Virtually nilpotent mod-p Iwasawa algebras are catenary

William Woods

Brasenose College

University of Oxford

A thesis submitted for the degree of

Doctor of Philosophy

Trinity 2016

Acknowledgements

I would like to express my sincere gratitude to my supervisor, Prof. Konstantin Ardakov, for the time and effort he put into advising me, and for many interesting and helpful conversations; to my colleagues in London and Oxford, and elsewhere, for their continuing encouragement and interest in my work; and to all those who supported me during the writing of this thesis.

This research was supported in part by an EPSRC studentship and in part by the University of Oxford, to whom I am very grateful.

Abstract

Fix a prime $p > 2$. Let G be a nilpotent-by-finite compact p-adic analytic group, and k a finite field of characteristic p. We prove that kG is a catenary ring.

Contents

Introduction

In this thesis, we study the prime ideal structure of completed group rings kG of compact p-adic analytic groups G over certain rings k. Most notably in the cases $k = \mathbb{Z}_p$ or $k = \mathbb{F}_p$, kG is sometimes referred to as the *Iwasawa algebra* of G. Throughout this thesis, k will be a field of characteristic p; many results will require stronger hypotheses (e.g. that k be finite), and we will always state these explicitly.

Recall that a ring R is called *catenary* if, given any two prime ideals $P \lneq Q$ of R, any two saturated chains of prime ideals beginning at P and ending at Q have the same length. The main result of this thesis is:

Theorem A. [Corollary 10.3.3] Let G be a nilpotent-by-finite compact p-adic analytic group, and k a finite field of characteristic $p > 2$. Then kG is a catenary ring. $\square$

In order to prove this, we will first need the concept of an *orbitally sound* compact p-adic analytic group.

Let G be a compact p-adic analytic group, and H a closed subgroup. Following Roseblade [24], we will say that H is *orbital* (or *G-orbital*) if it only has finitely many G-conjugates, or equivalently if its normaliser $\mathbf{N}_G(H)$ is open in G; and H is *isolated orbital* (or *G-isolated orbital*) if H is orbital, and given any other closed orbital subgroup H' of G with $H \lneq H'$, we have $[H' : H] = \infty$. G is then said to be *orbitally sound* if all its isolated orbital closed subgroups are in fact normal.

The majority of the work goes into proving:

Theorem B. [Theorem 10.1.12] Let G be a nilpotent-by-finite, *orbitally sound* compact p-adic analytic group, and k a finite field of characteristic $p > 2$. Then kG is a catenary ring. □

The main idea of the proof follows Roseblade [24]: we will show that, under certain hypotheses, we may reduce the problem of understanding prime ideals of kG to one of understanding prime ideals of kA for A a free abelian compact p-adic analytic group – that is, $A \cong \mathbb{Z}_p^d$ for some d, and kA a power series ring in d variables.

The link connecting Theorem B to Theorem A is as follows. We will say that a prime ideal P of kG is *faithful* if the natural group homomorphism $G \to (kG/P)^\times$ is injective.

Theorem C. Let G be a nilpotent-by-finite compact p-adic analytic group. Then

(i) [Definition 2.1.5 and Theorem 2.1.6(ii)] G contains an open characteristic subgroup $\mathrm{nio}(G)$ which is orbitally sound, and is the maximal such open normal subgroup.

(ii) [Theorem 10.2.7] Suppose G is *not* orbitally sound, and P is a faithful prime ideal of kG. Then P is *induced* from some proper open subgroup H of G containing $\mathrm{nio}(G)$: that is, there is an ideal L of kH such that P is the largest two-sided ideal contained in LkG. □

This is a corollary of a "vertices and sources" result (Theorem 10.2.7), a partial analogue of a theorem by Lorenz and Passman [17] for the case of group algebras of polycyclic-by-finite groups. Theorem C depends mostly on some arguments around prime and G-prime ideals, Krull(-Gabriel-Rentschler) dimension, etc. which are reasonably independent of the rest of the material in this thesis; this is the majority of §8.

In order to be able to address Theorem B, we will first need to understand the structure of nilpotent-by-finite compact p-adic analytic groups G.

We know already that there is an open characteristic subgroup $\mathrm{nio}(G)$ of G. We may define also the two closed characteristic subgroups

$$\begin{aligned}\Delta \ &= \{x \in G \mid [G : \mathbf{C}_G(x)] < \infty\},\\ \Delta^+ &= \{x \in \Delta \mid o(x) < \infty\},\end{aligned}$$

and it will be clear that we have the inclusion

$$1 \leq \Delta^+ \leq \Delta \leq \mathrm{nio}(G) \leq G.$$

We will show the existence of another series of important closed characteristic subgroups:

Theorem D.

(i) [§2.5] Let G be a nilpotent-by-finite compact p-adic analytic group. Then there exists an open characteristic subgroup $\mathbf{FN}_p(G)$ which is maximal among those open normal subgroups H containing Δ^+ with the property that H/Δ^+ is nilpotent and p-valuable. (This is the *finite-by-(nilpotent p-valuable)* radical of G.) Also, $\mathrm{nio}(G)/\mathbf{FN}_p(G)$ is isomorphic to a subgroup of $t(\mathbb{Z}_p^\times)$, the (cyclic) group of torsion units of the ring $\mathbb{Z}_p$.

(ii) [§2.3] Let N be a p-valuable group. Then there exists a unique fastest descending series of isolated orbital closed normal subgroups of N, the *isolated lower central series*,

$$N = N_1 \rhd N_2 \rhd \dots,$$

with the properties that each N_i is characteristic in N, N_i/N_{i+1} is abelian for each i, $[N_i, N_j] \leq N_{i+j}$ for all i and j, and there exists some r with $N_r = 1$ if and only if N is nilpotent.

There exists also a unique fastest descending series of isolated orbital closed normal subgroups of N, the *isolated derived series*,

$$N = N^{(0)} \rhd N^{(1)} \rhd \dots,$$

with the properties that each $N^{(i)}$ is characteristic in N, $N^{(i)}/N^{(i+1)}$ is abelian for each i, and there exists some r with $N^{(r)} = 1$ if and only if N is soluble. $\square$

In the case when G is nilpotent-by-finite, we will take $N = \mathbf{FN}_p(G)/\Delta^+$, and write H_i for the preimage in G of $N_i = H_i/\Delta^+$. With this notation, we show:

Theorem E. [§2.5] Let G be a nilpotent-by-finite compact p-adic analytic group. With notation as above, let a be a preimage in $\mathrm{nio}(G)$ of a generator of $\mathrm{nio}(G)/\mathbf{FN}_p(G)$. Then conjugation by a acts on each H_i, and hence induces an action on the (free, finite-rank) $\mathbb{Z}_p$-modules $H_i/H_{i+1} = A_i$. In multiplicative notation, there is some scalar $\zeta \in t(\mathbb{Z}_p^\times)$ such that $x^a = x^{\zeta^i}$ for all $x \in A_i$. $\square$

Putting these ingredients together allows us to understand the structure of a nilpotent-by-finite compact p-adic analytic group G, which, for convenience, we display in the following diagram.

$$
\begin{tikzcd}
 & G \arrow[d, dash] \\
 & \mathrm{nio}(G) \arrow[d, equal, "\lesssim t(\mathbb{Z}_p^\times)"] \\
H_1 \arrow[r, equal] \arrow[d, equal, "a\colon \zeta \circlearrowright \mathbb{Z}_p^{d_1} \cong A_1"'] & H \arrow[ddddd, equal, "\text{nilpotent, } p\text{-valuable}"] \\
H_2 \arrow[d, dash] & \\
\vdots \arrow[d, dash] & \\
H_{r-1} \arrow[d, equal, "a\colon \zeta^{r-1} \circlearrowright \mathbb{Z}_p^{d_{r-1}} \cong A_{r-1}"'] & \\
H_r \arrow[r, equal] & \Delta^+ \arrow[d, dash] \\
 & 1
\end{tikzcd}
$$

Let H be a closed normal subgroup of G. We will say that an ideal I of kG is *controlled by* H if $(I \cap kH)kG = I$.

To prove the analogue of Theorem B in the case of polycyclic group algebras, Roseblade [24] first showed that faithful prime ideals P were controlled by Δ. Ardakov [4] has proved an analogue of this result in the case of nilpotent p-valuable compact p-adic analytic groups:

Theorem. [4, 8.4, 8.6] Let G be a nilpotent p-valuable group and k a field of characteristic p. Then faithful primes P are controlled by the centre of G. $\square$

The idea behind Roseblade's proof is as follows. As Δ is finite-by-(torsion-free abelian), its centre A is of finite index. If we are able to reduce from prime ideals of kG to certain (semi)prime ideals of $k\Delta$, and then (by a finite-index argument) to certain (semi)prime ideals of kA, then we have reduced our problem to one of *commutative* algebra.

In §§3–4, we will explore the structure of the ring kG/M, where M is an arbitrary minimal prime ideal of kG. It is known already, due to Ardakov, that the minimal primes of kG are intimately connected with the minimal primes of $k\Delta^+$: we review this connection in Lemma 1.5.1. We strengthen the results in [5, Propositions 10.1, 10.4] and [3], which deal only with cases such as when $G = F \times U$, for F a finite group and U a uniform pro-p group, as below.

Our first result along these lines is as follows.

Theorem F. [Theorem 4.1.5(ii)] Let G be a compact p-adic analytic group with G/Δ^+ pro-p, and let k be a finite field of characteristic p. Take a minimal prime $\mathfrak{p}$ of $k\Delta^+$ which is G-invariant, so that $\mathfrak{p}kG$ is a minimal prime of kG. Then there exist a positive integer t, a finite field extension k'/k, and an isomorphism

$$\psi : kG/\mathfrak{p}kG \to M_t\Big(k'[[G/\Delta^+]]\Big). \qquad \square$$

(The "G-invariant" condition is not too restrictive; we will return to this issue later.)

In fact, in proving this theorem, we give a more explicit construction of such an isomorphism, so as to be able to keep track of images of ideals and subrings.

In the general case, if G is a compact p-adic analytic group, G will have an open normal subgroup H satisfying the conditions of Theorem F; but this may not in general extend to an isomorphism

$$kG/\mathfrak{p}kG \to M_t\Big(k'[[G/\Delta^+]]\Big).$$

However, this is not too far off. We show that a similar result does hold, provided we are willing to replace $k'[[G/\Delta^+]]$ by a closely related ring $\big(k'[[G/\Delta^+]]\big)_\alpha$, a *central 2-cocycle twist* of $k'[[G/\Delta^+]]$. We define this fully in Definition 4.2.2, and then show that the twisting process $(-)_\alpha$ preserves some desirable properties.

Theorem G. [Theorem 4.2.10] Let G be a compact p-adic analytic group and H an open normal subgroup containing Δ^+ with H/Δ^+ pro-p, and let k be a finite field of characteristic p. Take a minimal prime $\mathfrak{p}$ of $k\Delta^+$ which is G-invariant (note that then $\mathfrak{p}kH$ is a minimal prime of kH and $\mathfrak{p}kG$ is a minimal prime of kG). Then the isomorphism

$$\psi : kH/\mathfrak{p}kH \to M_t\Big(k'[[H/\Delta^+]]\Big)$$

of Theorem F (applied to the group H) extends to an isomorphism

$$\tilde{\psi} : kG/\mathfrak{p}kG \to M_t\Big(\big(k'[[G/\Delta^+]]\big)_\alpha\Big).$$ □

Studying this isomorphism in detail allows us to understand the behaviour of ideals of kG containing $\mathfrak{p}kG$ by understanding ideals of $\big(k'[[G/\Delta^+]]\big)_\alpha$. We derive some consequences of Theorem G that will be useful in later work.

In Definition 1.6.2 below, we will say that an ideal I of kG is *faithful* if the natural map $G \to (kG/I)^\times$ is an injection, and *almost faithful* if its kernel is finite. A measure of the failure of I to be faithful is given by the normal subgroup $I^\dagger := \ker(G \to (kG/I)^\times)$.

Theorem H. [Corollaries 3.2.3 and 4.2.11] With notation as in Theorem G, let A be an ideal of kH containing $\mathfrak{p}kH$. Write $\psi(A/\mathfrak{p}kH) = M_t(\mathfrak{a})$ for some ideal $\mathfrak{a}$ of $k'[[H/\Delta^+]]$. Then

(i) A is prime in kH if and only if $\mathfrak{a}$ is prime in $k'[[H/\Delta^+]]$.

(ii) A is stable under conjugation by G if and only if $\mathfrak{a}$ is stable under conjugation by G/Δ^+ in the ring $\big(k'[[G/\Delta^+]]\big)_\alpha$.

(iii) A is almost faithful as an ideal of kH if and only if $\mathfrak{a}$ is (almost) faithful as an ideal of $k'[[H/\Delta^+]]$. □

We state all of these results together here for convenience. Statement (i) above is an easy consequence of Morita equivalence, given in Lemma 1.6.5, but statements (ii) and (iii) rely crucially on explicit calculations under the isomorphism ψ.

We note here briefly that $\mathfrak{p}$ will not necessarily be G-invariant, but may have a (finite) G-orbit, say of size r. In this case, we can extend Theorem G to the following:

Theorem I. [Lemma 4.3.1] Let G be a compact p-adic analytic group and H an open normal subgroup containing Δ^+ with H/Δ^+ pro-p, and let k be a finite field of characteristic p. Take a minimal prime $\mathfrak{p}$ of $k\Delta^+$ which is *not necessarily* G-invariant, and let its stabiliser G_1 have index r in G. Then there is an isomorphism

$$kG/Q \to M_r(kG_1/\mathfrak{p}kG_1),$$

so that the isomorphism

$$kG_1/\mathfrak{p}kG_1 \to M_t\Big(\big(k'[[G_1/\Delta^+]]\big)_\alpha\Big)$$

of Theorem G (applied to the group G_1) extends to an isomorphism

$$kG/Q \to M_{rt}\Big(\big(k'[[G_1/\Delta^+]]\big)_\alpha\Big). \qquad \square$$

We prove a much more precise statement of this theorem in §3.1, but do not state it here as the notation is rather technical. The more precise statement helps in understanding the relationship between ideals of kG and ideals of kH, when H is a closed normal subgroup of G. When H acts transitively on the G-orbit of $\mathfrak{p}$, as in the special case of Theorem G, it is not hard to generalise Theorem H; but the G-orbit of $\mathfrak{p}$ may split into several H-orbits, possibly of different sizes, and it is important to keep track of the isomorphism.

Using these various simplifications, we are almost able to extend the theorem of Ardakov to a stronger analogue of Roseblade's control theorem. We first prove the following intermediate result:

Theorem J. [Proposition 7.3.3] Let G be a nilpotent-by-finite compact p-adic analytic group and k a field of characteristic $p > 2$. Let $H = \mathbf{FN}_p(G)$, and let P be a G-stable, almost faithful prime ideal of kH. Then PkG is prime.

The proof of this theorem is fairly technical. For the majority of the work, we assume $\Delta^+ = 1$, so that H is nilpotent p-valuable; in §5 we construct an appropriate p-valuation on H, and in §7 we use this to form a filtration on a partial quotient ring of kH/P which respects a particular crossed product decomposition $kG/PkG = kH/P * F$, and the proof of Theorem [J] follows from studying the graded ring with respect to this filtration.

Finally, we get:

Theorem K. [Theorem 9.3.7] Let G be a nilpotent-by-finite, orbitally sound compact p-adic analytic group, k a finite field of characteristic $p > 2$, and P an almost faithful prime ideal of kG. Then P is controlled by Δ.

The deduction from Theorem K of Theorem B is adapted from methods outlined in [24], and then Theorem A is deduced by mimicking results from [15], [16], [17], and others.

Chapter 1

Preliminaries

1.1 Compact p-adic analytic groups

Our primary object of study will be the completed group algebras of compact p-adic analytic groups. These are perhaps most simply defined as closed subgroups G of the (profinite) group $GL_n(\mathbb{Z}_p)$ for some $n \geq 0$. It is known that

$$\left\{\begin{matrix}\text{uniform groups}\\ \text{[9, Definition 4.1]}\end{matrix}\right\} \subseteq \left\{\begin{matrix}p\text{-valuable groups}\\ \text{[13, III, 2.1.2]}\end{matrix}\right\} \subseteq \left\{\begin{matrix}\text{compact } p\text{-adic}\\ \text{analytic groups}\\ \text{[9, Definition 8.14]}\end{matrix}\right\},$$

with the first inclusion coming from [9, Definition 1.15; notes at end of chapter 4], and the second from [9, Corollary 8.34]. We will say more about p-valuable groups in §1.3.

Note also that compact p-adic analytic groups G are profinite groups satisfying **Max**: every nonempty set of closed subgroups of G contains a maximal element. Indeed, in the case when G is p-valuable, this follows from [13, III, 3.1.7.5]. In the general case, G contains a uniform open normal subgroup U by [9, 8.34]; and, given a nonempty set $\mathcal{A}_G$ of closed subgroups of G, we can consider the related nonempty set $\mathcal{A}_U = \{X \cap U | X \in \mathcal{A}_G\}$ of closed subgroups of U. A maximal element Y of $\mathcal{A}_U$ must come from an element X of $\mathcal{A}_G$ with $Y = X \cap U$, and $[X : Y] \leq [G : U] < \infty$, so if X is not maximal, choose an element $Z \in \mathcal{A}_G$ strictly containing X; an induction argument on the index $[Z : Y]$ shows that we will find a maximal closed subgroup in finitely many steps.

Finally, we remark that [9, 8.34] implies that compact p-adic analytic groups are precisely extensions of uniform (or p-valuable) groups by finite groups.

1.2 Orbital subgroups, Δ and Δ^+

Definition 1.2.1. Let G be a profinite group. A closed subgroup H of G is G-*orbital* (or just *orbital*, when the group G is clear from context) if H has only finitely many G-conjugates, i.e. if $\mathbf{N}_G(H)$ is open in G. Similarly, an element $x \in G$ is *orbital* if $[G : \mathbf{C}_G(x)] < \infty$.

Definition 1.2.2. The *FC-centre* $\Delta(G)$ of a profinite group G is the subgroup of all orbital elements of G. The *finite radical* $\Delta^+(G)$ of G is the subgroup of all torsion orbital elements of G.

Remark. Throughout this thesis, we will write as shorthand $\Delta^+ = \Delta^+(G)$ and $\Delta = \Delta(G)$. Also throughout, all homomorphisms will be continuous, etc. unless otherwise specified; see e.g. [9, Corollary 1.20].

Lemma 1.2.3. Let G be a compact p-adic analytic group. For convenience, we record a few basic properties of Δ and Δ^+.

(i) Δ^+ is finite.

(ii) If H is an open subgroup of G, then $\Delta^+(H) \leq \Delta^+(G)$ and $\Delta(H) \leq \Delta(G)$.

(iii) When G is compact p-adic analytic, Δ^+ and Δ are closed in G.

(iv) Δ^+ and Δ are characteristic subgroups of G.

(v) Δ/Δ^+ is a torsion-free abelian group.

Proof.

(i) Δ^+ is generated by the finite normal subgroups of G [22, 5.1(iii)]. It is obvious that the compositum of two finite normal subgroups is again finite and normal. Now suppose that Δ^+ is infinite, and take an open uniform subgroup H of G [9, 4.3]: then $\Delta^+ \cap H$ is non-trivial, and so we must have some finite normal subgroup F with $F \cap H$ non-trivial. But F is torsion, so this contradicts the fact that H is torsion-free [9, 4.5].

(ii) If an element $x \in H$ has finitely many H-conjugates, and H has finite index in G, then x has finitely many G-conjugates.

(iii) Δ^+ is closed because it is finite.

For the case of Δ, suppose first that G is p-valued [13, III, 2.1.2]. Now, any orbital $x \in G$ has $\mathbf{C}_G(x)$ open in G, and so, for any $g \in G$, there exists some n with $g^{p^n} \in \mathbf{C}_G(x)$, i.e. $g^{p^n}x = xg^{p^n}$. This implies that $(g^x)^{p^n} = g^{p^n}$, and so by [13, III, 2.1.4], we get $g^x = g$. Hence $\mathbf{C}_G(x) = G$. In other words, $\Delta = Z(G)$, which is closed in G.

When G is not p-valued, it still has an open p-valued subgroup N [9, 4.3]. Clearly $\Delta(N) = \Delta(G) \cap N$, and so $[\Delta(G) : \Delta(N)] \leq [G : N] < \infty$. So $\Delta(G)$ is a finite union of translates of $Z(N)$, which is closed in N and hence closed in G.

(iv) See [21, discussion after lemma 4.1.2 and lemma 4.1.6].

(v) See [21, lemma 4.1.6]. $\square$

Throughout the remainder of this subsection, G is a profinite group unless stated otherwise.

Definition 1.2.4. An orbital closed subgroup H of G is *isolated* if, for all orbital closed subgroups H' of G with $H \lneq H' \leq G$, we have $[H' : H] = \infty$. (We will sometimes say that a closed subgroup is *G-isolated orbital* as shorthand for *isolated as an orbital closed subgroup of G*.) Following Passman [22, definition 19.1], if all isolated orbital closed subgroups of G are in fact normal, we shall say that G is *orbitally sound*.

We record a few basic properties, before showing that this definition is the same as the one given in [24, 1.3] and [4, 5.8] (in Lemma 1.2.10 below).

Lemma 1.2.5. Let N be a closed normal subgroup of G.

(i) Suppose H is a closed subgroup of G containing N. Then H/N is (G/N)-orbital if and only if H is G-orbital; and H/N is (G/N)-isolated orbital if and only if H is G-isolated orbital.

(ii) Suppose G is orbitally sound. Then G/N is orbitally sound.

(iii) Suppose N is finite and G/N is orbitally sound. Then G is orbitally sound.

Proof.

(i) It is easily checked that $\mathbf{N}_{G/N}(H/N) = \mathbf{N}_G(H)/N$, and so

$$[G : \mathbf{N}_G(H)] = [G/N : \mathbf{N}_G(H)/N] = [G/N : \mathbf{N}_{G/N}(H/N)].$$

So H is orbital if and only if H/N is orbital. Suppose these two groups are both orbital, and let H' be an orbital closed subgroup of G with $H \lneq H' \leq G$: then $[H' : H] = [H'/N : H/N]$, so H is isolated if and only if H/N is isolated.

(ii) Let H/N be an isolated orbital closed subgroup of G/N. Then, by (i), H is an isolated orbital subgroup of G, so $H \lhd G$, and so $H/N \lhd G/N$.

(iii) Let H be an isolated orbital closed subgroup of G. As N is normal in G, clearly $\mathbf{N}_G(HN) = \mathbf{N}_G(H)$, so that HN is G-orbital. But $[HN : H] < \infty$, and so we must have $HN = H$ as H is *isolated* orbital. So, by (i), H/N is (G/N)-*isolated* orbital, and hence normal, as G/N is orbitally sound by assumption. But this means that H is normal in G. $\square$

From now on, we assume that G is a profinite group satisfying the *maximum condition* on closed subgroups: every nonempty set of closed subgroups of G has a maximal element.

Recall our earlier remark that, if G is compact p-adic analytic, it satisfies the maximum condition on closed subgroups.

Definition 1.2.6. If H is an orbital closed subgroup of G, we define its *isolator* $\mathrm{i}_G(H)$ in G to be the closed subgroup of G generated by all orbital closed subgroups L of G containing H as an open subgroup, i.e. with $[L : H] < \infty$.

Once we have proved that $\mathrm{i}_G(H)$ is indeed an isolated orbital closed subgroup of G containing H as an open subgroup, it will be clear from the definition that it is the unique such closed subgroup.

We now prove some basic properties of $\mathrm{i}_G(H)$, following [22].

Proposition 1.2.7. Suppose H is an orbital closed subgroup of G. Then H is open in $\mathrm{i}_G(H)$.

Proof. We first show that, if L_1 and L_2 are orbital subgroups of G containing H as an open subgroup, then $\left[\overline{\langle L_1, L_2\rangle} : H\right] < \infty$. Write $(-)^\circ$ for $\bigcap_{g\in G}(-)^g$. Suppose without loss of generality that $G = \overline{\langle L_1, L_2\rangle}$, and that $H^\circ = 1$ (by passing to G/H°).

For $i = 1, 2$, as $[L_i : H] < \infty$ and as H, L_i are all orbital, we may take an open normal subgroup N of G such that $[N, L_i] \subseteq H$. Indeed, $\mathbf{N}_G(L_i)$ is a subgroup of finite index in G, and permutes the (finitely many) left cosets of H in L_i by left multiplication; take N_i to be the kernel of this action, and set $N = N_1 \cap N_2$.

Hence $[N \cap H, L_i] \subseteq N \cap H$, i.e. both L_1 and L_2 normalise $N \cap H$, so G normalises $N \cap H$. So $N \cap H$ is a normal subgroup of G contained in H, and by assumption must be trivial. But N was an open subgroup of G, so H must have been finite, and so L_1 and L_2 must be *finite* orbital subgroups of G. This implies that $L_i \leq \Delta^+$, and hence $G = \Delta^+$, so that G is finite, as required.

Now, in the general case, G satisfies the maximal condition on closed subgroups, so we can choose L maximal subject to L being orbital and $[L : H] < \infty$. This L is $\mathrm{i}_G(H)$ and contains H as an open subgroup. $\square$

Lemma 1.2.8.

(i) Suppose H is an orbital closed subgroup of G. Then $\mathrm{i}_G(H)$ is an isolated orbital closed subgroup of G. Furthermore, if H is normal in G, then so is $\mathrm{i}_G(H)$.

(ii) Suppose G is orbitally sound and H is a closed subgroup of finite index. Then H is orbitally sound.

Proof.

(i) If $\mathrm{i}_G(H)$ is orbital, then by Proposition 1.2.7, it is isolated (by construction). But H has finite index in $\mathrm{i}_G(H)$, so $\mathrm{i}_G(H)$ must be generated by a finite number of closed orbital subgroups $L_1, \dots, L_n$ containing H as a subgroup of finite index. So

$$\bigcap_{i=1}^{n} \mathbf{N}_G(L_i) \leq \mathbf{N}_G(\mathrm{i}_G(H)),$$

and as each $\mathbf{N}_G(L_i)$ is open in G, so is $\mathbf{N}_G(\mathrm{i}_G(H))$.

Now suppose that H is normal in G. To see that $\mathrm{i}_G(H)$ is normal in G, fix $g \in G$, and note that conjugation by g fixes H and therefore simply permutes the set of orbital closed subgroups L of G containing H as an open subgroup, i.e. permutes the set of subgroups of G that generate $\mathrm{i}_G(H)$ (see Definition 1.2.6).

(ii) Let K be an isolated H-orbital closed subgroup of H. Then K is G-orbital, so $\mathrm{i}_G(K)$ is an isolated orbital subgroup of G, and so is normal in G. Hence $\mathrm{i}_G(K) \cap H$ is normal in H. But $[\mathrm{i}_G(K) : K] < \infty$, so $[\mathrm{i}_G(K) \cap H : K] < \infty$, and hence $\mathrm{i}_G(K) \cap H = K$, as K was assumed to be isolated in H. □

Lemma 1.2.9. Let H be an open normal subgroup of G. Then there is a one-to-one correspondence

$$\left\{\begin{array}{c}\text{isolated orbital}\\ \text{closed subgroups of } G\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{isolated orbital}\\ \text{closed subgroups of } H\end{array}\right\}$$
$$G' \longmapsto G' \cap H,$$
$$\mathrm{i}_G(H') \longleftarrow H'.$$

Proof. Suppose first that H' is an arbitrary orbital closed subgroup of H. That is, $\mathbf{N}_H(H')$ is open in H, hence also in G, and so $\mathbf{N}_G(H')$ must be open in G. Therefore H' is also G-orbital, and so, by Lemma 1.2.8(i), $\mathrm{i}_G(H')$ is an isolated orbital closed subgroup of G.

Next, take a G-isolated orbital closed subgroup G' of G. As G' and H are both G-orbital, so is $G' \cap H$, and so we may take its G-isolator; we will show that $\mathrm{i}_G(G' \cap H) = G'$. But both G' and $\mathrm{i}_G(G' \cap H)$ are G-isolated orbital (G' by assumption, $\mathrm{i}_G(G' \cap H)$ by definition) and contain $G' \cap H$ as an open subgroup, so by uniqueness (see Definition 1.2.6), they are equal.

Furthermore, as $G' \cap H$ is G-orbital, it is also H-orbital. Take some closed orbital subgroup L of H containing $G' \cap H$ as an open subgroup; then, by the previous paragraph, L is contained in $\mathrm{i}_H(G' \cap H) \leq \mathrm{i}_G(G' \cap H) = G'$; and L is contained in H

by assertion, so must in fact be contained in $G' \cap H$. Hence we conclude that $G' \cap H$ is its own H-isolator, and is hence already isolated orbital in H.

Finally, take an isolated orbital closed subgroup H' of H; it remains to show that $\mathrm{i}_G(H') \cap H = H'$. To do this, note that $\mathrm{i}_G(H')$ contains H' as an open subgroup by Proposition 1.2.7, so $\mathrm{i}_G(H') \cap H$ is an H-orbital closed subgroup (by the correspondence above) containing the H-isolated orbital H' as an open subgroup, and so by definition the two must be equal. $\square$

Lemma 1.2.10. The following are equivalent:

(i) G is orbitally sound, i.e. any isolated orbital closed subgroup H of G is normal.

(ii) Any orbital closed subgroup K of G contains a subgroup N of finite index in K which is normal in G.

Proof.

$\boxed{\text{(i)} \Rightarrow \text{(ii)}}$ Let K be an orbital closed subgroup of G. By Lemma 1.2.8(i), $\mathrm{i}_G(K)$ is an isolated orbital closed subgroup of G, and so (by assumption) is normal in G. Therefore, as it contains K as a subgroup of finite index (by Proposition 1.2.7), it must contain each conjugate K^g (for any $g \in G$) as a subgroup of finite index. But as K is G-orbital, it only has finitely many G-conjugates, and so their intersection K° still has finite index in $\mathrm{i}_G(K)$ and hence also in K, and K° is normal in G by construction.

$\boxed{\text{(ii)} \Rightarrow \text{(i)}}$ Let H be an isolated orbital closed subgroup of G, and write H° for the largest normal subgroup of G contained in H, which by (ii) must have finite index in H. Now clearly $H \leq \mathrm{i}_G(H^\circ)$ by definition of $\mathrm{i}_G(H^\circ)$, but also $\mathrm{i}_G(H^\circ) \leq H$ as H is isolated and contains H°. So H is the G-isolator of a normal subgroup, and so by Lemma 1.2.8(i), H is also normal in G. $\square$

1.3 p-valuations

Recall [13, III, 2.1.2] that a *p-valuation* of a group G is a function

$$\omega : G \to \mathbb{R} \cup \{\infty\}$$

satisfying the following properties:

- $\omega(x) = \infty$ if and only if $x = 1$,
- $\omega(x) > (p-1)^{-1}$,
- $\omega(x^{-1}y) \geq \inf\{\omega(x), \omega(y)\}$,
- $\omega([x, y]) \geq \omega(x) + \omega(y)$,
- $\omega(x^p) = \omega(x) + 1$,

for all $x, y \in G$. The group G, when endowed with the p-valuation ω, is called *p-valued*. On the other hand, a group G is called *p-valuable* [13, III, 3.1.6] if there exists a p-valuation ω of G with respect to which G is *complete* of *finite rank*. We will usually carefully distinguish between the two, as we will be considering more than one p-valuation on p-valuable groups in §5.

Definition 1.3.1. Recall from [4, 4.2] that an *ordered basis* for a p-valuable group G (with p-valuation ω) 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 $\mathbb{Z}_p$.

As in [4], we will often write

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

as shorthand, where $\lambda = (\lambda_1, \dots, \lambda_e) \in \mathbb{Z}_p^e$.

We recall a property of ordered bases.

Lemma 1.3.2. Let G 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 and B_G is an ordered basis for G.

Proof. This follows from [4, proof of Lemma 8.5(a)]. □

Remark. It may be helpful to think of this as follows:

$$B_G = \{ \underbrace{x_1, \dots, x_r}_{B_{G/N}}, \underbrace{x_{r+1}, \dots, x_s}_{B_N} \},$$

where $B_{G/N} = B_G \setminus B_N$ can in fact be taken to be any preimage in G of any ordered basis for G/N.

Let G be a p-valuable group with p-valuation ω. Then we may form an *associated graded group* $\mathrm{gr}_\omega G$ as follows. Write

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

and define

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

Each element $1 \neq x \in G$ has a *principal symbol*

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

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

1.4 Completed group rings

Definition 1.4.1. [8, Introduction] Let G be a profinite group and k a commutative *pseudocompact* ring (e.g. a commutative profinite ring). Then the completed group ring kG is defined to be

$$kG = \varprojlim_N k[G/N],$$

where the inverse limit ranges over all open normal subgroups N of G, and $k[G/N]$ denotes the usual group ring of the (finite) group G/N over k.

Remark. When it helps to reduce ambiguity, we will write kG as $k[[G]]$.

Recall from [18, 1.5.2] that, for any finite group F, there is a natural embedding of groups $i_F : F \to (k[F])^\times$. By taking the inverse limit of the maps $\{i_{G/N}\}$, we get a continuous embedding $i : G \to (kG)^\times$.

Lemma 1.4.2 (Universal property of completed group rings)**.** Let G be a profinite group and k a commutative pseudocompact ring. Then the completed group ring kG satisfies the following universal property: given any pseudocompact k-algebra R and any continuous group homomorphism $f : G \to R^\times$, there is a unique homomorphism $f^* : kG \to R$ of pseudocompact k-algebras satisfying $f^* \circ i = f$. (Here, $(kG)^\times$ and $R^\times$ are naturally viewed as subsets of kG and R respectively.)

Proof. Let $f : G \to R^\times$ be a continuous group homomorphism, and let I be an open ideal of R which is a neighbourhood of zero. Then $(I+1)\cap R^\times$ must be open in $R^\times$, and so its preimage $I^\dagger := f^{-1}((I+1)\cap R)$ must be open in G. Thus the map f descends to a homomorphism of (abstract) groups $f_I : G/I^\dagger \to R^\times/(I+1)\cap R^\times \to (R/I)^\times$, and $G/I^\dagger$ is finite.

Now, by the universal property for (usual) group rings [18, 1.5.2], we get a unique ring homomorphism $k[G/I^\dagger] \to R/I$ extending f_I, and hence a ring homomorphism $kG \to k[G/I^\dagger] \to R/I$ by definition. But as R is the inverse limit of these R/I, and the maps f_I are all clearly compatible by uniqueness, we get a continuous ring homomorphism $kG \to R$ extending f. $\square$

1.5 Minimal prime ideals

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

Lemma 1.5.1.

(i) Write $J := J(k\Delta^+)$. Then JkG is a two-sided ideal of kG contained in the prime radical of kG. Hence, denoting by $\overline{(\cdot)}$ images under the natural map $kG \to kG/JkG$, there is a one-to-one correspondence

$$\left\{\begin{matrix}\text{minimal prime}\\ \text{ideals of } kG\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{minimal prime}\\ \text{ideals of } \overline{kG}\end{matrix}\right\}.$$

(ii) Retain the notation of (i).

Let $X = \{e_1, \dots, e_r\}$ be a G-orbit of centrally primitive idempotents of $\overline{k\Delta^+}$, and write $f = e_1 + \cdots + e_r$. Then $\overline{M}_X := (1-f)\overline{kG}$ is a minimal prime ideal of $\overline{kG}$, hence (by (i)) its preimage M_X in kG is a minimal prime ideal in kG.

Conversely, let M be a minimal prime ideal of kG. Then there exists a G-orbit X of centrally primitive idempotents of $k\overline{\Delta^+}$ such that $M = M_X$.

This sets up a one-to-one correspondence

$$\left\{\begin{matrix}\text{minimal prime}\\ \text{ideals of } kG\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}G\text{-orbits of centrally}\\ \text{primitive idempotents of } \overline{k\Delta^+}\end{matrix}\right\}.$$

(iii) Given a centrally primitive idempotent $e \in \overline{k\Delta^+}$, there exists some $t > 0$ and some finite field extension k'/k with $e\cdot\overline{k\Delta^+} \cong M_t(k')$. Hence, if A is a k-algebra, we may identify the rings

$$e \cdot \overline{k\Delta^+} \underset{k}{\otimes} A \overset{=}{\longleftrightarrow} e \cdot \overline{k\Delta^+} \underset{k'}{\otimes} (k' \underset{k}{\otimes} A) \overset{=}{\longleftrightarrow} M_t(k' \underset{k}{\otimes} A).$$

Proof.

(i) This follows from [3, 5.2].

(ii) This follows from [3, §5, in particular 5.7].

(iii) $e\cdot\overline{k\Delta^+}$ is a simple finite-dimensional k-algebra, so the isomorphism $e\cdot\overline{k\Delta^+} \cong M_t(k')$ follows from Wedderburn's theorem. The rest is a simple calculation. □

We will use this correspondence very often, so will immediately set up notation which we will use for the rest of this thesis.

Notation 1.5.2. If an ideal $I \lhd kG$ contains a minimal prime ideal, then it contains a *unique* minimal prime ideal, say M. Then, under the correspondence of Lemma 1.5.1(ii), we obtain a unique G-orbit X of centrally primitive idempotents of $\overline{k\Delta^+}$ corresponding to M.

Throughout this thesis, we will write

$$\mathrm{cpi}^{\overline{k\Delta^+}}(I) \quad (\text{or } \mathrm{cpi}^{\overline{k\Delta^+}}(M))$$

for this set X. Given a centrally primitive idempotent $e \in \mathrm{cpi}^{\overline{k\Delta^+}}(I)$, we will write $f = e|^G$ to mean

$$f = \sum_{g \in \mathbf{C}_G(e)\backslash G} e^g,$$

where $\mathbf{C}_G(e)\backslash G$ denotes the (finite) set of right cosets of $\mathbf{C}_G(e)$ in G. In other words, if we write $e = e_1$ and $X = \{e_1, \dots, e_r\}$, then $f = e|^G$ means $f = e_1 + \cdots + e_r$.

Throughout this thesis, when invoking Lemma 1.5.1, $\overline{(\cdot)}$ will always mean the quotient by JkG unless otherwise stated. Thus,

- $\overline{M} = (1-f)\overline{kG}$,
- $f \cdot \overline{kG} = \overline{kG}/\overline{M} \cong kG/M$,
- $f \cdot \overline{I} = \overline{I}/\overline{M} \cong I/M$, etc.

1.6 Faithfulness and control

Let G be a compact p-adic analytic group, and k a field of characteristic p.

Definition 1.6.1. Let P be a prime ideal of the ring R. We say that P is *controlled by* the subring S if $(P \cap S)R = P$. Following Roseblade [24, 1.1], if $R = kG$ and $S = kH$ for some closed normal subgroup H of G, we say P is *controlled by* H.

Definition 1.6.2. For any ideal I of kG, define also

$$I^\dagger = \{x \in G \,\big|\, x - 1 \in I\}.$$

This is the kernel of the natural group homomorphism $G \to (kG/I)^\times$, and so is a normal subgroup of G. If $I^\dagger = 1$, we say that I is a *faithful* ideal; if $I^\dagger$ is finite, we say that I is *almost faithful*.

The next two lemmas are technical results about controller subgroups: see the remarks at the start of section 3.2 for the big picture.

Lemma 1.6.3. Suppose now that k is finite. Let P be an ideal of kG containing a prime ideal, and write

$$e = \mathrm{cpi}^{\overline{k\Delta^+}}(P), f = e|^G$$

as in Notation 1.5.2. Let H be any closed subgroup of G containing Δ^+. Then the following are equivalent:

- $(P \cap kH)kG = P$,
- $(\overline{P} \cap \overline{kH})\overline{kG} = \overline{P}$,
- $(f \cdot \overline{P} \cap f \cdot \overline{kH})f \cdot \overline{kG} = f \cdot \overline{P}$.

Proof. Firstly, $JkG \subseteq P$ by Lemma 1.5.1(i), and so by the modular law we have

$$(P \cap kH) + JkG = P \cap (kH + JkG)$$

from which we can deduce

$$\overline{P \cap kH} = \overline{P} \cap \overline{kH},$$

and so

$$\overline{(P \cap kH)kG} = (\overline{P} \cap \overline{kH})\overline{kG}.$$

Conversely, the preimage in kG of $\overline{(P \cap kH)kG}$ is $(P \cap kH)kG + JkG$, but this is just $(P \cap kH)kG$ as $J \subseteq P \cap kH$.

Secondly, $(1-f)\overline{kG} \subseteq \overline{P}$, and so just as above we may deduce by the modular law

$$f \cdot ((\overline{P} \cap \overline{kH})\overline{kG}) = (f \cdot \overline{P} \cap f \cdot \overline{kH})f \cdot \overline{kG}.$$

Similarly, $1 - f \in \overline{P} \cap \overline{kH}$, so the preimage in $\overline{kG}$ of $(f \cdot \overline{P} \cap f \cdot \overline{kH})f \cdot \overline{kG}$ is $(\overline{P} \cap \overline{kH})\overline{kG}$. $\square$

In order to retrieve information from Lemma 1.5.1(iii), we need a matrix control lemma:

Lemma 1.6.4. Let R be a ring, I an ideal of R, and S a subring of R. Let t be a positive integer. Then the following are equivalent:

(i) $(I \cap S)R = I$

(ii) $(M_t(I) \cap M_t(S))M_t(R) = M_t(I)$

Proof.

$\boxed{\text{(i)} \Rightarrow \text{(ii)}}$ Identify R, S and I with their images under the diagonal embedding $R \hookrightarrow M_t(R)$. It is clear that

$$I \cdot M_t(R) \subseteq M_t(I),$$

and conversely if $a_{kl} \in I$ for all $1 \leq k, l \leq t$ then

$$(a_{ij})_{i,j} = \sum_{k,l} a_{kl} E_{kl}$$

where $E_{kl} \in M_t(R)$ is the elementary matrix with (i, j)-entry $\delta_{ik}\delta_{jl}$. So we see that $I \cdot M_t(R) = M_t(I)$. But clearly

$$\begin{aligned} M_t(I) = I \cdot M_t(R) &= (I \cap S)R \cdot M_t(R) \\ &= (I \cap S)M_t(R) \\ &\subseteq (M_t(I) \cap M_t(S))M_t(R) \\ &\subseteq M_t(I), \end{aligned}$$

and so these are all equal.

$\boxed{\text{(ii)} \Rightarrow \text{(i)}}$ Write $d : R \to M_t(R)$ for the natural diagonal map $r \mapsto rI$, where I is the identity element of $M_t(R)$. We will show that $(M_t(I) \cap M_t(S))M_t(R) = M_t((I \cap S)R)$.

Then, by intersecting both sides of the equality $M_t((I \cap S)R) = M_t(I)$ with the subring $d(R)$, which we may identify with R, we see that it implies $(I \cap S)R = I$.

First, it is clear by definition that $M_t(I) \cap M_t(S) = M_t(I \cap S)$.

Next, in order to show that $M_t((I \cap S)R) = M_t(I \cap S)d(R)$, we note simply that, for any $r \in R$ and elementary matrix E_{ij} as above, we have $rE_{ij} = E_{ij}d(r)$. So, given some $x \in M_t((I \cap S)R)$, we may write

$$x = \sum_{i,j=1}^{t} x_{ij} E_{ij},$$

with each $x_{ij} \in (I \cap S)R$, so that

$$x_{ij} = \sum_{k=1}^{n_{ij}} y_{ijk} r_{ijk},$$

with each $y_{ijk} \in I \cap S$, each $r \in R$ and each n_{ij} some positive integer. Now, reordering the factors of each product as above, we see that

$$x = \sum_{i,j,k} (y_{ijk} E_{ij}) d(r_{ijk})$$

is clearly an element of $M_t(I \cap S)d(R)$; the converse is similar.

Finally, the inclusion $M_t(I \cap S)d(R) \subseteq M_t(I \cap S)M_t(R)$ is trivial; and the reverse inclusion is proved using a similar trick to the above, i.e. any element $x \in M_t(R)$ can be written as

$$x = \sum_{i,j=1}^{t} y_{ij} E_{ij} = \sum_{i,j=1}^{t} E_{ij} d(y_{ij})$$

for some $y_{ij} \in R$, and $M_t(I \cap S)E_{ij} \subseteq M_t(I \cap S)$. This establishes the equality. $\square$

Finally, we recall some basic properties of Morita equivalence:

Lemma 1.6.5. If R and S are Morita equivalent rings, then there is an order-preserving one-to-one correspondence between the ideals of R and the ideals of S, and this correspondence preserves primality. R is Morita equivalent to $M_t(R)$ for any positive integer t.

Proof. This is [18, 3.5.5, 3.5.9]. □

1.7 Crossed products

Definition 1.7.1. Let A and G be groups. Suppose we have a function *of sets*

$$\sigma : G \to \mathrm{Aut}(A)$$

– that is, G "acts on" A, but this action does *not* necessarily respect the group structure of G. (We will write the image of $a \in A$ under the automorphism $\sigma(g)$ as $a^{\sigma(g)}$.) Let $\alpha : G \times G \to A$ be a function *of sets.*

If, for all $x, y, z \in G$, we have

$$\alpha(xy, z)\alpha(x, y)^{\sigma(z)} = \alpha(x, yz)\alpha(y, z), \tag{1.7.1}$$

then α is a *2-cocycle (for the action of G on A*, or *with respect to σ).* We will write the set of such functions α as

$$Z^2_\sigma(G, A).$$

Let G be a finite group, R a ring, and $S = R{*}G$ a fixed crossed product. Recall [22, §1] that this means that:

- S is a free R-module on a generating set $\overline{G} \subseteq S$, where $|\overline{G}| = |G|$, and we shall write its elements as $\overline{g}$ for $g \in G$;

- multiplication in S is given by

$$r\overline{g} = \overline{g}r^{\sigma(g)} \qquad \text{for all } r \in R, g \in G,$$

$$\overline{g}\overline{h} = \overline{gh}\tau(g,h) \qquad \text{for all } g, h \in G,$$

where

$$\sigma : G \to \mathrm{Aut}(R), \qquad \text{the } \textit{action},$$

$$\tau : G \times G \to R^{\times}, \qquad \text{the } \textit{twisting},$$

are two functions *of sets* satisfying

$$\sigma(x)\sigma(y) = \sigma(xy)\eta(x,y) \tag{1.7.2}$$

$$\tau(xy,z)\tau(x,y)^{\sigma(z)} = \tau(x,yz)\tau(y,z), \tag{1.7.3}$$

where $\eta(x,y)$ is the automorphism of R given by conjugation (on the right) by $\tau(x,y)$.

Equation (1.7.3) says that τ is a 2-cocycle for σ with values in $R^{\times}$, i.e. $\tau \in Z^2_{\sigma}(G, R^{\times})$.

Notation 1.7.2. We will often need to write this structure explicitly as

$$S = R \underset{\langle \sigma, \tau \rangle}{*} G.$$

Chapter 2

The structure of nilpotent-by-finite, orbitally sound G

2.1 Orbital soundness and the Roseblade subgroup $\mathrm{nio}(G)$

We begin this section by remarking that "orbitally sound" is not too restrictive a condition. Recall:

Lemma 2.1.1. Let G be a p-valuable group. Then G is orbitally sound. $\square$

Proof. This is [4, Proposition 5.9], after remarking that the definitions of "orbitally sound" given in Definition 1.2.4 and in [4, 5.8] are equivalent by Lemma 1.2.10. $\square$

The following two lemmas will allow us to find a large class of orbitally sound groups.

For the next lemma, fix the following notation. Let G be a compact p-adic analytic group, and consider its $\mathbb{Q}_p$-Iwasawa algebra $\mathbb{Q}_pG := (\mathbb{Z}_pG)\left[\frac{1}{p}\right]$. Write I for its augmentation ideal

$$I = \ker(\mathbb{Q}_pG \to \mathbb{Q}_p).$$

Now, I^k is generated over $\mathbb{Q}_pG$ by $\{(x_1 - 1)\dots(x_k - 1) \,|\, x_i \in G\}$. Now it is clear that G acts *unipotently* on the series

$$\mathbb{Q}_pG \geq I \geq I^2 \geq I^3 \geq \dots,$$

i.e. for all $g \in G$, we have $(g-1)\mathbb{Q}_pG \subseteq I$ and $(g-1)I^k \subseteq I^{k+1}$.

Write also $\mathcal{U}_n$ for the subgroup of $GL_n(\mathbb{Q}_p)$ consisting of upper triangular unipotent matrices.

Lemma 2.1.2. Let G be a compact p-adic analytic group. Write

$$D_k = \ker(G \to (\mathbb{Q}_pG/I^k)^\times),$$

the *k-th rational dimension subgroup* of G, for all $k \geq 1$. Then the D_k are a descending chain of isolated orbital closed normal subgroups of G. This chain eventually stabilises: that is, there exists some t such that $D_n = D_t$ for all $n \geq t$.

Furthermore, if G is torsion-free and nilpotent, then $D_t = 1$, and G is isomorphic to a closed subgroup of $\mathcal{U}_m$ for some m.

Proof. By definition, it is clear that the D_k are closed normal (hence orbital) subgroups of G; to show that they are isolated orbital, we will show that each G/D_k is torsion-free.

Fix k. Consider the series of finite-dimensional $\mathbb{Q}_p$-vector spaces

$$\mathbb{Q}_pG/I^k > I/I^k > I^2/I^k > I^3/I^k > \dots > I^k/I^k,$$

and choose a basis for $\mathbb{Q}_pG/I^k$ which is filtered relative to this series: i.e. by repeatedly extending a basis for I^r/I^k to a basis for I^{r-1}/I^k for $r = k, k-1, \dots, 1$, we get a basis

$$B = \{e_1, \dots, e_l\}$$

and integers

$$0 = n_k < n_{k-1} < n_{k-2} < \dots < n_1 < n_0 = l$$

with the property that $\{e_1, \dots, e_{n_r}\}$ is a basis for I^r/I^k for each $0 \leq r \leq k$ (where we write $I^0 = \mathbb{Q}_pG$ for convenience).

As G acts *unipotently* (by left multiplication) on $\mathbb{Q}_pG/I^k$, and by definition of the basis B, we see that with respect to B, each $g \in G$ acts by a unipotent upper-triangular matrix, i.e. we get a continuous group homomorphism $G \to \mathcal{U}_l$. Now D_k is just the kernel of this map; but $\mathcal{U}_l$ is torsion-free, so D_k must be isolated.

Recall the *dimension* $\dim H$ of a pro-p group H of finite rank from [9, 4.7]. As G has finite rank, it also has finite dimension [9, 3.11, 3.12], and we must have $\dim D_i \geq \dim D_{i+1}$ for all i by [9, 4.8]. But if $\dim D_i = \dim D_{i+1}$, then D_i/D_{i+1} is a p-valued group (as D_{i+1} is isolated) of dimension 0 (again by [9, 4.8]), and so must be trivial. Hence the sequence (D_i) stabilises after at most $t := 1 + \dim G$ terms, and so

$$D_t = \bigcap_{n \geq 1} D_n.$$

Now suppose that G is nilpotent. Then, by [3, Theorem A], it follows that I is localisable. Let $R = (\mathbb{Q}_pG)_I$ be its localisation, and $J(R) = \mathfrak{m}$ its unique maximal ideal: then the ideal

$$A = \bigcap_{n \geq 1} \mathfrak{m}^n$$

satisfies $A = \mathfrak{m}A$, so by Nakayama's lemma [18, 0.3.10], we must have $A = 0$. This implies that

$$\bigcap_{n\geq 1} I^n \subseteq \ker(\mathbb{Q}_pG \to R).$$

Assuming further that G is torsion-free, we see that $\mathbb{Q}_pG$ is a domain [20, Theorem 1], and so the localisation map $\mathbb{Q}_pG \to R$ is injective. Hence $\bigcap_{n\geq 1} I^n = 0$, and so

$$D_t = \bigcap_{n\geq 1} D_n = \left(\bigcap_{n\geq 1}(I^n + 1) \cap G\right) \subseteq \left(\bigcap_{n\geq 1} I^n\right) + 1 = 1.$$

Now the representation $G \to \mathrm{Aut}(\mathbb{Q}_pG/I^t) \cong GL_m(\mathbb{Q}_p)$ is faithful and has image in $\mathcal{U}_m$. □

Lemma 2.1.3. Let G be a (topologically) finitely generated nilpotent pro-p group. Then G is p-valuable if and only if it is torsion-free.

Proof. If G is torsion-free, then Lemma 2.1.2 gives an injective map $G \to \mathcal{U}_m$. Now, as G is topologically finitely generated, its image in $\mathcal{U}_m$ must lie inside the set $\frac{1}{p^t}M_m(\mathbb{Z}_p) \cap \mathcal{U}_m$ for some t. Hence, by conjugating by the diagonal element

$$\mathrm{diag}(p, p^2, \ldots, p^m)^{t+\varepsilon} \in GL_m(\mathbb{Q}_p),$$

where

$$\varepsilon = \begin{cases} 1 & p > 2, \\ 2 & p = 2, \end{cases}$$

we see that G is isomorphic to a subgroup of

$$\Gamma_\varepsilon = \left\{\gamma \in GL_m(\mathbb{Z}_p) \,\middle|\, \gamma \equiv 1 (\mathrm{mod}\ p^\varepsilon)\right\},$$

the εth congruence subgroup of $GL_m(\mathbb{Z}_p)$, which is uniform (and hence p-valuable) by [9, Theorem 5.2].

The reverse implication is clear from the definition of a p-valuation [13, III, 2.1.2]. $\square$

Now we have found a large class of orbitally sound compact p-adic analytic groups.

Corollary 2.1.4. If G is a finite-by-nilpotent compact p-adic analytic group, then it is orbitally sound.

Proof. $\overline{G} := G/\Delta^+$ must be a nilpotent compact p-adic analytic group with $\Delta^+(\overline{G}) = 1$, and so $\overline{G}$ is torsion-free by [23, 5.2.7]. Now Lemma 2.1.3 shows that $\overline{G}$ is p-valuable, and from Lemma 2.1.1 we may deduce that $\overline{G}$ is orbitally sound. But now Lemma 1.2.5(iii) implies that G is orbitally sound. $\square$

Remark. It is well known that finite-by-nilpotent implies nilpotent-by-finite, but not conversely. Not all nilpotent-by-finite compact p-adic analytic groups are orbitally sound: indeed, the wreath product

$$G = \mathbb{Z}_p \wr C_2 = (\mathbb{Z}_p \times \mathbb{Z}_p) \rtimes C_2$$

is *abelian*-by-finite, and the infinite procyclic subgroup $H = \mathbb{Z}_p \times \{0\}$ is orbital, but the largest G-normal subgroup contained in H is the trivial subgroup.

We can now define the Roseblade subgroup.

Definition 2.1.5. As in Roseblade [24, 1.3], write $\mathrm{nio}(G)$ for the closed subgroup of G defined by

$$\mathrm{nio}(G) = \bigcap_H \mathbf{N}_G(H),$$

where the intersection ranges over the isolated orbital closed subgroups H of G.

Theorem 2.1.6. Let G be a compact p-adic analytic group.

(i) An orbitally sound open normal subgroup $N \lhd G$ normalises every closed isolated orbital subgroup $H \leq G$.

(ii) $\mathrm{nio}(G)$ is an orbitally sound open characteristic subgroup of G.

Proof.

(i) Since H is isolated orbital in G, we must have that $H \cap N$ is isolated orbital (and hence normal) in N. However, it follows from Lemma 1.2.9 that $H = \mathrm{i}_G(H \cap N)$. Hence H is generated by all the (finitely many) closed orbital subgroups $L_1, \dots, L_k$ of G containing $H \cap N$ as a subgroup of finite index. Conjugation by $n \in N$ permutes these L_i, and so fixes H.

(ii) Let N be a complete p-valued open normal subgroup of G (e.g. by [9, 8.34]). Then Lemma 2.1.1 shows that N is orbitally sound, and hence by (i) N normalises all closed isolated orbital subgroups of G. So, by definition, $N \leq \mathrm{nio}(G)$, and so $[G : \mathrm{nio}(G)] \leq [G : N] < \infty$. Therefore $\mathrm{nio}(G)$ is open in G as required. But by definition, $\mathrm{nio}(G)$ is the largest subgroup that normalises all isolated orbital subgroups of G, so by the correspondence of Lemma 1.2.9 and Lemma 1.2.8(i), it normalises all isolated orbital subgroups of $\mathrm{nio}(G)$, i.e. it is orbitally sound. $\square$

Proof of Theorem C(i). This follows from Definition 2.1.5 and Theorem 2.1.6(i), (ii). $\square$

2.2 Two worked examples

Example 2.2.1. Let $p \neq 2$, and fix some $\lambda \in \mathbb{Z}_p$. Set

$$H = H_\lambda = \overline{\left\langle \begin{array}{c|c} a, b, c, d; & [a,b] = 1, \quad [a,c] = y, \quad [a,d] = z, \\ y, z \text{ central} & [b,c] = z, \quad [b,d] = y^\lambda, [c,d] = 1 \end{array} \right\rangle},$$

a compact p-adic analytic group which is nilpotent of nilpotency class 2. Write

$$Z = Z(H) = \overline{\langle y, z \rangle}$$

for its centre. Then set

$$G = H \rtimes \langle \alpha | \alpha^2 \rangle,$$

where α acts on H by

$$a^\alpha = a^{-1}z, \quad b^\alpha = b^{-1}, \quad c^\alpha = c^{-1}, \quad d^\alpha = d^{-1},$$
$$y^\alpha = y, \qquad z^\alpha = z.$$

Let $h = a^i b^j c^k d^l y^m z^n$ be an element of H (with $i, j, k, l, m, n \in \mathbb{Z}_p$), and consider the map $C_h : H/Z \to Z$ given by $x \mapsto [h, x]$. As H/Z and Z are both abelian, we may consider them as free $\mathbb{Z}_p$-modules $(H/Z)_+$ and Z_+ (the subscript "+" shows that we are now writing them *additively*), with bases given by the generators as above:

$$(H/Z)_+ = \mathbb{Z}_p\mathbf{a} \oplus \mathbb{Z}_p\mathbf{b} \oplus \mathbb{Z}_p\mathbf{c} \oplus \mathbb{Z}_p\mathbf{d}, \qquad Z_+ = \mathbb{Z}_p\mathbf{y} \oplus \mathbb{Z}_p\mathbf{z}.$$

Now, C_h is a $\mathbb{Z}_p$-linear map:

- given $\mathbf{u}, \mathbf{v} \in (H/Z)_+$, we have $C_h(\mathbf{u} + \mathbf{v}) = C_h(\mathbf{u}) + C_h(\mathbf{v})$, by [9, 0.1].
- Given $\mathbf{u} \in (H/Z)_+$ and a positive integer μ, we have $C_h(\mu\mathbf{u}) = \mu C_h(\mathbf{u})$, by [9, 0.2]; hence this equality holds for all $\mu \in \mathbb{Z}_p$ by continuity,

and so, with respect to the bases for $(H/Z)_+$ and Z_+ given above, we can write the matrix corresponding to C_h as

$$M_h = \begin{pmatrix} -k & -\lambda l & i & \lambda j \\ -l & -k & j & i \end{pmatrix}.$$

When this matrix has rank 2, we know that it is surjective considered as a linear map

$$(H/Z)_+ \underset{\mathbb{Z}_p}{\otimes} \mathbb{Q}_p \to Z_+ \underset{\mathbb{Z}_p}{\otimes} \mathbb{Q}_p.$$

In other words, if N is a normal subgroup of H containing h, then it must contain all of $C_h(H/Z) = [h, H]$, and hence contains an *open* subgroup of Z. However, if there exists some h such that M_h has rank ≤ 1, then $[h, H]$ generates a subgroup of Z with ($\mathbb{Z}_p$-)rank less than that of Z, so in particular it is a subgroup of infinite index.

So we will write down the six 2×2 minors of M_h, and use this observation to answer the question of whether G is orbitally sound:

$$\begin{cases} m_1 = k^2 - \lambda l^2 \\ m_2 = i^2 - \lambda j^2 \\ m_3 = il - jk \\ m_4 = \lambda jk - \lambda il \\ m_5 = ik - \lambda jl \\ m_6 = \lambda jl - ik. \end{cases}$$

Now we split this question into two cases.

Case (a): λ is not a square in $\mathbb{Z}_p$. Recall that $i, j, k, l \in \mathbb{Z}_p$; hence, in this case, we see immediately that, whenever $m_1 = m_2 = 0$, we have $i = j = k = l = 0$: that is, for any non-central $h \in H$, we deduce that $[h, H]$ generates an open subgroup of Z.

We claim that, in this case, G is orbitally sound.

Let N be any orbital subgroup of G. In order to show that G is orbitally sound, we will show that N contains an open subgroup N' which is normal in G, and then invoke Lemma 1.2.10. First, note that $N \cap H$ is an open subgroup of N (as H is an open subgroup of G), and that the normal core K in H of $N \cap H$ is an open subgroup of $N \cap H$ (as $N \cap H$ is orbital, and H is orbitally sound by Corollary 2.1.4) which is normal in H by construction. Now $\mathrm{core}_G(K) = K \cap K^\alpha$ is a normal subgroup of G, and we claim that it is open in K, and hence open in N.

Clearly, if $K \leq Z$, then $k^\alpha = k$ for all $k \in K$ (as α has been defined to act trivially on the generators of Z), and so $K \cap K^\alpha = K$, so we are done in this case. Otherwise, K contains some element $h \in H \setminus Z$, and so contains all of $[h, K]$ (as K is normal in H). By the calculations above, M_h has maximal rank, and therefore $[h, K]$ generates an *open* subgroup of Z, so that $[KZ : K] < \infty$.

This allows us to assume, without loss of generality, that K contains all of Z. But then

$$[K : K \cap K^\alpha] = [K/Z : (K/Z) \cap (K/Z)^\alpha],$$

and as $(hZ)^\alpha = (hZ)^{-1}$ for all $h \in H$, we see that $(K/Z)^\alpha = K/Z$. This concludes the proof that G is orbitally sound.

Case (b): $\lambda = \mu^2$ for some $\mu \in \mathbb{Z}_p$. Then taking $i = \mu, j = 1, k = l = 0$ satisfies $m_1 = \cdots = m_6 = 0$: that is, when $h = a^\mu b$, we deduce that $C_h(H)$ is not an open subgroup of $Z \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$ (indeed, we can calculate it easily to be $\overline{\langle y^\mu z \rangle} \cong \mathbb{Z}_p$).

We claim that, in this case, G is *not* orbitally sound.

Let $N = \overline{\langle h \rangle}^H$, the normal closure in H of the procyclic subgroup generated by h. (This must be orbital in G, as it is orbital in a finite-index subgroup of G.) By the above calculation, we must have

$$N = \overline{\langle h, y^\mu z \rangle},$$

and hence

$$\begin{aligned} N^\alpha &= \overline{\langle h^\alpha, (y^\mu z)^\alpha \rangle} \\ &= \overline{\langle h^{-1} z^\mu, y^\mu z \rangle}. \end{aligned}$$

Therefore

$$\begin{aligned} N \cdot N^\alpha &= \overline{\langle h, y^\mu z, h^\alpha, (y^\mu z)^\alpha \rangle} \\ &= \overline{\langle h, y^\mu z, z^\mu \rangle}, \end{aligned}$$

a free abelian pro-p group of rank 3. So we see that $N \cap N^\alpha$ has rank 1 as a $\mathbb{Z}_p$-mobule, and therefore must have infinite index in N.

Example 2.2.2. A modification of the previous example: if the action of the semidirect product is chosen well, orbital soundness can be made independent of the parameter λ.

Fix an element $\lambda \in \mathbb{Z}_p$, and let $H = H_\lambda$ and $G = H \rtimes \langle \alpha | \alpha^2 \rangle$ as in 2.2.1, with all the same notation, but now define the action of α as follows:

$$\begin{gathered} a^\alpha = a^{-1}, \quad b^\alpha = b^{-1}, \quad c^\alpha = c^{-1}, \quad d^\alpha = d^{-1}, \\ y^\alpha = y, \qquad z^\alpha = z. \end{gathered}$$

When λ is not a square in $\mathbb{Z}_p$, G is orbitally sound as above. So suppose λ is a square in $\mathbb{Z}_p$. Then writing $\lambda = \mu^2$ for one of its square roots, we have as before

$$\begin{aligned} m_1 = \cdots = m_6 = 0 &\Leftrightarrow i = \mu j,\ k = \mu l \\ &\Leftrightarrow h = a^{\mu j} b^j c^{\mu l} d^l \quad \text{modulo central elements,} \end{aligned}$$

and it is again easy to see that, for this choice of h,

$$\begin{aligned}[h, H] &= \overline{\langle y^{\mu l} z^l, y^{\mu j} z^j \rangle} \\ &= \overline{\langle (y^\mu z)^{p^r} \rangle}\end{aligned}$$

for some r with $p^r = \mathrm{hcf}(j, l)$. Then take $N = \overline{\langle h \rangle}^H = \overline{\langle h, (y^\mu z)^{p^r} \rangle}$. In this case, a calculation shows that

$$h^\alpha = h^{-1}(y^\mu z)^{2\mu j l},$$

and clearly we have $p^r | 2\mu j l$, so that $N^\alpha = N$.

It is now clear that G is orbitally sound. Indeed, let N be a normal subgroup of H; then either $N \leq Z(H)$ (and is therefore normal in G), or N contains an element $h \in H$ with $\mathrm{rank}(M_h) = 2$ (which is dealt with in Example 2.2.1, case (a)), or N is a product of subgroups of the form $\overline{\langle h \rangle}$, for $h \in H$ of the form given in the previous paragraph, and in this case we have just shown that N is normal in G.

2.3 Isolators and p-saturations

Let G be a p-valuable group, and fix a p-valuation ω on G, so that G is complete p-valued of finite rank. Recall the definition of the *p-saturation* $\mathrm{Sat}\, G$ of G (with respect to ω) from [13, IV, 3.3.1.1]: this is again a complete p-valued group of finite rank, and there is a natural isometry identifying G with an open subgroup of $\mathrm{Sat}\, G$ [13, IV, 3.3.2.1]. We will prove a few basic facts about p-saturations.

Firstly, we will prove a basic relationship between isolators and p-saturations.

Lemma 2.3.1. Let G be a complete p-valued group of finite rank, and let H be a closed normal (and hence orbital) subgroup of G. Then $\mathrm{i}_G(H) = \mathrm{Sat}\, H \cap G$ (considered as subgroups of $\mathrm{Sat}\, G$).

Proof. $[\mathrm{Sat}\, H : H] < \infty$ by [13, IV, 3.4.1], and $\mathrm{Sat}\, H$ is a closed normal subgroup of $\mathrm{Sat}\, G$ by [13, IV, 3.3.3], so $S := \mathrm{Sat}\, H \cap G$ is a closed normal (and hence orbital) subgroup of G, and contains H as a subgroup of finite index. Hence, by Definition 1.2.6, S is contained in $\mathrm{i}_G(H)$.

To show the reverse inclusion, we will consider the group $\mathrm{i}_G(H)/S$, which is a finite subgroup of G/S (as it is a quotient of $\mathrm{i}_G(H)/H$, which is finite by Proposition 1.2.7). But G/S is isomorphic to $G\mathrm{Sat}\, H/\mathrm{Sat}\, H$, a subgroup of the torsion-free group $\mathrm{Sat}\, G/\mathrm{Sat}\, H$ (see [13, IV, 3.4.2] or [13, III, 3.3.2.4]). In particular, G/S has no non-trivial finite subgroups, so we must have $\mathrm{i}_G(H) = S$. $\square$

Remark. Of course, $\mathrm{i}_G(H)$ is independent of the choice of ω.

Lemma 2.3.2. Let G be a complete p-valued group of finite rank, which we again identify with an open subgroup of its p-saturation S. Suppose S' is a p-saturated closed normal subgroup of S, and set $G' = S' \cap G$. Then there is a natural isometry $S/S' \cong \mathrm{Sat}\,(G/G')$.

Proof. We will show that S/S' satisfies the universal property for $\mathrm{Sat}\,(G/G')$ [13, IV, 3.3.2.4]. Clearly we may regard $G/G' \cong GS'/S'$ as a subgroup of S/S'. Note also that S/S' is p-saturated, by [13, III, 3.3.2.4]. Also, as G' is open in S' and S' is p-saturated, we have that $S' = \mathrm{Sat}\, G'$.

Let H be an arbitrary p-saturated group and $\varphi : G/G' \to H$ a homomorphism of p-valued groups. We must first construct a map $\psi : S/S' \to H$. To do this, we first compose φ with the natural surjection $G \to G/G'$ to get a map $\alpha : G \to H$, which we may then extend uniquely to a map $\beta : S \to H$ using the universal property of $S = \mathrm{Sat}\, G$, so that $\alpha = \beta|_G$ and the following diagram commutes.

$$\begin{tikzcd}
G \arrow[r, two heads] \arrow[rr, bend left, "\alpha"] \arrow[d, hook] & G/G' \arrow[r, "\varphi"'] & H \\
S \arrow[urr, bend right, "\beta"'] & &
\end{tikzcd}$$

Now we wish to show that β descends to a map $S/S' \to H$. To do this, we first study the restriction of α to G' and of β to S'. The following diagram commutes:

$$\begin{tikzcd}
G' \arrow[r, "\alpha|_{G'}"] \arrow[d, hook] & H \\
S' \arrow[ur, "\beta|_{S'}"'] &
\end{tikzcd}$$

and so, since $S' = \operatorname{Sat} G'$, $\beta|_{S'}$ must be the *unique* extension of $\alpha|_{G'}$ to a map $S' \to H$, as $S' = \operatorname{Sat} G'$. But α factors through G/G', i.e. $\alpha|_{G'}$ is the trivial homomorphism $G' \to H$, so it extends to the trivial homomorphism $S' \to H$. By uniqueness, we must have $S' \subseteq \ker \beta$. This shows that β induces a map $\psi : S/S' \to H$.

Finally, suppose $\varphi : G/G' \to H$ has two distinct extensions $\psi_1, \psi_2 : S/S' \to H$. Then we may compose them with the natural surjection $S \to S/S'$ to get two distinct maps $\beta_1, \beta_2 : S \to H$. Their restrictions $\alpha_1, \alpha_2 : G \to H$ to G must therefore also be distinct, for if not, then the map $\alpha_1 = \alpha_2 : G \to H$ has (at least) two distinct extensions to maps $S \to H$, contradicting the universal property of $S = \operatorname{Sat} G$. Finally, if α_1 and α_2 are distinct, then they descend to distinct maps $\varphi_1, \varphi_2 : G/G' \to H$, contradicting our assumption. So the extension of φ to ψ is unique. $\square$

Remark. Lemma 2.3.2 holds even if G does not have finite rank, and hence is only closed (not necessarily open) in its p-saturation S.

Definition 2.3.3. Let G be an arbitrary group. A *central series* for G is a sequence of subgroups

$$G = G_1 \rhd G_2 \rhd \cdots \rhd G_n = 1$$

with the property that $[G, G_i] \leq G_{i+1}$ for each i. (For the purposes of this definition, G_j is understood to mean 1 if $j > n$, and G if $j < 1$.)

We will say that a central series is *strongly* central if also $[G_i, G_j] \leq G_{i+j}$ for all i and j.

An *abelian series* for G a sequence of subgroups

$$G = G_1 \rhd G_2 \rhd \cdots \rhd G_n = 1$$

with the property that $[G_i, G_i] \leq G_{i+1}$ for each i.

When G is a topological group, we will insist further that all of the G_i should be *closed* subgroups of G.

Remark. We will be working with nilpotent p-valuable groups G. It will be useful for us to define the *isolated lower central series* of G, which will turn out to be the fastest descending central series of closed subgroups

$$G = G_1 \rhd G_2 \rhd \cdots \rhd G_r = 1$$

with the property that the successive quotients G_i/G_{i+1} are torsion-free (and hence p-valuable, by [13, IV, 3.4.2]). We will also prove that the isolated lower central series is a *strongly* central series. (We demonstrate an *isolated derived series* for soluble p-valued groups at the same time.)

Lemma 2.3.4. Let G be a complete p-valued group of finite rank, and $G_1 \geq G_2$ closed normal subgroups of G with G_1/G_2 an abelian pro-p group (which is not necessarily p-valued). Let $S_i = \operatorname{Sat} G_i$ for $i = 1, 2$. Then S_1/S_2 is abelian and torsion-free (and hence p-valued), and has the same rank as G_1/G_2 as a $\mathbb{Z}_p$-module.

Proof. As S_2 is p-saturated, S_1/S_2 is torsion-free, and so

$$G_1/(S_2 \cap G_1) \cong G_1S_2/S_2 \leq S_1/S_2$$

is torsion-free. G_1/G_2 maps onto $G_1/(S_2 \cap G_1)$ with finite kernel (by Lemma 2.3.1 and Proposition 1.2.7, and the assumption that G has finite rank), so $G_1/(S_2 \cap G_1)$ is abelian of the same $\mathbb{Z}_p$-rank as G_1/G_2. By Lemma 2.3.2, S_1/S_2 is the p-saturation of $G_1/(S_2 \cap G_1)$, so is still abelian of the same $\mathbb{Z}_p$-rank. □

Before proving the main result of this section, we first need a technical lemma.

Lemma 2.3.5. Let G be a complete p-valued group of finite rank, and let H and N be two orbital closed subgroups. Then, denoting by $\overline{(\cdot)}$ topological closure inside G, we have

$$[\mathrm{i}_G(H), \mathrm{i}_G(N)] \leq \mathrm{i}_G(\overline{[H,N]}).$$

Proof. Write $L := \mathrm{i}_G(\overline{[H,N]})$. This is normal in G, as G is orbitally sound (Lemma 2.1.1), and the quotient G/L is still p-valued as it is torsion-free [13, IV, 3.4.2].

Suppose first that $L = 1$, so that $[H,N] = 1$. Then, for any $h \in \mathrm{i}_G(H)$, there is some integer n such that $h^{p^n} \in H$, so that $[g, h^{p^n}] = 1$ for all $g \in N$. But this is the same as saying that $h^{p^n} = (h^g)^{p^n}$; and, as G is p-valued, [13, III, 2.1.4] implies that $h = h^g$. As g and h were arbitrary, we see that $[\mathrm{i}_G(H), N] = 1$. Repeat this argument for N to show that $[\mathrm{i}_G(H), \mathrm{i}_G(N)] = 1$.

If $L \neq 1$, we may pass to G/L. Write $\pi : G \to G/L$ for the natural surjection, so that

$$\pi\big([\mathrm{i}_G(H), \mathrm{i}_G(N)]\big) = [\pi(\mathrm{i}_G(H)), \pi(\mathrm{i}_G(N))]. \tag{2.3.1}$$

Now, $\pi(H)$ is a closed orbital subgroup of $\pi(G)$, and $\pi(\mathrm{i}_G(H))$ is a closed orbital subgroup of $\pi(G)$ containing $\pi(H)$ as an open subgroup, so that

$$\mathrm{i}_{\pi(G)}(\pi(H)) \geq \pi(\mathrm{i}_G(H)),$$

and similarly for N. Together with (2.3.1), this implies that

$$\pi\big([\mathrm{i}_G(H), \mathrm{i}_G(N)]\big) \leq [\mathrm{i}_{\pi(G)}(\pi(H)), \mathrm{i}_{\pi(G)}(\pi(N))].$$

But the right-hand side is now equal to $\pi(1)$, by the previous case, which shows that $[\mathrm{i}_G(H), \mathrm{i}_G(N)] \leq L$ as required. □

Corollary 2.3.6. Let G be a p-valuable group. Define two series:

$$G_i = \mathrm{i}_G(\overline{\gamma_i}), \text{ where } \begin{cases} \gamma_1 = G, \\ \gamma_{i+1} = [\gamma_i, G] \quad \text{for } i \geq 1; \end{cases}$$

$$G^{(i)} = \mathrm{i}_G(\overline{\mathcal{D}_i}), \text{ where } \begin{cases} \mathcal{D}_0 = G, \\ \mathcal{D}_{i+1} = [\mathcal{D}_i, \mathcal{D}_i] \quad \text{for } i \geq 0, \end{cases}$$

where the bars denote topological closure inside G. If G is nilpotent, then (G_i) is a strongly central series for G, i.e. a central series in which $[G_i, G_j] \leq G_{i+j}$. If G is soluble, then $(G^{(i)})$ is an abelian series for G. The quotients G_i/G_{i+1} and $G^{(i)}/G^{(i+1)}$ are torsion-free, and hence p-valuable.

Remark. We prove this using p-saturations, but the resulting closed subgroups G_i and $G^{(i)}$ are independent of the choice of p-valuation ω on G.

The series $(G^{(i)})$ above is a generalisation of the series studied in [19, proof of lemma 2.2.1], there called (G_i).

Proof. Fix a p-valuation ω on G throughout.

Firstly, we will show that (G_i) is an abelian series. The claim that $(G^{(i)})$ is an abelian series will follow by an identical argument.

The (abstract) lower central series (γ_i) is an abelian series for G as an abstract group (i.e. the subgroups γ_i are not necessarily closed in G), and so the series $(\overline{\gamma_i})$ is a series of *closed* normal subgroups of G, which is still an abelian series by continuity. (That is, γ_i/γ_{i+1} is central in G/γ_{i+1}, and hence $\gamma_i/\overline{\gamma_{i+1}}$ is central in $G/\overline{\gamma_{i+1}}$, and now by continuity we have that all of $\overline{\gamma_i}/\overline{\gamma_{i+1}}$ is central.) Now, applying Lemma 2.3.4 shows that $(\mathrm{Sat}\,\overline{\gamma_i})$ is also an abelian series; and by Lemma 2.3.1, we see that $G_i = \mathrm{Sat}\,\overline{\gamma_i} \cap G$ for each i, so that (G_i) is an abelian series.

Secondly, we address the claim that the quotients G_i/G_{i+1} are torsion-free and hence p-valuable: this follows from [13, III, 3.1.7.6 / IV, 3.4.2], as the G_{i+1} are isolated in G. The case of the quotients $G^{(i)}/G^{(i+1)}$ is again identical.

Thirdly, we must show that G_{i-1}/G_i is central in G/G_i. Certainly $\gamma_{i-1}G_i/G_i$ is central in G/G_i, because $\gamma_i \leq G_i$, and so

$$\overline{\gamma_{i-1}}G_i/G_i \leq Z(G/G_i)$$

by continuity. However, [4, lemma 8.4(a)] says that $Z(G/G_i)$ is isolated in G/G_i, so by taking (G/G_i)-isolators of both sides, we must have

$$\mathrm{i}_{G/G_i}\big(\overline{\gamma_{i-1}}G_i/G_i\big) \leq Z(G/G_i);$$

and the left-hand side is clearly equal to G_{i-1}/G_i by Lemma 1.2.5(i) and Definition 1.2.6.

Finally, note that

$$[\gamma_i, \gamma_j] \leq \gamma_{i+j}$$

by [23, 5.1.11(i)], and so by taking closures,

$$\overline{[\gamma_i, \gamma_j]} \leq \overline{\gamma_{i+j}}.$$

But $[\overline{\gamma_i}, \overline{\gamma_j}] \leq \overline{[\gamma_i, \gamma_j]}$, as the function $G \times G \to G$ given by $(a, b) \mapsto [a, b]$ is continuous.

Hence

$$[\overline{\gamma_i}, \overline{\gamma_j}] \leq \overline{\gamma_{i+j}},$$

which implies

$$\overline{[\overline{\gamma_i}, \overline{\gamma_j}]} \leq \overline{\gamma_{i+j}},$$

and so, by Lemma 2.3.5, we may take isolators to show that

$$[\mathrm{i}_G(\overline{\gamma_i}), \mathrm{i}_G(\overline{\gamma_j})] \leq \mathrm{i}_G\left(\overline{[\overline{\gamma_i}, \overline{\gamma_j}]}\right) \leq \mathrm{i}_G(\overline{\gamma_{i+j}}),$$

i.e. $[G_i, G_j] \leq G_{i+j}$. □

Definition 2.3.7. When G is a nilpotent (resp. soluble) p-valued group of finite rank, the series (G_i) (resp. $(G^{(i)})$) defined in Corollary 2.3.6 is the *isolated lower central series* (resp. *isolated derived series*) of G.

Proof of Theorem D(ii). The majority of this theorem follows from Corollary 2.3.6.

It remains only to prove that these descending series are the *unique fastest* such series, in an appropriate sense. We will state and prove this precisely for the case of the isolated lower central series of a nilpotent p-valuable group; the soluble case is very similar.

Let G be a nilpotent p-valuable group, and let

$$G = G_1 \rhd G_2 \rhd \cdots \rhd G_r = 1$$

be its isolated lower central series. Take also any central series

$$G = H_1 \rhd H_2 \rhd \cdots \rhd H_r \rhd \dots$$

for G of isolated orbital closed normal subgroups. We will show that $G_i \leq H_i$ for each i.

We proceed by induction. We clearly have $G_1 \leq H_1$; now suppose that, for some k, we have $G_i \leq H_i$ for all $i < k$. Now clearly

$$[G, G_{k-1}] \leq [G, H_{k-1}] \leq H_k;$$

as H_k is already closed and G-isolated, we may take the closure and G-isolator of the first and last terms of this inclusion to get

$$\mathrm{i}_G\left(\overline{[G, G_{k-1}]}\right) \leq H_k.$$

But the left-hand expression here clearly contains $\mathrm{i}_G(\overline{\gamma_k})$, which is just G_k. $\square$

2.4 The conjugation action of G

In this subsection, we will study how nilpotent-by-finite compact p-adic analytic groups G act by conjugation on certain torsion-free abelian and nilpotent subquotients. First, we slightly extend the term "orbitally sound".

Definition 2.4.1. Let G and H be profinite groups, and suppose G acts (continuously) on H. Then G permutes the closed subgroups of H. We say that the action of G on H is *orbitally sound* if, for any closed subgroup K of H with finite G-orbit, there exists an open subgroup K' of K which is normalised by G.

Recall the group of torsion units of $\mathbb{Z}_p$:

$$t(\mathbb{Z}_p^\times) = \begin{cases} \{\pm 1\} & p = 2 \\ \mathbb{F}_p^\times & p > 2. \end{cases}$$

Lemma 2.4.2. Let A be a free abelian pro-p group of finite rank. Let G be a profinite group of finite rank acting orbitally soundly and by automorphisms of finite order on A. Then, for each $g \in G$, there exists

$$\zeta = \zeta_g \in t(\mathbb{Z}_p^\times)$$

such that $g \cdot x = \zeta x$ for all $x \in A$. This is multiplicative in G, in the sense that $\zeta_g \zeta_h = \zeta_{gh}$ for all $g, h \in G$.

Proof. Write φ for the automorphism of A given by conjugation by g. We may view φ as an automorphism of the $\mathbb{Q}_p$-vector space $A_{\mathbb{Q}_p} := A \underset{\mathbb{Z}_p}{\otimes} \mathbb{Q}_p$.

As the action of G on A is orbitally sound and G has finite rank, in particular, we have

$$\langle x \rangle \cap \langle \varphi(x) \rangle \neq \{0\}$$

(as $\mathbb{Q}_p$-vector subspaces) for every $x \in A_{\mathbb{Q}_p}$. But this just means that x is an eigenvector of the linear map φ. If all elements of $A_{\mathbb{Q}_p}$ are eigenvectors of φ, then they must have a common eigenvalue, say ζ. The statement that G acts on A by automorphisms of finite order means that the eigenvalue ζ for x is of finite order, $\zeta \in t(\mathbb{Z}_p^\times)$.

Multiplicativity is clear from the fact that $(gh) \cdot x = g \cdot (h \cdot x)$ for all $g, h \in G$. $\square$

Remark. Assume that G is a nilpotent-by-finite, orbitally sound compact p-adic analytic group. In the case when H is an open subgroup of G containing Δ^+, with the property that $N := H/\Delta^+$ is nilpotent p-valuable, we may consider the isolated lower central series of Corollary 2.3.6 for N:

$$N = N_1 \rhd N_2 \rhd \cdots \rhd N_r = 1,$$

and take their preimages in G to get a series of characteristic subgroups of H:

$$H = H_1 \rhd H_2 \rhd \cdots \rhd H_r = \Delta^+,$$

with the property that each $A_i := H_i/H_{i+1}$ is a free abelian pro-p group of finite rank.

G clearly acts orbitally soundly on each A_i, as G is itself orbitally sound. Furthermore, as $[H, H_i] \leq H_{i+1}$ for each i, we see that the action $G \to \mathrm{Aut}(A_i)$ contains the open subgroup H in its kernel, and so G acts by automorphisms of finite order. Thus we may apply Lemma 2.4.2 to see that G acts on each A_i via a homomorphism $\xi_i : G \to t(\mathbb{Z}_p^\times)$.

That is, given any $g \in G$ and $h \in H_i$, and writing $\zeta = \xi_i(g)$ and $a = hH_{i+1} \in A_i$, we have

$$(h^g)h^{-\zeta} \in H_{i+1},$$

or equivalently (still in multiplicative notation)

$$a^g = a^\zeta.$$

We now show that the action of an automorphism of G on the quotients A_i is strongly controlled by its action on A_1. This is an important property that the isolated lower central series shares with the usual lower central series of abstract nilpotent groups; cf. [23, 5.2.5] and the surrounding discussion.

Lemma 2.4.3. Let H be a finite-by-(nilpotent p-valuable) group, and continue to write $A_i := H_i/H_{i+1}$ as in the remark above. Let α be an automorphism of H inducing multiplication by $\zeta_i \in t(\mathbb{Z}_p^\times)$ on each A_i. Then $\zeta_i = \zeta_1^i$ for each i.

Proof. Choose i, and fix some $x \in H_1, y \in H_i$. The map

$$A_1 \underset{\mathbb{Z}_p}{\otimes} A_i \to A_{i+1}$$

$$xH_2 \otimes yH_{i+1} \mapsto [x,y]H_{i+2}$$

is a $\mathbb{Z}_p\langle\alpha\rangle$-module homomorphism, and its image is open in A_{i+1} (by definition of the isolated lower central series). Write $\zeta_1 = \zeta$, and proceed by induction on i: suppose that $\zeta_i = \zeta^i$. Now, for any positive integers a and b, we have

$$[x^a, y^b]H_{i+2} = [x,y]^{ab}H_{i+2}$$

by [9, 0.2(i), (ii)] and by using the fact that $[x,y]H_{i+2}$ is central in H/H_{i+2}. Hence, by continuity, this is true for any $a, b \in \mathbb{Z}_p$, and so

$$\begin{aligned}\alpha([x,y]H_{i+2}) &= [x^\zeta, y^{\zeta^i}]H_{i+2}\\ &= [x,y]^{\zeta^{i+1}}H_{i+2}.\end{aligned}$$

□

We deduce:

Corollary 2.4.4. Let G be a nilpotent-by-finite, orbitally sound compact p-adic analytic group, and H an open normal subgroup of G containing Δ^+ such that H/Δ^+ is nilpotent p-valuable. Then the conjugation action of G on H induces an action of G on H/H_2 given by the map $\xi_1 : G \to t(\mathbb{Z}_p^\times) \leq \mathrm{Aut}(H/H_2)$ defined above. Moreover, $H \leq \ker \xi_1$. □

Remark. If $N = H/\Delta^+$ is p-saturable, we may take its corresponding Lie algebra L by Lazard's isomorphism of categories [13, IV, 3.2.6]. As in [4, proof of lemma 8.5]: using [4, lemma 4.2] and the fact that the N/N_i are torsion-free, we can pick an *ordered basis* [13, III, 2.2.4] B for N which is *filtered* relative to the filtration on N:

that is,

$$B = \{n_1, n_2, \ldots, n_e\},$$

and there exists a filtration of sets

$$B = B_1 \supset B_2 \supset \cdots \supset B_{r-1} \neq \emptyset$$

such that B_i is an ordered basis for N_i for each $1 \leq i \leq r-1$. We may order the elements so that, for some integers $1 = k_1 < k_2 < \cdots < k_{r-1} < e$, we have $B_i = \{n_{k_i+1}, \ldots, n_e\}$ for each $1 \leq i \leq r-1$. Taking logarithms of these basis elements gives us a basis for L, and then Lemma 2.4.3 implies that, with respect to this basis, the automorphism of L induced by α has the special block lower triangular form

$$\begin{pmatrix} \zeta I_{d_1} & 0 & 0 & \ldots & 0 \\ * & \zeta^2 I_{d_2} & 0 & \ldots & 0 \\ * & * & \zeta^3 I_{d_3} & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ * & * & * & \ldots & \zeta^{r-1} I_{d_{r-1}} \end{pmatrix},$$

where $d_i = \mathrm{rk}(L_i/L_{i+1}) = \mathrm{rk}(M_i)$ and I denotes the identity matrix.

2.5 The finite-by-(nilpotent p-valuable) radical

Let G be a nilpotent-by-finite compact p-adic analytic group. Consider the set

$$\mathcal{S}(G) = \left\{ H \underset{O}{\lhd} G \;\middle|\; H/\Delta^+(H) \text{ is nilpotent and } p\text{-valuable} \right\},$$

where "$H \underset{O}{\lhd} G$" means "H is an open normal subgroup of G". $\mathcal{S}(G)$ is nonempty, as we can pick an open normal nilpotent uniform subgroup of G by [9, 4.1], and hence contains a maximal element. We will show that this maximal element is *unique*, and we will call this element the *finite-by-(nilpotent p-valuable) radical* of G, and once we have shown its uniqueness we will denote it by $\mathbf{FN}_p(G)$.

Remark. Once we have shown the existence and uniqueness of $\mathbf{FN}_p(G)$, it will be clear that it is a *characteristic* open subgroup of G (as automorphisms of G leave $\mathcal{S}(G)$ invariant), and contained in $\mathrm{nio}(G)$ (by Corollary 2.1.4 and Theorem A).

The quotient group

$$\mathrm{nio}(G)/\mathbf{FN}_p(G)$$

is isomorphic to a subgroup of $t(\mathbb{Z}_p^\times)$ by Corollary 2.4.4. When $p > 2$, $t(\mathbb{Z}_p^\times)$ is a p'-group, and so $\mathbf{FN}_p(G)/\Delta^+$ is the unique Sylow pro-p subgroup of $\mathrm{nio}(G)/\Delta^+$. (This fails for $p = 2$: the "2-adic dihedral group" $G = \mathbb{Z}_2 \rtimes C_2$ has $\Delta^+(G) = 1$, $\mathrm{nio}(G) = G$, and is its own Sylow 2-subgroup, but $\mathbf{FN}_p(G) = \mathbb{Z}_2$.)

In looking for maximal elements H of $\mathcal{S}(G)$, we may make an immediate simplification. By maximality, any such H must have $\Delta^+(H) = \Delta^+$, i.e. maximal elements of $\mathcal{S}(G)$ are in one-to-one correspondence with maximal elements of

$$\mathcal{S}'(G) = \left\{ H \underset{O}{\lhd} G \;\middle|\; \Delta^+ \leq H,\ H/\Delta^+ \text{ is nilpotent and } p\text{-valuable} \right\},$$

and this set is clearly in order-preserving one-to-one correspondence with the set $\mathcal{S}(G/\Delta^+)$. Hence we may immediately assume without loss of generality that $\Delta^+ = 1$.

Lemma 2.5.1. Let G be a nilpotent-by-finite compact p-adic analytic group with $\Delta^+ = 1$. Then

(i) there exists a nilpotent p-valuable open normal subgroup H of G which contains

Δ,

(ii) any such H satisfies the property that $Z(H) = \Delta$.

Proof. First, suppose we are given a nilpotent p-valuable open normal subgroup H. Take $x \in \Delta$: $\mathbf{C}_G(x)$ is open in G by definition, and so

$$\mathbf{C}_H(x) = \mathbf{C}_G(x) \cap H$$

is open in H. Therefore, for any $h \in H$, we can find some integer k such that $h^{p^k} \in \mathbf{C}_H(x)$. This means that $(x^{-1}hx)^{p^k} = h^{p^k}$, and so by [13, III, 2.1.4], we may take (p^k)th roots inside H to see that $x^{-1}hx = h$. In other words, $x \in \mathbf{C}_\Delta(H)$.

Now suppose further that H contains Δ. Then $x \in Z(H)$. In fact, as we have $Z(H) \leq \Delta(H)$ by definition and $\Delta(H) \subseteq \Delta$ by Lemma 1.2.3(ii), we see that Δ is all of the centre of H. This establishes (ii).

To prove (i), let N be an open normal nilpotent uniform subgroup [9, 4.1] of G. Form $H = N\Delta$, again an open normal subgroup of G. The first paragraph above shows that $[N, \Delta] = 1$; we also know from Lemma 1.2.3(v) that Δ is abelian and N is nilpotent. This forces H to be nilpotent and open in G, and to contain Δ in its centre.

It remains only to show that H is p-valuable – in fact, we will show it is uniform. As H is nilpotent, its set $t(H)$ of torsion elements forms a normal subgroup [23, 5.2.7], and if $t(H)$ is non-trivial then $t(H) \cap Z(H)$ must be non-trivial [23, 5.2.1]; but $Z(H) = \Delta$ is torsion-free by Lemma 1.2.3(v), so H must be torsion-free. Now it is easy to check that H is powerful as in [9, 3.1], so that H is uniform by [9, 4.5]. $\square$

Lemma 2.5.2. Let G be a nilpotent-by-finite compact p-adic analytic group. Then $\mathcal{S}(G)$ is closed under finite joins, and hence contains a *unique* maximal element H, which is characteristic as a subgroup of G.

Proof. First, observe that, for an open normal subgroup K of G, we have $K \in \mathcal{S}(G)$ if and only if $\overline{K} \in \mathcal{S}(\overline{G})$ (where bars denote quotient by Δ^+). So we continue to assume without loss of generality that $\Delta^+ = 1$.

Suppose we are given $K, L \in \mathcal{S}(G)$: then we must show that $KL \in \mathcal{S}(G)$. As K and L are open and normal, it is obvious that KL is too; and since K and L are also nilpotent, Fitting's theorem [27, 1B, Proposition 15] implies that KL is nilpotent. But now, again by [23, 5.2.7], $t(KL) = \Delta^+(KL) \leq \Delta^+ = 1$ – that is, KL is torsion-free, and hence p-valuable by Lemma 2.1.3.

Now let H be a maximal element of $\mathcal{S}(G)$. Assume for contradiction that H does not contain every other element of $\mathcal{S}(G)$ as a subgroup. Then we may pick some $L \in \mathcal{S}(G)$ not contained in H, and form $HL \in \mathcal{S}(G)$; but now $H \lneq HL$, a contradiction to the maximality of H. So H must be the *unique* maximal element of $\mathcal{S}(G)$.

As the set $\mathcal{S}(G)$ is invariant under automorphisms of G, this maximal element H is characteristic in G. $\square$

Definition 2.5.3. Let G be a nilpotent-by-finite compact p-adic analytic group. Its *finite-by-(nilpotent p-valuable) radical* $\mathbf{FN}_p(G)$ is the open characteristic subgroup defined in Lemma 2.5.2.

Proof of Theorem D(i). This follows from Lemma 2.5.2 and the remark made at the beginning of this section.

Proof of Theorem E. This follows from Lemma 2.4.3 and Theorem D(i). $\square$

Chapter 3

Quotients kG/M by minimal prime ideals

3.1 The untwisting theorem

Definition 3.1.1 (Universal property of completed tensor product)**.** [8, §2] Let R be a pseudocompact k-algebra, and let A be a right and B a left pseudocompact R-module. Then the completed tensor product

$$A \hat{\underset{R}{\otimes}} B$$

is a k-module satisfying the following universal property: there is a unique R-bihomomorphism

$$A \times B \to A \hat{\underset{R}{\otimes}} B$$

through which any given R-bihomomorphism $A \times B \to C$ into a pseudocompact k-module C factors uniquely. (An *R-bihomomorphism* $\theta : A \times B \to C$ is a continuous k-module homomorphism satisfying $\theta(ar, b) = \theta(a, rb)$ for all $a \in A, b \in B, r \in R$.)

If $R = k$, and A and B are k-algebras, then their completed tensor product is also a k-algebra.

We give also a construction.

Lemma 3.1.2. [8, §2] Let k be a commutative pseudocompact ring and R a pseudocompact k-algebra. Let A be a right and B a left pseudocompact R-module: then the k-module defined by

$$A \hat{\underset{R}{\otimes}} B := \varprojlim_{U,V} \left(A/U \underset{R}{\otimes} B/V \right)$$

where U and V range over the open submodules of A and B respectively, satisfies the universal property for the completed tensor product of A and B. $\square$

Theorem 3.1.3 (untwisting)**.** Let G be a compact p-adic analytic group, k a commutative pseudocompact ring, and kG the associated completed group ring. Suppose H is a closed normal subgroup of G, and I is an ideal of kH such that $I \cdot kG = kG \cdot I$. Write $\overline{(\cdot)} : kG \to kG/IkG$, so that $\overline{kH} = kH/I$. Suppose also that we have a continuous group homomorphism $\delta : G \to \overline{kH}^\times$ satisfying

(i) $\delta(g) = \overline{g}$ for all $g \in H$,

(ii) $\delta(g)^{-1}\overline{g}$ centralises $\overline{kH}$ for all $g \in G$.

Then there exists an isomorphism of pseudocompact k-algebras

$$\Psi : \overline{kG} \to \overline{kH} \hat{\underset{k}{\otimes}} k[[G/H]],$$

where $\hat{\otimes}$ denotes the completed tensor product.

Proof. Firstly, the function $G \to \left(\overline{kH} \hat{\underset{k}{\otimes}} k[[G/H]] \right)^\times$ given by

$$g \mapsto \delta(g) \otimes gH$$

is clearly a continuous group homomorphism, and so the universal property of completed group rings allows us to extend this function uniquely to a continuous ring homomorphism

$$\Psi' : kG \to \overline{kH} \hat{\underset{k}{\otimes}} k[[G/H]].$$

In the same way, we may extend δ uniquely to a map $\delta : kG \to \overline{kH}$, and by assumption (i), $\delta|_{kH}$ is just the natural quotient map $kH \to \overline{kH}$. Hence $\ker \delta$ must contain the two-sided ideal IkG, so that Ψ' descends to a continuous ring homomorphism

$$\Psi : \overline{kG} \to \overline{kH} \hat{\underset{k}{\otimes}} k[[G/H]].$$

We claim that this is the desired isomorphism. To show that Ψ is an isomorphism, we will construct a continuous ring homomorphism

$$\Phi : \overline{kH} \hat{\underset{k}{\otimes}} k[[G/H]] \to \overline{kG}$$

and show that Φ and Ψ are mutually inverse.

Consider the continuous function $\varepsilon : G \to \overline{kG}^{\times}$ given by

$$\varepsilon(g) = \delta(g)^{-1}\overline{g}.$$

ε is a group homomorphism: indeed, for all $g, h \in G$, we have

$$\begin{aligned} \varepsilon(g)\varepsilon(h) &= \delta(g)^{-1}\overline{g}\,\delta(h)^{-1}\overline{h} \\ &= \boxed{\delta(g)^{-1}\overline{g}}\boxed{\delta(h)^{-1}}\,\overline{h} \\ &= \boxed{\delta(h)^{-1}}\boxed{\delta(g)^{-1}\overline{g}}\,\overline{h} && \text{by assumption (ii)} \\ &= \delta(gh)^{-1}\overline{gh} = \varepsilon(gh). \end{aligned}$$

It is clear that, by assumption (i), $\ker \varepsilon$ contains H, and so descends to a continuous group homomorphism $\varepsilon : G/H \to \overline{kG}^{\times}$; and so again by the universal property we get a continuous ring homomorphism $\varepsilon : k[[G/H]] \to \overline{kG}$. We also clearly have a continuous inclusion $\overline{kH} \to \overline{kG}$.

These functions, and the universal property of Definition 3.1.1, allow us to define the desired map $\Phi : \overline{kH} \hat{\underset{k}{\otimes}} k[[G/H]] \to \overline{kG}$ by

$$\Phi(x \otimes y) = x\varepsilon(y).$$

This map Φ is clearly bilinear in its arguments; to show that it is a ring homomorphism, we need only show that

$$\Phi(x_1 \otimes y_1)\Phi(x_2 \otimes y_2) = \Phi(x_1x_2 \otimes y_1y_2),$$

i.e. that $\varepsilon(y_1)$ commutes with x_2 inside $\overline{kG}$: but this is assumption (ii).

It now remains only to check that Φ and Ψ are mutually inverse. Indeed, for all $g \in G$ and $x \in \overline{kH}$,

$$\begin{aligned}
\Phi(\Psi(\overline{g})) &= \Phi(\delta(g) \otimes gH) \\
&= \Phi(\delta(g) \otimes H)\Phi(1 \otimes gH) \\
&= (\delta(g))(\varepsilon(g)) \\
&= \overline{g},
\end{aligned}$$

and

$$\begin{aligned}\Psi(\Phi(x \otimes gH)) &= \Psi(x\varepsilon(g)) \\ &= \Psi(x\delta(g)^{-1})\Psi(\overline{g}) \\ &= (x\delta(g)^{-1} \otimes 1)(\delta(g) \otimes gH) \\ &= x \otimes gH. \qquad \square\end{aligned}$$

Remark. Let M be a minimal prime of kG, and $e \in \mathrm{cpi}^{\overline{k\Delta^+}}(M)$ (as in Notation 1.5.2). For the rest of §3, and much of §4, we will insist on the mild condition that G centralise e, or equivalently that $M \cap k\Delta^+$ remain prime as an ideal of $k\Delta^+$. This is mostly to keep the notation simple: we will return briefly to this issue in §4.3, and show that we have not lost much generality by doing this.

Corollary 3.1.4. Let G be a compact p-adic analytic group, k a finite field of characteristic p, and M a minimal prime of kG. In Notation 1.5.2, choose $e \in \mathrm{cpi}^{\overline{k\Delta^+}}(M)$, and assume (as in the above remark) that G centralises e, so that $(1-e)\overline{kG} = \overline{M}$ and

$$kG/M \cong \overline{kG}/\overline{M} = e \cdot \overline{kG}.$$

Suppose we are given a continuous group homomorphism

$$\delta : G \to (e \cdot \overline{k\Delta^+})^\times,$$

satisfying

(i) $\delta(g) = e \cdot \overline{g}$ for all $g \in \Delta^+$,

(ii) $\delta(g)^{-1}\overline{g}$ centralises $e \cdot \overline{k\Delta^+}$ for all $g \in G$.

Then there exists an isomorphism

$$\Psi : e \cdot \overline{kG} \to e \cdot \overline{k\Delta^+} \underset{k}{\otimes} k[[G/\Delta^+]],$$

and hence also an isomorphism

$$\psi : e \cdot \overline{kG} \to M_t(k'[[G/\Delta^+]])$$

for some positive integer t and some finite field extension k'/k.

Proof. In Theorem 3.1.3, take $H = \Delta^+$, and take I to be the ideal of $k\Delta^+$ generated by $J(k\Delta^+)$ and $1 - a$, where $a \in k\Delta^+$ is any element whose image in $\overline{k\Delta^+}$ is e. This gives the isomorphism

$$\Psi : e \cdot \overline{kG} \to e \cdot \overline{k\Delta^+} \hat{\underset{k}{\otimes}} k[[G/\Delta^+]];$$

but now, as $e \cdot \overline{k\Delta^+}$ is finite-dimensional as a vector space over k, [8, Lemma 2.1(ii)] implies that the right hand side is equal to the ordinary tensor product

$$e \cdot \overline{k\Delta^+} \underset{k}{\otimes} k[[G/\Delta^+]].$$

Now the isomorphism ψ is given by composing Ψ with the isomorphism of Lemma 1.5.1(iii). □

Remark. This result is a strong generalisation of the result given in [5, 10.1], in the case when $G \cong N \times \Delta^+$. In that case, we may simply take δ to be the composite of the natural map $N \times \Delta^+ \to \Delta^+$ given by projection onto the second factor, and the inclusion map $\Delta^+ \hookrightarrow (e \cdot \overline{k\Delta^+})^\times$.

3.2 Almost-faithfulness and untwisted ideals

Throughout this section:

- G is a compact p-adic analytic group, and k is a finite field of characteristic p,
- M is a minimal prime ideal of kG and $e \in \mathrm{cpi}^{\overline{k\Delta^+}} M$, so that Notation 1.5.2 applies
- assume further that G centralises e, and that we have an untwisting map

$$\delta : G \to (e \cdot \overline{k\Delta^+})^\times$$

  satisfying the hypotheses of Corollary 3.1.4, and write

$$\psi : e \cdot \overline{kG} \to M_t(k'[[G/\Delta^+]])$$

  for the corresponding isomorphism given by Corollary 3.1.4,
- write $q : kG \to e \cdot \overline{kG}$ for the natural quotient map.

(We leave it until section 4.1 to find such a δ for a certain large class of groups G.)

In this setting, we have the following one-to-one correspondences of ideals:

$$\begin{tikzcd} \left\{\begin{array}{c}\text{ideals of}\\ kG \text{ which}\\ \text{contain } M\end{array}\right\} \arrow[r, leftrightarrow] \arrow[r, bend right, "q"'] & \left\{\begin{array}{c}\text{ideals of}\\ e \cdot \overline{kG}\end{array}\right\} \arrow[r, leftrightarrow] \arrow[r, bend right, "\psi"'] & \left\{\begin{array}{c}\text{ideals of}\\ M_t(k'[[G/\Delta^+]])\end{array}\right\} \arrow[r, leftrightarrow, "\text{Morita equiv.}"] & \left\{\begin{array}{c}\text{ideals of}\\ k'[[G/\Delta^+]]\end{array}\right\}. \end{tikzcd}$$

Lemmas 1.6.3 and 1.6.4 may now be interpreted as demonstrating that the first and third correspondences in this diagram preserve some notion of *control* (as defined in Definition 1.6.1). The middle correspondence trivially preserves control, as ψ is an isomorphism. We remark also that all three correspondences preserve primality, the third by Lemma 1.6.5.

In this section, we show that some appropriate notion of almost-faithfulness (see Definition 1.6.2) is also preserved by these correspondences. That is, let P be any ideal of kG containing M. Then we have

$$\psi \circ q(P) = M_t(\mathfrak{p}),$$

where $\mathfrak{p}$ is some ideal of $k'[[G/\Delta^+]]$. Recall the definition of $(-)^\dagger$ from Definition 1.6.2: we intend to show that the groups $P^\dagger$ (a subgroup of G) and $\mathfrak{p}^\dagger$ (a subgroup of G/Δ^+) are closely related.

We will abuse notation to identify the two rings

$$e \cdot \overline{k\Delta^+} \underset{k}{\otimes} k[[G/\Delta^+]] = e \cdot \overline{k\Delta^+} \underset{k'}{\otimes} k'[[G/\Delta^+]]$$

in the obvious way. Then, laying out the structure more explicitly, we have

$$\Psi(e \cdot \overline{P}) = e \cdot \overline{k\Delta^+} \underset{k'}{\otimes} \mathfrak{p}$$

in the notation of Corollary 3.1.4.

Suppose that $g\Delta^+ \in \mathfrak{p}^\dagger$ for some $g \in G$, i.e. $(g-1)\Delta^+ \in \mathfrak{p}$. Then

$$(1 \otimes g\Delta^+) - (1 \otimes \Delta^+) \in \Psi(e \cdot \overline{P}),$$

so

$$\Phi(1 \otimes g\Delta^+) - \Phi(1 \otimes \Delta^+) = \delta(g)^{-1}\overline{g} - e \in e \cdot \overline{P}.$$

This motivates the following definition:

Definition 3.2.1. Write

$$P_\delta^\dagger = \{g \in G \,|\, \delta(g)^{-1}\overline{g} - e \in e \cdot \overline{P}\},$$

so that $P_\delta^\dagger$ is the kernel of the composite map

$$G \xrightarrow{\varepsilon} (e \cdot \overline{kG})^\times \xrightarrow{\sim} (kG/M)^\times \twoheadrightarrow (kG/P)^\times,$$

where $\varepsilon : G \to (e \cdot \overline{kG})^\times$ is defined by $\varepsilon(g) = \delta(g)^{-1}\overline{g}$. (As we saw in the proof of Theorem 3.1.3, ε is a continuous group homomorphism.) Compare this with Definition 1.6.2: this is a "twisted" version of $P^\dagger$.

Now, since $\varepsilon(g) = 1$ for all $g \in \Delta^+$, we have $\Delta^+ \leq P_\delta^\dagger$ for any ideal P. We say that P is *δ-faithful* if $P_\delta^\dagger = \Delta^+$ (and P is *δ-unfaithful* if $P_\delta^\dagger$ is infinite).

Lemma 3.2.2. The following are equivalent:

(i) P is almost faithful (as an ideal of kG).

(ii) P is δ-faithful.

(iii) $\mathfrak{p}$ is faithful (as an ideal of $k'[[G/\Delta^+]]$).

Proof.

$\boxed{\text{(ii)} \Leftrightarrow \text{(iii)}}$ By the above calculation, we see that P is defined to be a δ-faithful ideal of kG precisely when $\mathfrak{p}$ is a faithful ideal of $k'[[G/\Delta^+]]$.

$\boxed{\text{(i)} \Leftrightarrow \text{(ii)}}$ Let $m = |\mathrm{im}(\delta)|$. Note that $m < \infty$ as k is assumed to be a finite field. Then $\delta(g^m) = e$ for all $g \in G$, so

$$
\begin{aligned}
g^m \in P_\delta^\dagger &\Leftrightarrow \delta(g^m)\overline{g^m}^{-1} - e \in e \cdot \overline{P} \\
&\Leftrightarrow e\overline{g^m}^{-1} - e \in e \cdot \overline{P} \\
&\Leftrightarrow e(\overline{g^m}^{-1} - 1) \in e \cdot \overline{P} \\
&\Leftrightarrow \overline{g^m}^{-1} - \overline{1} \in \overline{P} \\
&\Leftrightarrow g^{-m} - 1 \in P \\
&\Leftrightarrow g^{-m} \in P^\dagger \\
&\Leftrightarrow g^m \in P^\dagger,
\end{aligned}
$$

so writing $(P^\dagger)^m := \langle g^m | g \in P^\dagger \rangle$, and likewise $(P_\delta^\dagger)^m$, we see that these two subgroups are equal.

Now, suppose P is almost faithful, and so in particular $P^\dagger$ is torsion; then the subgroup $(P^\dagger)^m = (P_\delta^\dagger)^m$ is also torsion, and since g^m is torsion for any $g \in P_\delta^\dagger$, we have that g must also be torsion. So $P_\delta^\dagger$ is a torsion subgroup of G. Hence it must be finite: indeed, given any open normal uniform subgroup U of G, the kernel of the composite map $P_\delta^\dagger \hookrightarrow G \to G/U$ is a subgroup of $U \cap P_\delta^\dagger$, which is trivial as U is torsion-free [9, 4.5]. So $P_\delta^\dagger$ embeds into the finite group G/U, and as $P_\delta^\dagger$ is also normal in G by Definition 3.2.1, it is a finite orbital subgroup of G and hence must be a subgroup of Δ^+, i.e. P is δ-faithful. The converse is similar. $\square$

In summary:

Corollary 3.2.3. Assume the hypotheses of Corollary 3.1.4. Let P be an ideal of kG containing M, and denote by $q : kG \to kG/M$ the natural quotient map. Write $\psi \circ q(P) = M_t(\mathfrak{p})$, where $\mathfrak{p}$ is an ideal of $k'[[G/\Delta^+]]$. Then $\mathfrak{p}$ is faithful if and only if P is almost faithful; and $\mathfrak{p}$ is prime if and only if P is prime. $\square$

Chapter 4

The untwisting map

4.1 The case when G is finite-by-(pro-p)

In this section, we introduce a group A_H for each closed subgroup H of G. By studying the structure of the group A_G in the case when G/Δ^+ is pro-p, we will find an untwisting map $\delta : G \to (e \cdot \overline{k\Delta^+})^\times$ satisfying the conditions of Corollary 3.1.4.

Let G be a compact p-adic analytic group, k a finite field of characteristic p, M a minimal prime of kG, and $e \in \mathrm{cpi}^{\overline{k\Delta^+}}(M)$, which we continue to suppose is centralised by G. Then $e \cdot \overline{k\Delta^+} \cong M_t(k')$, and in particular its automorphisms are all inner by the Skolem-Noether theorem [28, Tag 074P].

Note that both G and $(e \cdot \overline{k\Delta^+})^\times$ act on the ring $e \cdot \overline{k\Delta^+}$ by conjugation, and so we get group homomorphisms $G \to \mathrm{Inn}(e \cdot \overline{k\Delta^+})$ and $(e \cdot \overline{k\Delta^+})^\times \to \mathrm{Inn}(e \cdot \overline{k\Delta^+})$.

Definition 4.1.1. For any closed subgroup $H \leq G$, define A_H to be the fibre product of H and $(e \cdot \overline{k\Delta^+})^\times$ over $\mathrm{Inn}(e \cdot \overline{k\Delta^+})$ with respect to the above maps,

$$A_H = (e \cdot \overline{k\Delta^+})^\times \underset{\mathrm{Inn}(e \cdot \overline{k\Delta^+})}{\times} H,$$

a subgroup of $(e \cdot \overline{k\Delta^+})^\times \times H$. Write the projection map onto the second factor as $\pi_H : A_H \to H$.

As $e \cdot \overline{k\Delta^+} \cong M_t(k')$, we have $(e \cdot \overline{k\Delta^+})^\times \cong GL_t(k')$. The centre of $(e \cdot \overline{k\Delta^+})^\times$ is therefore isomorphic to $Z(GL_t(k'))$, which we will identify with $k'^\times$, and the inner automorphism group $\mathrm{Inn}(e \cdot \overline{k\Delta^+})$ is isomorphic to $PGL_t(k')$. In particular, A_H is an extension of H by $k'^\times$. Indeed, the following diagram commutes and has exact rows:

$$\begin{tikzcd}
1 \arrow[r] & k'^\times \arrow[r, "i"] \arrow[d, equal] & A_H \arrow[r, dotted, "\pi_H"] \arrow[d, dotted] & H \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & k'^\times \arrow[r] & (e \cdot \overline{k\Delta^+})^\times \arrow[r] & \mathrm{Inn}(e \cdot \overline{k\Delta^+}) \arrow[r] & 1.
\end{tikzcd}$$

The inclusion $i : k'^\times \to A_H$ is given by $i(x) = (x, 1)$. (The image of i is just $A_{\{1\}}$.)

We will now examine the subgroup structure of A_G.

Lemma 4.1.2. If N is a closed normal subgroup of G, then $A_N \lhd A_G$, and $A_G/A_N \cong G/N$.

Proof. Firstly, clearly A_N is naturally a subgroup of A_G, and the following diagram commutes and has exact rows:

$$\begin{tikzcd}
1 \arrow[r] & k'^\times \arrow[r] \arrow[d, equal] & A_N \arrow[r, "\pi_N"] \arrow[d, hook] & N \arrow[r] \arrow[d, hook] & 1 \\
1 \arrow[r] & k'^\times \arrow[r] & A_G \arrow[r, "\pi_G"'] & G \arrow[r] & 1.
\end{tikzcd}$$

Let $(r, n) \in A_N$ and $(s, g) \in A_G$. For any $x \in (e \cdot \overline{k\Delta^+})$, we have $x^r = x^n$ and $x^s = x^g$, so we get $x^{s^{-1}rs} = x^{g^{-1}ng}$. As $g^{-1}ng \in N$, we have

$$(s, g)^{-1}(r, n)(s, g) = (s^{-1}rs, g^{-1}ng) \in A_N,$$

and so $A_N \lhd A_G$.

Hence we may take cokernels of the vertical maps, completing the above diagram to the following commutative diagram, whose columns and first two rows are exact:

$$\begin{tikzcd}
 & 1 \arrow[d] & 1 \arrow[d] & 1 \arrow[d] & \\
1 \arrow[r] & k'^{\times} \arrow[r] \arrow[d, equal] & A_N \arrow[r] \arrow[d] & N \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & k'^{\times} \arrow[r] \arrow[d] & A_G \arrow[r] \arrow[d] & G \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & 1 \arrow[r] \arrow[d] & A_G/A_N \arrow[r] \arrow[d] & G/N \arrow[r] \arrow[d] & 1 \\
 & 1 & 1 & 1 &
\end{tikzcd}$$

By the Nine Lemma [12, Chapter XII, Lemma 3.4], the third row is now also exact. □

Consider the natural map $\Delta^+ \to (e \cdot \overline{k\Delta^+})^\times$ given by $g \mapsto e \cdot \overline{g}$. There is a "diagonal" inclusion map $d : \Delta^+ \to A_G$ given by $g \mapsto (e \cdot \overline{g}, g)$, and the image $d(\Delta^+)$ is normal in A_G: indeed, suppose we are given $(x, h) \in A_G$. Then

$$\begin{aligned}
d(g)^{(x,h)} &= (x,h)^{-1}(e \cdot \overline{g}, g)(x,h) \\
&= ((e \cdot \overline{g})^x, g^h) \\
&= ((e \cdot \overline{g})^h, g^h) && \text{by definition of } A_G \\
&= d(g^h).
\end{aligned}$$

Remark. The map d, considered as a map from Δ^+ to A_{Δ^+}, splits the map π_{Δ^+}.

Hence there are copies of $k'^{\times}$ and Δ^+ in A_{Δ^+}, and they commute: given $x \in k'^{\times}$, $g \in \Delta^+$, we have

$$i(x)d(g) = (x,1)(e \cdot \overline{g}, g) = (e \cdot \overline{g}, g)(x,1) = d(g)i(x)$$

as x commutes with $e \cdot \overline{g}$ inside $e \cdot \overline{k\Delta^+}$. In other words,

$$A_{\Delta^+} = i(k'^{\times})d(\Delta^+) \cong k'^{\times} \times \Delta^+.$$

Lemma 4.1.3. Let G be a compact p-adic analytic group. Suppose that we have an injective group homomorphism $\sigma : G \to A_G$ splitting π_G such that, for all $g \in \Delta^+$, we have $\sigma(g) = (e \cdot \overline{g}, g)$. Then we can find a δ satisfying the conditions of Corollary 3.1.4.

Proof. Define δ to be the composite of $\sigma : G \to A_G$ with the projection $A_G \to (e \cdot \overline{k\Delta^+})^\times$. $\square$

We assume for the remainder of this subsection that G/Δ^+ **is pro-**p, and find a map σ satisfying Lemma 4.1.3 for this case.

Write $P = G/\Delta^+$. Note that $A_G/d(\Delta^+)$ is an extension of A_G/A_{Δ^+} (which is isomorphic to P, a pro-p group, by Lemma 4.1.2) by $A_{\Delta^+}/d(\Delta^+)$ (which is isomorphic to $k'^\times$, a p'-group, by the discussion above). Hence, as k is still assumed to be finite, we may apply Sylow's theorems [9, §1, exercise 11] to find a Sylow pro-p subgroup $L/d(\Delta^+)$ of $A_G/d(\Delta^+)$ which is isomorphic to P.

This information is summarised in the following diagram.

$$
\begin{tikzcd}
& A_G \arrow[dd, dash, "P"] \arrow[dr, dash] & \\
& & L \arrow[dd, dash, "P"] \\
& A_{\Delta^+} \arrow[dl, dash, "\Delta^+"'] \arrow[dr, dash, "k'^\times"] & \\
i(k'^\times) \arrow[dr, dash, "k'^\times"'] & & d(\Delta^+) \arrow[dl, dash, "\Delta^+"] \\
& 1 &
\end{tikzcd}
$$

Lemma 4.1.4. Suppose G/Δ^+ is pro-p. Then there is a map σ splitting the surjection $\pi_G : A_G \to G$ satisfying the hypotheses of Lemma 4.1.3.

Proof. Consider $\pi_G|_L : L \to G$. Now, $\ker(\pi_G) = i(k'^\times)$, so

$$\begin{aligned}\ker(\pi_G|_L) &= i(k'^\times) \cap L \\ &= (i(k'^\times) \cap A_{\Delta^+}) \cap L \\ &= i(k'^\times) \cap (A_{\Delta^+} \cap L) \\ &= i(k'^\times) \cap d(\Delta^+) = 1,\end{aligned}$$

so $\pi_G|_L$ is injective. Also,

$$i(k'^\times) \cdot L = A_{\Delta^+} \cdot L = A_G,$$

so

$$\begin{aligned}G = \pi_G(A_G) &= \pi_G(i(k'^\times) \cdot L) \\ &= \pi_G(i(k'^\times)) \cdot \pi_G(L) \\ &= \pi_G(L)\end{aligned}$$

as $\pi_G(i(x)) = \pi_G((x, 1)) = 1$ for $x \in k'^\times$, and hence $\pi_G|_L$ is surjective. So $\pi_G|_L$ is in fact an isomorphism $L \to G$.

Define $\sigma : G \to L \to A_G$ (i.e. $(\pi_G|_L)^{-1}$ followed by inclusion). By construction, this σ splits π_G. Also, as $\pi_G(\sigma(g)) = \pi_G(d(g)) = g$ for all $g \in \Delta^+$, we have that $\sigma(g)d(g)^{-1} \in \ker \pi_G \cap L = 1$, and so $\sigma(g) = d(g) = (e \cdot \overline{g}, g)$ for $g \in \Delta^+$ as required. $\square$

Now we may define $\delta : G \to (e \cdot \overline{k\Delta^+})^\times$ as in the proof of Lemma 4.1.3, allowing us to deduce the following theorem, in which we continue to write $q : kG \to e \cdot \overline{kG}$ for the natural quotient map:

Theorem 4.1.5. Let G be a compact p-adic analytic group with G/Δ^+ pro-p, and let k be a finite field. Write $N = G/\Delta^+$. Let M be a minimal prime of kG, and $e \in \mathrm{cpi}^{\overline{k\Delta^+}}(M)$, and suppose that e is centralised by G. Then we can find a $\delta : G \to (e \cdot \overline{k\Delta^+})^\times$ satisfying the conditions of Corollary 3.1.4. In particular:

(i) There exists an isomorphism

$$\Psi : e \cdot \overline{kG} \to e \cdot \overline{k\Delta^+} \underset{k}{\otimes} kN.$$

(ii) There exist a finite field extension k'/k and a positive integer t, and an isomorphism

$$\psi : e \cdot \overline{kG} \to M_t(k'N).$$

Furthermore, let A be an ideal of kG with $M \subseteq A$, so that $\psi \circ q(A) = M_t(\mathfrak{a})$ for some ideal $\mathfrak{a}$ of $k'N$. Then:

(iii) A is prime if and only if $\mathfrak{a}$ is prime. Also, A is almost (G-)faithful if and only if $\mathfrak{a}$ is (N-)faithful.

Proof.

(i) The map δ as defined by Lemmas 4.1.3 and 4.1.4 satisfies the conditions of Corollary 3.1.4, which gives the isomorphism $\Psi : e \cdot \overline{kG} \to e \cdot \overline{k\Delta^+} \underset{k}{\otimes} k[[G/\Delta^+]]$.

(ii) As in Corollary 3.1.4, we may identify $e \cdot \overline{k\Delta^+} \underset{k}{\otimes} k[[G/\Delta^+]]$ with $M_t(k'[[G/\Delta^+]])$ by appealing to Lemma 1.5.1(iii).

(iii) This is just Corollary 3.2.3. □

Proof of Theorem F. This follows from Theorem 4.1.5. □

4.2 Central twists by 2-cocycles, and the general case

Suppose we are given a ring R, a finite group G, and a fixed crossed product

$$S = R \underset{\langle \sigma, \tau \rangle}{*} G$$

as in Notation 1.7.2; and suppose further that we wish to define some new crossed product, keeping the action the same but changing the twisting, say

$$S' = R \underset{\langle \sigma, \tau' \rangle}{*} G.$$

For the rest of this section, until stated otherwise, we will write $A = Z(R^\times)$.

Lemma 4.2.1. S' is well-defined as a ring if and only if there exists $\alpha \in Z^2_\sigma(G, A)$ satisfying $\tau'(x, y) = \tau(x, y)\alpha(x, y)$ for all $x, y \in G$.

Proof. Equation (1.7.2), applied to both S and S', gives

$$\begin{aligned} \sigma(x)\sigma(y) &= \sigma(xy)\eta(x, y) && \text{and} \\ \sigma(x)\sigma(y) &= \sigma(xy)\eta'(x, y) && \text{for all } x, y \in G, \end{aligned}$$

where $\eta(x, y)$ and $\eta'(x, y)$ are the automorphisms induced by conjugation by $\tau(x, y)$ and $\tau'(x, y)$ respectively. This implies that $\eta = \eta'$. In other words, writing $\alpha = \tau^{-1}\tau'$ pointwise, we see that conjugation by $\alpha(x, y)$ induces the trivial automorphism on R, and so

$$\alpha : G \times G \to Z(R^\times) = A,$$

and it follows from equation (1.7.3) that, in order for S' to be a ring, α must be a 2-cocycle for σ taking values in A. The converse is identical. $\square$

Definition 4.2.2. When the crossed product $S = R * G = R \underset{\langle\sigma,\tau\rangle}{*} G$ and the central 2-cocycle α are fixed, write the ring S' defined above as S_α: we will say that S_α is the *central 2-cocycle twist of S by α with respect to the decomposition $S = R \underset{\langle\sigma,\tau\rangle}{*} G$*, meaning that

$$S_\alpha = R \underset{\langle\sigma,\tau\alpha\rangle}{*} G.$$

Sometimes it will not be necessary to specify all of this information in full; we may simply refer to S_α as *a central 2-cocycle twist of S*, or similar.

Note that S_α depends not only on the map τ, but also on the choice of basis $\overline{G}$ for $S = R * G$.

Remark. Fix a crossed product $S = R * G$, and choose some $\alpha \in Z^2_\sigma(G, A)$. Write the resulting crossed product decompositions as

$$S = \bigoplus_{g \in G} R\overline{g}, \quad S_\alpha = \bigoplus_{g \in G} R\hat{g}.$$

We say that S and S_α differ by a *diagonal change of basis* if, for each $g \in G$, there is some unit $u_g \in R^\times$ such that $\hat{g} = \overline{g}u_g$. (In particular, if S and S_α differ by a diagonal change of basis, they are isomorphic.) By [22, exercise 1.1], S and S_α differ by a diagonal change of basis if and only if α is a *2-coboundary* for σ, i.e. there is some function $\varphi : G \to R^\times$ with

$$\alpha(x, y) = \varphi(xy)^{-1}\varphi(x)^{\sigma(y)}\varphi(y)$$

for all $x, y \in G$. Hence S and S_α are non-isomorphic only if α has non-trivial cohomology class. But we will not develop this idea any further in this thesis.

Remark. We note that similar twists have been studied by Aljadeff *et al.*, e.g. in [1].

Central 2-cocycle twists will occur naturally in the theory later. For now, we see where this will be applied:

Definition 4.2.3. [22, Lemma 12.3] Let R be a prime ring. An automorphism $\varphi : R \to R$ is *X-inner* if there exist nonzero elements $a, b, c, d \in R$ such that, for all $x \in R$,

$$axb = cx^{\varphi}d.$$

(Here x^{φ} denotes the image of x under φ.) Write $\mathrm{Xinn}(R)$ to denote the subgroup of $\mathrm{Aut}(R)$ of X-inner automorphisms.

Now let G be a group, and fix a crossed product

$$S = R * G = R \underset{\langle \sigma, \tau \rangle}{*} G.$$

Write $\mathrm{Xinn}_S(R; G)$ for the normal subgroup of G consisting of elements $g \in G$ that act by X-inner automorphisms on R, i.e.

$$\mathrm{Xinn}_S(R; G) = \sigma^{-1}(\sigma(G) \cap \mathrm{Xinn}(R)).$$

Theorem 4.2.4. Fix a crossed product $S = R * G$ with R prime, G finite. Then $\mathrm{Xinn}_S(R; G) = \mathrm{Xinn}_{S_\alpha}(R; G)$ for every $\alpha \in Z^2_\sigma(G, A)$. In particular, if $\mathrm{Xinn}_S(R; G) = 1$, then S_α is a prime ring for every $\alpha \in Z^2_\sigma(G, A)$.

Proof. It is clear from the definition that $\mathrm{Xinn}_{S_\alpha}(R; G)$ depends only on the map σ, and so $\mathrm{Xinn}_{S_\alpha}(R; G) = \mathrm{Xinn}_S(R; G)$ for all α. A special case of [22, Corollary 12.6] implies that, if $\mathrm{Xinn}_{S_\alpha}(R; G) = 1$, then S_α is a prime ring. $\square$

This theorem will be important in §7.

Now we turn our attention back to the problem of understanding quotients of completed group algebras.

Let G be a compact p-adic analytic group, M a minimal prime of kG, and $e \in \mathrm{cpi}^{\overline{k\Delta^+}}(M)$ (as in Notation 1.5.2) centralised by G. In this more general case, we may not be able to find a group homomorphism

$$\delta : G \to (e \cdot \overline{k\Delta^+})^\times$$

satisfying the hypotheses of Corollary 3.1.4, so we may not be able to find an isomorphism

$$\psi : e \cdot \overline{kG} \to M_t(k'[[G/\Delta^+]]).$$

In this case, fix an open normal pro-p subgroup N of G/Δ^+ (e.g. by taking the normal core in G of an open uniform pro-p subgroup, as in [9, Theorem 8.32]), and write H for the preimage of N in G, so that by Theorem 4.1.5 we *do* get an isomorphism

$$\psi : e \cdot \overline{kH} \to M_t(k'N).$$

Now we will have to rely on the crossed product structure of kG. That is, writing $F = G/H$, we can find a crossed product decomposition

$$kG = kH * F.$$

In the following discussion, we will construct a related crossed product $k'N * F$ (not necessarily isomorphic to $k'[[G/\Delta^+]]$), and show that the isomorphism ψ extends to an isomorphism

$$\tilde{\psi} : e \cdot \overline{kG} \to M_t(k'N * F).$$

Studying the structure of this crossed product $k'N * F$ will allow us to understand the prime ideals of kG. In fact, we will show that $k'N * F$ is a central 2-cocycle twist of $k'[[G/\Delta^+]]$.

Recall the map $\delta : H \to (e \cdot \overline{k\Delta^+})^\times$ from Theorem 4.1.5, and continue to write

$$\begin{aligned} \varepsilon : H &\to (e \cdot \overline{kH})^\times \\ h &\mapsto \delta(h)^{-1}\overline{h} \end{aligned}$$

for all $h \in H$, as in the proof of Theorem 3.1.3.

For the remainder of this section, we fix an element $g \in G$.

Fix $M_g \in (e\cdot\overline{k\Delta^+})^\times$, an arbitrary lift of the image of g under the map $G \to \mathrm{Inn}(e\cdot\overline{k\Delta^+})$, i.e. any element such that $x^g = x^{M_g}$ for all $x \in e \cdot \overline{k\Delta^+}$, and hence $(M_g, g) \in A_G$. Define

$$\widetilde{g} = M_g^{-1}\overline{g} \in (e \cdot \overline{kG})^\times \tag{4.2.1}$$

– this element will play the role of "$\varepsilon(g)$" when $g \notin H$.

Recall also the isomorphisms

$$e \cdot \overline{kH} \underset{\Phi}{\overset{\Psi}{\rightleftarrows}} e \cdot \overline{k\Delta^+} \underset{k}{\otimes} kN$$

of the proof of Theorem 3.1.3.

Conjugation on the right by $\widetilde{g}$ is a ring automorphism $\varphi_g \in \mathrm{Aut}(e\cdot\overline{kH})$, which induces a ring automorphism

$$\Psi \circ \varphi_g \circ \Phi =: \theta_g \in \mathrm{Aut}(e \cdot \overline{k\Delta^+} \underset{k}{\otimes} kN).$$

That is:

$$\begin{array}{ccc} e \cdot \overline{kH} & \xrightarrow{\varphi_g} & e \cdot \overline{kH} \\ \uparrow{\scriptstyle \Phi} & & \downarrow{\scriptstyle \Psi} \\ e \cdot \overline{k\Delta^+} \underset{k}{\otimes} kN & \xrightarrow[\theta_g]{} & e \cdot \overline{k\Delta^+} \underset{k}{\otimes} kN \end{array}$$

For ease of notation, we will write these maps on the left as before, though note that e.g. $\theta_{g_1} \circ \theta_{g_2}(x) = \theta_{g_2 g_1}(x)$ for all $g_1, g_2 \in G$.

Given $r \in e \cdot \overline{k\Delta^+}$ and $h\Delta^+ \in N$, we wish to calculate $\theta_g(r \otimes h\Delta^+)$ explicitly.

We begin with a trivial remark:

Lemma 4.2.5. By construction, $\varphi_g(r) = r$, and so $\theta_g(r \otimes 1) = r \otimes 1$. □

Next, a computational lemma:

Lemma 4.2.6. Suppose N is pro-p and $k'^\times$ contains no non-trivial pro-p subgroups. Then $\delta(h)^g = \delta(h^g)$ for all $h \in H$.

Proof. Define $\beta_g : H \to (e \cdot \overline{k\Delta^+})^\times$ by $\beta_g(h) = \delta(h^g)^{-1}\delta(h)^g$. We aim to show that $\beta_g(h) = 1$ for all h.

For any $r \in e \cdot \overline{k\Delta^+}$, we have that

$$\begin{aligned} r^{\delta(h^g)} &= r^{h^g} \\ &= ((r^{g^{-1}})^h)^g \\ &= ((r^{g^{-1}})^{\delta(h)})^g = r^{\delta(h)^g}, \end{aligned}$$

and so $r^{\beta_g(h)} = r$, i.e. $\beta_g(h)$ is in the centre of $(e \cdot \overline{k\Delta^+})^\times$. So β_g is a map from H to $k'^\times$.

Let $h_1, h_2 \in H$. Since $\beta_g(h_1) = \delta(h_1^g)^{-1}\delta(h_1)^g$ is central in $(e \cdot \overline{k\Delta^+})^\times$, in particular it centralises $\delta(h_2^g)^{-1}$, and so

$$\begin{aligned}\beta_g(h_1h_2) &= \delta((h_1h_2)^g)^{-1}\delta(h_1h_2)^g \\ &= \delta(h_2^g)^{-1}\delta(h_1^g)^{-1}\delta(h_1)^g\delta(h_2)^g \\ &= \boxed{\delta(h_2^g)^{-1}}\,\boxed{\delta(h_1^g)^{-1}\delta(h_1)^g}\,\delta(h_2)^g \\ &= \boxed{\delta(h_1^g)^{-1}\delta(h_1)^g}\,\boxed{\delta(h_2^g)^{-1}}\,\delta(h_2)^g \\ &= \beta_g(h_1)\beta_g(h_2),\end{aligned}$$

so β_g is a group homomorphism $H \to k'^{\times}$. Furthermore, when $h \in \Delta^+$,

$$\begin{aligned}\beta_g(h) &= \delta(h^g)^{-1}\delta(h)^g \\ &= (e \cdot \overline{h^g})^{-1}(e \cdot \overline{h})^g = 1.\end{aligned}$$

So $\Delta^+ \leq \ker \beta_g$, and so β_g in fact descends to a homomorphism from N (a pro-p group) to $k'^{\times}$ (containing no non-trivial pro-p subgroups), and so must be trivial. $\square$

Continue to write $\varepsilon(h) = \delta(h)^{-1}\overline{h}$ for all $h \in H$. Then, finally, we can conclude:

Corollary 4.2.7. Suppose N is pro-p and $k'^{\times}$ contains no non-trivial pro-p subgroups. Then $\varepsilon(h)^{\widetilde{g}} = \varepsilon(h^g)$ for all $h \in H$.

Proof. We have

$$\begin{aligned}\varepsilon(h)^{\widetilde{g}} &= \varepsilon(h)^g && \text{as } \varepsilon(h) \text{ centralises } M_g \\ &= (\delta(h)^g)^{-1}\overline{h^g} \\ &= (\delta(h^g))^{-1}\overline{h^g} && \text{by Lemma 4.2.6} \\ &= \varepsilon(h^g),\end{aligned}$$

as required. $\square$

Now we can calculate the action of θ_g on $e \cdot \overline{k\Delta^+} \underset{k}{\otimes} kN$:

Lemma 4.2.8. Given $r \in e \cdot \overline{k\Delta^+}$ and $h\Delta^+ \in N$, with N pro-p and $k'^{\times}$ containing no non-trivial pro-p subgroups as above, we have

$$\theta_g(r \otimes h\Delta^+) = r \otimes (h\Delta^+)^{g\Delta^+}.$$

Proof.

$$\begin{aligned}
\theta_g(r \otimes h\Delta^+) &= \Psi(\varphi_g(\Phi(r \otimes h\Delta^+))) && \\
&= \Psi(\varphi_g(r\varepsilon(h))) && \text{by definition} \\
&= \Psi(r^{\widetilde{g}}\varepsilon(h)^{\widetilde{g}}) && \\
&= \Psi(r\varepsilon(h^g)) && \text{by Corollary 4.2.7 and Lemma 4.2.5} \\
&= \Psi(\Phi(r \otimes h^g\Delta^+)) && \text{by definition} \\
&= r \otimes h^g\Delta^+ && \text{by Theorem 3.1.3} \\
&= r \otimes (h\Delta^+)^{g\Delta^+}. && \square
\end{aligned}$$

We will need one final definition.

Definition 4.2.9. Let G be a compact p-adic analytic group, H an open normal subgroup, $F = G/H$, and I a G-stable ideal of kH. Suppose we are given elements $x_i \in (kG/IkG)^{\times}$ such that

$$kG/IkG = \bigoplus_{i=1}^{m} x_i(kH/I)$$

is a decomposition of kG/IkG as a kH/I-module, or equivalently,

$$\overline{F} := \{x_1, \dots, x_m\} \subseteq (kG/IkG)^{\times}$$

is a basis for a crossed product decomposition $kG/IkG = kH/I * F$. We will say that this decomposition is *standard* if each x_i is the image of some $g_i \in G$ under the natural map $G \to (kG/IkG)^\times$.

Now finally we can prove the main theorem of this section.

Let G be a compact p-adic analytic group and H an open normal subgroup containing Δ^+ with H/Δ^+ a pro-p group. Suppose k is a finite field of characteristic p. Fix a minimal prime M of kH, and $e \in \mathrm{cpi}^{\overline{k\Delta^+}}(M)$, and suppose that e is centralised by G.

As H satisfies the conditions of Theorem 4.1.5, there exist a finite field extension k'/k and a positive integer t, and isomorphisms

$$\Psi : e \cdot \overline{kH} \to e \cdot \overline{k\Delta^+} \underset{k'}{\otimes} k'N,$$

$$\psi : e \cdot \overline{kH} \to M_t\Big(k'[[H/\Delta^+]]\Big).$$

(Note that, here, we have identified the two rings $e \cdot \overline{k\Delta^+} \underset{k}{\otimes} kN$ and $e \cdot \overline{k\Delta^+} \underset{k'}{\otimes} k'N$ as in Lemma 1.5.1(iii).)

Fix a crossed product decomposition

$$k'[[G/\Delta^+]] = k'[[H/\Delta^+]] \underset{\langle\sigma,\tau\rangle}{*} (G/H) \tag{‡}$$

which is *standard* in the sense of Definition 4.2.9.

Theorem 4.2.10. Notation as above. Then there exists

$$\alpha \in Z^2_\sigma\Big(G/H,\ Z(k'[[H/\Delta^+]]^\times)\Big)$$

such that Ψ extends to an isomorphism

$$\tilde{\Psi} : e \cdot \overline{kG} \to e \cdot \overline{k\Delta^+} \underset{k'}{\otimes} \big(k'[[G/\Delta^+]]\big)_{\alpha},$$

where the 2-cocycle twist $(k'[[G/\Delta^+]])_{\alpha}$, as defined in Definition 4.2.2, is taken with respect to the standard crossed product decomposition (‡) above.

Hence ψ also extends to an isomorphism

$$\tilde{\psi} : e \cdot \overline{kG} \to M_t\Big(\big(k'[[G/\Delta^+]]\big)_{\alpha}\Big).$$

Proof. We know that $e \cdot \overline{k\Delta^+} \cong M_t(k')$ for some t and k' by Lemma 1.5.1, and so $e \cdot \overline{k\Delta^+}$ contains a set $\{e_{ij}\}$ of t^2 matrix units. Set

$$Z_H := Z_{e \cdot \overline{kH}}\Big(\{e_{ij}\}\Big) \subseteq e \cdot \overline{kH},$$

the centraliser of all of these matrix units, and likewise $Z_G \subseteq e \cdot \overline{kG}$ and $Z_{\Delta^+} \subseteq e \cdot \overline{k\Delta^+}$. Then the statement and proof of [21, 6.1.5] show that

$$e \cdot \overline{kH} \cong e \cdot \overline{k\Delta^+} \underset{Z_{\Delta^+}}{\otimes} Z_H$$

and

$$e \cdot \overline{kG} \cong e \cdot \overline{k\Delta^+} \underset{Z_{\Delta^+}}{\otimes} Z_G.$$

Since $e \cdot \overline{k\Delta^+} \cong M_t(k')$, it is clear that $Z_{\Delta^+} \cong k'$, the diagonal copy of k' inside $M_t(k')$. Using the isomorphism Ψ of Theorem 4.1.5, we can also understand the structure of Z_H:

$$\Psi(Z_H) = Z_{\Delta^+} \underset{k}{\otimes} k[[H/\Delta^+]] \cong k'[[H/\Delta^+]],$$

so Ψ restricts to an explicit isomorphism $Z_H \to k'[[H/\Delta^+]]$. Now we would like to understand the structure of Z_G.

As $F := G/H$ is finite, we may write $\{x_1, \dots, x_n\}$ for the basis of the crossed product (‡). This will be a set of representatives in G of $F = \{x_1H, \dots, x_nH\}$.

For each x_i, form $\widetilde{x}_i \in Z_G^\times$ as in equation (4.2.1). Then $e \cdot \overline{kG}$ is a free $e \cdot \overline{kH}$-module of rank n: $e \cdot \overline{kG}$ can be written as the internal direct sum

$$e \cdot \overline{kG} = \bigoplus_{i=1}^{n} \widetilde{x}_i(e \cdot \overline{kH}).$$

Intersecting both sides of this equation with Z_G gives

$$Z_G = \bigoplus_{i=1}^{n} \widetilde{x}_i Z_H,$$

showing that Z_G is a crossed product $Z_H * F$, and is therefore isomorphic to $k'[[H/\Delta^+]] * F$. Lemma 4.2.8 may now be restated to say that this $k'[[H/\Delta^+]] * F$ is just a central 2-cocycle twist of the decomposition (‡) of $k'[[G/\Delta^+]]$. This is the map $\tilde{\Psi}$, and the map $\tilde{\psi}$ then also follows from Lemma 1.5.1(iii). $\square$

Further, keeping the above notation, let A be an ideal of kH with $M \subseteq A$. Continuing as before to write $q : kG \to e \cdot \overline{kG}$ for the natural quotient map, we see by Theorem 4.1.5 that $\psi \circ q(A) = M_t(\mathfrak{a})$ for some ideal $\mathfrak{a}$ of $k'[[H/\Delta^+]]$.

Corollary 4.2.11. The following are equivalent:

(i) A is G-stable as an ideal of kH.

(ii) $\mathfrak{a}$ is (G/Δ^+)-stable as an ideal of $k'[[G/\Delta^+]]$.

(iii) $\mathfrak{a}$ is (G/Δ^+)-stable as an ideal of $(k'[[G/\Delta^+]])_\alpha$.

Moreover, when these conditions hold, we have

$$\tilde{\psi} \circ q(AkG) = M_t\Big(\mathfrak{a}\,\left(k'[[G/\Delta^+]]\right)_\alpha\Big).$$

Proof. The equivalence of statements (ii) and (iii) is clear since, by definition, the conjugation action of G/Δ^+ on the ring $k'[[G/\Delta^+]]$ is the same as the conjugation action of G/Δ^+ on the ring $(k'[[G/\Delta^+]])_\alpha$. The equivalence of (i) and (ii) follows easily from Lemma 4.2.8. Then

$$\begin{aligned}\tilde{\psi} \circ q(AkG) &= \left(\tilde{\psi} \circ q(A)\right) \cdot \left(\tilde{\psi} \circ q(kG)\right)\\ &= M_t(\mathfrak{a}) \cdot M_t\Big(\left(k'[[G/\Delta^+]]\right)_\alpha\Big)\\ &= M_t\Big(\mathfrak{a}\,\left(k'[[G/\Delta^+]]\right)_\alpha\Big).\end{aligned}$$ □

Proof of Theorem G. This follows from Theorem 4.2.10. □

Proof of Theorem H. This follows from Corollaries 3.2.3 and 4.2.11. □

4.3 Matrix units and the Peirce decomposition

From section 3.1 onwards, we often stipulated a stronger condition than in Lemma 1.5.1, namely that the conjugation action of G on $\overline{kG}$ should fix the idempotent e (in Notation 1.5.2). In general, e will have some non-trivial (but finite) G-orbit, so it will only make sense to consider $f \cdot \overline{kG}$, where $f = e|^G$.

The following result already gives us a lot of information:

Lemma 4.3.1. [21, 6.1.6] Let R be a ring, and let $1 = e_1 + e_2 + \cdots + e_n$ be a decomposition of 1 into a sum of orthogonal idempotents. Let G be a subgroup of the group of units of R, and assume that G permutes the set $\{e_1, e_2, \ldots, e_n\}$ transitively by conjugation. Then $R \cong M_n(S)$, where S is the ring $S = e_1 R e_1$. $\square$

For instance, if M is a faithful minimal prime of kG, $e \in \mathrm{cpi}^{\overline{k\Delta^+}}(M)$ and $f = e|^G$, this lemma implies that

$$f \cdot \overline{kG} \cong M_n(e \cdot \overline{kG} \cdot e),$$

and it is easy to show that

$$e \cdot \overline{kG} \cdot e = e \cdot \overline{kG_1}$$

where G_1 is the closed subgroup of elements of G (here identified with the natural subgroup of $(f \cdot \overline{kG})^\times$) that fix e under conjugation.

Proof of Theorem I. This follows from Lemma 4.3.1. $\square$

Now, if P is any ideal containing M, and the image of $f \cdot \overline{P}$ in $M_n(e \cdot \overline{kG_1})$ is $M_n(e \cdot \overline{Q})$ for some ideal Q (with Q containing JkG, and $\overline{Q}$ containing $1 - e$), it is easy to see that:

Lemma 4.3.2. *P is prime if and only if Q is prime.*

Proof. By Lemma 1.6.3, it suffices to show that $f \cdot \overline{P} \cong M_n(e \cdot \overline{Q})$ is prime if and only if $e \cdot \overline{Q}$ is prime; but this is true because Morita equivalence preserves primality (Lemma 1.6.5). $\square$

With a little more care, it is also possible to use the proof of Lemma 4.3.1 to show that

$$P^\dagger = \bigcap_{g \in G} (Q^\dagger)^g.$$

(See Lemmas 4.3.5 and 4.3.6 for a proof of this statement.)

Later, we will show that certain prime ideals P of kG are controlled by certain closed normal subgroups H containing Δ^+. By Lemma 1.6.3, it clearly suffices to show that

$$(f \cdot \overline{P} \cap f \cdot \overline{kH}) f \cdot \overline{kG} = f \cdot \overline{P}.$$

If now $f = e|^H$, we may apply Lemma 4.3.1 to reduce to the case when $f = e$, and then apply the isomorphism ψ of Theorem 4.2.10 and Lemma 1.6.4 to reduce the problem to a simpler one.

However, Lemma 4.3.1 is not always precise enough for our purposes. It may be the case that $f = e|^G \neq e|^H$, i.e. the G-orbit of e splits into more than one H-orbit: then $f \cdot \overline{kH}$ is not a full matrix ring, but a direct sum

$$f \cdot \overline{kH} = \left(f_H^{(1)} \cdot \overline{kH} \right) \oplus \dots \oplus \left(f_H^{(s)} \cdot \overline{kH} \right)$$

of several matrix rings (which may be non-isomorphic), and the same tools become messier to apply.

For this reason, it will be useful to keep track of the isomorphism in Lemma 4.3.1 more carefully, and so we will develop a more precise set of tools for handling this isomorphism.

Let R be a ring, and fix a subgroup $G \leq R^\times$. Suppose we have a G-orbit of mutually orthogonal idempotents $e_1, \dots, e_r \in R$ whose sum is 1. Recall the *Peirce decomposition* of R with respect to this set of idempotents,

$$R = \bigoplus_{i,j=1}^{r} R_{ij} = \begin{pmatrix} R_{11} & R_{12} & \dots & R_{1r} \\ R_{21} & R_{22} & \dots & R_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ R_{r1} & R_{r2} & \dots & R_{rr} \end{pmatrix},$$

where $R_{ij} := e_i R e_j$.

Remark. Each R_{ii} is naturally a ring with identity $1_{R_{ii}} = e_i$ under the multiplication inherited from R. Each R_{ij} is an (R_{ii}, R_{jj})-bimodule, and the restriction of the multiplication map $R \underset{R}{\otimes} R \to R$ gives a homomorphism of (R_{ii}, R_{kk})-bimodules $R_{ij} \underset{R_{jj}}{\otimes} R_{jk} \to R_{ik}$ for all i, j, k.

Let A be any ideal of R, and write $A_{ij} = A \cap R_{ij} = e_i A e_j$.

Lemma 4.3.3. $A_{ij} R_{kl} = \delta_{jk} A_{il}$ (where δ_{jk} is the Kronecker delta symbol).

Proof. If $j \neq k$, it is clear from the definitions that $A_{ij} R_{kl} = 0$.

Suppose $j = k$, and let $g \in G$ be such that $e_k g = g e_l$, so that $0 \neq e_k g e_l \in R_{kl}$. Then, given any $a \in A$, we can write

$$e_i a e_l = e_i a g^{-1} g e_l = (e_i a g^{-1} e_k)(e_k g e_l),$$

showing that $A_{il} \subseteq A_{ik} R_{kl}$. The reverse inclusion is trivial. □

In this section, we aim to study the relationship between an ideal $A \lhd R$ and the various ideals $A_{ii} \lhd R_{ii}$. To that end, write for convenience $S_i := R_{ii}$ and $B_i := A_{ii}$ from now on. Also, we have fixed the group G inside $R^\times$: its analogue inside $S_i^\times$ is $e_i G e_i$, which we note is isomorphic to $G_i := \mathbf{C}_G(e_i)$ in the natural way.

Recall from Definition 1.6.2 that, if I is an ideal of kG, we define

$$I^\dagger = (I + 1) \cap G = \ker(G \to (kG/I)^\times).$$

Below is the appropriate analogue for the current situation.

Definition 4.3.4. With notation as above,

$$A^\dagger = (A + 1_R) \cap G = \ker(G \to (R/A)^\times),$$

$$B_i^\dagger = (B_i + 1_{S_i}) \cap G_i = \ker(G_i \to (S_i/B_i)^\times).$$

The following lemma relates these groups.

Lemma 4.3.5.

(i) If $A \neq R$, then $A^\dagger \leq \bigcap_{i=1}^r G_i$.

(ii) $A^\dagger = \bigcap_{i=1}^r B_i^\dagger$.

(iii) The $\{B_i^\dagger\}$ are a G-orbit under conjugation.

Proof.

(i) Suppose not: then there exist some $i \neq j$ and some $g \in A^\dagger$ with $e_i g = g e_j$, so that $e_i g e_i = 0$. Then

$$g - 1 \in A \implies e_i(g-1)e_i \in A \implies e_i \in A,$$

but then by conjugating by elements of G we see that $e_k \in A$ for all k, and so $1 = \sum_k e_k \in A$, so $A = R$, which is a contradiction.

(ii) $\boxed{\leq}$ Fix i. If $g - 1 \in A$, then $g \in G_i$ by the previous lemma, so $e_i(g-1)e_i \in B_i$.

$\boxed{\geq}$ Let $g \in \bigcap_i B_i^\dagger$, so that $e_i g e_j = g e_i e_j = 0 \in A$ for all $i \neq j$, and $e_i(g-1)e_i \in B_i \subseteq A$ for all i. Then $g - 1 = \sum_{i \neq j} e_i g e_j + \sum_i e_i(g-1)e_i \in A$.

(iii) A is G-stable, so if $e_i^g = e_j$ then $B_i^g = (e_i A e_i)^g = e_j A e_j = B_j$. Also, $G_i^g = G_j$. It follows that $(B_i^\dagger)^g = B_j^\dagger$. $\square$

We finish by applying this to the problem mentioned at the beginning of this section. Recall the definition of *control* from Definition 1.6.1.

Lemma 4.3.6. Let G be a compact p-adic analytic group, H a closed normal subgroup containing Δ^+, and k a field of characteristic p. Let P be an ideal of kG

containing a prime ideal.

Write $e \in \mathrm{cpi}^{\overline{k\Delta^+}}(P)$, $f = e|^G$, where the G-orbit of $e = e_1$ is $\{e_1, \ldots, e_r\}$. For each $1 \leq i \leq r$, write G_i for the stabiliser in G of e_i (so that $e_i \cdot \overline{kG} \cdot e_i = e_i \cdot \overline{kG_i}$), and similarly $H_i = H \cap G_i$, and set Q_i equal to the preimage in kG_i of the ideal $e_i \cdot \overline{P} \cdot e_i \lhd e_i \cdot \overline{kG_i}$.

Then

(i) P is controlled by H if and only if each Q_i is controlled by H_i,

(ii) $P^\dagger = \bigcap_{i=1}^r Q_i^\dagger$.

Proof. Take R to be $f \cdot \overline{kG}$, and identify G with its image in $(f \cdot \overline{kG})^\times$. Let A be the ideal $f \cdot \overline{P}$, and B_i the ideal $e_i \cdot \overline{Q_i}$.

Write $D = f \cdot \overline{kH}$ and $D_i = e_i \cdot \overline{kH_i}$. By Lemma 1.6.3, it suffices to show: $(A \cap D)R = A$ if and only if $(B_i \cap D_i)S_i = B_i$ for each i.

$\boxed{\Rightarrow}$ Take the equation $(A \cap D)R = A$, and intersect it with S_i.

$\boxed{\Leftarrow}$ Note that $\bigoplus_i B_i = \bigoplus_i (B_i \cap D_i)S_i$ by assumption, and we have automatically that $(A \cap D)R \subseteq A$. Since $\bigoplus_i S_i \subseteq R$, we have that

$$\bigoplus_i B_i = \bigoplus_i (B_i \cap D_i)S_i \subseteq (A \cap D)R \subseteq A.$$

Hence

$$\left(\bigoplus_i B_i\right) R \subseteq (A \cap D)R \subseteq AR = A,$$

i.e.

$$\left(\bigoplus_i A_{ii}\right)\left(\bigoplus_{j,k} R_{jk}\right) \subseteq (A \cap D)R \subseteq A.$$

But the left hand side can easily be computed by Lemma 4.3.3 and is equal to

$$\bigoplus_{i,k} A_{ik}$$

– that is, A.

This shows that P is controlled by H, completing the proof of (i).

Comparing Definitions 1.6.2 and 4.3.4, we can see that $P^\dagger = A^\dagger$ and $Q_i^\dagger = B_i^\dagger$. Statement (ii) is now a direct consequence of Lemma 4.3.5(ii). $\square$

Chapter 5

p-valuations and crossed products

5.1 Separating a free abelian quotient

Let G be a p-valuable group with p-valuation ω, and let $\sigma \in \mathrm{Aut}(G)$. In this section and the next, we seek to establish conditions under which a given automorphism σ of G will preserve the "dominant" part of certain elements $x \in G$ (with respect to ω). That is, we are looking for a condition under which

$$\mathrm{gr}_\omega(\sigma(x)) = \mathrm{gr}_\omega(x).$$

Clearly it is necessary and sufficient that the following holds:

$$\omega(\sigma(x)x^{-1}) > \omega(x). \tag{5.1.1}$$

Our aim is to invoke the following technical result.

Theorem 5.1.1. 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 σ of G preserving L, so that σ induces an automorphism $\overline{\sigma}$ of G/L, and hence an automorphism $\hat{\sigma} = \varphi \circ \overline{\sigma} \circ \varphi^{-1}$ of $\mathbb{Z}_p^d$. Let M_σ be the matrix of $\hat{\sigma}$ with respect to the basis $\{e_1, \ldots, e_d\}$.

Suppose there exists some p-valuation ω on G with the following properties:

(i) (5.1.1) 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 $M_\sigma - 1 \in pM_d(\mathbb{Z}_p)$.

Before proving this, we will define a particular p-valuation on abelian p-valuable groups.

Definition 5.1.2. 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, $\omega(1) = \infty$.)

Lemma 5.1.3. Let A and t be as in the above definition.

(i) The (t, p)-filtration ω is a p-valuation on A.

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

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

Proof.

(i) This is a trivial check from the definition [13, III, 2.1.2].

(ii) By [13, III, 2.2.4], we see that

$$\alpha(a_1^{\lambda_1}\dots a_d^{\lambda_d}) = t + \inf_{1\leq i\leq d}\{v_p(\lambda_i)\},$$

which is precisely the (t,p)-filtration.

(iii) The subgroups A^{p^n} are clearly characteristic in A. $\square$

Remark. The (t,p)-filtration as defined above is equivalent to the definition given in [13, II, 3.2.1] for free abelian pro-p groups of finite rank.

Remark. Given an arbitrary p-valuable group G with p-valuation ω, and a closed normal subgroup K such that G/K is torsion-free, we may define the *quotient p-valuation* Ω induced by ω 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 [13, I, 2.1.7], and is modified to the case of filtered groups in [13, the remark after II, 1.1.4.1]. The specialisation from filtered groups to p-saturable groups is done in [13, III, 3.3.2.4], where it is proved that Ω is indeed still a p-valuation on G/K; and the general case is stated in [13, III, 3.1.7.6], and eventually proved in [13, IV, 3.4.2].

With this in mind, we remark the following: suppose ω satisfies hypothesis (iii) of Theorem 5.1.1. Then hypothesis (ii) is equivalent to the statement that the quotient filtration induced by ω on G/L is actually the (t,p)-filtration on G/L.

Proof of Theorem 5.1.1. Define the function $\Omega : \mathbb{Z}_p^d \to \mathbb{R} \cup \{\infty\}$ by

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

By the remark above, Ω 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

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

so by assumption (ii), $\Omega(e_i) = t$. Hence, by Lemma 5.1.3(ii), Ω 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 5.1.2),

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

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. □

5.2 Constructing p-valuations

In this subsection, we address the issue of hypotheses (ii) and (iii) of Theorem 5.1.1, by constructing a p-valuation on an arbitrary nilpotent p-valuable group satisfying certain nice technical properties. We will not address the case when the group in question is abelian.

Fix some $n \geq 2$, and write $\mathcal{U} := \mathcal{U}(GL_n(\mathbb{Z}_p))$ for the closed subgroup of $GL_n(\mathbb{Z}_p)$ consisting of unipotent upper triangular matrices, i.e.

$$\mathcal{U} = \begin{pmatrix} 1 & \mathbb{Z}_p & \mathbb{Z}_p & \dots & \mathbb{Z}_p \\ 0 & 1 & \mathbb{Z}_p & \dots & \mathbb{Z}_p \\ 0 & 0 & 1 & \dots & \mathbb{Z}_p \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix},$$

and write $\Gamma(k) := \Gamma(k, GL_n(\mathbb{Z}_p))$ for the kth congruence subgroup of $GL_n(\mathbb{Z}_p)$, i.e.

$$\Gamma(k) = \{X \in GL_n(\mathbb{Z}_p) | X \equiv 1 \mod p^k\}.$$

Write $\varepsilon = 0$ if $p \neq 2$ and $\varepsilon = 1$ if $p = 2$.

Lemma 5.2.1. The group $\Gamma(1+\varepsilon)$ has p-valuation ω defined by

$$\omega(x) = k,$$

where k is the positive integer such that $x \in \Gamma(k) \setminus \Gamma(k+1)$.

Proof. This follows from [26, Proposition 2.1] and [9, Theorem 5.2]. $\square$

Recall from Lemma 2.1.2 that, if G is a non-abelian nilpotent p-valuable group, then there is some $n \geq 2$ for which there is a continuous embedding $G \to \mathcal{U}_n$. Recall also from Corollary 2.3.6 the *isolated lower central series* of a nilpotent p-valuable group G: if (γ_i) is the abstract lower central series of G, then defining $G_i := \mathrm{i}_G(\overline{\gamma_i})$, we have that (G_i) is a strongly central series for G consisting of isolated normal closed subgroups. We will also write $G' = G_2$.

Note that

$$\mathcal{U}_2 = \begin{pmatrix} 1 & \boxed{0} & \mathbb{Z}_p & \mathbb{Z}_p & \dots & \mathbb{Z}_p \\ 0 & 1 & \boxed{0} & \mathbb{Z}_p & \dots & \mathbb{Z}_p \\ 0 & 0 & 1 & \boxed{0} & \dots & \mathbb{Z}_p \\ 0 & 0 & 0 & 1 & \dots & \mathbb{Z}_p \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 \end{pmatrix}, \ \mathcal{U}_3 = \begin{pmatrix} 1 & 0 & \boxed{0} & \mathbb{Z}_p & \dots & \mathbb{Z}_p \\ 0 & 1 & 0 & \boxed{0} & \dots & \mathbb{Z}_p \\ 0 & 0 & 1 & 0 & \dots & \mathbb{Z}_p \\ 0 & 0 & 0 & 1 & \dots & \mathbb{Z}_p \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 \end{pmatrix}, \dots$$

– that is, for $2 \leq k \leq n$, $\mathcal{U}_k$ is obtained from $\mathcal{U}$ by setting the entries in the first $k-1$ superdiagonals equal to zero.

Write $P = \mathrm{diag}(1, p, p^2, \dots, p^{n-1}) \in GL_n(\mathbb{Q}_p)$. Note that $P^{-n}\mathcal{U}P^n \leq \Gamma(n)$.

Define a sequence of p-valuations on $\mathcal{U}$ as follows. Let ω be the p-valuation on $\Gamma(1+\varepsilon)$ defined above. Then, for any $X \in \mathcal{U}$, and for all $r > 0$, define

$$\omega_r(X) = \omega(P^{-1-\varepsilon-r} X P^{1+\varepsilon+r}),$$

so that $\omega_{r+1}(X) = \omega_r(P^{-1}XP)$.

Lemma 5.2.2. Fix some $Y \in \mathcal{U}_k \setminus \mathcal{U}_{k+1}$ (so, in particular, $Y \neq 1$). Then we have $\omega_{r+1}(Y) \geq \omega_r(Y) + k$ for all r; moreover, there exists some integer N such that, for all $r > N$, we have $\omega_{r+1}(Y) = \omega_r(Y) + k$.

Proof. Write

$$Z := P^{-1-\varepsilon} Y P^{1+\varepsilon} = 1 + S_k + S_{k+1} + \dots + S_{n-1},$$

where each matrix S_ℓ has (i, j)-entry equal to zero for $j - i \neq \ell$. (That is, S_ℓ is the ℓ-th superdiagonal of Z.) By assumption, $Y \in \mathcal{U}_k \setminus \mathcal{U}_{k+1}$, so $S_k \neq 0$.

It is easy to see that

$$P^{-r}ZP^{r} = 1 + p^{rk}S_k + p^{r(k+1)}S_{k+1} + \cdots + p^{r(n-1)}S_{n-1}.$$

For any matrix $A = (a_{ij}) \in M_n(\mathbb{Z}_p)$, define $v(A) = \inf\{v_p(a_{ij})\}$. Then

$$\begin{aligned}
\omega_{r+1}(Y) &= \inf\{v(p^{(r+1)\ell}S_\ell)\} \\
&= \inf\{v(S_\ell) + (r+1)\ell\} \\
&\geq \inf\{v(S_\ell) + r\ell\} + k \\
&= \inf\{v(p^{r\ell}S_\ell)\} + k \\
&= \omega_r(Y) + k,
\end{aligned}$$

where all of the above infima are taken over the range $k \leq \ell \leq n-1$.

We now need to show that this inequality becomes an equality for sufficiently large r: that is, there exists some N such that, for $r > N$, we have

$$\inf_{k \leq \ell \leq n-1}\{v(S_\ell) + (r+1)\ell\} = \inf_{k \leq \ell \leq n-1}\{v(S_\ell) + r\ell\} + k. \tag{5.2.1}$$

It will be enough to show that, for all $r > N$, we have

$$\inf_{k \leq \ell \leq n-1}\{v(S_\ell) + r\ell\} = v(S_k) + rk, \tag{5.2.2}$$

i.e. this infimum is attained when $\ell = k$ for all $r > N$; or equivalently that

$$v(S_k) + rk \leq v(S_\ell) + r\ell \tag{5.2.3}$$

for all $k \leq \ell \leq n-1$: indeed, substituting (5.2.2) for both the left- and right-hand sides of (5.2.1) shows clearly that they are equal.

Rearranging the inequality (5.2.3), we get

$$r(\ell - k) \geq v(S_k) - v(S_\ell)$$

for all $k \leq \ell \leq n-1$, and so we see that it suffices to take $N > v(S_k)$. $\square$

Finally, we derive the following result.

Lemma 5.2.3. Let G be a non-abelian nilpotent p-valuable group. Choose an ordered basis $\{g_{d+1}, \dots, g_e\}$ for G', and extend it to an ordered basis $\{g_1, \dots, g_e\}$ for G by Lemma 1.3.2. To each p-valuation α, assign the real number

$$R(\alpha) = \inf_{d+1 \leq i \leq e} \{\alpha(g_i)\} - \inf_{1 \leq i \leq d} \{\alpha(g_i)\}.$$

Then there exists some p-valuation α for G with $R(\alpha) > 0$.

Remark. This ensures that there is some $1 \leq i \leq d$ with $\alpha(g_i) < \alpha(x)$ for *every* $x \in G'$.

Proof. First, choose an embedding $\psi : G \to \mathcal{U}$. Let k be the greatest integer such that $\psi(G) \leq \mathcal{U}_k$: then $\psi(G') \leq (\mathcal{U}_k)' \leq \mathcal{U}_{k+1}$. Hence we must have some $1 \leq i_0 \leq d$ such that $\psi(g_{i_0}) \in \mathcal{U}_k \setminus \mathcal{U}_{k+1}$, and for each $d+1 \leq i \leq e$ we must have $\psi(g_i) \in \mathcal{U}_{k+1}$.

Fix i_0 as above, and for any p-valuation α and any $d-1 \leq i \leq e$, write

$$R_0^i(\alpha) := \alpha(g_i) - \alpha(g_{i_0}),$$

so that

$$R(\alpha) \geq \inf_{d+1 \leq i \leq e} \{R_0^i(\alpha)\},$$

and so it will suffice to find α such that $R_0^i(\alpha) > 0$ for each $d+1 \leq i \leq e$.

Now fix some $d+1 \leq i \leq e$, and write $Y = \psi(g_{i_0})$ and $X = \psi(g_i)$. By Lemma 5.2.2, there is some large N_i such that the following hold for all $r > N_i$:

$$\omega_{r+1}(Y) = \omega_r(Y) + k,$$

$$\omega_{r+1}(X) \geq \omega_r(X) + k + 1.$$

Subtracting, we get

$$\omega_{r+1}(X) - \omega_{r+1}(Y) \geq \omega_r(X) - \omega_r(Y) + 1.$$

In other words, if we set $\alpha_r = \omega_r \circ \psi$ for all $r > N_i$, then

$$R_0^i(\alpha_{r+1}) > R_0^i(\alpha_r).$$

Now set $N = \sup_{d+1 \leq i \leq e}\{N_i\}$. Then, for all $d+1 \leq i \leq e$, the sequence $(R_0^i(\alpha_r))_{r>N}$ is an increasing sequence of integers; hence they must eventually all be positive. $\square$

Now we prove a general theorem about "lifting" p-valuations from torsion-free quotients.

Theorem 5.2.4. Let G be a p-valuable group, 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 α is a p-valuation on G, and β 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. α and β are both filtrations on G (in the sense of [13, II, 1.1.1]), and so by [13, II, 1.2.10], ω is also a filtration. Following [13, III, 2.1.2], for ω 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 α 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 α 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 β 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 ω. $\square$

Definition 5.2.5. Let G be a p-valuable group, and suppose we have a proper closed isolated normal subgroup L containing G'. Choose an ordered basis $\{g_{d+1}, \ldots, g_e\}$ for L, and extend it to an ordered basis $\{g_1, \ldots, g_e\}$ for G by Lemma 1.3.2. We will say that ω satisfies property (A_L) if it satisfies hypotheses (ii) and (iii) of Theorem 5.1.1, i.e.

$$\left.\begin{array}{lr} & \omega(g_1) = \cdots = \omega(g_d), \\ \text{and, for all } \ell \in L, & \omega(g_1) < \omega(\ell). \end{array}\right\} \qquad (\mathsf{A}_L)$$

Corollary 5.2.6. Let G be a nilpotent p-valuable group, and suppose we have a proper closed isolated normal subgroup L containing the isolated derived subgroup G'. Then there exists some p-valuation ω for G satisfying (A_L).

Proof. Let α_1 be a p-valuation for G satisfying $R(\alpha_1) > 0$ as in Lemma 5.2.3. Take an ordered basis $\{g_{d+1}, \dots, g_e\}$ for L and extend it to an ordered basis $\{g_1, \dots, g_e\}$ for G by Lemma 1.3.2, as in Definition 5.2.5. Fix two numbers t_1 and t_2 satisfying

$$(p-1)^{-1} < t_2 < t_1 \leq \inf_{1\leq i\leq e} \alpha(g_i).$$

Applying Theorem 5.2.4 with $N = G'$ and $\overline{\beta_1}$ the (t_1, p)-filtration on G/G', we see that $\alpha_2 = \inf\{\alpha_1, \beta_1\}$ is a p-valuation for G, and by construction α_2 satisfies $(\mathsf{A}_{G'})$. Now let $\overline{\beta_2}$ be the (t_2, p)-filtration on G/L, and apply Theorem 5.2.4 again to see that $\omega = \inf\{\alpha_2, \beta_2\}$ is a p-valuation for G and satisfies (A_L). $\square$

Remark. Suppose that L is characteristic. If ω satisfies (A_L) as above, write $t := \omega(g_1)$. Then, for any automorphism σ of G and any $1 \leq i \leq d$, we have

$$\omega(\sigma(g_i)) = t.$$

This follows from Lemma 5.1.3(iii). Indeed, by construction, we have $G_t = G$, and $G_{t^+} = G^p \cdot L$, an open normal subgroup; and since L is characteristic, G_{t^+} is characteristic.

5.3 Invariance under the action of a crossed product

Definition 5.3.1. Let R be a ring, and fix a subgroup $G \leq R^\times$; let F be a group. Fix a crossed product

$$S = R \underset{\langle\sigma,\tau\rangle}{*} F.$$

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 $x \in G, f \in F$. (N_G)

The image $\tau(F,F)$ normalises G. (N'_G)

The image $\tau(F,F)$ is a subset of G. (P_G)

In the case when G is p-valuable, consider the set of p-valuations of G. Then $\mathrm{Aut}(G)$ acts on this set as follows: given an automorphism φ of G and a p-valuation ω of G, we may define a p-valuation $\varphi \cdot \omega$ on G by setting, for all $x \in G$,

$$(\varphi \cdot \omega)(x) = \omega(x^\varphi).$$

Remark. We have written φ on the left for ease of notation, but in fact this is a *right* action: given φ, ψ, we have $(\psi \cdot (\varphi \cdot \omega))(x) = (\varphi \cdot \omega)(x^\psi) = \omega((x^\psi)^\varphi)$.

When S satisfies (N'_G), we get a map $\rho : \tau(F,F) \to \mathrm{Aut}(G)$ (with elements of $\tau(F,F)$ acting by conjugation), so it will make sense to consider the following property:

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

Lemma 5.3.2. 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 ω 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

$$\begin{aligned}(t \cdot \omega)(x) &= \omega(x^t) \\ &= \omega(t^{-1}xt) \\ &= \omega(x \cdot [x, t]) \\ &\geq \min\{\omega(x), \omega([x, t])\} = \omega(x),\end{aligned}$$

and so (by symmetry) $\omega(t^{-1}xt) = \omega(x)$.

$\square$

Definition 5.3.3. Recall, from Definition 4.2.2, that if we have a fixed crossed product

$$S = R \underset{\langle\sigma,\tau\rangle}{*} F \tag{5.3.1}$$

and a 2-cocycle

$$\alpha \in Z^2_\sigma(F, Z(R^\times)),$$

then we may define the ring

$$S_\alpha = R \underset{\langle \sigma, \tau\alpha \rangle}{*} F,$$

the *2-cocycle twist (of R, by α, with respect to the decomposition (5.3.1))*.

Lemma 5.3.4. Continuing with the notation above,

(i) S satisfies (N_G) if and only if S_α satisfies (N_G).

(ii) S satisfies (Q_G) if and only if S_α satisfies (Q_G).

Proof.

(i) Trivial from Definitions 5.3.1 and 5.3.3.

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

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

Lemma 5.3.5. If S satisfies (N_G), then, given any $g \in F$ and p-valuation ω on G, the function $g \cdot \omega$ given by

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

is again a p-valuation. 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 $g, h \in F$,

$$\begin{aligned}(g \cdot (h \cdot \omega))(x) &= h \cdot \omega(x^{\sigma(g)}) \\ &= \omega(x^{\sigma(g)\sigma(h)}) \\ &= \omega(x^{\sigma(gh)\tau(g,h)}) \\ &= \omega(x^{\sigma(gh)}) && \text{by } (\mathsf{Q}_G) \\ &= (gh \cdot \omega)(x). \end{aligned}$$ $\square$

The following lemma will finally allow us to prove the existence of a p-valuation sufficiently "nice" for our purposes.

Lemma 5.3.6. Suppose S satisfies (N_G) and (Q_G), so that σ induces an action of F on the set of p-valuations as in the above lemma. Let ω be a p-valuation. If the F-orbit of ω is finite, then $\omega'(x) = \inf_{g \in F}(g \cdot \omega)(x)$ defines an F-invariant p-valuation.

Furthermore, if L is a closed isolated characteristic subgroup of G containing G', and ω satisfies (A_L) (as in Definition 5.2.5), then ω' satisfies (A_L).

Proof. The function ω' satisfies condition [13, III, 2.1.2.2], since the F-orbit of ω is finite, and is hence a p-valuation that is F-stable by the remark in [13, III, 2.1.2].

Suppose ω satisfies (A_L). That is, for some $t > (p-1)^{-1}$, ω 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 5.1.3(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 ω' also satisfies (A_L). $\square$

Definition 5.3.7. 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 Definition 4.2.9 that the crossed product decomposition

$$kG/PkG = kH/P \underset{\langle\sigma,\tau\rangle}{*} F$$

is *standard* if the basis $\overline{F}$ is a subset of the image of the map

$$G \hookrightarrow (kG/PkG)^{\times}.$$

Lemma 5.3.8. Suppose that $kG/PkG = kH/P \underset{\langle\sigma,\tau\rangle}{*} F$ is a standard crossed product decomposition. Take any $\alpha \in Z^2_\sigma(F, Z((kH/P)^\times))$, and form the central 2-cocycle twist $(kG/PkG)_\alpha$ (Definition 4.2.2) with respect to this decomposition. Consider H as a subgroup of $(kH/P)^\times$: then conjugation by elements of $\overline{G}$ inside $((kG/PkG)_\alpha)^\times$ induces a group action of F on the set of p-valuations of H, as in Lemma 5.3.5.

Remark. As the notation suggests, this lemma simply says that the action of F on H, via σ, 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 5.3.2(iii), kG/PkG also satisfies (Q_H). Now Lemma 5.3.4 shows that $(kG/PkG)_\alpha$ also satisfies (N_H) and (Q_H), so that σ induces a group action of F on the p-valuations of H inside $(kG/PkG)_\alpha$ by Lemma 5.3.5. □

Let L be a closed isolated characteristic subgroup of H containing H'.

Corollary 5.3.9. With notation as above, we can find an F-stable p-valuation ω on H satisfying (A_L).

Proof. This now follows immediately from Corollary 5.2.6 and Lemma 5.3.6. □

Chapter 6

A graded ring

6.1 Generalities on ring filtrations

Definition 6.1.1. 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 6.1.2. 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 $0 = v(1) = v(uu^{-1}) \geq v(u) + v(u^{-1})$. 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 $v(xu) = v(x)$. $\square$

We will fix the following notation for this subsection.

Notation 6.1.3. Let G be a p-valuable group equipped with the p-valuation ω, and k a field of characteristic p. Take an ordered basis (defined in [4, 4.2]) $\{g_1, \ldots, g_d\}$ for G, and write $b_i = g_1 - 1 \in kG$ for all $1 \leq i \leq d$. As in [4], we make the following definitions:

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

Definition 6.1.4. With notation as above, let w be the valuation on kG defined in [4, 6.2], given by

$$\sum_{\alpha \in \mathbb{N}^d} \lambda_\alpha \mathbf{b}^\alpha \mapsto \inf_{\alpha \in \mathbb{N}^d} \big\{ \langle \alpha, \omega(\mathbf{g}) \rangle \mid \lambda_\alpha \neq 0 \big\}.$$

Note that, in light of this formula [4, Corollary 6.2(b)], and by the construction [13, 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 $\{g_1^\varphi, \ldots, g_d^\varphi\}$ is another ordered basis of G; hence if ω is φ-stable (in the sense that $\omega(g^\varphi) = \omega(g)$ for all

$g \in G$), then w is φ-stable (in the sense that $w(x^{\varphi}) = w(x)$ for all $x \in kG$, where φ here denotes the natural extension to kG).

We will need the following result:

Lemma 6.1.5. Let

$$b = b_0 + b_1 p + b_2 p^2 + \cdots \in \mathbb{Z}_p,$$

$$n = n_0 + n_1 p + n_2 p^2 + \cdots + n_s p^s \in \mathbb{N},$$

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

$$\binom{b}{n} \equiv \prod_{i=0}^{s} \binom{b_i}{n_i} \mod p.$$

Proof. See e.g. [2, Theorem]. □

Corollary 6.1.6. Let $b \in \mathbb{Z}_p$, $n \in \mathbb{N}$. If

$$v_p\left(\binom{b}{n}\right) = 0, \tag{6.1.1}$$

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

$$\inf\left\{n \in \mathbb{N} \;\middle|\; v_p\left(\binom{b}{n}\right) = 0\right\} = p^{v_p(b)}.$$

Proof. From Lemma 6.1.5 above, we can see that

$$\binom{b}{n} \equiv 0 \mod p$$

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 6.1.5 that $n = p^{v_p(b)}$ satisfies (6.1.1), and is the least $n \in \mathbb{N}$ with $v_p(b) \leq v_p(n)$. $\square$

Theorem 6.1.7. Take any $x \in G$, and $t = \inf \omega(G)$. Then $w(x-1) > t$ implies $\omega(x) > t$.

Proof. Write $x = \mathbf{g}^\alpha$. In order to show that $\omega(\mathbf{g}^\alpha) > t$, 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 ith entry $\delta_{ij}p^{v_p(\alpha_j)}$. Then, of course,

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

and by Corollary 6.1.6, we have

$$\binom{\alpha}{\beta^{(j)}} \not\equiv 0 \mod p.$$

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

$$\begin{aligned}
\mathbf{g}^\alpha - 1 &= \prod_{1 \leq i \leq d} (1 + b_i)^{\alpha_i} - 1 & \text{(ordered product)} \\
&= \sum_{\beta \in \mathbb{N}^d} \iota \binom{\alpha}{\beta} \mathbf{b}^\beta - 1 \\
&= \sum_{\beta \neq 0} \iota \binom{\alpha}{\beta} \mathbf{b}^\beta,
\end{aligned}$$

so that

$$w(\mathbf{g}^\alpha - 1) = \inf \left\{ \langle \beta, \omega(\mathbf{g}) \rangle \;\middle|\; \beta \neq 0, \binom{\alpha}{\beta} \not\equiv 0 \mod p \right\}.$$

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

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

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

6.2 Constructing a suitable valuation

Let H be a nilpotent p-valuable group with centre Z. If k is a field of characteristic p, and $\mathfrak{p}$ is a faithful prime ideal of kZ, then by [4, Theorem 8.4], the ideal $P := \mathfrak{p}kH$ is again a faithful prime ideal of kH.

We will fix the following notation for this subsection.

Notation 6.2.1. Let G be a nilpotent-by-finite compact p-adic analytic group, with $\Delta^+ = 1$, and let $H = \mathbf{FN}_p(G)$ (as in Definition 2.5.3), here a *nilpotent* p-valuable radical, so that $\Delta = Z := Z(H)$. We will also write $F = G/H$.

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

Suppose further that the prime ideal $\mathfrak{p} \lhd kZ$ is invariant under conjugation by elements of G.

Choose a crossed product decomposition

$$kG/PkG = kH/P \underset{\langle\sigma,\tau\rangle}{*} F$$

which is *standard* in the sense of the notation of Corollary 5.3.9. Choose also any $\alpha \in Z^2_\sigma(F, Z((kH/P)^\times))$, and form as in Definition 4.2.2 the central 2-cocycle twist

$$(kG/PkG)_\alpha = kH/P \underset{\langle\sigma,\tau\alpha\rangle}{*} F.$$

Now the (right) divisor set $(kZ/\mathfrak{p}) \setminus \{0\}$ is G-stable by assumption, so by [22, Lemma 37.7], we may define the partial quotient ring

$$R := Q \underset{\langle\sigma,\tau\alpha\rangle}{*} F. \tag{6.2.1}$$

Our aim in this subsection is to construct an appropriate filtration f on the ring R. We will build this up in stages, following [4]. First, we define a finite set of valuations on Q'.

Definition 6.2.2. In [4, Theorem 7.3], Ardakov defines a valuation on $\mathbf{Q}(kH/P)$; let v_1 be the restriction of this valuation to Q', so that $v_1(x + \mathfrak{p}) \geq w(x)$ for all $x \in kZ$ (where w is as in Definition 6.1.4).

Lemma 6.2.3. σ 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 $x \in \mathbf{Q}(kZ/\mathfrak{p})$ 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 σ. □

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

Lemma 6.2.4. 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 [6, 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 [6, VI.3, Proposition 3], there exists a positive real number λ with $v_i = \lambda(g \cdot v_i)$, and so $v_i = \lambda^n(g^n \cdot v_i)$ (as the actions of λ 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 [6, VI.4, Proposition 6(c)], that the valuations $v_1, \ldots, v_s$ are independent. □

Definition 6.2.5. 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 6.2.6. $\mathrm{gr}_v Q' \cong \bigoplus_{i=1}^{s} \mathrm{gr}_{v_i} Q'$.

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 $\mathrm{gr}_v Q' \to \bigoplus_{i=1}^{s} \mathrm{gr}_{v_i} Q'$. The surjectivity of this map now follows from the Approximation Theorem [6, VI.7.2, Théorème 1], as the v_i are independent by Lemma 6.2.4. □

Next, we will extend the v_i and v from Q' to Q, as in the proof of [4, 8.6].

Notation 6.2.7. Continue with the notation above. Now, as H is p-valuable, and by Lemma 5.3.8, F acts on the set of p-valuations of H; hence, by Lemma 5.3.6 (or Corollary 5.3.9), we may choose a p-valuation ω which is F-stable. Fix such an ω, and construct the valuation w on kH from it as defined in Definition 6.1.4.

Let $\{y_{e+1}, \dots, y_d\}$ be an ordered basis for Z, and extend it to an ordered basis $\{y_1, \dots, y_d\}$ for H as in Lemma 1.3.2. For each $1 \leq j \leq e$, set $c_j = y_j - 1$ inside the ring kH/P.

Recall from [4, 8.5] that elements of Q may be written uniquely as

$$\sum_{\gamma \in \mathbb{N}^e} r_\gamma \mathbf{c}^\gamma,$$

where $r_\gamma \in Q'$ and $\mathbf{c}^\gamma := c_1^{\gamma_1} \dots c_e^{\gamma_e}$, so that $Q \subseteq Q'[[c_1, \dots, c_e]]$ as a left Q'-module.

Definition 6.2.8. For each $1 \leq i \leq s$, as in [4, proof of Theorem 8.6], we will define the valuation $f_i : Q \to \mathbb{R} \cup \{\infty\}$ by

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

(We remark here a slight abuse of notation: the domain of w is kH, and so $w(\mathbf{c}^\gamma)$ must be understood to mean $w(\mathbf{b}^\gamma)$, where $b_j = y_j - 1$ 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.)

Note in particular that $f_i|_{Q'} = v_i$, and $\mathrm{gr}_{f_i} Q$ is a commutative domain, again by [4, proof of Theorem 8.6].

Lemma 6.2.9. σ 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

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

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

Lemma 6.2.10. $f_1, \ldots, f_s$ 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 $y_k^g = z\mathbf{y}^\alpha$ for some $\alpha \in \mathbb{Z}_p^e$ and $z \in Z$, so that

$$\begin{aligned} c_k^g = y_k^g - 1 = z\mathbf{y}^\alpha - 1 & \\ &= (z-1) + z\left(\prod_{i=1}^{e}(1+c_i)^{\alpha_i} - 1\right) \qquad \text{(ordered product)} \\ &= (z-1) + z\left(\sum_{\beta \neq 0} \iota\binom{\alpha}{\beta}\mathbf{c}^\beta\right), \end{aligned}$$

and hence

$$\begin{aligned} (g \cdot f_i)(c_k) &= \inf\left\{ v_i(z-1), w(\mathbf{c}^\beta) \;\middle|\; \iota\binom{\alpha}{\beta} \neq 0 \right\} && \text{by Definition 6.2.8} \\ &\geq \inf\left\{ w(z-1), w(\mathbf{c}^\beta) \;\middle|\; \iota\binom{\alpha}{\beta} \neq 0 \right\} && \text{by Definition 6.2.2} \\ &= w(c_k^g), \end{aligned}$$

with this final equality following from [4, Lemma 8.5(b)]. But now, as ω has been chosen to be G-stable, w is also G-stable (see the remark in Definition 6.1.4), so that $w(c_k^g) = w(c_k)$.

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 $f_i(x) \leq f_j(x^{g^{-1}})$ 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 6.2.5:

Definition 6.2.11. 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 6.2.8).

Lemma 6.2.12. Take any $x \in Q$, and write it in standard form as

$$x = \sum_{\gamma \in \mathbb{N}^e} r_\gamma \mathbf{c}^\gamma.$$

Then we have

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

Proof. Immediate from Definitions 6.2.5, 6.2.8 and 6.2.11. $\square$

Now we can extend Lemma 6.2.6 to Q:

Lemma 6.2.13. $\mathrm{gr}_f Q \cong \bigoplus_{i=1}^{s} \mathrm{gr}_{f_i} Q$.

Proof. As in the proof of Lemma 6.2.6, we get an injective map

$$\mathrm{gr}_f Q \to \bigoplus_{i=1}^{s} \mathrm{gr}_{f_i} Q.$$

The proof of [4, 8.6] gives a map

$$(\mathrm{gr}_v(kZ/\mathfrak{p}))[Y_1, \ldots, Y_e] \to \mathrm{gr}_f(kH/P)$$

and isomorphisms

$$(\mathrm{gr}_{v_i}(kZ/\mathfrak{p}))[Y_1, \ldots, Y_e] \cong \mathrm{gr}_{f_i}(kH/P)$$

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

Now, $\mathrm{gr}\, kH$ is a gr-*free* [10, §I.4.1, p. 28] $\mathrm{gr}\, kZ$-module with respect to f and each f_i, and each of these filtrations is discrete on kH by construction (see [4, Corollary 6.2 and proof of Theorem 7.3]), so by [10, I.6.2(3)], kH is a *filt-free* kZ-module with respect to f and each f_i; and by [10, I.6.14], these maps extend to a map $(\mathrm{gr}_v Q')[Y_1, \ldots, Y_e] \to \mathrm{gr}_f Q$ and isomorphisms $(\mathrm{gr}_{v_i} Q')[Y_1, \ldots, Y_e] \cong \mathrm{gr}_{f_i} Q$ for each i.

Applying Lemma 6.2.10 to each $1 \leq i \leq s$, we get isomorphisms

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

which give a commutative diagram

$$\begin{tikzcd}
(\mathrm{gr}_v Q')[Y_1, \ldots, Y_e] \arrow[r, "\cong"] \arrow[d] & \bigoplus_{i=1}^{s} (\mathrm{gr}_{v_i} Q')[Y_1, \ldots, Y_e] \arrow[d, "\cong"] \\
\mathrm{gr}_f Q \arrow[r, hook] & \bigoplus_{i=1}^{s} \mathrm{gr}_{f_i} Q.
\end{tikzcd}$$

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

Now we return to the ring $R = Q * F$ defined in (7.3.2).

Definition 6.2.14. We can extend the filtration f on Q to an F-stable filtration on R by giving elements of the basis $\overline{F}$ value 0. That is, writing $\overline{F} = \{\overline{g}_1, \dots, \overline{g}_m\}$, any element of $Q * F$ can be expressed uniquely as $\sum_{r=1}^{m} \overline{g}_r x_r$ for some $x_r \in Q$: the assignment

$$\begin{aligned} Q * F &\to \mathbb{R} \cup \{\infty\} \\ \sum_{r=1}^{m} \overline{g}_r x_r &\mapsto \inf_{1 \leq r \leq m} \Big\{ f(x_r) \Big\} \end{aligned}$$

is clearly a filtration on $Q * F$ 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 λ,

$$\begin{aligned} (Q * F)_{\hat{f},\lambda} &= \bigoplus_{i=1}^{m} \overline{g_i}(Q_{f,\lambda}), \\ (Q * F)_{\hat{f},\lambda^+} &= \bigoplus_{i=1}^{m} \overline{g_i}(Q_{f,\lambda^+}), \end{aligned}$$

so that

$$\begin{aligned} \mathrm{gr}_{\hat{f}}(Q * F) &= \bigoplus_{\lambda \in \mathbb{R}} \left(\bigoplus_{i=1}^{m} \overline{g_i}(Q_{f,\lambda}/Q_{f,\lambda^+}) \right) \\ &= \bigoplus_{i=1}^{m} \overline{g_i} \left(\bigoplus_{\lambda \in \mathbb{R}} (Q_{f,\lambda}/Q_{f,\lambda^+}) \right) = \bigoplus_{i=1}^{m} \overline{g_i} \left(\mathrm{gr}_f(Q) \right). \end{aligned}$$

That is, given the data of a crossed product $Q*F$ as in (7.3.2), we may view $\mathrm{gr}_{\hat{f}}(Q*F)$ as $\mathrm{gr}_f(Q) * F$ in a natural way.

We will finally record this as:

Lemma 6.2.15.

$$\begin{aligned}\mathrm{gr}_f(Q * F) = \mathrm{gr}_f(Q) * F &\cong \left(\bigoplus_{i=1}^{s} \mathrm{gr}_{f_i} Q\right) * F\\ &\cong \left(\bigoplus_{i=1}^{s} (\mathrm{gr}_{v_i} Q')[Y_1, \dots, Y_e]\right) * F,\end{aligned}$$

where each $\mathrm{gr}_{f_i} Q$ (or equivalently each $\mathrm{gr}_{v_i} Q'$) is a domain (see Definition 6.2.8). F permutes the f_i (or equivalently the v_i) transitively by conjugation. $\square$

6.3 Automorphisms trivial on a free abelian quotient

We will fix the following notation for this subsection.

Notation 6.3.1. Let H be a nilpotent but non-abelian p-valuable group with centre Z. Write H' for the isolated derived group of H (Definition 2.3.7), and 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 7.2.3.) Fix a p-valuation ω on H satisfying (A_L) (which is possible by Corollary 5.3.9).

Let $\{g_{m+1}, \dots, g_n\}$ be an ordered basis for Z. Using Lemma 1.3.2 twice, extend this to an ordered basis $\{g_{l+1}, \dots, g_n\}$ for L, and then extend this to an ordered basis $\{g_1, \dots, g_n\}$ for H. Diagrammatically:

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

in the notation of the remark after Lemma 1.3.2. Here, $0 < l \leq m < n$, corresponding to the chain of subgroups $1 \lneq Z \leq L \lneq H$.

Let k be a field of characteristic p. As before, let $\mathfrak{p}$ be a faithful prime ideal of kZ, so that $P := \mathfrak{p}kH$ 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 $\alpha \in \mathbb{N}^m$, $\mathbf{b}^\alpha$ means the (ordered) product $b_1^{\alpha_1} \dots b_m^{\alpha_m} \in kH/P$,
- for each $\alpha \in \mathbb{Z}_p^m$, $\mathbf{g}^\alpha$ means the (ordered) product $g_1^{\alpha_1} \dots g_m^{\alpha_m} \in H$,
- for each $\alpha \in \mathbb{N}^m$, $\langle \alpha, \omega(\mathbf{g}) \rangle$ means $\displaystyle\sum_{i=1}^{m} \alpha_i \omega(g_i)$.

Note the use of m rather than n in each case. This means that every element $x \in H$ may be written uniquely as

$$x = z\mathbf{g}^\alpha$$

for some $\alpha \in \mathbb{Z}_p^m$ and $z \in Z$; and every element $y \in kH/P$ may be written uniquely as

$$y = \sum_{\gamma \in \mathbb{N}^m} r_\gamma \mathbf{b}^\gamma$$

for some elements $r_\gamma \in kZ/\mathfrak{p}$.

Recall the definitions of the filtrations w on kH (Definition 6.1.4), v on $kZ/\mathfrak{p}$ (Definition 6.2.5) and f on kH/P (Definition 6.2.11). We will continue to abuse notation slightly for w, as in Definition 6.2.8.

Recall also that, as we have chosen ω to satisfy (A_L), we have that

$$w(b_1) = \dots = w(b_l) < w(b_r)$$

for all $r > l$.

Let σ 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 σ as an automorphism of kH/P, preserving the subgroup $H \subseteq (kH/P)^{\times}$.

Corollary 6.3.2. 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

$$\sigma(b_i) - b_i = \sum_{\gamma \in \mathbb{N}^m} r_\gamma \mathbf{b}^\gamma,$$

for some $r_\gamma \in kZ$, and suppose that $f(\sigma(b_i) - b_i) > f(b_i)$. That is, by Lemma 6.2.12,

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

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

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

Case 1: $w(\mathbf{b}^\gamma) > w(b_i)$. Then, as w takes non-negative values on kH, we are already done.

Case 2: $w(\mathbf{b}^\gamma) \leq w(b_i)$. 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 [4, 6.2], r_γ must be a unit in kZ, and so $f(r_\gamma) = 0$ by Lemma 6.1.2, a contradiction.

Hence $w(r_\gamma) + w(\mathbf{b}^\gamma) > w(b_i)$ for all $\gamma \in \mathbb{N}^m$. But, as w is discrete by [4, 6.2], we may now take the infimum over all $\gamma \in \mathbb{N}^m$, and the inequality remains strict. $\square$

Let σ be an automorphism of H, and recall that H/L is a free abelian pro-p group of rank l. Choose a basis $e_1, \dots, e_l$ 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, σ induces an automorphism of H/L, which gives a matrix $M_\sigma \in GL_l(\mathbb{Z}_p)$ under this isomorphism.

Write

$$\overline{\omega} : H/L \to \mathbb{R} \cup \{\infty\}$$

for the quotient p-valuation on H/L induced by ω, i.e.

$$\overline{\omega}(xL) = \sup_{\ell \in L}\{\omega(x\ell)\}$$

– note that this is just the (t, p)-filtration (Definition 5.1.2), as we have chosen ω to satisfy (A_L). Then write

$$\Omega : \mathbb{Z}_p^l \to \mathbb{R} \cup \{\infty\}$$

for the map $\Omega = \overline{\omega} \circ j^{-1}$, the (t, p)-filtration on $\mathbb{Z}_p^l$ corresponding to $\overline{\omega}$ 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.

As earlier, we will write $\Gamma(1) = 1 + pGL_l(\mathbb{Z}_p)$, the open subgroup of $GL_l(\mathbb{Z}_p)$ whose elements are congruent to the identity element modulo p.

Corollary 6.3.3. 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 $1 \leq i \leq l$,

$$\begin{aligned} f(\sigma(b_i) - b_i) > f(b_i) &\implies w(\sigma(b_i) - b_i) > w(b_i) && \text{by Corollary 6.3.2,} \\ &\implies \omega(\sigma(g_i)g_i^{-1}) > \omega(g_i) && \text{by Theorem 6.1.7,} \end{aligned}$$

– which is condition (5.1.1). Now we may invoke Theorem 5.1.1. □

Corollary 6.3.4. Suppose now further that σ 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 σ induces the identity automorphism on H/L. $\square$

Proof. We have shown that $M_\sigma \in \Gamma(1)$, a p-valuable (hence torsion-free) group; and if σ has finite order, then M_σ must have finite order. So M_σ is the identity map. $\square$

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

Example 6.3.5. Let $p = 2$, and let

$$H = \overline{\langle x, y, z \mid [x, y] = z, [x, z] = 1, [y, z] = 1\rangle}$$

be the (2-valuable) $\mathbb{Z}_2$-Heisenberg group. Let σ be the automorphism sending x to x^{-1}, y to y^{-1} and z to z. Take $L = \overline{\langle z\rangle}$, and $P = 0$.

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

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

and so $\sigma(X) - X = X^2 - X^3 + \dots$ (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 $M_\sigma \neq 1$.

Chapter 7

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

7.1 X-inner automorphisms

Recall the notation $\mathrm{Xinn}_S(R; G)$ from Definition 4.2.3.

Lemma 7.1.1. *R a prime ring and $R{*}G$ a crossed product. Let $G_{\mathrm{inn}} := \mathrm{Xinn}_{R*G}(R; G)$.*

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

(ii) *If H is a subgroup of G containing G_{inn}, and $R * H$ is a prime ring, then $R * G$ 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 $\mathrm{Q}_s(R)$, and the fact that $Z(R)$ stays central in $\mathrm{Q}_s(R)$: see [22, §12] for details.

(ii) This follows from [22, Corollary 12.6]: if I is a nonzero ideal of $R * G$, then

$I \cap R * G_{\text{inn}}$ is nonzero, and hence $I \cap R * H$ is nonzero. $\square$

7.2 Properties of $\mathbf{FN}_p(G)$

We prove here some important facts about the group $\mathbf{FN}_p(G)$.

Lemma 7.2.1. Let G be a nilpotent-by-finite compact p-adic analytic group with $\Delta^+ = 1$. Let $H = \mathbf{FN}_p(G)$, and write

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

where H' denotes the isolated derived subgroup of H. Then $K = H$.

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

Secondly, suppose that H is p-saturated. By the same argument as in Lemma 2.4.3, 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 [13]. That is, we get a group representation $\mathrm{Ad} : K \to \mathrm{Aut}(\mathfrak{h})$, and $(\mathrm{Ad}(k) - 1)(\mathfrak{h}_i) \subseteq \mathfrak{h}_{i+1}$ for each $k \in K$ and each i. (Here, $\mathfrak{h}_i$ denotes the ith term in the lower central series for $\mathfrak{h}$.)

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

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

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

Furthermore, $\ker \mathrm{Ad}$ 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 Δ. But $\Delta = Z(H)$ by Lemma 2.5.1(ii).

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 Lemma 2.1.3, and so must be contained in H by definition of $\mathbf{FN}_p(G)$.

Now suppose H is not p-saturated. Conjugation by $k \in K$ induces the trivial automorphism on H/H', so by [13] it does also on $\operatorname{Sat}(H/H')$, which is naturally isomorphic to $\operatorname{Sat} H/(\operatorname{Sat} H)'$ by Lemma 2.3.2. This shows that $K \subseteq K_G(\operatorname{Sat} H)$. But now, writing $\mathfrak{h}$ for the Lie algebra associated to $\operatorname{Sat} H$, the same argument as above, *mutatis mutandis*, shows that $K_G(\operatorname{Sat} H) = H$. □

Some properties.

Lemma 7.2.2. Let G be a compact p-adic analytic group with $\Delta^+ = 1$, and write $H = \mathbf{FN}_p(G)$. If H is not abelian, then $H/Z = \mathbf{FN}_p(G/Z)$.

Proof. H/Z is a nilpotent p-valuable open normal subgroup of G/Z, so must be contained within $\mathbf{FN}_p(G/Z)$. Conversely, the preimage in G of $\mathbf{FN}_p(G/Z)$ is a central extension of Z by $\mathbf{FN}_p(G/Z)$, two nilpotent and torsion-free groups, and hence is nilpotent and torsion-free, so must be p-valuable by Lemma 2.1.3, which shows that it must be contained within H. □

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

Lemma 7.2.3. Let H be a nilpotent p-valuable group. If H is not abelian, then $H \neq \mathrm{i}_H(H'Z)$.

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 [13]. If $\mathfrak{h} = \mathfrak{h}_2\mathfrak{z}$ (writing $\mathfrak{h}_2$ for the second term in the lower central series of $\mathfrak{h}$), then by applying $[\mathfrak{h}, -]$ to both sides, we see that $\mathfrak{h}_2 = \mathfrak{h}_3$. But as $\mathfrak{h}$ is nilpotent, this implies that $\mathfrak{h}_2 = 0$, so that $\mathfrak{h}$ is abelian, a contradiction.

When H is not p-saturated: note that $\mathrm{i}_H(H'Z) = \mathrm{Sat}(H'Z) \cap H$, by Lemma 2.3.1, and so that $\mathrm{Sat}(H/\mathrm{i}_H(H'Z)) \cong \mathrm{Sat}(H)/\mathrm{Sat}(H'Z)$ by Lemma 2.3.2. Hence $H/\mathrm{i}_H(H'Z)$ has the same (in particular non-zero) rank as $\mathrm{Sat}(H)/\mathrm{Sat}(H'Z)$. □

Lemma 7.2.4. Let G be a nilpotent-by-finite compact p-adic analytic group with $\Delta^+ = 1$. Let $H = \mathbf{FN}_p(G)$, and assume that H is not abelian. Write

$$M := M_G(H) = \{x \in G \mid [H, x] \leq \mathrm{i}_H(H'Z)\},$$

where H' denotes the isolated derived subgroup of H and Z its centre. Then $M = H$.

Proof. Clearly $Z \leq M$. We will calculate M/Z.

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

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

$$(H/Z)' = \mathrm{i}_{H/Z}\big(\overline{[H,H]Z/Z}\big) = \mathrm{i}_{H/Z}\big(\overline{[H,H]}Z/Z\big),$$

so that

$$\mathrm{i}_H(H'Z)/Z = (H/Z)'.$$

But $x \in M$ if and only if $[H, x] \leq \mathrm{i}_H(H'Z)$, 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 7.2.1. So $M/Z = H/Z$, and hence $M = H$. $\square$

7.3 The extension theorem

Proposition 7.3.1. Let G be a nilpotent-by-finite compact p-adic analytic group with $\Delta^+ = 1$. Let $H = \mathbf{FN}_p(G)$, and write $F = G/H$. 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 5.3.7) decomposition

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

for some $\alpha \in Z^2_\sigma(F, Z((kH)^\times))$, as in Theorem 4.2.10. 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

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

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 Lemma 2.5.1, $\Delta \leq H$, and so we have $G = H$ and there is nothing to prove.

So suppose henceforth that $Z \lneq H$, and write $L := \mathrm{i}_H(H'Z)$, so that, by Lemma

7.2.3, we have $L \lneq H$. 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 $R * F'$, where R is a certain commutative domain and F' is a certain subgroup of F, with the following property: if $R * F'$ 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 4.2.3), so that $R * F'$ is a prime ring.

By Corollary 5.3.9, we can see that H admits an F-stable p-valuation ω satisfying (A_L). Hence, in the notation of §6.1, we may define the filtration w from ω as in Definition 6.1.4. Furthermore, we write

$$Q' = \mathbf{Q}(kZ/P \cap kZ), \qquad Q = Q' \underset{kZ}{\otimes} kN,$$

as in §6.2; and we endow Q with the F-orbit of filtrations f_i $(1 \leq i \leq s)$ and the filtration f of Definitions 6.2.8 and 6.2.11, defined in terms of the filtration w above.

By [18, 2.1.16(vii)], in order to show that the crossed product

$$kH/P \underset{\langle\sigma,\tau\alpha\rangle}{*} F \tag{7.3.1}$$

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

$$Q \underset{\langle\sigma,\tau\alpha\rangle}{*} F \tag{7.3.2}$$

is prime, where this crossed product is defined in §6.2. Then, by [10, II.3.2.7], it suffices to show that

$$\mathrm{gr}_f(Q * F) \tag{7.3.3}$$

is prime. Details of this graded ring are given in Lemma 6.2.15: in particular, note that

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

Now, as noted in Definition 6.2.8, each $\mathrm{gr}_{f_i} Q$ is a commutative domain, and by construction, F permutes the summands $\mathrm{gr}_{f_i} Q$ transitively. So by [22, Corollary 14.8] it suffices to show that

$$\mathrm{gr}_{f_1} Q * F' \tag{7.3.4}$$

is prime, where $F' = \mathrm{Stab}_F(f_1)$.

Notation 7.3.2. We set up notation in order to be able to apply the results of §6.3. Let $\{y_{m+1}, \dots, y_n\}$ be an ordered basis for Z, which we extend to an ordered basis $\{y_{l+1}, \dots, y_n\}$ for L, which we extend to an ordered basis $\{y_1, \dots, y_n\}$ for H. Set $b_i = y_i - 1 \in kH/P$, and let $Y_i = \mathrm{gr}_{f_1}(b_i)$ for all $1 \leq i \leq m$. Then

$$\mathrm{gr}_{f_1} Q \cong \left(\mathrm{gr}_{v_1} Q'\right)[Y_1, \dots, Y_m].$$

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

$$\left(\mathrm{gr}_{v_1} Q'\right)[Y_1, \dots, Y_m] * F'. \tag{7.3.5}$$

from (7.3.4). Writing $R := \left(\mathrm{gr}_{v_1} Q'\right)[Y_1, \dots, Y_m]$, we have now shown, by passing along the chain

$$(7.3.5) \to (7.3.4) \to (7.3.3) \to (7.3.2) \to (7.3.1),$$

that we need only show that $R * F'$ is prime.

Write F'_{inn} for the subgroup of F' acting on R by X-inner automorphisms in the crossed product (7.3.5), i.e.

$$F'_{\mathrm{inn}} = \mathrm{Xinn}_{R*F'}(R; F')$$

in the notation of Definition 4.2.3. By the obvious abuse of notation, we will denote this action as the map of sets $\mathrm{gr}\ \sigma : F' \to \mathrm{Aut}(R)$.

Take some $g \in F'$. If $\mathrm{gr}\ \sigma(g)$ acts non-trivially on R, then as R is commutative, we have $g \notin F'_{\mathrm{inn}}$. Hence, as by Lemma 7.1.1(ii) we need only show that $R*F'_{\mathrm{inn}}$ 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

$$\mathrm{gr}\ \sigma(g)(Y_i) = Y_i \Leftrightarrow f(\sigma(g)(b_i) - b_i) > f(b_i).$$

Now we see from Corollary 6.3.4 that $\sigma(g)$ induces the identity automorphism on H/L, and hence from Lemma 7.2.4 that $g \in H$. That is, F'_{inn} is the trivial group, so that $R * F'_{\mathrm{inn}} = R$ is automatically prime.

Case 2. Suppose some $x \in F$ does not centralise Z. Write F_{inn} for the subgroup of F acting by X-inner automorphisms on kH/P in the crossed product (7.3.1), i.e.

$$F_{\mathrm{inn}} := \mathrm{Xinn}_{(kG)_\alpha/P(kG)_\alpha}(kH/P; F).$$

Then, by Lemma 7.1.1(i), $x \notin F_{\mathrm{inn}}$; so F_{inn} is contained in $\mathbf{C}_F(Z)$, and we need only prove that the sub-crossed product $(kH/P) * \mathbf{C}_F(Z)$ is prime by Lemma 7.1.1(ii). This reduces the problem to Case 1. □

Proposition 7.3.3. Let G be a nilpotent-by-finite compact p-adic analytic group, and k a finite field of characteristic $p > 2$. Let $H = \mathbf{FN}_p(G)$, and write $F = G/H$.

Let P be a G-stable, almost faithful prime ideal of kH. Then PkG is prime.

Proof. Recall Notation 1.5.2. Let $e \in \mathrm{cpi}^{\overline{k\Delta^+}}(P)$, and write $f_H = e|^H$, $f = e|^G$. Then PkG is a prime ideal of kG if and only if $f \cdot \overline{PkG}$ is prime in $f \cdot \overline{kG}$.

Write $H_1 = \mathrm{Stab}_H(e)$ and $G_1 = \mathrm{Stab}_G(e)$. Then, by the Matrix Units Lemma 4.3.1, we get an isomorphism

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

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

$$f_H \cdot \overline{kH} \cong M_{s'}(e \cdot \overline{kH_1}),$$

under which $f_H \cdot \overline{P} \mapsto M_{s'}(e \cdot \overline{P_1})$, so that P_1 is prime by Morita equivalence (Lemma 1.6.5). We also know from Lemma 4.3.6 (or the remark after Lemma 4.3.2) that

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

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

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

for all $h \in H$, as $q(\Delta) = Z(q(H))$ by definition of H (see Lemma 2.5.1(ii)); and so

$$q\left(P^\dagger \cap \Delta\right) = q\left(P_1^\dagger \cap \Delta\right) = q(1).$$

But $q\left(P_1^\dagger\right)$ is a normal subgroup of the nilpotent group $q\left(H_1\right)$. 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 [23, 5.2.1]. That is, $P_1^\dagger \leq \Delta^+(H_1) = \Delta^+$.

Now, in order to show that $M_s(e \cdot \overline{P_1 kG_1})$ is prime, we may equivalently (by Morita equivalence) show that $e \cdot \overline{P_1 kG_1}$ is prime. By Theorem 4.2.10, we get an isomorphism

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

for some integer t, some finite field extension k'/k, and a central 2-cocycle twist (Definition 4.2.2) of $k'[[G_1/\Delta^+]]$ with respect to a standard crossed product decomposition

$$k'[[G_1/\Delta^+]] = k'[[H_1/\Delta^+]] \underset{\langle\sigma,\tau\rangle}{*} (G_1/H_1)$$

given by some

$$\alpha \in Z^2_\sigma\left(G_1/H_1, Z\left(\left(k'[[H_1/\Delta^+]]\right)^\times\right)\right).$$

Writing the image of $e \cdot \overline{P_1}$ as $M_t(\mathfrak{p})$ for some ideal $\mathfrak{p} \in k'[[H_1/\Delta^+]]$, we see by Corollaries 3.2.3 and 4.2.11 that $\mathfrak{p}$ is a faithful, (G_1/Δ^+)-stable prime ideal of $k'[[H_1/\Delta^+]]$. It now remains only to show that the extension of $\mathfrak{p}$ to $k'[[G_1/\Delta^+]]$ is prime; but this now follows from Proposition 7.3.1.

□

Proof of Theorem J. This follows from Proposition 7.3.3.

Chapter 8

Heights of primes and Krull dimension

8.1 Prime and G-prime ideals

Definition 8.1.1. Let G be a compact p-adic analytic group. Suppose the group G acts (continuously) on the ring R, and that the ideal $I \lhd R$ is G-stable. Then, following [22, §14], we will say that I is *G-prime* if, whenever $A, B \lhd R$ are G-stable ideals and $AB \subseteq I$, then either $A \subseteq I$ or $B \subseteq I$.

Lemma 8.1.2. Let G be a compact p-adic analytic group and H a closed normal subgroup.

(i) If P is a prime ideal of kG, then $P \cap kH$ is a G-prime ideal of kH. If H is open in G, then P is a minimal prime ideal above $(P \cap kH)kG$.

(ii) Let Q be a G-prime ideal of kH, and P any minimal prime of kH above Q. Then $Q = \bigcap_{x \in G} P^x$. Furthermore, the set of minimal primes of kG above Q is $\{P^x | x \in G\}$.

Proof.

(i) The former statement follows from [22, Lemma 14.1(i)], and the latter from [22, Theorem 16.2(i)].

(ii) This follows from [22, Lemma 14.2(i)(ii)]. □

Definition 8.1.3. Let P be a prime ideal of a ring R. Then we define the *height* of P to be the greatest integer $h(P) := r$ for which there exists a chain

$$P_0 \lneq P_1 \lneq \cdots \lneq P_r = P$$

of prime ideals in R (or ∞ if no such longest chain exists). Similarly, if the group G acts on R by automorphisms, and P is a G-prime ideal of R, then the *G-height* of P is the greatest integer $h_G(P) := r$ for which there exists a chain

$$P_0 \lneq P_1 \lneq \cdots \lneq P_r = P$$

of G-prime ideals in R (or ∞ if no such longest chain exists).

We note the following immediate consequence of the correspondence of Lemma 8.1.2:

Corollary 8.1.4. Let G be a compact p-adic analytic group and H an open normal subgroup. Take P a prime ideal of kG, and let Q be a minimal prime of kH above $P \cap kH$. Then $h(P) = h_G(P \cap kH) = h(Q)$. □

8.2 Inducing ideals

Definition 8.2.1. Let H be an open (not necessarily normal) subgroup of G, and let L be an ideal of kH. We define the *induced ideal* $L^G \lhd kG$ to be the largest (two-sided) ideal contained in the right ideal $LkG \underset{r}{\lhd} kG$. In other words, by [16, 2.1],

L^G is the annihilator of kG/LkG as a right kG-module, or by [22, Lemma 14.4(ii)],

$$L^G = \bigcap_{g \in G} L^g kG.$$

Lemma 8.2.2. Induction of ideals is *transitive*: if H and K are open subgroups of G with $H \leq K \leq G$, and $L \lhd kH$, then $L^G = (L^K)^G$.

Proof. Let N be an open normal subgroup of G contained in H, and write $\overline{(\cdot)}$ to denote the quotient by N, so that we have $kG = kN * \overline{G}$ with $\overline{H} \leq \overline{K} \leq \overline{G}$, and we may view L as an ideal of $kN * \overline{H}$. The result now follows from [17, Lemma 1.2(iii)]. □

8.3 Krull dimension

We recall some facts about Krull dimension, used here in the sense of Gabriel and Rentschler.

Definition 8.3.1. Let $0 \neq M$ be an R-module, and fix some ordinal α. We define the following notation inductively:

- $\mathrm{Kdim}(M) = 0$ if M is an Artinian module,
- $\mathrm{Kdim}(M) \leq \alpha$ if, for every descending chain

  $$M_0 \geq M_1 \geq M_2 \geq \dots$$

  of submodules of M, we have $\mathrm{Kdim}(M_i/M_{i+1}) < \alpha$ for all but finitely many i.

Of course, if there exists some α such that $\mathrm{Kdim}(M) \leq \alpha$, but we do not have $\mathrm{Kdim}(M) \leq \beta$ for any $\beta < \alpha$, then we write $\mathrm{Kdim}(M) = \alpha$.

Remark. Kdim(M) is a measure of complexity of the poset of submodules of M.

Kdim(M) may not be defined for some modules M – that is, we may not have Kdim(M) $\leq \alpha$ for any ordinal α. However, if M is a noetherian module, then Kdim(M) is defined [11, Lemma 15.3].

Definition 8.3.2. Suppose that Kdim(M) $= \alpha$. We say that M is *α-homogeneous* if Kdim(N) $= \alpha$ for all nonzero submodules N of M.

Examples 8.3.3.

(i) Nonzero Artinian modules are 0-homogeneous.

(ii) Prime rings R, as modules over themselves, are α-homogeneous (where we set α equal to Kdim(R_R)) [11, Exercise 15E].

(iii) The property of being α-homogeneous is inherited by products [11, Corollary 15.2] and (nonzero) submodules (by definition).

We now cite and adapt some standard results on Krull dimension.

Lemma 8.3.4.

(i) [16, 1.4(ii)] Let the ring R be α-homogeneous as a right R-module. If $x \in R$ satisfies Kdim(R/xR) $<$ Kdim(R), then x is a regular element of R.

(ii) [14, Théorème 5.3] Suppose B is a finite normalising extension of A, and let M be a B-module. Then Kdim(M_B) exists if and only if Kdim(M_A) does, and if so, then they are equal.

(iii) [11, Exercise 15R] If R is a right noetherian subring of a ring S such that S is finitely generated as an R-module, and M is a finitely generated S-module, then Kdim(M_S) $\leq$ Kdim(M_R).

Corollary 8.3.5. Suppose $A \subseteq C \subseteq B$ are right noetherian rings, and B is a finite normalising extension of A. Let M be a finitely generated B-module. Then, if $\mathrm{Kdim}(M_B)$ exists, we have

$$\mathrm{Kdim}(M_A) = \mathrm{Kdim}(M_C) = \mathrm{Kdim}(M_B).$$

Proof. This follows immediately from Lemma 8.3.4(ii) and two applications of Lemma 8.3.4(iii). □

Lemma 8.3.6. Let G be a compact p-adic analytic group, H an open subgroup of G, and k a field of characteristic p. Let M be a finitely generated kG-module.

(i) $\mathrm{Kdim}(M_{kG}) = \mathrm{Kdim}(M_{kH})$.

(ii) Suppose that $M = WkG$ for some submodule W of M_{kH}. Then we have $\mathrm{Kdim}(M_{kG}) = \mathrm{Kdim}(W_{kH})$.

(iii) M_{kG} is α-homogeneous if and only if M_{kH} is α-homogeneous.

Proof. (Adapted from [16, 1.4(iii)-(v)].)

(i) Let N be the (open) largest normal subgroup of G contained in H, so that kG is a finite normalising extension of kN. Now apply Corollary 8.3.5.

(ii) Let N be as in (i). Then, by (i), it suffices to prove that $\mathrm{Kdim}(M_{kN}) = \mathrm{Kdim}(W_{kN})$. But, as a kN-module, M is a finite sum of modules $(Wg)_{kN}$ for various $g \in G$, and these are all isomorphic, so in particular have isomorphic submodule lattices and therefore the same Kdim.

(iii) It is clear from the definition that, if M_{kH} is α-homogeneous, then M_{kG} is α-homogeneous. Conversely, suppose that M_{kG} is α-homogeneous, and let W be a nonzero submodule of M_{kH}. Then $(WkG)_{kG}$ is a nonzero submodule of M_{kG}, so has Krull dimension α by assumption, and hence also $\mathrm{Kdim}(W_{kH}) = \alpha$ by (ii). □

Lemma 8.3.7. Let G be a finite group, H a subgroup, and $R * G$ a fixed crossed product. Fix a semiprime ideal I of $R * G$. If $R * G/I$ is α-homogeneous, then $R * H/(I \cap R * H)$ is α-homogeneous.

Proof. (Adapted from [7, Lemma 4.2(i)].) Let M be a nonzero right ideal of the ring $R * H/(I \cap R * H)$, and write $\beta = \mathrm{Kdim}(M_{R*H})$. We wish to show that $\beta = \alpha$.

M is a right module over both $R * H$ and R; and $R * G/I$ is a right module over both $R * G$ and R. As $R * G$ and $R * H$ are both finite normalising extensions of R, we may apply Lemma 8.3.4(ii) to both of these situations to see that

$$\beta = \mathrm{Kdim}(M_{R*H}) = \mathrm{Kdim}(M_R)$$

and

$$\alpha = \mathrm{Kdim}((R * G/I)_{R*G}) = \mathrm{Kdim}((R * G/I)_R).$$

Now, as right R-modules, we have

$$R * H/(I \cap R * H) \cong (R * H + I)/I \leq R * G/I,$$

and so M is isomorphic to some nonzero R-submodule of $R * G/I$. In particular, this means that

$$\beta = \mathrm{Kdim}(M_R) \leq \mathrm{Kdim}((R * G/I)_R) = \alpha.$$

But now $(R*G/I)_R$ is α-homogeneous by Corollary 8.3.5, so we must have $\beta = \alpha$. $\square$

Corollary 8.3.8. Let G be a compact p-adic analytic group, H be an open subgroup of G, and N the largest open normal subgroup of G contained in H. Take k to be a field of characteristic p, and let Q be a prime ideal of kH, $I = Q^G \cap kN$, and $\alpha = \mathrm{Kdim}(kH/Q)$. Then kH/Q, kG/Q^G, kG/IkG are all α-homogeneous rings.

Proof. As we observed in Example 8.3.3(ii), kH/Q is already α-homogeneous, as it is prime of Krull dimension α.

We know from Definition 8.2.1 that the ideal Q^G can be written as $\bigcap_{g\in G} Q^g kG$, and that this intersection can be taken to be finite. Hence, as a right kG-module, kG/Q^G is isomorphic to a (nonzero) submodule of the direct product of the various (finitely many) $kG/Q^g kG$; and each $kG/Q^g kG$ is generated as a kG-module by kH^g/Q^g, which is ring-isomorphic to kH/Q. Hence $\mathrm{Kdim}(kG/Q^G) = \mathrm{Kdim}(kH/Q)$ by Lemma 8.3.4(ii).

Finally, as $Q^G = \bigcap_{g\in G}(QkG)^g$, we see that

$$I = \bigcap_{g\in G}(QkG)^g \cap kN = \bigcap_{g\in G}(QkG \cap kN)^g = \bigcap_{g\in G}(Q \cap kN)^g,$$

and so, as above, kN/I is a (nonzero) subdirect product of the various $kN/(Q\cap kN)^g$, which are all ring-isomorphic to $kN/Q\cap kN$; now Lemma 8.3.7 implies that $kN/Q\cap kN$ is α-homogeneous, so kN/I is also, and kG/IkG is generated as a kG-module by kN/I, so finally kG/IkG also inherits this property. □

We borrow a result from the standard proof of Goldie's theorem.

Lemma 8.3.9. [29, Lemma 3.13] Suppose R is a semiprime ring, satisfying the ascending chain condition on right annihilators of elements, and which does not contain an infinite direct sum of nonzero right ideals. If I is an *essential* right ideal of R (i.e. a right ideal that has nonzero intersection $I \cap J$ with each nonzero right ideal J of R), then I contains a regular element. □

These hypotheses are satisfied when R is G-prime and noetherian, for example.

Proposition 8.3.10. With notation as in Corollary 8.3.8, suppose P is a prime ideal of kG containing Q^G. If P is minimal over Q^G, then $h(P) = h(Q)$.

Proof. First, set $I = Q^G \cap kN$. This is a G-prime ideal contained in $P \cap kN$.

Suppose for contradiction that the inclusion $I \subseteq P \cap kN$ is strict.

First, we will show that $P \cap kN/I$ is essential as a right ideal inside kN/I. Indeed, the left annihilator L in kN/I of $P \cap kN/I$ is a G-invariant ideal which annihilates the nonzero G-invariant ideal $P \cap kN/I$, so we must have $L = 0$; and so, given any right ideal T of kN/I having zero intersection with $P \cap kN/I$, as we must have $T \leq L$, we conclude that $T = 0$.

Hence, by Lemma 8.3.9, we may find an element $c \in P \cap kN \subseteq kN$ which is regular modulo I. As kG/IkG is a free kN/I-module, c may also be considered as an element of $P \subseteq kG$ which is regular modulo IkG. Hence

$$\begin{aligned}
&\mathrm{Kdim}\big(kG/(Q^G + ckG)\big)_{kG} \\
&\qquad \leq \mathrm{Kdim}\big(kG/(IkG + ckG)\big)_{kG} && \text{as } IkG + ckG \subseteq Q^G + ckG \\
&\qquad < \mathrm{Kdim}(kG/IkG)_{kG} && \text{by Lemma 8.3.4(i)} \\
&\qquad = \mathrm{Kdim}(kG/Q^G)_{kG} && \text{by Corollary 8.3.8,}
\end{aligned}$$

which, again by Lemma 8.3.4(i), shows that $c \in P$ is regular modulo Q^G.

However, we may now deduce from a reduced rank argument that P cannot be minimal over Q^G, as follows. Write ρ for the reduced rank [11, §11, Definition] of a right module over the semiprime noetherian (hence Goldie) ring $R = kG/Q^G$, and write $\overline{(\cdot)}$ for images under the map $kG \to R$. Now, $c \in P$ implies $\bar{c}R \subseteq \overline{P}$, and so by [11, Lemma 11.3] we have $\rho(R/\bar{c}R) \geq \rho(R/\overline{P})(\geq 0)$. Further, if $\bar{c}$ is a regular element of R, then $\bar{c}R \cong R$ as right R-modules, so $\rho(R/\bar{c}R) = 0$, again by [11, Lemma 11.3]. But now [11, Exercise 11C] implies that $\overline{P}$ cannot be a minimal prime of R.

This contradicts the assumption we made at the start of the proof, and so we have shown that $P \cap kN = Q^G \cap kN$.

We observed during the proof of Corollary 8.3.8 that

$$Q^G \cap kN = \bigcap_{g \in G} (Q \cap kN)^g.$$

But Q is a prime ideal of kH, so $Q \cap kN$ is an H-prime ideal of kN, so may be written as

$$Q \cap kN = \bigcap_{h \in H} Q_0^h$$

for some prime ideal Q_0 of kN. Combining these two shows that

$$(P \cap kN =) Q^G \cap kN = \bigcap_{g \in G} Q_0^g.$$

Now, by applying [22, corollary 16.8] to both $P \cap kN$ and $Q \cap kN$, we have that

$$h(P) = h(Q_0) = h(Q)$$

as required. $\square$

Chapter 9

Control theorem

9.1 The abelian case

We will require some facts about prime ideals in power series rings.

Lemma 9.1.1. Let A be a free abelian pro-p group of finite rank and B a closed isolated (normal) subgroup. Take k to be a field of characteristic p. Write $\mathrm{Spec}^B(kA)$ for the set of primes of kA that are controlled by B. Then the maps

$$\mathrm{Spec}^B(kA) \leftrightarrow \mathrm{Spec}(kB)$$
$$P \mapsto P \cap kB$$
$$QkA \mapsfrom Q$$

are well-defined and mutual inverses, and preserve faithfulness.

Proof. If P is a prime ideal of kA, then $P \cap kB$ is an A-prime ideal (and hence a prime ideal) of kB by Lemma 8.1.2(i).

Conversely, note that, as B is isolated in A, the quotient A/B is again free abelian pro-

p; so we may write $A = B \oplus C$, where the natural quotient map $A \to A/B$ induces an isomorphism $A/B \cong C$. Now, if Q is a prime ideal of kB, then $kA/QkA = (kB/Q)[[C]]$ is a power series ring with coefficients in the commutative domain kB/Q, and is hence itself a domain.

It follows from [3, Lemma 5.1] that $QkA \cap kB = Q$, and by assumption, if P is controlled by B then we already have $(P \cap kB)kA = P$.

Now suppose the prime ideals $P \lhd kA$ and $Q \lhd kB$ correspond under these maps. Then, again viewing A as $B \oplus C$, we may similarly consider kA/P as the completed tensor product $kB/Q \hat{\underset{k}{\otimes}} kC$. Then the map $A \to (kA/P)^\times$ can be written as

$$\begin{aligned} B \oplus C &\to (kB/Q)^\times \oplus (kC)^\times \lesssim (kB/Q \hat{\underset{k}{\otimes}} kC)^\times \\ (b, c) &\mapsto ((b + Q), c), \end{aligned}$$

so it is clear that P is faithful if and only if Q is faithful. $\square$

Lemma 9.1.2. Let A, B, k be as in Lemma 9.1.1. Take two neighbouring prime ideals $P \lneq Q$ of kA, and suppose B controls P. Then

(i) $h(P) + \dim(A/P) = r(A)$,

(ii) $h(Q) = h(P) + 1$,

(iii) $h(P) = h(P \cap kB)$.

Proof.

(i) This follows from [25, Ch. VII, §10, Corollary 1].

(ii) This follows from [25, Ch. VII, §10, Corollary 2].

(iii) Under the correspondence of Lemma 9.1.1, any saturated chain of prime ideals $0 = Q_0 \lneq Q_1 \lneq \cdots \lneq Q_n = P \cap kB$ of kB extends to a chain of prime ideals

$0 = P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n = P$ of kA. As any two saturated chains of prime ideals in kA have the same length [25, Ch. VII, §10, Theorem 34 and Corollary 1], we need only check that this chain is saturated.

Take two adjacent prime ideals $I_1 \subsetneq I_2$ of kB, so that $h(I_2) = h(I_1) + 1$ [25, Ch. VII, §10, Corollary 2] and $I_1 kA \subsetneq I_2 kA$ are prime. We will show that $I_1 kA$ and $I_2 kA$ are adjacent by showing that their heights also differ by 1. By performing induction on $r(A/B)$, it will suffice to prove this for the case $r(A/B) = 1$, i.e. $kA = kB[[X]]$.

It is clear that, when R is a commutative ring, $\dim(R[[X]]) \geq 1 + \dim(R)$ (where dim denotes the classical Krull dimension). But, giving $R[[X]]$ the (X)-adic filtration, we see that $\mathrm{gr}(R[[X]]) \cong R[x]$. By [18, 6.5.6], we have $\dim(R[[X]]) \leq \dim(\mathrm{gr}(R[[X]])) = \dim(R[x]) = 1 + \dim(R)$, where this last equality follows from [18, 6.5.4(i)].

Hence, for any prime ideal I, we have

$$\dim(kA/IkA) - \dim(kB/I) = \dim((kB/I)[[X]]) - \dim(kB/I) = 1.$$

But, from (i), we see that

$$\dim(kA/IkA) = r(A) - h(IkA),$$
$$\dim(kB/I) = r(B) - h(I),$$

and hence we conclude that $h(I) = h(IkA)$. Setting $I = I_1, I_2$ now shows that $h(I_2 kA) = h(I_1 kA) + 1$ as required. $\square$

9.2 A finite-by-abelian result

We slightly extend the correspondence of Lemma 9.1.1.

Corollary 9.2.1. Let Δ be finite-by-(abelian p-valuable) with finite radical Δ^+, and let Γ be a closed isolated normal subgroup of Δ (so that, in particular, $\Delta^+ \leq \Gamma$). Let k be a finite field of characteristic p. If P is a prime ideal of $k\Gamma$, then $Pk\Delta$ is a prime ideal of $k\Delta$. Finally, P is almost faithful if and only if $Pk\Delta$ is almost faithful.

Proof. We will use Notation 1.5.2. Let $e \in \mathrm{cpi}^{\overline{k\Delta^+}}(P)$.

Case 1. Suppose Δ centralises e. Then there is an isomorphism

$$\psi : e \cdot \overline{k\Delta} \to M_m(k'[[\Delta/\Delta^+]])$$

for some finite field extension k'/k and some positive integer m, by Theorem 4.1.5; under this map, $\psi(e \cdot \overline{P}) = M_m(\mathfrak{p})$ for some prime ideal $\mathfrak{p}$ of $k'[[\Gamma/\Delta^+]]$. It suffices to show that $\mathfrak{p}k'[[\Delta/\Delta^+]]$ is prime, and that this correspondence preserves faithfulness; but this now follows from Lemma 9.1.2(iii).

Case 2. If Δ does not centralise e, take $f = e|^{\Delta}$. Then there is an isomorphism $\theta : f \cdot \overline{k\Delta} \to M_n(e \cdot \overline{k\Delta_1})$, where Δ_1 centralises e; under this isomorphism, $\theta(f \cdot \overline{Pk\Delta}) = M_n(e \cdot \overline{\mathfrak{p}k\Delta_1})$ for some prime ideal $\mathfrak{p} \lhd k\Gamma_1$. It suffices to show that $\mathfrak{p}k\Delta_1$ is prime; but this follows from Case 1. $\square$

9.3 Faithful primes are controlled by Δ

First, recall the control theorem of [4, 8.6]:

Theorem 9.3.1. Let G be a nilpotent p-valued group of finite rank with centre Z.

(i) If $\mathfrak{p}$ is a prime ideal of kZ, then $\mathfrak{p}kG$ is a prime ideal of kG.

(ii) If P is a faithful prime ideal of kG, then P is controlled by Z.

Proof. This is [4, 8.4, 8.6]. $\square$

Lemma 9.3.2. Let G be finite-by-(nilpotent p-valuable), i.e. $G = \mathbf{FN}_p(G)$. Then $Z(G/\Delta^+) = \Delta/\Delta^+$.

Proof. Given $x \in G$, the two conditions $[G/\Delta^+ : \mathbf{C}_{G/\Delta^+}(x\Delta^+)] < \infty$ and $[G : \mathbf{C}_G(x)] < \infty$ are equivalent, as Δ^+ is finite; this shows that we have $\Delta(G/\Delta^+) = \Delta/\Delta^+$. Take some $x \in \Delta$, so that x satisfies this condition: then, given arbitrary $g \in G$, there exists some k such that $g^{p^k}\Delta^+ \in \mathbf{C}_{G/\Delta^+}(x\Delta^+)$, so that $(x^{-1}gx)^{p^k}\Delta^+ = g^{p^k}\Delta^+$, and it now follows from [13, III, 2.1.4] that $x^{-1}gx\Delta^+ = g\Delta^+$. This shows that $\Delta/\Delta^+ \leq Z(G/\Delta^+)$. Conversely, we must have $Z(G/\Delta^+) \leq \Delta(G/\Delta^+)$ by definition. $\square$

We extend Theorem 9.3.1 to:

Proposition 9.3.3. Let G be a finite-by-(nilpotent p-valuable) group.

(i) If $\mathfrak{p}$ is a G-prime ideal of $k\Delta$, then $\mathfrak{p}kG$ is a prime ideal of kG.

(ii) If P is an almost faithful prime ideal of kG, then P is controlled by Δ.

Proof. Adopt Notation 1.5.2. Let $e \in \mathrm{cpi}^{\overline{k\Delta^+}}(\mathfrak{p})$, and write $f = e|^G$. It suffices to prove that the ideal $f \cdot \overline{\mathfrak{p}kG} \lhd f \cdot \overline{kG}$ is prime. But, by the Matrix Units Lemma 4.3.1, we have an isomorphism

$$f \cdot \overline{kG} \cong M_s(e \cdot \overline{kG_1}),$$

where G_1 is the stabiliser in G of e, and under which $f \cdot \overline{\mathfrak{p}kG} \mapsto M_s(e \cdot \overline{\mathfrak{p}_1 kG_1})$ for some G_1-prime ideal $\mathfrak{p}_1$ of $k[[\Delta \cap G_1]]$. So, by Morita equivalence, it will suffice to show that the ideal $e \cdot \overline{\mathfrak{p}_1 kG_1} \lhd e \cdot \overline{kG_1}$ is prime.

Now recall from Theorem 4.1.5 that we have an isomorphism

$$\psi : e \cdot \overline{kG_1} \cong M_t(k'[[G_1/\Delta^+]])$$

under which $e \cdot \overline{\mathfrak{p}_1 kG_1} \mapsto \mathfrak{q}k'[[G_1/\Delta^+]]$ for a (G_1/Δ^+)-prime ideal $\mathfrak{q}$ of $k'[[\Delta \cap G_1/\Delta^+]]$. Hence we need now only show that $\mathfrak{q}k'N \lhd k'N$ is prime, where $N = G_1/\Delta^+$.

Note that, as G_1 is open in G, we have $\Delta(G_1) = \Delta \cap G_1$; and from Lemma 9.3.2, $\Delta(G_1)/\Delta^+ = Z(G_1/\Delta^+)$. Hence, still writing $N = G_1/\Delta^+$, we see that $\mathfrak{q}$ is an N-prime ideal of $k'[[Z(N)]]$, and hence a prime ideal. But now $\mathfrak{q}k'N$ is prime by Theorem 9.3.1(i). This establishes part (i) of the proposition.

To show part (ii), take an almost faithful prime ideal P of kG. We would like to show that P is a minimal prime ideal above $(P \cap k\Delta)kG$. But this is clearly true when $\Delta^+ = 1$ by Theorem 9.3.1; and in the general case, another application of the Matrix Units Lemma 4.3.1 and Theorem 4.1.5, as above, reduces to the case $\Delta^+ = 1$.

Hence, finally, we need only show that $(P \cap k\Delta)kG$ is prime; but $P \cap k\Delta$ is a G-prime ideal of $k\Delta$ (again by Lemma 8.1.2(i)), so we are done by part (i) of the proposition. $\square$

Until the end of this section, we will write $(-)^\circ$ to mean $\bigcap_{g \in G} (-)^g$.

Corollary 9.3.4. Let G be a finite-by-(nilpotent p-valuable) group, and H an open normal subgroup of G containing Δ. If P is an almost faithful G-prime ideal of kH, then PkG is a prime ideal of kG.

Proof. Take a minimal prime Q of kH above P. Then we have $Q^\circ = P$, so $Q^\dagger$ is finite (as G is orbitally sound). Hence Q is controlled by Δ, by Proposition 9.3.3(ii), and by applying $(-)^\circ$ to both sides of the equality $Q = (Q \cap k\Delta)kH$, we see that P is also: $P = (P \cap k\Delta)kH$. In particular $PkG = (P \cap k\Delta)kG$. But now Proposition

9.3.3(i) shows that $(P \cap k\Delta)kG$ is prime. $\square$

Proposition 9.3.5. Let G be a nilpotent-by-finite, orbitally sound compact p-adic analytic group, and k a finite field of characteristic $p > 2$. Let $H = \mathbf{FN}_p(G)$. If P is an almost faithful prime ideal of kG, then P is controlled by H.

Proof. Let Q be a minimal prime ideal of kH above $P \cap kH$. Then $(Q^\dagger)^\circ = P^\dagger \cap H$ is finite, so, as G is orbitally sound, $Q^\dagger$ is also finite. By [22, Corollary 14.8], in order to prove that $(P \cap kH)kG$ is prime, it suffices to show that QkS is prime, where S is the stabiliser in G of Q.

Let $T = \mathbf{FN}_p(S)$. As H is a finite-by-(nilpotent p-valuable) open normal subgroup of S, we see that H must be an open normal subgroup of T. It is also clear that $\Delta(H) = \Delta(T) = \Delta(S) = \Delta(G)$. Now, by Corollary 9.3.4, QkT must be prime; and we have that $(QkT)^\dagger$ is finite. Now, by Proposition 7.3.3, $(QkT)kS = QkS$ is prime. $\square$

Lemma 9.3.6. Let G be a nilpotent-by-finite compact p-adic analytic group, and let $H \geq K$ be any two closed normal subgroups of G. Take P to be a prime ideal of kG. Let Q be a minimal prime ideal of kH above $P \cap kH$. If P is controlled by H and Q is controlled by K, then P is controlled by K.

Proof. By Lemma 8.1.2(ii), we have $Q^\circ = P \cap kH$, and so

$$\begin{aligned}
(P \cap kK)kG &= ((P \cap kH) \cap kK)kG \\
&= (Q^\circ \cap kK)kG \\
&= (Q \cap kK)^\circ kG && \text{as } K \text{ is normal in } G \\
&= ((Q \cap kK)kH)^\circ kG && \text{as } H \text{ is normal in } G \\
&= Q^\circ kG && \text{as } Q \text{ is controlled by } K \\
&= (P \cap kH)kG = P && \text{as } P \text{ is controlled by } H.
\end{aligned}$$

□

Now back to:

Theorem 9.3.7. Let G be a nilpotent-by-finite, orbitally sound compact p-adic analytic group, k a finite field of characteristic $p > 2$, and P an almost faithful prime ideal of kG. Then P is controlled by Δ.

Proof. Proposition 9.3.5 shows that P is controlled by H. Let Q be a minimal prime of kH above $P \cap kH$: then $Q^\circ = P \cap kH$ by Lemma 8.1.2(ii), so we see that $(Q^\dagger)^\circ = P^\dagger \cap H$ is finite, so (as G is orbitally sound) $Q^\dagger$ must also be finite. Hence, as Q is almost faithful, Proposition 9.3.3(ii) shows that it is controlled by Δ. Now Lemma 9.3.6 applies. □

Proof of Theorem K. This follows from Theorem 9.3.7.

9.4 Primes adjacent to faithful primes

Lemma 9.4.1. Let G be a nilpotent-by-finite, orbitally sound compact p-adic analytic group with $\Delta^+ = 1$, and let N be an isolated normal subgroup of G contained in Δ. Then we have either $\mathbf{FN}_p(G/N) = \mathbf{FN}_p(G)/N$ or $N = \Delta = \mathbf{FN}_p(G)$.

Proof. Write $H = \mathbf{FN}_p(G)$, and $\widehat{H}$ for the preimage of $\widehat{H}/N = \mathbf{FN}_p(G/N)$.

If $G = \mathbf{FN}_p(G)$, then we clearly have $\mathbf{FN}_p(G/N) = \mathbf{FN}_p(G)/N$ for any closed normal subgroup N. So suppose that $H \lneq \widehat{H} \leq G$, and take some $z \in \widehat{H} \setminus H$. Now conjugation by z induces the automorphism $x \mapsto x^\zeta$ on H/H' (where H' denotes the isolated derived subgroup), and hence also on $H/H'N$, for some $\zeta \in t(\mathbb{Z}_p^\times)$ (Lemma 2.4.2) satisfying $\zeta \neq 1$ (Lemma 7.2.1).

If $H/H'N$ has nonzero rank, we may take an element $x \in H$ whose image in $H/H'N$ has infinite order; and now the image in $\widehat{H}/H'N$ of $\overline{\langle x, z\rangle}$ is not finite-by-nilpotent, contradicting the definition of $\widehat{H}$. So we must have $H = \mathrm{i}_H(H'N)$.

In particular, this implies that $H = \mathrm{i}_H(H'Z)$, where $Z = Z(H) = \Delta(G)$, and so, by Lemma 7.2.3, we see that H is abelian, i.e. $H = \Delta$. Furthermore, this implies that $H' = 1$, and as N is already H-isolated orbital, the equality $H = \mathrm{i}_H(H'N)$ simplifies to give $H = N$. This is what we wanted to prove. $\square$

Remark. If G is a compact p-adic analytic group, H is a closed normal subgroup, and Q is a G-stable ideal of kH, then $Q^\dagger = (Q+1) \cap H$ is normal in G.

Lemma 9.4.2. Let G be a nilpotent-by-finite, orbitally sound compact p-adic analytic group, and let k be a finite field of characteristic $p > 2$. If Q is a G-prime ideal of $k\Delta$, and $\mathbf{FN}_p(G/Q^\dagger) = \mathbf{FN}_p(G)/Q^\dagger$, then QkG is a prime ideal of kG.

Remark. The hypothesis

$$\mathbf{FN}_p(G/Q^\dagger) = \mathbf{FN}_p(G)/Q^\dagger \tag{9.4.1}$$

has the following consequence. Let G be a nilpotent-by-finite, orbitally sound compact p-adic analytic group with $\Delta^+ = 1$, k a finite field of characteristic $p > 2$, and let

$P \lneq Q$ be adjacent prime ideals of kG, with P almost faithful. Then P is controlled by Δ, by Theorem 9.3.7. Consider $(Q \cap k\Delta)^\dagger$: if this is not equal to Δ, then by Lemma 9.4.1, the hypothesis (9.4.1) is satisfied. So suppose it is equal to Δ: then Q contains the ideal $\ker(kG \to k[[G/\Delta]])$ (the augmentation ideal of Δ). Now, if $\mathbf{FN}_p(G) = \Delta$, then kG/Q is a *finite* prime ring, which is therefore simple, and so Q must be a *maximal* ideal of kG of $\mathrm{i}_G(\Delta) = G$; otherwise, we again have (9.4.1) by Lemma 9.4.1.

That is, under these conditions, we always have (9.4.1) unless Q is a maximal ideal of kG and G is virtually abelian, in which case $Q^\dagger$ is open in G.

Proof. Write $H = \mathbf{FN}_p(G)$.

As Q is a G-prime, we may write it as $\bigcap_{g\in G} I^g$ for some minimal prime ideal I above Q. Suppose the G-orbit of I splits into distinct H-orbits $\mathcal{O}_1, \dots, \mathcal{O}_r$, and write $P_i := \bigcap_{A\in\mathcal{O}_i} A$. Then P_i is an H-prime of $k\Delta$, and $\bigcap_{i=1}^r P_i = Q$. In particular, since P_i is an H-prime of $k\Delta$, we have that $P_i kH$ is prime by Proposition 9.3.3(i).

It remains to show that $\left(\bigcap_{g\in G} (P_i kH)^g\right) kG$ is prime. By [22, Corollary 14.8], it suffices to show that $P_i kS$ is prime, where $S = \mathrm{Stab}_G(P_i)$.

Write $\mathfrak{p} = P_i kH$, and note that $\mathfrak{p}^\dagger = P_i^\dagger \leq \Delta$. Now, if $\mathbf{FN}_p(G)/\Delta^+$ is non-abelian, we have $\mathbf{FN}_p(S/\mathfrak{p}^\dagger) = \mathbf{FN}_p(S)/\mathfrak{p}^\dagger$. If, on the other hand, $\mathbf{FN}_p(G)/\Delta^+$ is abelian, then we must have $Q^\dagger \lneq \Delta$, and as $Q^\dagger$ is H-isolated orbital, we have $[\Delta : Q^\dagger] = \infty$. But as G is orbitally sound, and $Q^\dagger = \bigcap_{g\in G} (P_i^\dagger)^g$, we must have that $Q^\dagger$ is open in $P_i^\dagger$, so that in particular $[\Delta : \mathfrak{p}^\dagger] = \infty$. Hence again we have $\mathbf{FN}_p(S/\mathfrak{p}^\dagger) = \mathbf{FN}_p(S)/\mathfrak{p}^\dagger$.

Write $\overline{(\cdot)}$ for the quotient map $S \to S/\mathfrak{p}^\dagger$. Now, to show that $P_i kS = \mathfrak{p}kS$ is prime, we need only show that $\overline{\mathfrak{p}}k\overline{S}$ is prime. But $\overline{\mathfrak{p}}$ is a faithful prime ideal of $k\overline{H}$, and $\overline{H} = \mathbf{FN}_p(\overline{S})$, so by Proposition 7.3.3, we are done. $\square$

Lemma 9.4.3. Let k be a finite field of characteristic $p > 2$. Let G be a nilpotent-by-finite, orbitally sound compact p-adic analytic group, and let $P \lneq Q$ be adjacent prime ideals of kG, with P almost faithful. Suppose that Q is not a maximal ideal of kG. Then Q is controlled by Δ.

Proof. $Q \cap k\Delta$ is a G-prime of $k\Delta$, and so $(Q \cap k\Delta)kG$ is prime by Lemma 9.4.2 and the accompanying remark. But

$$P = (P \cap k\Delta)kG \leq (Q \cap k\Delta)kG \leq Q,$$

(with the equality as a result of Theorem 9.3.7), and P and Q are adjacent, so $(Q \cap k\Delta)kG$ must equal either P or Q.

Let us assume for contradiction that $(Q \cap k\Delta)kG = P$. Then we must have

$$P \cap k\Delta \leq Q \cap k\Delta \leq (Q \cap k\Delta)kG = P,$$

and by intersecting each of these with $k\Delta$, we see that $P \cap k\Delta = Q \cap k\Delta$. In particular, by taking $(\cdot)^\dagger$ of both sides of this equality, we see that $Q^\dagger \cap \Delta$ is finite (as P is almost faithful).

Let N be an open normal nilpotent p-valued subgroup of G, and let $Z = Z(N)$. By Lemma 1.2.3(ii), $Z = \Delta(N)$ is a finite-index torsion-free subgroup of Δ, and so $Q^\dagger \cap Z = 1$. Now, as N is nilpotent and the normal subgroup $Q^\dagger \cap N$ has trivial intersection with its centre, [23, 5.2.1] implies that $Q^\dagger \cap N = 1$, and hence $Q^\dagger$ must be a finite normal subgroup of G. So $Q^\dagger \leq \Delta^+$, and in particular $Q^\dagger = Q^\dagger \cap \Delta$, which we earlier determined is finite. Hence Q is almost faithful, and must be controlled by Δ by Theorem 9.3.7. In particular, we must have $P \cap k\Delta \neq Q \cap k\Delta$. But this contradicts our assumption. $\square$

Chapter 10

Catenarity

10.1 The orbitally sound case: plinths and a height function

Much of the material in this subsection is adapted from [24].

Until stated otherwise, G is an arbitrary compact p-adic analytic group, and k is a finite field of characteristic p. We start by outlining our plan of attack:

Lemma 10.1.1. Let R be a ring in which every prime ideal has finite height. Suppose we are given a function $h : \mathrm{Spec}(R) \to \mathbb{N}$ satisfying

- $h(P) = 0$ whenever P is a minimal prime of R,
- $h(P') = h(P) + 1$ for each pair of adjacent primes $P \lneq P'$ of R.

Then R is a catenary ring.

Proof. Obvious. $\square$

Lemma 10.1.2. kG has finite classical Krull dimension, i.e. the maximal length of any chain of prime ideals is bounded.

Proof. The classical Krull dimension of kG is bounded above by $\mathrm{Kdim}(kG)$ by [18, Lemma 6.4.5], which is equal to $\mathrm{Kdim}(\mathbb{F}_pG)$ by [18, Proposition 6.6.16(ii)], and this is bounded above by the *dimension* (in the sense of [9, Theorem 8.36]) of G, which is finite by definition (see the remarks after [9, Definition 3.12]). $\square$

Definition 10.1.3. Let V be a $\mathbb{Q}_pG$-module, and suppose it has finite dimension as a vector space over $\mathbb{Q}_p$. Take a chain

$$0 = V_0 \lneq V_1 \lneq \cdots \lneq V_r = V$$

of G–orbital subspaces – that is, $\mathbb{Q}_p$-vector subspaces of V with finitely many G-conjugates, or equivalently $\mathbb{Q}_p$-vector subspaces that are $\mathbb{Q}_pN$-submodules for some open subgroup N of G. Assume further that this chain is *saturated*, in the sense that it cannot be made longer by the addition of some G–orbital subspace $V_i \lneq V' \lneq V_{i+1}$. Such a chain is necessarily finite, as it is bounded above in length by $\dim_{\mathbb{Q}_p}(V) + 1$. We call the number r the *G–plinth length* of V, written $p_G(V)$. If $p_G(V) = 1$, we say that V is a *plinth* for G.

Remark. The number r is independent of the V_i chosen. Indeed, fix a *longest possible* chain

$$0 = V_0 \lneq V_1 \lneq \cdots \lneq V_r = V$$

of G-orbital subspaces, and let G_0 be the intersection of the normalisers $\mathbf{N}_G(V_i)$, i.e. the largest subgroup of G such that each V_i is a $\mathbb{Q}_pG_0$-module. G_0 is open in G. Now, given any chain

$$0 = W_0 \lneq W_1 \lneq \cdots \lneq W_s = V$$

of G-orbital subspaces, take $H_0 = \bigcap_{j=1}^{s} \mathbf{N}_G(W_j)$, and note that $G_0 \cap H_0$ is a finite-index open subgroup of G that normalises each V_i and W_j. Hence, by the Jordan-Hölder theorem [11, Theorem 4.11], the chain W_j may be refined to a chain of length r; so if the chain W_j is saturated, then $s = r$.

Definition 10.1.4. A G*-group* is a topological group H endowed with a continuous action of G. For example, closed subgroups of G, and quotients of G by closed normal subgroups of G, are G-groups under the action of conjugation.

Let H be a nilpotent-by-finite compact p-adic analytic group with a continuous action of G. We aim to define $p_G(H)$. In fact, as plinths are insensitive to finite factors, we may immediately replace H by the open subgroup formed by the intersection of the (finitely many) G-conjugates of any given open normal nilpotent uniform subgroup of H. Then there is a series

$$1 = H_0 \lhd H_1 \lhd \cdots \lhd H_n = H \tag{10.1.1}$$

of G-subgroups such that $A_i = H_i/H_{i-1}$ is abelian for each $i = 1, \dots, n$. Let $V_i = A_i \underset{\mathbb{Z}_p}{\otimes} \mathbb{Q}_p$ for each $i = 1, \dots, n$, with G–action given by conjugation. In this case, we define

$$p_G(H) = \sum_{i=1}^{n} p_G(V_i).$$

Lemma 10.1.5. $p_G(H)$ is well-defined, and does not depend on the series (10.1.1).

Proof. Apply the Jordan-Hölder theorem, as in the remark above. □

For our purposes, the most important property of p_G is that it is additive on short exact sequences of G-groups, which also follows from the Jordan-Hölder theorem. We record this as:

Lemma 10.1.6. Suppose that $1 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 1$ is a short exact sequence of G-groups. Then $p_G(A) + p_G(C) = p_G(B)$. □

We now define Roseblade's function λ. (Later, we will show that, in the case when G is nilpotent-by-finite and orbitally sound, λ is actually equal to the height function on $\mathrm{Spec}(kG)$.)

Definition 10.1.7.

$$\lambda(P) = \begin{cases} p_G(P^\dagger) + \lambda(P^\pi) & P^\dagger \neq 1 \\ h_G(P \cap k\Delta) & P^\dagger = 1, \end{cases}$$

where P^π is the image of P under the map

$$\pi : kG \to kG/(P^\dagger - 1)kG \cong k[[G/P^\dagger]].$$

This definition is recursive, in that if P is an unfaithful prime ideal, then $\lambda(P)$ is defined with reference to $\lambda(P^\pi)$; but P^π is then a faithful prime ideal of kG^π, so this process terminates after at most two steps.

We make the following remark on this definition immediately:

Lemma 10.1.8. Let G be a nilpotent-by-finite, orbitally sound compact p-adic analytic group, k a finite field of characteristic $p > 2$, and P a faithful prime of $k\Delta$. Then $\lambda(P) = h(P)$.

Proof. $\lambda(P)$ is defined to be $h_G(P \cap k\Delta)$. But, by Theorem 9.3.7 and Lemma 9.4.2, we see that there is a one-to-one, inclusion-preserving correspondence between faithful prime ideals of kG and faithful G-prime ideals of $k\Delta$, so that $h_G(P \cap k\Delta) = h(P)$. $\square$

We return to the general case of G an arbitrary compact p-adic analytic group.

Lemma 10.1.9. Let $P \lneq Q$ be neighbouring prime ideals of kG, and write

$$\pi : kG \to kG/(P^\dagger - 1)kG \cong k[[G/P^\dagger]].$$

Then

$$\lambda(Q) - \lambda(P) = \lambda(Q^\pi) - \lambda(P^\pi).$$

Proof. Firstly, as $P \leq Q$, we have $P^\dagger \leq Q^\dagger$, so the map

$$\rho : kG \to k[[G/Q^\dagger]]$$

factors as

$$\begin{tikzcd} kG \arrow[r, "\pi"] \arrow[rr, bend right, "\rho"'] & k[[G/P^\dagger]] \arrow[r, "\sigma"] & k[[G/Q^\dagger]]. \end{tikzcd}$$

We now compute $\lambda(Q) - \lambda(P)$ using Definition 10.1.7:

$$\begin{aligned}
\lambda(Q) - \lambda(P) &= p_G(Q^\dagger) - p_G(P^\dagger) + \lambda(Q^\rho) - \lambda(P^\pi) \\
&= p_G((Q^\dagger)^\pi) + \lambda(Q^\rho) - \lambda(P^\pi) && \text{by Lemma 10.1.6} \\
&= p_G((Q^\dagger)^\pi) + \lambda(Q^{\pi\sigma}) - \lambda(P^\pi) && \text{by definition of } \rho \\
&= p_G((Q^\pi)^\dagger) + \lambda((Q^\pi)^\sigma) - \lambda(P^\pi) && \text{as } (Q^\dagger)^\pi = (Q^\pi)^\dagger \\
&= \lambda(Q^\pi) - \lambda(P^\pi) && \text{by Definition 10.1.7.} \quad \square
\end{aligned}$$

Remark. Suppose G is a nilpotent-by-finite compact p-adic analytic group, and suppose we are given a subquotient A of G which is a plinth, with G-action induced from the conjugation action of G on itself. Then it is easy to see that $\dim_{\mathbb{Q}_p}(A \underset{\mathbb{Z}_p}{\otimes} \mathbb{Q}_p) = 1$. (Roseblade calls such plinths *centric*.) Indeed, suppose $A = H/K$, where H and K are closed normal subgroups of G with K contained in H. Then we may replace G by an open normal nilpotent uniform subgroup G', and A by $A' = H'/K'$, where $H' = H \cap G'$ and $K' = \mathrm{i}_{H'}(K \cap G')$; after doing this, we still have that A' is a plinth for G', and that $\dim_{\mathbb{Q}_p}(A \underset{\mathbb{Z}_p}{\otimes} \mathbb{Q}_p) = \dim_{\mathbb{Q}_p}(A' \underset{\mathbb{Z}_p}{\otimes} \mathbb{Q}_p)$. But, as G'/K' is nilpotent, and A' is a non-trivial normal subgroup, A' must meet the centre $Z(G'/K')$ non-trivially; and as A' is torsion-free, we must have that $A' \cap Z(G'/K')$ is a plinth for G', and so must be equal to A'. Hence G' centralises A', and its plinth length is simply equal to its rank.

Again, we will write $(-)^\circ$ to mean $\bigcap_{g\in G}(-)^g$.

Lemma 10.1.10. Let G be a nilpotent-by-finite compact p-adic analytic group. Let U be a G-prime of $k\Delta$, and write $\rho : k\Delta \to k[[\Delta/U^\dagger]]$. Then $h(U) = h_G(U^\rho) + p_G(U^\dagger)$.

Proof. Let $A = Z(\Delta)$, and let U_1 be a minimal prime of kA above $U \cap kA$, so that $U \cap kA = U_1^\circ$. Then $h_G(U) = h(U_1)$ by Corollary 8.1.4, and so $h_G(U^\rho) = h(U_1^\rho)$. Now, from Lemma 9.1.2(i), we have $h(U_1) + \dim(kA/U_1) = r(A)$ and $h(U_1^\rho) + \dim(kA/U_1) = r(A^\rho)$, from which we may deduce that

$$h(U_1) = h(U_1^\rho) + r(A) - r(A^\rho).$$

But $r(A) - r(A^\rho) = r(A \cap \ker\rho) = p_G(U^\dagger \cap A)$ by the above remark. Now this is just $p_G(U^\dagger)$, as A is open in Δ. $\square$

Lemma 10.1.11. Let G be arbitrary compact p-adic analytic. Let H be a closed normal subgroup of G, and let K be an open subgroup of H which is normal in G. If P is a G-prime ideal of kH, then $h_G(P) = h_G(P \cap kK)$.

Proof. [Adapted from [24, Lemma 29].] We know that $P = Q^\circ$ for some prime Q of kH, and $Q \cap kK = \bigcap_{h\in H} V^h$ for some prime V of kK. Hence $P \cap kK = V^\circ$. Then, writing h_G^{orb} for the height function on *G-orbital primes*,

$$\begin{aligned} h_G(P) &= h_G^{\mathrm{orb}}(Q) && \text{by Lemma 8.1.2(ii)} \\ &= h_G^{\mathrm{orb}}(V) && \text{by Lemma 8.1.2(i)} \\ &= h_G(P \cap kK) && \text{by Lemma 8.1.2(ii).} \end{aligned}$$ $\square$

Here, we deduce from Theorem 9.3.7 and [24, proof of theorem H2] the following corollary:

Theorem 10.1.12. Let G be a nilpotent-by-finite, orbitally sound compact p-adic analytic group, and k a finite field of characteristic $p > 2$. Then kG is a catenary ring.

Proof. Let $P \lneq Q$ be neighbouring prime ideals of kG. We will first show that $\lambda(Q) = \lambda(P) + 1$.

By passing to $k[[G/P^\dagger]]$, we may assume that P is a faithful prime ideal, by Lemma 10.1.9. Hence, by Theorem 9.3.7 (and as $p > 2$), we have that $(P \cap k\Delta)kG = P$. We also have either that $(Q \cap k\Delta)kG = Q$, by Lemma 9.4.3, or $Q^\dagger \geq \Delta$ by the remark of Lemma 9.4.2; and so, in either case, we have $P \cap k\Delta \lneq Q \cap k\Delta$. These must be neighbouring G-primes of $k\Delta$: indeed, if J is a G-prime strictly between them, then again by Lemma 9.4.2 and the remark made there, we see that JkG is a prime ideal of kG. JkG must then lie strictly between P and Q – indeed, if $JkG = Q$, then intersecting both sides with $k\Delta$ shows that $J = Q \cap k\Delta$, and likewise if $JkG = P$. This is a contradiction.

Hence $h_G(Q \cap k\Delta) = h_G(P \cap k\Delta) + 1$. The right hand side is, by definition, just equal to $\lambda(P) + 1$; and we have $\lambda(Q) = \lambda(Q^\rho) + p_G(Q^\dagger)$, where $\rho : G \to G/Q^\dagger$. It remains to show that this is equal to $h_G(Q \cap k\Delta)$.

Case 1. $Q^\dagger$ is not open in G. Then Q is controlled by Δ by Lemma 9.4.3 and the remark of Lemma 9.4.2, and so Q^ρ is controlled by Δ^ρ, and in particular by $\mathrm{i}_{G^\rho}(\Delta^\rho) \leq \mathrm{i}_{G^\rho}(\Delta(G^\rho))$. Write $A = Z(\Delta(G^\rho))$ and $B = A \cap \mathrm{i}_{G^\rho}(\Delta^\rho)$: as Q^ρ is controlled by $\mathrm{i}_{G^\rho}(\Delta^\rho)$, we have that $Q^\rho \cap kA$ is controlled by B. Furthermore, we can write

$Q^\rho \cap kA = \mathfrak{q}^\circ$ for some prime $\mathfrak{q}$ of kA, so that $\mathfrak{q}$ is also controlled by B, and hence

$$\begin{aligned}
\lambda(Q^\rho) &= h_G(Q^\rho \cap k[[\Delta(G^\rho)]]) && \text{by definition}\\
&= h_G(Q^\rho \cap kA) && \text{by Lemma 10.1.11}\\
&= h(\mathfrak{q}) && \text{by Corollary 8.1.4}\\
&= h(\mathfrak{q} \cap kB) && \text{by Lemma 9.1.2(iii)}\\
&= h_G(Q^\rho \cap kB) && \text{by Corollary 8.1.4}\\
&= h_G(Q^\rho \cap k[[\mathrm{i}_{G^\rho}(\Delta^\rho)]]) && \text{by Lemma 10.1.11}\\
&= h_G(Q^\rho \cap k\Delta^\rho) && \text{by Lemma 10.1.11.}
\end{aligned}$$

We also have $p_G(Q^\dagger) = p_G((Q \cap k\Delta)^\dagger)$. Hence

$$\lambda(Q) = h_G((Q \cap k\Delta)^\rho) + p_G((Q \cap k\Delta)^\dagger).$$

Now we are done by Lemma 10.1.10.

Case 2. $Q^\dagger$ is open in G. We have already seen that this case only occurs when $G = \mathrm{i}_G(\Delta)$, and so $\lambda(Q^\rho) = \lambda(0) = 0$, and $p_G(Q^\dagger) = p_G(G)$, and $h_G(Q \cap k\Delta) = h_G(Q \cap kA)$ $= r(A)$. These are clearly equal, as A is open in G.

In order to invoke Lemma 10.1.1, it remains only to show that $\lambda(P) = 0$ when P is a minimal prime. But as all minimal primes are induced from Δ^+, this follows immediately from the definition of λ: we will have $P^\dagger \leq \Delta^+$ (and hence $p_G(P^\dagger) = 0$), and $P^\pi \cap k\Delta^\pi$ will be a minimal G-prime of $k\Delta^\pi$ (and hence $h_G(P^\pi \cap k\Delta^\pi) = 0$). □

Proof of Theorem B. This follows from Theorem 10.1.12. □

10.2 Vertices and sources

We now study a more general setting. Let G be an arbitrary compact p-adic analytic group, and P an arbitrary prime ideal of kG.

Remark. Suppose G is orbitally sound and nilpotent-by-finite, N is a closed normal subgroup of G, and I is a prime ideal of kG with $N \leq I^\dagger$ and $[I^\dagger : N] < \infty$. Writing $\overline{(\cdot)}$ for the natural map $kG \to k[[G/N]]$, it is clear that the prime ideal $\overline{I} \lhd k[[G/N]]$ is almost faithful, and so, by Theorem 9.3.7, is controlled by $\Delta(G/N)$, and that I is the complete preimage in kG of $\overline{I}$, and is therefore controlled by the preimage in G of $\Delta(G/N)$.

This motivates the following definition:

Definition 10.2.1. Let I be an ideal of kG, and N a closed subgroup of G. We say that I is *almost faithful mod* N if $I^\dagger$ contains N as a subgroup of finite index. We also write $\nabla_G(N)$ for the subgroup of $\mathbf{N}_G(N)$ defined by

$$\nabla_G(N)/N = \Delta(\mathbf{N}_G(N)/N).$$

Diagrammatically:

$$\begin{tikzcd}[arrows=dash]
G \arrow[d] & \\
\mathbf{N}_G(N) \arrow[d] \arrow[r, dotted] & \mathbf{N}_G(N)/N \arrow[d] \\
\nabla_G(N) \arrow[d] \arrow[r, dotted] & \Delta(\mathbf{N}_G(N)/N) \arrow[d] \\
N \arrow[d] \arrow[r, dotted] & N/N \\
1 &
\end{tikzcd}$$

We will extend this notion to ideals I with $I^\dagger$ *contained in* N as a subgroup of finite index.

Lemma 10.2.2. Let H be an open subgroup of N. Then there exists an open characteristic subgroup M of N contained in H.

Proof. (Adapted from [22, 19.2].) Let $[N : H] = n < \infty$. Now, as N is topologically finitely generated, there are only finitely many continuous homomorphisms $N \to S_n$. where S_n is the symmetric group. Take M to be the intersection of the kernels of these homomorphisms. $\square$

Lemma 10.2.3. Let N be a closed subgroup of G, and $A = \mathbf{N}_G(N)$. Suppose I is an ideal of kA, and $I^\dagger \leq N$ with $[N : I^\dagger] < \infty$. Then there is a closed normal subgroup M of A such that I is almost faithful mod M. Furthermore, this M can be chosen so that $\nabla_G(N) = \nabla_A(M)$.

Proof. Set $H = I^\dagger$ in Lemma 10.2.2: then the subgroup M is characteristic in N, hence normal in A; M contains $I^\dagger$; and M is open in N, so we must have $[I^\dagger : M] < \infty$.

By definition, we have $\nabla_G(N) = \nabla_A(N)$. Now, N/M is a finite normal subgroup of A/M, so is contained in $\Delta^+(A/M)$. Hence the preimage under the natural quotient map $A/M \to A/N$ of $\Delta(A/N)$ is $\Delta(A/M)$. But this is the same as saying that $\nabla_A(N) = \nabla_A(M)$. $\square$

When G is a general compact p-adic analytic group, we will use the following lemma to translate between prime ideals of kG and prime ideals of kA for certain open subgroups A of G.

Lemma 10.2.4. Let H be an open normal subgroup of G. Suppose P is a prime of kG, and write Q for a minimal prime of kH above $P \cap kH$. Let B be the stabiliser in G of Q, and let A be any open subgroup of G containing B, so that

$$H \leq B \leq A \leq G.$$

Then there is a prime ideal T of kA with $P = T^G$, and furthermore this T satisfies $T \cap kH = \bigcap_{a \in A} Q^a$.

Proof. This follows from [22, 14.10(i)]. $\square$

Definition 10.2.5. A prime $P \lhd kG$ is *standard* if it is controlled by Δ and we have $P \cap k\Delta = \bigcap_{x \in G} L^x$ for some almost faithful prime $L \lhd k\Delta$.

Lemma 10.2.6. Let G be a nilpotent-by-finite compact p-adic analytic group and H an open normal subgroup. Let P be a prime ideal of kG, and Q a minimal prime of kH above P, so that $P \cap kH = \bigcap_{x \in G} Q^x$. If Q is a standard prime, then P is a standard prime.

Proof. (Adapted from [22, 20.4(i)].) Write $\Delta = \Delta(G), \Delta_H = \Delta(H)$, and

$$P \cap k\Delta = \bigcap_{x \in G} S^x \qquad \text{and} \qquad Q \cap k\Delta_H = \bigcap_{y \in H} T^y,$$

for prime ideals $S \lhd k\Delta$ and $T \lhd k\Delta_H$. On the one hand,

$$\begin{aligned} P \cap k\Delta_H &= (P \cap k\Delta) \cap k\Delta_H \\ &= \left(\bigcap_{x \in G} S^x \right) \cap k\Delta_H \\ &= \bigcap_{x \in G} \left(S \cap k\Delta_H \right)^x, \end{aligned}$$

but on the other hand,

$$\begin{aligned} P \cap k\Delta_H &= (P \cap kH) \cap k\Delta_H \\ &= \left(\bigcap_{x \in G} Q^x \right) \cap k\Delta_H \\ &= \bigcap_{x \in G} (Q \cap k\Delta_H)^x \\ &= \bigcap_{x \in G} T^x. \end{aligned}$$

Now, the conjugation action of G on Δ_H has kernel $\mathbf{C}_G(\Delta_H)$, which contains $\mathbf{C}_G(\Delta)$ by Lemma 1.2.3(ii). But $\mathbf{C}_G(\Delta) = \bigcap \mathbf{C}_G(a)$, where the intersection runs over a set of topological generators a for Δ, and each $\mathbf{C}_G(a)$ is open in G by definition of Δ. Now, as Δ is topologically finally generated, we see that $\mathbf{C}_G(\Delta)$ and hence $\mathbf{C}_G(\Delta_H)$ are also open in G.

That is, the conjugation action of G on Δ_H factors through the finite group $G/\mathbf{C}_G(\Delta_H)$, and hence the intersections above are finite, so that (by the primality of T), we have

$$S \cap k\Delta_H \subseteq T^x$$

for some $x \in G$.

Now, by assumption, Q is standard, so T is almost faithful. This means that

$$S^\dagger \cap \Delta_H \subseteq (T^\dagger)^x$$

is a finite group, and so, since $[\Delta : \Delta_H] < \infty$, we have that $S^\dagger$ is also finite, so S is almost faithful.

It remains to show that $S^\circ kG = P$. By Proposition 7.3.3, we see that $S^\circ kG = P'$ is a prime ideal of kG contained in P. Now,

$$\begin{aligned}(P \cap kH)kG &= \left(\bigcap_{g\in G} Q^g\right) kG \\ &= \left(\bigcap_{g\in G}\left(\bigcap_{h\in H} T^h kH\right)^g\right) kG \\ &= \left(\bigcap_{g\in G} T^g\right) kG \\ &= (P \cap k\Delta_H)kG && \text{by calculation above} \\ &\subseteq (P \cap k\Delta)kG = P' \subseteq P,\end{aligned}$$

and as H is open and normal in G, we know from Lemma 8.1.2(i) that P is a minimal prime above $(P \cap kH)kG$, so that $P = P'$. $\square$

Finally, the main theorem of this subsection:

Theorem 10.2.7. Let G be a nilpotent-by-finite compact p-adic analytic group, P a prime ideal of kG, H an orbitally sound open normal subgroup of G, Q a minimal prime ideal above $P \cap kH$, and $N = \mathrm{i}_G(Q^\dagger)$. Then there exists an ideal $L \lhd k[[\nabla_G(N)]]$ with $P = L^G$.

Remark. The subgroup N is a *vertex* of the prime ideal P, and the ideal L is a *source* of P corresponding to the vertex H.

Proof. We follow the proof of [17, 2.3], as reproduced in [22, 20.5].

Trivially, H stabilises Q, i.e. $H \leq B := \mathrm{Stab}_G(Q)$; and B normalises $Q^\dagger$. Set $N := \mathrm{i}_G(Q^\dagger)$. Now we must have $\mathbf{N}_G(Q^\dagger) \leq A := \mathbf{N}_G(N)$: indeed, if $x \in G$ normalises $Q^\dagger$, then it permutes the (finitely many) closed orbital subgroups K of G containing $Q^\dagger$ as an open subgroup, and hence it normalises N, which is generated by those K (Definition 1.2.6).

We are in the following situation:

$$\begin{tikzcd}
 & & G \arrow[d, dash] & \\
 & & A \arrow[r, equal] \arrow[d, dash] \arrow[ddl, dash] & \mathbf{N}_G(N) \\
 & & B \arrow[r, equal] \arrow[d, dash] & \mathrm{Stab}_G(Q) \\
 & \nabla_G(N) \arrow[d, dash] & H \arrow[r, dotted, dash] \arrow[dd, dash] & \text{orbitally sound} \\
\mathrm{i}_G(Q^\dagger) \arrow[r, equal] & N \arrow[dr, dash] & & \\
 & & Q^\dagger &
\end{tikzcd}$$

Now, Lemma 10.2.4 shows that there is a prime ideal T of kA with $P = T^G$ and $T \cap kH = \bigcap_{a \in A} Q^a$. It will suffice to show the existence of a prime ideal L of $k[[\nabla_G(N)]]$ with $T = L^A$, by Lemma 8.2.2.

Let M be an open characteristic subgroup of N contained in $Q^\dagger$, whose existence is guaranteed by Lemma 10.2.2. Write $\nabla = \nabla_G(N)$, which we know is equal to $\nabla_A(M)$ by Lemma 10.2.3, and denote by $\overline{(\cdot)}$ images under the natural map $kA \to k[[A/M]]$.

Now Q is a prime ideal of kH with $M \leq Q^\dagger$ an open subgroup, so $\overline{Q}$ is an almost faithful prime ideal of $k\overline{H}$; hence, as $\overline{H}$ is orbitally sound (Lemma 1.2.5(ii)), we see that $\overline{Q}$ is a *standard* prime of $k\overline{H}$.

But $T \cap kH = \bigcap_{a \in A} Q^a$ clearly implies $\overline{T} \cap k\overline{H} = \bigcap_{\overline{a} \in \overline{A}} \overline{Q}^{\overline{a}}$, by the modular law. Now Lemma 10.2.6 implies that $\overline{T}$ is also a standard prime ideal of $k\overline{A}$: that is, there is an almost faithful prime ideal $\overline{L}$ of $k[[\Delta(\overline{A})]]$ with $\overline{T} = \overline{L}^{\overline{A}}$. Lifting this back to kA, we see that we have an almost faithful mod M prime ideal L of $k\nabla$ with $T = L^A$ as required. $\square$

Proof of Theorem C(ii). This follows from Theorem 10.2.7. $\square$

We end this subsection with an important application of this theorem. Recall the definition of $\mathrm{nio}(G)$ from Definition 2.1.5.

Corollary 10.2.8. Suppose G is a nilpotent-by-finite compact p-adic analytic group which is not orbitally sound. Let P be a faithful prime ideal of kG. Then P is induced from some proper open subgroup of G containing $\mathrm{nio}(G)$.

Proof. Write $H = \mathrm{nio}(G)$. H is orbitally sound by Theorem 2.1.6.

Let Q be a minimal prime ideal above $P \cap kH$, so that $N = \mathrm{i}_G(Q^\dagger)$ is a vertex for P by Theorem 10.2.7. Then P is induced from $\nabla_G(N)$, which is contained in $\mathbf{N}_G(N)$, and so P is induced from $\mathbf{N}_G(N)$ itself by Lemma 8.2.2. But, as $\mathrm{nio}(G)$ is orbitally sound, in particular it must normalise N (Theorem 2.1.6(i)). Hence, if $\mathbf{N}_G(N)$ is a proper subgroup of G, we are done.

Suppose instead that $\mathbf{N}_G(N) = G$, i.e. that $\mathrm{i}_G(Q^\dagger)$ is a normal subgroup of G. Then, for each $g \in G$, $(Q^\dagger)^g$ is a finite-index subgroup of $\mathrm{i}_G(Q^\dagger)$ (Proposition 1.2.7); and $Q^\dagger$ is orbital in G, so there are only finitely many $(Q^\dagger)^g$, and their intersection $(Q^\dagger)^\circ$ must also have finite index in $\mathrm{i}_G(Q^\dagger)$. But $(Q^\dagger)^\circ = P^\dagger = 1$, so in particular we have $\mathrm{i}_G(Q^\dagger) = \Delta^+$, and hence P is induced from $\nabla_G(N) = \Delta$, again by Theorem 10.2.7. Hence, as $\mathrm{nio}(G)$ contains Δ, P must be induced from $\mathrm{nio}(G)$ itself. □

10.3 The general case: inducing from open subgroups

Now we will proceed to show that kG is catenary.

Lemma 10.3.1. Let H be an open subgroup of G, and P a prime ideal of kG. Suppose Q is an ideal of kH maximal amongst those ideals A of kH with $A^G \subseteq P$.

Then Q is prime, and P is a minimal prime ideal above Q^G.

Proof. Suppose I and J are ideals strictly containing Q: then, by the maximality of Q, we see that I^G and J^G must strictly contain P. Hence $I^G J^G \subseteq (IJ)^G$ [22, Lemma 14.5] strictly contains P, and so IJ strictly contains Q. Hence Q is prime.

P is clearly a prime ideal containing Q^G, so to show it is minimal it suffices to find any ideal A of kH with P a minimal prime above A^G. Let N be the normal core of H in G, and take $A = (P \cap kN)^H$: then by Lemma 8.2.2 we have $A^G = (P \cap kN)^G = (P \cap kN)kG$, and by Lemma 8.1.2(i), P is a minimal prime above this. $\square$

Lemma 10.3.2. Let H be an open subgroup of G with kH catenary. If $P \lneq P'$ are adjacent primes of kG, and P is induced from kH, then $h(P') = h(P) + 1$.

Proof. (Adapted from [16, 3.3].) Choose an ideal Q (resp. Q') of kH which is maximal amongst those ideals A of kH with $A^G \subseteq P$ (resp. $A^G \subseteq P'$). Then Q and Q' are prime, and P (resp. P') is a minimal prime ideal over Q^G (resp. Q'^G), by Lemma 10.3.1. Hence, by Proposition 8.3.10, we see that it suffices to show that $h(Q') = h(Q) + 1$.

Suppose not. Then there exists some prime ideal I of kH with $Q \lneq I \lneq Q'$; and we may choose a prime ideal J of kG which is minimal over I^G. Then $P \leq J \leq P'$. But $h(Q) < h(I) < h(Q')$ implies (by another application of Proposition 8.3.10) that $h(P) < h(J) < h(P')$, contradicting our assumption that P and P' were adjacent primes. $\square$

Corollary 10.3.3. Let G be a nilpotent-by-finite compact p-adic analytic group, and k a finite field of characteristic p. Then kG is a catenary ring.

Proof. (Adapted from [16, 3.3].) Take two adjacent prime ideals $P \lneq Q$ of kG, and assume without loss of generality that P is faithful. We proceed by induction on the index $[G : \mathrm{nio}(G)]$. When this index equals 1, we are already done by Theorem 10.1.12, so suppose not. Then Corollary 10.2.8 implies that P is induced from some proper open subgroup H of G containing $\mathrm{nio}(G)$. As $\mathrm{nio}(G)$ is an orbitally sound open normal subgroup of H, it must be contained in $\mathrm{nio}(H)$ (by the maximality of $\mathrm{nio}(H)$), and so we have $[H : \mathrm{nio}(H)] < [G : \mathrm{nio}(G)]$. By induction, kH is catenary, so we may now invoke Lemma 10.3.2 to show that $h(Q) = h(P) + 1$. $\square$

Proof of Theorem A. This follows from Corollary 10.3.3. $\square$

Bibliography

[1] E. Aljadeff and D.J.S. Robinson. Semisimple algebras, Galois actions and group cohomology. *Journal of Pure and Applied Algebra*, 94:1–15, 1994.

[2] R.C. Alperin. p-adic binomial coefficients MOD P. *The American Mathematical Monthly*, 92(8):576–578, 1985.

[3] K. Ardakov. Localisation at augmentation ideals in Iwasawa algebras. *Glasgow Mathematical Journal*, 48(2):251–267, 2006.

[4] K. Ardakov. Prime ideals in nilpotent Iwasawa algebras. *Inventiones mathematicae*, 190(2):439–503, 2012.

[5] K. Ardakov and S.J. Wadsley. Characteristic elements for p-torsion Iwasawa modules. *J. Algebraic Geometry*, 15:339–377, 2006.

[6] N. Bourbaki. *Commutative Algebra*. Springer, 1998.

[7] K.A. Brown. The structure of modules over polycyclic groups. *Math. Proc. Cambridge Philos. Soc.*, 89:257–283, 1981.

[8] A. Brumer. Pseudocompact algebras, profinite groups and class formations. *Journal of Algebra*, 4:442–470, 1966.

[9] J.D. Dixon, M.P.F. du Sautoy, A. Mann and D. Segal. *Analytic Pro-p Groups*. Cambridge University Press, 1999.

[10] Li Huishi and Freddy van Oystaeyen. *Zariskian Filtrations.* Springer Science+Business Media, 1996.

[11] K.R. Goodearl, R.B. Warfield, Jr. *An Introduction to Noncommutative Noetherian Rings.* Cambridge University Press, 2004.

[12] S. Mac Lane. *Homology.* Springer, 1963.

[13] Michel Lazard. Groupes analytiques p-adiques. *Publications Mathématiques de l'IHÉS*, 26:5–219, 1965.

[14] B. Lemonnier. Dimension de Krull et codéviation. Application au théorème d'Eakin. *Communications in Algebra*, 6:16:1647–1665, 1978.

[15] Edward S. Letzter. Prime ideals in finite extensions of noetherian rings. *Journal of Algebra*, 135:412–439, 1990.

[16] M. Lorenz, E. Letzter. Polycyclic-by-finite group algebras are catenary. *Math. Res. Lett.*, 6:183–194, 1999.

[17] M. Lorenz and D. S. Passman. Prime ideals in group algebras of polycyclic-by-finite groups. *Proc. London Math. Soc.*, 43:520–543, 1981.

[18] J.C. McConnell and J.C. Robson. *Noncommutative Noetherian Rings.* American Mathematical Society, 2001.

[19] J. Nelson. *Localisation and Euler Characteristics of Soluble Iwasawa Algebras.* PhD thesis, University of Cambridge, 2013.

[20] A. Neumann. Completed group algebras without zero divisors. *Arch. Math.*, 51:496–499, 1988.

[21] Donald S. Passman. *Algebraic Structure of Group Rings.* John Wiley & Sons, 1977.

[22] Donald S. Passman. *Infinite Crossed Products*. Academic Press Inc., 1989.

[23] Derek J.S. Robinson. *A course in the theory of groups*. Springer-Verlag New York, 1996.

[24] J.E. Roseblade. Prime ideals in group rings of polycyclic groups. *Proc. London Math. Soc.*, 36:385–447, 1978.

[25] O. Zariski, P. Samuel. *Commutative Algebra*. D. Van Nostrand Company, 1965.

[26] T. Schmidt. Auslander regularity of p-adic distribution algebras. *Representation Theory*, 12:37–57, 2008.

[27] D. Segal. *Polycyclic groups*. Cambridge University Press, 2005.

[28] The Stacks Project Authors. *Stacks Project*. `http://stacks.math.columbia.edu`, 2016.

[29] R.G. Swan. Goldie's theorem. `http://math.uchicago.edu/~swan/expo/Goldie.pdf`.