Extensions of almost faithful prime ideals in virtually nilpotent mod-$p$ Iwasawa algebras

William Woods

April 26, 2017

Abstract

Let $G$ be a nilpotent-by-finite compact $p$-adic analytic group for some $p > 2$, and $H = \text{FN}_p(G)$ its finite-by-(nilpotent $p$-valuable) radical. Fix a finite field $k$ of characteristic $p$, and write $kG$ for the completed group ring of $G$ over $k$. We show that almost faithful $G$-stable prime ideals $P$ of $kH$ extend to prime ideals $PKG$ of $kG$.

2010 Mathematics Subject Classification: 16S34, 16D25, 16S35, 16W60.
## Contents

1. **p-valuations and crossed products**
   1.1 Preliminaries on p-valuations .................. 6
   1.2 Ordered bases ................................ 8
   1.3 Separating a free abelian quotient .......... 10
   1.4 Invariance under the action of a crossed product .. 12

2. **A graded ring**
   2.1 Generalities on ring filtrations ............... 16
   2.2 Constructing a suitable valuation .............. 18
   2.3 Automorphisms trivial on a free abelian quotient .. 24

3. **Extending prime ideals from \( \text{FN}_p(G) \)**
   3.1 X-inner automorphisms ......................... 27
   3.2 Properties of \( \text{FN}_p(G) \) ................... 28
   3.3 The extension theorem .......................... 30
Introduction

Let $G$ be a nilpotent-by-finite compact $p$-adic analytic group and $k$ a finite field of characteristic $p$.

Recall the characteristic open subgroup $H = \text{FN}_p(G)$, the finite-by-(nilpotent $p$-valuable) radical of $G$, defined in [10, Theorem C]. This plays an important role in the structure of the group $G$: for instance, see the structure theorem [10, Theorem D].

In this paper, we demonstrate a connection between certain prime ideals of $kH$ and those of $kG$. The main result of this paper is:

**Theorem A.** Fix some prime $p > 2$. Let $G$ be a nilpotent-by-finite compact $p$-adic analytic group, $H = \text{FN}_p(G)$, and $k$ a finite field of characteristic $p$. Let $P$ be an almost faithful, $G$-stable prime ideal of $kH$. Then $P kG$ is a prime ideal of $kG$.

The proof (given in Propositions 3.7 and 3.8) comprises several technical elements, which we outline below.

First, let $G$ be a nilpotent-by-finite compact $p$-adic analytic group with finite radical $\Delta^+ = 1$ [10, Definition 1.2], and let $H = \text{FN}_p(G)$. Note that $H$ is $p$-valuable [6, III, 2.1.2], and that $G$ acts on the set of $p$-valuations of $H$ as follows: if $\alpha$ is a $p$-valuation on $H$ and $g \in G$, then we may define a new $p$-valuation $g \cdot \alpha$ on $H$ by

$$g \cdot \alpha(x) = \alpha(g^{-1}xg).$$

(In fact, we do this in a slightly more general case, but the details are identical. See Lemma 1.17 for the setup.)

Recall the definition of an isolated orbital (closed) subgroup $L$ of $H$ from [10, Definition 1.4], and that normal subgroups are automatically orbital. We show in Definition 1.2 that, if $\omega$ is a $p$-valuation on $H$ and $L$ is a closed isolated normal subgroup of $H$, then $\omega$ induces a quotient $p$-valuation $\Omega$ on $H/L$. We also define the $(t, p)$-filtration (actually a $p$-valuation) on a free abelian pro-$p$ group $A$ of finite rank in Definition 1.2: this is a particularly “uniform” $p$-valuation on $A$, analogous to the $p$-adic valuation $v_p$ on $\mathbb{Z}_p$.

It is now easy to show the following.

**Theorem B.** With the above notation: let $L$ be a proper closed isolated normal subgroup of $H$ containing the commutator subgroup $[H, H]$. Then there exists a $p$-valuation $\omega$ on $H$ with the following properties:

(i) $\omega$ is $G$-invariant,

(ii) there exists a real number $t > (p - 1)^{-1}$ such that $\omega|_L > t$, and the quotient $p$-valuation induced by $\omega$ on $G/L$ is the $(t, p)$-filtration.
Continue to take $G$ to be a nilpotent-by-finite compact $p$-adic analytic group with $\Delta^+ = 1$, and $H = FN_p(G)$. Let $p$ be a prime, $k$ a field of characteristic $p$, and $P$ a faithful prime ideal of $kH$. It is shown in [2, Theorem 8.4] that $P = pkH$ for some prime ideal $p$ of $kZ$, where $Z$ is the centre of $H$; and, furthermore, in [2, proof of Theorem 8.6], that there exist an integer $e$ and a ring filtration $f$ on $kH/P$ such that

$$gr_f(kH/P) \cong (gr_v(kZ/p))[Y_1, \ldots, Y_e]$$

where $v = f|_{kZ/p}$ is a valuation, and $gr_f(kZ/p)$ is a commutative domain. The valuation $f$ is partly constructed using the $p$-valuation $\omega$ on the group $H$.

Our next theorem is an extension of this result. Write $f_1$ for the ring filtration constructed above. Suppose now that $P$ is $G$-stable so that we may consider the ring $kG/PkG$, and fix a crossed product decomposition $(kH/P) \ast F$ of this ring, where $F = G/H$.

Write $Q'$ for the classical ring of quotients of $kZ/p$. The filtration $f_1$ restricts to a valuation on $kZ/p$, which extends naturally to a valuation on $Q'$, which we will call $v_1$. $F$ acts on the set of valuations of $Q'$, and $v_1$ has some orbit $\{v_1, \ldots, v_s\}$.

Write $Q$ for a certain partial ring of quotients of $kH/P$ containing $Q'$. We may naturally form $Q \ast F$ as an overring of $(kH/P) \ast F$.

**Theorem C.** In the above notation: there exists a filtration $\hat{f}$ on $Q \ast F$ such that

1. $gr_{\hat{f}}(Q \ast F) \cong gr_f(Q) \ast F$, where the right-hand side is some crossed product,
2. $gr_{\hat{f}}(Q) \cong \bigoplus_{i=1}^{s} gr_{f_i}(Q)$,
3. $gr_{f_i}(Q) \cong (gr_v(Q'))[Y_1, \ldots, Y_e]$ for all $1 \leq i \leq s$,

where $s$ and $e$ are determined as in (†), and the action of $F$ in the crossed product of (i) permutes the $s$ summands in the decomposition of (ii) transitively by conjugation.

We combine Theorems B and C as follows.

Theorem C, of course, only invokes (†) in the case when $Q \neq Q'$, so we suppose that we are in this case, which occurs precisely when $H$ is non-abelian. Take $L$ to be the smallest closed isolated normal subgroup of $H$ containing both the isolated derived subgroup $H'$ [10, Theorem B] and the centre $Z$ of $H$. Now $L$ is a proper subgroup by Lemma 3.5, and we will choose $\omega$ for $L$ as in Theorem B.

We may arrange it in (†) and Theorem C so that, for some $l \leq e$, the elements $Y_1, \ldots, Y_l$ correspond to a $Z_p$-module basis $x_1, \ldots, x_l$ for $H/L$; and here the value of the filtration $\hat{f}$ can be understood in terms of the $p$-valuation $\omega$. We show that:
Theorem D. Take an automorphism $\sigma$ of $H$. Suppose that the induced automorphism on $\text{gr}_f(Q \ast F)$ fixes each of the valuations $v_1, \ldots, v_s$ and fixes each of the elements $Y_1, \ldots, Y_l$. Then the induced automorphism on $H/L$ (which can be seen as a matrix $M_\sigma \in \text{GL}_l(\mathbb{Z}_p)$) lies in the first congruence subgroup of $\text{GL}_l(\mathbb{Z}_p)$, i.e. it takes the form $M_\sigma \in 1 + pX$ for some $X \in M_l(\mathbb{Z}_p)$. In particular, when $p > 2$, $\sigma$ has finite order if and only if it is the identity automorphism.

A special case of Theorem A, in which $\Delta^+ = 1$, is now deduced from Theorem D via a long but elementary argument about $X$-inner automorphisms: see Definition 3.1 and Proposition 3.7 for details.

The case when $\Delta^+ \neq 1$ now follows as a consequence of the “untwisting” results of [11, Theorems B and C], which allow us to understand the prime ideals of $kH$, along with the conjugation action of $G$, in terms of the corresponding information for $k'[[H/\Delta^+]]$ (for various finite field extensions $k'/k$). Now, as $\Delta^+(G/\Delta^+) = 1$ and $H/\Delta^+ = \text{FN}_p(G/\Delta^+)$, we are back in the previous case. See Proposition 3.8 for details.
1  $p$-valuations and crossed products

1.1 Preliminaries on $p$-valuations

**Definition 1.1.** Recall from [6, III, 2.1.2] that a $p$-valuation on a group $G$ is a function $\omega : G \to \mathbb{R} \cup \{\infty\}$ satisfying:

- $\omega(xy^{-1}) \geq \min\{\omega(x), \omega(y)\}$ for all $x, y \in G$
- $\omega([x, y]) \geq \omega(x) + \omega(y)$ for all $x, y \in G$
- $\omega(x) = \infty$ if and only if $x = 1$
- $\omega(x) > \frac{1}{p^{1-p}}$ for all $x \in G$
- $\omega(x^p) = \omega(x) + 1$ for all $x \in G$.

Throughout this paper we will often be considering several $p$-valuations admitted by a group $G$, so to clarify we may refer to $G$ together with a $p$-valuation $\omega$ as the $p$-valued group $(G, \omega)$ (though when the $p$-valuation in question is clear from context, we will simply write $G$).

Given a $p$-valuation $\omega$ on a group $G$, we may write

$$ G_{\omega, \lambda} := G_{\lambda} := \omega^{-1}([\lambda, \infty]), $$

$$ G_{\omega, \lambda^+} := G_{\lambda^+} := \omega^{-1}((\lambda, \infty]) $$

and define the graded group

$$ \text{gr}_\omega G := \bigoplus_{\lambda \in \mathbb{R}} G_{\lambda}/G_{\lambda^+}. $$

Then each element $1 \neq x \in G$ has a principal symbol

$$ \text{gr}_\omega(x) := xG_{\mu^+} \subseteq G_{\mu}/G_{\mu^+} \leq \text{gr}_\omega G, $$

where $\mu$ is defined such that $\mu = \omega(x)$.

**Remark.** Let $(G, \omega)$ be a $p$-valued group, and $N$ an arbitrary subgroup of $G$. Then $(N, \omega|_N)$ is $p$-valued. Moreover, if $G$ has finite rank [6], then so does $N$; and if $G$ is complete with respect to $\omega$ and $N$ is a closed subgroup of $G$, then $N$ is complete with respect to $\omega|_N$.

**Definition 1.2.** Given an arbitrary complete $p$-valued group $(G, \omega)$ of finite rank, and a closed isolated normal subgroup $K$ (i.e. a closed normal subgroup $K$ such that $G/K$ is torsion-free), we may define the quotient $p$-valuation $\Omega$ induced by $\omega$ on $G/K$ as follows:

$$ \Omega(gK) = \sup_{k \in K} \{\omega(gk)\}. $$
This is defined by Lazard, but the definition is spread across several results, so we collate them here for convenience. The definition in the case of filtered modules is [6 I, 2.1.7], and is modified to the case of filtered groups in [6] the remark after II, 1.1.4.1]. The specialisation from filtered groups to $p$-saturable groups is done in [6 III, 3.3.2.4], where it is proved that $\Omega$ is indeed still a $p$-valuation on $G/K$; and the general case is stated in [6 III, 3.1.7.6], and eventually proved in [6 IV, 3.4.2].

As a partial inverse to the above process of passing to a quotient $p$-valuation, we prove the following general result about “lifting” $p$-valuations from torsion-free quotients.

**Theorem 1.3.** Let $G$ be a complete $p$-valued group of finite rank, and $N$ a closed isolated orbital (hence normal) subgroup of $G$. Suppose we are given two functions

$$\alpha, \beta : G \to \mathbb{R} \cup \{\infty\},$$

such that $\alpha$ is a $p$-valuation on $G$, and $\beta$ factors through a $p$-valuation on $G/N$, i.e.

$$\overline{\beta} : G/N \to \mathbb{R} \cup \{\infty\}.$$

Then $\omega = \inf\{\alpha, \beta\}$ is a $p$-valuation on $G$.

**Proof.** $\alpha$ and $\beta$ are both filtrations on $G$ (in the sense of [6 II, 1.1.1]), and so by [6 II, 1.2.10], $\omega$ is also a filtration. Following [6 III, 2.1.2], for $\omega$ to be a $p$-valuation, we need to check the following three conditions:

(i) $\omega(x) < \infty$ for all $x \in G$, $x \neq 1$.

This follows from the fact that $\alpha$ is a $p$-valuation, and hence $\alpha(x) < \infty$ for all $x \in G$, $x \neq 1$.

(ii) $\omega(x) > (p-1)^{-1}$ for all $x \in G$.

This follows from the fact that $\alpha(x) > (p-1)^{-1}$ and $\beta(x) > (p-1)^{-1}$ for all $x \in G$ by definition.

(iii) $\omega(x^p) = \omega(x) + 1$ for all $x \in G$.

Take any $x \in G$. As $\alpha$ is a $p$-valuation, we have by definition that $\alpha(x^p) = \alpha(x) + 1$.

If $x \in N$, this alone is enough to establish the condition, as $\omega|_N = \alpha|_N$ (since $\beta(x) = \infty$).

Suppose instead that $x \in G \setminus N$. Then, as $N$ is assumed isolated orbital in $G$, we also have $x^p \in G \setminus N$, so by definition of $\beta$ we have

$$\beta(x^p) = \overline{\beta}((xN)^p) = \overline{\beta}(xN) + 1 = \beta(x) + 1,$$

with the middle equality coming from the fact that $\overline{\beta}$ is a $p$-valuation. Now it is clear that $\omega(x^p) = \omega(x) + 1$ by definition of $\omega$. \qed
Finally, the following function will be crucial. (It is in fact a $p$-valuation, but we delay the proof of this fact until Lemma 1.6.)

**Definition 1.4.** Let $A$ be a free abelian pro-$p$ group of rank $d > 0$ (here written multiplicatively). Choose a real number $t > (p-1)^{-1}$. Then the $(t, p)$-filtration on $A$ is the function $\omega : A \to \mathbb{R} \cup \{\infty\}$ defined by

$$\omega(x) = t + n,$$

where $n$ is the non-negative integer such that $x \in A^{p^n} \setminus A^{p^{n-1}}$. (By convention, $\omega(1) = \infty$.)

1.2 Ordered bases

**Definition 1.5.** Recall from [2, 4.2] that an **ordered basis** for a $p$-valued group $(G, \omega)$ is a set \{g_1, \ldots, g_e\} of elements of $G$ such that every element $x \in G$ can be uniquely written as the (ordered) product

$$x = \prod_{1 \leq i \leq e} g_i^{\lambda_i}$$

for some $\lambda_i \in \mathbb{Z}_p$, and

$$\omega(x) = \inf_{1 \leq i \leq e} \{\omega(g_i) + v_p(\lambda_i)\},$$

where $v_p$ is the usual $p$-adic valuation on $\mathbb{Z}_p$. (Note that an ordered basis for $(G, \omega)$ need not be an ordered basis for $(G, \omega')$ for another $p$-valuation $\omega'$.)

As in [2], we will often write

$$g^\lambda := \prod_{1 \leq i \leq e} g_i^{\lambda_i}$$

as shorthand, where $\lambda \in \mathbb{Z}_p^e$.

We now show that the function given in Definition 1.4 is indeed a $p$-valuation, and demonstrate some of its properties.

**Lemma 1.6.** Let $A$ and $t$ be as in Definition 1.4

(i) The $(t, p)$-filtration $\omega$ is a $p$-valuation on $A$.

(ii) Suppose we are given a $\mathbb{Z}_p$-module basis $B = \{a_1, \ldots, a_d\}$ for $A$, and a $p$-valuation $\alpha$ on $A$ satisfying $\alpha(a_1) = \cdots = \alpha(a_d) = t$. Then $\alpha$ is the $(t, p)$-filtration on $A$, and $B$ is an ordered basis for $(A, \alpha)$.

(iii) The $(t, p)$-filtration $\omega$ is completely invariant under automorphisms of $A$, i.e. the subgroups $A_{\omega, \lambda}$ and $A_{\omega, \lambda^p}$ are characteristic in $A$.

**Proof.**
(i) This is a trivial check from the definition [6, III, 2.1.2].

(ii) By [6, III, 2.2.4], we see that
\[ \alpha(a_1^{\lambda_1} \cdots a_d^{\lambda_d}) = t + \inf_{1 \leq i \leq d} \{ v_p(\lambda_i) \}, \]
which is precisely the \((t, p)-filtration\).

(iii) The subgroups \(A^n_p\) are clearly characteristic in \(A\).

Remark. The \((t, p)-filtration\) as defined here is equivalent to the definition given in [6, II, 3.2.1] for free abelian pro-\(p\) groups of finite rank.

Recall from [10] Definitions 1.1 and 1.4 that a closed subgroup \(H\) of a profinite group \(G\) is \((G-)orbital\) if it has finitely many \(G\)-conjugates, and isolated orbital if any \(G\)-orbital \(H' \geq H\) satisfies \([H' : H] = \infty\).

The following is a general property of ordered bases.

**Lemma 1.7.** Let \((G, \omega)\) be a complete \(p\)-valued group of finite rank, and \(N\) a closed isolated normal subgroup of \(G\). Then there exist sets \(B_N \subseteq B_G\) such that \(B_N\) is an ordered basis for \((N, \omega|_N)\) and \(B_G\) is an ordered basis for \((G, \omega)\).

**Proof.** This was established in [2, proof of Lemma 8.5(a)].

Remark. It may be helpful to think of this as follows:
\[ B_G = \{ x_1, \ldots, x_r, \underbrace{x_{r+1}, \ldots, x_s}_{B_N} \}, \]
where \(B_G/N = B_G \setminus B_N\) is in fact some appropriate preimage in \(G\) of any ordered basis for \((G/N, \Omega)\), where \(\Omega\) is the quotient \(p\)-valuation.

**Lemma 1.8.** Let \((G, \alpha)\) be a complete \(p\)-valued group of finite rank, and \(N\) a closed isolated orbital (hence normal) subgroup of \(G\). Take also a \(p\)-valuation \(\beta\) on \(G/N\). Suppose we are given sets
\[ B_G = \{ x_1, \ldots, x_r, \underbrace{x_{r+1}, \ldots, x_s}_{B_N} \}, \]
such that
- \(B_N\) is an ordered basis for \((N, \alpha|_N)\),
- \(B_G\) is an ordered basis for \((G, \alpha)\), and
- the image in \(G/N\) of \(B_G/N\) is an ordered basis for \((G/N, \beta)\).

In the notation of Theorem 1.3, write \(\beta\) for the composite of \(G \to G/N\) with \(\beta\), and form the \(p\)-valuation \(\omega = \inf \{ \alpha, \beta \}\) for \(G\).

Then \(B_G\) is an ordered basis for \((G, \omega)\).
Proof. We need only check that
\[ \omega(x^\lambda) = \inf_{1 \leq i \leq s} \{ \omega(x_i) + v_p(\lambda_i) \} \]
for any \( \lambda \in \mathbb{Z}_p^s \). But we have by definition that
\[ \alpha(x^\lambda) = \inf_{1 \leq i \leq s} \{ \alpha(x_i) + v_p(\lambda_i) \}, \]
\[ \beta(x^\lambda) = \inf_{1 \leq i \leq r} \{ \beta(x_i) + v_p(\lambda_i) \}, \]
and the result follows trivially. \( \square \)

1.3 Separating a free abelian quotient

Results in later sections will require the existence of a \( p \)-valuation on an appropriate group \( G \) satisfying a certain technical property, which we can now finally state:

Definition 1.9. Let \( (G, \omega) \) be a complete \( p \)-valued group of finite rank, and \( L \) a closed isolated normal subgroup containing \([G, G]\) (and hence containing the isolated derived subgroup \( G' \), which was defined and written as \( G^{(1)} \) in [10, Theorem B]). We will say that \( \omega \) satisfies property \((A_L)\) if there is an ordered basis \( \{g_{d+1}, \ldots, g_e\} \) for \( (L, \omega|_L) \), contained in an ordered basis \( \{g_1, \ldots, g_e\} \) for \((G, \omega)\) (e.g. constructed by Lemma 1.7), such that the following hold:

\[ \omega(g_1) = \cdots = \omega(g_d), \]
\[ \omega(g_1) < \omega(\ell). \] \( (A_L) \)

Remark. In the notation of the above definition, suppose that \( \omega \) satisfies \( \omega(g_1) < \omega(\ell) \) for all \( \ell \in L \). Then, by our earlier remarks, we note that the condition \((A_L)\) is equivalent to the statement that the quotient \( p \)-valuation induced by \( \omega \) on \( G/L \) is the \((t, p)\)-filtration for \( t := \omega(g_1) \).

Definition 1.10. Following [6, III, 2.1.2], we will say that a group \( G \) is \( p \)-valuable if there exists a \( p \)-valuation \( \omega \) for \( G \), and \( G \) is complete with respect to \( \omega \) and has finite rank.

Lemma 1.11. Let \( G \) be a nilpotent \( p \)-valuable group, and \( L \) a closed isolated normal subgroup containing \( G' \). Then there exists some \( p \)-valuation \( \omega \) for \( G \) satisfying \((A_L)\).

Proof. Let \( \alpha \) be a \( p \)-valuation on \( G \). Take an ordered basis \( \{g_{d+1}, \ldots, g_e\} \) for \((L, \alpha|_L)\) and extend it to an ordered basis \( \{g_1, \ldots, g_e\} \) for \((G, \alpha)\) by Lemma 1.7.

Fix a number \( t \) satisfying
\[ (p - 1)^{-1} < t \leq \inf_{1 \leq i \leq e} \alpha(g_i). \]
Applying Theorem 1.3 with \( N = L \) and \( \beta \) the \((t,p)\)-filtration on \( G/L \), we see that \( \omega = \inf\{\alpha, \beta\} \) is a \( p \)-valuation for \( G \); and by Lemma 1.8, \( \{g_1, \ldots, g_e\} \) is still an ordered basis for \((G, \omega)\), so we can check easily that \( \omega \) satisfies \((A_L)\) by construction.

**Remark.** In fact, by analysing the construction in Theorem 1.3, we can see that we have shown something stronger: that any \( p \)-valuation \( \alpha \) may be refined to such an \( \omega \) satisfying \( \omega \mid_L = \alpha \mid_L \). But we will not use this fact in this paper.

**Remark.** If \( \omega \) satisfies \((A_L)\) as above, write \( t := \omega(g_1) \). Then, for any automorphism \( \sigma \) of \( G \) and any \( 1 \leq i \leq d \), we have

\[
\omega(\sigma(g_i)) = t.
\]

This follows from Lemma 1.6(iii). Indeed, by construction, we have \( G_t = G \), and \( G_t \cdot L \) is characteristic, \( G \) is characteristic.

Now let \( G \) be a \( p \)-valuable group with fixed \( p \)-valuation \( \omega \), and let \( \sigma \in \text{Aut}(G) \). In this subsection and the next, we seek to establish conditions under which a given automorphism \( \sigma \) of \( G \) will preserve the “dominant” part of certain elements \( x \in G \) (with respect to \( \omega \)). That is, we are looking for a condition under which

\[
gr_\omega(\sigma(x)) = gr_\omega(x).
\]

Clearly it is necessary and sufficient that the following holds:

\[
\omega(\sigma(x)x^{-1}) > \omega(x).
\]  \hspace{1cm} (1.1)

The results of this paper rely on our ability to invoke the following technical result.

**Theorem 1.12.** Let \( G \) be a \( p \)-valuable group, and let \( L \) be a proper closed isolated orbital (hence normal) subgroup containing \([G,G]\), so that we have an isomorphism \( \varphi : G/L \to \mathbb{Z}_p^d \) for some \( d \geq 1 \). Write \( q : G \to G/L \) for the natural quotient map.

Choose a \( \mathbb{Z}_p \)-basis \( \{e_1, \ldots, e_d\} \) for \( \mathbb{Z}_p^d \). For each \( 1 \leq i \leq d \), fix an element \( g_i \in G \) with \( \varphi \circ q(g_i) = e_i \). Fix an automorphism \( \sigma \) of \( G \) preserving \( L \), so that \( \sigma \) induces an automorphism \( \overline{\sigma} \) of \( G/L \), and hence an automorphism \( \overline{\sigma} = \varphi \circ \overline{\sigma} \circ \varphi^{-1} \) of \( \mathbb{Z}_p^d \).

Let \( M_\sigma \) be the matrix of \( \overline{\sigma} \) with respect to the basis \( \{e_1, \ldots, e_d\} \).

Suppose there exists some \( p \)-valuation \( \omega \) on \( G \) with the following properties:

(i) \( (1.1) \) holds for all \( x \in \{g_1, \ldots, g_d\} \),

(ii) \( \omega(g_1) = \cdots = \omega(g_d) = t \), say,

(iii) \( \omega(\ell) > t \) for all \( \ell \in L \).

Then \( M_\sigma - 1 \in pM_d(\mathbb{Z}_p) \).
Remark. Conditions (ii) and (iii) are just the statement that $\omega$ satisfies ($A_L$).

Proof. Define the function $\Omega : \mathbb{Z}_p^d \to \mathbb{R} \cup \{\infty\}$ by

$$\Omega = \sup_{\ell \in L} \{\omega(g\ell)\}.$$  

By the remarks made in Definition 1.2, $\Omega$ is in fact a $p$-valuation.

By assumption (iii), we see that, for each $1 \leq i \leq d$ and any $\ell \in L$, we have $\omega(g_i) = \omega(g_i\ell)$, so that

$$\Omega(e_i) = \sup_{\ell \in L} \{\omega(g_i\ell)\} = \omega(g_i),$$

so by assumption (ii), $\Omega(e_i) = t$. Hence, by Lemma 1.6(ii), $\Omega$ must be the $(t,p)$-filtration on $\mathbb{Z}_p^d$. Now, by assumption (i), we have

$$\Omega(\hat{\sigma}(x) - x) > t$$

for all $x \in \{e_1, \ldots, e_d\}$, and hence, as $\Omega - t$ takes integer values (by Definition 1.4),

$$\Omega(\hat{\sigma}(x) - x) \geq t + 1,$$

and so $\hat{\sigma}(x) - x \in p\mathbb{Z}_p^d$ for each $x \in \{e_1, \ldots, e_d\}$, which is what we wanted to prove. \hfill \Box

Remark. With Lemma 1.6 in mind, we note the following: suppose $\omega$ satisfies hypothesis (iii) of Theorem 1.12. Then hypothesis (ii) is equivalent to the statement that the quotient filtration induced by $\omega$ on $G/L$ is actually the $(t,p)$-filtration on $G/L$.

### 1.4 Invariance under the action of a crossed product

**Definition 1.13.** Let $R$ be a ring, and fix a subgroup $G \leq R^\times$; let $F$ be a group. Fix a crossed product

$$S = R \ast_{(\sigma, \tau)} F.$$  

Consider the following properties that this crossed product may satisfy:

- The image $\sigma(F)$ normalises $G$, i.e. $x^{\sigma(f)} \in G$ for all $x \in G, f \in F$. \hfill ($N_G$)
- The image $\tau(F,F)$ normalises $G$. \hfill ($N_G'$)
- The image $\tau(F,F)$ is a subset of $G$. \hfill ($P_G$)

In the case when $G$ is $p$-valuable, consider the set of $p$-valuations of $G$. Then $\text{Aut}(G)$ acts on this set as follows:

$$(\varphi \cdot \omega)(x) = \omega(x^\varphi).$$
When \( S \) satisfies \((N'_G)\), \( \tau(F,F) \subseteq G \), so we get a map \( \rho : \tau(F,F) \to \text{Inn}(G) \) (with elements of \( G \) acting by conjugation), so we will also consider the following property:

Every \( p \)-valuation \( \omega \) of \( G \) is invariant under elements of \( \tau(F,F) \). \( (Q_G) \)

**Lemma 1.14.** In the notation above:

(i) If \( S \) satisfies \((N_G)\), then \( S \) satisfies \((N'_G)\).
(ii) If \( S \) satisfies \((P_G)\), then \( S \) satisfies \((N'_G)\).
(iii) If \( S \) satisfies \((P_G)\), then \( S \) satisfies \((Q_G)\).

**Proof.**

(i) Note that \( \rho \circ \tau(x,y) = \sigma(xy)^{-1}\sigma(x)\sigma(y) \).

(ii) Obvious.

(iii) By (ii), we see that \( S \) satisfies \((N'_G)\), so it makes sense to consider \((Q_G)\).

Let \( \omega \) be a \( p \)-valuation of \( G \), and take \( t \in \tau(F,F) \). As \( S \) satisfies \((P_G)\), we actually have \( t \in G \). Then, for any \( x \in G \), we have

\[
(t \cdot \omega)(x) = \omega(x^t) = \omega(t^{-1}xt) = \omega(x \cdot [x,t]) \geq \min\{\omega(x), \omega([x,t])\} = \omega(x),
\]

and so (by symmetry) \( \omega(t^{-1}xt) = \omega'(x) \).

**Definition 1.15.** Recall, from [11, Definition 5.4], that if we have a fixed crossed product

\[
S = R \ast_{(\sigma,\tau)} F
\]

and a 2-cocycle

\[
\alpha \in Z^2(\sigma(F, Z(R^\times))),
\]

then we may define the ring

\[
S_\alpha = R \ast_{(\sigma,\tau,\alpha)} F,
\]

the 2-cocycle twist (of \( R \), by \( \alpha \), with respect to the decomposition \((1.2)\)).

**Lemma 1.16.** Continuing with the notation above,

(i) \( S \) satisfies \((N_G)\) if and only if \( S_\alpha \) satisfies \((N_G)\).
(ii) $S$ satisfies $(Q_G)$ if and only if $S_\alpha$ satisfies $(Q_G)$.

**Proof.**

(i) Trivial from Definitions 1.13 and 1.15.

(ii) As $\alpha(F, F) \subseteq Z(R)^\times$, conjugation by $\alpha$ is the identity automorphism on $G$.

These properties will be interesting to us later as they will allow us to invoke the following lemma:

**Lemma 1.17.** If $S$ satisfies $(N_G)$, then, given any $g \in F$ and $p$-valuation $\omega$ on $G$, the function $g \cdot \omega$ given by

\[(g \cdot \omega)(x) = \omega(x^{\sigma(g)})\]

is again a $p$-valuation on $G$. If, further, $S$ satisfies $(Q_G)$, then this is a group action of $F$ on the set of $p$-valuations of $G$.

**Proof.** If $x \in G$, then $x^{\sigma(g)} \in G$ because $S$ satisfies $(N_G)$, so it makes sense to consider $\omega(x^{\sigma(g)})$. The definition above does indeed give a group action when $S$ satisfies $(Q_G)$, as, for all $g, h \in F$,

\[
(g \cdot (h \cdot \omega))(x) = h \cdot \omega(x^{\sigma(g)})
= \omega(x^{\sigma(g)\sigma(h)})
= \omega(x^{\sigma(gh)\tau(g, h)})
= \omega(x^{\sigma(gh)})
= (gh \cdot \omega)(x).
\]

The following lemma will allow us to prove the existence of a sufficiently “nice” $p$-valuation.

**Lemma 1.18.** Suppose $S$ satisfies $(N_G)$ and $(Q_G)$, so that $\sigma$ induces an action of $F$ on the set of $p$-valuations on $G$ as in the above lemma. Let $\omega$ be a $p$-valuation on $G$. If the $F$-orbit of $\omega$ is finite, then $\omega'(x) = \inf_{g \in F}(g \cdot \omega)(x)$ defines an $F$-invariant $p$-valuation on $G$.

Furthermore, if $L$ is a closed isolated characteristic subgroup of $G$ containing $G'$, and $\omega$ satisfies $(A_L)$ (as in Definition 1.9), then $\omega'$ satisfies $(A_L)$.

**Proof.** The function $\omega'$ satisfies condition [6, III, 2.1.2.2], since the $F$-orbit of $\omega$ is finite, and is hence a $p$-valuation that is $F$-stable by the remark in [6, III, 2.1.2].

Suppose $\omega$ satisfies $(A_L)$. That is, for some $t > (p - 1)^{-1}$, $\omega$ induces the $(t, p)$-filtration on $G/L$, and $\omega(\ell) > t$ for all $\ell \in L$. But, given any $g \in F$,
clearly $g \cdot \omega$ still induces the $(t, p)$-filtration on $G/L$ by Lemma 1.6(iii), and
$(g \cdot \omega) (\ell) = \omega (\ell^{\sigma(g)}) > t$, since $\ell^{\sigma(g)} \in L$ as $L$ is characteristic. Taking the infimum over the finitely many distinct $g \cdot \omega, g \in F$, shows that $\omega'$ also satisfies $(A_L)$. \qed

Recall the finite radical $\Delta^+ = \Delta^+(G)$ from [10, Definition 1.2].

**Definition 1.19.** Let $G$ be an arbitrary compact $p$-adic analytic group with $\Delta^+ = 1$, $H$ an open normal subgroup of $G$, $F = G/H$, and $P$ a faithful $G$-stable ideal of $kH$. Recall from [11, Definition 5.11] that the crossed product decomposition

$$kG/PkG = kH/P_{\langle \sigma, \tau \rangle} F$$

is *standard* if the basis $F$ is a subset of the image of the map $G \mapsto (kG/PkG)\times$.

**Lemma 1.20.** Suppose that $kG/PkG = kH/P_{\langle \sigma, \tau \rangle} F$ is a standard crossed product decomposition. Take any $\alpha \in Z^2_F(F, Z((kH/P)\times))$, and form the central 2-cocycle twist

$$(kG/PkG)_{\alpha} := kH/P_{\langle \sigma, \tau \alpha \rangle} F$$

with respect to this decomposition [11, Definition 5.4].

Consider $H$ as a subgroup of $(kH/P)^\times$: then conjugation by elements of $G$ inside $(kG/PkG)_{\alpha}$ induces a group action of $F$ on the set of $p$-valuations of $H$, as in Lemma 1.17.

**Remark.** As the crossed product notation suggests, this lemma simply says that the action of $F$ on $H$, via $\sigma$, is unchanged after applying $(-)_{\alpha}$.

**Proof.** As the decomposition is standard, $kG/PkG$ trivially satisfies both $(N_H)$ (as $H$ is normal in $G$) and $(P_H)$. By Lemma 1.14(iii), $kG/PkG$ also satisfies $(Q_H)$. Now Lemma 1.10 shows that $(kG/PkG)_{\alpha}$ also satisfies $(N_H)$ and $(Q_H)$, so that $\sigma$ induces a group action of $F$ on the $p$-valuations of $H$ inside $(kG/PkG)_{\alpha}$ by Lemma 1.17. \qed

Let $L$ be a closed isolated characteristic subgroup of $H$ containing $[H, H]$.

**Corollary 1.21.** With notation as above, we can find an $F$-stable $p$-valuation $\omega$ on $H$ satisfying $(A_L)$.

**Proof.** This now follows immediately from Lemmas 1.11 and 1.18. \qed

**Proof of Theorem B.** This follows from Corollary 1.21. \qed
2 A graded ring

2.1 Generalities on ring filtrations

Definition 2.1. Recall that a filtration $v$ on the ring $R$ is a function $v : R \to \mathbb{R} \cup \{\infty\}$ satisfying, for all $x, y \in R$,

- $v(x + y) \geq \min\{v(x), v(y)\}$,
- $v(xy) \geq v(x) + v(y)$,
- $v(0) = \infty$, $v(1) = 0$.

If in addition we have $v(xy) = v(x) + v(y)$ for all $x, y \in R$, then $v$ is a valuation on $R$.

First, a basic property of ring filtrations.

Lemma 2.2. Suppose $v$ is a filtration on $R$ which takes non-negative values, i.e. $v(R) \subseteq [0, \infty)$, and let $u \in R^\times$. Then $v(ux) = v(xu) = v(x)$ for all $x \in R$.

Proof. By the definition of $v$, we have $0 = v(1) = v(u^{-1}) \geq v(u) + v(u^{-1})$. As $v(u) \geq 0$ and $v(u^{-1}) \geq 0$, we must have $v(u) = 0 = v(u^{-1})$. Then

$$v(x) = v(u^{-1}ux) \geq v(u^{-1}) + v(ux) = v(ux) \geq v(u) + v(x) = v(x),$$

from which we see that $v(x) = v(ux)$; and by a symmetric argument, we also have $v(xu) = v(x)$.

We will fix the following notation for this subsection.

Notation. Let $G$ be a $p$-valuable group equipped with the fixed $p$-valuation $\omega$, and $k$ a field of characteristic $p$. Take an ordered basis $\{g_1, \ldots, g_d\}$ for $G$, and write $b_i = g_1 - 1 \in kG$ for all $1 \leq i \leq d$. As in [2], we make the following definitions:

- for each $\alpha \in \mathbb{N}^d$, $b^\alpha$ means the (ordered) product $b_1^{\alpha_1} \cdots b_d^{\alpha_d} \in kG$,
- for each $\alpha \in \mathbb{Z}_p^d$, $g^\alpha$ means the (ordered) product $g_1^{\alpha_1} \cdots g_d^{\alpha_d} \in G$,
- for each $\alpha \in \mathbb{N}^d$, $\langle \alpha, \omega(g) \rangle$ means $\sum_{i=1}^d \alpha_i \omega(g_i)$,
- the canonical ring homomorphism $\mathbb{Z}_p \to k$ will sometimes be left implicit, but will be denoted by $\iota$ when necessary for clarity.

Definition 2.3. With notation as above, let $w$ be the valuation on $kG$ defined in [2 6.2], given by

$$\sum_{\alpha \in \mathbb{N}^d} \lambda_\alpha b^\alpha \mapsto \inf_{\alpha \in \mathbb{N}^d} \{\langle \alpha, \omega(g) \rangle \mid \lambda_\alpha \neq 0\}.$$
Note that, in light of this formula [2 Corollary 6.2(b)], and by the construction III, 2.3.3] of w, it is clear that the value of w is in fact independent of the ordered basis chosen. In particular, if ϕ is an automorphism of G, then \{g^{\hat{\varphi}}_1, \ldots, g^{\hat{\varphi}}_d\} is another ordered basis of G; hence if ω is ϕ-stable (in the sense that ω(g^{\hat{\varphi}}) = ω(g) for all g ∈ G), then w is ϕ-stable (in the sense that w(x^{\hat{\varphi}}) = w(x) for all x ∈ kG, where \hat{\varphi} here denotes the natural extension of ϕ to kG, obtained by the universal property [11 Lemma 2.2]).

We will need the following result:

**Lemma 2.4.** Let

\[ b = b_0 + b_1p + b_2p^2 + \cdots \in \mathbb{Z}_p, \]
\[ n = n_0 + n_1p + n_2p^2 + \cdots + n_sp^s \in \mathbb{N}, \]

where all \( b_i, n_i \in \{0, 1, \ldots, p-1\} \). Then

\[ \binom{b}{n} \equiv p \prod_{i=0}^{s} \binom{b_i}{n_i} \pmod{p}. \]

**Proof.** See e.g. [1, Theorem]. □

**Corollary 2.5.** Let \( b \in \mathbb{Z}_p, n \in \mathbb{N} \). If

\[ v_p \left( \binom{b}{n} \right) = 0, \]

then \( v_p(b) \leq v_p(n) \). Further, for fixed \( b \in \mathbb{Z}_p \),

\[ \inf \left\{ n \in \mathbb{N} \mid v_p \left( \binom{b}{n} \right) = 0 \right\} = p^{v_p(b)}. \]

**Proof.** From Lemma 2.4 above, we can see that

\[ \binom{b}{n} \equiv 0 \pmod{p} \]

if and only if, for some \( 0 \leq i \leq s \),

\[ \binom{b_i}{n_i} = 0, \]

which happens if and only if one of the pairs \( (b_i, n_i) \) for \( 0 \leq i \leq s \) has \( b_i = 0 \neq n_i \). Hence, to ensure that this does not happen, we must have \( v_p(b) \leq v_p(n) \). It is clear from Lemma 2.4 that \( n = p^{v_p(b)} \) satisfies (2.1), and is the least \( n \in \mathbb{N} \) with \( v_p(b) \leq v_p(n) \). □

**Theorem 2.6.** Take any \( x \in G \), and \( t = \inf \omega(G) \). Then \( w(x-1) > t \) implies \( \omega(x) > t \).
Proof. Write $x = g^\alpha$. In order to show that $\omega(g^\alpha) > t$, it suffices to show that $\omega(g_j) + v_p(\alpha_j) > t$ for each $j$ (as there are only finitely many), and hence that $v_p(\alpha_j) \geq 1$ for all $j$ such that $\omega(g_j) = t$. This is equivalent to the claim that $p^{v_p(\alpha_j)} > 1$, which we will write as $p^{v_p(\alpha_j)} \omega(g_j) > t$ for all $j$ with $\omega(g_j) = t$.

Let $\beta(j)$ be the $d$-tuple with $i$th entry $\delta_{ij}p^\alpha$. Then, of course,

$$\langle \beta(j), \omega(g) \rangle = p^{v_p(\alpha_j)} \omega(g_j),$$

and by Corollary 2.5 we have

$$\left( \frac{\alpha}{\beta(j)} \right) \not\equiv 0 \mod p.$$

Now suppose that $w(g^\alpha - 1) > t$. We perform binomial expansion in $kG$ to see that

$$g^\alpha - 1 = \prod_{1 \leq i \leq d} (1 + b_i)^{\alpha_i} - 1 \quad \text{(ordered product)}$$

$$= \sum_{\beta \in \mathbb{N}^d} t^{\alpha/\beta} b^\beta - 1$$

$$= \sum_{\beta \neq 0} t^{\alpha/\beta} b^\beta,$$

so that

$$w(g^\alpha - 1) = \inf \left\{ \langle \beta, \omega(g) \rangle \left| \beta \neq 0, \left( \frac{\alpha}{\beta} \right) \neq 0 \mod p \right. \right\}.$$

So in particular, for all $j$ satisfying $\omega(g_j) = t$, we have

$$t < w(g^\alpha - 1) \leq \langle \beta(j), \omega(g) \rangle = p^{v_p(\alpha_j)} \omega(g_j),$$

which is what we wanted to prove. \hfill \square

2.2 Constructing a suitable valuation

Let $H$ be a nilpotent $p$-valuable group with centre $Z$. If $k$ is a field of characteristic $p$, and $p$ is a faithful prime ideal of $kZ$, then by [21, Theorem 8.4], the ideal $P := pkH$ is again a faithful prime ideal of $kH$.

We will fix the following notation for this subsection.

Notation. Let $G$ be a nilpotent-by-finite compact $p$-adic analytic group, with $\Delta' = 1$, and let $H = \text{FN}_p(G)$ [10, Definition 5.3], here a nilpotent $p$-valuable radical, so that $\Delta = Z := Z(H)$ [10, proof of Lemma 1.2.3(iii)]. We will also write $F = G/H$. 

18
Define $Q' = \mathbb{Q}(kZ/p)$, the (classical) field of fractions of the (commutative) domain $kZ/p$, and $Q = Q' \otimes kH$, a tensor product of $kZ$-algebras, which (as $P = pkH$) we may naturally identify with the (right) localisation of $kH/P$ with respect to $(kZ/p) \setminus \{0\}$ - a subring of the Goldie ring of quotients $\mathbb{Q}(kH/P)$.

Suppose further that the prime ideal $p \triangleleft kZ$ is invariant under conjugation by elements of $G$.

Choose a crossed product decomposition
\[ kG/PkG = kH/P \rtimes F \]
which is standard in the sense of the notation of Corollary 1.21. Choose also any $\alpha \in Z_2^2(F, Z((kH/P)^*))$, and form as in [11, Definition 5.4] the central 2-cocycle twist
\[ (kG/PkG)_\alpha = kH/P \rtimes \langle \sigma, \tau \rangle F. \]

Now the (right) divisor set $(kZ/p) \setminus \{0\}$ is $G$-stable by assumption, so by [8, Lemma 37.7], we may define the partial quotient ring
\[ R := Q_{\langle \sigma, \tau \rangle} \rtimes F. \quad (2.2) \]

Our aim in this subsection is to construct an appropriate filtration $f$ on the ring $R$. We will build this up in stages, following [2].

**Definition 2.7.** In [2, Theorem 7.3], Ardakov defines a valuation on $\mathbb{Q}(kH/P)$: let $v_1$ be the restriction of this valuation to $Q'$, so that $v_1(x + p) \geq w(x)$ for all $x \in kZ$ (where $w$ is as in Definition 2.3).

**Lemma 2.8.** $\sigma$ induces a group action of $F$ on the set of valuations of $Q'$.

**Proof.** Let $u$ be a valuation of $Q'$. $G$ acts on the set of valuations of $Q'$ as follows:
\[ (g \cdot u)(x) = u(g^{-1}xg). \]
Clearly, if $g \in H$, then $g^{-1}xg = x$ (as $x \in \mathbb{Q}(kZ/p)$ where $Z$ is the centre of $H$). Hence $H$ lies in the kernel of this action, and we get an action of $F$ on the set of valuations. By our choice of $\overline{F}$ as a subset of the image of $G$, this is the same as $\sigma$. \hfill $\square$

Write $\{v_1, \ldots, v_s\}$ for the $F$-orbit of $v_1$.

**Lemma 2.9.** The valuations $v_1, \ldots, v_s$ are independent.

**Proof.** The $v_i$ are all non-trivial valuations with value groups equal to subgroups of $\mathbb{R}$ by definition. Hence, by [3, VI.4, Proposition 7], they have height 1.
They are also pairwise inequivalent: indeed, suppose \( v_i \) is equivalent to \( g \cdot v_i \) for some \( g \in F \). Then by \([3, VI.3, Proposition 3]\), there exists a positive real number \( \lambda \) with \( v_i = \lambda (g \cdot v_i) \), and so \( v_i = \lambda^n (g^n \cdot v_i) \) (as the actions of \( \lambda \) and \( g \) commute) for all \( n \). But \( F \) is a finite group: so, taking \( n = o(g) \), we get \( v_i = \lambda^n v_i \). As \( v_i \) is non-trivial, we must have that \( \lambda^n = 1 \), and so \( \lambda = 1 \). So we may conclude, from \([3, VI.4, Proposition 6(c)]\), that the valuations \( v_1, \ldots, v_s \) are independent.

**Definition 2.10.** Let \( v \) be the filtration of \( Q' \) defined by

\[
v(x) = \inf_{1 \leq i \leq s} v_i(x)
\]

for each \( x \in Q' \).

**Lemma 2.11.** \( \text{gr}_v Q' \cong \bigoplus_{i=1}^{s} \text{gr}_{v_i} Q' \).

**Proof.** The natural map

\[
Q_{v,\lambda} \to \bigoplus_{i=1}^{s} Q'_{v_i,\lambda}/Q'_{v_i,\lambda^+}
\]

clearly has kernel \( \bigcap_{i=1}^{s} Q'_{v_i,\lambda^+} = Q'_{v,\lambda^+} \), giving an injective map \( \text{gr}_v Q' \to \bigoplus_{i=1}^{s} \text{gr}_v Q' \).

The surjectivity of this map now follows from the Approximation Theorem \([3, VI.7.2, Théorème 1]\), as the \( v_i \) are independent by Lemma 2.9.

Next, we will extend the \( v_i \) and \( v \) from \( Q' \) to \( Q \), as in the proof of \([2, 8.6]\).

**Notation.** Continue with the notation above. Now, \( H \) is \( p \)-valuable, and by Lemma \([1,20]\) \( F \) acts on the set of \( p \)-valuations of \( H \); hence, by Lemma \([1,18]\) (or Corollary \([1,21]\)), we may choose a \( p \)-valuation \( \omega \) which is \( F \)-stable. Fix such an \( \omega \), and construct the valuation \( w \) on \( kH \) from it as defined in Definition \([2,3]\).

Let \( \{y_{e+1}, \ldots, y_d\} \) be an ordered basis for \( Z \), and extend it to an ordered basis \( \{y_1, \ldots, y_d\} \) for \( H \) as in Lemma \([1,7]\) (noting that \( Z \) is a closed isolated normal subgroup of \( H \) by \([2, Lemma 8.4(a)]\)). For each \( 1 \leq j \leq e \), set \( c_j = y_j - 1 \) inside the ring \( kH/P \).

Recall from \([2, 8.5]\) that elements of \( Q \) may be written uniquely as

\[
\sum_{\gamma \in \mathbb{N}^e} r_{\gamma} c^\gamma,
\]

where \( r_{\gamma} \in Q' \) and \( c^\gamma := c_1^{\gamma_1} \cdots c_e^{\gamma_e} \), so that \( Q \subseteq Q'[c_1, \ldots, c_e] \) as a left \( Q' \)-module.
**Definition 2.12.** For each $1 \leq i \leq s$, as in [2] proof of Theorem 8.6], we will define the valuation $f_i : Q \to \mathbb{R} \cup \{\infty\}$ by

$$f_i \left( \sum_{\gamma \in \mathbb{N}^s} r_\gamma c_\gamma^{\gamma} \right) = \inf_{\gamma \in \mathbb{N}^s} \{ v_i(r_\gamma) + w(c_\gamma^{\gamma}) \}.$$ 

(We remark here a slight abuse of notation: the domain of $w$ is $kH$, and so $w(c_\gamma^{\gamma})$ must be understood to mean $w(b_\gamma^{\gamma})$, where $b_\gamma = y_j - 1$ inside the ring $kH$ for each $1 \leq j \leq e$. That is, $b_j$ is the “obvious” lift of $c_j$ from $kH/P$ to $kH$. This relies on the assumption that $P$ is faithful.)

Note in particular that $f_i|_{Q'} = v_i$, and $gr_{f_i} Q$ is a commutative domain, again by [2] proof of Theorem 8.6].

**Lemma 2.13.** $\sigma$ induces a group action of $F$ on the set of valuations of $Q$.

**Proof.** Let $u$ be a valuation of $Q$. Again, $G$ acts on the set of valuations of $Q$ by $(g \cdot u)(x) = u(g^{-1}xg)$. Now, any $n \in H$ can be considered as an element of $Q \times$, so that

$$(n \cdot u)(x) = u(n^{-1}x) = u(n^{-1}) + u(x) + u(n) = u(x). \quad \square$$

In the following lemma, we crucially use the fact that $\omega$ has been chosen to be $F$-stable.

**Lemma 2.14.** $f_1, \ldots, f_s$ is the $F$-orbit of $f_1$.

**Proof.** Take some $g \in F$ and some $1 \leq i, j \leq s$ such that $v_j = g \cdot v_i$. We will first show that, for all $x \in Q$, we have $f_j(x) \leq g \cdot f_i(x)$. Indeed, as $f_j|_{Q'} = v_j = g \cdot v_i = g \cdot f_i|_{Q'}$, and both $f_j$ and $g \cdot f_i$ are valuations, it will suffice to show that $(w(c_k) = f_j(c_k) \leq g \cdot f_i(c_k)$ for each $1 \leq k \leq e$.

Fix some $1 \leq k \leq e$. Write $y_k^g = zy^\alpha$ for some $\alpha \in \mathbb{Z}_p^e$ and $z \in \mathbb{Z}$, so that

$$c_k^g = y_k^g - 1 = zy^\alpha - 1$$

$$= (z - 1) + z \left( \prod_{i=1}^{e} (1 + c_i)^{n_i} - 1 \right) \quad \text{(ordered product)}$$

$$= (z - 1) + z \left( \sum_{\beta \neq 0} t_{\beta}^{\alpha} c_\beta^{\beta} \right),$$

and hence

$$(g \cdot f_i)(c_k) = \inf \left\{ v_i(z - 1), w(c_\beta^{\beta}) \mid t_{\beta}^{\alpha} \neq 0 \right\} \text{ by Definition 2.12}$$

$$\geq \inf \left\{ w(z - 1), w(c_\beta^{\beta}) \mid t_{\beta}^{\alpha} \neq 0 \right\} \text{ by Definition 2.7}$$

$$= w(c_k^g),$$
with this final equality following from [2, Lemma 8.5(b)]. But now, as \( \omega \) has been chosen to be \( G \)-stable, \( w \) is also \( G \)-stable (see the remark in Definition 2.3), so that \( w(e_k^2) = w(e_k) \).

Now, we have shown that, if \( v_j = g \cdot v_i \) on \( Q' \), then \( f_j \leq g \cdot f_i \) on \( Q \).

Similarly, we have \( v_i = g^{-1} \cdot v_j \) on \( Q' \), so \( f_i \leq g^{-1} \cdot f_j \) on \( Q \). But \( f_i(x) \leq f_j(xg^{-1}) \) for all \( x \in Q \) is equivalent to \( f_i(y^g) \leq f_j(y) \) for all \( y \in Q \) (by setting \( x = y^g \)). Hence we have \( f_i = g \cdot f_j \) on \( Q \), and we are done. \( \square \)

As in Definition 2.10

**Definition 2.15.** Let \( f \) be the filtration of \( Q \) defined by

\[
f(x) = \inf_{1 \leq i \leq s} f_i(x)
\]

for each \( x \in Q \).

We now verify that the relationship between \( f \) and \( v \) is the same as that between the \( f_i \) and the \( v_i \) (Definition 2.12).

**Lemma 2.16.** Take any \( x \in Q \), and write it in standard form as

\[
x = \sum_{\gamma \in \mathbb{N}^e} r_\gamma c^\gamma.
\]

Then we have

\[
f(x) = \inf_{\gamma \in \mathbb{N}^e} \{ v(r_\gamma) + w(c^\gamma) \}.
\]

**Proof.** Immediate from Definitions 2.10, 2.12 and 2.15. \( \square \)

Now we can extend Lemma 2.11 to \( Q \):

**Lemma 2.17.** \( \text{gr}_f Q \cong \bigoplus_{i=1}^s \text{gr}_{f_i} Q \).

**Proof.** As in the proof of Lemma 2.11 we get an injective map

\[
\text{gr}_f Q \rightarrow \bigoplus_{i=1}^s \text{gr}_{f_i} Q.
\]

The proof of [2, 8.6] gives a map

\[
(\text{gr}_v(kZ/p))[Y_1, \ldots, Y_c] \rightarrow \text{gr}_f(kH/P)
\]

and isomorphisms

\[
(\text{gr}_{v_i}(kZ/p))[Y_1, \ldots, Y_c] \cong \text{gr}_{f_i}(kH/P)
\]

22
for each $1 \leq i \leq s$, in each case mapping $Y_j$ to $\text{gr}(c_j)$ for each $1 \leq j \leq e$.

Now, $\text{gr}kH$ is a $\text{gr}$-free \cite{5} §I.4.1, p. 28] $\text{gr}kZ$-module with respect to $f$ and each $f_i$, and each of these filtrations is discrete on $kH$ by construction (see \cite{2} Corollary 6.2 and proof of Theorem 7.3), so by \cite{5} I.6.2(3), $kH$ is a filt-free $kZ$-module with respect to $f$ and each $f_i$; and by \cite{5} I.6.14, these maps extend to a map $(\text{gr}_rQ')[Y_1, \ldots, Y_e] \to \text{gr}_fQ$ and isomorphisms $(\text{gr}_rQ')[Y_1, \ldots, Y_e] \cong \text{gr}_{f_i}Q$ for each $i$.

Applying Lemma 2.14 to each $1 \leq i \leq s$, we get isomorphisms

$$(\text{gr}_rQ')[Y_1, \ldots, Y_e] \to \text{gr}_{f_i}Q,$$

which give a commutative diagram

$$
\begin{array}{ccc}
(\text{gr}_rQ')[Y_1, \ldots, Y_e] & \cong & \bigoplus_{i=1}^{s}(\text{gr}_rQ')[Y_1, \ldots, Y_e] \\
\downarrow & & \downarrow \\
\text{gr}_fQ & \cong & \bigoplus_{i=1}^{s}\text{gr}_{f_i}Q.
\end{array}
$$

Hence clearly all maps in this diagram are isomorphisms. \hfill \square

Now we return to the ring $R = Q \ast F$ defined in (3.2).

**Definition 2.18.** We can extend the filtration $f$ on $Q$ to an $F$-stable filtration on $R$ by giving elements of the basis $F$ value 0. That is, writing $F = \{g_1, \ldots, g_m\}$, any element of $Q \ast F$ can be expressed uniquely as $\sum_{r=1}^{m} g_r x_r$ for some $x_r \in Q$: the assignment

$$(Q \ast F) \to \mathbb{R} \cup \{\infty\}$$

$$\sum_{r=1}^{m} g_r x_r \mapsto \inf_{1 \leq r \leq m} \left\{ f(x_r) \right\}$$

is clearly a filtration on $Q \ast F$ whose restriction to $Q$ is just $f$. We will temporarily refer to this filtration as $\hat{f}$, though later we will drop the hat and simply call it $f$.

Note that, for any real number $\lambda$,

$$(Q \ast F)_{f,\lambda} = \bigoplus_{i=1}^{m} \mathfrak{g}_i(Q_{f,\lambda}),$$

$$(Q \ast F)_{f,\lambda^+} = \bigoplus_{i=1}^{m} \mathfrak{g}_i(Q_{f,\lambda^+}),$$

23
so that

\[
\text{gr}_f(Q \ast F) = \bigoplus_{\lambda \in \mathbb{R}} \left( \bigoplus_{i=1}^{m} \text{gr}_i(Q_{f,\lambda}/Q_{f,\lambda^+}) \right) = \bigoplus_{i=1}^{m} \text{gr}_i(Q_{f,\lambda}/Q_{f,\lambda^+}) = \bigoplus_{i=1}^{m} \text{gr}_i(Q).
\]

That is, given the data of a crossed product \( Q \ast F \) as in (3.2), we may view \( \text{gr}_f(Q \ast F) \) as \( \text{gr}_f(Q \ast F) \) in a natural way.

We will finally record this as:

**Lemma 2.19.**

\[
\text{gr}_f(Q \ast F) = \text{gr}_f(Q \ast F) \cong \left( \bigoplus_{i=1}^{s} \text{gr}_i Q \right) \ast F \cong \left( \bigoplus_{i=1}^{s} (\text{gr}_i Q')[Y_1, \ldots, Y_e] \right) \ast F,
\]

where each \( \text{gr}_i Q \) (or equivalently each \( \text{gr}_i Q' \)) is a domain (see Definition 2.12). \( F \) permutes the \( f_i \) (or equivalently the \( v_i \)) transitively by conjugation.

\[\square\]

**Proof of Theorem C.** This is Lemma 2.19.

\[\square\]

### 2.3 Automorphisms trivial on a free abelian quotient

We will fix the following notation for this subsection.

**Notation.** Let \( H \) be a nilpotent but non-abelian \( p \)-valuable group with centre \( Z \). Write \( H' \) for its isolated derived subgroup \([10, \text{Theorem B}]\). Suppose we are given a closed isolated proper characteristic subgroup \( L \) of \( H \) which contains \( H' \) and \( Z \). (We will show that such an \( L \) always exists in Lemma 3.5.) Fix a \( p \)-valuation \( \omega \) on \( H \) satisfying (A\( L \)) (which is possible by Corollary 1.21).

Let \( \{g_{m+1}, \ldots, g_n\} \) be an ordered basis for \( Z \). Using Lemma 1.7 twice, extend this to an ordered basis \( \{g_{l+1}, \ldots, g_n\} \) for \( L \), and then extend this to an ordered basis \( \{g_1, \ldots, g_n\} \) for \( H \). Diagrammatically:

\[
B_H = \{ \underbrace{g_1, \ldots, g_l}_{B_{H/L}}, \underbrace{g_{l+1}, \ldots, g_m}_{B_{L/Z}}, \underbrace{g_{m+1}, \ldots, g_n}_{B_Z} \},
\]

extending the notation of the remark after Lemma 1.7 in the obvious way. Here, \( 0 < l \leq m < n \), corresponding to the chain of subgroups \( 1 \leq Z \leq L \leq H \).

Let \( k \) be a field of characteristic \( p \). As before, let \( p \) be a faithful prime ideal of \( kZ \), so that \( P := pkH \) is a faithful prime ideal of \( kH \), and write \( b_j = g_j - 1 \in kH/P \) for all \( 1 \leq j \leq m \).
In this subsection, we will write:

- for each $\alpha \in \mathbb{N}^m$, $b^\alpha$ means the (ordered) product $b_1^{\alpha_1} \cdots b_m^{\alpha_m} \in kH/P$,
- for each $\alpha \in \mathbb{Z}_p^m$, $g^\alpha$ means the (ordered) product $g_1^{\alpha_1} \cdots g_m^{\alpha_m} \in H$,
- for each $\alpha \in \mathbb{N}^m$, $\langle \alpha, \omega(g) \rangle$ means $\sum_{i=1}^{m} \alpha_i \omega(g_i)$.

Note the use of $m$ rather than $n$ in each case. This means that every element $x \in H$ may be written uniquely as $x = zg^\alpha$ for some $\alpha \in \mathbb{Z}_p^m$ and $z \in Z$; and every element $y \in kH/P$ may be written uniquely as $y = \sum_{\gamma \in \mathbb{N}^m} r_{\gamma} b^\gamma$ for some elements $r_{\gamma} \in kZ/p$.

Recall the definitions of the filtrations $w$ on $kH$ (Definition 2.3), $v$ on $kZ/p$ (Definition 2.10) and $f$ on $kH/P$ (Definition 2.15). We will continue to abuse notation slightly for $w$, as in Definition 2.12.

Recall also that, as we have chosen $\omega$ to satisfy ($A_L$), we have that $w(b_1) = \cdots = w(b_l) < w(b_r)$ for all $r > l$.

Let $\sigma$ be an automorphism of $H$, and suppose that, when naturally extended to an automorphism of $kH$, it satisfies $\sigma(P) = P$. Hence we will consider $\sigma$ as an automorphism of $kH/P$, preserving the subgroup $H \subseteq (kH/P)^\times$.

**Corollary 2.20.** With the above notation, fix $1 \leq i \leq l$. If $f(\sigma(b_i) - b_i) > f(b_i)$, then $w(\sigma(b_i) - b_i) > w(b_i)$.

**Proof.** Write in standard form $\sigma(b_i) - b_i = \sum_{\gamma \in \mathbb{N}^m} r_{\gamma} b^\gamma$,

for some $r_{\gamma} \in kZ$, and suppose that $f(\sigma(b_i) - b_i) > f(b_i)$. That is, by Lemma 2.16,

$$v(r_{\gamma}) + w(b^\gamma) > w(b_i)$$

for each fixed $\gamma \in \mathbb{N}^m$.

We will show that $w(r_{\gamma}) + w(b^\gamma) > w(b_i)$ for each $\gamma$. We deal with two cases.

**Case 1:** $w(b^\gamma) > w(b_i)$. Then, as $w$ takes non-negative values on $kH$, we are already done.
**Case 2:** \( w(b \gamma) \leq w(b_i) \). Then, by (A.L), we have either \( w(r_\gamma) > w(b_i) \) or \( w(r_\gamma) = 0 \). In the former case, we are done automatically, so assume we are in the latter case and \( w(r_\gamma) = 0 \). Then, by (2.6.2), \( r_\gamma \) must be a unit in \( kZ \), and so \( f(r_\gamma) = 0 \) by Lemma 2.2, a contradiction.

Hence \( w(r_\gamma) + w(b \gamma) > w(b_i) \) for all \( \gamma \in \mathbb{N}^m \). But, as \( w \) is discrete by (2.6.2), we may now take the infimum over all \( \gamma \in \mathbb{N}^m \), and the inequality remains strict. \( \square \)

Let \( \sigma \) be an automorphism of \( H \), and recall that \( H/L \) is a free abelian pro-\( p \) group of rank \( l \). Choose a basis \( e_1, \ldots, e_l \) for \( \mathbb{Z}_p^l \); then the map \( g_i L \mapsto e_i \) for \( 1 \leq i \leq l \) is an isomorphism \( j : H/L \to \mathbb{Z}_p^l \). As \( L \) is characteristic in \( H \) by assumption, \( \sigma \) induces an automorphism of \( H/L \), which gives a matrix \( M_\sigma \in GL_l(\mathbb{Z}_p) \) under this isomorphism.

Write
\[
\varpi : H/L \to \mathbb{R} \cup \{\infty\}
\]
for the quotient \( p \)-valuation on \( H/L \) induced by \( \omega \), i.e.
\[
\varpi(xL) = \sup_{\ell \in L} \{\omega(x\ell)\}
\]
– note that this is just the \((t, p)\)-filtration (Definition 1.4), as we have chosen \( \omega \) to satisfy (A.L). Then write
\[
\Omega : \mathbb{Z}_p^l \to \mathbb{R} \cup \{\infty\}
\]
for the map \( \Omega = \varpi \circ j^{-1} \), the \((t, p)\)-filtration on \( \mathbb{Z}_p^l \) corresponding to \( \varpi \) under the isomorphism \( j \).

**Remark.** If \( x \in \mathbb{Z}_p^l \) has \( \Omega(x) \geq t + 1 \), then \( x \in p\mathbb{Z}_p^l \), by the definition of the \((t, p)\)-filtration.

We will write \( \Gamma(1) = 1 + pGL_l(\mathbb{Z}_p) \) for the first congruence subgroup of \( GL_l(\mathbb{Z}_p) \), the open subgroup of \( GL_l(\mathbb{Z}_p) \) whose elements are congruent to the identity element modulo \( p \).

**Corollary 2.21.** With the above notation, if \( f(\sigma(b_i) - b_i) > f(b_i) \) for all \( 1 \leq i \leq l \), then \( M_\sigma \in \Gamma(1) \).

**Proof.** We have, for all \( 1 \leq i \leq l \),
\[
\begin{align*}
f(\sigma(b_i) - b_i) &> f(b_i) \\
\implies w(\sigma(b_i) - b_i) &> w(b_i) \quad \text{by Corollary 2.20} \\
\implies \omega(\sigma(g_i)g_i^{-1}) &> \omega(g_i) \quad \text{by Theorem 2.6}
\end{align*}
\]
– which is condition (1.1). Now we may invoke Theorem 1.12. \( \square \)

**Corollary 2.22.** Suppose now further that \( \sigma \) is an automorphism of \( H \) of finite order. If \( p > 2 \) and \( f(\sigma(b_i) - b_i) > f(b_i) \) for all \( 1 \leq i \leq l \), then \( \sigma \) induces the identity automorphism on \( H/L \).

\( \square \)
Proof. We have shown that $M_\sigma \in \Gamma(1)$, which is a $p$-valuable (hence torsion-free) group for $p > 2$ by [4, Theorem 5.2]; and if $\sigma$ has finite order, then $M_\sigma$ must have finite order. So $M_\sigma$ is the identity map.

Proof of Theorem D. This now follows from Corollaries 2.21 and 2.22.

Remark. When $p = 2$, $\Gamma(1)$ is no longer $p$-valuable.

Example 2.23. Let $p = 2$, and let $H = \langle x, y, z \mid [x, y] = z, [x, z] = 1, [y, z] = 1 \rangle$ be the (2-valuable) $\mathbb{Z}_2$-Heisenberg group. Let $\sigma$ be the automorphism sending $x$ to $x^{-1}$, $y$ to $y^{-1}$ and $z$ to $z$. Take $L = \langle z \rangle$, and $P = 0$.

Write $X = x - 1 \in kH/P$, and likewise $Y = y - 1$ and $Z = z - 1$. Now,

$$\sigma(X) = \sigma(x) - 1 = x^{-1} - 1 = (1 + X)^{-1} - 1 = -X + X^2 - X^3 + \ldots,$$

and so $\sigma(X) - X = X^2 - X^3 + \ldots$ (as char $k = 2$). Hence $f(\sigma(X) - X) = f(X^2) > f(X)$; but

$$M_\sigma = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in \Gamma(1, GL_2(\mathbb{Z}_2)), $$

and in particular $M_\sigma \neq 1$.

3 Extending prime ideals from $\text{FN}_p(G)$

3.1 X-inner automorphisms

Definition 3.1. We recall the notation of [11, §5]: given $R$ a ring, $G$ a group and a fixed crossed product $S$ of $R$ by $G$, we will sometimes write the structure explicitly as

$$S = R_{\langle \sigma, \tau \rangle}^* \text{Aut}(R),$$

where $\sigma : G \to \text{Aut}(R)$ is the action and $\tau : G \times G \to R^\times$ the twisting.

Furthermore, we say that an automorphism $\phi \in \text{Aut}(R)$ is $X$-inner if there exist nonzero elements $a, b, c, d \in R$ such that, for all $x \in R$,

$$axb = cx^d d,$$

where $x^d$ denotes the image of $x$ under $\phi$. Write $\text{Xinn}(R)$ for the subgroup of $\text{Aut}(R)$ consisting of $X$-inner automorphisms; and, given a crossed product as in the previous paragraph, we will write $\text{Xinn}_S(R; G) = \sigma^{-1}(\sigma(G) \cap \text{Xinn}(R))$.

Lemma 3.2. $R$ a prime ring and $R_{\ast}G$ a crossed product. Let $G_{\text{inn}} := \text{Xinn}_{R_{\ast}G}(R; G)$.

(i) If $\sigma \in \text{Aut}(R)$ is $X$-inner, then $\sigma$ is trivial on the centre of $R$. 

27
If $H$ is a subgroup of $G$ containing $G_{inn}$, and $R \ast H$ is a prime ring, then $R \ast G$ is a prime ring.

Proof.

(i) This follows from the description of X-inner automorphisms of $R$ as restrictions of inner automorphisms of the Martindale symmetric ring of quotients $Q_s(R)$, and the fact that $Z(R)$ stays central in $Q_s(R)$: see [8, §12] for details.

(ii) This follows from [8, Corollary 12.6]: if $I$ is a nonzero ideal of $R \ast G$, then $I \cap R \ast G_{inn}$ is nonzero, and hence $I \cap R \ast H$ is nonzero. 

3.2 Properties of $\text{FN}_p(G)$

We prove here some important facts about the group $\text{FN}_p(G)$ (defined in [10, Theorem C]).

Lemma 3.3. Let $G$ be a nilpotent-by-finite compact $p$-adic analytic group with $\Delta^+ = 1$. Let $H = \text{FN}_p(G)$, and write

$$K := K_G(H) = \{ x \in G \mid [H, x] \leq H' \},$$

where $H'$ denotes the isolated derived subgroup of $H$ [10, Theorem B]. Then $K = H$.

Proof. Firstly, note that $K$ clearly contains $H$, by definition of $H'$.

Secondly, suppose that $H$ is $p$-saturable. By the same argument as in [10, Lemma 4.3], $K$ acts nilpotently on $H$, and so $K$ acts nilpotently on the Lie algebra $\mathfrak{h}$ associated to $H$ under Lazard’s isomorphism of categories [6]. That is, we get a group representation $\text{Ad} : K \rightarrow \text{Aut}(\mathfrak{h})$, and $(\text{Ad}(k) - 1)(\mathfrak{h}_i) \subseteq \mathfrak{h}_{i+1}$ for each $k \in K$ and each $i$. (Here, $\mathfrak{h}_i$ denotes the $i$th term in the lower central series for $\mathfrak{h}$.)

Choosing a basis for $\mathfrak{h}$ adapted to the flag

$$\mathfrak{h} \supseteq \mathfrak{h}_2 \supseteq \cdots \supseteq \mathfrak{h}_r = 0,$$

we see that $\text{Ad}$ is a representation of $K$ for which $\text{Ad}(k) - 1$ is strictly upper triangular for each $k \in K$; in other words, $\text{Ad} : K \rightarrow \mathcal{U}$, where $\mathcal{U}$ is a closed subgroup of some $GL_n(\mathbb{Z}_p)$ consisting of unipotent upper-triangular matrices. Hence the image $\text{Ad}(K)$ is nilpotent and torsion-free.

Furthermore, $\ker \text{Ad}$ is the subgroup of $K$ consisting of those elements $k$ which centralise $\mathfrak{h}$, and therefore centralise $H$. This clearly contains $Z(H)$. On the other hand, if $k$ centralises $H$, then $k$ is centralised by $H$, an open subgroup of $G$, and so $k$ must be contained in $\Delta$. But $\Delta = Z(H)$ by [10, Lemma 5.1(iii)].

28
Hence $K$ is a central extension of two nilpotent, torsion-free compact $p$-adic analytic groups of finite rank, and so is such a group itself; hence $K$ is nilpotent $p$-valuable by [10] Lemma 2.3, and so must be contained in $H$ by definition of $\text{FN}_p(G)$.

Now suppose $H$ is not $p$-saturable, and fix a $p$-valuation on $H$. Conjugation by $k \in K$ induces the trivial automorphism on $H/H'$, so by [6] it does also on $\text{Sat}(H/H')$, which is naturally isomorphic to $\text{Sat}(H/(\text{Sat} H)')$ by [10] Lemma 3.2. This shows that $K \subseteq K_G(\text{Sat} H)$. But now, writing $\mathfrak{h}$ for the Lie algebra associated to $\text{Sat} H$, the same argument as above, mutatis mutandis, shows that $K_G(\text{Sat} H) = H$.

Some properties.

**Lemma 3.4.** Let $G$ be a compact $p$-adic analytic group with $\Delta^+ = 1$, and write $H = \text{FN}_p(G)$. If $H$ is not abelian, then $H/Z = \text{FN}_p(G/Z)$.

**Proof.** $H/Z$ is a nilpotent $p$-valuable open normal subgroup of $G/Z$, so must be contained within $\text{FN}_p(G/Z)$. Conversely, the preimage in $G$ of $\text{FN}_p(G/Z)$ is a central extension of $Z$ by $\text{FN}_p(G/Z)$, two nilpotent and torsion-free groups, and hence is nilpotent and torsion-free, so must be $p$-valuable by [10] Lemma 2.3, which shows that it must be contained within $H$. □

Recall that, if $J$ is a closed isolated subgroup of $H$, then there exists a unique smallest isolated orbital subgroup of $H$ containing $J$, which we call its isolator, and denote $i_H(J)$, as in [10] Definition 1.6.

The (closed, isolated orbital, characteristic) subgroup $i_H(H'Z)$ of $H = \text{FN}_p(G)$ will be crucial throughout this section, so we record some results.

**Lemma 3.5.** Let $H$ be a nilpotent $p$-valuable group. If $H$ is not abelian, then $H \neq i_H(H'Z)$.

**Proof.** Suppose first that $H$ is $p$-saturated, and write $\mathfrak{h}$ and $\mathfrak{z}$ for the Lie algebras of $H$ and $Z$ respectively under Lazard’s correspondence [3]. If $h = h_2 \mathfrak{z}$ (writing $h_2$ for the second term in the lower central series of $\mathfrak{h}$), then by applying $[h, -]$ to both sides, we see that $h_2 = h_3$. But as $\mathfrak{h}$ is nilpotent, this implies that $h_2 = 0$, so that $\mathfrak{h}$ is abelian, a contradiction.

When $H$ is not $p$-saturated: note that $i_H(H'Z) = \text{Sat}(H'Z) \cap H$, by [10] Lemma 3.1, and so that $\text{Sat}(H/i_H(H'Z)) \cong \text{Sat}(H)/\text{Sat}(H'Z)$ by Lemma [10] Lemma 3.2. Hence $H/i_H(H'Z)$ has the same (in particular non-zero) rank as $\text{Sat}(H)/\text{Sat}(H'Z)$.

**Lemma 3.6.** Let $G$ be a nilpotent-by-finite compact $p$-adic analytic group with $\Delta^+ = 1$. Let $H = \text{FN}_p(G)$, and assume that $H$ is not abelian. Write

$$M := M_G(H) = \{x \in G \mid [H, x] \leq i_H(H'Z)\},$$
where $H'$ denotes the isolated derived subgroup of $H$, and $Z$ the centre of $H$.
Then $M = H$.

**Proof.** Clearly $Z \subseteq M$. We will calculate $M/Z$.

First, note that $i_H(H'Z)/Z$ is an isolated normal subgroup of $H/Z$, as the quotient is isomorphic to $H/i_H(H'Z)$, which is torsion-free. Also, as $i_H(H'Z)$ contains $H'$ and hence $[H, H/Z]$ as an open subgroup, clearly $i_H(H'Z)/Z$ contains $[H, H]Z/Z$ as an open subgroup, so that $i_H(H'Z)/Z \leq i_H/Z([H, H]Z/Z)$.

Now, $[H/Z, H/Z] = [H, H]Z/Z$ as abstract groups, so by taking their closures followed by their $(H/Z)$-isolators, we see that $(H/Z)' = i_H/Z([H, H]Z/Z) = i_H/Z([H, H]Z/Z)$, so that $i_H(H'Z)/Z = (H/Z)'$.

But $x \in M$ if and only if $[H, x] \leq i_H(H'Z)$, which is equivalent to $[H/Z, xZ] \leq (H/Z)'$, or in other words $xZ \in K_{G/Z}(H/Z) = H/Z$ by Lemma 3.3. So $M/Z = H/Z$, and hence $M = H$.

### 3.3 The extension theorem

**Proposition 3.7.** Fix a prime $p > 2$ and a finite field $k$ of characteristic $p$. Let $G$ be a nilpotent-by-finite compact $p$-adic analytic group with $\Delta^+ = 1$. Suppose $H = \text{FN}_p(G)$, and write $P = G/H$. Let $P$ be a $G$-stable, faithful prime ideal of $kH$. Let $(kG)_{\alpha}$ be a central 2-cocycle twist of $kG$ with respect to a standard (Definition 1.11) decomposition

$$kG = kH \ast_{\langle \sigma, \tau \rangle} F,$$

for some $\alpha \in Z_2^+(F, Z((kH)^{\times}))$, as in [11] Theorem 5.12]. Then $P(kG)_{\alpha}$ is a prime ideal of $(kG)_{\alpha}$.

**Proof.** First, we note that the claim that $P(kG)_{\alpha}$ is a prime ideal of $(kG)_{\alpha}$ is equivalent to the claim that

$$(kG)_{\alpha}/P(kG)_{\alpha} = kH/P \ast_{\langle \sigma, \tau \alpha \rangle} F$$

is a prime ring.

**Case 1.** Suppose that $G$ centralises $Z$.

If $H$ is abelian, so that $H = Z$, then every $g \in G$ is centralised by $Z$, an open subgroup of $G$. Hence $g \in \Delta$, i.e. $G = \Delta$. But, by [11] Theorem D), $\Delta \leq H$, and so we have $G = H$ and there is nothing to prove.
So suppose henceforth that $Z \leq H$, and write $L := i_H(H'Z)$, so that, by Lemma 3.5, we have $L \leq H$. As the decomposition of $kG$ is standard, we may view $F$ as a subset of $G$.

The idea behind the proof is as follows. We will construct a crossed product $R \ast F'$, where $R$ is a certain commutative domain and $F'$ is a certain subgroup of $F$, with the following property: if $R \ast F'$ is a prime ring, then $P(kG)_\alpha$ is a prime ideal. Then, by using the well-understood structure of $R$, we will show that the action of $F'$ on $R$ is $X$-outer (in the sense of Definition 3.1), so that $R \ast F'$ is a prime ring.

By Corollary 1.21, we can see that $H$ admits an $F$-stable $p$-valuation $\omega$ satisfying $(A)_L$. Hence, in the notation of (2.1), we may define the filtration $w$ from $\omega$ as in Definition 2.3. Furthermore, we write

$$Q' = Q(kZ/P \cap kZ), \quad Q = Q' \otimes kN,$$

as in (2.2) and we endow $Q$ with the $F$-orbit of filtrations $f_i \ (1 \leq i \leq s)$ and the filtration $f$ of Definitions 2.12 and 2.15 defined in terms of the filtration $w$ above.

By [7, 2.1.16(vii)], in order to show that the crossed product

$$kH/P \ast_{(\sigma, \tau, \alpha)} F$$

is a prime ring, it suffices to show that the related crossed product

$$Q \ast_{(\sigma, \tau, \alpha)} F$$

is prime, where this crossed product is defined in (2.2). Then, by [5, II.3.2.7], it suffices to show that

$$\text{gr}_f(Q \ast F)$$

is prime. Details of this graded ring are given in Lemma 2.19; in particular, note that

$$\text{gr}_f(Q \ast F) \cong \left( \bigoplus_{i=1}^{s} \text{gr}_{f_i} Q \right) \ast F.$$

Now, as noted in Definition 2.12, each $\text{gr}_{f_i} Q$ is a commutative domain, and by construction, $F$ permutes the summands $\text{gr}_{f_i} Q$ transitively. So by [8, Corollary 14.8] it suffices to show that

$$\text{gr}_{f_1} Q \ast F'$$

is prime, where $F' = \text{Stab}_F(f_1)$.
Notation. We set up notation in order to be able to apply the results of §2.3.

Let \( \{ y_{m+1}, \ldots, y_n \} \) be an ordered basis for \( Z \), which we extend to an ordered basis \( \{ y_1, \ldots, y_n \} \) for \( L \), which we extend to an ordered basis \( \{ y_1, \ldots, y_n \} \) for \( H \). Set \( b_i = y_i - 1 \in kH/P \), and let \( Y_i = \text{gr}_f(b_i) \) for all \( 1 \leq i \leq m \). Then

\[
\text{gr}_f \not\sim (\text{gr}_v Q') [Y_1, \ldots, Y_m].
\]

The ring on the right-hand side inherits a crossed product structure

\[
(\text{gr}_v Q') [Y_1, \ldots, Y_m] * F'.
\]

from (3.4). Writing \( R := (\text{gr}_v Q') [Y_1, \ldots, Y_m] \), we have now shown, by passing along the chain

(3.5) \( \rightarrow \) (3.4) \( \rightarrow \) (3.3) \( \rightarrow \) (3.2) \( \rightarrow \) (3.1),

that we need only show that \( R * F' \) is prime.

Write \( F'_\text{inn} \) for the subgroup of \( F' \) acting on \( R \) by \( X \)-inner automorphisms in the crossed product (3.4), i.e.

\[
F'_\text{inn} = \text{Xinn}_{R*F'}(R; F')
\]

in the notation of Definition 3.1. By the obvious abuse of notation, we will denote this action as the map of sets \( \text{gr} \sigma : F' \rightarrow \text{Aut}(R) \).

Take some \( g \in F' \). If \( \text{gr} \sigma(g) \) acts non-trivially on \( R \), then as \( R \) is commutative, we have \( g \notin F'_\text{inn} \). Hence, as by Lemma 3.2(ii) we need only show that \( R * F'_\text{inn} \) is prime, we may restrict our attention to those \( g \in F' \) that act trivially on \( R \). In particular, such a \( g \in F' \) must centralise each \( Y_i \). But

\[
\text{gr} \sigma(g)(Y_i) = Y_i \Leftrightarrow f(\sigma(g)(b_i) - b_i) > f(b_i).
\]

Now we see (as \( p > 2 \)) from Corollary 2.22 that \( \sigma(g) \) induces the identity automorphism on \( H/L \), and hence from Lemma 3.6 that \( g \in H \). That is, \( F'_\text{inn} \) is the trivial group, so that \( R * F'_\text{inn} = R \) is automatically prime.

Case 2. Suppose some \( x \in F \) does not centralise \( Z \). Write \( F_{\text{inn}} \) for the subgroup of \( F \) acting by \( X \)-inner automorphisms on \( kH/P \) in the crossed product (3.1), i.e.

\[
F_{\text{inn}} := \text{Xinn}_{(kG)_{/P}(kG)_{/P}}(kH/P; F).
\]

Then, by Lemma 3.2(i), \( x \notin F_{\text{inn}} \); so \( F_{\text{inn}} \) is contained in \( C_F(Z) \), and we need only prove that the sub-crossed product \( (kH/P) * C_F(Z) \) is prime by Lemma 3.2(ii). This reduces the problem to Case 1.

Proposition 3.8. Let \( G \) be a nilpotent-by-finite compact \( p \)-adic analytic group, and \( k \) a finite field of characteristic \( p > 2 \). Let \( H = \text{FN}_p(G) \), and write \( F = G/H \). Let \( P \) be a \( G \)-stable, almost faithful prime ideal of \( kH \). Then \( PkG \) is prime.
Proof. We assume familiarity with [11] Lemma 1.1, and adopt the notation of [11] Notation 1.2 for this proof.

Let \( e \in \operatorname{cpi}^\Delta(P) \), and write \( f_H = e|_H, f = e|_G \). Then \( PkG \) is a prime ideal of \( kG \) if and only if \( f \cdot P = \overline{kG} \) is prime in \( f \cdot \overline{kG} \).

Write \( H_1 = \operatorname{Stab}_H(e) \) and \( G_1 = \operatorname{Stab}_G(e) \). Then, by the Matrix Units Lemma [11, Lemma 6.1], we get an isomorphism

\[
f \cdot kG \cong M_s(e \cdot \overline{kG_1})
\]

for some \( s \), under which the ideal \( f \cdot P kG \) is mapped to \( M_s(e \cdot \overline{P kG_1}) \), where \( P_1 \) is the preimage in \( kH_1 \) of \( e \cdot P \cdot e \). It is easy to see that \( P_1 \) is prime in \( kH_1 \); indeed, applying the Matrix Units Lemma to \( kH \), we get

\[
f_H \cdot kH \cong M_s'(e \cdot \overline{kH_1}),
\]

under which \( f_H \cdot P \mapsto M_s'(e \cdot \overline{P \cdot e}) \), so that \( P_1 \) is prime by Morita equivalence (see e.g. [11, Lemma 1.7]). We also know from [11, Lemma 6.6] (or the remark after [11, Lemma 6.2]) that

\[
P^\dagger = \bigcap_{h \in H} (P_1^\dagger)^h.
\]

Now, writing \( q \) to denote the natural map \( G \to G/\Delta^+ \),

\[
q \left( (P_1^\dagger \cap \Delta)^h \right) = q \left( P_1^\dagger \cap \Delta \right)
\]

for all \( h \in H \), as \( q(\Delta) = Z(q(H)) \) by definition of \( H \) (see [10] Lemma 5.1(ii)); and so

\[
q \left( P_1^\dagger \cap \Delta \right) = q \left( P_1^\dagger \cap \Delta \right) = q(1).
\]

But \( q \left( P_1^\dagger \right) \) is a normal subgroup of the nilpotent group \( q(H_1) \). Hence, as the intersection of \( q \left( P_1^\dagger \right) \) with the centre \( q(\Delta) \) of \( q(H) \) is trivial, we must have that \( q \left( P_1^\dagger \right) \) is trivial also [9, 5.2.1]. That is, \( P_1^\dagger \leq \Delta^+(H_1) = \Delta^+ \).

Now, in order to show that \( M_s(e \cdot P_1 kG_1) \) is prime, we may equivalently (by Morita equivalence) show that \( e \cdot P_1 kG_1 \) is prime. By [11] Theorem 5.12, we get an isomorphism

\[
e \cdot kG_1 \cong M_t((k'[[G_1/\Delta^+]])_{\alpha}),
\]

for some integer \( t \), some finite field extension \( k'/k \), and a central 2-cocycle twist (see above or [11] Definition 5.4) of \( k'[[[G_1/\Delta^+]] \) with respect to a standard crossed product decomposition

\[
k'[[[G_1/\Delta^+]] = k'[[[H_1/\Delta^+]]] \ast (G_1/H_1)
\]

33
given by some
\[ \alpha \in Z^2 \left( G_1/H_1, Z \left( (k'[\llbracket H_1/\Delta^+ \rrbracket])^\times \right) \right). \]

Writing the image of \( e \cdot \overline{\pi} \) as \( M_t(p) \) for some ideal \( p \in k'[\llbracket H_1/\Delta^+ \rrbracket] \), we see by (see above or [11, Theorem C]) that \( p \) is a faithful, \((G_1/\Delta^+)-stable\) prime ideal of \( k'[\llbracket H_1/\Delta^+ \rrbracket] \). It now remains only to show that the extension of \( p \) to \( k'[\llbracket G_1/\Delta^+ \rrbracket] \) is prime; but this now follows from Proposition 3.7. \( \square \)

**Proof of Theorem A.** This follows from Proposition 3.8. \( \square \)

**References**

[1] R.C. Alperin. \textit{p}-adic binomial coefficients MOD \( P \). \textit{The American Mathematical Monthly}, 92(8):576–578, 1985.

[2] K. Ardakov. Prime ideals in nilpotent Iwasawa algebras. \textit{Inventiones mathematicae}, 190(2):439–503, 2012.

[3] N. Bourbaki. \textit{Commutative Algebra}. Springer, 1998.

[4] J.D. Dixon, M.P.F. du Sautoy, A. Mann and D. Segal. \textit{Analytic Pro-p Groups}. Cambridge University Press, 1999.

[5] Li Huishi and Freddy van Oystaeyen. \textit{Zariskian Filtrations}. Springer Science+Business Media, 1996.

[6] Michel Lazard. Groupes analytiques \( p \)-adiques. \textit{Publications Mathématiques de l'IHÉS}, 26:5–219, 1965.

[7] J.C. McConnell and J.C. Robson. \textit{Noncommutative Noetherian Rings}. American Mathematical Society, 2001.

[8] Donald S. Passman. \textit{Infinite Crossed Products}. Academic Press Inc., 1989.

[9] Derek J.S. Robinson. \textit{A course in the theory of groups}. Springer-Verlag New York, 1996.

[10] W. Woods. On the structure of virtually nilpotent compact \( p \)-adic analytic groups. Preprint, \texttt{arXiv:1608.03137 [math.GR]}, 2016. To appear in \textit{J. Group Theory}.

[11] W. Woods. Maximal prime homomorphic images of mod-\( p \) iwasawa algebras. Preprint, \texttt{arXiv:1608.07755 [math.RT]}, 2016.