Hangzhou Summer School by R. Sujatha

Lecture Course on Aspects of non Commutative Algebra.

Lecture I: Background on Iwasawa Algebras.

- If R is a noncommutative ring, module will mean a left R-module.

§: Compact p-adic Analytic groups: p a prime.

Def: A topological space X is a p-adic analytic manifold if there is an atlas of p-adic charts on X; i.e:

$\exists$ a triple $\{(U_i, \phi_i, n_i) \mid i \in I\}$ where

- $\forall\ i \in I$, $U_i \subseteq X$ is open and ϕ_i is a homeomorphism of U onto an open subset of $\mathbb{Z}_p^{n_i}$
- $\forall\ i, j \in I$, (U_i, ϕ_i, n_i) and (U_j, ϕ_j, n_j) are compatible in the usual sense [(pairwise compatible); $\phi_j \cdot \phi_i^{-1}|_{\phi_i(U_i \cap V)}$ and $\phi_i \cdot \phi_j^{-1}|_{\phi_j(U_i \cap V)}$ are analytic functions on $\phi_i(U_i \cap V)$ and $\phi_j(U_i \cap V)$].
- $X = \bigcup_{i \in I} U_i$

(Here analytic functions means that they are given by formal power series over $\mathbb{Q}_p$ in finitely many variables.

A p-adic analytic group G is a topological group which is a p-adic analytic manifold, along with a group structure such that the group operations are given by analytic functions. If G is in addition compact, it is a compact p-adic analytic group.

Eg. : i) $(\mathbb{Q}_p, +)$, $X = Gl_n(\mathbb{Q}_p)$ with subspace topology from $M_n(\mathbb{Q}_p) \simeq \mathbb{Q}_p^{n^2}$ are p-adic analytic groups.

ii) $\mathbb{Z}_p$, $\mathbb{Z}_p^r$, $(Gl_n(\mathbb{Z}_p), \cdot)$, $(U_n = Id + p M_n(\mathbb{Z}_p), \cdot)$ are compact p-adic analytic groups.

Recall that a profinite group is an inverse limit of finite groups; it is compact and totally disconnected.

Eg. i) Galois groups of fields

ii) If Γ is a group and $\mathcal{N}$ a family of normal subgroups of finite index in Γ, directed by reverse inclusion, then the family $(\Gamma/N)_{N \in \mathcal{N}}$ of quotients forms an inverse system of finite groups and the inverse limit

$$\hat{\Gamma}_{\mathcal{N}} = \varprojlim (\Gamma/N)_{N \in \mathcal{N}}$$

is a profinite group.

There is a natural homomorphism

$$\Gamma \longrightarrow \hat{\Gamma}_{\mathcal{N}}$$

with kernel $K = \bigcap_{N \in \mathcal{N}} N$, and $\Gamma/K \hookrightarrow \hat{\Gamma}_{\mathcal{N}}$ is a dense embedding. In this case $\hat{\Gamma}_{\mathcal{N}}$ is called the profinite completion of Γ.

ii) $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n$ is a profinite group. In fact, it is a pro-p group, i.e. a projective limit of p-primary groups.

Iwasawa algebras: Let G be a compact p-adic analytic group. The Iwasawa algebra

$$\Lambda(G) = \mathbb{Z}_p[[G]] := \varprojlim_{N \triangle^o G} \mathbb{Z}_p[G/N],$$

where the inverse limit is taken over open normal subgroups of G. Note that G/N is finite and $\mathbb{Z}_p[G/N]$ denotes the usual group ring.

- $\mathbb{Z}_p[G] \longrightarrow \mathbb{Z}_p[[G]]$

as a dense embedding.

Example: Let Γ be a topological group isomorphic to $\mathbb{Z}_p$ and considered multiplicatively. Let γ be a fixed generator so that the isomorphism may be written

$$\begin{aligned} \mathbb{Z}_p &\longrightarrow \Gamma \\ x &\longmapsto \gamma^x \end{aligned}$$

Let $\Gamma_n = \Gamma/\Gamma^{p^n} \simeq \mathbb{Z}/p^n$, so that Γ_n is cyclic of order p^n, generated by the image of γ. We have a commutative diagram

$$\begin{array}{ccc} \mathbb{Z}_p[\Gamma_{n+1}] & \longrightarrow & \mathbb{Z}_p[T]/(T^{p^{n+1}}-1) \\ \downarrow & & \downarrow \\ \mathbb{Z}_p[\Gamma_n] & \longrightarrow & \mathbb{Z}_p[T]/(T^{p^n}-1) \end{array}$$

Let $X = T-1$, then clearly $\mathbb{Z}_p[T] \simeq \mathbb{Z}_p[X]$ and

$$\mathbb{Z}_p[T]/(T^{p^n}-1) \simeq \mathbb{Z}_p[X]/((X+1)^{p^n}-1).$$

Let

$$h_n = h_n(X) = (1+X)^{p^n} - 1;$$

then

$$h_n = X^{p^n} + \dots$$

with all coefficients other than the leading coefficient being divisible by p.

Def: Such a polynomial is called distinguished.

We first define a homomorphism

$$\epsilon : \mathbb{Z}_p[[X]] \longrightarrow \varprojlim \mathbb{Z}_p[X]/(h_n).$$

To do this, first note that if h is a distinguished polynomial, then

$$\mathbb{Z}_p[X]/(h) \simeq \mathbb{Z}_p[[X]]/(h). \qquad (1)$$

Indeed, this will follow from the Euclidean algorithm which we shall prove below, as a consequence of which both the modules in (1) will be free $\mathbb{Z}_p$-modules of rank equal to degree h. We thus obtain a natural map for each n, compatible with the projections,

$$\mathbb{Z}_p[[X]] \longrightarrow \mathbb{Z}_p[\Gamma_n] = \mathbb{Z}_p[X]/(h_n),$$

and hence a homomorphism

$$\epsilon : \mathbb{Z}_p[[X]] \longrightarrow \varprojlim \mathbb{Z}_p[X]/(h_n).$$

Theorem 1: The map ϵ is an isomorphism.

pf: clearly $h_0(X) \in (p, X)$, and as

$$\frac{h_{n+1}(X)}{h_n(X)} = \frac{(1+X)^{p^{n+1}} - 1}{(1+X)^{p^n} - 1},$$

an induction argument shows that $h_k(X) \in (p, X)^{k+1}$. Hence, if $f \in \mathbb{Z}_p[[X]]$ maps to zero, then $f \in \bigcap_{n=0}^{\infty} \langle h_n \rangle$, and hence $f \in \bigcap_{n=0}^{\infty} (p, X)^n$ and this is zero.

To see surjectivity, note that if $m \geq n \geq 0$, then $f_m(X) - f_n(X) \in \langle h_n \rangle$, hence $\{f_0, f_1, \dots\}$ forms a Cauchy sequence in $\mathbb{Z}_p[X]$ with respect to the topology of the maximal ideal (p, X). As $\mathbb{Z}_p[[X]]$ is the completion of $\mathbb{Z}_p[X]$ with respect to this topology, $\lim\{f_m\}$ exists and gives an element $f \in \mathbb{Z}_p[[X]]$, which maps to $(f_0, f_1, \dots)$. //

Lemma 2: (Euclidean algorithm) Let R be a complete local ring with maximal ideal m_R. Let $f(X) = \sum_{i=0}^{\infty} a_i X^i$ be a power series in $R[[X]]$, such that not all $a_i \in m_R$. Suppose $a_0, \dots, a_{n-1} \in m_R$, and $a_n \notin m_R$. Then given $g \in R[[X]]$, we can solve the equation

$$g = qf + r$$

uniquely with $q \in R[[X]]$ and $r \in R[X]$ with degree $r \leq n-1$.

pf: Let α and $\tau = \tau_n$ be the operators defined as follows:

$$\alpha : R[[X]] \longrightarrow R[[X]]$$
$$\sum_{i=0}^{\infty} b_i X^i \longmapsto \sum_{i=0}^{n-1} b_i X^i = b_0 + b_1 X + \dots + b_{n-1} X^{n-1}.$$

$$\tau : R[[X]] \longrightarrow R[[X]]$$
$$\sum_{i=0}^{\infty} b_i X^i \longmapsto b_n + b_{n+1} X + b_{n+2} X^2 + \dots$$

clearly,

- $\tau(x^n h) = h \quad \forall\ h \in R[[X]]$
- $\tau(h) = 0$ if and only if h is a polynomial of degree $< n$.

Hence existence of q, r as in the theorem is equivalent to the condition that there exists q such that

$$\tau(g) = \tau(qf).$$

Now

$$f = \alpha(f) + x^n \tau(f)$$

Hence our problem is equivalent to solving

$$\tau(g) = \tau(q(\alpha(f) + x^n \tau(f))) = \tau(q\alpha(f)) + \tau(q x^n \tau(f)).$$

But $\tau(q x^n \tau(f)) = \tau(x^n q \tau(f)) = q\tau(f)$.

Hence we need to solve

$$\tau(g) = \tau(q\alpha(f)) + q\tau(f). \qquad (2)$$

Note that $\tau(f)$ is invertible because we have assumed $a_n \in R^*$.

Put $z = q\tau(f)$, then (2) is equivalent to

$$\tau(g) = \tau\left(z \frac{\alpha(f)}{\tau(f)}\right) + z$$

$$= \left(1 + \tau \cdot \frac{\alpha(f)}{\tau(f)}\right) z .$$

Here $\tau \circ \left(\frac{\alpha(f)}{\tau(f)}\right)(p)$ for $p \in R[[X]]$ is $\tau\left(p \cdot \frac{\alpha(f)}{\tau(f)}\right)$.

But $\tau \cdot \frac{\alpha(f)}{\tau(f)} : R[[X]] \longrightarrow m_R \cdot R[[X]]$

because, by hypothesis, $\alpha(f)/\tau(f) \in m_R \cdot R[[X]]$. Therefore $\left(1 + \tau \cdot \frac{\alpha(f)}{\tau(f)}\right)$ is invertible in $R[[X]]$ and hence we can solve for z, namely $z = \left(1 + \tau \cdot \frac{\alpha(f)}{\tau(f)}\right)^{-1} \tau(g)$. * → This uses the fact that R is complete and the above property of $\tau \circ \frac{\alpha(f)}{\tau(f)}$ noting that $\left(1 + \tau \circ \frac{\alpha(f)}{\tau(f)}\right)^{-1} = 1 - \tau \circ \frac{\alpha(f)}{\tau(f)} + \left(\tau \cdot \frac{\alpha(f)}{\tau(f)}\right)^2 - \cdots$

This proves both existence and uniqueness.

Theorem 3: (Weierstrass preparation) The power series f in the above lemma can be written in the form

$$f(X) = (X^n + b_{n-1}X^{n-1} + \cdots + b_0)u,$$

where $b_i \in m_S$ and u is a unit in $R[[X]]$.

Proof: By Lemma 2, we may write

$$X^n = qf + r;$$

now q is invertible because we have

$$q = c_0 + c_1 X + \cdots, \quad f = a_0 + \cdots + a_n X^n + \cdots, \text{ with}$$

$a_i \in m_S$ for $0 \le i \le n-1$ and $a_n \in R^\times$.

This gives

$$c_0 a_n \equiv 1 \pmod{m_S}$$

so that c_0, and hence q is a unit. Thus we get

$$qf = X^n - r, \text{ and } f = q^{-1}(X^n - r), \text{ with } r \equiv 0 \pmod{m_S}.$$

Remark: An induction argument using Lemma 2, will show that if $G \simeq \mathbb{Z}_p^d$, $d \ge 1$, then $\Lambda(G) \simeq \mathbb{Z}_p[[T_1, \ldots, T_d]]$. If $\gamma_1, \ldots, \gamma_d$ are (fixed) topological generators for G, then under this isomorphism $\gamma_i \longmapsto (T_i + 1)$.

We will next show that if G is a pro-p group, then the Iwasawa algebra $\Lambda(G)$ is a local ring

Lemma 4: Suppose that $R = \varprojlim R_i$ and each map $\varphi_i : R \longrightarrow R_i$ is a non-zero surjective ring homomorphism. If each R_i is a profinite local ring, then R is a profinite local ring.

Pf:

- A profinite ring is a local ring if it has a unique maximal open right ideal. First observe that if R is a local ring, then its maximal right ideal I is a two sided ideal. Clearly $Iu \subseteq I \ \forall u \in I$ If $u \in R/I$, then the map $x \longmapsto ux + I$ is a non-zero module homomorphism φ from $R \longrightarrow R/I$. But R/I is simple and the kernel of $\varphi = I$. Hence $uI \subseteq I$ and I is two-sided.

Now if J_1, J_2 are two open maximal right ideals, then $J_1 \cap J_2$ is open. As $\{\ker \varphi_i\}$ forms a basis of open nbhds of R, we see that $\ker \varphi_i \subseteq J_1 \cap J_2$ for some i.

$$\varphi_i : R \longrightarrow R_i$$

But as R_i is local, the images of J_1 and J_2 are equal, being maximal open right ideals in R_i. Hence J_1 and J_2 are themselves equal. //

Lemma 5: Let k be a commutative profinite ring and G a pro-p group. If k is a pro-p local ring, then the completed group algebra $k[[G]]$ is a profinite local ring.

Pf: We have $k[[G]] = \varprojlim k_i[G_i]$, where k_i is a p-primary ring and G_i is a finite p-group. By Lemma 4, it suffices to show that $k_i[G_i]$ is local for each i.

Let J be a maximal right ideal for $k_i[G_i]$ and M be the simple $k_i[G_i]$-module, $k_i[G_i]/J$. Then M is finite and hence has order a power of p. We need the following lemma:

Lemma 6: Suppose that P is a finite p-group and A is a simple P-module of order a power of p. Then $|A| = p$ and $A = A^P$; (where $A^P = \{a \in A \mid pa = a \ \forall\, p \in P\}$.

pf: First note that A^P is a P-submodule of A and hence A^P is either 0 or all of A. Now A is the disjoint union of its orbits and the orbit of $x \in A \setminus A^P$ has cardinality a power of p. This forces $A = A^P$, which in turn makes all subgroups of A, P-submodules and hence $|A| = p$ as it is assumed to be simple. //

We return to the proof of Lemma 5. By Lemma 6, we see that $m(g-1) = 0 \ \forall\, m \in M$ and $g \in G_i$. In particular, taking $m = [1]$ in $k_i[G_i]/J$, we see that $(g-1) \in J \ \forall\, g \in G_i$. This implies that the augmentation ideal

$$I = \ker(k_i[G_i] \longrightarrow k_i),$$

which is generated by $(g-1)$, $g \in G$, is contained in J. But k_i is local and therefore the image of J in $k_i[G_i]/I = k_i$ must be the unique maximal right ideal of k_i, so that $J = I + m_{k_i}$, where m_{k_i} = maximal ideal of k_i. Hence $k_i[G_i]$ is local. //

Corollary 7: Let G be a pro-p p-adic Lie group. Then the Iwasawa algebra $\Lambda(G) = \mathbb{Z}_p[[G]]$ is local.

Our next aim is to show that if G is any compact p-adic Lie group, then the Iwasawa algebra $\Lambda(G)$ is semi-local. Let us quickly recall some definitions:

Def: a) The radical of a ring A, denoted $\underline{r}(A)$, is the intersection of all left maximal ideals of A.

- It can be shown that $\underline{r}(A)$ is a two sided ideal and in fact has other characterisations.

b) A ring A is semi-simple if it is a finite product $\prod_{i=1}^{k} M_{n_i}(D_i)$, where D_i is a division ring.

- Again, there are various equivalent definitions of semi-simplicity.

c) A ring A is said to be semi-local if ~~the radical of A is such that A is semi-simple, or equivalently,~~ $\frac{A}{\underline{r}(A)}$ is left and right Artinian.

eg. Semisimple rings are semi-local.

- If A is commutative, this is equivalent to A having only finitely many maximal ideals. But for non commutative rings the above definition implies that A has only finitely many maximal ideals, but the converse implication need not be true.

We shall also need some general facts and definitions from the theory of p-adic Lie groups.

FACT AG 1 : Every p-adic analytic group which is compact, contains an open pro-p subgroup.

- This is a very weak version of the existence of pro-p open subgroups with more properties, we will need them later. This is contained in Lazard's work, see also "Analytic Pro-p groups" by Dixon, du Sautoy et al, chapter 8.

- Since, for the purposes of Iwasawa algebras arising in number theory, we shall be mainly interested in compact (closed) subgroups of $GL_n(\mathbb{Z}_p)$, we shall illustrate our facts for this specific class of p-adic Lie groups. In this case, it is known that (easily seen)

$$G_1 := \mathrm{Ker}\{GL_n(\mathbb{Z}_p) \longrightarrow GL_n(\mathbb{F}_p)\}$$

is pro-p and open, normal in $GL_n(\mathbb{Z}_p)$. If H is any closed subgroup of $GL_n(\mathbb{Z}_p)$, then $H \cap G_1$ is an open pro-p subgroup of H.

Now therefore let G be a compact p-adic Lie group and G' an open normal subgroup (necessarily of finite index in G). Let $R = \Lambda(G')$ and $S = \Lambda(G)$. It is easy to see that the following are true:

(a) $R \subseteq S$ is a subring and S is finitely generated as an R-module. In fact $S = \sum_{i=1}^{n} a_i R$, where $\{a_i\}$ is a set of representatives for the cosets in G/G'.

(b) As G' is normal in G, $a_i R = R a_i$; hence S is a finite normalizing extension of R.

In this case, it is a well-known result in non-commutative algebra (cf. McConnell-Robson, chapter 10, Cor 4.15) that $\underline{r}(R) = \underline{r}(S) \cap R$. We can use this to now prove

Theorem 8: Let G be a compact p-adic analytic group. Then the Iwasawa algebra $\Lambda(G)$ is semi-local.

pf: Let G' be a pro-p open normal subgroup of G so that $\Lambda(G') \subseteq \Lambda(G)$ and $\Lambda(G)$ is a finite normalizing extension of $\Lambda(G')$. We know that the ring $\Lambda(G)$ is a local ring. Hence $\underline{r}(\Lambda(G'))$ is the maximal ideal and $\frac{\Lambda(G')}{\underline{r}(\Lambda(G'))}$ is $\mathbb{F}_p$. On the other hand, by the result quoted above, we see that $\frac{\Lambda(G')}{\underline{r}(\Lambda(G'))} \hookrightarrow \frac{\Lambda(G)}{\underline{r}(\Lambda(G))}$ is a finite extension and hence $\frac{\Lambda(G)}{\underline{r}(\Lambda(G))}$ is Artinian, thereby establishing that $\Lambda(G)$ is semi-local. //

Recall that the prime radical of a ring A, denoted $\underline{n}(A)$ is the intersection of all prime ideals of A. It contains all the nilpotent elements of the ring A. Any ideal $I \subseteq \underline{n}(A)$ is nilpotent in the sense $I^n = 0$. (Recall that an ideal P in A is said to be prime if A/P is a prime ring; where a ring R is prime if $0 \neq a, b \in R$, then $aRb \neq 0$.)

A ring A is said to be semiprime if $\underline{n}(A) = 0$.

We shall now prove that $\Lambda(G)$ is semi prime for G a compact p-adic analytic group. The original proof when G is pro-p is due to A. Neumann (Arch. Math. Vol. 51, 496-499, (1988)) and P. Schneider noticed that it works for any compact p-adic group G.

Lemma 9: Let G be any group. Then the group ring $\mathbb{Z}_p[G]$ is semi-prime.

Pf: For $x = \sum x_g g \in \mathbb{Z}_p[G]$, define $tr(x) := x_1$. It can be checked that if x is nilpotent, then $tr(x) = 0$. Let $I \subseteq \mathbb{Z}_p[G]$ be an ideal such that $I^2 = 0$, consider an element $x \in I$. For all $g \in G$, $xg^{-1} \in I$ and hence xg^{-1} is also nilpotent. In particular, this implies that $tr(xg^{-1}) = x_g = 0 \ \forall g$. Hence $x = 0$ and $\mathbb{Z}_p[G]$ is semi-prime as we have shown that it contains no nonzero nilpotent ideals.

Proposition 10: Let G be a compact p-adic analytic group. Then the Iwasawa algebra $\Lambda(G)$ is semi-prime.

Pf: We shall show that G has no nonzero nilpotent ideals. Let J be a non zero ideal of $\Lambda(G)$; then for some open normal subgroup N of G, the image of J in $\mathbb{Z}_p[G/N]$ is not zero (here we are using the fact that $\mathbb{Z}_p[G] \hookrightarrow \mathbb{Z}_p[[G]]$) and as the latter is semiprime, $J^2 \neq 0$.

We shall next show that $\Lambda(G)$ is a left and right Noetherian ring. The strategy we shall employ is the following. Suppose that $R \subseteq \Lambda(G)$ is a subring such that $\Lambda(G)$ is finite as an R-module. Then it is clear that if R is Noetherian, then $\Lambda(G)$ is noetherian. We shall show that G has an open normal subgroup G' with the property that $\Lambda(G')$ is left and right noetherian. In fact, $\Lambda(G')$ will have the additional property that it is an integral domain i.e. has no zero divisors.

Def : (Lazard, chap. III, Def. 2.1.2) A <u>p-valuation</u> on G is a function $\omega : G \longrightarrow (0, \infty]$ satisfying the following axioms for all g and h in G :

(i) $\omega(1) = \infty$ and $\frac{1}{p-1} < \omega(g) < \infty$ for $g \neq 1$.

(ii) $\omega(gh^{-1}) \geq \min\{\omega(g), \omega(h)\}$.

(iii) $\omega(g^{-1}h^{-1}gh) \geq \omega(g) + \omega(h)$

(iv) $\omega(g^p) = \omega(g) + 1$.

We say that G is <u>p-valued</u> if it possesses a p-valuation.

<u>Facts about p-valued groups</u> :

- If G is p-valued, then G is automatically pro-p and has no element of order p.
- Any closed subgroup of a p-valued group is p-valued.

Eg : $G = Gl_n(\mathbb{Z}_p)$; if p is odd, the Congruence subgroup G_1 is p-valued.

If $p = 2$, then $G_1 := \ker(Gl_n(\mathbb{Z}_2) \longrightarrow Gl_n(\mathbb{Z}/4\mathbb{Z}))$ is p-valued.

More generally, if $p > n+1$, then Lazard (p. 101) has proven that every closed pro-p subgroup of $Gl_n(\mathbb{Z}_p)$ is p-valued.

- Any compact p-adic analytic group contains an open normal subgroup which is p-valued.
- For $p \geq n+1$, any closed pro-p subgroup of $Gl_n(\mathbb{Z}_p)$ is p-valued.

We shall show that if G is a p-valued, p-adic analytic group, then $\Lambda(G)$ is left and right Noetherian and has no zero divisors. This will be done using techniques from filtered and graded rings. We quickly recall some of these.

Filtered rings: A ring R is a filtered ring if there is an ascending chain of additive subgroups of R, $\{F_n R\}_{n \in \mathbb{Z}}$ such that:

$1 \in F_0 R$, $F_n R \subseteq F_{n+1} R$ and $F_n R \, F_m R \subseteq F_{n+m} R$ $\forall\, m, n \in \mathbb{Z}$.

- The filtration is exhaustive if $\bigcup_n F_n R = R$
- The filtration is separated if $\bigcap_n F_n R = 0$
- R is said to be complete (w.r.t. the filtration topology) if R is separated and every Cauchy sequence in R converges. As usual, Cauchy sequences are defined w.r.t. the filtration topology.

Similary filtered modules are defined to be R-modules M equipped with a filtration $(F_n M)_{n \in \mathbb{Z}}$ with the property that $F_n R \cdot F_k M \subseteq F_{n+k} M$. Given a filtered ring (resp. module) R (resp. M), we can form the associated graded ring $Gr R$ (resp. $Gr M$) defined by

$$Gr R = \bigoplus_{n \in \mathbb{Z}} \frac{F_n R}{F_{n-1} R}, \qquad Gr M = \bigoplus_{n \in M} F_n M / F_{n-1} M.$$

Clearly $\mathrm{Gr}M$ is a $\mathrm{Gr}R$-module. We also have the Principal symbol map $\#$,

$$\#: R \longrightarrow \mathrm{Gr}R, \quad M \longrightarrow \mathrm{Gr}M,$$
$$r \longmapsto r^{\#}, \quad m \longmapsto m^{\#},$$

where $r^{\#} \in F_nR/F_{n-1}R$ ($m^{\#} \in F_nM/F_{n-1}M$) is the class of r in $F_nR/F_{n-1}R$ (resp. of m in $F_nM/F_{n-1}M$) and where r (resp. m) belongs to $F_nR \setminus F_{n-1}R$ (resp. $F_nM \setminus F_{n-1}M$). We stress that $\#$ is only a map, note however that on R it has the property that if $r, s \in R$, then if $\mathrm{Gr}R$ is a domain, we have

$$(rs)^{\#} = r^{\#}s^{\#}.$$

Theorem 11: Suppose R is a complete filtered ring with filtration $F.R$ and M is an R-filtered module with separated exhaustive filtration $F.M$. If $\mathrm{Gr}M$ is finitely generated as a $\mathrm{Gr}R$-module, then M is finitely generated as an R-module.

pf: clearly, we may choose a finite set of homogeneous generators, $m_1^{\#}, m_2^{\#}, \ldots m_k^{\#}$, say, for $\mathrm{Gr}M$ considered as a GR-module where $m_i \in F_{k_i}M \setminus F_{k_i-1}M$ for some $k_i \in \mathbb{Z}$. Let $m_1, \ldots, m_s$ be lifts in $F_{k_i}M$. If $(GM)_n$ denotes the homogeneous elements of degree n in $\mathrm{Gr}M$, then

$$(\mathrm{Gr}M)_n = \sum_{i=1}^{s} (GR)_{n-k_i} m_{k_i};$$

$$F_nM = \sum_{i=1}^{s} F_{n-k_i}R \cdot m_i + F_{n-1}M.$$

Let $m \in M$; as the filtration is exhaustive, we can choose an $n \in \mathbb{Z}$ such that $m \in F_n M$ and $m \notin F_{n-1} M$. Then

$$m = \sum_{i=1}^{s} r_{n-k_i} m_i + m_{n-1} \quad , \quad r_{n-k_i} \in F_{n-k_i} R, \; m_{n-1} \in F_{n-1} M.$$

Similarly, write

$$m_{n-1} = \sum_{i=1}^{s} r_{n-k_i-1} m_i + m_{n-2} \; , \; r_{n-k_i-1} \in F_{n-k_i-1} R, \; m_{n-2} \in F_{n-2} M,$$

$$\Rightarrow m = \sum_{i=1}^{s} r_{n-k_i} m_i + \sum_{i=1}^{s} r_{n-k_i-1} m_i + m_{n-2} = \sum_{i=1}^{s} (r_{n-k_i} + r_{n-k_i-1}) + m_{n-2}.$$

Proceeding in this fashion, we get for each $q \geq 0$,

$$m - \sum_{i=1}^{s} \Big(\sum_{j=1}^{q} r_{n-k_i-j} \Big) m_i = m_{n-q-1} \in F_{n-q-1} M, \; r_{n-k_i-j} \in F_{n-k_i-j} R.$$

Since R is complete, we may define

$$r_i = \sum_{j=1}^{\infty} r_{n-k_i-j} \quad \text{for } 1 \leq i \leq s.$$

Now

$$\begin{aligned} m - \sum_{i=1}^{s} r_i m_i &= m - \sum_{i=1}^{s} \Big(\sum_{j=1}^{\infty} r_{n-k_i-j} \Big) m_i \\ &= m - \sum_{i=1}^{s} \Big(\sum_{j=1}^{q} r_{n-k_i-j} \Big) m_i - \sum_{i=1}^{s} \Big(\sum_{j=q+1}^{\infty} r_{n-k_i-j} \Big) m_i \\ &= m_{n-q-1} - \sum_{i=1}^{s} \Big(\sum_{j=q+1}^{\infty} r_{n-k_i-j} \Big) m_i \\ &\in F_{n-q-1} M \quad \forall \, q. \end{aligned}$$

But M is separated $\Rightarrow m = \sum_{i=1}^{s} r_i m_i$,

hence $M = \sum_{i=1}^{s} F_{n-k_i} R \, m_i = \sum_{i=1}^{s} R m_i$,

which proves that M is finitely generated as an R-module.

$\square$

Prop. 12 : Suppose R as in the above theorem. Then if $\mathrm{Gr} R$ is an (integral) domain, so is R.

Pf: Let $r, s \in R$ such that $rs = 0$. This implies that

$$(rs)^{\#} = r^{\#} s^{\#} = 0$$

and so GR is a domain and the filtration on R is separated, $\gamma=0$ or $\delta=0$. //

We shall use these results to show that G is a p-valued p-adic Lie group, then the Iwasawa algebra $\Lambda(G)$ is a Noetherian (left and right) domain. The main thrust of the proof consists of showing that under this hypothesis, $\Lambda(G)$ possesses an exhaustive, complete separated filtration such that the associated graded ring $Gr(\Lambda(G))$ is a polynomial ring over $\mathbb{F}_p$. We shall content ourselves with sketching a proof of this, referring to [CSS, Prop. 7.2] and [Lazard] for complete details.

Lemma 13: Suppose that G is a p-valued analytic group. Then there exists a p-valuation w' on G such that, for all $g \in G$ with $g \neq 1$, $w'(g) \in e^{-1}\mathbb{Z}$, for some fixed integer $e \geq 1$, and $gr_{w'}(G)$ is an abelian Lie algebra over $\mathbb{F}_p[\pi]$.

pf: (Sketch) Step 1: Use Lazard's results to show that G has finite rank in the following sense: if G is p-valued.

for any profinite group P, define the Frattini subgroup of P, denoted $\Phi(P)$, by

$$\Phi(P) = \bigcap \{M \mid M \text{ is a maximal proper open subgroup of } P\}.$$

One of the definitions for the rank of P, denoted $r(P)$ is

$$r(P) = \dim_{\mathbb{F}_p}\left(P/\Phi(P)\right).$$

Step 2: $\mathbb{F}_p[\pi]$-action on $gr_w(G)$:

In fact, if G is p-valued, we have the closed normal subgroups

$$G_{\omega,\nu} = \{g \in G : \omega(g) \geq -\nu\}, \quad G_{\omega,\nu^+} = \{g \in G : \omega(g) > -\nu\},$$

for $\nu \in \mathbb{R}$. These subgroups are also open in G, and the natural map

$$G \xrightarrow{\sim} \varprojlim G/G_{\omega,\nu}$$

is an isomorphism. Put

$$\mathrm{Gr}_\omega(G) = \bigoplus_{\nu \in \mathbb{R}} \frac{G_{\omega,\nu}}{G_{\omega,\nu^+}}.$$

One shows that the commutator induces a Lie bracket on $(L,]_\omega)$ $\mathrm{Gr}_\omega(G)$ which makes it into a graded Lie algebra over $\mathbb{F}_p$. Let $\mathbb{F}_p[\pi]$ denote the polynomial ring in one variable π over $\mathbb{F}_p$, viewed as a graded algebra over $\mathbb{F}_p$, with π of degree -1. The map

$$\Pi : g\, G_{\omega,\nu^+} \longmapsto g^p\, G_{\omega,(\nu-1)^+}$$

is $\mathbb{F}_p$-linear on $\mathrm{Gr}_\omega(G)$, and homogeneous of degree -1. Further $[\Pi \bar{g}, \bar{h}]_\omega = \Pi [\bar{g}, \bar{h}]_\omega$ for homogeneous elements $\bar{g}, \bar{h}$ of $\mathrm{Gr}_\omega(G)$. Making π act via Π, it is easily seen that $\mathrm{Gr}_\omega(G)$ becomes an $\mathbb{F}_p[\pi]$-module.

Step 3: Modify the given p-valuation ω to another p-valuation ω' on G such that $\omega'(g) \in \mathbb{Q}$ (a priori $\omega'(g) \in \mathbb{R}$) for all $g \neq 1$ and such that $\mathrm{gr}_{\omega'}(G)$ is an abelian Lie algebra, while it still retains the property of being finitely generated over $\mathbb{F}_p[\pi]$.

Step 4: Show that ω' in Step 3 can be chosen so that $\omega'(G \setminus \{1\}) \subseteq a_1 + \mathbb{N}_0 \cup \dots \cup a_r + \mathbb{N}_0$ for finitely many rational numbers $a_1, \dots, a_r$. Now choose e to be a common denominator for $a_1, \dots, a_r$. //

We use this to prove

Proposition 14 : Assume that G is a compact p-adic Lie group which is p-valued. Then $\Lambda(G)$ possesses a complete, separated and exhaustive filtration $F.\Lambda(G)$ such that $Gr.\Lambda(G)$ is isomorphic as a graded ring to the polynomial ring $\mathbb{F}_p[X_0, \ldots, X_d]$ in $(d+1)$-variable, where $d = \dim G$. In particular, $\Lambda(G)$ is a Noetherian domain.

Proof (Sketch) : By the above lemma, we can choose a p-adic valuation w' on G such that $Gr_{w'}(G)$ is an abelian Lie algebra over $Gr(\mathbb{Z}_p) \simeq \mathbb{F}_p[\pi]$. It can be shown that w' determines a complete filtration on $\Lambda(G)$ (one first extends the filtration to $\mathbb{Z}_p[G]$ and then to the completion), which a priori is indexed by $\mathbb{R}$. On the other hand, it can be proved that the associated graded ring for $\Lambda(G)$ with this filtration is isomorphic as a graded algebra, to the universal enveloping algebra of the $\mathbb{F}_p[\pi]$-algebra $gr_{w'}(G)$. But $gr_{w'}(G)$ is an abelian Lie algebra, which is in fact free of rank $d = \dim(G)$. Hence the universal enveloping algebra is a polynomial ring in d variables over $\mathbb{F}_p[\pi]$. The degrees of the generators, by the above lemma, belong to $e^{-1}\mathbb{Z}$, and hence the filtration on $\Lambda(G)$ can be indexed by $e^{-1}\mathbb{Z}$. By rescaling, it can even be indexed by $\mathbb{Z}$ and the proof of the proposition is complete; noting that Thm. 11 & Prop. 12 now applies.

Remark : i) An alternate approach would be to use the notion of "extra powerful" analytic groups and use the filtration by maximal ideals (cf. Wilson : Profinite groups, DDMS).

We shall now consider some homological properties of the ring $\Lambda(G)$.

Group homology and cohomology: Let G be any group and M a G-module. Recall that the cohomology groups denoted $H^n(G,M)$ $(n \geq 0)$ and $H_n(G,M)$ respectively are defined by:

$$H^n(G,M) = \mathrm{Ext}^n_{\mathbb{Z}_p[G]}(\mathbb{Z}_p, M),$$

$$H_n(G,M) = \mathrm{Tor}^{\mathbb{Z}_p[G]}_n(\mathbb{Z}_p, M),$$

where $\mathbb{Z}_p$ is considered as a trivial module over $\mathbb{Z}_p$.

Now if G is a p-adic analytic group, we demand that the action on a topological module M be continuous. If M is compact, we set

$$H^n(G,M) := \mathrm{Ext}^n_{\Lambda(G)}(\mathbb{Z}_p, M), \text{ and if } M \text{ is discrete},$$

we set $H_n(G,M) = \mathrm{Tor}_n^{\Lambda(G)}(\mathbb{Z}_p, M)$,

where now Ext^* is considered as the higher derived functors of Hom, which denotes continuous homomorphisms. Similarly Tor_* denotes the higher derived functors with respect to $\hat{\otimes}$, the completed tensor product. However, if M is finitely generated, these groups are the usual Ext and Tor groups.

Let $M^\vee$ denote the Pontryagin dual of a compact module M, i.e. $M^\vee = \mathrm{Hom}_{\mathrm{cont},\mathbb{Z}_p}(M, \mathbb{Q}_p/\mathbb{Z}_p)$. Then $M^\vee$ is a

discrete G-module.

Def: The p-cohomological dimension $\mathrm{cd}_p G$ of (a profinite group) G is the least integer n such that $H^{n+i}(G, M)$ for all $i \geq 1$ and p-primary torsion, discrete G-modules M.

Recall that if G is commutative and isomorphic to $\mathbb{Z}_p^d$, then $\Lambda(G) \simeq \mathbb{Z}_p[[T_1, \ldots, T_d]]$ which is a commutative, regular local ring. One of the properties of such rings is that the residue field k has a free resolution of finite length and such that each free module in the resolution is of finite rank. For $\Lambda(G)$, using the Koszul resolution, one sees that the trivial $\mathbb{Z}_p[[T_1, \ldots, T_d]]$ module $\mathbb{Z}_p$ has a finite free resolution of length $d = \dim G$.

We want to investigate similar properties for arbitrary compact p-adic analytic groups G. We shall use the following properties of cd_p (Ref: Serre, Cohomologie Galoisienne):

- If U is a closed subgroup of G, then $\mathrm{cd}_p U \leq \mathrm{cd}_p G$.
- If further U is also open and $\mathrm{cd}_p G$ is finite, then $\mathrm{cd}_p U = \mathrm{cd}_p G$ (Tate).
- (Serre-Lazard): If G has no elements of order p, then $\mathrm{cd}_p(U) = \mathrm{cd}_p(G)$ for any open subgroup U of G.

Lemma 15: Let G be a pro-p group. Then $cd_p(G) < n$ if and only if $H^n(G, \mathbb{F}_p) = 0$.

Pf: If $cd_p(G) < n$, then clearly $H^n(G, \mathbb{F}_p) = 0$. Conversely, suppose that $H^n(G, \mathbb{F}_p) = 0$. We need to show that $H^i(G, A) = 0$ for all p-primary torsion discrete G-modules A and $i \geq n$. If A is a simple G-module such that $pA = 0$, recall that $A \simeq \mathbb{F}_p$ with G acting trivially. By an induction argument on length, we can then show that $H^n(G, A) = 0$ for all p-primary $\Lambda(G)$-modules which are finite. Further, writing $A = \varinjlim A_i$ for any p-primary torsion $\Lambda(G)$-module, with A_i being finitely generated p-primary torsion (hence finite) and noting that $H^n(G, A) = \varinjlim H^n(G, A_i)$, we conclude that $H^n(G, A) = 0$ for all p-primary torsion discrete G-modules A. For $i > n$, one again reduces to the case of a simple G-module by using the long exact sequence in cohomology and an induction argument on i. ∎

We shall show that if G is p-valued, then $cd_p G = n = \dim G$. We shall again need to use filtered-graded techniques for doing this.

Lemma 16: Suppose that a ring R is complete with respect to its filtration topology and that it is (left) noetherian. Suppose M is any finitely generated module with a "good" filtration. Then any projective resolution of $gr.M$ over $gr.R$ can be lifted to a projective resolution of M.

Def: A filtration $F_\cdot M$ of M is a "good filtration" if $\exists\ m_1, \ldots m_s \in$ and integers $k_1, \ldots k_s \in \mathbb{Z}$ such that for all $n \in \mathbb{Z}$,

$$F_n M = \sum_{i=1}^{s} F_{n-k_i} R \cdot m_i .$$

Clearly, if a filtration is good, then the associated graded module $Gr.M$ is finitely generated over $Gr.R$.

Pf: (Sketch) The idea is as follows: Start with $Gr.M$, as it is finitely generated over $Gr.R$, there is a module L_0, which is graded (i.e. L_0 is a $Gr.R$-module)-free of finite rank, with a surjection

$$L_0 \xrightarrow{\varphi_0} Gr.M \to 0 .$$

Once then considers the free R-module generated by lifts of the generators of L_0, denote it by L_0. Now L_0 carries a canonical good filtration on it and a surjective filtered map

$$L_0 \xrightarrow{f_0} M$$

such that on the associated graded level it induces

$$L_0 \xrightarrow{\varphi_0} gr M .$$

Repeating this, one can show that there is a projective resolution of M whose "associated graded" gives a projective resolution of $gr.M$; or rather that any graded projective resolution of $gr.M$ lifts to a projective resolution of M which induces the original one. The hypothesis of completeness ensures that at each level, we can preserve exactness and freeness if the original graded module is free. (See Serre, Algèbre Locale for more details).

Theorem 17: Let G be a compact p-adic analytic group such that G has no elements of order p. Then $cd_p G = d = \dim G$.

pf: By the Serre-Lazard theorem on cohomological dimension, it suffices to show that the theorem is true for p-valued groups G. Therefore we assume that G is p-valued. By Prop. 14, we know that $\Lambda(G)$ is filtered with the property that $gr.\Lambda(G) \simeq \mathbb{F}_p[\pi][T_1, \ldots, T_d] \simeq \mathbb{F}_p[\pi, T_1, \ldots, T_d]$. But this is a domain with the property that $(\pi, T_1, \ldots, T_d)$ is a regular sequence. Then the classical Koszul resolution (cf. Serre, Algèbre Locale) gives a graded resolution

$$0 \to \mathcal{F}_d \longrightarrow \mathcal{F}_{d-1} \longrightarrow \cdots \longrightarrow \mathcal{F}_0 = \mathbb{F}_p[\pi] \longrightarrow 0$$

where each $\mathcal{F}_i$ is a graded free module over $gr.\Lambda(G)$ of finite rank. In particular, as

$$H^n(G, \mathbb{F}_p) = Ext^n_{\Lambda(G)}(\mathbb{Z}_p, \mathbb{F}_p),$$

we see that $H^{d+i}(G, \mathbb{F}_p) = 0$ for $i \geq 1$. Further $H^d(G, \mathbb{F}_p)$ is an $\mathbb{F}_p$-vector space isomorphic to $\Lambda^d(H^1(G, \mathbb{F}_p))$, and $H^1(G, \mathbb{F}_p)$ is of dimension equal to d. Hence $cd_p(G) = d$ by Lemma 15 and the theorem is proved.

Def: Let R be a compact noetherian ring and M a compact f.g. R-module. Then the homological dimension of M, $hd_R M$ is the least integer n for which there exists a projective resolution over R of length n.

The global dimension of R, $gl.dim\ R = \sup_M \{hd_R M\}$, where the supremum is taken over all finitely generated compact modules.

Theorem 18: Let G be a compact p-adic analytic group. Then $\text{gl.dim } \Lambda(G) = 1 + cd_p G = 1+d$, where $d = \dim G$, whenever G is p-torsion free.

pf: (Sketch) The proof combines many of the properties listed or used above of the compact p-adic analytic groups, along with techniques from homological algebra. For a more general result, see [Brumer, J. Alg. 4, 442-470, (1966)]. We shall list and provide some details of the main steps in the proof:

Step 1: Show that $\text{gl.dim}(\Lambda(G)) < n \iff \text{Ext}^n_{\Lambda(G)}(C, D) = 0$ for all simple $\Lambda(G)$-modules C and D.

The necessity is clear. To show the converse, assume that $\text{Ext}^n_{\Lambda(G)}(C, D) = 0$ for all simple $\Lambda(G)$-modules C and D. If M is any compact $\Lambda(G)$-module, we write $M = \varprojlim M_i$, where each M_i is a finite $\Lambda(G)$-module, and use induction along with the hypothesis and the fact that $\text{Ext}^n_{\Lambda(G)}(\varprojlim M_i, D) = \varinjlim \text{Ext}^n_{\Lambda(G)}(M_i, D)$.

Step 2: Replacing G by its p-Sylow subgroup G_p.

To see this reduction, we note that G_p is pro-p and $|G/G_p|$ is relatively prime to p. In this situation, one sees that the restriction map

$$\text{Ext}^n_{\Lambda(G)}(A, C) \longrightarrow \text{Ext}^n_{\Lambda(G_p)}(A, C)$$

is injective and hence one is reduced to considering G_p.

Step 3: Show that if G is pro-p and has no elements of order p, then $\text{gl.dim } \Lambda(G) = 1 + cd_p G = 1 + d$.

The last equality follows from Theorem 17. Thus we just have to prove that $\text{gl.dim } \Lambda(G) = 1 + cd_p G$.

In the proof of Theorem 17, we had actually shown that $\mathrm{hd}_{\Lambda(G)} \mathbb{Z}_p = d = \dim G$. By our reduction in step 2, we know that $\Lambda(G)$ is a local ring with residue field $\mathbb{F}_p$. By step 1, we need to show that $\mathcal{E}xt^n_{\Lambda(G)}(\mathbb{F}_p, \mathbb{F}_p) = 0$ for all $n > d+1$ and $\mathcal{E}xt^{d+1}_{\Lambda(G)}(\mathbb{F}_p, \mathbb{F}_p)$ is non-zero, as $\mathbb{F}_p$ is the only simple $\Lambda(G)$-module. Consider the long exact sequence on Ext-groups induced by the exact sequence

$$0 \to \mathbb{Z}_p \xrightarrow{p} \mathbb{Z}_p \to \mathbb{F}_p \to 0$$

of $\Lambda(G)$-modules. We get (applying $\mathrm{Hom}_{\Lambda(G)}(-, \mathbb{F}_p)$)

$$0 \to \mathrm{Hom}_{\Lambda(G)}(\mathbb{F}_p, \mathbb{F}_p) \to \mathrm{Hom}_{\Lambda(G)}(\mathbb{Z}_p, \mathbb{F}_p) \xrightarrow{p} \mathrm{Hom}_{\Lambda(G)}(\mathbb{Z}_p, \mathbb{F}_p) \to \mathcal{E}xt^1_{\Lambda(G)}(\mathbb{F}_p, \mathbb{F}_p) \to$$

$$\xrightarrow{p} \mathcal{E}xt^d_{\Lambda(G)}(\mathbb{Z}_p, \mathbb{F}_p) \to \mathcal{E}xt^{d+1}_{\Lambda(G)}(\mathbb{F}_p, \mathbb{F}_p) \to \mathcal{E}xt^{d+1}_{\Lambda(G)}(\mathbb{Z}_p, \mathbb{F}_p) \xrightarrow{p}$$

As $\mathcal{E}xt^d_{\Lambda(G)}(\mathbb{Z}_p, \mathbb{F}_p) = H^d(G, \mathbb{F}_p)$ is non-zero and multiplication by p in the long exact sequence above is the zero homomorphism, we see that $\mathcal{E}xt^{d+1}_{\Lambda(G)}(\mathbb{F}_p, \mathbb{F}_p)$ is non-zero and $\mathcal{E}xt^{d+i}_{\Lambda(G)}(\mathbb{F}_p, \mathbb{F}_p) = 0 \ \forall\ i > 1$.

This completes the proof of the theorem. //

Remark: i) More generally, for any local, compact noetherian ring Ω, (i.e. $\Omega = \varprojlim \Omega_i$, each Ω_i finite), we have

$$\mathrm{gl.dim}\, \Omega(G) = \mathrm{gl.dim}\, \Omega + \mathrm{cd}_p G. \quad //$$

ii) The content of the above theorem is that as in the commutative case, for the purposes of global dimension, one can work with the residue field $\mathbb{F}_p$ as the test case.

We shall quote the following theorem of Walker [Proc. LMS, 24, 27-45, (1972)] to deduce a slightly more general result:

Theorem: Let R be a Noetherian ring satisfying (1) R is semiprime (2) All finitely generated projective R-modules are stably free (3) R has finite global dimension.

Then R has no zero divisors.

Corollary 19: Let G be a pro-p analytic p-adic group with no elements of order p. Then $\Lambda(G)$ is a domain.

Pf: By Lemma 9, $\Lambda(G)$ is semiprime. Further as G is pro-p, by Lemma 5, it is also local. Hence any finitely generated projective R-module is even free. By Theorem 18, as G has no elements of order p, gl. dim $\Lambda(G)$ is finite. Hence by the theorem of Walker quoted above, $\Lambda(G)$ is a domain. //

We shall end by listing the properties we have proved:

- G a cpct p-adic analytic Lie group. Then:

→ $\Lambda(G)$ is semi-local and semi-prime.

→ $\Lambda(G)$ is local if G is pro-p

→ gl. dim $\Lambda(G)$ and $cd_p(G)$ are finite if G has no elements of order p

→ $\Lambda(G)$ is a domain if G is pro-p and has no elements of order p. //

Measures: The motivation behind this section is that it is the 'analytic' face of Iwasawa algebras. Having so far studied many algebraic properties of Iwasawa algebras, we shall present the view point of looking at completed group algebras as $\mathbb{Z}_p$-valued distributions.

For simplicity, we shall only consider pro-p groups G. Let A be an abelian group (usually $\mathbb{Z}_p$; $\mathcal{O}$ = ring of integers of a local field; or $\mathbb{C}_p$ = Completion of algebraic closure of $\mathbb{Q}_p$).

We write $G = \varprojlim_{i \in I} G_i$, where $G_i = G/H_i$ and $\{H_i\}_{i \in I}$ are open normal subgroups of G. We have the canonical projections

$$\pi_{ij} : G/H_i \longrightarrow G/H_j \quad \text{for } i \geq j$$

and also the projections

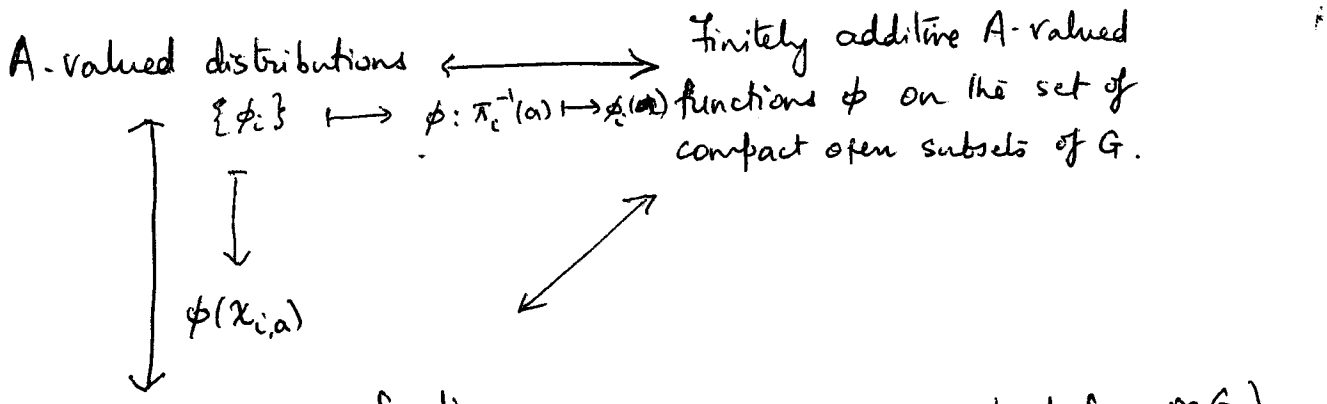
$$\pi_i : G \longrightarrow G_i .$$

Def: Suppose that for each i, we have a function ϕ_i on G_i, with values in an abelian group A, with the property that if $i \geq j$,

$$\phi_j(x) = \sum_{\pi_{ij}(y) = x} \phi_i(y).$$

Then the collections of maps $\{\phi_i\}$ is called an A-valued distribution.

In fact, there are other equivalent ways to define distributions viz.:



($\chi_{i,a}$ = char. fn. on the compact open subset $\pi_i^{-1}(a)$).

Def: The distribution $\{\phi_i\}$ is a bounded measure if $|\phi_i(a)| \leq C$, for some fixed $C \in \mathbb{R}$, and for all $i \in I$, $a \in G_i$. Equivalently, if ϕ is a linear functional on $\mathrm{Step}(G, A)$, then $|\phi(f)| \leq C \|f\|_{\sup}$, $\forall$ $f \in \mathrm{Step}(G, A)$.

- $\mathrm{Step}(G, A)$ is dense in the Banach space, $C(G, A)$, of all continuous functions $G \longrightarrow A$, w.r.t. the sup norm, $\| \ \|_{\sup}$. (Any continuous function $f \in C(G, A)$ can be uniformly approximated by locally constant functions).

Def: If ϕ is a bounded linear functional, $\phi : \mathrm{Step}(G, A) \to A$, then ϕ extends uniquely to a well-defined linear functional

$$\phi : C(G, A) \longrightarrow A$$
$$f \longmapsto \int_G f \, d\phi := \lim_i \phi(f_i), \text{ where } f_i \in \mathrm{Step}(G, A) \text{ and } f_i \to f \text{ w.r.t. } \| \ \|_{\sup}.$$

- When $A = \mathbb{Z}_p$, there is a 1–1 correspondence

$$\mathbb{Z}_p\text{-valued distributions} \longleftrightarrow \mathbb{Z}_p[[G]].$$
$$\{\phi_i\} \longleftrightarrow (\ldots, x_i, \ldots) \ ; \ x_i \in \mathbb{Z}_p[G/G_i], \quad x_i = \sum_{g \in G/G_i} \phi_i(g)\, g$$

• If ψ is a finite character of G, i.e. a character which factors through G/H for some H open normal in G, then the action of ψ can be extended to all of $\mathbb{Z}_p[[G]]$. Treating ψ as an element in $C(G, \mathbb{C}_p)$, we can integrate using the above definition and we have

$$\int_G \psi \, d\phi = \psi(\alpha),$$

where $\alpha \in \mathbb{Z}_p[[G]]$ corresponds to ϕ under the above equivalence.

Our final result on the algebraic theory will be a structure theorem for finitely generated torsion modules over $\Lambda(G)$ when $G \simeq \mathbb{Z}_p^d$. We shall state this result and prove it in the more general framework of torsion modules which are finitely generated over integrally closed domains (of course noetherian!). We shall need some results from commutative algebra which we recall below. From now on R is commutative

• Let R be a commutative noetherian ring and M a finitely generated R-module. Recall that

$$\begin{aligned} \operatorname{Supp} M &= \{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{p} \supseteq \operatorname{ann} M\} \\ &= \{\mathfrak{p} \in \operatorname{Spec} R \mid M_{\mathfrak{p}} \neq 0\}. \end{aligned}$$

Recall that a prime ideal $\mathfrak{p}$ is <u>associated</u> to M, denoted $\mathfrak{p} \in \operatorname{Ass} M \iff \mathfrak{p} = \operatorname{ann}(m)$ for some $m \in M$.

$\operatorname{Ass} M \subseteq \operatorname{Supp} M$ and both have the same set of minimal elements.

- R is an integrally closed noetherian domain iff conditions R_1 and S_2 of Serre are satisfied.
  - Condition R_1 : $\forall\ \mathfrak{p} \in \operatorname{Spec} R$ of ht ≤ 1, $R_{\mathfrak{p}}$ is a discrete valuation ring.
  - Condition S_2 : $\forall\ \mathfrak{p} \in \operatorname{Spec} R$ of ht ≥ 2, depth $R_{\mathfrak{p}} \geq 2$.

- Recall depth of a local ring (S, m_S) is the maximal length of an R-sequence in m_S i.e. the maximal number of elements $(x_1, \ldots, x_s)$ such that $x_i \in m_S$ and x_{i+1} is a non-zero divisor in $S/(x_1, \ldots x_i)$ $\forall\ 1 \leq i \leq s-1$.

- M a finitely generated R-module. Then

$$\operatorname{grade}(M) = \inf\{n \in \mathbb{N} \text{ s.t. } \operatorname{Ext}^n_R(M, R) \neq 0\}$$
$$= \text{maximal length of an } R\text{-regular sequence in } \operatorname{ann}(M).$$

Def : R a commutative noetherian ring. A finitely generated module M is pseudonull if $M_{\mathfrak{p}} = 0$ for all prime ideals $\mathfrak{p} \in \operatorname{Spec} R$ of height ≤ 1. Equivalently, $\operatorname{Supp} M$ does not contain any prime ideals of height ≤ 1.

Lemma 20 : Let R be an integrally closed noetherian domain and M a finitely generated R-module. Then M is pseudonull $\iff \operatorname{Ext}^i_R(M, R) = 0$ for $i = 0, 1$.

Pf : Necessity : We are given that $M_{\mathfrak{p}} = 0$ $\forall\ \mathfrak{p} \in \operatorname{Spec} R$ of ht ≤ 1. As $(0) \in \operatorname{Spec} R$, this implies that M is torsion and hence $\operatorname{ann}(M) \neq 0$ and $\operatorname{Ext}^0_R(M, R) = \operatorname{Hom}_R(M, R) = 0$.

As $\operatorname{ann}(M)$ is a non-zero ideal, it contains non-zero divisors of R as R is domain. Let $x \in \operatorname{ann}(M)$ be a non-zero divisor. Consider the ring $R/(x)$. As R is normal, it can be checked [cf. Serre, Algèbre Locale, III-IV, Prop. 9 (b)] that $\operatorname{Ass}(R/(x))$ consists of prime ideals of height 1; say $\mathfrak{p}_1, \ldots \mathfrak{p}_k \in \operatorname{Spec} R$. As M is pseudonull, none of these $\mathfrak{p}_i \in \operatorname{Ass}(M)$ and hence $(\operatorname{ann} M)$ is not contained in any of these $\mathfrak{p}_i$'s. But the zero divisors of $R/(x)$ are precisely the union of $\mathfrak{p}_i$'s and we have

$$\operatorname{ann}(M) \nsubseteq \bigcup_{i=1}^{k} \mathfrak{p}_i = \text{set of zero divisors of } R/(x).$$

Hence there exists $y \in \operatorname{ann}(M)$ such that y is a non zero divisor of $R/(x)$ which implies that $\operatorname{grade}(M) \geq 2$.

Sufficiency: As before $\operatorname{Hom}_R(M,R) = 0$ implies that M is R-torsion and hence $0 \notin \operatorname{Supp}(M)$. We prove that M contains no prime ideal of height 1 in its support. Clearly, we may localise at a height 1 prime ideal and assume that R is a discrete valuation ring and that M is a finitely generated torsion R-module such that $\operatorname{Ext}^1_R(M,R) = 0$. Let $\mathfrak{m}$ be the maximal ideal of R. It is clear that $\mathfrak{m} \in \operatorname{Ass}(M) = \operatorname{Supp}(M)$ as $M \neq 0$ and $0 \notin \operatorname{Supp}(M)$; in particular M is of finite length and by an induction on length, we may assume that $M = R/\mathfrak{m} = k$. We thus have $\operatorname{Ext}^1_R(k,R) = 0$. But this is a contradiction as this implies that $\operatorname{grade}(R/\mathfrak{m}) > 1$. Indeed, by the alternative definition of grade via R-sequences, it is clear that $\operatorname{grade}(R/\mathfrak{m}) = 1$. Hence $M = 0$, which means that our original module M localised

at any height 1 prime ideal is zero. Hence M is pseudonull.

Def: A homomorphism $f : M \to N$ of R-modules is said to be a pseudoisomorphism, denoted $M \sim N$ if $\ker f$ and $\operatorname{coker} f$ are pseudonull.

We now prove the structure theorem.

Theorem 21: Let R be a noetherian integrally closed domain, and M a f.g. torsion R-module. Then M is pseudo isomorphic to $\bigoplus_{i \in I} R/\mathfrak{p}_i^{n_i}$ where $\{\mathfrak{p}_i\}_{i \in I}$ is a finite family of height 1 prime ideals. The integers n_i and the set $\{\mathfrak{p}_i\}$ are uniquely determined up to renumbering.

Pf: As M is torsion, the prime ideal $0 \notin \operatorname{Supp}(M)$.

Let $P(R)$ = height 1 prime ideals of R = the set of ht. 1 prime ideals in $\operatorname{Spec} R$.

Set $P_M(R) := \{\mathfrak{p} \in P(R) \mid \mathfrak{p} \in \operatorname{Supp} M\}$

$= \{\mathfrak{p} \in P(R) \mid \mathfrak{p} \in \operatorname{Ass} M\}$,

as $\operatorname{Ass}(M)$ and $\operatorname{Supp}(M)$ have the same set of minimal primes. Clearly $P_M(R)$ is a finite set as it is contained in $\operatorname{Ass}(M)$.

We define

$$S = R \setminus \bigcup_{\mathfrak{p} \in P_M(R)} \mathfrak{p}.$$

The set S is a multiplicative subset of R. Consider the ring $S^{-1}R$; then the only prime ideals in $S^{-1}R$ are $S^{-1}\{0\} = (0)$ and $S^{-1}\mathfrak{p}$, for $\mathfrak{p} \in P_M(R)$. Therefore $S^{-1}R$ is an integrally

closed noetherian domain of dimension 1 with finitely many prime ideals. In other words, $S^{-1}R$ is a semi-local Dedekind domain, hence principal (cf. Bourbaki, Comm. Alg., chap. VII, § 2.2, Proposition 1).

Now, the module $S^{-1}M$ is a finitely generated torsion module over $S^{-1}R$. By the structure theorem for finitely generated modules over PID's, we see that

$$S^{-1}M \simeq \bigoplus_{i \in I} S^{-1}R/S^{-1}\mathfrak{p}_i^{n_i},$$

where I is a finite set and the ideals $\mathfrak{p}_i$ and integers n_i are determined up to renumbering. We can lift this isomorphism to an R-homomorphism

$$f : M \longrightarrow \bigoplus_{i \in I} R/\mathfrak{p}_i^{n_i}$$

with the property that if K and C denote the kernel and cokernel of f, then $S^{-1}K = S^{-1}C = 0$. We claim that this implies the pseudonullity of K and C.

Clearly, both K and C are torsion, and hence $0 \notin \operatorname{Supp} K$ and $0 \notin \operatorname{Supp} C$. We should show that there are no prime ideals of height 1 either in their supports.

If we consider the kernel K, then as $\operatorname{Supp}(K) \subseteq \operatorname{Supp}(M)$, any prime ideal of height 1 in $\operatorname{Supp}(K)$ is necessarily in $P_M(R)$ and hence it suffices to show that $P_M(R) \cap \operatorname{Supp}(K)$ is empty. If $\mathfrak{p} \in P_M(R)$ and

$S_{\mathfrak{p}} := R \setminus \mathfrak{p}$, then $S \subseteq S_{\mathfrak{p}}$. Hence $S^{-1}K = 0$ implies that $S_{\mathfrak{p}}^{-1} K = K_{\mathfrak{p}} = 0$ and therefore $\mathfrak{p} \notin \mathrm{Supp}(K)$.

Hence K is pseudo-null.

For the cokernel C, we conclude by a similar argument, noting that the prime ideals of height 1 in $\mathrm{Supp}\left(\bigoplus_{i \in I} A/\mathfrak{p}_i^{n_i}\right)$ coincides with the set $P_M(R)$.

Hence the theorem is proved.

We conclude by mentioning that a similar but weaker structure theorem holds for non commutative Iwasawa algebras $\Lambda(G)$, whenever G is a p-valued, p-adic analytic group. Indeed it is shown in [CSS] that if we define a module M over $\Lambda(G)$ to be pseudonull whenever $\mathrm{Ext}^i_{\Lambda(G)}(M, \Lambda(G)) = 0$ for $i = 0, 1$, then we have the following theorem:

Theorem: Let G be a p-valued, p-adic analytic group and M a finitely generated torsion $\Lambda(G)$-module. Then there exists a finite set of reflexive (left) ideals J_i, $1 \le i \le k$ such that there is a homomorphism

$$f : \bigoplus_{i \in I} \frac{\Lambda(G)}{J_i} \longrightarrow M$$

with pseudonull kernel and cokernel.

Note: An ideal J is reflexive if the natural homomorphism $J \to \mathrm{Hom}_{\Lambda(G)}(\mathrm{Hom}_{\Lambda(G)}(J, \Lambda(G)), \Lambda(G))$ is an isomorphism.

REFERENCES

BOURBAKI : Commutative Algebra, chapters 1–7, Springer.

CSS : J. Coates, P. Schneider, R. Sujatha ; Modules over Iwasawa algebras, Journal of the Inst. of Math. Jussieu (2003) 2 (1), 73 - 108.

DDMS : J. D. Dixon, M. P. F. Du Sautoy, A. Mann, D. Segal ; Analytic pro-p groups, Cambridge University Press (1999).

L : M. Lazard ; Groupes analytiques p-adiques, Publ. Math. IHES 26 (1965), 389 - 603.

Mc-R : J. C. Mc Connell, J. C. Robson, Non Commutative Noetherian Rings, Graduate Studies in Mathematics, Vol. 30, AMS, (2001).

N : A. Neumann : Completed group algebras without zero divisors, Arch. Math. 51, (1988), 496 - 499.

S : J.-P. Serre : Sur la dimension cohomologique des groupes profinis, Topology 3 (1965), 413–420.

J.-P. Serre : Cohomologie Galoisienne, SLN Vol. 5, (1973).

J.-P. Serre : Algèbre Locale ; Mutiplicités, SLN Vol. 11 (1975).

W : R. Walker ; Local rings and normalizing sets of elements, Proc. LMS. 24, (1972), 27 - 45.