, is of the form $\mathcal{L} = M_\lambda$ for a unique λ in $\Lambda(\mathfrak{G})$.*

Proof. The element λ can be obtained as follows. For each open subgroup $\mathfrak{H}$ of $\mathfrak{G}$, and each coset x of $\mathfrak{G}/\mathfrak{H}$, we put $c_{\mathfrak{H}}(x) = \mathcal{L}(\chi_x)$ where χ_x is the characteristic function of x, and then define $\lambda_{\mathfrak{H}}$ by the formula $\lambda_{\mathfrak{H}} = \sum_{\sigma \in \mathfrak{G}/\mathfrak{H}} c_{\mathfrak{H}}(\sigma)\sigma$. These elements $\lambda_{\mathfrak{H}}$ are clearly compatible and so give an element in $\Lambda(\mathfrak{G})$. □

Observation. If $\lambda = g$ in $\mathfrak{G}$, then dg is the Dirac measure given by

$$\int_{\mathfrak{G}} f dg = f(g)$$

Observation. The product in $\Lambda(\mathfrak{G})$ corresponds to the convolution of measures which we recall is defined by

$$\int_{\mathfrak{G}} f(x) d(\lambda_1 * \lambda_2)(x) = \int_{\mathfrak{G}} (\int_{\mathfrak{G}} f(x+y) d\lambda_1(x)) d\lambda_2(y)$$

Observation. If $\nu : \mathfrak{G} \to \mathbb{C}_p$ is a continuous group homomorphism, then one sees easily that we can extend ν to a continuous algebra homomorphism,

$$\nu : \Lambda(\mathfrak{G}) \to \mathbb{C}_p$$

by the formula $\nu(\lambda) = \int_{\mathfrak{G}} \nu d\lambda$.

Observation. To take account of the fact that the p-adic analogue of the complex Riemann zeta function also has a pole, we now introduce the notion of a p-adic pseudo-measure on $\mathfrak{G}$. Let $\mathcal{Q}(\mathfrak{G})$ be the total ring of fractions of $\Lambda(\mathfrak{G})$, i.e. the set of all quotients α/β with α and β in $\Lambda(\mathfrak{G})$ and β a non-zero divisor. We say that an element λ of $\mathcal{Q}(\mathfrak{G})$ is a pseudo-measure on $\mathfrak{G}$ if $(g-1)\lambda$ is in $\Lambda(\mathfrak{G})$ for all g in $\mathfrak{G}$.

Suppose that λ is a pseudo-measure on $\mathfrak{G}$ and let ν be a homomorphism from $\mathfrak{G}$ to $\mathbb{C}_p$ which is not identically one. We can then define

$$\int_{\mathfrak{G}} \nu d\lambda = \frac{\int_{\mathfrak{G}} \nu d((g-1)\lambda)}{\nu(g)-1}$$

where g is any element of $\mathfrak{G}$ with $\nu(g) \neq 1$. This is independent of the choice of g because, as remarked earlier ν extends to a ring homomorphism from $\Lambda(\mathfrak{G})$ to $\mathbb{C}_p$.

2 Mahler transform

We now specialize our argument for the Iwasawa algebra of $\mathbb{Z}_p$.

Let be $R = \mathbb{Z}_p[\![T]\!]$ the ring of formal power series.

Definition. *As usual we define*

$$\binom{x}{n} = \begin{cases} 1 & n = 0 \\ \frac{x\cdot(x-1)\cdot\ldots\cdot(x-n+1)}{n!} & \textit{otherwise} \end{cases}$$

Theorem. *The functions*

$$\binom{x}{0}\ ,\ \binom{x}{1}\ ,\ \binom{x}{2}\ ,\ \binom{x}{3}\ ,\ \ldots$$

form an orthonormal basis (Mahler basis) of $\mathscr{C}(\mathbb{Z}_p, \mathbb{C}_p)$.

Theorem (Mahler)**.** *Let $f : \mathbb{Z}_p \to \mathbb{C}_p$ be any continuous function. Then f can be written uniquely in the form:*

$$f(x) = \sum_{n=0}^{\infty} a_n \binom{x}{n}$$

where $a_n \in \mathbb{C}_p$ tends to 0 as $n \to \infty$.

Proof. We take

$$a_n(f) = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f(k)$$

The idea of the proof is very easy. It is clear that

$$f(n) = \sum_{k=0}^{n} a_k(f)\binom{n}{k}$$

If we show that $\lim_{n\to\infty} |a_n(f)|_p = 0$ then the series

$$\sum_{k=0}^{\infty} a_k(f)\binom{x}{k}$$

converges uniformly and, since f is continous, its sum is $f(x)$ in view of the relation for $f(n)$ and the fact that non-negative integers are dense in $\mathbb{Z}_p$.
A complete proof can be found in
[*A Simple Proof of Mahlers Theorem on Approximation of Continuous Functions of a p − adic Variable by Polynomials − R. Bojanic*] □

Note that the coefficients a_n are given by $a_n = (\nabla^n f)(0)$ where

$$\nabla f(x) = f(x+1) - f(x)$$

Lemma. *$|\binom{x}{n}| \leq 1$ for all $x \in \mathbb{Z}_p$ and $n \in \mathbb{Z}$.*

Proof. For any $x \in \mathbb{Z}_p$ we can choose $y \in \mathbb{Z}$ such that

$$|\frac{x-y}{n!}|_p \leq 1$$

The existence of such a y is given by the density of $\mathbb{Z}$ in $\mathbb{Z}_p$.
For $k = 0, 1, 2, \ldots, n$, $\binom{y}{n-k}$ is a positive integer. Hence

$$|\binom{y}{n-k}|_p \leq 1$$

Further $\binom{x-y}{0} = 1$ and

$$\binom{x-y}{k} = \frac{(x-y)(x-y-1)\ldots(x-y-k+1)}{k!} = \frac{x-y}{n!}\lambda_k$$

where λ_k is a p-adic integer. Therefore

$$|\binom{x-y}{k}|_p \leq 1$$

The identity (Vandermonde Convolution)

$$\binom{x}{n} = \sum_{k=0}^{n} \binom{x-y}{k}\binom{y}{n-k}$$

implies

$$|\binom{x}{n}|_p \leq 1 \Longrightarrow \binom{x}{n} \in \mathbb{Z}_p$$

□

Since $|\binom{x}{n}|_p \leq 1$ for all x in $\mathbb{Z}_p$, it follows that $||f|| = \sup |a_n|_p$.
If λ is any element of $\Lambda(\mathbb{Z}_p)$, it follows from that

$$c_n(\lambda) = \int_{\mathbb{Z}_p} \binom{x}{n} d\lambda \qquad (n \geq 0)$$

lies in $\mathbb{Z}_p$. This leads to the following definition.

Definition. *We define the Mahler transform* $\mathcal{M} : \Lambda(\mathbb{Z}_p) \to R$ *by*

$$\mathcal{M}(\lambda) = \sum_{n=0}^{\infty} c_n(\lambda) T^n$$

for $\lambda \in \Lambda(\mathbb{Z}_p)$.

Theorem. *The Mahler transform is an isomorphism of* $\mathbb{Z}_p$*-algebras.*

Proof. It is clear from the previous theorem that $\mathcal{M}$ is injective, and is a $\mathbb{Z}_p$-module homomorphism. To see that it is bijective, we construct an inverse $\Upsilon : R \to \Lambda(\mathbb{Z}_p)$ as follows. Let $g(T) = \sum_{n=0}^{\infty} c_n T^n$ be any element of R. We can then define a linear functional $\mathcal{L}$ on $\mathscr{C}(\mathbb{Z}_p, \mathbb{C}_p)$ by

$$\mathcal{L}(f) = \sum_{n=0}^{\infty} a_n c_n$$

where f has Mahler expansion $f(x) = \sum_{n=0}^{\infty} a_n \binom{x}{n}$. Of course, the series on the right converges because a_n tends to zero as $n \to \infty$. Since the c_n lie in $\mathbb{Z}_p$, it is clear that $|\mathcal{L}(f)|_p \leq ||f||$ for all f. Hence there exists λ in $\Lambda(\mathbb{Z}_p)$ such that $\mathcal{L} = M_\lambda$, and we define $\Upsilon(g(T)) = \lambda$. It is plain that Υ is an inverse of $\mathcal{M}$. In fact, it can also be shown that $\mathcal{M}$ preserves products, although we omit the proof here. □

Lemma. *We have* $\mathcal{M}(1_{\mathbb{Z}_p}) = 1 + T$*, and thus* $\mathcal{M} : \Lambda(\mathbb{Z}_p) \to R$ *is the unique isomorphism of topological* $\mathbb{Z}_p$*-algebras which sends the topological generator* $1_{\mathbb{Z}_p}$ *of* $\mathbb{Z}_p$ *to* $(1 + T)$.

Proof. Take $\lambda = 1_{\mathbb{Z}_p}$. By definition,

$$\mathcal{M}(\lambda) = \sum_{n=0}^{\infty} c_n(\lambda) T^n$$

where

$$c_n(\lambda) = \int_{\mathbb{Z}_p} \binom{x}{n} d\lambda = \binom{1}{n}$$

whence the first assertion is clear. For the second assertion, we note that it is well-known, that for each choice of a topological generator γ of $\mathbb{Z}_p$, there is a unique topological isomorphism of $\mathbb{Z}_p$-algebras, which maps γ to $(1 + T)$. □

Lemma. *For all* g *in* R*, and all integers* $k \geq 0$*, we have the integral*

$$\int_{\mathbb{Z}_p} x^k d(\Upsilon(g(T))) = (D^k g(T))_{T=0}$$

where $D = (1 + T)\frac{d}{dT}$.

Proof. For fixed $g(T) = \sum_{n=0}^{\infty} c_n T^n$ in R, consider the linear functional $\mathcal{L}$ on $\mathscr{C}(\mathbb{Z}_p, \mathbb{C}_p)$ defined by

$$\mathcal{L}(f) = \int_{\mathbb{Z}_p} xf(x) d\Upsilon(g(T))$$

Clearly, we have $|\mathcal{L}(f)|_p \leq ||f||$, and so $\mathcal{L} = M_\lambda$ for some $\lambda \in \Lambda(\mathbb{Z}_p)$, whence we obtain

$$\int_{\mathbb{Z}_p} xf(x) d\Upsilon(g(T)) = \int_{\mathbb{Z}_p} f(x) d\lambda$$

We first claim that

$$\mathcal{M}(\lambda) = Dg(T)$$

To prove this, we note that

$$Dg(T) = \sum_{n=0}^{\infty} (nc_n + (n+1)c_{n+1})T^n$$

On the other hand, by definition, $\mathcal{M}(\lambda) = \sum_{n=0}^{\infty} e_n T^n$, where

$$e_n = \int_{\mathbb{Z}_p} x \binom{x}{n} d\Upsilon(g(T))$$

But we have the identity

$$x\binom{x}{n} = (n+1)\binom{x}{n+1} + n\binom{x}{n} \qquad (n \geq 0)$$

whence we get $e_n = nc_n + (n+1)c_{n+1}$ for all $n \geq 0$, thereby proving that $\mathcal{M}(\lambda) = Dg(T)$.
But, for all $h(T) \in R$, we have

$$\int_{\mathbb{Z}_p} d\Upsilon(h(T)) = h(0)$$

Indeed, $\Upsilon(h(T)) = \lambda \in \Lambda(\mathbb{Z}_p)$ such that, if

$$f(x) = \sum_{n=0}^{\infty} \alpha_n \binom{x}{n} \qquad \textit{and} \qquad h(T) = \sum_{n=0}^{\infty} \beta_n T^n$$

then

$$\int_{\mathbb{Z}_p} f(x) d\lambda = \sum_{n=0}^{\infty} \alpha_n \beta_n$$

Hence, if $f = 1$ then $f = \sum_{n=0}^{\infty} \delta_{0,n} \binom{x}{n}$ and so

$$\int_{\mathbb{Z}_p} 1 \; d(\Upsilon(h(T))) = \sum_{n=0}^{\infty} \delta_{0,n} \beta_n = \beta_0 = h(0)$$

So the assertion of the lemma is equivalent to

$$\int_{\mathbb{Z}_p} x^k d(\Upsilon(g(T))) = \int_{\mathbb{Z}_p} d\Upsilon(D^k g(T)) \qquad (k \geq 0)$$

By an induction argument, we have

$$\int_{\mathbb{Z}_p} d\Upsilon(D^k g(T)) = \int_{\mathbb{Z}_p} x^{k-1} d(\Upsilon(Dg(T)))$$

It is now plain by the fact that $\mathcal{M}(\lambda) = Dg(T)$ and $\int_{\mathbb{Z}_p} xf(x)d\Upsilon(g(T)) = \int_{\mathbb{Z}_p} f(x)d\lambda$ that this is equal to

$$\int_{\mathbb{Z}_p} x^k d\Upsilon(g(T))$$

and the proof of the lemma is complete. □