IWASAWA ALGEBRAS AND p-ADIC MEASURES

PRELIMINARIES

Let G be a profinite group. The Iwasawa algebra of G is defined to be

$$\Lambda(G) = \mathbf{Z}_p[[G]] := \varprojlim_{H} \mathbf{Z}_p[G/H],$$

where in the inverse limit, H runs over all open normal subgroups of G.

The natural topology on $\Lambda(G)$ is the inverse limit topology. Let $\mathfrak{m}$ be the Jacobson radical of $\Lambda(G)$, then the $\mathfrak{m}$-adic topology of $\Lambda(G)$ is finer than the natural topology.

If $[G : G_p] < \infty$, where G_p is any Sylow p-subgroup of G, then the ring $\Lambda(G)$ is semilocal. If furthermore G is pro-p, then $\Lambda(G)$ is local; its maximal ideal is (p, I_G), where $I_G = \ker(\Lambda(G) \to \mathbf{Z}_p)$ is the augmentation ideal.

One fundamental result. Suppose $G \cong \mathbf{Z}_p$, and we fix a topological generator γ of G. Then the map

$$\mathbf{Z}_p[[G]] \to \mathbf{Z}_p[[T]], \qquad \gamma \mapsto 1 + T$$

is an isomorphism. Since this isomorphism depends on the choice of γ, it is not canonical.

Idea of proof. Since $G \cong \mathbf{Z}_p$, and $\mathbf{Z}_p = \mathbf{Z}_p/p^n$, we have

$$\mathbf{Z}_p[[G]] = \varprojlim \mathbf{Z}_p[G/G^{p^n}] = \varprojlim \mathbf{Z}_p[T]/((1+T)^{p^n} - 1) = \varprojlim \mathbf{Z}_p[T]/((1+T)^{p^n} - 1, p^n).$$

On the other hand, we have

$$\mathbf{Z}_p[[T]] = \varprojlim \mathbf{Z}_p[T]/(T^{p^n}) = \varprojlim \mathbf{Z}_p[T]/(T^{p^n}, p^n).$$

Now it is not difficult to prove that the two families of ideals

$$\{I_n = ((1+T)^{p^n} - 1, p^n)\}, \qquad \text{and} \qquad \{I'_n = (T^{p^n}, p^n)\}$$

are co-filtered, i.e., for a fixed I_n, one has $I'_m \subset I_n$ for large m; and vice versa. (Check!) Once this is achieved, the result follows immediately.

1. INTEGRATION

Let $C(G, \mathbf{C}_p)$ denote the space of continuous functions $G \to \mathbf{C}_p$. If $f \in C(G, \mathbf{C}_p)$, we define the norm

$$\|f\| := \sup_{\sigma \in G} |f(\sigma)|_p.$$

It is finite because G is compact. This is the metric on $C(G, \mathbf{C}_p)$ that we work with. We say f is locally constant if f factors as $G \to G/H \to \mathbf{C}_p$ for some open normal subgroup H of G.

Now we construct the following

$$\mathbf{Z}_p[[G]] \to \{\text{linear functionals (measures) on } C(G, \mathbf{C}_p)\}, \qquad \lambda \mapsto d\lambda. \qquad (\dagger)$$

The definition of $d\lambda$ mimics the construction in the usual measure theory.

Step 1. Suppose that f is locally constant, say $f: G \to G/H \to \mathbf{C}_p$. We can write the image λ_H of λ in $\mathbf{Z}_p[G/H]$ as

$$\lambda_H = \sum_{x \in G/H} c_H(x) x,$$

where $c_H(x)$ lies in $\mathbf{Z}_p$. And we define

$$\int_G f \, d\lambda := \sum c_H(x) f(x).$$

The RHS is independent of the choice of H. (Check!) Also $|\int_G f \, d\lambda|_p \leqslant \|f\|$.

Step 2. Suppose that $f \in C(G, \mathbf{C}_p)$ is arbitrary. Then one can find a sequence f_n of locally constant functions such that $f_n \to f$ (i.e., $\|f_n - f\| \to 0$). Then $\int_G f_n \, d\lambda$ converges and we define

$$\int_G f \, d\lambda := \lim_{n \to \infty} \int_G f_n \, d\lambda.$$

This completes the construction of (†).

Basic properties. (Check!) (i) $|\int_G f \, d\lambda|_p \leqslant \|f\|$.

(ii) The map (†) is injective. (Well, this trivial fact seems to be quite useful.)

(iii) If $\lambda = \sigma \in G \subset \mathbf{Z}_p[[G]]$, then $d\sigma$ is the Dirac measure at x, i.e., $\int_G f \, d\sigma = f(\sigma)$.

(iv) The map (†) converts product to convolution. I.e.,

$$\int_G f(x) \, d(\lambda_1 \lambda_2)(x) = \int_G \Big(\int_G f(x+y) \, d\lambda_1(x) \Big) d\lambda_2(y).$$

Clearly if $f \in C(G, \mathbf{Q}_p)$, then $\int_G f \, d\lambda \in \mathbf{Q}_p$. So the map (†) gives

$$\mathbf{Z}_p[[G]] \to \{\mathbf{Q}_p\text{-linear functionals } L \text{ on } C(G, \mathbf{Q}_p) \text{ such that } |L(f)|_p \leqslant \|f\|\}. \qquad (*)$$

Claim: This map is bijective. In fact, given such a functional L, we construct the corresponding element λ. For each open normal subgroup H of G, define $\lambda \in \mathbf{Z}_p[G/H]$ by

$$\lambda_H = \sum_{x \in G/H} L(\varepsilon_x) x,$$

where ε_x is the characteristic function at x. Then these λ_H are compatible and thus give an element $\lambda \in \Lambda(G)$. It is easy to check that λ does map to L.

2. Mahler transform

Theorem 1 (Mahler)**.** *Let $f: \mathbf{Z}_p \to \mathbf{C}_p$ be a continuous function. Then it can be written uniquely as*

$$f(x) = \sum_{n \geqslant 0} a_n \binom{x}{n},$$

where $a_n \in \mathbf{C}_p$ and $a_n \to 0$ as $n \to \infty$.

The uniqueness is obvious. The difficulty is to prove that $a_n \to 0$. The proof is omitted. (I do not know if brute force would work in this case. I haven't tried.)

The Mahler transform is the following

$$M: \Lambda(\mathbf{Z}_p) \to \mathbf{Z}_p[[T]] \qquad \lambda \mapsto \int_{\mathbf{Z}_p} (1+T)^x \, d\lambda(x). \qquad (1)$$

This is an abuse of notation. What we really mean on the RHS is

$$\int_{\mathbf{Z}_p} (1+T)^x \, d\lambda(x) = \int_{\mathbf{Z}_p} \sum \binom{x}{n} T^n \, d\lambda(x) = \sum \Big(\int_{\mathbf{Z}_p} \binom{x}{n} d\lambda(x) \Big) T^n.$$

This is the real notation. But personally I find the notation in (1) much easier to remember and to use.

Using the same formula, we can define the Mahler transform of any measure on $C(\mathbf{Z}_p, \mathbf{C}_p)$ or on $C(\mathbf{Z}_p, \mathbf{Q}_p)$. But we will not use them.

Theorem 2 (Mahler). *The map* (1) *is an isomorphism of* $\mathbf{Z}_p$*-algebras.*

Proof. The map M is clearly $\mathbf{Z}_p$-linear. We show that M also preserves products. Using the basic property (iv) above, we have

$$\begin{aligned} M(\lambda_1\lambda_2) &= \int (1+T)^x \, d(\lambda_1\lambda_2)(x) \\ &= \int \Big(\int (1+T)^{x+y} \, d\lambda_1(x) \Big) d\lambda_2(y) \\ &= \Big(\int (1+T)^x \, d\lambda_1(x) \Big) \Big(\int (1+T)^y d\lambda_2(y) \Big) \\ &= M(\lambda_1) \cdot M(\lambda_2) \end{aligned}$$

Therefore M is an $\mathbf{Z}_p$-algebra homomorphism. Clearly $M(1_{\mathbf{Z}_p}) = 1 + T$. But we already mentioned that such a homomorphism is necessarily an isomorphism. $\square$

Lemma 1. Let $Y : \mathbf{Z}_p[[T]] \to \Lambda(\mathbf{Z}_p)$ be the inverse of M. Then for any $g \in \mathbf{Z}_p[[T]]$, and any integer $k \geqslant 0$, we have

$$\int_{\mathbf{Z}_p} x^k d(Yg) = (D^k g(T))_{T=0},$$

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

Proof. Indeed, by definition, we have $\int_{\mathbf{Z}_p} (1+T)^x \, d(Yg) = g(T)$. Applying the operator D^k on both sides, we get

$$\int_{\mathbf{Z}_p} D^k (1+T)^x \, d(Yg) = D^k g(T).$$

Simple induction shows that $D^k(1+T)^x = x^k(1+T)^x$. Taking $T = 0$ on both sides, the lemma follows. $\square$

Remark. The explicit description of the map Y is given in Thm. 3.3.3 in the book.

3. Restriction of measures

The subset $\mathbf{Z}_p^\times$ is not a subgroup of $\mathbf{Z}_p$. However, we shall use $(*)$ to construct a canonical map $\Lambda(\mathbf{Z}_p^\times) \to \Lambda(\mathbf{Z}_p)$. The method is the following

$$\begin{tikzcd} \Lambda(\mathbf{Z}_p^\times) \arrow[r] \arrow[d, dashed, "i"] & \left\{ \begin{array}{c} \mathbf{Q}_p \text{ linear functionals } L \text{ on } C(\mathbf{Z}_p^\times, \mathbf{Q}_p) \\ \text{such that } |L(f)|_p \leqslant \|f\| \end{array} \right\} \arrow[d] \\ \Lambda(\mathbf{Z}_p) \arrow[r] & \left\{ \begin{array}{c} \mathbf{Q}_p \text{ linear functionals } L \text{ on } C(\mathbf{Z}_p, \mathbf{Q}_p) \\ \text{such that } |L(f)|_p \leqslant \|f\| \end{array} \right\} \end{tikzcd}$$

The horizontal maps are bijective. Hence if we can construct a map on the RHS, we would have a map on the LHS.

The construction is almost trivial: it is merely the "restriction on $\mathbf{Z}_p^\times$". Given any linear function L on $C(\mathbf{Z}_p^\times, \mathbf{Q}_p)$, we can define a linear functional L' on $C(\mathbf{Z}_p, \mathbf{Q}_p)$ by

$$L'(f) := L(f|_{\mathbf{Z}_p^\times}).$$

This is the vertical map on the RHS. Correspondingly, the dashed map i is defined by the formula (here $\eta \in \Lambda(\mathbf{Z}_p^\times)$)

$$\int_{\mathbf{Z}_p} f\, d(i\eta) = \int_{\mathbf{Z}_p^\times} f|_{\mathbf{Z}_p^\times}\, d\eta, \quad \text{for all } f \in C(\mathbf{Z}_p, \mathbf{Q}_p).$$

We can also "restrict an element $\lambda \in \Lambda(\mathbf{Z}_p)$ to $\mathbf{Z}_p^\times$", as follows. Let $\lambda \in \Lambda(\mathbf{Z}_p)$. Then the functional

$$f \mapsto \int_{\mathbf{Z}_p^\times} f\, d\lambda \qquad f \in \Lambda(\mathbf{Z}_p)$$

clearly falls in the RHS of $(*)$. Therefore it comes from an element $\#\lambda \in \Lambda(\mathbf{Z}_p)$. That is, we define $\#\lambda$ by the following formula

$$\int_{\mathbf{Z}_p^\times} f\, d\lambda = \int_{\mathbf{Z}_p} f\, d(\#\lambda), \quad \text{for all } f \in C(\mathbf{Z}_p, \mathbf{Q}_p). \tag{2}$$

(One should think $d(\#\lambda)$ as $d\lambda|_{\mathbf{Z}_p^\times}$.) We also define an operator $S : \mathbf{Z}_p[[T]] \to \mathbf{Z}_p[[T]]$ by

$$S(g(T)) = g(T) - \frac{1}{p} \sum_{\xi \in \mu_p} g(\xi(1+T) - 1) = g(T) - \varphi\psi(g)(T).$$

Lemma 2. For any $\lambda \in \Lambda(\mathbf{Z}_p)$, we have $S(M(\lambda)) = M(\#\lambda)$. In particular, $\#\lambda = \lambda$ if and only if $S(M(\lambda)) = M(\lambda)$, or equivalently if and only if $M(\lambda)$ falls in $\mathbf{Z}_p[[T]]^{\psi=0}$.

Proof. Since $M(\lambda) = \int_{\mathbf{Z}_p} (1+T)^x\, d\lambda$, and noticing that $1 + (\xi(1+T) - 1) = \xi(1+T)$, we have

$$S(M(\lambda)) = \int_{\mathbf{Z}_p} (1+T)^x\, d\lambda - \int_{\mathbf{Z}_p} \sum_{\xi \in \mu_p} \frac{1}{p} \xi^x (1+T)^x\, d\lambda.$$

But $\sum \frac{1}{p} \xi^x = 0$ or 1 according to whether $x \in \mathbf{Z}_p^\times$ or $x \in p\mathbf{Z}_p$ (check!), so the second term above is nothing but $\int_{p\mathbf{Z}_p} (1+T)^x\, d\lambda$. Taking difference, we see that

$$S(M(\lambda)) = \int_{\mathbf{Z}_p^\times} (1+T)^x\, d\lambda.$$

Now the lemma follows from the very definition of $\#\lambda$ (2). ☐

The following lemma identifies the image of i.

Lemma 3. We have $i(\Lambda(\mathbf{Z}_p^\times)) = \{\lambda \in \Lambda(\mathbf{Z}_p) : \#\lambda = \lambda\}$. In particular, we have $M(i(\Lambda(\mathbf{Z}_p^\times))) = \mathbf{Z}_p[[T]]^{\psi=0}$.

This is a straightforward check. Proof left to the readers.

4. THE FUNDAMENTAL SEQUENCE

Recall that $\mathcal{G}$ is the Galois group of $\mathbf{Q}_p(\mu_{p^\infty})$ over $\mathbf{Q}_p$. $\mathcal{G}$ is canonically isomorphic to $\mathbf{Z}_p^\times$, thus $\Lambda(\mathcal{G})$ is canonically isomorphic to $\Lambda(\mathbf{Z}_p^\times)$. We shall also identify $\Lambda(\mathcal{G}) = \Lambda(\mathbf{Z}_p^\times)$ as a subset of $\Lambda(\mathbf{Z}_p)$ via i (lemma 3). Then lemma 3 again says that we have an isomorphism (here $\widetilde{M} = M \circ i$)

$$\widetilde{M} : \Lambda(\mathcal{G}) \xrightarrow{\sim} \mathbf{Z}_p[[T]]^{\psi=0}.$$

Recall that we have an operator $\mathcal{L}$ defined as follows: for $f \in \mathbf{Z}_p[[T]]^\times$, put

$$\mathcal{L}(f) = \frac{1}{p}\log\Big(\frac{f(T)^p}{\varphi(f)(T)}\Big).$$

$$\widetilde{\mathcal{L}} : U_\infty \to \Lambda(\mathcal{G}) \qquad u \mapsto \widetilde{M}^{-1}(\mathcal{L}(f_u)),$$

where f_u is the Coleman series of u.

Theorem 3. *We have an exact sequence of $\mathcal{G}$-modules*

$$0 \to \mu_{p-1} \times T_p\mu \to U_\infty \xrightarrow{\widetilde{\mathcal{L}}} \Lambda(\mathcal{G}) \xrightarrow{\beta} T_p\mu \to 0,$$

where the first map is the natural inclusion, and the map β is given by $\beta(\lambda) = \zeta^{\int_{\mathcal{G}} \chi\, d\lambda}$, where ζ is a fixed topological generator of $T_p\mu$, χ is the cyclotomic character.

Idea of proof. We already saw the following exact sequence in Sujatha's talk

$$0 \to A \to W \xrightarrow{\mathcal{L}} \mathbf{Z}_p[[T]]^{\psi=0} \to \mathbf{Z}_p \to 0.$$

Our sequence is a re-statement of this exact sequence. The corresponding terms are all isomorphic, and one needs to verify that all maps involves are compatible, i.e., they make every square commutative. Check it as an exercise.