Presentation of an Iwasawa Algebra: The Case of $\Gamma_1 SL(2, \mathbb{Z}_p)$

Laurent Clozel [1]

Received: July 1, 2010
Revised: February 17, 2011

Communicated by Takeshi Saito

Abstract. We give an explicit presentation of the p-adic Iwasawa algebra of the subgroup of level one of $SL(2, \mathbb{Z}_p)$ for $p \neq 2$.

2010 Mathematics Subject Classification: 11F85, 11S31,22E50
Keywords and Phrases: Non-commutative Iwasawa agebras, p-adic groups

Assume G is a semi–simple Chevalley group, so $G(\mathbb{Z}_p) \subset G(\mathbb{Q}_p)$ is a maximal compact subgroup. Both the p–adic representation theory of $G(\mathbb{Q}_p)$ and non–commutative Iwasawa theory involve the Iwasawa algebra of $G(\mathbb{Z}_p)$ or suitable congruence subgroups. It seems to have been assumed that explicit descriptions, by generators and relations, of these algebras were inaccessible. However, it is a general principle that natural objects coming from semi–simple (split) groups have explicit presentations. Famous examples are Serre's presentation of the semi–simple algebras and Steinberg's presentation of the Chevalley groups [7, 8]. In this paper we will give a presentation for the Iwasawa algebra of the subgroup of level 1 in $SL(2, \mathbb{Z}_p)$ ($p \neq 2$).

I thank M. Duflo and, once more, J.–P. Serre for useful discussions. Thanks are also due to P. Schneider for reading a first draft and suggesting several corrections, and to the referee for his careful work which eliminated an embarrassing mistake.

[1]Membre de l'Institut Universitaire de France

1

Let $\underline{G} = SL(2)$ and let G be the subgroup of level 1 in $\underline{G}(\mathbb{Z}_p)$:

$$G = \{g \in SL(2, \mathbb{Z}_p) : g \equiv 1[p]\}\,.$$

We assume $p > 2$, so G has no p–torsion. It has a triangular decomposition

$$G = N^- \; T \; N^+$$

where $N^- = \begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix}$, $N^+ = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ (entries $*$ in $p\mathbb{Z}_p$) and $T = \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}$ (entries in $1 + p\mathbb{Z}_p$). We identify N^-, N^+ with $\mathbb{Z}_p$ by $* = px$ ($x \in \mathbb{Z}_p$). Similarly $T \cong \mathbb{Z}_p$ by

$$x \longmapsto \begin{pmatrix} (1+p)^x & \\ & (1+p)^{-x} \end{pmatrix} \qquad (x \in \mathbb{Z}_p)\,.$$

We consider the Iwasawa algebra Λ_G of $\mathbb{Z}_p$–valued measures (or distributions, in the sense of [9]), on G, which we will denote by $\mathcal{D}(G, \mathbb{Z}_p)$. The triangular decomposition of G, as an analytic manifold, yields a decomposition of $\mathcal{D}(G, \mathbb{Z}_p)$ as a topological $\mathbb{Z}_p$–MODULE :

$$\mathcal{D}(G, \mathbb{Z}_p) = \mathcal{D}(N^-, \mathbb{Z}_p)\widehat{\otimes}\mathcal{D}(T, \mathbb{Z}_p)\widehat{\otimes}\mathcal{D}(N^+, \mathbb{Z}_p)\,, \tag{1.1}$$

the factors of (1.1) being the spaces of distributions on the factors of G. If f is a function on G and U, V, W distributions on N^-, T, N^+,

$$< U \otimes V \otimes W, f > := < U \otimes V \otimes W, f(uhn) > \tag{1.2}$$

where $u \in N^-$, $h \in T$, $n \in N^+$ and f is therefore seen as a function on $N^- \times T \times N^+$. The natural definition of the completed tensor product is equivalent to the explicit description of $\mathcal{D}(G, \mathbb{Z}_p)$ reviewed below.
The algebra $\Lambda_{\mathbb{Z}_p} = \mathcal{D}(\mathbb{Z}_p,\ \mathbb{Z}_p)$ is identified with the ring of power series $\mathbb{Z}_p[[T]]$ by Iwasawa's theorem. For $\mu \in \Lambda_{\mathbb{Z}_p}$, the associated series is given by the Fourier–Amice transform

$$\widehat{\mu}(t) = \int_{\mathbb{Z}_p} (1+t)^x d\mu(x) \qquad (t \in \mathbb{Z}_p, |t| < 1)\,.$$

In particular, $\delta(x)$ being the Dirac measure at x :

$$\widehat{\delta(1)} = 1 + T\,,$$

$$\text{so} \qquad T = \widehat{\delta(1)} - \widehat{\delta(0)}\,.$$

In each factor of the decomposition (1.1), we therefore have the Dirac measures :

$$\mu_- = \delta(\begin{pmatrix} 1 & \\ p & 1 \end{pmatrix}), \qquad \widehat{\mu}_- = 1 + Y \in \mathcal{D}(N^-, \mathbb{Z}_p) \cong \cong \mathbb{Z}_p[[Y]]$$

$$\mu_+ = \delta(\begin{pmatrix} 1 & p \\ & 1 \end{pmatrix}), \qquad \widehat{\mu}_+ = 1 + X \in \mathcal{D}(N^+, \mathbb{Z}_p) \cong \cong \mathbb{Z}_p[[X]]$$

$$\mu_0 = \delta(\begin{pmatrix} (1+p) & \\ & (1+p)^{-1} \end{pmatrix}), \quad \widehat{\mu}_0 = 1 + H \in \mathcal{D}(T, \mathbb{Z}_p) \cong \cong \mathbb{Z}_p[[H]]$$

For each factor, $U = N^-$, T or N^+ of G, $\mathcal{D}(U, \mathbb{Z}_p)$ is naturally sent to $\mathcal{D}(G, \mathbb{Z}_p)$, by integrating a function $f \in C(G, \mathbb{Z}_p)$ against $\mu \in \mathcal{D}(U, \mathbb{Z}_p)$ on the U–factor. This map is compatible with the convolution product. We therefore write, unambiguously, Y^n, X^n, H^n $(n \geq 0)$ in $\mathcal{D}(G, \mathbb{Z}_p)$. A distribution λ in this space can then be written uniquely

$$\lambda = \sum_n \lambda_n \, Y^{n_1} \; H^{n_2} \; X^{n_3} \qquad (n \in \mathbb{N}^3) \tag{1.3}$$

with $\lambda_n \in \mathbb{Z}_p$. This is the meaning of the completed tensor product (1.1). The expansion is convergent in $\mathcal{D}(G, \mathbb{Z}_p)$. Of course the product $Y^{n_1} H^{n_2} X^{n_3} := Y^{n_1} \otimes H^{n_2} \otimes X^{n_3}$ is defined as above. This easily follows from Mahler's theorem in several variables (cf. Lazard [4, Théorème 1.2.4]).

It immediately follows from formula (1.2) that the distributions Y, H, $X \in \mathcal{D}(G, \mathbb{Z}_p)$ multiply in the obvious fashion when the variables are taken in the "natural order", i.e.

$$\begin{aligned} Y \otimes H &= Y * H \\ Y \otimes X &= Y * X \\ H \otimes X &= H * X \, , \end{aligned}$$

the convolution product being taken on G. We will simply write, consistent with previous notation :

$$YH = Y * H \, , \; YX = Y * X \, , \; HX = H * X \, . \tag{1.4}$$

To determine the product structure in $\mathcal{D}(G, \mathbb{Z}_p)$ is to understand first the product of monomials in a different order.

Consider first the product HY. It suffices to compute, in G, the product $\mu_0 \mu_- = \delta(h_0)\delta(u_0)$, say. We compute $h_0 u_0 h_0^{-1}$.

Since

$$\begin{pmatrix} t & \\ & t^{-1} \end{pmatrix} \begin{pmatrix} 1 & \\ x & 1 \end{pmatrix} \begin{pmatrix} t^{-1} & \\ & t \end{pmatrix} = \begin{pmatrix} 1 & \\ t^{-2}x & 1 \end{pmatrix},$$

we have $h_0 u_0 h_0^{-1} = u_0^{(1+p)^{-2}}$ if we write the group N^- multiplicatively. The equation

$$\mu_0 \mu_- = \delta(h_0 u_0 h_0^{-1}) \delta(h_0)\,,$$

and the fact that $\mathcal{D}(N^-, \mathbb{Z}_p) \cong \mathbb{Z}_p[[Y]]$ is a homomorphism, show that

$$(1+H)(1+Y) = (1+Y)^q (1+H) \tag{1.5}$$

where we have set

$$q = (1+p)^{-2} \equiv 1 \qquad [p]\,. \tag{1.6}$$

Similarly consider XH. Let n_0 be the generator of N^+. Now $\delta(n_0)\delta(h_0)$ reduces to $h_0^{-1} n_0 h_0$. Again

$$\begin{pmatrix} t^{-1} & \\ & t \end{pmatrix} \begin{pmatrix} 1 & x \\ & 1 \end{pmatrix} \begin{pmatrix} t & \\ & t^{-1} \end{pmatrix} = \begin{pmatrix} 1 & t^{-2}x \\ & 1 \end{pmatrix}\,,$$

so $h_0^{-1} n_0 h_0 = n_0^{(1+p)^{-2}} = n_0^q$, whence

$$(1+X)(1+H) = (1+H)(1+X)^q\,. \tag{1.7}$$

Finally, to express XY we have to decompose

$$n_0 u_0 = \begin{pmatrix} 1 & p \\ & 1 \end{pmatrix} \begin{pmatrix} 1 & \\ p & 1 \end{pmatrix} = \begin{pmatrix} 1+p^2 & p \\ p & 1 \end{pmatrix}\,.$$

Since

$$\begin{pmatrix} 1 & \\ a & 1 \end{pmatrix} \begin{pmatrix} t & \\ & t^{-1} \end{pmatrix} \begin{pmatrix} 1 & b \\ & 1 \end{pmatrix} = \begin{pmatrix} t & tb \\ ta & abt + t^{-1} \end{pmatrix}\,,$$

we see that

$$p = ta = tb$$

with

$$1 + p^2 = t = (1+p)^P\,, \qquad P \in \mathbb{Z}_p\,.$$

This yields, since $t_0 = 1 + p$ is the parameter of h_0 :

$$(1+X)(1+Y) = (1+Y)^Q (1+H)^P (1+X)^Q \tag{1.8}$$

with

$$Q = (1+p^2)^{-1} \equiv 1[p^2]\,,\ P = \frac{\log(1+p^2)}{\log(1+p)}\,. \tag{1.9}$$

For $p > 2$, we have

$$\begin{aligned} \log(1+p) &= p - \tfrac{p^2}{2} + \tfrac{p^3}{3} \cdots = p(1 + O(p)) \\ \log(1+p^2) &= p^2(1 + O(p^2)) \end{aligned}$$

whence

$$P = p(1 + O(p)) . \tag{1.10}$$

Note that we have simply written HY for $H * Y$, etc... This will cause no confusion if we remember that a product such as HY, for variables not in the natural order, is not given by the ostensible product of monomials in the expression (1.3).
To summarize, we have :

PROPOSITION 1.1. *Set $Q = (1 + p^2)^{-1}$, $q = (1 + p)^{-2}$, $P = \frac{\log(1+p^2)}{\log(1+p)}$. Then the elements X, Y, H of $\mathcal{D}(G, \mathbb{Z}_p)$ verify the relations*

(a) $(1 + H)(1 + Y) = (1 + Y)^q(1 + H)$

(b) $(1 + X)(1 + H) = (1 + H)(1 + X)^q$

(c) $(1 + X)(1 + Y) = (1 + Y)^Q(1 + H)^P(1 + X)^Q$.

Consider now the universal, non–commutative p–adic algebra in the variables Y, H, X : thus

$$\mathcal{A} = \mathbb{Z}_p\{\{Y, H, X\}\}$$

is composed of all the non–commutative series

$$f = \sum_{n \geq 0} \sum_i a_i x^i \tag{1.11}$$

where the coefficients $a_i \in \mathbb{Z}_p$ and, for all $n \geq 0$, i runs over all maps $\{1, 2, \dots n\} \longrightarrow \{1, 2, 3\}$; we set $x_1 = Y$, $x_2 = H$, $x_3 = X$ and $x^i = x_{i(1)} \cdots x_{i(n)}$. The topology on $\mathcal{A}$ is the product topology on $\prod_n \mathbb{Z}_p^{I(n)}$ where $I(n)$ is the set of maps ($\equiv$ of non–commutative monomials of degree n). The algebra $\mathcal{A}$ has a maximal ideal $\mathcal{M}_{\mathcal{A}}$ generated by (p, x_1, x_2, x_3) and a prime ideal $\mathcal{P}_{\mathcal{A}}$ generated by (x_1, x_2, x_3). Its topology is given by the powers of $\mathcal{M}_{\mathcal{A}}$.
The non–commutative polynomial algebra

$$A = \mathbb{Z}_p\{Y, H, X\}$$

is a dense subalgebra of $\mathcal{A}$.
Let $\mathcal{R}$ be the closed two–sided ideal generated in $\mathcal{A}$ by the relations (a, b, c).
Our main result is

THEOREM 1.2. *The Iwasawa algebra Λ_G is naturally isomorphic to $\mathcal{A}/\mathcal{R}$.*

The proof will in fact rely on the corresponding result with coefficients in $\mathbb{F}_p$. So let $\Omega_G = \Lambda_G \bigotimes_{\mathbb{Z}_p} \mathbb{F}_p$ be the Iwasawa algebra with finite coefficients, $\overline{\mathcal{A}} = \mathbb{F}_p\{\{Y, H, X\}\}$ the algebra of non–commutative series with coefficients in $\mathbb{F}_p$, with its natural linearly compact topology, given by its maximal ideal $\mathcal{M}_{\overline{\mathcal{A}}}$.
Let $\overline{\mathcal{R}}$ be the image of $\mathcal{R}$ in $\overline{\mathcal{A}}$.

Lemma 1.3. *$\overline{\mathcal{R}}$ is the closed two–sided ideal generated in $\overline{\mathcal{A}}$ by the image of the relations (a, b, c).*

Proof.– Denote by $\mathcal{I} \subset \mathcal{A}$ the ideal generated by the relations ; let $\mathcal{J} \subset \overline{\mathcal{A}}$ be the similar ideal. Then $\mathcal{J}$ is obviously the image of $\mathcal{I}$ in $\overline{\mathcal{A}}$; we denote it by $\overline{\mathcal{I}}$. Let $\overline{\mathcal{R}}$ be the reduction of $\mathcal{R}$, and consider the closure $cl(\overline{\mathcal{I}})$ of $\overline{\mathcal{I}}$ in $\overline{\mathcal{A}}$. If $f \in \mathcal{R}$, we have $f = \lim_n f_n$ $(f_n \in \mathcal{I})$ for the topology given by $(\mathcal{M}_{\mathcal{A}}^N)$. This implies that $\overline{f} = \lim \overline{f}_n$ for the topology given by $\mathcal{M}_{\overline{\mathcal{A}}}^N$ on $\overline{\mathcal{A}}$, thus $\overline{f} \in cl(\overline{\mathcal{I}})$. Conversely assume $\overline{f} \in \overline{\mathcal{A}}$ can be written $\overline{f} = \lim \overline{f}_n$ with $\overline{f}_n \in \overline{\mathcal{I}}$. Then $\overline{f}_n$ is the reduction of a series $f_n \in \mathcal{I} \subset \mathcal{R}$. Since $\mathcal{R}$ is closed and $\mathcal{A}$ compact, we may assume that f_n converges to $g \in \mathcal{R}$. Then, by definition of the topologies, $\overline{f} = \lim \overline{f}_n = \overline{g}$. Thus $cl(\overline{\mathcal{I}}) = \overline{\mathcal{R}}$, which finishes the proof.

Theorem 1.4. *The Iwasawa algebra mod p, Ω_G, is naturally isomorphic to $\overline{\mathcal{A}}/\overline{\mathcal{R}}$.*

The proof of these results will occupy § 2, 3.

2

We consider the natural map

$$A \longrightarrow \Lambda_G$$

given by the universal property of A. Note that the topology of Λ_G, as a distribution algebra, coincides with its topology when it is seen as the algebra of distributions on the commutative group $\mathbb{Z}_p^3$. In particular a basis of neighbourhoods of 0 is given by the family of $\mathbb{Z}_p$–modules $\mathcal{M}_\Lambda^N (\Lambda = \Lambda_G)$, where

$$\mathcal{M}_\Lambda^N = \{\lambda \in \Lambda_G\,,\ \lambda = \sum_n \lambda_n Y^{n_1} H^{n_2} X^{n_3}\,,\ v(\lambda_n) + |n| \geq N\} \tag{2.1}$$

with the usual notation $|n| = n_1 + n_2 + n_3$. For a linear monomial $x = Y$, H or X, we have $w(x) = 1$, w being the function on Λ given by

$$w(\lambda) = \inf_n (v(\lambda_n) + |n|)\,. \tag{2.2}$$

We will use the following deep result of Lazard :

Proposition 2.1 (Lazard). *The valuation w is additive : $w(\lambda * \mu) = w(\lambda) + w(\mu)$ $(\lambda, \mu \in \Lambda_G)$.*

Cf. [4, III 2.3.3]. Lazard proves, in fact, that the associated graded ring is an enveloping algebra, thus an integral domain, and this implies the additivity. I am indebted to the paper of Schneider and Teitelbaum [6] for a lucid exposition of Lazard's results.
In fact, it follows from Lazard's results that $\mathcal{M}_\Lambda^N$ is indeed the N-th power of the maximal ideal $\mathcal{M}_\Lambda$ of Λ_G. Indeed, let J_N be defined by $w(\lambda) \geq N$. It is

easy to check that $J_1 = \mathcal{M}_\Lambda$. The additivity implies that $\mathcal{M}_\Lambda^N$ is contained in J_N. Since every linear monomial belongs to the maximal ideal, the expression (2.1) implies the converse inclusion since $\mathcal{M}_\Lambda^N$ is closed.
Consider now the filtration of $\mathcal{A}$ by the powers of its maximal ideal. It is defined by a valuation $w_\mathcal{A}$ given by a formula similar to (2.2) : if

$$f = \sum_i a_i\ x^i\,,$$
$$w_\mathcal{A}(f) = \inf_i(v(a_i) + |i|)$$

where $|i| = n$ is the degree of i (cf. after (1.11)). We now have the following ("ideal" means two–sided ideal unless otherwise indicated).

Proposition 2.2. *The natural map $\varphi : A \to \Lambda_G$ extends continuously to a surjective homomorphism $\mathcal{A} \to \Lambda_G$. In fact,*

$$\varphi(\mathcal{M}_\mathcal{A}^N) \subset \mathcal{M}_\Lambda^N \qquad (N \geq 0)\,.$$

Proof : The continuity is implied by the stronger property

$$w(\varphi(x^i)) = n = |i| \tag{2.3}$$

where n, as after (1.11), is the degree of the monomial. By induction on n, this follows from Proposition 2.1. If $f \in \mathcal{M}_\mathcal{A}^N$, we have $w_\mathcal{A}(f) \geq N$ and the continuity follows from (2.3) by $\mathbb{Z}_p$–linearity. The surjectivity follows from the fact that φ is already surjective if $\mathcal{A}$ is replaced by the set of linear combinations of well-ordered monomials (i increasing).

Corollary 2.3. *There is a natural, continuous surjection*

$$\mathcal{B} = \mathcal{A}/\mathcal{R} \longrightarrow \Lambda_G\,.$$

Corollary 2.4. *There is a continuous surjection*

$$\overline{\varphi} : \overline{\mathcal{B}} = \overline{\mathcal{A}}/\overline{\mathcal{R}} \longrightarrow \Omega_G\,.$$

This follows from Lemma 1.3.
It follows from Abelian distribution theory that Ω_G is, as a space, isomorphic to

$$\mathbb{F}_p[[Y, H, X]]$$

with the compact topology. An obvious computation shows that

$$\mathcal{M}_\Omega^N = \{\lambda \in \Omega_G : v_\Omega(\lambda) \geq N\}\,,$$

v_Ω being the usual valuation on power series, is the image of $\mathcal{M}_\Lambda^N$. In particular it is an ideal ; for $N = 1$, $\mathcal{M}_\Omega$ is the maximal (two–sided) ideal, and $(\mathcal{M}_\Omega)^N \subset \mathcal{M}_\Omega^N$. (Reduce mod p the corresponding property for Λ.)

Similarly in $\mathcal{A}$, we find that the reduction $\mod p$ (image in $\overline{\mathcal{A}}$) of $\mathcal{M}_{\mathcal{A}}^N$ is the ideal of series

$$\overline{f} = \sum_i \alpha_i \; x^i \qquad (\alpha_i \in \mathbb{F}_p)$$

such that $|i| \geq N$. For $N = 1$ we obtain the maximal ideal in $\overline{\mathcal{A}}$. Furthermore in this case too $(\mathcal{M}_{\overline{\mathcal{A}}})^N = \mathcal{M}_{\overline{\mathcal{A}}}^N$.

3

In this paragraph we will directly study the quotient algebra $\overline{\mathcal{B}} = \overline{\mathcal{A}}/\overline{\mathcal{R}}$, using the properties of the relations (a, b, c).
Consider the natural filtration of $\overline{\mathcal{A}}$ by the powers of $\mathcal{M}_{\overline{\mathcal{A}}}$, which we denote by $F^n\overline{\mathcal{A}}$. We have $F^n\overline{\mathcal{A}}/F^{n+1}\overline{\mathcal{A}} = gr^n\overline{\mathcal{A}} \cong \mathbb{F}_p^{I(n)}$ where $I(n)$ is the set of maps $\{1, \ldots, n\} \to \{1, 2, 3\}$ (§1). The filtration F^n induces a filtration on $\overline{\mathcal{B}} = \overline{\mathcal{A}}/\overline{\mathcal{R}}$:

$$F^n\overline{\mathcal{B}} = F^n\overline{\mathcal{A}} + \overline{\mathcal{R}}$$

whence a graduation

$$\begin{aligned} gr^n\overline{\mathcal{B}} &= F^n\overline{\mathcal{A}} + \overline{\mathcal{R}}/F^{n+1}\overline{\mathcal{A}} + \overline{\mathcal{R}} \\ &= F^n\overline{\mathcal{A}}/F^{n+1}\overline{\mathcal{A}} + (F^n\overline{\mathcal{A}} \cap \overline{\mathcal{R}}) \,. \end{aligned}$$

Let $S_n = S_n(X, Y, Z)$ be the space of commutative polynomials over $\mathbb{F}_p$ of degree n ; thus $\dim S_n = \frac{(n+1)(n+2)}{2}$. Let Σ_n be the space of homogeneous non–commutative polynomials of degree n ; thus $\Sigma_n \to F^n\overline{\mathcal{A}}/F^{n+1}\overline{\mathcal{A}}$, and therefore $\Sigma_n \to gr^n\overline{\mathcal{B}}$, is surjective.

Proposition 3.1. $\dim gr^n\overline{\mathcal{B}} \leq \dim S_n$.

In order to prove this we consider the relations defining $\mathcal{R}$ (or rather $\overline{\mathcal{R}}$). Consider first the relation (a) :

$$(1 + H)(1 + Y) = (1 + Y)^q(1 + H)$$

with $q \equiv 1$ $[p]$. Expanding the power series gives

$$1 + H + Y + HY = (1 + qY + \binom{q}{2} Y^2 + \cdots)(1 + H) \,.$$

We note that $\displaystyle\binom{q}{2} = \frac{q(q-1)}{2} \equiv 0$ $[p]$. Thus in $\overline{\mathcal{A}}/\overline{\mathcal{R}}$:

$$1 + H + Y + HY = (1 + qY)(1 + H) + R(Y)(1 + H) \,,$$

the term $R(Y)$ being of degree ≥ 3, so

$$\begin{aligned} HY &= (q-1)Y + qYH + R_1(Y, H) \\ &= YH + R_1(Y, H) \end{aligned}$$

since $q \equiv 1$, $R_1(Y,H)$ of degree ≥ 3. This shows that in $\overline{\mathcal{B}} = \overline{\mathcal{A}}/\overline{\mathcal{R}}$:

$$HY = YH \mod F^3\overline{\mathcal{B}} \text{ i.e.} \tag{3.1}$$

$$HY = YH \text{ in } gr^2\overline{\mathcal{B}}.$$

The computation for relation (b) is obviously similar, yielding in $\overline{\mathcal{B}}$

$$XH = HX \qquad \mod F^3\overline{\mathcal{B}}. \tag{3.2}$$

Consider now the identity (c) :

$$(1+X)(1+Y) = (1+Y)^Q(1+H)^P(1+X)^Q.$$

We have $Q \equiv 1$ $[p^2]$, $P \equiv p$ $[p^2]$. Again the coefficients $\dfrac{Q(Q-1)}{2}$ of Y^2, X^2 in the power series vanish $\mod p$. Modulo $\mathcal{M}^3_{\overline{\mathcal{A}}}$, whose image is in $F^3\overline{\mathcal{B}}$, we then have

$$(1+X)(1+Y) \equiv (1+QY)(1+H)^P(1+QX).$$

Since $P \equiv p$ $[p^2]$ and since 2 is invertible, $(1+H)^P \equiv 1 \mod (p, H^3)$. Thus

$$1 + X + Y + XY \equiv 1 + QX + QY + Q^2YX \;(\mod F^3\overline{\mathcal{B}}),$$

and since $Q \equiv 1$:

$$XY \equiv YX \qquad (\mod F^3\overline{\mathcal{B}}). \tag{3.3}$$

Since $gr^2\overline{\mathcal{B}}$ is generated by these three monomials and the squares Y^2, H^2, X^2 , the identities (3.1)–(3.3) show that dim $gr^2\overline{\mathcal{B}} \leq 6$, whence the result for $n = 2$. The proposition for general n is deduced from this case. Consider an arbitrary monomial of degree n,

$$x^i = x_{i_1}...x_{i_n}.$$

The following lemma is obvious :

Lemma 3.2. *We can change x^i into a well–ordered monomial $x^{i'}$ (i' increasing) by a sequence of transpositions $x_{i_\alpha}x_{i_{\alpha+1}} \mapsto x_{i_{\alpha+1}}x_{i_\alpha}$.*

(Consider the set of inversions $\{\alpha < \beta : i_\alpha > i_\beta\}$. Assume $i_\gamma > i_{\gamma+1}$, and replace in x^i the term $x_{i_\gamma}x_{i_{\gamma+1}}$ by $x_{i_{\gamma+1}}x_{i_\gamma}$. It is easy to check that the set of inversions decreases by one element.)

We now write $x^i = x^j x_{i_\alpha}x_{i_{\alpha+1}}x^\ell$. We will prove by induction

Lemma 3.3. *In $\overline{\mathcal{B}}$, $x^i \equiv x^{i'} \mod F^{n+1}\overline{\mathcal{B}}$, where i' is well–ordered.*

But this is now equally obvious. Let r, s be the degrees of x^j, x^ℓ, so $n = r+s+2$. Then $x^j \equiv x^{j'}[F^{r+1}\overline{\mathcal{B}}]$, $x^\ell \equiv x^{\ell'}[F^{s+1}\overline{\mathcal{B}}]$ and $x_{i_\alpha}x_{i_{\alpha+1}} \equiv x_{i_{\alpha+1}}x_{i_\alpha}[F^3\overline{\mathcal{B}}]$; we are of course assuming $i_\alpha > i_{\alpha+1}$. Factoring the congruences gives

$x^i \equiv x^{j'} x_{i_{\alpha+1}} x_{i_\alpha} x^{\ell'} [F^{n+1}\overline{\mathcal{B}}]$ since the filtration F^n, image of F^n on $\overline{\mathcal{A}}$, verifies $F^n F^m \subset F^{n+m}$. Using induction if necessary, we obtain the Lemma, whence Proposition 3.1.

Proof of Theorem 1.4.– The natural map $\varphi : \mathcal{A} \to \Lambda_G$ sends $\mathcal{M}^n_{\mathcal{A}}$ to $\mathcal{M}^n_\Lambda$. Since $F^\bullet$ is on $\overline{\mathcal{B}}$ the filtration inherited from the natural filtration on $\overline{\mathcal{A}}$, we see that $\overline{\varphi}$ sends $F^n\overline{\mathcal{B}}$ to $\mathcal{M}^n_\Omega$. We then have a natural map $gr\overline{\varphi} : gr^\bullet\overline{\mathcal{B}} \to gr^\bullet\Omega_G$, surjective since $\overline{\varphi}$ is so. It is an isomorphism since dim $gr^n\overline{\mathcal{B}} \leq$ dim $S_n =$ dim $gr^n\Omega_G$. (The last equality follows from the considerations after Cor.2.4 ; cf also [3, Theorem 7.24]). Therefore $\overline{\varphi}$ is isomorphic since the filtration on $\overline{\mathcal{B}}$ is complete. The last point follows from the fact that $\overline{\mathcal{B}} = \overline{\mathcal{A}}/\overline{\mathcal{R}}$ where $\overline{\mathcal{R}}$ is closed and therefore complete for the filtration induced from that of $\overline{\mathcal{A}}$: see e.g. [5, Thm 4 (5) p. 31].

Proof of Theorem 1.2.– The reduction of $\varphi : \mathcal{A}/\mathcal{R} \to \Lambda_G$ is $\overline{\varphi}$. Recall that $\overline{\mathcal{R}}$ is the image of $\mathcal{R}$ in $\overline{\mathcal{A}}$. Assume $f \in \mathcal{A}$ satisfies $\varphi(f) = 0$. We then have $\overline{f} \in \overline{\mathcal{R}}$ by Theorem 1.3, so $f = r_1 + pf_1$, $r_1 \in \mathcal{R}$, $f_1 \in \mathcal{A}$. Then $\varphi(f_1) = 0$. Inductively, we obtain an expression $f = r_n + p^n f_n$ of the same type. Since $p^n f_n \to 0$ in $\mathcal{A}$ and $\mathcal{R}$ is closed, we see that $f \in \mathcal{R}$, QED.

4

In this section, we show that the description of Λ_G given in § 1 allows one to give different proofs of some results of Ardakov and to understand them in terms of the growth of coefficients in the Iwasawa expansion.
Ardakov's main result in [1] is that the centre of the Iwasawa algebra reduces to the Iwasawa algebra of the centre of G, trivial in our case. We will see that the fact of being central is incompatible with the boundedness of the Iwasawa coefficients.
It will be instructive to compare this behaviour with what happens for the centre of the enveloping algebra. Recall that instead of the Iwasawa distributions, or measures, we can consider the analytic distributions (or hyperfunctions), dual to the locally analytic functions on G (cf. Schneider–Teitelbaum [6]). They admit an expansion (1.3), but with now

$$|\lambda_n| r^{|n|} \longrightarrow 0 \qquad \forall r < 1\,,\ |n| = n_1 + n_2 + n_3\,. \tag{4.1}$$

Among these we have the Casimir operator (seen as a distribution with support at 1)

$$\omega = h^2 + 2(xy + yx) = h^2 - 2h + 4xy$$

(cf. e.g. Borel [2, p. 19]) where h, x, y are the infinitesimal generators of the groups T, N^+, N^-. It suffices to compute ω on a function f given by

$$f(utn) = (1+Y)^{x_1}(1+H)^{x_2}(1+X)^{x_3}$$

where u, t, n have parameters x_1, x_2, $x_3 \in \mathbb{Z}_p$ and Y, H, X belong to the disc $|w| < 1$ in $\mathbb{C}_p$ or even $\mathbb{Q}_p$ (such functions are dense). Now

$$\begin{aligned}
(xyf)(1) &= \frac{d}{dt}\Big|_0 yf(e^{tx}) = \frac{d}{dt}\Big|_0 \frac{d}{ds}\Big|_0 f(e^{sy}e^{tx}) \\
&= \frac{d}{dt}\Big|_0 \frac{d}{ds}\Big|_0 f\left(\begin{pmatrix} 1 & \\ s & 1 \end{pmatrix}\begin{pmatrix} 1 & t \\ & 1 \end{pmatrix}\right) \\
&= \tfrac{\partial^2}{\partial s \partial t}\Big|_0 (1+Y)^{s/p}(1+X)^{t/p} \\
&= \tfrac{1}{p^2}\log(1+Y)\log(1+X)\,,
\end{aligned}$$

$$\begin{aligned}
hf(1) &= \frac{d}{dt}\Big|_0 f\begin{pmatrix} e^t & \\ & e^{-t} \end{pmatrix} \\
&= \frac{1}{\log(1+p)}\frac{d}{dt}\Big|_0 f\begin{pmatrix} (1+p)^t & \\ & (1+p)^{-t} \end{pmatrix} \\
&= \frac{1}{\log(1+p)}\log(1+H)\,, \\
h^2f(1) &= \frac{1}{\log^2(1+p)}\frac{d^2}{dp^2}\Big|_0 f\begin{pmatrix} (1+p)^t & \\ & (1+p)^{-t} \end{pmatrix} \\
&= \frac{1}{\log^2(1+p)}[\log(1+H)]\,,
\end{aligned}$$

Thus the Amice transform of ω is

$$F(Y,H,X) =$$
$$= \frac{1}{\log^2(1+p)}\log^2(1+H) - \frac{2}{\log(1+p)}\log(1+H) + \frac{4}{p^2}\log(1+Y)\log(1+X)\,.$$

This obviously has an expansion (4.1) – and is an element of the ring of convergent series on $D(1)^3$, $D(1) \subset \overline{\mathbb{Q}}_p$ being the open unit disc – but it is not an element of Λ_G.
We will see that the invariance under T suffices to impose such a logarithmic behaviour. This leads to :

Theorem 4.1. *The space of elements on Λ_G invariant by conjugation under T is equal to the Iwasawa algebra $\Lambda_T \subset \Lambda_G$.*

Assume indeed $\lambda \in \Lambda_G$ is T–invariant, with Amice transform

$$F(Y,H,X)\,.$$

We have $Y = u_0 - 1$, with $h_0 u_0 h_0^{-1} = u_0^{(1+p)^{-2}}$; thus the automorphism $Ad(h_0)$ of G sends $1+Y$ to $(1+Y)^{(1+p)^{-2}}$. Similarly, $h_0 n_0 h_0^{-1} = n_0^{(1+p)^2}$, so $1+X$

is sent to $(1+X)^{(1+p)^2}$. Of course H is left invariant. If λ is T–invariant we therefore have

$$F(Y,H,X)=F(Y',H,X') \tag{4.2}$$

where $1+Y'=(1+Y)^{(1+p)^{-2}}$, $1+X'=(1+X)^{(1+p)^2}$. Since $p\neq 2$, $(1+p)^2$ is a topological generator of $1+\mathbb{Z}_p$. Therefore (4.2) remains true if

$$1+Y'=(1+Y)^u\,,\ 1+X'=(1+X)^{u^{-1}}\,,\ u\in 1+p\mathbb{Z}_p\,. \tag{4.3}$$

In the following computations consider F as an element of the Lazard ring in three variables. If we fix a value of H in $\mathbb{C}_p$ such that $|H|<1$, say H_0, $F(Y,H_0,X):=F_1(Y,X)$ becomes an Iwasawa series in the two variables, still invariant under (4.3). Now set

$$U=\log(1+Y)\,,\ V=\log(1+X)\,, \tag{4.4}$$

two series convergent in $D(1)$. We have

$$F_1(Y,X)=G_1(U,V)$$

where G_1 converges absolutely in the domain of convergence of the exponential, i.e. for $|U|,|V|<r_0=p^{-\frac{1}{p-1}}$. Moreover G_1 is invariant by $U\mapsto uU$, $V\mapsto u^{-1}V$, $|u-1|<p^{-1}$. This implies that

$$G_1(U,V)=G_2(UV)$$

with $G_2(z)$ convergent for $|z|<r_0^2$.
Let

$$\begin{aligned}
G_2(z) &= \sum_0^\infty b_q z^q\,,\\
F_1(Y,X) &= \sum_{m,n} a_{mn}Y^mX^n \quad (|a_{mn}|\leq 1)\,.\\
\text{Then}\quad F_1(Y,X) &= G_2(\log(1+Y)\log(1+X))\,,\\
\log(1+Y) &= Y\sum_0^\infty \frac{(-1)^k}{k+1}Y^k := YL_1(Y)\\
\log(1+X) &= X\sum_0^\infty \frac{(-1)^\ell}{\ell+1}Y^\ell := XL_1(X)
\end{aligned}$$

Thus $(\log(1+Y)\log(1+X))^q$ contains only terms the degree of which in Y AND X is at least q. We have of course $b_0=a_0$, and the previous remark implies that

$$\sum_{n\geq 0} a_{1n}\;Y\;X^n+\sum_{m\geq 0} a_{m_1}Y^mX$$

is identical with the sum of terms of these degrees in

$$b_1\ YX\ L_1(Y)L_1(X)\,,$$

i.e. with

$$b_1\ YX\ (L_1(Y)+L_1(X)-1)\,.$$

Since the a_{mn} are integral, this implies that $b_1 = 0$ as the denominators in the log–series are not bounded.
By induction assume that $b_1 = \cdots b_{N-1} = 0$, so

$$G_2 = \sum_N^\infty b_q z^q\,.$$

We then find that

$$F_1(Y,X) = b_N Y^N X^N L_1(Y)^N L_1(X)^N \tag{4.4}$$

+ terms of degree $> N$ in X and Y.

$$\begin{aligned} \text{Now}\quad L_1(Y) &= 1 + YM_1(Y)\,, \quad \text{say}\,,\\ L_1(X) &= 1 + XM_1(X) \end{aligned}$$

so (4.4) implies that

$$\begin{aligned} &F_1(Y,X) = b_N Y^N X^N (1 + NYM_1(Y) + NXM_1(X))\\ &+ \text{terms of degree } > N \text{ in } X \text{ and } Y\,. \end{aligned}$$

Since M_1 does not have bounded denominators, we deduce that $b_N = 0$.
Finally we have proved that $F_1 = b_0$, i.e. $F(Y,H,X) \equiv b_0(H)$ for any $H \in \mathbb{C}_p$, $|H| < 1$, This implies that $F(Y,H,X) = F(H)$ has no terms involving X or Y, whence the result.

Corollary 4.2. *The centre of Λ_G is composed of the multiples of the Dirac measure at* 1.

For assume that $\lambda \in \Lambda_G$ is central, so invariant by all conjugates of T in G. By Thm. 4.1 its support is contained in the intersection of the tori gTg^{-1} $(g \in G)$. This intersection is reduced to $\{1\}$.
We note that Theorem 4.1 itself follows from Ardakov's results [1, Proposition 2.2]: a simple computation shows that the only finite orbits of T in G are the elements of T (use the triangular decomposition).

5

This section is devoted to conjectural remarks on a formal extension of the main result.
Consider the formulas of Proposition 1, for example

(a) $(1+H)(1+Y) = (1+Y)^{(1+p)^{-2}}(1+H)$

(c) $(1+X)(1+Y) = (1+Y)^{(1+p^2)^{-1}}(1+H)^{\frac{\log(1+p^2)}{\log(1+p)}}(1+X)^{(1+p^2)^{-1}}$.

In the p–adic computation the series for, say, $(1+X)^x$ $(x \in \mathbb{Z}_p)$ converges as an Iwasawa expansion because of the integrality of the binomial function $\binom{x}{n}$. However, replace now Λ_G by $k[[Y,H,X]]$ where k is a field of characteristic zero. Set $p = \varepsilon$, another formal variable, which should however be considered as a small parameter. The binomial coefficients, namely

$$\binom{(1+\varepsilon)^{-2}}{n} = \frac{(1+\varepsilon)^{-2}((1+\varepsilon)^{-2}-1)\cdots((1+\varepsilon)^{-2}-n+1)}{n!} \tag{5.1}$$

and similarly

$$\binom{\log(1+\varepsilon^2)/\log(1+\varepsilon)}{n}$$

are well–defined series in $k[[\varepsilon]]$. Formulas (a,b,c) therefore define the products HY, XH and XY in $k[[\varepsilon]][[Y,H,X]]$. The p–adic results do not seem to imply that this extends to an associative product in this ring of power series. Note that if it were so, equations (a,b,c) at $\varepsilon = 0$ would simply yield $HY = YH$, $XH = HX$ and $XY = YX$. Such an extension would therefore define, quite naturally, a formal deformation of the algebra of power series $k[[Y,H,X]]$ associated to the group $SL(2)$. It would be interesting to understand this deformation in group–theoretic terms (or in terms of the Lie algebra) –assuming, of course, it exists. In this respect one should note that formulas (a,b) allow one to define inductively the products H^nY^m and X^nH^m. However I do not see how to define X^nY^m, even granting (c).

References

[1] K. Ardakov, *The centre of completed algebras of pro–p groups*, Documenta Math. 9 (2004), 599–606.

[2] A. Borel, *Automorphic forms on $SL(2,\mathbb{R})$*, Cambridge Univ. Press, 1997.

[3] J.D. Dixon, M.P.F. Du Sautoy, A. Mann, D. Segal, *Analytic pro-p groups*, 2nd edition, Cambridge University Press (1999).

[4] M. Lazard, *Groupes analytiques p–adiques,* Publ. IHES 26 (1965), 389–603.

[5] Li Huishi, F. van Oystaeyen, *Zariskian filtrations,* Kluwer, 1997.

[6] P. Schneider, J. Teitelbaum, *Algebras of p–adic distributions and admissible representations,* Inv. Math. 153 (2003), 145–196.

[7] J.–P. Serre, *Algèbres de Lie semi–simples complexes,* Benjamin, 1966.

[8] R. Steinberg, *Lectures on Chevalley groups,* mimeographed notes, Yale University, 1967.

[9] L. Washington, *Introduction to cyclotomic fields,* Springer, 1982.

Laurent Clozel
Mathématique
Université Paris-Sud 11
Bât. 425
91405 Orsay CEDEX
France