

ON THE SECOND COHOMOLOGY OF THE NORM ONE GROUP OF A p -ADIC DIVISION ALGEBRA

MIKHAIL ERSHOV

with an appendix on

exp $-\log$ **correspondence for powerful p -central \mathbb{Z}_p -Lie algebras and pro- p groups**

by MIKHAIL ERSHOV and THOMAS WEIGEL

To Gopal Prasad on the occasion of his 75th birthday

ABSTRACT. Let F be a p -adic field, that is, a finite extension of \mathbb{Q}_p . Let D be a finite-dimensional central division algebra over F and let $SL_1(D)$ be the group of elements of reduced norm 1 in D . Prasad and Raghunathan proved that $H^2(SL_1(D), \mathbb{R}/\mathbb{Z})$ is a cyclic p -group whose order is bounded from below by the number of p -power roots of unity in F , unless D is a quaternion algebra over \mathbb{Q}_2 . In this paper we give an explicit upper bound for the order of $H^2(SL_1(D), \mathbb{R}/\mathbb{Z})$ for $p \geq 5$, and determine $H^2(SL_1(D), \mathbb{R}/\mathbb{Z})$ precisely when F is cyclotomic, $p \geq 19$ and the degree of D is not a power of p .

1. INTRODUCTION

Let F be a nonarchimedean local field of residue characteristic p , that is, a finite extension of \mathbb{Q}_p or the field of Laurent series over a finite field of characteristic p . Let G be the group of rational points of a connected simply-connected simple algebraic group \mathbb{G} defined over F . By results of Moore [Mo2] and Prasad and Raghunathan [PR1],[PR2], the second continuous cohomology group $^1 H^2(G, \mathbb{R}/\mathbb{Z})$ classifies topological central extensions of G (see [PR1, Chapter 10] for a detailed discussion). If F has characteristic zero, finiteness of $H^2(G, \mathbb{R}/\mathbb{Z})$ follows from a general theorem of Raghunathan [Ra]. ² However, the exact determination of the above group (for F of either characteristic) is a deeper problem which received a lot of attention since mid 60's starting with a work of Moore [Mo1] and culminating in works of Prasad and Raghunathan [PR1] and [PR2]. It is now known that if \mathbb{G} is **isotropic** over F then $H^2(G, \mathbb{R}/\mathbb{Z})$ is isomorphic to the group of roots of unity in F . Using Moore's paper [Mo1], Matsumoto [Ma] proved this result for F -split groups, and the case of F -quasi-split groups is due to Deodhar [De] and Deligne

The author is grateful for the support and hospitality of the Institute for Advanced Study where part of this research was carried out. The author was supported by the National Science Foundation under agreement No. DMS-0111298.

¹Here \mathbb{R}/\mathbb{Z} is endowed with its usual topology, and the action of G on \mathbb{R}/\mathbb{Z} is trivial

²A very short proof of this fact was later found by Prasad [Pr1].

(unpublished). Almost all remaining cases were handled in [PR1], and finally the complete answer was obtained in [PRp].³

If \mathbb{G} is anisotropic over F , then by Tits' classification G is isomorphic to $SL_1(D)$ for some finite-dimensional central division algebra D over F . Since $SL_1(D)$ is profinite, $H^2(SL_1(D), \mathbb{R}/\mathbb{Z})$ is isomorphic to $H^2(SL_1(D), \mathbb{Q}/\mathbb{Z})$, where \mathbb{Q}/\mathbb{Z} is endowed with discrete topology (see [PR2, 2.0]). Moreover, $H^2(SL_1(D), \mathbb{Q}/\mathbb{Z})$ is isomorphic to $H^2(SL_1(D), (\mathbb{Q}/\mathbb{Z})_p)$, where $(\mathbb{Q}/\mathbb{Z})_p$ is the p -primary component of \mathbb{Q}/\mathbb{Z} (see [PR2, 2.1]). The main result of [PR2] asserts that $H^2(SL_1(D), (\mathbb{Q}/\mathbb{Z})_p)$ is a cyclic p -group whose order is bounded from below by the number of p -power roots of unity in F , unless D is the quaternion division algebra over \mathbb{Q}_2 . Moreover, $H^2(SL_1(D), (\mathbb{Q}/\mathbb{Z})_p)$ is trivial if F has no p -power roots of unity (in particular, if F has characteristic p) and D is not a quaternion division algebra over \mathbb{Q}_3 .

The goal of this paper is to obtain an explicit upper bound for the order of $H^2(SL_1(D), \mathbb{R}/\mathbb{Z})$ when F has characteristic zero and $p \geq 5$. Part (a) of the following theorem provides such a bound in the general case, parts (b) and (c) give stronger bounds in some special cases, and part (d) gives a precise order for $H^2(SL_1(D), \mathbb{R}/\mathbb{Z})$ in the case of cyclotomic fields:

Theorem 1.1. *Let F be a finite extension of \mathbb{Q}_p , let e be the ramification index of F , and let p^w be the highest power of p dividing e . Let D be a finite-dimensional central division algebra over F , and let p^N be the order of $H^2(SL_1(D), \mathbb{R}/\mathbb{Z}) \cong H^2(SL_1(D), (\mathbb{Q}/\mathbb{Z})_p)$.*

- (a) *Assume that $p \geq 5$. Then $N \leq w + 6$.*
- (b) *Assume that $p \geq 4w + 15$. Then $N \leq w + 1$.*
- (c) *Assume that $p \geq 19$, the degree of D is not a power of p , the extension F/\mathbb{Q}_p is Galois, and F contains p^2 th primitive root of unity. Then $N \leq w + 1$.*
- (d) *Assume that $p \geq 19$, the degree of D is not a power of p , and F is a cyclotomic field. Then $N = w + 1$.*

Note that Theorem 1.1(d) immediately follows from Theorem 1.1(b)(c) and [PR2, Theorem 8.1]. Indeed, if $F = \mathbb{Q}_p(\sqrt[p]{1})$ and p^k is the highest power of p dividing n , then $e = p^{k-1}(p-1)$ and $w = k-1$. Thus $|H^2(SL_1(D), \mathbb{R}/\mathbb{Z})| \leq p^k$ by Theorem 1.1(c) if $k \geq 2$ and by Theorem 1.1(b) if $k = 1$, while [PR2, Theorem 8.1] yields $|H^2(SL_1(D), \mathbb{R}/\mathbb{Z})| \geq p^k$.

We now give a brief sketch of the proof of Theorem 1.1. Let $G = SL_1(D)$. In [PR2] it is shown that $H^2(G, (\mathbb{Q}/\mathbb{Z})_p)$ is isomorphic to $H^2(G, \mathbb{Z}/p^k\mathbb{Z})$ for sufficiently large k . Both G and $\mathbb{Z}/p^k\mathbb{Z}$ are p -adic analytic, so it is natural to ask if the order of $H^2(G, \mathbb{Z}/p^k\mathbb{Z})$ can be computed using Lie algebras. In the theory of p -adic analytic groups there is a well-known exp-log correspondence between (finitely generated) powerful torsion-free pro- p groups and powerful torsion-free \mathbb{Z}_p -Lie algebras. This is not enough for our purposes; however, what we can use is a work of Weigel [Weig], who extended the above correspondence to the classes of powerful p -central pro- p groups and Lie algebras (see § 3 for definitions).

³The argument in [PRp] uses global fields, but later Prasad [Pr2] found a purely local proof.

Now consider the congruence subgroup $H = SL_1^{de+1}(D)$ where d is the degree of D . It is easy to see that H is powerful and torsion-free. Let $\mathbf{res}_{G|H}$ be the restriction map from $H^2(G, \mathbb{Z}/p^k\mathbb{Z})$ to $H^2(H, \mathbb{Z}/p^k\mathbb{Z})$. At the end of § 5 we will show that $\mathbf{res}_{G|H}$ has small kernel (see Proposition 5.9). Next we will prove that any cohomology class lying in the image of $\mathbf{res}_{G|H}$ is represented by a (central) extension $1 \rightarrow \mathbb{Z}/p^k\mathbb{Z} \rightarrow \widehat{H} \rightarrow H \rightarrow 1$ where \widehat{H} is powerful and p -central (see Lemma 6.3). Applying Weigel's log functor we obtain the corresponding extension of powerful p -central Lie algebras. This extension, in turn, represents some cohomology class in $H^2(\mathfrak{h}, \mathbb{Z}/p^k\mathbb{Z})$, where \mathfrak{h} is the \mathbb{Z}_p -Lie algebra of H . Moreover, the obtained cohomology class is invariant under the natural action of G on $H^2(\mathfrak{h}, \mathbb{Z}/p^k\mathbb{Z})$. These results lead to an upper bound for the order of $H^2(G, \mathbb{Z}/p^k\mathbb{Z})$ in terms of the exponent of the G -invariant part of $H^2(\mathfrak{h}, \mathbb{Z}/p^k\mathbb{Z})$. Finally, in § 7 we obtain an explicit description of G -invariant classes in $H^2(\mathfrak{h}, \mathbb{Z}/p^k\mathbb{Z})$, which yields the bound given in Theorem 1.1(a).

The proof of Theorem 1.1(b) is based on similar ideas, but is considerably more technical. Instead of Weigel's correspondence we use Lazard's exp-log correspondence between finite groups and finite Lie rings of p -power order and nilpotency class less than p . The reduction of Theorem 1.1(b) to computation of cohomology of finite p -groups is based on the analysis of the inflation map $H^2(G/G_m, \mathbb{Z}/p^k\mathbb{Z}) \rightarrow H^2(G, \mathbb{Z}/p^k\mathbb{Z})$ for $m \in \mathbb{N}$, where $G_m = SL_1^m(D)$.

Finally, to prove Theorem 1.1(c) we use the following simple fact pointed out to the author by Gopal Prasad: If F/F_0 is an extension of p -adic fields and D is a central division algebra over F whose degree is relatively prime to $[F : F_0]$, then $D \cong D_0 \otimes_{F_0} F$ for some division algebra D_0 over F_0 . Furthermore, certain information about the restriction map $H^2(SL_1(D), \mathbb{R}/\mathbb{Z}) \rightarrow H^2(SL_1(D_0), \mathbb{R}/\mathbb{Z})$ is provided by [PR2]. Using this idea, we reduce the proof of Theorem 1.1(c) to the case of division algebras over p -adic fields of small degree, where Theorem 1.1(b) becomes applicable.

Organization. In § 2 we discuss the basic relation between cohomology and central extensions for profinite groups and Lie algebras. In § 3 we describe exp-log correspondence between certain classes of p -adic analytic pro- p groups and \mathbb{Z}_p -Lie algebras. We then use this correspondence to establish a relationship between the second cohomology of pro- p groups and Lie algebras belonging to those classes. In § 4 we review basic facts about division algebras over local fields. In § 5 we study group-theoretic properties of central extensions of $SL_1(D)$ where D is a division algebra over a p -adic field. In § 6 we deduce parts (a) and (b) of Theorem 1.1 from certain results on Lie algebra cohomology which, in turn, are proved in § 7. Finally, in § 8 we prove Theorem 1.1(c).

Restrictions on p . While all parts of Theorem 1.1 require at least that $p \geq 5$, most of our auxiliary results hold for $p = 3$ and some even for $p = 2$. In § 5 and § 7 we will impose a general restriction on p and d (where d is the degree of the division algebra D under consideration) at the beginning of the section; in other sections we will state the restrictions separately for each result.

Basic notations. Throughout the paper \mathbb{Z} will stand for integers, \mathbb{N} for positive integers, \mathbb{Z}_p for p -adic integers and \mathbb{F}_p for a finite field of order p . If G is a topological group, $\gamma_n G$ will denote the closure of the n^{th} term of the lower central series of G , and G^n the closed subgroup of G generated by n^{th} powers. If A and B are subsets of G , let $[A, B]$ be the closed subgroup generated by $\{[a, b] : a \in A, b \in B\}$, where $[a, b] = a^{-1}b^{-1}ab$. If x_1, \dots, x_k are elements of some Lie ring L , the left-normed commutator $[x_1, \dots, x_k]$ is defined inductively by $[x_1, \dots, x_k] = [[x_1, \dots, x_{k-1}], x_k]$ for $k \geq 3$.

Acknowledgements. I am very grateful to Gopal Prasad for posing the problem, very interesting conversations, and suggesting an idea that resulted in significant improvement of the results of this paper. I am very thankful to Thomas Weigel for sending me his unpublished manuscript [Weig]. I would also like to thank Andrei Jaikin and Thomas Weigel for helpful discussions related to this paper and the anonymous referee for a number of useful suggestions.

2. CENTRAL EXTENSIONS AND SECOND COHOMOLOGY

2.1. Central extensions and cohomology for profinite groups. In this subsection we briefly recall the connection between topological central extensions of a profinite group and its second continuous cohomology.

Let H be a profinite group and let A be an abelian profinite group, considered as a trivial H -module. Denote by $\text{Ext}(H, A)$ the set of equivalence classes of *topological central extensions* of H by A , that is, extensions of the form

$$1 \rightarrow A \xrightarrow{\iota} \widehat{H} \xrightarrow{\varphi} H \rightarrow 1 \quad \text{or, in abbreviated form,} \quad A \xhookrightarrow{\iota} \widehat{H} \twoheadrightarrow^{\varphi} H,$$

where ι and φ are continuous and $\iota(A)$ is central in \widehat{H} (note that the group \widehat{H} is automatically profinite). Recall that two extensions $1 \rightarrow A \xrightarrow{\iota_1} \widehat{H}_1 \xrightarrow{\varphi_1} H \rightarrow 1$ and $1 \rightarrow A \xrightarrow{\iota_2} \widehat{H}_2 \xrightarrow{\varphi_2} H \rightarrow 1$ are equivalent if there exists a (continuous)⁴ isomorphism $\alpha : \widehat{H}_1 \rightarrow \widehat{H}_2$ which makes the following diagram commutative:

$$(2.1) \quad \begin{array}{ccccccc} 1 & \longrightarrow & A & \xrightarrow{\iota_1} & \widehat{H}_1 & \xrightarrow{\varphi_1} & H \longrightarrow 1 \\ & & \downarrow & & \downarrow \alpha & & \downarrow \text{id} \\ & & 1 & \longrightarrow & A & \xrightarrow{\iota_2} & \widehat{H}_2 \xrightarrow{\varphi_2} H \longrightarrow 1 \end{array}$$

To avoid complicated notations we will not be explicitly distinguishing between extensions and their equivalence classes.

Next recall that $\text{Ext}(H, A)$ is an abelian group with respect to the Baer sum defined as follows: let $\mathcal{E}_1 = (A \xhookrightarrow{\iota_1} \widehat{H}_1 \twoheadrightarrow^{\varphi_1} H)$ and $\mathcal{E}_2 = (A \xhookrightarrow{\iota_2} \widehat{H}_2 \twoheadrightarrow^{\varphi_2} H)$ be two elements of $\text{Ext}(H, A)$. Then

$$\mathcal{E}_1 + \mathcal{E}_2 = (A \xhookrightarrow{\iota} \widehat{H}/\widehat{N} \twoheadrightarrow^{\varphi} H)$$

⁴Since profinite groups are compact and Hausdorff, the inverse map α^{-1} is automatically continuous as well.

where $\widehat{H} = \{(x_1, x_2) \in \widehat{H}_1 \times \widehat{H}_2 : \varphi_1(x_1) = \varphi_2(x_2)\}$, $\widehat{N} = \{(\iota_1(a), \iota_2(a^{-1})) : a \in A\}$, $\iota(a) = (\iota_1(a), 1)\widehat{N} = (1, \iota_2(a))\widehat{N}$, and $\varphi((x_1, x_2)\widehat{N}) = \varphi_1(x_1) = \varphi_2(x_2)$.

For any element $\mathcal{E} = (A \xrightarrow{\iota} \widehat{H} \xrightarrow{\varphi} H)$ of $\text{Ext}(H, A)$ its inverse is $-\mathcal{E} = (A \xrightarrow{\iota'} \widehat{H} \xrightarrow{\varphi} H)$ where $\iota'(a) = \iota(a)^{-1}$ for all $a \in A$.

Now let $H^2(H, A)$ be the second continuous cohomology of H , that is, the second cohomology based on the standard complex where cochains are required to be continuous. Thus $H^2(H, A) = Z^2(H, A)/B^2(H, A)$ where the group $Z^2(H, A)$ of 2-cocycles consists of continuous functions $f : H \times H \rightarrow A$ such that

$$f(xy, z) + f(x, y) = f(y, z) + f(x, yz) \text{ for all } x, y, z \in H$$

and the group $B^2(H, A)$ of 2-coboundaries consists of continuous functions $f : H \times H \rightarrow A$ of the form $f(x, y) = u(x) + u(y) - u(xy)$ for some continuous function $u : H \rightarrow A$.

There exists a canonical isomorphism of abelian groups $H^2(H, A) \cong \text{Ext}(H, A)$ defined as follows:

Given $C \in H^2(H, A)$, let $Z : H \times H \rightarrow A$ be a 2-cocycle whose cohomology class is equal to C . Let \widehat{H} be the set of pairs $\{(h, a) : h \in H, a \in A\}$ with multiplication given by

$$(2.2) \quad (h_1, a_1) \cdot (h_2, a_2) = (h_1 h_2, a_1 + a_2 + Z(h_1, h_2))$$

The central extension corresponding to C is $A \xrightarrow{\iota} \widehat{H} \xrightarrow{\varphi} H$ where $\iota(a) = (1, a)$ and $\varphi((h, a)) = h$ for any $a \in A$ and $h \in H$. We will denote (the equivalence class of) this extension by $\text{Ext}(C)$.

Conversely, let $\mathcal{E} = (1 \rightarrow A \xrightarrow{\iota} \widehat{H} \xrightarrow{\varphi} H \rightarrow 1)$ be an element of $\text{Ext}(H, A)$. Let $\psi : H \rightarrow \widehat{H}$ be a continuous section of φ , that is, a continuous map $H \rightarrow \widehat{H}$ such that $\varphi \circ \psi = \text{id}_H$ (such a section exists since \widehat{H} and H are profinite – see, e.g. [Wil, 1.3.3]), and define $Z : H \times H \rightarrow A$ by

$$Z(h_1, h_2) = \iota^{-1}(\psi(h_1 h_2)^{-1} \psi(h_1) \psi(h_2)).$$

Then Z is a 2-cocycle whose cohomology class $[Z]$ is independent of the choice of ψ , and $\text{Ext}([Z]) = \mathcal{E}$.

2.2. Central extensions and cohomology for Lie algebras. On the Lie algebra side, we will discuss the connection between central extensions and cohomology in the abstract (discrete) case since we are not aware of the corresponding reference in the topological case. The discrete case will be sufficient for the purposes of this paper since we will work with extensions inside the category of \mathbb{Z}_p -Lie algebras which are finitely generated as \mathbb{Z}_p -modules, and any homomorphism between such Lie algebras is automatically continuous with respect to pro- p topologies (see the discussion at the beginning of § 3).

Fix a commutative ring R with 1, let \mathfrak{h} be an R -Lie algebra, and let \mathfrak{a} be an R -module considered as an abelian R -Lie algebra and as a trivial \mathfrak{h} -module. As in the group case, denote by $\text{Ext}(\mathfrak{h}, \mathfrak{a})$ the set of equivalence classes of central R -Lie

algebra extensions $0 \rightarrow \mathfrak{a} \xrightarrow{\iota} \widehat{\mathfrak{h}} \xrightarrow{\varphi} \mathfrak{h} \rightarrow 0$. The addition is defined in complete analogy with the group case.

It is still true that $\text{Ext}(\mathfrak{h}, \mathfrak{a})$ is isomorphic to $H^2(\mathfrak{h}, \mathfrak{a})$; however, we are not aware of a simple-to-describe cochain complex that can be used to compute the cohomology groups. Here the cohomology groups are defined functorially as $H^k(\mathfrak{h}, \mathfrak{a}) = \text{Ext}_{\mathcal{U}\mathfrak{h}}^k(R, \mathfrak{a})$ where $\mathcal{U}\mathfrak{h}$ is the universal enveloping algebra of \mathfrak{h} and R is considered as a trivial \mathfrak{h} -module.

Consider now the important special case where \mathfrak{h} is a free R -module. In this case, one can compute the cohomology groups $H^k(\mathfrak{h}, \mathfrak{a})$ similarly to the group case, using the Chevalley-Eilenberg complex. In particular, $H^2(\mathfrak{h}, \mathfrak{a})$ is isomorphic to $Z^2(\mathfrak{h}, \mathfrak{a})/B^2(\mathfrak{h}, \mathfrak{a})$ where $Z^2(\mathfrak{h}, \mathfrak{a})$ consists of R -bilinear functions $f : \mathfrak{h} \times \mathfrak{h} \rightarrow \mathfrak{a}$ such that

- (i) $f(x, x) = 0$ for all $x \in \mathfrak{h}$
- (ii) $f([x, y], z) + f([y, z], x) + f([z, x], y) = 0$ for all $x, y, z \in \mathfrak{h}$.

and $B^2(\mathfrak{h}, \mathfrak{a}) \subseteq Z^2(\mathfrak{h}, \mathfrak{a})$ is the set of all R -bilinear maps $f : \mathfrak{h} \times \mathfrak{h} \rightarrow \mathfrak{a}$ of the form $f(x, y) = u([x, y])$ for some R -linear function $u : \mathfrak{h} \rightarrow \mathfrak{a}$.

The canonical isomorphism between $H^2(\mathfrak{h}, \mathfrak{a})$ and $\text{Ext}(\mathfrak{h}, \mathfrak{a})$ in this special case is defined similarly to groups:

If $c \in H^2(\mathfrak{h}, \mathfrak{a})$ and $z : \mathfrak{h} \times \mathfrak{h} \rightarrow \mathfrak{a}$ is a 2-cocycle representing c , we define $\text{Ext}(c) \in \text{Ext}(\mathfrak{h}, \mathfrak{a})$ to be the extension $0 \rightarrow \mathfrak{a} \xrightarrow{\iota} \widehat{\mathfrak{h}} \xrightarrow{\varphi} \mathfrak{h} \rightarrow 0$, where $\widehat{\mathfrak{h}} = \mathfrak{h} \oplus \mathfrak{a}$ as an R -module with Lie bracket $[(h_1, a_1), (h_2, a_2)] = ([h_1, h_2], z(h_1, h_2))$.

Conversely, let $\mathcal{E} = (0 \rightarrow \mathfrak{a} \xrightarrow{\iota} \widehat{\mathfrak{h}} \xrightarrow{\varphi} \mathfrak{h} \rightarrow 0)$ be an element of $\text{Ext}(\mathfrak{h}, \mathfrak{a})$. Since \mathfrak{h} is a free R -module, there exists an R -linear section $\psi : \mathfrak{h} \rightarrow \widehat{\mathfrak{h}}$, and it is easy to check that $\mathcal{E} = \text{Ext}([z])$ where $z \in Z^2(\mathfrak{h}, \mathfrak{a})$ is defined by

$$(2.3) \quad z(h, k) = \iota^{-1}(\psi([h, k]) - [\psi(h), \psi(k)]).$$

Going back to the general case (where \mathfrak{h} is not necessarily free), one can still define the groups $Z^2(\mathfrak{h}, \mathfrak{a})$ and $B^2(\mathfrak{h}, \mathfrak{a})$ and the map $\text{Ext} : Z^2(\mathfrak{h}, \mathfrak{a})/B^2(\mathfrak{h}, \mathfrak{a}) \rightarrow \text{Ext}(\mathfrak{h}, \mathfrak{a})$ as above; however, this map need not be surjective. In [HZ] it was shown that at least in the special case $R = \mathbb{Z}$ there are natural generalizations $\widetilde{Z}^2(\mathfrak{h}, \mathfrak{a})$ and $\widetilde{B}^2(\mathfrak{h}, \mathfrak{a})$ of the spaces $Z^2(\mathfrak{h}, \mathfrak{a})$ and $B^2(\mathfrak{h}, \mathfrak{a})$ defined above with the property that $\widetilde{Z}^2(\mathfrak{h}, \mathfrak{a})/\widetilde{B}^2(\mathfrak{h}, \mathfrak{a}) \cong \text{Ext}(\mathfrak{h}, \mathfrak{a})$. However, we do not know if there is a natural cochain complex whose cohomology groups are isomorphic to $H^k(\mathfrak{h}, \mathfrak{a})$ which yields the same definitions of 2-cocycles and 2-coboundaries.

2.3. Restriction and inflation maps. In this subsection we will define the restriction and inflation maps on the second cohomology groups for profinite groups and Lie algebras directly in terms of the associated central extensions. We will also describe the image of the inflation map in terms of the associated central extensions.

We start by recalling the usual definition of the restriction and inflation maps for profinite groups in terms of cocycles. So let H be a profinite group, N a closed subgroup of H and A an abelian profinite group considered as a trivial H -module.

The restriction $\text{res} : H^2(H, A) \rightarrow H^2(N, A)$ is induced from the restriction map (in the obvious sense) on cocycles $\text{Res} : Z^2(H, A) \rightarrow Z^2(N, A)$.

If N is normal in H , the inflation $\text{inf} : H^2(H/N, A) \rightarrow H^2(H, A)$ is induced from the map $\text{Inf} : Z^2(H/N, A) \rightarrow Z^2(H, A)$ given by $(\text{Inf } f)(x, y) = f(xN, yN)$ for all $f \in Z^2(H/N, A)$ and $x, y \in H$.

Let us now rephrase these definitions in terms of central extensions. So let $c \in H^2(H, A)$, and let $\mathcal{E} = (A \xrightarrow{\iota} \widehat{H} \xrightarrow{\varphi} H) \in \text{Ext}(H, A)$ be the corresponding central extension. Then it is easy to see that $\text{res}(\mathcal{E}) \in \text{Ext}(N, A)$, the restriction of \mathcal{E} , is given by $\text{res}(\mathcal{E}) = (A \xrightarrow{\iota} \varphi^{-1}(N) \xrightarrow{\varphi} N)$.

Assume now that N is normal in H , $c \in H^2(H/N, A)$ and

$$\mathcal{E} = (A \xrightarrow{\iota} E \xrightarrow{\varphi} H) \in \text{Ext}(H/N, A)$$

is the corresponding central extension. Let $\pi : H \rightarrow H/N$ be the natural projection, and let P be the pullback of the diagram $E \xrightarrow{\varphi} H/N \xleftarrow{\pi} H$, that is,

$$P = \{(x, y) \in E \times H : \varphi(x) = \pi(y)\}.$$

It takes a little work (see, e.g. [Weib, Exercise 6.6.4, p. 285]) to check that the inflation $\text{inf}(\mathcal{E}) \in \text{Ext}(H, A)$ is given by $\text{inf}(\mathcal{E}) = (A \xrightarrow{\iota'} P \xrightarrow{\varphi'} H)$ where $\iota'(a) = (\iota(a), 1)$ for all $a \in A$ and $\varphi'(x, y) = y$ for all $(x, y) \in P$.

Both definitions of the restriction and inflation maps have direct analogues for R -Lie algebras. The definitions in terms of central extensions (which are most suitable for our purposes) remain exactly the same. The definitions in terms of cocycles extend (with obvious changes) to the subsets of the cohomology groups corresponding to extensions which split on the level of R -modules; for the general case (which is still quite similar) we refer the reader to [HZ].

The next lemma provides a characterization for the image of the inflation map between second cohomology groups in terms of the associated central extensions. Although this is a standard result, we are not aware of a reference in the literature.

Lemma 2.1. *Let H be a profinite group, N a closed normal subgroup of H , and let A be an abelian profinite group (considered as a trivial H -module). Fix $c \in H^2(H, A)$ with $\text{Ext}(c) = (1 \rightarrow A \xrightarrow{\iota} \widehat{H} \xrightarrow{\varphi} H \rightarrow 1)$. Let $\text{inf} : H^2(H/N, A) \rightarrow H^2(H, A)$ be the inflation map.*

- (a) *Suppose that $c = \text{inf}(c')$ for some $c' \in H^2(H/N, A)$. Then there exists a continuous section ψ of φ (i.e. a map $\psi : H \rightarrow \widehat{H}$ with $\varphi\psi = \text{id}_H$) such that $\psi(N)$ is a normal subgroup of \widehat{H} .*
- (b) *Conversely, suppose that φ has a continuous section ψ such that $\psi(N)$ is a normal subgroup of \widehat{H} . Let $c' \in H^2(H/N, A)$ be the cohomology class corresponding to the extension*

$$\mathcal{E}' = (1 \rightarrow A \xrightarrow{\iota'} \widehat{H}/\psi(N) \xrightarrow{\varphi'} H/N \rightarrow 1)$$

where ι' and φ' are induced by ι and φ , respectively. Then $c = \text{inf}(c')$.

Proof. In both parts we let $Q = H/N$ and $\pi : H \rightarrow Q$ is the natural projection.

(a) Let $(A \xrightarrow{\iota'} \widehat{Q} \xrightarrow{\varphi'} Q)$ be the extension corresponding to c' . Then (up to equivalence) we have $\text{Ext}(c) = (A \xrightarrow{\iota} \widehat{H} \xrightarrow{\varphi} H)$ where $\widehat{H} = \{(x, y) \in \widehat{Q} \times H : \varphi'(x) = \pi(y)\}$, and ι and φ are defined by $\iota(m) = (\iota'(m), 1)$ for any $m \in A$ and $\varphi(x, y) = y$ for any $y \in H$.

Now choose a continuous section $\psi' : Q \rightarrow \widehat{Q}$ of φ' such that $\psi'(1) = 1$, and define $\psi : H \rightarrow \widehat{H}$ by $\psi(y) = (\psi'(\pi(y)), y)$. Clearly, ψ is a continuous section of φ , and $\psi(N) = \{(1, y) : y \in N\}$ is a normal subgroup of \widehat{H} .

(b) Let $c'' = \inf(c')$. Then by definition $\text{Ext}(c'') = (A \hookrightarrow P \twoheadrightarrow H)$ where $P = \{(x, y) \in \widehat{H}/\psi(N) \times H : \varphi'(x) = \pi(y)\}$. It is straightforward to check that the map $\alpha : \widehat{H} \rightarrow P$ given by $\alpha(z) = (z\psi(N), \pi(z))$ is a continuous isomorphism (hence also bi-continuous since both groups are compact) which yields equivalence of the extensions $(A \hookrightarrow P \twoheadrightarrow H)$ and $(A \hookrightarrow \widehat{H} \twoheadrightarrow H)$. Thus $c = c''$, as desired. \square

2.4. Equivariant extensions and cohomology classes. Let H and A be profinite groups with A abelian, and suppose that G is another group which acts on both H and A by continuous automorphisms. An extension $A \xrightarrow{\iota} \widehat{H} \xrightarrow{\varphi} H$ will be called **G -equivariant** if there exists an action of G on \widehat{H} by continuous automorphisms which is compatible with the G -action on H and A , that is,

$$\iota(a)^g = \iota(a^g) \text{ for any } a \in A \text{ and } g \in G, \text{ and } \varphi(x^g) = \varphi(x)^g \text{ for any } x \in \widehat{H} \text{ and } g \in G.$$

We will denote the subset of G -equivariant extensions by $\text{Ext}(H, A)^G$.

An element $c \in H^2(H, A)$ will be called G -equivariant if $\text{Ext}(c) \in \text{Ext}(H, A)^G$, and $H^2(H, A)^G$ will denote the set of G -equivariant elements. Note that the standard meaning of $H^2(H, A)^G$ is different from ours: $H^2(H, A)^G$ usually denotes the set of cohomology classes which are invariant with respect to the canonical action of G on $H^2(H, A)$. It is not hard to show that G -equivariant cohomology classes are invariant under the G -action of $H^2(H, A)$, but the converse is not necessarily true (these facts will not be used in our paper).

Likewise if $\mathfrak{h}, \mathfrak{a}$ are R -Lie algebras, with \mathfrak{a} abelian, and G acts on both \mathfrak{h} and \mathfrak{a} by R -Lie algebra automorphisms, we define $\text{Ext}(\mathfrak{h}, \mathfrak{a})^G$ and $H^2(\mathfrak{h}, \mathfrak{a})^G$ in the same way.

All parts of Lemma 2.2 below are straightforward and follow immediately from the definitions of addition and inversion in Ext groups and the definitions of restriction and inflation maps in terms of central extensions.

Lemma 2.2. *The following hold:*

- (a) *Let H and A be profinite groups, with H abelian, and let G be a group which acts on both H and A by continuous automorphisms. Then*
 - (i) *$\text{Ext}(H, A)^G$ is a subgroup of $\text{Ext}(H, A)$.*
 - (ii) *Let N be a G -invariant closed subgroup of H . Then the restriction map $\text{Ext}(H, A) \rightarrow \text{Ext}(N, A)$ sends $\text{Ext}(H, A)^G$ to $\text{Ext}(N, A)^G$.*
 - (iii) *Let N be a G -invariant closed normal subgroup of H . Then the inflation map $\text{Ext}(H/N, A) \rightarrow \text{Ext}(H, A)$ sends $\text{Ext}(H/N, A)^G$ to $\text{Ext}(H, A)^G$.*

- (b) Let R be a commutative ring with 1, let \mathfrak{h} and \mathfrak{a} be R -Lie algebras, with \mathfrak{h} abelian, and let G be a group which acts on both \mathfrak{h} and \mathfrak{a} by R -Lie algebra automorphisms. Then
- (i) $\text{Ext}(\mathfrak{h}, \mathfrak{a})^G$ is a subgroup of $\text{Ext}(\mathfrak{h}, \mathfrak{a})$.
 - (ii) Let \mathfrak{n} be a G -invariant Lie subalgebra of \mathfrak{h} . Then the restriction map $\text{Ext}(\mathfrak{h}, \mathfrak{a}) \rightarrow \text{Ext}(\mathfrak{n}, \mathfrak{a})$ sends $\text{Ext}(\mathfrak{h}, \mathfrak{a})^G$ to $\text{Ext}(\mathfrak{n}, \mathfrak{a})^G$.
 - (iii) Let \mathfrak{n} be a G -invariant ideal of \mathfrak{h} . Then the inflation map $\text{Ext}(\mathfrak{h}/\mathfrak{n}, \mathfrak{a}) \rightarrow \text{Ext}(\mathfrak{h}, \mathfrak{a})$ sends $\text{Ext}(\mathfrak{h}/\mathfrak{n}, \mathfrak{a})^G$ to $\text{Ext}(\mathfrak{h}, \mathfrak{a})^G$.

3. EXP-LOG CORRESPONDENCE

3.1. Exp and log functors and their basic properties. We will say that a \mathbb{Z}_p -Lie algebra L is of *finite rank* if L is finitely generated as a \mathbb{Z}_p -module. Any such L is isomorphic as a \mathbb{Z}_p -module to $\mathbb{Z}_p^n \oplus P$ for some $n \in \mathbb{Z}_{\geq 0}$ and finite abelian p -group P , and thus $(L, +)$ has a structure of a finitely generated pro- p group. This structure is independent of the choice of an isomorphism $L \cong \mathbb{Z}_p^n \oplus P$, e.g., since any homomorphism between finitely generated pro- p groups is continuous⁵. Moreover, in this way L becomes a (Hausdorff) topological \mathbb{Z}_p -Lie algebra, that is, the addition and Lie bracket are continuous as maps from $L \times L$ to L and scalar multiplication is continuous as a map from $\mathbb{Z}_p \times L$ to L .

Let $\mathfrak{L}_{\mathbb{Z}_p}$ (resp. $\mathfrak{G}_{\mathbb{Z}_p}$) be the category whose objects are \mathbb{Z}_p -Lie algebras of finite rank (resp. p -adic analytic pro- p groups) and whose morphisms are \mathbb{Z}_p -Lie algebra (resp. group) homomorphisms. Since p -adic analytic pro- p groups are finitely generated, by the explanation in the previous paragraph any morphism in $\mathfrak{L}_{\mathbb{Z}_p}$ or $\mathfrak{G}_{\mathbb{Z}_p}$ is automatically continuous.

If \mathfrak{L} is a subcategory of $\mathfrak{L}_{\mathbb{Z}_p}$ and \mathfrak{G} is a subcategory of $\mathfrak{G}_{\mathbb{Z}_p}$, by an **exp-log correspondence** between \mathfrak{L} and \mathfrak{G} we mean a pair of functors $\text{exp} : \mathfrak{L} \rightarrow \mathfrak{G}$ and $\text{log} : \mathfrak{G} \rightarrow \mathfrak{L}$ such that the compositions $\text{exp} \circ \text{log}$ and $\text{log} \circ \text{exp}$ are naturally equivalent to the identity functors on \mathfrak{G} and \mathfrak{L} , respectively. We will describe such correspondence in the following cases (all relevant definitions are given later in this section). In all cases below we assume that \mathfrak{L} and \mathfrak{G} are full subcategories of $\mathfrak{L}_{\mathbb{Z}_p}$ and $\mathfrak{G}_{\mathbb{Z}_p}$, respectively.

1. $(\mathfrak{L}, \mathfrak{G}) = (\mathfrak{L}_{<p}, \mathfrak{G}_{<p})$ where $\mathfrak{L}_{<p}$ (resp. $\mathfrak{G}_{<p}$) is the category of finite Lie rings (resp. finite groups) of p -power order and nilpotency class $< p$.
2. $(\mathfrak{L}, \mathfrak{G}) = (\mathfrak{L}_{ptf}, \mathfrak{G}_{ptf})$ where \mathfrak{L}_{ptf} (resp. \mathfrak{G}_{ptf}) is the category of powerful torsion-free \mathbb{Z}_p -Lie algebras of finite rank (resp. finitely generated powerful torsion-free pro- p groups).⁶
3. $(\mathfrak{L}, \mathfrak{G}) = (\mathfrak{L}_{ppc}, \mathfrak{G}_{ppc})$ where \mathfrak{L}_{ppc} (resp. \mathfrak{G}_{ppc}) is the category of powerful p -central \mathbb{Z}_p -Lie algebras of finite rank (resp. finitely generated powerful p -central pro- p groups) and $p \geq 5$.

⁵This fact is not very hard to prove – see [DDMS, Corollary 1.19]. It is even true that any homomorphism between finitely generated profinite groups is continuous, but this is a very deep theorem of Nikolov and Segal [NS1, NS2]

⁶Finitely generated powerful torsion-free pro- p groups are precisely the uniformly powerful (or *uniform*) pro- p groups [DDMS, Theorem 4.5].

Cases 1 and 2 of exp-log correspondence are due to Lazard. The correspondence $\mathfrak{L}_{<p} \cong \mathfrak{G}_{<p}$ is a special case of [La1, Theorem 4.6]. Equivalence between \mathfrak{L}_{ptf} and \mathfrak{G}_{ptf} is essentially established in Lazard's famous 1965 paper on p -adic analytic groups [La2], although the notion of a powerful group was introduced more than 20 years later by Lubotzky and Mann [LM2]. For a detailed account of the theory of powerful groups the reader is referred to the excellent book on analytic pro- p groups [DDMS]; we shall just state the main definitions and results.

Definition. A pro- p group G (resp. a \mathbb{Z}_p -Lie algebra L) is called *powerful*, if $[G, G] \subseteq G^q$ (resp. $[L, L] \subseteq qL$) where $q = p$ if $p > 2$ and $q = 4$ if $p = 2$.

The following well-known criterion of analyticity of pro- p groups was first stated in [LM2] and is easily deduced from results in [La2].

Theorem 3.1. *A finitely generated pro- p group is p -adic analytic if and only if it contains a finite index powerful subgroup. Moreover, every finitely generated powerful pro- p group contains a finite index subgroup which is powerful and torsion-free.*

The book [DDMS] contains a full proof of Theorem 3.1 “from scratch” as well as an explicit proof of equivalence $\mathfrak{G}_{ptf} \cong \mathfrak{L}_{ptf}$ between the categories of finitely generated powerful torsion-free pro- p groups and \mathbb{Z}_p -Lie algebras of finite rank. Lazard's counterpart of this result [La2, Chapter IV, Theorem 3.2.6] is a correspondence between the categories of “ p -saturable” pro- p groups and Lie algebras. Any finitely generated torsion-free powerful pro- p group is p -saturable; conversely, a p -saturable pro- p group is p -adic analytic and torsion-free, but not necessarily powerful. Thus, Lazard's exp-log correspondence is more general than the one between \mathfrak{G}_{ptf} and \mathfrak{L}_{ptf} ; however, powerful torsion-free pro- p groups are usually easier to work with than p -saturable ones (for more on this see [K]).

The last case of exp-log correspondence used in this paper is Weigel's generalization of the correspondence $\mathfrak{L}_{ptf} \cong \mathfrak{G}_{ptf}$ to certain classes of pro- p groups and \mathbb{Z}_p -Lie algebras that are powerful but not necessarily torsion-free.

Definition. Assume that $p > 2$. A pro- p group G (resp. a \mathbb{Z}_p -Lie algebra L) is called *p -central*, if any $g \in G$ such that $g^p = 1$ (resp. $u \in L$ such that $pu = 0$) lies in the center of G (resp. L).

In [Weig], ⁷ Weigel constructed exp-log correspondence $\mathfrak{L}_{ppc} \cong \mathfrak{G}_{ppc}$ between the categories of powerful p -central pro- p groups and \mathbb{Z}_p -Lie algebras for $p \geq 5$. Note that a torsion-free pro- p group is always p -central, and more generally, a central extension of a torsion-free pro- p group is always p -central. Thus, Weigel's correspondence is well suited for computing the second cohomology of powerful torsion-free pro- p groups.

Construction of the exp functor. We shall now explain how to construct the pro- p group $\exp(L)$ corresponding to a \mathbb{Z}_p -Lie algebra L where $L \in \text{Ob}(\mathfrak{L}_{<p})$ or

⁷In fact, Weigel introduced a general technique for establishing exp-log correspondence between categories of p -adic analytic groups and \mathbb{Z}_p -Lie algebras satisfying certain conditions. This technique is applicable to all cases of exp-log correspondence discussed in this paper.

$L \in \text{Ob}(\mathfrak{L}_{ppc})$. While there exist distinct ways to define $\exp(L)$ formally, they are all based on the Baker-Cambell-Hausdorff (BCH) formula.

Let $\mathcal{A} = \mathbb{Q}\langle\langle x_1, x_2 \rangle\rangle$ be the algebra of power series over \mathbb{Q} in two non-commuting variables x_1 and x_2 . The power series $\Phi = \text{Log}(\text{Exp}(x_1) \cdot \text{Exp}(x_2))$ is called the *Baker-Campbell-Hausdorff series* (here $\text{Exp}(x) = 1 + x + \frac{x^2}{2} + \dots$ and $\text{Log}(1 + x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \dots$).

Theorem 3.2. *The Baker-Campbell-Hausdorff (BCH) series Φ lies in the closed \mathbb{Q} -Lie subalgebra of \mathcal{A} generated by x_1 and x_2 . In other words, $\Phi = \sum_{c \in S} \lambda_c c$, where S is the set of all left-normed commutators in x_1, x_2 and each $\lambda_c \in \mathbb{Q}$. Moreover, if $wt(c)$ denotes the weight of a commutator c , then*

$$p^{\lfloor \frac{wt(c)-1}{p-1} \rfloor} \lambda_c \in \mathbb{Z}_p \text{ for any } c \in S \quad \text{where } \lfloor t \rfloor \text{ is the largest integer } \leq t.$$

Remark: There is an explicit expression for Φ (as a linear combination of commutators), called the Baker-Campbell-Hausdorff formula. The last assertion of Theorem 3.2 due to Lazard [La2] is a consequence of that formula.

Now let $\mathfrak{L} = \mathfrak{L}_{<p}$ or \mathfrak{L}_{ppc} , and let L be an object of \mathfrak{L} . We define the pro- p group $\exp(L)$ as follows. As a set $\exp(L) = L$, and the group operation \cdot is defined by

$$u_1 \cdot u_2 = \Phi(u_1, u_2).$$

where $\Phi(u_1, u_2) \in L$ is defined below. Informally, one should think of $\Phi(u_1, u_2)$ as the result of “evaluating” the BCH series at $x_1 = u_1$ and $x_2 = u_2$. The formal definition of $\Phi(u_1, u_2)$ will be different in the cases $\mathfrak{L} = \mathfrak{L}_{<p}$ and $\mathfrak{L} = \mathfrak{L}_{ppc}$.

Case 1: $\mathfrak{L} = \mathfrak{L}_{<p}$. Given a left-normed commutator c in x_1, x_2 , we define $c(u_1, u_2)$ by substituting u_1 for x_1 and u_2 for x_2 in c . Thus, if $c = [x_{i_1}, x_{i_2}, \dots, x_{i_k}]$, then $c(u_1, u_2) = [u_{i_1}, u_{i_2}, \dots, u_{i_k}]$. Since the nilpotency class of L is less than p , we have $c(u_1, u_2) = 0$ whenever $wt(c) \geq p$. Thus, we set

$$\Phi(u_1, u_2) = \sum_{c \in S, wt(c) < p} \lambda_c c(u_1, u_2)$$

(using the notations of Theorem 3.2). In other words, $\Phi(u_1, u_2)$ is obtained by plugging in u_1 and u_2 into the BCH series truncated after degree $p - 1$. Since $\lambda_c \in \mathbb{Z}_p$ whenever $wt(c) < p$, the obtained expression is well-defined.

Case 2: $\mathfrak{L} = \mathfrak{L}_{ppc}$ and $p \geq 5$. Once again, let $c = [x_{i_1}, x_{i_2}, \dots, x_{i_k}]$ be a left-normed commutator of weight $k \geq 2$. In this case for any $u_1, u_2 \in L$ we can define the value $\frac{1}{p^{k-2}} c(u_1, u_2)$ as follows. If $k = 2$, this is done in the obvious way.

Assume now that $k = 3$, so that $c = [x_{i_1}, x_{i_2}, x_{i_3}]$. Since L is powerful, there exists $v_1 \in L$ such that $[u_{i_1}, u_{i_2}] = pv_1$, and we define $\frac{1}{p} c(u_1, u_2) = [v_1, u_{i_3}]$. The last expression is independent of the choice of v_1 because L is p -central. Indeed, if $[u_{i_1}, u_{i_2}] = pv'_1$ for some $v'_1 \neq v_1$, then $p(v'_1 - v_1) = 0$, whence $v'_1 - v_1$ lies in the center of L .

For $k \geq 4$ we proceed inductively – write $c = [d, x_{i_k}]$ where d is a left-normed commutator of weight $k - 1$, and define $\frac{1}{p^{k-2}} c(u_1, u_2) = [\frac{1}{p} \cdot \frac{1}{p^{k-3}} d(u_1, u_2), u_{i_k}]$ where

$\frac{1}{p}w$ is any element of L such that $p \cdot \frac{1}{p}w = w$ (again the choice of such an element does not affect the value $\frac{1}{p^{k-2}}c(u_1, u_2)$ since L is p -central).

Now recall from Theorem 3.2 that $p^{\lfloor \frac{k-1}{p-1} \rfloor} \lambda_c \in \mathbb{Z}_p$ where λ_c is the coefficient of c in the (chosen expansion of) BCH series Φ . Since $\lfloor \frac{k-1}{p-1} \rfloor \leq k-2$ for $p \geq 3$, we can define $\lambda_c c(u_1, u_2) \in L$ by setting $\lambda_c c(u_1, u_2) = (p^{k-2} \lambda_c) \cdot \frac{1}{p^{k-2}} c(u_1, u_2)$. Moreover, the series $\sum_c \lambda_c c(u_1, u_2)$ converges in L , and we let $\Phi(u_1, u_2)$ be its sum.

It is now clear how to define the functor $\exp : \mathfrak{L} \rightarrow \mathfrak{G}$ where $(\mathfrak{L}, \mathfrak{G}) = (\mathfrak{L}_{<p}, \mathfrak{G}_{<p})$ or $(\mathfrak{L}_{ppc}, \mathfrak{G}_{ppc})$:

- if L is an object of \mathfrak{L} , the corresponding object of \mathfrak{G} is the group $\exp(L)$ as defined above
- if L_1, L_2 are objects of \mathfrak{L} and $f : L_1 \rightarrow L_2$ is a Lie algebra homomorphism, the corresponding group homomorphism $\exp(f) : \exp(L_1) \rightarrow \exp(L_2)$ coincides with f as a set map.

Of course, there is a number of things to check here for both $\mathfrak{L} = \mathfrak{L}_{<p}$ and $\mathfrak{L} = \mathfrak{L}_{ppc}$, but the arguments in the latter case are much more involved. Proving that $G = \exp(L)$ is a group with respect to the operation defined by Φ turns out to be technically most difficult, and requires the assumption $p \geq 5$ (so far we only used that $p \geq 3$). Once this is done, it is fairly easy to check that G is an object of \mathfrak{G} and for any Lie algebra homomorphism f between two objects of \mathfrak{L} , the corresponding map $\exp(f)$ is a group homomorphism.

The functor $\log : \mathfrak{G} \rightarrow \mathfrak{L}$ is defined somewhat similarly, but both the construction and its justification are more demanding. Let \mathcal{L} be the closed \mathbb{Q} -Lie subalgebra of $\mathbb{Q}\langle\langle x_1, x_2 \rangle\rangle$ generated by x_1 and x_2 . To define \log , one first expresses the addition and the Lie bracket on \mathcal{L} in terms of the multiplication given by Φ . The obtained expressions, denoted by Ψ_A and Ψ_B , are no longer power series; instead they are infinite products of “root-commutators” which are defined as left-normed commutators, except that one is allowed to extract p^{th} -root a limited number of times (e.g. the root-commutator $[[[x_1, x_2]^{1/p}, x_3]^{1/p}, x_4]$ would correspond to the element $\frac{1}{p^2}[x_1, x_2, x_3, x_4]$ in the Lie algebra case). Then, given a pro- p group $G \in \text{Ob}(\mathfrak{G})$, one defines the addition and the Lie bracket on G by evaluating the infinite products Ψ_A and Ψ_B on G (similarly to how we evaluated Φ on Lie algebras in $\text{Ob}(\mathfrak{L})$).

We now formally state the main result on exp-log correspondence (Theorem 3.3 below) established by Lazard [La1] for the pair $(\mathfrak{L}_{<p}, \mathfrak{G}_{<p})$ and by Weigel [Weig] for the pair $(\mathfrak{L}_{ppc}, \mathfrak{G}_{ppc})$. Since Weigel’s manuscript [Weig] is not easily available, a proof of Theorem 3.3 in the case of Weigel’s correspondence will be given in the appendix.

Theorem 3.3. *Let $(\mathfrak{G}, \mathfrak{L}) = (\mathfrak{G}_{ppc}, \mathfrak{L}_{ppc})$ with $p \geq 5$ or $(\mathfrak{G}, \mathfrak{L}) = (\mathfrak{G}_{<p}, \mathfrak{L}_{<p})$. There exist mutually inverse functors $\exp : \mathfrak{L} \rightarrow \mathfrak{G}$ and $\log : \mathfrak{G} \rightarrow \mathfrak{L}$ (that is, the compositions $\exp \circ \log$ and $\log \circ \exp$ are both the identity functors) satisfying the following properties:*

- (1) *For any object L of \mathfrak{L} we have $\exp(L) = L$ as a set and likewise for any object G of \mathfrak{G} we have $\log(G) = G$ as a set.*

- (2) If $\varphi : L \rightarrow M$ is any morphism in \mathfrak{L} and $\exp(\varphi) : \exp(L) \rightarrow \exp(M)$ is the corresponding morphism in \mathfrak{L} , then $\exp(\varphi) = \varphi$ as set maps. The analogous property holds for the \log functor.
- (3) For any object L of \mathfrak{L} the group operation on $G = \exp(L)$ is defined as described above (in terms of the BCH series Φ).

Below we collect several basic properties of the functors \log and \exp which will be used in this paper and easily follow from Theorem 3.3.

Proposition 3.4. *Let $(\mathfrak{G}, \mathfrak{L}) = (\mathfrak{G}_{ppc}, \mathfrak{L}_{ppc})$ with $p \geq 5$ or $(\mathfrak{G}, \mathfrak{L}) = (\mathfrak{G}_{<p}, \mathfrak{L}_{<p})$, and let $\exp : \mathfrak{L} \rightarrow \mathfrak{G}$ and $\log : \mathfrak{G} \rightarrow \mathfrak{L}$ be as in Theorem 3.3. Then \log satisfies properties (a)-(d) below and \exp satisfies their natural analogues:*

- (a) If $K, G, H \in \text{Ob}(\mathfrak{G})$ and $1 \rightarrow K \xrightarrow{\iota} G \xrightarrow{\varphi} H \rightarrow 1$ is an exact sequence, then the sequence $0 \rightarrow \log(K) \xrightarrow{\log(\iota)} \log(G) \xrightarrow{\log(\varphi)} \log(H) \rightarrow 0$ is also exact.
- (b) If $G \in \text{Ob}(\mathfrak{G})$ is abelian, then $\log(G) \in \mathfrak{L}$ is also abelian.
- (c) For any $G, H \in \text{Ob}(\mathfrak{G})$ we have $\log(G \times H) = \log(G) \times \log(H)$.
- (d) If $H, G \in \text{Ob}(\mathfrak{G})$ and H is a central subgroup of G , then $\log(H)$ is a central subalgebra of $\log(G)$.

Proof. The analogues of (a)-(d) for the \exp functor follow immediately from Theorem 3.3. For (b) and (d) we use the obvious fact that $\Phi(u, v) = u + v$ whenever u and v commute in some $L \in \text{Ob}(\mathfrak{L})$.

We could have argued similarly for the \log functor had we described the latter more explicitly, but it is actually easy to deduce (a)-(d) for \log directly from (a)-(c) for \exp and Theorem 3.3. Property (a) for \log is automatic by Theorem 3.3. Below we will give an argument for (b) and (d), with (c) being similar to (d).

(b) Suppose that $G \in \text{Ob}(\mathfrak{G})$ is abelian. Then G has a unique structure of an abelian \mathbb{Z}_p -Lie algebra where the addition is given by the group operation in G . If L is the obtained \mathbb{Z}_p -Lie algebra, it is clear that $\exp(L) = G$, and hence $\log(G) = \log(\exp(L)) = L$ is abelian by (b) for \exp .

(d) Take any $z \in H$ and $g \in G$. By assumption, z and g commute in G , and we need to show that they also commute in $\log(G)$. The (closed) subgroup of G generated by z and g is abelian and hence also lies in \mathfrak{G} . Call this subgroup K , and let $\iota : K \rightarrow G$ be the inclusion map. By Theorem 3.3, ι considered as a map from $\log(K)$ to $\log(G)$ is a Lie algebra homomorphism, and by (b) $\log(K)$ is abelian. Since $\log(K)$ contains both z and g , it follows that z and g commute in $\log(K)$ (and hence also in $\log(G)$), as desired. \square

3.2. Central extensions and \exp - \log correspondence. For the rest of the paper \mathfrak{G} (resp. \mathfrak{L}) will always denote either \mathfrak{G}_{ppc} (resp. \mathfrak{L}_{ppc}) with $p \geq 5$ or $\mathfrak{G}_{<p}$ (resp. $\mathfrak{L}_{<p}$). Whenever we specify a choice for \mathfrak{G} in a particular result, it will be assumed that \mathfrak{L} denotes the corresponding Lie algebra category.

Given $H \in \text{Ob}(\mathfrak{G})$ and $A \in \text{Ob}(\mathfrak{G})$, with A abelian, we define $\text{Ext}_{\mathfrak{G}}(H, A)$ to be the subset of $\text{Ext}(H, A)$ consisting of extensions $A \hookrightarrow \widehat{H} \rightarrow H$ such that $\widehat{H} \in \text{Ob}(\mathfrak{G})$

as well. Likewise, given $\mathfrak{h}, \mathfrak{a} \in \text{Ob}(\mathfrak{L})$, with \mathfrak{a} abelian, we define $\text{Ext}_{\mathfrak{L}}(\mathfrak{h}, \mathfrak{a})$ to be the subset of $\text{Ext}(\mathfrak{h}, \mathfrak{a})$ consisting of extensions $\mathfrak{a} \hookrightarrow \widehat{\mathfrak{h}} \twoheadrightarrow \mathfrak{h}$ such that $\widehat{\mathfrak{h}} \in \text{Ob}(\mathfrak{L})$ as well.

Proposition 3.5. *Let \mathfrak{L} and \mathfrak{G} be as above. Let $H, A \in \text{Ob}(\mathfrak{G})$ where A is abelian, and let $\mathfrak{h} = \log(H)$, $\mathfrak{a} = \log(A)$.*

- (a) *There exists a natural bijection $\text{Log} : \text{Ext}_{\mathfrak{G}}(H, A) \rightarrow \text{Ext}_{\mathfrak{L}}(\mathfrak{h}, \mathfrak{a})$.*
- (b) *Suppose that $\mathfrak{G} = \mathfrak{G}_{<p}$, or $\mathfrak{G} = \mathfrak{G}_{ppc}$ and H is torsion-free. Then*
 - (i) *$\text{Ext}_{\mathfrak{G}}(H, A)$ is a subgroup of $\text{Ext}(H, A)$*
 - (ii) *$\text{Ext}_{\mathfrak{L}}(\mathfrak{h}, \mathfrak{a})$ is a subgroup of $\text{Ext}(\mathfrak{h}, \mathfrak{a})$*
 - (iii) *The map $\text{Log} : \text{Ext}_{\mathfrak{G}}(H, A) \rightarrow \text{Ext}_{\mathfrak{L}}(\mathfrak{h}, \mathfrak{a})$ is an isomorphism of abelian groups.*

Proof. (a) is an immediate consequence of Proposition 3.4. Since the sum of extensions is defined in the same way for groups and Lie algebras, (b)(iii) also becomes automatic once (b)(i) and (b)(ii) are established.

The proofs of (b)(i) and (b)(ii) are similar; in fact, the proof of (b)(ii) is slightly easier, so we will only prove (b)(i).

Let $\mathcal{E}_1 = (A \xrightarrow{\iota_1} \widehat{H}_1 \xrightarrow{\varphi_1} H)$ and $\mathcal{E}_2 = (A \xrightarrow{\iota_2} \widehat{H}_2 \xrightarrow{\varphi_2} H)$ be two elements of $\text{Ext}_{\mathfrak{G}}(H, A)$. Recall that $\mathcal{E}_1 + \mathcal{E}_2 = (A \xrightarrow{\iota} \widehat{H}/\widehat{N} \xrightarrow{\varphi} H)$ where $\widehat{H} = \{(x_1, x_2) \in \widehat{H}_1 \times \widehat{H}_2 : \varphi_1(x_1) = \varphi_2(x_2)\}$, $\widehat{N} = \{(\iota_1(a), \iota_2(a^{-1})) : a \in A\}$, $\iota(a) = (\iota_1(a), 1)\widehat{N} = (1, \iota_2(a))\widehat{N}$, and $\varphi((x_1, x_2)\widehat{N}) = \varphi_1(x_1) = \varphi_2(x_2)$.

To prove (i) we need to show that $\widehat{H}/\widehat{N} \in \text{Ob}(\mathfrak{G})$. If $\mathfrak{G} = \mathfrak{G}_{<p}$, this is obvious since $\widehat{H}_1, \widehat{H}_2 \in \text{Ob}(\mathfrak{G}_{<p})$ and $\mathfrak{G}_{<p}$ is closed under subgroups, quotients and direct products.

Now assume that $\mathfrak{G} = \mathfrak{G}_{ppc}$ and H is torsion-free. We need to show that \widehat{H}/\widehat{N} is powerful and p -central. The p -centrality condition clearly holds since \widehat{H}/\widehat{N} is a central extension of H . To prove that \widehat{H}/\widehat{N} is powerful it is sufficient to prove that \widehat{H} is powerful. We shall use the following well-known criterion [DDMS, Lemma 3.4].

Lemma 3.6. *A finitely generated pro- p group G is powerful if and only if for any $x, y \in G$ there exists $z \in G$ such that $[x, y] = z^p$.*

Now take any $x, y \in \widehat{H}$. Thus $x = (x_1, x_2)$ and $y = (y_1, y_2)$, where $x_i, y_i \in \widehat{H}_i$ for $i = 1, 2$, $\varphi_1(x_1) = \varphi_2(x_2)$ and $\varphi_1(y_1) = \varphi_2(y_2)$. Since \widehat{H}_1 and \widehat{H}_2 are powerful, there exist $z_i \in \widehat{H}_i$, $i = 1, 2$ such that $[x_i, y_i] = z_i^p$. We have

$$(3.1) \quad [x, y] = [(x_1, x_2), (y_1, y_2)] = ([x_1, y_1], [x_2, y_2]) = (z_1^p, z_2^p) = (z_1, z_2)^p$$

Since $(z_1^p, z_2^p) = [x, y] \in \widehat{H}$, we must have $\varphi_1(z_1^p) = \varphi_2(z_2^p) \in H$. Since H is powerful torsion-free, the equality $\varphi_1(z_1)^p = \varphi_2(z_2)^p$ implies that $\varphi_1(z_1) = \varphi_2(z_2)$ by [DDMS, Lemma 4.10], whence $(z_1, z_2) \in \widehat{H}$. Thus \widehat{H} is powerful by (3.1) and Lemma 3.6. The proof of (i) is complete. \square

The next result relates G -equivariant central extensions in the categories \mathfrak{G} and \mathfrak{L} .

Proposition 3.7. *Let \mathfrak{L} and \mathfrak{G} be as above. Let $H, A \in \text{Ob}(\mathfrak{G})$ where A is abelian, and let $\mathfrak{h} = \log(H)$, $\mathfrak{a} = \log(A)$. Let G be a group which acts by (continuous) automorphisms on both H and A , and define $\text{Ext}_{\mathfrak{G}}(H, A)^G = \text{Ext}_{\mathfrak{G}}(H, A) \cap \text{Ext}(H, A)^G$. The following hold:*

- (a) G acts on \mathfrak{h} by \mathbb{Z}_p -Lie algebra automorphisms (where the action is the same as the action on H). Moreover, the map Log defined in Proposition 3.5(a) maps $\text{Ext}_{\mathfrak{G}}(H, A)^G$ onto $\text{Ext}_{\mathfrak{L}}(\mathfrak{h}, \mathfrak{a})^G$ (where by definition $\text{Ext}_{\mathfrak{L}}(\mathfrak{h}, \mathfrak{a})^G = \text{Ext}_{\mathfrak{L}}(\mathfrak{h}, \mathfrak{a}) \cap \text{Ext}(\mathfrak{h}, \mathfrak{a})^G$).
- (b) Assume $\mathfrak{G} = \mathfrak{G}_{<p}$ or $\mathfrak{G} = \mathfrak{G}_{ppc}$ and H is torsion-free. Then $\text{Ext}_{\mathfrak{G}}(H, A)^G$ and $\text{Ext}_{\mathfrak{L}}(\mathfrak{h}, \mathfrak{a})^G$ are subgroups of $\text{Ext}(H, A)$ and $\text{Ext}(\mathfrak{h}, \mathfrak{a})$, respectively, and $\text{Ext}_{\mathfrak{G}}(H, A)^G \cong \text{Ext}_{\mathfrak{L}}(\mathfrak{h}, \mathfrak{a})^G$.

Proof. (a) is an immediate consequence of Theorem 3.3 and Proposition 3.4(a)(d).

(b) $\text{Ext}_{\mathfrak{G}}(H, A)^G = \text{Ext}(H, A)^G \cap \text{Ext}_{\mathfrak{G}}(H, A)$ and $\text{Ext}_{\mathfrak{L}}(\mathfrak{h}, \mathfrak{a})^G = \text{Ext}(\mathfrak{h}, \mathfrak{a})^G \cap \text{Ext}_{\mathfrak{L}}(\mathfrak{h}, \mathfrak{a})$ are subgroups of $\text{Ext}(H, A)$ and $\text{Ext}(\mathfrak{h}, \mathfrak{a})$, respectively, by Lemma 2.2 and Proposition 3.5(b)(i)(ii). Proposition 3.5(b)(iii) and Proposition 3.7(a) imply that these subgroups are isomorphic to each other. \square

4. DIVISION ALGEBRAS OVER LOCAL FIELDS AND THEIR NORM ONE GROUPS

In this paper by a local field we will always mean a nonarchimedean local field. While the results of the paper only deal with division algebras over local fields of characteristic zero, that is, finite extensions of \mathbb{Q}_p for some p (we will call them *p-adic fields*), in this section we do not impose the characteristic restriction, as the basic structure of division algebras over local fields is very similar in zero and positive characteristics. We will only need very basic results about local fields which can be found, e.g., in Serre's book [Se]. Our basic reference for the structure of division algebras over local fields and their norm one groups is Riehm's paper [Ri].

Notation. Throughout the paper, if D is a finite-dimensional division algebra over a local field (in particular, D itself could be a local field), we will denote the ring of integers of D by O_D and the (unique) maximal ideal of O_D by \mathfrak{m}_D . A *uniformizer* of D is any generator of \mathfrak{m}_D . If K is a local field, its residue field O_K/\mathfrak{m}_K will be denoted by \overline{K} .

4.1. Division algebras over local fields. For the rest of this subsection we fix a prime p and a local field F of residue characteristic p . Let D be a finite-dimensional central division algebra over F , and let d be the degree of D . It is well known that there exists a maximal subfield W of D such that the extension W/F is unramified (note that $[W : F] = d$). Moreover there exist a uniformizer π of D and a generator σ of the Galois group $\text{Gal}(W/F)$ such that

$$(4.1) \quad \pi w \pi^{-1} = \sigma(w) \text{ for all } w \in W.$$

Then $\tau = \pi^d$ is a uniformizer of F , so $\mathfrak{m}_D = \pi O_D$, $\mathfrak{m}_D \cap W = \mathfrak{m}_W = \tau O_W$ and $\mathfrak{m}_D \cap F = \mathfrak{m}_F = \tau O_F$. Moreover we have the following direct sum decompositions:

$$(4.2) \quad D = W \oplus W\pi \oplus W\pi^2 \oplus \cdots \oplus W\pi^{d-1} \text{ as a left vector space over } W$$

$$(4.3) \quad O_D = O_W \oplus O_W\pi \oplus O_W\pi^2 \oplus \cdots \oplus O_W\pi^{d-1} \text{ as a left module over } O_W$$

As an immediate consequence of the second decomposition, the quotient $O_D/\pi O_D$ is naturally isomorphic to $O_W/\pi^d O_W = O_W/\tau O_W = \overline{W}$.

For each $n \in \mathbb{Z}$ the map $a \mapsto a\pi^n$ induces an isomorphism of abelian groups $\overline{W} \rightarrow \pi^n O_D/\pi^{n+1} O_D$. We will frequently identify $\pi^n O_D/\pi^{n+1} O_D$ with \overline{W} using this isomorphism.

The following formula for additive commutators in O_D is an immediate consequence of (4.1):

$$(4.4) \quad [a\pi^i, b\pi^j] = (a\sigma^i(b) - b\sigma^j(a))\pi^{i+j} \text{ for } a, b \in W \text{ and } i, j \in \mathbb{Z}.$$

The norm one group $SL_1(D)$. Let N_{red} (resp. T_{red}) denote the reduced norm (resp. reduced trace) map from D to F . One can define $N_{\text{red}}(a)$ (resp. $T_{\text{red}}(a)$) as the determinant (resp. trace) of the endomorphism of the left W -vector space D given by $x \mapsto xa$. The restriction of N_{red} (resp. T_{red}) to W coincides with the norm (resp. trace) map of the extension W/F .

It is straightforward to check that for $a \in W$ and $i \in \mathbb{Z}$ we have

$$(4.5) \quad T_{\text{red}}(a\pi^i) = 0 \text{ if } d \nmid i \quad \text{and} \quad T_{\text{red}}(a\pi^i) = \mathbf{tr}_{W/F}(a)\tau^{\frac{i}{d}} \text{ if } d \mid i.$$

Lemma 4.1. *Let $n \in \mathbb{Z}_{\geq 0}$. Then $T_{\text{red}}(\pi^n O_D) = \tau^{\lceil \frac{n}{d} \rceil} O_F$ and $N_{\text{red}}(1 + \pi^n O_D) = 1 + \tau^{\lceil \frac{n}{d} \rceil} O_F$ where $\lceil x \rceil$ is the smallest integer $\geq x$.*

Proof. The first assertion follows immediately from (4.5), (4.3) and the fact that $\mathbf{tr}_{W/F}(O_W) = O_F$. The second assertion is Lemma 5 in [Ri]. \square

Let $G = SL_1(D)$ denote the group of elements of reduced norm one in D . For $n \geq 1$ let

$$G_n = SL_1^n(D) = \{g \in G : g \equiv 1 \pmod{\pi^n O_D}\}.$$

It is easy to check that each G_n is a finite index pro- p subgroup of G .

For each $n \in \mathbb{N}$ define the map $\rho_n : 1 + \pi^n O_D \rightarrow \overline{W}$ by

$$\rho_n(1 + \pi^n a) = a \pmod{\pi O_D}$$

(where we identify $O_D/\pi O_D$ with \overline{W} as before). Note that ρ_n is a group homomorphism and $\text{Ker } \rho_n = 1 + \pi^{n+1} O_D$, so $\rho_n(G_n) \cong G_n/G_{n+1}$. The following result appears as Lemma 6 in [Ri].

Lemma 4.2. *Let $n \in \mathbb{N}$. If $d \nmid n$, then $\rho_n(G_n) = \overline{W}$. If $d \mid n$, then $\rho_n(G_n) = \mathfrak{sl}(\overline{W})$ where $\mathfrak{sl}(\overline{W}) = \{x \in \overline{W} : \mathbf{tr}_{\overline{W}/F}(x) = 0\}$.*

Proposition 4.3. *The following hold:*

- (a) G decomposes as a semi-direct product $G = G_1 \rtimes \Delta$ where Δ is the group consisting of roots of unity in W which have order prime to p and norm 1 over F .
- (b) $[G_i, G_j] \subseteq G_{i+j}$ for any $i, j \geq 1$. In particular, $\gamma_k G_i \subseteq \gamma_{ki} G_1$ for all $i, k \geq 1$. Assume now that $p \neq 2$ or $d \neq 2$. Then

$$[G_i, G_j] = \begin{cases} G_{i+j} & \text{if } d \nmid (i+j) \text{ or } d \mid (i+j) \text{ and } d \text{ is coprime to } i. \\ G_{i+j+1} & \text{if } d \mid i \text{ and } d \mid j \end{cases}$$

In particular, $G_i = \gamma_i G_1$ for all $i \geq 1$.

- (c) Assume that $\text{char } F = 0$, let e be the ramification index of F , and let $i > \frac{de}{p-1}$. Then $G_i^p = G_{i+de}$. Moreover, if $g \in G_i \setminus G_{i+1}$, then $g^p \in G_{i+de} \setminus G_{i+de+1}$.

Remark: Note that the above formula for $[G_i, G_j]$ does not cover all possible pairs (i, j) . A complete description of $[G_i, G_j]$ in the remaining cases is given in the proof below, but will not be needed for our purposes.

Proof. (a) Let $\rho : O_D \rightarrow \overline{W}$ be the natural projection (where we identify $O_D/\pi O_D$ with \overline{W} as before). It is straightforward to check that for any $a \in O_D$ we have $\rho(N_{\text{red}}(a)) = N_{\overline{W}/\overline{F}}(\rho(a))$ where $N_{\overline{W}/\overline{F}}$ is the norm of the extension $\overline{W}/\overline{F}$.

Thus, if $\overline{\Delta} = \{x \in \overline{W}^* : N_{\overline{W}/\overline{F}}(x) = 1\}$, then $\rho(G) \subseteq \overline{\Delta}$. Note that Δ has trivial intersection with $\text{Ker } \rho \cap G = G_1$ (e.g. since G_1 is a pro- p group and any element of Δ has finite order prime to p). Thus, to prove (a) it remains to show that $\rho(\Delta) = \overline{\Delta}$.

Take any $x \in \overline{\Delta}$. By Hensel's lemma there exists a root of unity $a \in W$ such that $\rho(a) = x$. Moreover, the (multiplicative) order of x is equal to the order of a and thus is coprime to p . Then $N_{\text{red}}(a)$ is also a root of unity of order coprime to p ; on the other hand, $a \in \text{Ker } \rho \cap O_D^*$ which is a pro- p group. Thus, we must have $N_{\text{red}}(a) = 1$, so $a \in \Delta$.

(b) The inclusion $[G_i, G_j] \subseteq G_{i+j}$ can be verified by an easy direct computation. Assume now that $(p, d) \neq (2, 2)$. The second assertion of Proposition 4.3(b) is a special case of [Ri, Theorem 21]; however, due to the technical nature of the statement of this theorem, we will briefly explain how to obtain the result. First, [Ri, Theorem 21] asserts that $[G_i, G_j] \supseteq G_{i+j+1}$, so the group $[G_i, G_j]$ is determined by its image in G_{i+j}/G_{i+j+1} . The second assertion of Proposition 4.3(b) can now be reformulated in terms of the map ρ_{i+j} : we need to show that $\rho_{i+j}([G_i, G_j]) = \rho_{i+j}(G_{i+j})$ if $d \nmid (i+j)$ or $d \mid (i+j)$ and d is coprime to i and $\rho_{i+j}([G_i, G_j]) = \{0\}$ if $d \mid i$ and $d \mid j$.

The equation (4.4) easily implies that $\rho_{i+j}([G_i, G_j])$ is equal to the set $S = \{\alpha \sigma^i(\beta) - \beta \sigma^j(\alpha) : \alpha \in \rho_i(G_i), \beta \in \rho_j(G_j)\}$. Here we use the fact that the natural map $\text{Gal}(W/F) \rightarrow \text{Gal}(\overline{W}/\overline{F})$ is an isomorphism since W/F is unramified, and the image of $\sigma \in \text{Gal}(W/F)$ under this isomorphism is also denoted by σ .

Recall from Lemma 4.2 that $\rho_k(G_k) = \overline{W}$ if $d \nmid k$ and $\rho_k(G_k) = \mathfrak{sl}(\overline{W})$ if $d \mid k$. It is clear that if $d \mid i$ and $d \mid j$, then $S = \{0\}$ (since $\sigma^d = id$). If $d \mid (i+j)$ but $d \nmid i$, we have $S = \{\alpha \sigma^i(\beta) - \beta \sigma^{-i}(\alpha) : \alpha, \beta \in \overline{W}\} = \{\sigma^i(\gamma) - \gamma : \gamma \in \overline{W}\}$. If in addition i is coprime to d , then σ^i is a generator of $\text{Gal}(\overline{W}/\overline{F})$, so by Hilbert's Theorem 90

$S = \mathfrak{sl}(\overline{W})$, and thus $S = \rho_{i+j}(G_{i+j})$. Finally, if $d \nmid (i+j)$, $S = \overline{W}$, as proved in [Ri].

(c) We first prove the second assertion. Assume that $i > \frac{de}{p-1}$ and take any $g \in G_i \setminus G_{i+1}$. Thus $g = 1 + \pi^i a + b$ for some $a \in O_D^* = O_D \setminus \pi O_D$ and $b \in \pi^{i+1} O_D$. Then $g^p = 1 + \sum_{j=1}^p \binom{p}{j} (\pi^i a + b)^j = 1 + p\pi^i a + c$ where $c \in \pi^{pi} O_D + p\pi^{i+1} O_D$. Let $v : O_D \rightarrow \mathbb{Z}_{\geq 0}$ be the (additive) valuation on D such that $v(\pi) = 1$, that is, $v(x) = i$ if and only if $x \in \pi^i O_D \setminus \pi^{i+1} O_D$. By definition of ramification index we have $v(p) = e \cdot v(\tau) = e \cdot v(\pi^d) = de$. Thus, $v(p\pi^i a) = i + de$ and $v(c) \geq \min\{pi, i+1+de\}$. Since $i > \frac{de}{p-1}$, we have $pi = i + (p-1)i > i + de$, so $i + de = v(p\pi^i a) < v(c)$ and hence $v(g^p - 1) = v(p\pi^i a + c) = i + de$. Therefore, $g^p \in G_{i+de} \setminus G_{i+de+1}$.

Now we prove the first assertion. We already proved that $G_i^p \subseteq G_{i+de}$. The computation in the previous paragraph also shows that the map $\rho_i(G_i) \rightarrow \rho_{i+de}(G_{i+de}^p)$ induced by the p -power map $x \mapsto x^p$ is given by multiplication by a nonzero element of \overline{W} (namely $\frac{p}{\tau^e} \bmod \pi O_D$). In particular this means that $\rho_i(G_i) = \rho_{i+de}(G_{i+de}^p)$. On the other hand, $\rho_{i+de}(G_{i+de}) = \rho_i(G_i)$ by Lemma 4.2.

Thus, $\rho_{i+de}(G_i^p) = \rho_{i+de}(G_{i+de})$, so $G_{i+de} \subseteq G_i^p G_{i+de+1}$. Since this inclusion holds for all $i > \frac{de}{p-1}$, arguing inductively, we deduce that $G_{i+de} \subseteq G_i^p G_k$ for all $k \in \mathbb{N}$. Since $\{G_k\}$ is a base of neighborhoods of identity in G (and since G_i^p is closed), we deduce that $G_{i+de} \subseteq G_i^p$ as desired. \square

Lie algebras of congruence subgroups and their quotients. If $n \geq de$, the group G_n is powerful and torsion-free by Proposition 4.3(b)(c), so we can consider the Lie algebra $\log(G_n)$ using Weigel's log functor. Also for any $m, n \in \mathbb{N}$ such that $n \leq m \leq pn$, we have $G_n/G_m \in \text{Ob}(\mathfrak{G}_{<p})$ by Proposition 4.3(b), so we can consider $\log(G_n/G_m)$, this time using Lazard's log functor.

As one might expect, the Lie algebras obtained in this way are isomorphic to \mathfrak{g}_n in the first case and $\mathfrak{g}_n/\mathfrak{g}_m$ in the second case where

$$\mathfrak{g}_n = \mathfrak{sl}(\pi^n O_D) = \{x \in \pi^n O_D : \text{T}_{\text{red}}(x) = 0\}.$$

Explicit isomorphisms between these Lie algebras are defined in our next proposition:

Proposition 4.4. *The following hold:*

- (a) *Let $n \geq de$. Let us define the maps $\text{Exp} : \pi^n O_D \rightarrow 1 + \pi^n O_D$ and $\text{Log} : 1 + \pi^n O_D \rightarrow \pi^n O_D$ by*

$$\text{Exp}(x) = \sum_{i=0}^{\infty} \frac{x^i}{i!} \quad \text{and} \quad \text{Log}(1+x) = \sum_{i=1}^{\infty} \frac{(-1)^{i-1} x^i}{i}.$$

Then Exp and Log are mutually inverse bijections and $\text{Exp}(\mathfrak{g}_n) = G_n$. Moreover, if $\log(G_n)$ is the Lie algebra of G_n where \log is Weigel's functor (recall that $\log(G_n) = G_n$ as sets), the map $x \mapsto \text{Exp}(x)$ is a Lie algebra isomorphism between \mathfrak{g}_n and $\log(G_n)$.

- (b) *Assume that $1 \leq n \leq m \leq pn$. Define the truncated exponential and logarithm mappings $\text{Exp}' : \pi^n O_D / \pi^m O_D \rightarrow (1 + \pi^n O_D) / (1 + \pi^m O_D)$ and*

$\text{Log}' : (1 + \pi^n O_D)/(1 + \pi^m O_D) \rightarrow \pi^n O_D/\pi^m O_D$ by

$$\text{Exp}'(x) = \sum_{i=0}^{p-1} \frac{x^i}{i!} \quad \text{and} \quad \text{Log}'(1+x) = \sum_{i=1}^{p-1} \frac{(-1)^{i-1} x^i}{i}.$$

Then Exp' and Log' are mutually inverse bijections and $\text{Exp}(\mathfrak{g}_n/\mathfrak{g}_m) = G_n/G_m$. Moreover, if $\log(G_n/G_m)$ is the Lie algebra of G_n/G_m where \log is Lazard's functor, the map $x \mapsto \text{Exp}'(x)$ is a Lie algebra isomorphism between $\mathfrak{g}_n/\mathfrak{g}_m$ and $\log(G_n/G_m)$.

- (c) Suppose that either $H = G_n$ and $\mathfrak{h} = \mathfrak{g}_n$ with $n \geq de$ or $H = G_n/G_m$ and $\mathfrak{h} = \mathfrak{g}_n/\mathfrak{g}_m$ with $1 \leq n \leq m \leq pn$. In both cases the conjugation action of G on H induces an action of G on $\log(H)$ by Proposition 3.7(a). Then under the isomorphisms $\mathfrak{h} \rightarrow \log(H)$ described in (a) and (b) this action corresponds to the conjugation action of G on \mathfrak{h} given by

$$(4.6) \quad u^g = g^{-1}ug \quad \text{for } u \in \mathfrak{g}_n \text{ and } g \in G$$

(and the corresponding induced action on $\mathfrak{g}_n/\mathfrak{g}_m$).

Remark: Note that we capitalize the first letters of the maps Exp , Log , Exp' and Log' defined in (a) and (b) to avoid confusion with the exp and log functors. Also in the proof below we will use Exp , Log , Exp' and Log' not just for the maps with the domain and codomain specified in Proposition 4.4, but any maps given by the same formulas.

Proof. (a) Since $n \geq de$, it is easy to check that both Exp and Log are well defined, that is, the series converge and all terms take values in the appropriate ideals (in fact, for this it would be enough to assume that $n > \frac{de}{p-1}$). We know that Exp and Log are mutually inverse as power series under substitution, and a routine convergence check shows that they are also mutually inverse as functions. To prove that $\text{Exp}(\mathfrak{g}_n) = G_n$ it suffices to check that $N_{\text{red}}(\text{Exp}(x)) = \text{Exp}(T_{\text{red}}(x))$ and $T_{\text{red}}(\text{Log}(1+x)) = \text{Log}(N_{\text{red}}(1+x))$ for all $x \in \pi^{de} O_D$. By definition of reduced trace and reduced norm this amounts to showing that $\det(\text{Exp}(A)) = \text{Exp}(\text{tr}(A))$ and $\text{tr}(\text{Log}(1+A)) = \text{Log}(\det(1+A))$ for any $d \times d$ matrix A over $\tau^d O_W$. Both equalities are well-known over \mathbb{C} . However, since both sides of either equality are clearly power series in the entries of A , they must coincide as power series, and hence the equalities holds over $\tau^d O_W$ as well.

Finally, the assertion that $x \mapsto \text{Exp}(x)$ is a Lie algebra isomorphism between \mathfrak{g}_n and $\log(G_n)$ is a direct consequence of Theorem 3.2 (recall that the group operation on $\log(G_n)$ is defined using the BCH series Φ).

(b) This time we do not have to worry about convergence, and since the coefficients in the expressions for Exp' and Log' are p -adic integers, Exp' and Log' are well defined functions between $\pi^n O_D/\pi^m O_D$ and $(1 + \pi^n O_D)/(1 + \pi^m O_D)$.

Let us check that Exp' and Log' are mutually inverse. It is clear from definitions that the polynomial $\text{Log}' \circ \text{Exp}'(x)$ coincides with the power series $\text{Log} \circ \text{Exp}(x) = x$ up to (and including) degree $p-1$. Therefore $\text{Log}' \circ \text{Exp}'(x) = x + \sum_{k=p}^{(p-1)^2} c_k x^k$ where

c_k are p -adic integers. Hence for all $x \in \pi^n O_D$ we have $\text{Log}' \circ \text{Exp}'(x) - x \in \pi^{pn} O_D \subseteq \pi^m O_D$ since $m \leq pn$. Thus, $\text{Log}' \circ \text{Exp}'(x) = x$ for all $x \in \mathfrak{g}_n/\mathfrak{g}_m$, as desired. The proof for the composition in reverse order is analogous.

Next we prove that $\text{Exp}'(\mathfrak{g}_n/\mathfrak{g}_m) = G_n/G_m$. The argument in (a) shows that if A is a $d \times d$ matrix with generic entries (a_{ij}) , then $\det(\text{Exp}(A)) = \text{Exp}(\text{tr}(A))$ and $\text{tr}(\text{Log}(1+A)) = \text{Log}(\det(1+A))$ as power series (say, over \mathbb{Q}) in formal commuting variables $\{a_{ij}\}$. If we now replace Exp and Log by Exp' and Log' , both sides of either equality above will not change modulo I^p where I is the ideal of $\mathbb{Q}[[\{a_{ij}\}]]$ generated by $\{a_{ij}\}$. Therefore $\det(\text{Exp}'(A)) \equiv \text{Exp}'(\text{tr}(A)) \pmod{I^p}$ and $\text{tr}(\text{Log}'(1+A)) \equiv \text{Log}'(\det(1+A)) \pmod{I^p}$.

It follows that $\det(\text{Exp}'(A)) = \text{Exp}'(\text{tr}(A))$ and $\text{tr}(\text{Log}'(1+A)) = \text{Log}'(\det(1+A))$ for all $A \in \text{Mat}_d(\tau^r O_D/\tau^s O_D)$ whenever $1 \leq r \leq s \leq pr$. As in the proof of (a) this implies that $\text{Exp}'(\mathfrak{g}_n/\mathfrak{g}_m) = G_n/G_m$ whenever $1 \leq n \leq m \leq pn$.

Let us now prove the last assertion of (b). Recall that the group operation on $\exp(\mathfrak{g}_n/\mathfrak{g}_m)$ is defined by $u \cdot v = \Phi'(u, v)$ where Φ' is the BCH series truncated after degree $p-1$. By Theorem 3.2 we have $\text{Exp}(x) \cdot \text{Exp}(y) = \text{Exp}(\Phi(x, y))$ where both sides are treated as formal power series in non-commuting variables x and y . If we replace Exp by Exp' and Φ by Φ' , both sides will still be congruent modulo the terms of degree $\geq p$. Since Exp' and Φ' are polynomials whose coefficients are p -adic integers, arguing as the first part of the proof of (b), we deduce that $\text{Exp}'(u) \cdot \text{Exp}'(v) = \text{Exp}'(\Phi'(u, v))$ for all $u, v \in \mathfrak{g}_n/\mathfrak{g}_m$. This means precisely that Exp' is a group isomorphism from $\exp(\mathfrak{g}_n/\mathfrak{g}_m)$ to G_n/G_m . Finally, by Theorem 3.3 we deduce that Exp' is also a Lie algebra isomorphism from $\log(\exp(\mathfrak{g}_n/\mathfrak{g}_m)) = \mathfrak{g}_n/\mathfrak{g}_m$ to $\log(G_n/G_m)$, as desired.

(c) follows immediately from definitions and the fact the conjugation actions of G on G_n , G_n/G_m , \mathfrak{g}_n and $\mathfrak{g}_n/\mathfrak{g}_m$ commute with the maps Exp , Log , Exp' and Log' (which is clear from the explicit formulas for these maps). \square

4.2. More on local fields. We finish this section with a collection of elementary facts which will come very handy when we compute the cohomology of \mathfrak{g}_n in § 7.

Given a local field K , we denote by \mathbf{k} the abelian group K/O_K (and use similar notations with K replaced by other capital Latin letters). Clearly, \mathbf{k} is an O_K -module. Since all automorphisms of local fields are continuous, any field automorphism $\varphi : K \rightarrow K$ preserves O_K and thus induces a map $\mathbf{k} \rightarrow \mathbf{k}$ which will also be denoted by φ .

Claim 4.5. *Let L/K be an unramified extension of local fields. Define the trace map $\text{tr}_{\mathbf{l}/\mathbf{k}} : \mathbf{l} \rightarrow \mathbf{k}$ by*

$$\text{tr}_{\mathbf{l}/\mathbf{k}}(x + O_L) = \text{tr}_{L/K}(x) + O_K$$

Let $\mathfrak{sl}(L) = \{x \in L : \text{tr}_{L/K}(x) = 0\}$ and $\mathfrak{sl}(\mathbf{l}) = \{x \in \mathbf{l} : \text{tr}_{\mathbf{l}/\mathbf{k}}(x) = 0\}$.

The following hold:

- (a) $\text{tr}_{\mathbf{l}/\mathbf{k}}(\varphi(\alpha)) = \text{tr}_{\mathbf{l}/\mathbf{k}}(\alpha)$ for all $\alpha \in \mathbf{l}$ and $\varphi \in \text{Gal}(L/K)$.
- (b) Let $\alpha \in \mathbf{l}$. Then α is fixed by all $\varphi \in \text{Gal}(L/K)$ if and only if $\alpha \in \mathbf{k}$.

- (c) Let $\alpha \in \mathbf{l}$ and σ a generator of $\text{Gal}(L/K)$. Then $\alpha \in \mathfrak{sl}(\mathbf{l})$ if and only if $\alpha = \beta - \sigma(\beta)$ for some $\beta \in \mathbf{l}$.
- (d) Let π be a uniformizer of K . Then $\text{tr}_{\mathbf{l}/\mathbf{k}}$ maps $\frac{1}{\pi^n}O_L/O_L$ onto $\frac{1}{\pi^n}O_K/O_K$ for every $n \in \mathbb{N}$.
- (e) If $\alpha \in \mathbf{l}$ is such that $\text{tr}_{\mathbf{l}/\mathbf{k}}(\alpha u) = 0$ for all $u \in O_L$, then $\alpha = 0$.
- (f) Let $\mathbf{n} = \{\alpha \in \mathbf{l} : \text{tr}_{\mathbf{l}/\mathbf{k}}(\alpha uv) = 0 \text{ for all } u, v \in \mathfrak{sl}(O_L)\}$. If $d > 2$, then $\mathbf{n} = \{0\}$, and if $d = 2$, then $\mathbf{n} = \mathfrak{sl}(\mathbf{l})$.
- (g) Let M be another local field with $M \subseteq K$ such that K/M is unramified, and let $\alpha \in \mathbf{l}$ be such that $\text{tr}_{\mathbf{l}/\mathbf{m}}(\alpha u) = 0$ for all $u \in O_L$ with $\text{tr}_{L/K}(u) = 0$. Then $\alpha \in \mathbf{k}$.

Proof. All parts of this claim can be proved using the same principle. For every $n \in \mathbb{N}$ and a local field M we set $R_n(M) = \frac{1}{\pi^n}O_M/O_M$ where π is a uniformizer of M . Then each $R_n(M)$ is an O_M -submodule and each quotient $Q_n(M) = R_n(M)/R_{n-1}(M)$ can be naturally identified with \bar{M} , the residue field of M . Also, under such identification, for any unramified extension of local fields L/K , the induced map $\text{Gal}(L/K) \rightarrow \text{Aut}(Q_n(L))$ is an isomorphism onto $\text{Gal}(\bar{L}/\bar{K})$.

This way we can reduce each of the parts (a)-(g) to the corresponding result about finite fields. The finite field analogues of (a)-(e) are well known. We will give a proof for the finite field counterpart of (g), with the proof of (f) being similar. But first let us give a full argument for (c) as an illustration of the general principle.

The backwards direction in (c) holds by (b). Suppose now that $\alpha \in \mathfrak{sl}(\mathbf{l})$. We know that $\alpha \in R_n(L)$ for some n . Since $\alpha \in \mathfrak{sl}(\mathbf{l})$, the projection of α to $Q_n(L)$, call it $\pi_n(\alpha)$, satisfies $\text{tr}_{\bar{L}/\bar{K}}(\pi_n(\alpha)) = 0$. By Hilbert's Theorem 90 (applied to the cyclic extension \bar{L}/\bar{K}) there exists $\beta \in R_n(L)$ such that $\pi_n(\beta - \sigma(\beta)) = \pi_n(\alpha)$. Let $\alpha' = \alpha - (\beta - \sigma(\beta))$. Then α' lies in $\mathfrak{sl}(\mathbf{l}) \cap R_{n-1}(L)$. Applying the same argument to α' and repeating the process $n - 1$ times, we deduce that $\alpha = \gamma - \sigma(\gamma)$ for some $\gamma \in \mathbf{l}$.

Let us now prove the analogue of (g) for finite fields which asserts the following. Let $F_1 \subseteq F_2 \subseteq F_3$ be a tower of finite fields. Let $\alpha \in F_3$ be such that $\text{tr}_{F_3/F_1}(\alpha\beta) = 0$ for all $\beta \in \mathfrak{sl}_{F_2}(F_3)$ where $\mathfrak{sl}_{F_2}(F_3) = \{\beta \in F_3 : \text{tr}_{F_3/F_2}(\beta) = 0\}$. Then $\alpha \in F_2$.

We first claim that $\text{tr}_{F_3/F_1}(u\beta) = 0$ for all $\beta \in \mathfrak{sl}_{F_2}(F_3)$ and $u \in F_2\alpha + F_2$. Indeed, write $u = f\alpha + f'$ with $f, f' \in F_2$. Then $f'\beta, f\beta \in \mathfrak{sl}_{F_2}(F_3)$ as well, so $\text{tr}_{F_3/F_1}(f'\beta) = \text{tr}_{F_2/F_1}(\text{tr}_{F_3/F_2}(f'\beta)) = 0$, $\text{tr}_{F_3/F_1}(\alpha \cdot f\beta) = 0$ by assumption on α and hence $\text{tr}_{F_3/F_1}(u\beta) = \text{tr}_{F_3/F_1}(f\alpha\beta + f'\beta) = 0$ as well.

Since $\text{tr}_{F_3/F_1} : F_3 \times F_3 \rightarrow F_1$ is a non-degenerate bilinear form and $\dim_{F_1}(\mathfrak{sl}_{F_2}(F_3)) = [F_3 : F_1] - [F_2 : F_1]$, its orthogonal complement must have F_1 -dimension $[F_2 : F_1]$. Hence $\dim_{F_1}(F_2\alpha + F_2) \leq [F_2 : F_1]$ whence $F_2\alpha = F_2$ and so $\alpha \in F_2$. \square

5. GROUP-THEORETIC STRUCTURE OF CENTRAL EXTENSIONS OF $SL_1(D)$

For the next three sections we fix a p -adic field F and a central division algebra D over F . We preserve all notations from § 4. Recall that $G = SL_1(D)$, d is the degree of D and e is the ramification index of F . Throughout this section we shall assume that $(p, d) \neq (2, 2)$.

Let A_∞ denote the group $\mathbb{Q}_p/\mathbb{Z}_p$ (note that $\mathbb{Q}_p/\mathbb{Z}_p$ is isomorphic to the p -primary component of \mathbb{Q}/\mathbb{Z}). Given $n \in \mathbb{N}$, let A_n be the group of elements of order $\leq p^n$ in A_∞ (of course, A_n is simply a cyclic group of order p^n , but it will be convenient to think of it as a subgroup of $\mathbb{Q}_p/\mathbb{Z}_p$). The symbol A will denote A_n for some n when the value of n is not important.

The following key observation appears in [PR2, 2.2]:

Lemma 5.1. *Let $k \in \mathbb{N}$, and let $\iota_k : H^2(G, A_k) \rightarrow H^2(G, A_\infty)$ be the homomorphism induced by the embedding map $A_k \rightarrow A_\infty$. Then*

- (a) *each ι_k is injective*
- (b) *$\iota_k(H^2(G, A_k))$ is the subgroup of elements of order $\leq p^k$ in $H^2(G, A_\infty)$.*
- (c) $H^2(G, A_\infty) = \bigcup_{k=1}^{\infty} \iota_k(H^2(G, A_k))$.

Proof. We only need to use two facts about G :

- (i) G is profinite.
- (ii) $G/[G, G]$ is finite of order prime to p (this holds by Proposition 4.3(a)).

In view of (ii), (a) and (b) follow from the long exact sequence of cohomology groups associated to the short exact sequence $1 \rightarrow A_k \rightarrow A_\infty \xrightarrow{\times p^k} A_\infty \rightarrow 1$.

Since G is profinite and A_∞ is discrete, any continuous map $G \times G \rightarrow A_\infty$ has finite image and thus lies in A_k for some k . This implies (c). \square

Remark: In view of Lemma 5.1 from now on we will identify each $H^2(G, A_k)$ with the subgroup of elements of order $\leq p^k$ in $H^2(G, A_\infty)$.

The main result of [PR2] asserts that $H^2(G, A_\infty)$ is a finite cyclic group of p -power order.

Corollary 5.2. *Each group $H^2(G, A_k)$ is cyclic of p -power order and (with the above identification) $H^2(G, A_\infty) = H^2(G, A_k)$ for all sufficiently large k .*

In this section we study group-theoretic properties of central extensions of G by A_k for $k \in \mathbb{N}$. Throughout this section we write $G_n = SL_1^n(D)$ for $n \geq 1$ and set $S = G_1$. The use of the letter S is “justified” by the fact that S is the Sylow pro- p subgroup of G . Recall that $G_n = \gamma_n S$ for $n \geq 1$ by Proposition 4.3(b).

The following proposition describes the basic power-commutator structure in extensions of G by A :

Proposition 5.3. *Let $c \in H^2(G, A)$ with $\text{Ext}(c) = A \xrightarrow{\iota} \widehat{G} \xrightarrow{\varphi} G$. Let $\widehat{S} = \varphi^{-1}(S)$ and $\widehat{G}_k = \varphi^{-1}(G_k)$ for $k \in \mathbb{N}$. The following hold:*

- (a) $\gamma_{k+de}\widehat{S} = (\gamma_k\widehat{S})^p$ for any $k > \frac{de}{p-1} + 1$;
- (b) For any $k \geq 1$ we have $\gamma_{2k+1+\delta}\widehat{S} \subseteq \gamma_2\widehat{G}_k \subseteq \gamma_{2k}\widehat{S}$ where $\delta = 0$ if $d \nmid k$ and $\delta = 1$ if $d \mid k$.
- (c) Let $x \in G_k \setminus G_{k+1}$ for some $k > \frac{de}{p-1} + 1$, and choose any $\hat{x} \in \gamma_k\widehat{S}$ such that $\varphi(\hat{x}) = x$. Then $\hat{x}^{p^n} \in \gamma_{k+nde}\widehat{S} \setminus \gamma_{k+1+nde}\widehat{S}$ for any $n \geq 0$.

Proof. The following property will be used several times in the computation below. If U and V are subgroups of \widehat{G} such that $\varphi(U) = \varphi(V)$, and W is another subgroup of \widehat{G} , then $[U, W] = [V, W]$. This holds since by assumption $\text{Ker } \varphi$ is central, so the equality $\varphi(U) = \varphi(V)$ implies that $U \subseteq V \cdot \text{Ker } \varphi \subseteq V \cdot Z(G)$ and similarly $V \subseteq U \cdot Z(G)$.

We will also use the well-known Hall-Petrescu formula [DDMS, Appendix A] which asserts the following: let a and b be elements of the same group and $H = \langle a, b \rangle$. Then for any integer $m \geq 2$ there exist elements c_2, \dots, c_m (all depending on m) such that $c_i \in \gamma_i H$ for all i and $(ab)^m = a^m b^m \prod_{i=2}^m c_i^{\binom{m}{i}}$.

If m is prime, letting $a = x^{-1}$ and $b = y^{-1}xy$ where x and y are elements of the same group, and using the fact that $\langle a, b \rangle = \langle x, [x, y] \rangle$ we deduce the following:

$$(5.1) \quad [x, y]^p \equiv [x^p, y] \pmod{K}$$

where K is the subgroup normally generated by the p^{th} powers of commutators in x and y involving at least two occurrences of x and commutators in x and y involving at least p occurrences of x .

We now proceed with the proof.

(a) By the Hall-Petrescu formula, every element of $(\gamma_k \widehat{S})^p$ is a product of an element of $\gamma_{pk} \widehat{S}$ and elements of the form $[u, v]^p$ with $u \in \gamma_{k-1} \widehat{S}$ and $v \in \widehat{S}$, and by (5.1), every such $[u, v]^p$ lies in $[(\gamma_{k-1} \widehat{S})^p, \widehat{S}] (\gamma_{2k-1} \widehat{S})^p \gamma_{p(k-1)+1} \widehat{S}$. Thus,

$$(\gamma_k \widehat{S})^p \subseteq [(\gamma_{k-1} \widehat{S})^p, \widehat{S}] (\gamma_{2k-1} \widehat{S})^p \gamma_{p(k-1)+1} \widehat{S}.$$

Replacing k by $2k - 1$ in the above inclusion, then by $2(2k - 1) - 1 = 4k - 3$ etc., after finitely many steps we conclude that

$$(5.2) \quad (\gamma_k \widehat{S})^p \subseteq [(\gamma_{k-1} \widehat{S})^p, \widehat{S}] \gamma_{p(k-1)+1} \widehat{S}.$$

By Proposition 4.3, $(\gamma_{k-1} S)^p = G_{k-1}^p = G_{k+de-1} = \gamma_{k+de-1} S$. Hence $\varphi((\gamma_{k-1} \widehat{S})^p) = \varphi(\gamma_{k+de-1} \widehat{S})$, so $[(\gamma_{k-1} \widehat{S})^p, \widehat{S}] = [\gamma_{k+de-1} \widehat{S}, \widehat{S}] = \gamma_{k+de} \widehat{S}$. It follows from (5.2) that $(\gamma_k \widehat{S})^p \subseteq \gamma_{\min(k+de, p(k-1)+1)} \widehat{S}$. Since $k > \frac{de}{p-1} + 1$, we have $k + de < p(k-1) + 1$, whence $(\gamma_k \widehat{S})^p \subseteq \gamma_{k+de} \widehat{S}$.

The reverse inclusion $\gamma_{k+de} \widehat{S} \subseteq (\gamma_k \widehat{S})^p$ is proved in a similar fashion: as we already showed, $\gamma_{k+de} \widehat{S} = [(\gamma_{k-1} \widehat{S})^p, \widehat{S}]$, and by the Hall-Petrescu formula and (5.1) we have

$$\gamma_{k+de} \widehat{S} = [(\gamma_{k-1} \widehat{S})^p, \widehat{S}] \subseteq (\gamma_k \widehat{S})^p (\gamma_{2k-1} \widehat{S})^p \gamma_{p(k-1)+1} \widehat{S} = (\gamma_k \widehat{S})^p \gamma_{p(k-1)+1} \widehat{S}.$$

Since $p(k-1) + 1 > k + de$, we showed that the subgroups $U = \gamma_{k+de} \widehat{S}$ and $V = (\gamma_k \widehat{S})^p$ of \widehat{S} satisfy $U \subseteq V[U, \widehat{S}]$. Since V is closed and \widehat{S} is pro- p , this easily implies that $U \subseteq V$, as desired.

(b) Since $\varphi(\widehat{G}_k) = \varphi(\gamma_k \widehat{S})$, we have $\gamma_2 \widehat{G}_k = [\widehat{G}_k, \gamma_k \widehat{S}] = [\gamma_k \widehat{S}, \gamma_k \widehat{S}]$, whence $\gamma_2 \widehat{G}_k \subseteq \gamma_{2k} \widehat{S}$. By Proposition 4.3(b) we have $[G_k, G_k] = G_{2k+\delta}$, whence $\varphi([\widehat{G}_k, \widehat{G}_k]) =$

$[\gamma_k S, \gamma_k S] = \gamma_{2k+\delta} S = \varphi(\gamma_{2k+\delta} \widehat{S})$. Therefore,

$$\gamma_2 \widehat{G}_k \supseteq [\gamma_2 \widehat{G}_k, \widehat{S}] = [\gamma_{2k+\delta} \widehat{S}, \widehat{S}] = \gamma_{2k+1+\delta} \widehat{S}.$$

(c) First note that an element \hat{x} with required properties always exists since $G_k = \gamma_k S = \varphi(\gamma_k \widehat{S})$. By part (a) we have $\hat{x}^{p^n} \in \gamma_{k+nde} \widehat{S}$. Now suppose that $\hat{x}^{p^n} \in \gamma_{k+1+nde} \widehat{S}$. Then $x^{p^n} = \varphi(\hat{x}^{p^n}) \in \varphi(\gamma_{k+1+nde} \widehat{S}) = G_{k+1+nde}$ which contradicts Proposition 4.3(c) since $x \notin G_{k+1}$ by assumption. \square

Depth and commutator breaks. Given $c \in H^2(G, A)$, there are two natural ways to measure the ‘‘complexity’’ of the associated extension which lead to the notions of inflation depth and commutator depth of c . However, we will show (see Proposition 5.4 below) that the two notions of depth always coincide.

Definition. Let $A = A_k$ for some $k \geq 1$. Let c be an element of $H^2(G, A)$ with $\text{Ext}(c) = A \xrightarrow{\iota} \widehat{G} \xrightarrow{\varphi} G$. Let $\widehat{S} = \varphi^{-1}(S)$.

- The *inflation depth* of c , denoted by $\text{infdep}(c)$, is the smallest integer m such that c lies in the image of the inflation map $\text{inf} : H^2(G/G_m, A) \rightarrow H^2(G, A)$.
- An integer $m > 1$ will be called a *commutator break* of c if

$$\text{Ker } \varphi \cap \gamma_m \widehat{S} \neq \text{Ker } \varphi \cap \gamma_{m+1} \widehat{S}.$$

- The *commutator depth* of c , denoted by $\text{comdep}(c)$, is the largest integer m such that $\text{Ker } \varphi \cap \gamma_m \widehat{S} \neq \{1\}$. Thus, $\text{comdep}(c)$ is the largest commutator break of c if there is at least one break, and $\text{comdep}(c) = 1$ if c has no breaks.

Proposition 5.4. *For any $c \in H^2(G, A)$ we have $\text{infdep}(c) = \text{comdep}(c)$.*

Remark: 1. Recall that we identify $H^2(G, A_r)$ with its image in $H^2(G, A_s)$ for any $s \geq r$. This leads to a potential ambiguity in the definitions of commutator breaks and inflation depth, but fortunately the problem does not occur. The fact that commutator breaks do not depend on the choice of s above will be proved in Lemma 5.7 below, and the analogous result for the inflation depth is a direct consequence of Lemma 5.7 and Proposition 5.4. Until such independence has been established, we will occasionally use the notation $\text{infdep}(c, A_s)$ for the inflation depth of some $c \in H^2(G, A_r)$ considered as an element of $H^2(G, A_s)$ with $s \geq r$. It is clear from the definitions that $\text{infdep}(c, A_s) \geq \text{infdep}(c, A_{s'})$ if $s \leq s'$.

2. The definitions of commutator and inflation depth make perfect sense for any profinite group G with an open pro- p subgroup S , where in the definition of inflation depth we set $G_i = \gamma_i S$. As our proof of Proposition 5.4 will show, the inequalities $\text{infdep}(c) - 1 \leq \text{comdep}(c) \leq \text{infdep}(c)$ will hold in general, but in order to rule out the possibility that $\text{comdep}(c) = \text{infdep}(c) - 1$ we will need to use rather specific information about $G = SL_1(D)$.

In order to prove Proposition 5.4, we will use the following deep result from [PR2].

Lemma 5.5. (see [PR2, Theorem 7.1]). *If F has no primitive p^{th} root of unity, the group $H^2(G, A_1)$ is trivial (and hence $H^2(G, A_\infty)$ is also trivial by Lemma 5.1(b)(c)).*

Otherwise, $H^2(G, A_1)$ has order p and for any non-trivial $c \in H^2(G, A_1)$ one has

$$\text{infdep}(c, A_s) = \frac{pde}{p-1}$$

for sufficiently large s . \square

Remark: 1. The existence of a primitive p^{th} root of unity in F implies that $p-1$ divides e .

2. The statement in [PR2] asserts that any non-trivial $c \in H^2(G, A_1)$ has inflation depth $\frac{pde}{p-1}$ as an element of $H^2(G, A_\infty)$. However, the above formulation is clearly equivalent since any element of $H^2(G/G_m, A_\infty)$ comes from $H^2(G/G_m, A_s)$ for some $s \in \mathbb{N}$, as G/G_s is finite (see the proof of Lemma 5.1(c)).

3. For our proof of Proposition 5.4 to go through it would be sufficient to know that $\text{infdep}(c) > 2$ for any $0 \neq c \in H^2(G, A_1)$. However, we will need the full power of Lemma 5.5 later in the paper anyway.

Corollary 5.6. *Let c be a non-trivial element of $H^2(G, A_r)$ for some r . Then*

$$\text{infdep}(c, A_s) \geq \frac{pde}{p-1} \text{ for all } s \geq r.$$

Proof. Suppose that c has order p^k . Fix $s \geq r$, and let $m = \text{infdep}(c, A_s)$. Thus c is the inflation image of some $c_1 \in H^2(G/G_m, A_s)$. Then $p^{k-1}c_1$ maps to $p^{k-1}c$, so $\text{infdep}(p^{k-1}c, A_s) \leq m$ and hence $\text{infdep}(p^{k-1}c, A_t) \leq m$ for sufficiently large t .

On the other hand, $p^{k-1}c$ has order p and thus lies in $H^2(G, A_1)$. Therefore $\text{infdep}(p^{k-1}c, A_t) = \frac{pde}{p-1}$ for sufficiently large t by Lemma 5.5, so $m \geq \frac{pde}{p-1}$, as desired. \square

Proof of Proposition 5.4. Let $A \xrightarrow{\iota} \widehat{G} \xrightarrow{\varphi} G$ be the extension corresponding to c .

We first prove that $\text{comdep}(c) \leq \text{infdep}(c)$. Let $n = \text{infdep}(c)$. By Lemma 2.1(a), there exists a continuous section $\psi : G \rightarrow \widehat{G}$ such that $\psi(G_n)$ is a normal subgroup of \widehat{G} . Since $G_n = \gamma_n S$, we have $\varphi(\psi(G_n)) = \varphi(\gamma_n \widehat{S})$. Since $\text{Ker } \varphi$ is central in \widehat{G} , we have $[\psi(G_n), \widehat{S}] = [\gamma_n \widehat{S}, \widehat{S}] = \gamma_{n+1} \widehat{S}$, and since $\psi(G_n)$ is normal, we conclude that $\gamma_{n+1} \widehat{S} \subseteq \psi(G_n)$. Since $\text{Im } \psi$ cannot contain non-trivial elements of $\text{Ker } \varphi$, it follows that $\gamma_{n+1} \widehat{S} \cap \text{Ker } \varphi = \{1\}$. Hence $\text{comdep}(c) \leq n$ by the definition of commutator depth.

Next we prove that $\text{comdep}(c) \geq \text{infdep}(c) - 1$. Let $m = \text{comdep}(c)$. Then $\text{Ker } \varphi \cap \gamma_{m+1} \widehat{S} = \{1\}$, whence φ maps $\gamma_{m+1} \widehat{S}$ isomorphically onto $\gamma_{m+1} S = G_{m+1}$. Therefore, φ has a continuous section ψ such that $\psi(G_{m+1}) = \gamma_{m+1} \widehat{S}$. Since \widehat{S} is normal in \widehat{G} , so is $\gamma_{m+1} \widehat{S}$ and therefore $\text{infdep}(c) \leq m+1$ by Lemma 2.1(b). Thus, we showed that $m \geq \text{infdep}(c) - 1$.

Finally, we will show that $\text{comdep}(c) \geq \text{infdep}(c)$ (thereby finishing the proof) using more specific information about $G = SL_1(D)$. If $c = 0$, Proposition 5.4 is trivially true, so from now on we assume that $c \neq 0$. By Corollary 5.6 we have $m \geq \frac{pde}{p-1} - 1$, whence $(\gamma_m \widehat{S})^p \subseteq \gamma_{m+1} \widehat{S}$ by Proposition 5.3(a). We can consider

$\gamma_m \widehat{S} / \gamma_{m+1} \widehat{S}$ as a vector space over \mathbb{F}_p , with the action of Δ , identifying Δ with $G/S \cong \widehat{G}/\widehat{S}$ (recall from Proposition 4.3(a) that Δ is the group of roots of unity of order prime to p in $G \cap W^*$).

Let \overline{K} be the subspace $(\gamma_m \widehat{S} \cap \text{Ker } \varphi) \gamma_{m+1} \widehat{S} / \gamma_{m+1} \widehat{S}$ of $\gamma_m \widehat{S} / \gamma_{m+1} \widehat{S}$. Clearly, \overline{K} is Δ -invariant, and since Δ is a finite group of order prime to p , we can find a Δ -invariant vector subspace \overline{L} of $\gamma_m \widehat{S} / \gamma_{m+1} \widehat{S}$ such that $\gamma_m \widehat{S} / \gamma_{m+1} \widehat{S} = \overline{L} \oplus \overline{K}$. Let H be the full preimage of \overline{L} under the projection $\gamma_m \widehat{S} \rightarrow \gamma_m \widehat{S} / \gamma_{m+1} \widehat{S}$. Then H lies between $\gamma_m \widehat{S}$ and $\gamma_{m+1} \widehat{S}$, so H is automatically normal in \widehat{S} . Moreover, H is Δ -invariant, so H is normal in \widehat{G} . By construction, $H \cap \text{Ker } \varphi = \{1\}$ and $\varphi(H) = \gamma_m S = G_m$, so φ has a continuous section ψ' such that $\psi'(G_m) = H$. Applying Lemma 2.1(b) as earlier in this proof, we conclude that $\text{infdep}(c) \leq m = \text{comdep}(c)$. \square

The following lemma combined with Proposition 5.4 ensures that there is no ambiguity in the definition of commutator breaks and inflation depth:

Lemma 5.7. *Let $c \in H^2(G, A_r)$ for some r , and let $s > r$. If $c' \in H^2(G, A_s)$ is the image of c under the natural mapping $H^2(G, A_r) \rightarrow H^2(G, A_s)$, then c and c' have the same set of commutator breaks. In particular, $\text{comdep}(c') = \text{comdep}(c)$.*

Proof. Let $Z \in Z^2(G, A_r)$ be a cocycle representing c . Suppose that $\text{Ext}(c) = A_r \hookrightarrow \widehat{G} \xrightarrow{\varphi} G$ and $\text{Ext}(c') = A_s \hookrightarrow \widehat{G}' \xrightarrow{\varphi'} G$. We can assume that $\widehat{G} = A_r \times G$, $\widehat{G}' = A_s \times G$ as topological spaces, both φ and φ' are the projections onto the second component and the multiplication in both \widehat{G} and \widehat{G}' is given by (2.2) (using the same cocycle Z in both cases).

If $\widehat{S} = \varphi^{-1}(S)$ and $\widehat{S}' = \varphi'^{-1}(S)$, then $\widehat{S} = A_r \times S$ and $\widehat{S}' = A_s \times S$, so \widehat{S} is a subgroup of \widehat{S}' , and \widehat{S}' is the product of \widehat{S} and the center of \widehat{S}' . Thus for all $m \geq 2$ we have $\gamma_m \widehat{S}' = \gamma_m \widehat{S}$ and hence $\text{Ker } \varphi' \cap \gamma_m \widehat{S}' = \text{Ker } \varphi \cap \gamma_m \widehat{S}$ (since $\text{Ker } \varphi = \text{Ker } \varphi' \cap \widehat{G}$). Hence by definition c and c' have the same commutator breaks. \square

Now we are ready to prove a formula for commutator breaks.

Proposition 5.8. *Let $c \in H^2(G, A_s)$ for some $s \in \mathbb{N}$, and suppose that $\text{ord}(c) = p^n$. Then c has exactly n commutator breaks $b_1 < \dots < b_n$, and moreover $b_i = de(i + \frac{1}{p-1})$ for all i . In particular, $\text{comdep}(c) = de(n + \frac{1}{p-1})$.*

Remark: An essentially equivalent statement was proved earlier by Prasad (unpublished) using a different method.

Proof. By Lemma 5.7 and Lemma 5.1(b) we can assume that $s = n$.

We will first show that $b_1 = de(1 + \frac{1}{p-1}) = \frac{pde}{p-1}$, then prove that c has exactly n commutator breaks and finally prove the formulas for the remaining breaks. In all parts of the proof we let $A_n \xrightarrow{\iota} \widehat{G} \xrightarrow{\varphi} G$ be the extension corresponding to c and $\widehat{S} = \varphi^{-1}(S)$.

Step 1: Consider the exact sequence $1 \rightarrow A_{n-1} \rightarrow A_n \xrightarrow{\times p^{n-1}} A_1 \rightarrow 1$, let $H^2(G, A_{n-1}) \rightarrow H^2(G, A_n) \rightarrow H^2(G, A_1)$ be the induced maps between the cohomology groups, and let \bar{c} be the image of c in $H^2(G, A_1)$. Since c has order p^n , it does not come from $H^2(G, A_{n-1})$, and hence \bar{c} is non-trivial. Hence $\text{comdep}(\bar{c}) = \text{infdep}(\bar{c}) = \frac{pde}{p-1}$ by Proposition 5.4 and Lemma 5.5.

It is easy to check that $\text{Ext}(\bar{c}) = A_1 \xrightarrow{\bar{c}} \widehat{G}/\iota(A_{n-1}) \xrightarrow{\bar{\varphi}} G$, where $\text{Ker } \bar{\varphi} = \bar{\iota}(A_1) = \iota(A_n)/\iota(A_{n-1})$. Also note that $(\bar{\varphi})^{-1}(S) = \widehat{S}/\iota(A_{n-1})$. We just showed that $b = \frac{pde}{p-1}$ is the unique commutator break of \bar{c} , so $\iota(A_n)/\iota(A_{n-1})$ is contained in $\gamma_b(\widehat{S}/\iota(A_{n-1}))$ and is not contained (and hence has trivial intersection with) $\gamma_{b+1}(\widehat{S}/\iota(A_{n-1}))$. Since $\iota(A_{n-1})$ is the unique maximal subgroup of $\iota(A_n)$, it follows that $\iota(A_n) \subseteq \gamma_b \widehat{S}$ while $\iota(A_n) \not\subseteq \gamma_{b+1} \widehat{S}$, so by definition the first commutator break of c is equal to $b = \frac{pde}{p-1}$.

Step 2: Now let $b_1 = \frac{pde}{p-1} < \dots < b_k$ be the commutator breaks of c . We want to show that $k = n$.

Since $\iota(A_n) \cap \gamma_{b_i} \widehat{S} \neq \iota(A_n) \cap \gamma_{b_{i+1}} \widehat{S}$ for any $1 \leq i \leq k$ and $|A_n| = p^n$, it is clear that $k \leq n$. Suppose now that $k < n$. Then for some i we must have $|\iota(A_n) \cap \gamma_{b_i} \widehat{S} / \iota(A_n) \cap \gamma_{b_{i+1}} \widehat{S}| \geq p^2$. This would imply that the group $\gamma_{b_i} \widehat{S} / \gamma_{b_{i+1}} \widehat{S}$ contains an element of order $\geq p^2$, namely the image of a generator of $\iota(A_n) \cap \gamma_{b_i} \widehat{S}$. Since $b_i \geq \frac{pde}{p-1} > \frac{de}{p-1} + 1$, we obtain a contradiction with Proposition 5.3(a).

The above argument also shows that for each $1 \leq i \leq n$ we have

$$(5.3) \quad \iota(A_n) \cap \gamma_{b_i} \widehat{S} = \iota(A_{n+1-i}) \text{ and } \iota(A_n) \cap \gamma_{b_{i+1}} \widehat{S} = \iota(A_{n-i})$$

We will use this observation in Step 3.

Step 3: Finally we prove that $b_i = de(i + \frac{1}{p-1})$ for $1 \leq i \leq n$ by induction on i . We already know that the result holds for $i = 1$.

Suppose now that $b_i = de(i + \frac{1}{p-1})$ for some $1 \leq i \leq n-1$. By the first equation in (5.3) $\iota(A_{n+1-i}) \subset \gamma_{b_i} \widehat{S}$ whence $\iota(A_{n-i}) = \iota(A_{n+1-i})^p \subset (\gamma_{b_i} \widehat{S})^p = \gamma_{b_i+de} \widehat{S}$, where the last equality holds by Proposition 5.3(a). On the other hand, applying the second equation in (5.3) with i replaced by $i+1$, we get $\iota(A_{n-i}) \not\subseteq \gamma_{b_{i+1}+1} \widehat{S}$. It follows that $b_{i+1} + 1 > b_i + de$, whence $b_{i+1} \geq b_i + de = (i + 1 + \frac{1}{p-1})de$.

Let us now prove the opposite inequality $b_{i+1} \leq (i + 1 + \frac{1}{p-1})de$. Let x be a generator of A_{n-i} ; then $x \in \gamma_{b_{i+1}} \widehat{S}$ by (5.3). We already know that $b_{i+1} > 2de$, so $\gamma_{b_{i+1}} \widehat{S} = (\gamma_{b_{i+1}-de} \widehat{S})^p$ by Proposition 5.3(a)(b). Moreover, $\gamma_{b_{i+1}-de} \widehat{S}$ is powerful, so $x = y^p$ for some $y \in \gamma_{b_{i+1}-de} \widehat{S}$ by Theorem 3.6.

We claim that $y \in \iota(A_n)$. Indeed, $\varphi(y)^p = \varphi(y^p) = \varphi(x) = 1$ since $x \in \iota(A_n)$. On the other hand, $\varphi(y) \in G_{b_{i+1}-de}$, and $G_{b_{i+1}-de}$ is torsion-free by Proposition 4.3(c). Therefore, $\varphi(y) = 1$, whence $y \in \iota(A_n)$.

Since x is a generator of $\iota(A_{n-i})$ and $x = y^p$, it follows that $y \notin \iota(A_{n-i})$, so $y \notin \iota(A_n) \cap \gamma_{b_{i+1}} \widehat{S}$ by (5.3). Since b_i and b_{i+1} are consecutive commutator breaks, $\iota(A_n) \cap \gamma_{b_i+1} \widehat{S} = \iota(A_n) \cap \gamma_{b_{i+1}} \widehat{S}$, so $y \notin \gamma_{b_i+1} \widehat{S}$. Since we previously established that

$y \in \gamma_{b_{i+1}-de}\widehat{S}$, it follows that $b_i+1 > b_{i+1}-de$ whence $b_{i+1} \leq b_i+de = (i+1+\frac{1}{p-1})de$, as desired. \square

The final result of this section is concerned with the kernel of the restriction map $H^2(G, A) \rightarrow H^2(G_n, A)$ where $A = A_s$ for some s .

Proposition 5.9. *Let $n \in \mathbb{N}$. Let K be the kernel of the restriction map $H^2(G, A) \rightarrow H^2(G_n, A)$, and let $m = \log_p |K|$. Then $m \leq \max\{0, \frac{2n+1}{de} - \frac{1}{p-1}\}$.*

Proof. Suppose that $m > 0$, and let c be an element of K of order p^m (recall that K is cyclic). Let $A \xrightarrow{\iota} \widehat{G} \xrightarrow{\varphi} G$ be the extension determined by c and $\widehat{G}_n = \varphi^{-1}(G_n)$. Since $c \in K$, the extension $A \xrightarrow{\iota} \widehat{G}_n \xrightarrow{\varphi} G_n$ splits, whence $\gamma_2 \widehat{G}_n \cap \iota(A) = \{1\}$. On the other hand, $\gamma_2 \widehat{G}_n \supseteq \gamma_{2n+2} \widehat{S}$ by Proposition 5.3(c), whence $\gamma_{2n+2} \widehat{S} \cap \iota(A) = \{1\}$, and therefore $\text{comdep}(c) \leq 2n+1$. On the other hand, $\text{comdep}(c) = (m + \frac{1}{p-1})de$ by Proposition 5.8, whence $m \leq \frac{2n+1}{de} - \frac{1}{p-1}$. \square

6. REDUCTION TO LIE ALGEBRAS

Notations. Recall that A_s denotes the cyclic group of order p^s for $s \in \mathbb{N}$. We set $\mathfrak{a}_s = \log(A_s)$; thus, $\mathfrak{a}_s \cong \mathbb{Z}/p^s\mathbb{Z}$ considered as an abelian Lie algebra. In analogy with the previous section, we will use the symbol A (resp. \mathfrak{a}) to denote A_s (resp. \mathfrak{a}_s) for some $s \in \mathbb{N}$ when the value of s is not important.

Also recall the basic notations from § 4: F is a p -adic field, e is the ramification index of F , D is a finite-dimensional central division algebra of degree d over F , $G = SL_1(D)$, and for $n \in \mathbb{Z}_{\geq 0}$ we let $\mathfrak{g}_n = \mathfrak{sl}(\pi^n O_D)$.

The following two results on Lie algebra cohomology will be established in the next section. In both theorems \overline{F} denotes the residue field of F .

Theorem 6.1. *Let $p \geq 3$ with $(p, d, |\overline{F}|) \neq (3, 2, 3)$, and let $n = de + 1$. Then the group $H^2(\mathfrak{g}_n, \mathfrak{a})^G$ has exponent $\leq p^{w+4}$, where as before p^w is the largest power of p dividing e .*

Theorem 6.2. *Let $p \geq 3$ with $(p, d, |\overline{F}|) \neq (3, 2, 3)$, and assume that $n \equiv l \equiv 1 \pmod{d}$ and $l > 2n$. Let $c \in H^2(\mathfrak{g}_n, \mathfrak{a})^G$ and let c_1 be the image of c in $H^2(\mathfrak{g}_l, \mathfrak{a})$. Then $\text{ord}(c_1) \leq p^{w+1}$. Furthermore, if $m \geq l + (w+1)de$, there exists $c_2 \in H^2(\mathfrak{g}_l/\mathfrak{g}_m, \mathfrak{a})$ such that $\text{ord}(c_2) \leq p^{w+1}$ and c_2 maps to c_1 under the inflation map $H^2(\mathfrak{g}_l/\mathfrak{g}_m, \mathfrak{a}) \rightarrow H^2(\mathfrak{g}_l, \mathfrak{a})$.*

In this section we will deduce parts (a) and (b) of Theorem 1.1 from Theorem 6.1 and Theorem 6.2, respectively. We start with the less technical proof of part (a).

Lemma 6.3. *Let $p \geq 5$, $n \geq de + 1$, and let $H^2(G_n, A)^\#$ be the image of the restriction map $H^2(G, A) \rightarrow H^2(G_n, A)$. Then $H^2(G_n, A)^\# \subseteq H_{\mathfrak{G}}^2(G_n, A)^G$ where $\mathfrak{G} = \mathfrak{G}_{ppc}$.*

Proof. Let $c \in H^2(G, A)$, and write $\text{Ext}(c) = (A \hookrightarrow \widehat{G} \xrightarrow{\varphi} G)$. Let $c_1 \in H^2(G_n, A)$ be the restriction of c ; then $\text{Ext}(c_1) = (A \hookrightarrow \widehat{G}_n \xrightarrow{\varphi} G_n)$ where $\widehat{G}_n = \varphi^{-1}(G_n)$.

We need to prove that $\text{Ext}(c_1) \in \text{Ext}_{\mathfrak{G}}(G_n, A)^G$ which amounts to showing that $\widehat{G}_n \in \text{Ob}(\mathfrak{G})$ and $\text{Ext}(c_1)$ is G -equivariant.

Let $\widehat{S} = \varphi^{-1}(S)$. By Proposition 5.3(b)(c) we have $\widehat{G}_n^p = \gamma_{n+de}\widehat{S}$ and $\gamma_2\widehat{G}_n \subseteq \gamma_{2n}\widehat{S}$. Since $n \geq de$, we conclude that $\gamma_2\widehat{G}_n \subseteq \widehat{G}_n^p$, so \widehat{G}_n is powerful. Since G_n is torsion-free, \widehat{G}_n is automatically p -central, so $\widehat{G}_n \in \text{Ob}(\mathfrak{G})$. Finally, G -equivariance of $\text{Ext}(c_1)$ is clear: the desired action of G on \widehat{G}_n is induced by the conjugation action of \widehat{G} . \square

Now we prove Theorem 1.1(a) whose statement is recalled below.

Theorem 1.1(a). *Assume that $p \geq 5$. Then $|H^2(G, \mathbb{Q}_p/\mathbb{Z}_p)| \leq p^{w+6}$.*

Proof. By Lemma 5.5 (and the remark after it) we can assume that $p-1$ divides e . By Corollary 5.2 we just need to show that for any $s \in \mathbb{N}$ any element of $H^2(G, A_s)$ has order $\leq p^{w+6}$. So let $A = A_s$ for some s , $\mathfrak{a} = \log(A)$, and take any $C \in H^2(G, A)$.

Let $n = de+1$, and let C_1 be the image of C under the restriction map $H^2(G, A) \rightarrow H^2(G_n, A)$. The kernel of this map has order $\leq p^2$ by Proposition 5.9 since $\frac{2n+1}{de} - \frac{1}{p-1} = 2 + \frac{3}{de} - \frac{1}{p-1} < 3$. Hence $\text{ord}(C_1) \geq \frac{\text{ord}(C)}{p^2}$.

By Lemma 6.3, $C_1 \in H_{\mathfrak{G}}^2(G_n, A)^G$ where $\mathfrak{G} = \mathfrak{G}_{ppc}$. Recall that G_n is torsion-free by Proposition 4.3(c). Hence by Proposition 3.7(b) $\text{Ext}_{\mathfrak{G}}(G_n, A)^G$ and $\text{Ext}_{\mathfrak{L}}(\mathfrak{g}_n, \mathfrak{a})^G$ are both groups isomorphic to each other. Therefore, $H_{\mathfrak{G}}^2(G_n, A)^G$ and $H_{\mathfrak{L}}^2(\mathfrak{g}_n, \mathfrak{a})^G$ are isomorphic groups, so in particular $H_{\mathfrak{G}}^2(G_n, A)^G$ is isomorphic to a subgroup of $H^2(\mathfrak{g}_n, \mathfrak{a})^G$. By Theorem 6.1, $H^2(\mathfrak{g}_n, \mathfrak{a})^G$ has exponent $\leq p^{w+4}$. Hence, $\text{ord}(C_1) \leq p^{w+4}$, whence $\text{ord}(C) \leq p^{w+6}$, as desired. \square

Now we turn to Theorem 1.1(b). The idea of the proof is similar to that of part (a) except that instead of Weigel's log functor we shall work with Lazard's log functor which will be applied to appropriate congruence quotients of G .

Lemma 6.4. *Let $m, n \in \mathbb{N}$ be such that $n \leq m \leq (p-1)n$. Let $A = A_s$ and $\mathfrak{a} = \mathfrak{a}_s$ for some s . Then there is a natural isomorphism*

$$\log_{n,m} : \text{Ext}(G_n/G_m, A) \rightarrow \text{Ext}(\mathfrak{g}_n/\mathfrak{g}_m, \mathfrak{a})$$

Moreover, $\log_{n,m}$ maps $\text{Ext}(G_n/G_m, A)^G$ onto $\text{Ext}(\mathfrak{g}_n/\mathfrak{g}_m, \mathfrak{a})^G$.

Proof. Since $m \leq (p-1)n$, the nilpotency class of the group G_n/G_m is at most $p-2$. Thus, if $1 \rightarrow A \rightarrow \widehat{H} \rightarrow G_n/G_m \rightarrow 1$ is any central extension, then \widehat{H} has nilpotency class $\leq p-1$. It follows that $\text{Ext}(G_n/G_m, A) = \text{Ext}_{\mathfrak{G}}(G_n/G_m, A)$ where $\mathfrak{G} = \mathfrak{G}_{<p}$, and similarly $\text{Ext}(\mathfrak{g}_n/\mathfrak{g}_m, \mathfrak{a}) = \text{Ext}_{\mathfrak{L}}(\mathfrak{g}_n/\mathfrak{g}_m, \mathfrak{a})$ where $\mathfrak{L} = \mathfrak{L}_{<p}$. Thus Lemma 6.4 follows directly from Propositions 3.7 which establishes an isomorphism $\log : \text{Ext}(G_n/G_m, A) \rightarrow \text{Ext}(\log(G_n/G_m), \mathfrak{a})$ mapping $\text{Ext}(G_n/G_m, A)^G$ onto $\text{Ext}(\log(G_n/G_m), \mathfrak{a})^G$ and Proposition 4.4(b) which establishes a G -equivariant isomorphism between $\log(G_n/G_m)$ and $\mathfrak{g}_n/\mathfrak{g}_m$. \square

We are now ready to prove Theorem 1.1(b). As with Theorem 1.1(a), we recall the statement.

Theorem 1.1(b). *Let p^w be the largest power of p dividing e . Suppose that $4w + 15 \leq p$. Then $|H^2(G, A)| \leq p^{w+1}$.*

Proof. Again we can assume that $p-1$ divides e by Lemma 5.5, and by Corollary 5.2 we just need to show that for any s , any element of $H^2(G, A_s)$ has order $\leq p^{w+1}$.

For the rest of the proof we fix $A = A_s$ for some s and set $H^2(H) = H^2(H, A)$ for any profinite group H .

Step 1: We claim that there exist $n, l, m \in \mathbb{N}$ such that

- (i) n and l satisfy the hypotheses of Theorem 6.2, that is, $n \equiv l \equiv 1 \pmod{d}$, $l > 2n$ and $m \geq l + (w+1)de$, and
- (ii) $2l + 1 < \frac{pde}{p-1}$, $m \leq n(p-1)$ and $m \geq (w+2 + \frac{1}{p-1})de$.

Indeed, first take $l \equiv 1 \pmod{d}$ such that $\frac{pde}{2(p-1)} - d - \frac{1}{2} \leq l < \frac{pde}{2(p-1)} - \frac{1}{2}$, then take $n \equiv 1 \pmod{d}$ such that $\frac{l}{2} - d \leq n < \frac{l}{2}$, and set $m = n(p-1)$. We have

$$\begin{aligned} m &\geq \left(\frac{l}{2} - d\right)(p-1) \geq \left(\frac{pde}{4(p-1)} - \frac{3d}{2} - \frac{1}{4}\right)(p-1) \\ &= de \left(\frac{p}{4} - \frac{3(p-1)}{2e} - \frac{p-1}{4de}\right) \geq de \left(w + \frac{15}{4} - \frac{3(p-1)}{2e} - \frac{p-1}{4de}\right). \end{aligned}$$

Since $p-1$ divides e and $p \geq 19$, we have $\frac{15}{4} - \frac{3(p-1)}{2e} - \frac{p-1}{4de} \geq \frac{15}{4} - \frac{3}{2} - \frac{1}{8} = \frac{17}{8} > 2 + \frac{1}{p-1}$. Thus all inequalities in part (ii) hold. The remaining inequality $m \geq l + (w+1)de$ in part (i) holds as well since $l + (w+1)de < \frac{pde}{p-1} + (w+1)de = (w+2 + \frac{1}{p-1})de$.

Now consider the following commutative diagram. All vertical arrows are restriction maps, horizontal arrows without labels are inflation maps, and the two labeled arrows are maps defined in Lemma 6.4 (with Ext groups replaced by the corresponding H^2 groups).

$$(6.1) \quad \begin{array}{ccccccc} & & & & H^2(G/G_m) & \longrightarrow & H^2(G) \\ & & & & \downarrow & & \downarrow \\ & & & & H^2(\mathfrak{g}_n) & \longleftarrow & H^2(\mathfrak{g}_n/\mathfrak{g}_m) \xleftarrow{\log_{n,m}} H^2(G_n/G_m) & \longrightarrow & H^2(G_n) \\ & & & & \downarrow & & \downarrow & & \downarrow \\ & & & & H^2(\mathfrak{g}_l) & \longleftarrow & H^2(\mathfrak{g}_l/\mathfrak{g}_m) \xleftarrow{\log_{l,m}} H^2(G_l/G_m) & \longrightarrow & H^2(G_l) \end{array}$$

Step 2: We will argue by contradiction, so assume that $H^2(G)$ contains an element C of order p^{w+2} . By Proposition 5.8, $\text{infdep}(C) = (w+2 + \frac{1}{p-1})de$, so by our assumptions $m \geq \text{infdep}(C)$. Thus C is the inflation image of some $C_1 \in H^2(G/G_m)$. Now let $C_2 \in H^2(G_n/G_m)$, $C_5 \in H^2(G_l/G_m)$, $C_3 \in H^2(G_n)$ and $C_4 \in H^2(G_l)$ be the images of C_1 in the commutative diagram (6.1). Since $2l + 1 < \frac{pde}{p-1}$, the map $H^2(G) \rightarrow H^2(G_l)$ is injective by Proposition 5.9. Therefore, $\text{ord}(C_2) \geq \text{ord}(C_5) \geq \text{ord}(C_4) = \text{ord}(C) = p^{w+2}$.

$$\begin{array}{ccccccc}
 & & & & C_1 & \longrightarrow & C \\
 & & & & \downarrow & & \downarrow \\
 c_3 & \longleftarrow & c_2 & \xleftarrow{\log_{n,m}} & C_2 & \longrightarrow & C_3 \\
 \downarrow & & \downarrow & & \downarrow & & \downarrow \\
 c_4 & \longleftarrow & c_5 & \xleftarrow{\log_{l,m}} & C_5 & \longrightarrow & C_4
 \end{array}$$

Step 3: Let $c_2 = \log_{n,m}(C_2) \in H^2(\mathfrak{g}_n/\mathfrak{g}_m)$ and $c_5 = \log_{l,m}(C_5) \in H^2(\mathfrak{g}_l/\mathfrak{g}_m)$ (recall that the log maps are defined in Lemma 6.4). Since both log maps are isomorphisms, we have $\text{ord}(c_2) \geq \text{ord}(c_5) \geq p^{w+2}$. Let $c_3 \in H^2(\mathfrak{g}_n)$ and $c_4 \in H^2(\mathfrak{g}_l)$ be the images of c_2 in (6.1).

We claim that c_3 and c_4 are G -equivariant, that is, $c_3 \in H^2(\mathfrak{g}_n)^G$ and $c_4 \in H^2(\mathfrak{g}_l)^G$. Indeed, C_2 and C_5 are G -equivariant by Lemma 2.2 since they are restriction images of an element of $H^2(G/G_m, A)$. Hence, by Lemma 6.4, the elements c_2 and c_5 are also G -equivariant. Finally, c_3 and c_4 are G -equivariant by Lemma 2.2 being inflation images of c_2 and c_5 , respectively.

Step 4: By Theorem 6.2, the image of $H^2(\mathfrak{g}_n)^G$ in $H^2(\mathfrak{g}_l)$ has exponent $\leq p^{w+1}$, and every element of $H^2(\mathfrak{g}_l)^G$ is inflated from some element of $H^2(\mathfrak{g}_l/\mathfrak{g}_m)$ of order $\leq p^{w+1}$. Since $c_4 \in H^2(\mathfrak{g}_l)^G$ is the restriction image of $c_3 \in H^2(\mathfrak{g}_n)^G$, it follows that $\text{ord}(c_4) \leq p^{w+1}$ and there exists $c'_5 \in H^2(\mathfrak{g}_l/\mathfrak{g}_m)$ such that $\text{ord}(c'_5) \leq p^{w+1}$, and c'_5 and c_5 both inflate to c_4 .

Step 5: Let K be the kernel of the inflation map $H^2(\mathfrak{g}_l/\mathfrak{g}_m, \mathfrak{a}) \rightarrow H^2(\mathfrak{g}_l, \mathfrak{a})$ where $\mathfrak{a} = \log(A)$. By the inflation-restriction sequence (see, e.g. [Weib, 7.5.3, p. 333]), K is equal to the transgression image of $H^1(\mathfrak{g}_m, \mathfrak{a})^{\mathfrak{g}_l} = \text{Hom}(\mathfrak{g}_m/[\mathfrak{g}_m, \mathfrak{g}_l], \mathfrak{a})$.

Since $l \equiv 1 \pmod{d}$ we have $[\mathfrak{g}_m, \mathfrak{g}_l] = \mathfrak{g}_{m+l}$ (this can be proved similarly to Proposition 4.3(b)). Since $l < de$ by assumption, $[\mathfrak{g}_m, \mathfrak{g}_l] \supset \mathfrak{g}_{m+de} = p\mathfrak{g}_m$. It follows that $\mathfrak{g}_m/[\mathfrak{g}_m, \mathfrak{g}_l]$ and hence also K has exponent $\leq p$.

On the other hand, K contains the element $c_5 - c'_5$ which has order $\geq p^{w+2}$ since $\text{ord}(c_5) \geq p^{w+2}$ by Step 3 while $\text{ord}(c'_5) \leq p^{w+1}$ by Step 4. The obtained contradiction finishes the proof. \square

7. COHOMOLOGY OF LIE ALGEBRAS

In this section we identify \mathfrak{a}_n with the abelian Lie algebra $\frac{1}{p^n}\mathbb{Z}_p/\mathbb{Z}_p$ for $n \in \mathbb{N}$. As before, \mathfrak{a} will denote \mathfrak{a}_n for some n when the value of n is not important. We also set $\mathfrak{a}_\infty = \cup_{n=1}^\infty \mathfrak{a}_n$. Note that \mathfrak{a}_∞ can be naturally identified with $\mathbb{Q}_p/\mathbb{Z}_p$.

The goal of this section is to prove Theorems 6.1 and 6.2. The main part of the proof consists of describing \mathfrak{a}_∞ -valued G -invariant cocycles of the Lie algebras \mathfrak{g}_N for $N \equiv 1 \pmod{d}$. Once this is achieved, both Theorems 6.1 and 6.2 follow very easily.

Throughout the section we will assume that $p \geq 3$, and if $p = 3$, we will assume that $(d, |\overline{F}|) \neq (2, 3)$ where \overline{F} is the residue field of F . We expect that Theorems 6.1

and 6.2 are also valid for $p = 2$ except when $d = 2$ or $(d, |\overline{F}|) = (3, 4)$ (apart from these 2 cases, the only step which does not work for $p = 2$ is the proof of Theorem 7.9). However, we decided not to deal with $p = 2$ since this would add extra technicalities to the proofs while all the parts of Theorem 1.1 require $p \geq 5$ anyway.

Let $\mathfrak{h} = \mathfrak{g}_N$ for some $N \in \mathbb{N}$ (eventually we will assume that $N \equiv 1 \pmod{d}$, but everything before Proposition 7.4 will be valid for all N). Since \mathfrak{h} is a free \mathbb{Z}_p -module, we can realize $H^2(\mathfrak{h}, \mathfrak{a})$ as $Z^2(\mathfrak{h}, \mathfrak{a})/B^2(\mathfrak{h}, \mathfrak{a})$ where $Z^2(\mathfrak{h}, \mathfrak{a})$ and $B^2(\mathfrak{h}, \mathfrak{a})$ are defined as in § 2.2.

Now let $\mathcal{E} = (\mathfrak{a} \xrightarrow{\iota} \widehat{\mathfrak{h}} \twoheadrightarrow \mathfrak{h})$ be an element of $\text{Ext}(\mathfrak{h}, \mathfrak{a})$. Given a linear section $\psi : \mathfrak{h} \rightarrow \widehat{\mathfrak{h}}$, let Z_ψ be the \mathfrak{a} -valued cocycle of \mathfrak{h} corresponding to ψ . If \mathfrak{a} is identified with $\iota(\mathfrak{a})$, the formula for Z_ψ given by (2.3) becomes

$$Z_\psi(u, v) = \psi([u, v]) - [\psi(u), \psi(v)].$$

Suppose that \mathcal{E} is a G -equivariant extension. Can we always choose ψ such that Z_ψ is G -invariant? We do not know the answer to this question; however, it is certainly possible to make Z_ψ invariant under the action of the smaller group Δ (defined in Proposition 4.3(a)) which, as we recall here, consists of roots of unity in $W^* \cap G$ of order prime to p .

Proposition 7.1. *Let \mathfrak{h} and \mathcal{E} be as above. The section ψ can be chosen in such a way that the cocycle $Z = Z_\psi$ is Δ -invariant, that is, $Z(u^g, v^g) = Z(u, v)$ for any $u, v \in \mathfrak{h}$ and $g \in \Delta$ (recall that the action of G on \mathfrak{a} is trivial).*

Proof. Let ψ be some section, and define $\mathfrak{z} : \Delta \rightarrow \text{Hom}(\mathfrak{h}, \mathfrak{a})$ by setting $\mathfrak{z}(g)(u) = \psi(u)^g - \psi(u^g)$. Define the left action of Δ on $\text{Hom}(\mathfrak{h}, \mathfrak{a})$ by setting $g * l(u) = l(u^g)$ (where $l \in \text{Hom}(\mathfrak{h}, \mathfrak{a})$ and $u \in \mathfrak{h}$). Then it is easy to check that \mathfrak{z} is a $\text{Hom}(\mathfrak{h}, \mathfrak{a})$ -valued 1-cocycle of Δ . Since the order of Δ is prime to p and $\text{Hom}(\mathfrak{h}, \mathfrak{a})$ has p -power order, the cohomology group $H^1(\Delta, \text{Hom}(\mathfrak{h}, \mathfrak{a}))$ is trivial, whence \mathfrak{z} is a coboundary. Hence, $\mathfrak{z}(g)(u) = l(u) - l(u^g)$ for some $l \in \text{Hom}(\mathfrak{h}, \mathfrak{a})$, so

$$(7.1) \quad \psi(u)^g - \psi(u^g) = l(u) - l(u^g).$$

Now define $\psi' : \mathfrak{h} \rightarrow \widehat{\mathfrak{h}}$ by $\psi'(u) = \psi(u) - l(u)$. Clearly, ψ' is also a section of \mathcal{E} . Note that $l(u)^g = l(u)$ for any $u \in \mathfrak{h}$ and $g \in \Delta$, since the action of Δ on \mathfrak{a} is trivial. Therefore, using (7.1) for any $u \in \mathfrak{h}$ and $g \in \Delta$ we have $\psi'(u^g) = \psi(u^g) - l(u^g) = \psi(u)^g - l(u) = (\psi(u) - l(u))^g = \psi'(u)^g$, and it follows that $Z_{\psi'}$ is Δ -invariant. \square

Our next goal is to determine all bilinear Δ -invariant maps from $\mathfrak{g}_N \times \mathfrak{g}_N$ to \mathfrak{a}_∞ . Since \mathfrak{g}_N is a finitely generated \mathbb{Z}_p -module, the image of such map lies in \mathfrak{a}_n for some n . But first we introduce some additional notations.

Let σ and π be as in § 4. For a subset U of W , we set

$$\mathfrak{sl}(U) = \{a \in U : \text{tr}_{W/F}(a) = 0\}.$$

Let W_{ur} (resp. F_{ur}) be the maximal unramified extension of \mathbb{Q}_p in W (resp. F). Then $F_{ur} = W_{ur} \cap F$, and the restriction map $\text{Gal}(W/F) \rightarrow \text{Gal}(W_{ur}/F_{ur})$ is an isomorphism (recall that the extension W/F is unramified by construction).

Let $O = O_{W_{ur}}$ be the ring of integers of W_{ur} . The extension W/W_{ur} is totally ramified of degree e with uniformizer $\tau = \pi^d$, so $O_W = \bigoplus_{i=0}^{e-1} \tau^i O = \bigoplus_{i=0}^{e-1} \pi^{di} O$. Combining this with the decomposition $O_D = \bigoplus_{j=0}^{d-1} \pi^j O_W$ given by (4.3) we deduce that

$$O_D = \bigoplus_{i=0}^{de-1} \pi^i O$$

Further if we set

$$(7.2) \quad O_i = \begin{cases} O & \text{if } d \nmid i \\ \mathfrak{sl}(O) & \text{if } d \mid i \end{cases}$$

then $\mathfrak{g}_0 = \bigoplus_{i=0}^{de-1} \pi^i O_i$ and moreover

$$(7.3) \quad \mathfrak{g}_N = \bigoplus_{i=N}^{N+de-1} \pi^i O_i \text{ for all } N \in \mathbb{N}.$$

Finally if we turn O_i into a Δ -module by setting

$$\alpha^g = \alpha \frac{g}{\sigma^i(g)} \text{ for any } \alpha \in O_i \text{ and } g \in \Delta,$$

it is easy to see that the map from O_i to \mathfrak{g}_0 given by $\alpha \mapsto \alpha\pi^i$ is a monomorphism of Δ -modules.

Definition. Let $C : \mathfrak{g}_N \times \mathfrak{g}_N \rightarrow \mathfrak{a}_\infty$ be a bilinear map. Given $i, j \geq n$, define $C_{i,j} : O_i \times O_j \rightarrow \mathfrak{a}_\infty$ by $C_{i,j}(\alpha, \beta) = C(\alpha\pi^i, \beta\pi^j)$.

Remark: Equation (7.3) implies that a bilinear map $C : \mathfrak{g}_N \times \mathfrak{g}_N \rightarrow \mathfrak{a}_\infty$ is completely determined by the corresponding $C_{i,j}$ for $N \leq i, j \leq N + de - 1$, and one can think of $C_{i,j}$ for i and j in this range as *homogeneous components* of C . However, it will be convenient to keep track of the maps $C_{i,j}$ for all $i, j \geq N$.

It is clear that a bilinear map $C : \mathfrak{g}_N \times \mathfrak{g}_N \rightarrow \mathfrak{a}_\infty$ is Δ -invariant if and only if each $C_{i,j}$ is Δ -invariant. A complete description of Δ -invariant maps from $O_i \times O_j$ to \mathfrak{a}_∞ is given by the following proposition. In order to state this and all subsequent results, we use the maps introduced in Claim 4.5 as well as the following shortcut notations:⁸ $\mathbf{w} = W_{ur}/O_{W_{ur}}$, $\mathbf{f} = F_{ur}/O_{F_{ur}}$, $\mathbf{Tr} = \mathbf{tr}_{\mathbf{w}/\mathbf{f}}$ and $\mathbf{tr} = \mathbf{tr}_{\mathbf{w}/\mathfrak{q}_p}$, where $\mathfrak{q}_p = \mathbb{Q}_p/\mathbb{Z}_p$. Recall that \mathfrak{q}_p can be naturally identified with \mathfrak{a}_∞ .

Proposition 7.2. Fix $i, j \in \mathbb{N}$ and let $E : O_i \times O_j \rightarrow \mathfrak{a}_\infty$ be bilinear and Δ -invariant.

- (a) If $d \nmid (i + j)$, then $E = 0$.
- (b) If $d \mid (i + j)$ and $d \nmid i$ (hence $d \nmid j$ as well), there exists $\lambda \in \mathbf{w}$ such that

$$E(\alpha, \beta) = \mathbf{tr}(\lambda \alpha \sigma^i(\beta)) \text{ for all } \alpha \in O_i \text{ and } \beta \in O_j.$$

⁸These notations are slightly different from § 4.2, e.g. \mathbf{w} denotes $W_{ur}/O_{W_{ur}}$ and not W/O_W .

Proof. First, without loss of generality we can assume that $d \nmid i$.

Let k be the smallest integer such that the image of E lies in \mathfrak{a}_k . We will prove (a) and (b) simultaneously by induction on k (with the case $k = 0$ being obvious).

Let $\mathfrak{o}_n = O_n/pO_n$, with the induced Δ -module structure. If $d \nmid n$, we can identify \mathfrak{o}_n with \overline{W} , the residue field of W (which is naturally isomorphic to the residue field of W_{ur}), and if $d \mid n$, we can identify \mathfrak{o}_n with $\mathfrak{sl}(\overline{W}) = \{x \in \overline{W} : \mathbf{tr}_{\overline{W}/\overline{F}}(x) = 0\}$.

Define the map $\overline{E} : \mathfrak{o}_i \times \mathfrak{o}_j \rightarrow \frac{1}{p}\mathbb{Z}_p/\mathbb{Z}_p$ by setting

$$\overline{E}(\alpha + pO_i, \beta + pO_j) = p^{k-1}E(\alpha, \beta).$$

Clearly, \overline{E} is Δ -invariant as well.

Claim 7.3. *There exists $\mu \in \overline{W}$ such that $\overline{E}(\alpha, \beta) = \mathbf{tr}_{\overline{W}/\overline{F}}(\mu\alpha\sigma^i(\beta))$ for any $\alpha \in \mathfrak{o}_i$ and $\beta \in \mathfrak{o}_j$. Moreover, $\mu = 0$ if $d \nmid (i + j)$.*

Claim 7.3 is essentially established in [PR2]; however since we cannot formally deduce it from the results stated in [PR2], we will provide a proof.

Proof of Claim 7.3. First, since by our assumptions the pair $(d, |\overline{F}|)$ is different from (3, 4) and (2, 3) and $d \nmid i$, by [Ri, Theorem 7] \mathfrak{o}_i is a simple $\overline{F}[\Delta]$ -module. This implies that any Δ -invariant bilinear map $\mathfrak{o}_i \times \mathfrak{o}_j \rightarrow \overline{F}$ is either the zero map or is non-degenerate on the left. In the latter case this map induces a non-trivial $\overline{F}[\Delta]$ -module homomorphism from \mathfrak{o}_i to the dual of \mathfrak{o}_j , which by [PR2, 1.8] is only possible if $d \mid (i + j)$. Thus, $\overline{E} = 0$ if $d \nmid (i + j)$.

Suppose now that $d \mid (i + j)$ (and hence $d \nmid j$ as well). For each $\mu \in \overline{W}$ define $E_\mu : \overline{W} \times \overline{W} \rightarrow \overline{F}$ by $E_\mu(\alpha, \beta) = \mathbf{tr}_{\overline{W}/\overline{F}}(\mu\alpha\sigma^i(\beta))$. It is straightforward to check that each E_μ is Δ -invariant (see (7.4) below); moreover the map $\mu \mapsto E_\mu$ is injective. Thus, the functions E_μ form a subspace of dimension $[\overline{W} : \overline{F}]$ in the space of all Δ -invariant bilinear forms $\overline{W} \times \overline{W} \rightarrow \overline{F}$. Any subspace of a larger dimension must contain a nonzero degenerate form, which is impossible by the previous paragraph. Hence any Δ -invariant bilinear form must equal E_μ for some μ . \square

We proceed with the proof of Proposition 7.2. Let μ be as in Claim 7.3, but now think of it as an element of $\frac{1}{p}O/O \subset \mathfrak{w} = W_{ur}/O$. Choose $\lambda \in \mathfrak{w}$ such that $p^{k-1}\lambda = \mu$ (if $\mu = 0$, set $\lambda = 0$). Define $E_1 : O_i \times O_j \rightarrow \mathfrak{a}_k$ by $E_1(\alpha, \beta) = \mathbf{tr}(\lambda\alpha\sigma^i(\beta))$. We claim that E_1 is Δ -invariant. Indeed, if $d \nmid (i + j)$, then $E_1 = 0$ and there is nothing to prove. If $d \mid (i + j)$, then for any $g \in \Delta$, $\alpha \in O_i$ and $\beta \in O_j$ we have

$$(7.4) \quad \alpha^g \sigma^i(\beta)^g = \alpha \frac{g}{\sigma^i(g)} \sigma^i(\beta) \sigma^i \left(\frac{g}{\sigma^j(g)} \right) = \alpha \sigma^i(\beta).$$

Now $E - E_1$ is a bilinear Δ -invariant map, and it follows from our construction that the image of $E - E_1$ lies in \mathfrak{a}_{k-1} . By induction, $(E - E_1)(\alpha, \beta) = \mathbf{tr}(\lambda_1\alpha\sigma^i(\beta))$ for some $\lambda_1 \in \mathfrak{w}$, whence E has the desired form. \square

Definition. Let $C : \mathfrak{g}_N \times \mathfrak{g}_N \rightarrow \mathfrak{a}_\infty$ be a bilinear map. A pair of integers (i, j) , with $i, j \geq N$, will be called *regular* for C if there exists $\lambda \in \mathfrak{w}$ such that

$$(7.5) \quad C_{i,j}(\alpha, \beta) = \mathbf{tr}(\lambda\alpha\sigma^i(\beta)) \text{ for all } \alpha \in O_i \text{ and } \beta \in O_j.$$

The set of regular pairs will be denoted by $I_{reg}(C)$.

One may ask if equation (7.5) determines λ uniquely. By Claim 4.5(e)(f), the answer is yes, unless $d = 2$, $d \mid i$ and $d \mid j$. In the latter case the set of all λ satisfying (7.5) has the form $\lambda_0 + \mathfrak{sl}(\mathbf{w})$ for some λ_0 ; since $p \neq 2$ by our assumptions, the set $\lambda_0 + \mathfrak{sl}(\mathbf{w})$ contains exactly one element of \mathbf{f} . This observation motivates our next definition.

Definition. Let C be as above and $(i, j) \in I_{reg}(C)$. Define $\lambda_{i,j}(C) \in \mathbf{w}$ as follows:

If $d > 2$ or $d \nmid i$ or $d \nmid j$, let $\lambda_{i,j}(C)$ be the unique $\lambda \in \mathbf{w}$ such that (7.5) holds.

If $d = 2$, $d \mid i$ and $d \mid j$, let $\lambda_{i,j}(C)$ be the unique $\lambda \in \mathbf{f}$ such that (7.5) holds.

Proposition 7.2 can now be restated as follows: if C is Δ -invariant, then $I_{reg}(C)$ contains all pairs (i, j) such that $d \nmid i$ or $d \nmid j$; moreover $\lambda_{i,j}(C) = 0$ whenever $d \nmid (i + j)$. If C is also a cocycle, we can say much more:

Proposition 7.4. *Let C be a Δ -invariant cocycle of \mathfrak{g}_N . For $(i, j) \in I_{reg}(C)$ set $\lambda_{i,j} = \lambda_{i,j}(C)$.*

(a) *The following relations hold provided all symbols occurring in them are defined:*

$$(R1) \quad \lambda_{i,j} = -\sigma^i(\lambda_{j,i})$$

$$(R2) \quad \lambda_{i+j,k} = \lambda_{i,j+k} + \sigma^i(\lambda_{j,i+k}) = \sigma^j(\lambda_{i,j+k}) + \lambda_{j,i+k} \text{ unless } i, j \text{ and } k \text{ are all divisible by } d.$$

(b) *Let $i \geq 2N$, $j \geq N$, with $d \mid i$ and $d \mid j$. Then $(i, j) \in I_{reg}(C)$ provided there exist $k, l \geq N$, with $k + l = i$ and $k \equiv 1 \pmod{d}$, such that*

$$\lambda_{k,l+j} + \sigma^k(\lambda_{l,k+j}) \in \mathbf{f} \quad (***)$$

Moreover, such k and l exist if $N \equiv 1 \pmod{d}$ and $p \nmid d$.

Proof. (a) Relation (R1) follows immediately from the equality $C(\alpha\pi^i, \beta\pi^j) = -C(\beta\pi^j, \alpha\pi^i)$, so we will only prove (R2).

First note that if $d \nmid (i + j + k)$, then all expressions in (R2) vanish by Proposition 7.2(a). So, from now on we assume that $d \mid (i + j + k)$. Applying the equation $C([u, v], w) + C([v, w], u) + C([w, u], v) = 0$ with $u = \alpha\pi^i$, $v = \beta\pi^j$ and $w = \gamma\pi^k$ and simplifying we have

$$(7.6) \quad \mathbf{tr}(\mu\alpha\sigma^i(\beta)\sigma^{-k}(\gamma) + \nu\beta\sigma^j(\alpha)\sigma^{-k}(\gamma)) = 0 \text{ whenever } \alpha\pi^i, \beta\pi^j, \gamma\pi^k \in \mathfrak{g}_N$$

where $\mu = \lambda_{i+j,k} + \sigma^i(\lambda_{j+k,i}) + \sigma^{-k}(\lambda_{k+i,j})$ and $\nu = \lambda_{i+j,k} + \sigma^{-k}(\lambda_{j+k,i}) + \sigma^j(\lambda_{k+i,j})$. It follows from (R1) that $\mu = \lambda_{i+j,k} - \lambda_{i,j+k} - \sigma^i(\lambda_{j,i+k})$ and $\nu = \lambda_{i+j,k} - \sigma^j(\lambda_{i,j+k}) - \lambda_{j,i+k}$, and all we have to show is that $\mu = \nu = 0$.

Recall that at least one of the numbers i, j and k is not divisible by d ; in fact, since we assume that $d \mid (i + j + k)$, at least two of these numbers are not divisible by d . It is easy to see that any permutation of i, j and k leaves the set $\{\mu, \sigma^{-i}(\mu), \sigma^k(\mu), \nu, \sigma^{-j}(\nu), \sigma^k(\nu)\}$ invariant. Thus, without loss of generality we can assume that $d \nmid j$ and $d \nmid k$.

Since $d \nmid k$, we can choose any $\gamma \in O$ in (7.6), and therefore by Claim 4.5(e), $\mu\alpha\sigma^i(\beta) - \nu\beta\sigma^j(\alpha) = 0$ for all $\alpha \in O_i$ and $\beta \in O_j$.

Assume now that $\nu \neq 0$; it is clear that $\mu \neq 0$ as well. Arguing as in the proof of Claim 4.5, we deduce that there exist nonzero elements $\mu_{res}, \nu_{res} \in \overline{W}$ (the residue field of W) with the following property:

$$\mu_{res}\alpha\sigma^i(\beta) - \nu_{res}\beta\sigma^j(\alpha) = 0$$

where $\beta \in \overline{W}$ is arbitrary and $\alpha \in \overline{W}$ is arbitrary if $d \nmid i$ and lies in $\mathfrak{sl}(\overline{W})$ if $d \mid i$.

Since now we have an equation in a field, we can rewrite it as $\frac{\mu_{res}}{\nu_{res}} = \frac{\beta\sigma^j(\alpha)}{\alpha\sigma^i(\beta)}$. Thus, the quotient $\frac{\beta\sigma^j(\alpha)}{\alpha\sigma^i(\beta)}$ is constant for all nonzero α, β as above. Clearly, this is impossible if $d \nmid i$ (in which case $\alpha, \beta \in \overline{W}$ are arbitrary). Thus, we can assume that $d \mid i$, in which case the condition simplifies to $\frac{\sigma^j(\alpha)}{\alpha}$ being constant for all nonzero $\alpha \in \mathfrak{sl}(\overline{W})$. A simple counting argument shows that the latter is possible only if $d = 2$, in which case $\alpha \in \mathfrak{sl}(\overline{W})$ if and only if $\frac{\sigma^j(\alpha)}{\alpha} = -1$ (since j is odd).

Thus, we proved that $\mu = \nu = 0$ unless $d = 2$, i is even and j and k are both odd, so we proceed with the latter case. The original equation (7.6) in this case immediately implies that $\mu = -\nu$. But recall that in this case the definition of λ 's is different. Since $d \mid i$ and $d \mid (j+k)$, we have $\lambda_{j+k,i} \in \mathbf{f}$ by definition, so $\sigma^t(\lambda_{j+k,i}) = \lambda_{j+k,i}$ for all t . Therefore, $\mu - \nu = \sigma^{-k}(\lambda_{k+i,j}) - \sigma^j(\lambda_{k+i,j}) = 0$ (since $-k \equiv j \pmod{d}$). Thus, we finally showed that $\mu = \nu = 0$.

(b) Let $k, l \geq N$ be such that $k+l = i$ and $k \equiv 1 \pmod{d}$. Apply the equation $C([u, v], w) + C([v, w], u) + C([w, u], v) = 0$ with $u = \alpha\pi^k$, $v = \pi^l$ and $w = \gamma\pi^j$, where $\alpha \in O$ and $\gamma \in \mathfrak{sl}(O)$. Since $(k, l+j), (l, k+j) \in I_{reg}(C)$ by Proposition 7.2, after simplifications we get

$$(7.7) \quad C((\alpha - \sigma^{-1}(\alpha))\pi^i, \gamma\pi^j) = \mathbf{tr}(\gamma(\sigma^{-1}(\nu\alpha) - \nu\alpha)),$$

where $\nu = \lambda_{k,l+j} + \sigma^k(\lambda_{l,k+j})$.

If we know that $\nu \in \mathbf{f}$, then $\sigma^{-1}(\nu\alpha) - \nu\alpha = \nu(\sigma^{-1}(\alpha) - \alpha)$. So, (7.7) implies that $C(\beta\pi^i, \gamma\pi^j) = \mathbf{tr}(\nu\beta\gamma)$ for all $\beta, \gamma \in \mathfrak{sl}(O)$ since any $\beta \in \mathfrak{sl}(O)$ is of the form $\alpha - \sigma^{-1}(\alpha)$ for some $\alpha \in O$ by Claim 4.5(c). Therefore, by definition $(i, j) \in I_{reg}(C)$.

Let us now prove the ‘moreover’ part. First, if $N \equiv 1 \pmod{d}$, we can always write $i = k+l$ as in the first line of the proof of (b) by setting $k = N$ and $l = i - N$. It remains to show that $\nu \in \mathbf{f}$ if $p \nmid d$. Replace α by $\alpha + 1$ in (7.7). The left-hand side does not change, and the right-hand side changes by $\mathbf{tr}(\gamma(\sigma^{-1}(\nu) - \nu))$. Thus $\mathbf{tr}(\gamma(\sigma^{-1}(\nu) - \nu)) = 0$ for any $\gamma \in \mathfrak{sl}(O)$, whence $\sigma^{-1}(\nu) - \nu \in \mathbf{f}$ by Claim 4.5(g). Now $\mathbf{Tr}(\sigma^{-1}(\nu) - \nu) = 0$; on the other hand, $\mathbf{Tr}(\mu) = d\mu$ for any $\mu \in \mathbf{f}$. Since $p \nmid d$, we conclude that $\sigma^{-1}(\nu) - \nu = 0$, whence $\nu \in \mathbf{f}$ by Claim 4.5(b). \square

New notations.

1. For the remainder of the section we fix $f \in \mathbb{N}$ and set $N = df + 1$.
2. For $m, n \in \mathbb{N}$, with $m \leq n$, we set $[m, n] = \{k \in \mathbb{N} : m \leq k \leq n\}$.
3. For $n \geq 2f + 1$, let $I_{n,f} = [df + 1, dn - (df + 1)]$.
4. (taken from [PR2]). Given $\lambda \in \mathbf{w}$ and $i \geq 0$, let

$$\lambda(i) = \lambda + \sigma(\lambda) + \dots + \sigma^{i-1}(\lambda).$$

Note that $\lambda(i) + \sigma^i(\lambda(j)) = \lambda(i+j)$.

Proposition 7.5. *Let C be a Δ -invariant cocycle of \mathfrak{g}_{df+1} and set $\lambda_{i,j} = \lambda_{i,j}(C)$ for $(i,j) \in I_{\text{reg}}(C)$. Let $n \geq 4f + 2$. The following hold:*

- (a) $I_{\text{reg}}(C)$ contains $(i, dn - i)$ for every $i \in I_{n,f}$.
- (b) There exists $\kappa_n \in \mathbf{w}$ such that $\lambda_{i, dn-i} = \kappa_n(i)$ for all $i \in I_{n,f}$.

First we make some preparations. Given i such that $(i, dn - i) \in I_{\text{reg}}(C)$, set

$$\mu_i = \lambda_{i, dn-i}(C).$$

By Proposition 7.2, μ_i is defined whenever $i \in I_{n,f}$ and $d \nmid i$. Moreover, if $d = 2$ (in which case $p \nmid d$ by our assumption), μ_i is defined for all $i \in I_{n,f}$ by Proposition 7.4(b), so we already proved Proposition 7.5(a) for $d = 2$.

Relation (R2) of Proposition 7.4(a) implies that

$$(7.8) \quad \mu_{i+j} = \mu_i + \sigma^i(\mu_j) = \mu_j + \sigma^j(\mu_i) \text{ unless } d \mid i \text{ and } d \mid j$$

(whenever μ_i, μ_j, μ_{i+j} are defined).

Claim 7.6. *Let $\mu = \mu_{df+1}$. Then $\mu_k - \mu(k) \in \mathbf{f}$ for all $k \in I_{n,f}$ with $k \equiv \pm 1 \pmod{d}$.*

Proof. Let $S = \{k \in I_{n,f} : \mu_k - \mu(k) \in \mathbf{f}\}$. We proceed in several steps.

Step 1: $k \in S$ if $k \in [df + 1, n - (2df + 2)]$ and $k \equiv 1 \pmod{d}$.

Subproof: The restrictions on k imply that $k + df + 1 \in I_{n,f}$. By (7.8) we have $\mu_{df+(k+1)} = \mu + \sigma(\mu_k) = \mu_k + \sigma^k(\mu)$. (Note that $\mu_{df+(k+1)}$ is defined since either $d = 2$ or $d \nmid (df + (k + 1))$). Therefore,

$$\sigma(\mu_k) - \mu_k = \sigma^k(\mu) - \mu = \sigma(\mu(k)) - \mu(k).$$

Hence $\sigma(\mu_k - \mu(k)) = \mu_k - \mu(k)$, and so $\mu_k - \mu(k) \in \mathbf{f}$ by Claim 4.5(b).

Step 2: $k \in S$ if $k \in [2df + 2, n - (df + 1)]$ and $k \equiv -1 \pmod{d}$.

Subproof: By step 1, $dn - k \in S$, so $\mu_{dn-k} - \mu(dn - k) \in \mathbf{f}$. By Proposition 7.4(a) we have $\mu_k = -\sigma^k(\mu_{dn-k})$. Thus, $\mu_k + \sigma^k(\mu(dn - k)) = -\sigma^k(\mu_{dn-k} - \mu(dn - k)) \in \mathbf{f}$. Since $\sigma^k(\mu(dn - k)) = \mu(dn) - \mu(k) = n\mathbf{Tr}(\mu) - \mu(k)$, it follows that $\mu_k - \mu(k) = \mu_k + \sigma^k(\mu(dn - k)) - n\mathbf{Tr}(\mu) \in \mathbf{f}$, and so $k \in S$.

Step 3: if $i, j \in I_{n,f}$ are such that $i \equiv j \equiv \pm 1 \pmod{d}$ and $i + j \in I_{n,f}$, then $i \in S$ if and only if $j \in S$.

Subproof: Since $i \equiv j \equiv \pm 1 \pmod{d}$, we have $\sigma^i = \sigma^j = \sigma^{\pm 1}$, and (7.8) yields $\mu_i - \mu_j = \sigma^{\pm 1}(\mu_i - \mu_j)$ whence $\mu_i - \mu_j \in \mathbf{f}$. Since $\mu(i) - \mu(j) = \frac{i-j}{d}\mathbf{Tr}(\mu) \in \mathbf{f}$, the assertion of step 3 is clear.

Step 4: $k \in S$ for any $k \in I_{n,f}$ with $k \equiv -1 \pmod{d}$.

Subproof: Let $i = df + (d - 1)$ and $j = 2df + (d - 1)$. By step 2 we have $j \in S$. Since $i + j = d(3f + 2) - 2 \leq dn - df - 2$ (recall that $n \geq 4f + 2$ by the hypotheses in Proposition 7.5), step 3 implies that $i = df + (d - 1) \in S$. Once again by step 3, we get that $k \in S$ for any $k \in [df + d - 1, 2df + (d - 1)]$ with $k \equiv -1 \pmod{d}$. Combining this result with step 2, we conclude that $k \in S$ for any $k \in I_{n,f}$ with $k \equiv -1 \pmod{d}$.

Step 5: $k \in S$ for any $k \in I_{n,f}$ with $k \equiv 1 \pmod{d}$.

Subproof: This follows from Step 4 and equality $\mu_k = -\sigma^k(\mu_{dn-k})$ by the same argument as in Step 2. \square

Proof of Proposition 7.5(a). We already know that $(i, dn - i) \in I_{reg}(C)$ if $d \nmid i$. Since C is a cocycle, $(i, dn - i) \in I_{reg}(C)$ if and only if $(dn - i, i) \in I_{reg}(C)$. Thus it suffices to prove that $(i, dn - i) \in I_{reg}(C)$ when $i \geq dn/2$ and $d \mid i$.

Fix such i . Note that $i \geq 2df + d$ since $n \geq 4f + 2$, so we can choose $k, l > df$ such that $k + l = i$, $l \equiv 1 \pmod{d}$ (hence $k \equiv -1 \pmod{d}$). We will show that $\mu_k + \sigma^k(\mu_l) \in \mathbf{f}$, which would imply that $(i, dn - i) \in I_{reg}(C)$ by Proposition 7.4(b).

By Claim 7.6, we have $\mu_k - \mu(k) \in \mathbf{f}$ and $\mu_l - \mu(l) \in \mathbf{f}$ where $\mu = \mu_{df+1}$ as before. Therefore, $\mu_k + \sigma^k(\mu_l) - (\mu(k) + \sigma^k(\mu(l))) = (\mu_k - \mu(k)) + \sigma^k(\mu_l - \mu(l)) \in \mathbf{f}$. Since $\mu(k) + \sigma^k(\mu(l)) = \mu(k+l) = \mu(i) = \frac{i}{d} \mathbf{Tr}(\mu) \in \mathbf{f}$, we deduce that $\mu_k + \sigma^k(\mu_l) \in \mathbf{f}$, as desired.

Once we proved part (a), we know that μ_i is defined for all $i \in I_{n,f}$. We will now establish one more auxiliary result before proving part (b).

Claim 7.7. *Recall that $\mu = \mu_{df+1}$. For each $k \in I_{n,f}$ define $\nu_k = \mu_k - \mu(k)$. Then*

- (i) $\nu_k \in \mathbf{f}$ for all $k \in I_{n,f}$
- (ii) $\nu_{i+j} = \nu_i + \nu_j$ whenever $d \nmid i$ or $d \nmid j$.

Proof. We will prove (i) and (ii) simultaneously. First if $d \nmid i$ or $d \nmid j$ and $i, j, i+j \in I_{n,f}$, (7.8) yields

$$(7.9) \quad \nu_{i+j} = \mu_{i+j} - \mu(i+j) = \mu_i + \sigma^i(\mu_j) - \mu(i) - \sigma^i(\mu(j)) = \nu_i + \sigma^i(\nu_j).$$

Thus, if we already know that $\nu_i, \nu_j \in \mathbf{f}$ for some i and j with $d \nmid i$ or $d \nmid j$, then $\nu_{i+j} \in \mathbf{f}$ (resp. $\nu_{i-j} \in \mathbf{f}$) whenever $i+j \in I_{n,f}$ (resp. $i-j \in I_{n,f}$).

By Claim 7.6 $\nu_i \in \mathbf{f}$ for all $i \in I_{n,f}$ with $i \equiv \pm 1 \pmod{d}$. Starting with this fact and using the observation in the previous paragraph, it is easy to deduce that $\nu_k \in \mathbf{f}$ for all $k \in I_{n,f}$. This proves (i), and (ii) now follows directly from (7.9). \square

Proof of Proposition 7.5(b). We will use the notations introduced in Claim 7.7.

Case 1: $d \neq 2$. For any $i \in [df+1, dn-2df-3]$ we have $\nu_{df+(i+2)} = \nu_{i+1} + \nu_{df+1} = \nu_i + \nu_{df+2}$, whence $\nu_{i+1} - \nu_i = \nu_{df+2} - \nu_{df+1}$ (if $d = 2$ and i is even, both i and $df+2$ are divisible by d , so the above equalities may not hold). Therefore, for each $i \in [df+1, dn-2df-2]$ we have $\nu_i = \nu_{df+1} + (i-df-1)\nu$ where $\nu = \nu_{df+2} - \nu_{df+1}$.

Since $\nu_{2df+2} = 2\nu_{df+1}$ by Claim 7.7(ii), we get $\nu_{df+1} + (df+1)\nu = 2\nu_{df+1}$ and therefore $\nu_{df+1} = (df+1)\nu$. So, for $i \in [df+1, dn-2df-2]$ we have $\nu_i = i\nu$, whence $\mu_i = \mu(i) + i\nu = \{\mu + \nu\}(i)$. The formula $\mu_i = \{\mu + \nu\}(i)$ is easily seen to hold for $dn-2df-2 < i \leq dn-df-1$ as well, e.g. by (7.8).

Case 2: $d = 2$. Let $i \in [2f+1, 2n-4f-3]$. If i is odd, $\nu_{i+1} - \nu_i = \nu_{2f+2} - \nu_{2f+1}$ as in case 1. Similarly, $\nu_{i+1} - \nu_i = \nu_{2f+3} - \nu_{2f+2}$ if i is even. Now let $\alpha = \nu_{2f+2} - \nu_{2f+1}$ and $\beta = \nu_{2f+3} - \nu_{2f+2}$. Arguing as above, we conclude that

$$\nu_{2f+(2i+1)} = \nu_{2f+1} + i(\alpha + \beta) \quad \text{and} \quad \nu_{2f+2i} = \nu_{2f+1} - \beta + i(\alpha + \beta) \quad \text{for } i \in [0, n-3f-2].$$

The equation $\nu_{2f+1} + \nu_{2f+2} = \nu_{4f+3}$ yields $\nu_{2f+1} = f(\alpha + \beta) + \beta$, while the equation $2\nu_{2f+1} = \nu_{4f+2}$ yields $\nu_{2f+1} = f(\alpha + \beta) + \alpha$. It follows that $\alpha = \beta$ and $\nu_{2f+1} = (2f+1)\alpha$. The rest of the proof is the same as in case 1. \square

The assertions of Propositions 7.2 and 7.5 motivate the following definition.

Definition. A bilinear map $C : \mathfrak{g}_{df+1} \times \mathfrak{g}_{df+1} \rightarrow \mathfrak{a}_\infty$ will be called *regular* if there exists a sequence $\{\kappa_n\}_{n=2f+1}^\infty$ such that for any $i, j \geq df+1$ we have $(i, j) \in I_{reg}(C)$ and

$$\lambda_{i,j}(C) = \begin{cases} 0 & \text{if } d \nmid (i+j) \\ \kappa_{(i+j)/d}(i) & \text{if } d \mid (i+j) \end{cases}$$

We will say that $\{\kappa_n\}$ is the *defining sequence* of C (each κ_n is uniquely determined by C , e.g. since $\lambda_{i+1, dn-(i+1)}(C) - \lambda_{i, dn-i}(C) = \sigma^i(\kappa_n)$ for any $i \in [df+1, 2df]$).

Our next result asserts that Δ -invariant cocycles are not far from being regular.

Claim 7.8. *Let C be a Δ -invariant cocycle of \mathfrak{g}_{df+1} . The following hold:*

- (a) *Let $l = dm + 1$ with $m \geq 2f + 1$. Then the restriction of C to $\mathfrak{g}_l \times \mathfrak{g}_l$ is a regular cocycle.*
- (b) *Assume that $f \leq e$. Then $p^3 C$ is a regular cocycle of \mathfrak{g}_{df+1} .*

Proof. (a) is a direct consequence of Proposition 7.2 and Proposition 7.5(b).

(b) Let $D = p^3 C$. Clearly, D is Δ -invariant as well, so $\lambda_{i,j}(D) = 0$ if $d \nmid (i+j)$ by Proposition 7.2. It remains to show that for any $n \geq 2f+1$ there exists $\kappa_n \in \mathfrak{w}$ such that $\lambda_{i, dn-i}(D) = \kappa_n(i)$ for all $i \in I_{n,f}$.

By Proposition 7.5(b) we already know that such κ_n exists for all $n \geq 4f+2$.

Recall that $\tau = \pi^d$ is a uniformizer of F . Since the extension F/F_{ur} is totally ramified of degree e , O_F is a free $O_{F_{ur}}$ -module with basis $1, \tau, \dots, \tau^{e-1}$. Moreover, $\frac{p^3}{\tau^{3e}} \in O_F$, so there exists a unique sequence $\{d_k \in O_{F_{ur}}\}_{k=3e}^{4e-1}$ such that $p^3 = \sum_{k=3e}^{4e-1} d_k \tau^k$. For any $n \geq 2f+1$, $i \in I_{n,f}$, $\alpha \in O_i$, and $\beta \in O_{dn-i}$ we have

$$\begin{aligned} D(\alpha\pi^i, \beta\pi^{dn-i}) &= C(\alpha\pi^i, p^3\beta\pi^{dn-i}) = \sum_{k=3e}^{4e-1} C(\alpha\pi^i, \beta d_k \pi^{dn-i+dk}) = \\ &= \sum_{k=3e}^{4e-1} \mathbf{tr}(\kappa_{n+k}(i)\alpha\sigma^i(\beta)d_k) = \mathbf{tr}(\kappa'_n(i)\alpha\sigma^i(\beta)), \end{aligned}$$

where $\kappa'_n = \sum_{k=3e}^{4e-1} d_k \kappa_{n+k}$ (the right-hand side of the last equality is defined since for $k \geq 3e$ we have $n+k \geq (2f+1) + 3e \geq 5f+1 \geq 4f+2$).

Thus, $\lambda_{i, dn-i}(D) = \kappa'_n(i)$ for all $n \geq 2f+1$ and $i \in I_{n,f}$, as desired. \square

We are now ready to give a full characterization of regular Δ -invariant cocycles. This characterization involves the coefficients of the minimal polynomial of τ over F_{ur} . Since τ is a uniformizer of F , there exists a unique sequence $\{c_k \in O_{F_{ur}}\}_{k=0}^{e-1}$ such that

$$(7.10) \quad \tau^e = p \sum_{k=0}^{e-1} c_k \tau^k.$$

Moreover, c_0 must be a unit of $O_{F_{ur}}$.

Definition. A sequence $\{\kappa_n \in \mathfrak{w}\}_{n=2f+1}^\infty$ will be called *compatible* if for any $n \geq 2f+1$ we have

$$(C1) \quad \kappa_{n+e} = p \sum_{k=0}^{e-1} c_k \kappa_{n+k} \quad (\text{where } \{c_k\} \text{ are given by (7.10)})$$

$$(C2) \quad n \mathbf{Tr}(\kappa_n) = 0.$$

Theorem 7.9. *A sequence $\{\kappa_n\}_{n=2f+1}^\infty$ is the defining sequence of some regular Δ -invariant cocycle of \mathfrak{g}_{df+1} if and only if $\{\kappa_n\}$ is compatible.*

Proof. Let C be a regular Δ -invariant cocycle and let $\{\kappa_n\}$ be the defining sequence of C . By relation (R1) of Proposition 7.4 we have $\kappa_n(i) + \sigma^i(\kappa_n(dn-i)) = 0$, whence $n \mathbf{Tr}(\kappa_n) = 0$, so (C2) holds.

Condition (C1) is a consequence of the identity $C(u, pv) = pC(u, v)$. Indeed, let $n \geq 2f+1$, $i \in I_{n,f}$. For any $\alpha \in O_i$ and $\beta \in O_{dn-i}$ we have $C(\alpha\pi^i, \beta\pi^{d(n+e)-i}) = C(\alpha\pi^i, \beta\pi^{dn-i}\tau^e) = C(\alpha\pi^i, \beta\pi^{dn-i} \cdot p \sum_{k=0}^{e-1} c_k \tau^k) = p \sum_{k=0}^{e-1} C(\alpha\pi^i, c_k \beta \pi^{d(n+k)-i})$. Hence,

$$\mathbf{tr}(\kappa_{n+e}(i)\alpha\sigma^i(\beta)) = p \sum_{k=0}^{e-1} \mathbf{tr}(\kappa_{n+k}(i)c_k\alpha\sigma^i(\beta)), \text{ and (C1) follows immediately.}$$

Conversely, let $\{\kappa_n\}$ be compatible. Given $i, j \geq df+1$, let $\lambda_{i,j} = \kappa_{(i+j)/d}(i)$ if $d \mid (i+j)$ and $\lambda_{i,j} = 0$ if $d \nmid (i+j)$. By equation (7.3) there exists a unique bilinear map $C : \mathfrak{g}_{df+1} \times \mathfrak{g}_{df+1} \rightarrow \mathfrak{a}_\infty$ such that $C_{i,j}(\alpha, \beta) = \mathbf{tr}(\lambda_{i,j}\alpha\sigma^i(\beta))$ for all $i, j \in [df+1, df+de]$, $\alpha \in O_i$ and $\beta \in O_j$. Condition (C1) ensures that the same formulas for $C_{i,j}$ are valid for all $i, j \geq df+1$. By direct computation, C is Δ -invariant.

We also claim that $\lambda_{i,j}(C) = \lambda_{i,j}$. This holds automatically except possibly when $d = 2, d \mid i, d \mid j$. Recall that in the latter case the definition of $\lambda_{i,j}(C)$ is different and we need to check that $\lambda_{i,j} \in \mathfrak{f}$. This holds since by our definition $\lambda_{i, dn-i} = \kappa_n(i) = \frac{i}{d} \mathbf{Tr}(\kappa_n)$ if $d \mid i$.

Condition (C2) implies that $\{\lambda_{i,j}\}$ satisfy relations (R1) and (R2) of Proposition 7.4; moreover (R2) holds even if i, j and k are all divisible by d . It is now easy to deduce that C is a cocycle. The equation $C([u, v], w) + C([v, w], u) + C([w, u], v) = 0$ follows immediately from (R2) by the computation in (7.6).

To prove that C is alternating it suffices to show that

- (i) $C_{j,i}(\beta, \alpha) = -C_{i,j}(\alpha, \beta)$ for all $i, j \geq df+1$ and
- (ii) $C_{i,i}(\alpha, \alpha) = 0$ for all $i \geq df+1$

Condition (i) follows immediately from (R1) of Proposition 7.4. If $d \nmid 2i$, then (ii) is automatic by construction, so assume that $d \mid 2i$. In this case we get

$$C_{i,i}(\alpha, \alpha) = \mathbf{tr}(\lambda_{i,i}\alpha\sigma^i(\alpha)) = \mathbf{tr}(\sigma^i(\lambda_{i,i})\sigma^i(\alpha)\sigma^{2i}(\alpha)) = -C_{i,i}(\alpha, \alpha)$$

where the last equality holds since $d \mid 2i$ and $\sigma^i(\lambda_{i,i}) = -\lambda_{i,i}$ by (R1). Thus, $2C_{i,i}(\alpha, \alpha) = 0$, and since $p > 2$, we deduce that $C_{i,i}(\alpha, \alpha) = 0$, as desired. \square

Next we show that for any compatible sequence $\{\kappa_n\}$, there is a better bound on the orders of $\mathbf{Tr}(\kappa_n)$ than the one given by (C2) alone.

Lemma 7.10. *Let p^w be the highest power of p dividing e . If $\{\kappa_n\}$ is a compatible sequence, then $p^{w+1} \mathbf{Tr}(\kappa_n) = 0$ for all n .*

Proof. Let $\mu_n = \mathbf{Tr}(\kappa_n)$ for $n \geq 2f + 1$. Note that the sequence $\{\mu_n\}$ is compatible as well.

Let l be the smallest integer such that $p^l \mu_n = 0$ for all n , and let m be the largest integer such that $p^{l-1} \mu_m \neq 0$. Such l and m indeed exist and moreover $m \leq 2f + e$ since $\mu_n = p \sum_{k=0}^{e-1} c_k \mu_{n-e+k}$ for $n \geq 2f + e + 1$. We know that $m \mu_m = 0$, so p^l divides m .

Now consider the equality $\mu_{m+e} = p \sum_{k=0}^{e-1} c_k \mu_{m+k}$. The element $\sum_{k=0}^{e-1} c_k \mu_{m+k}$ has order p^l because $c_0 \mu_m$ has order p^l (as c_0 is a unit in $O_{F_{ur}}$) and $c_k \mu_{m+k}$ has order at most p^{l-1} for $k > 0$ (by the choice of m). So, μ_{m+e} has order p^{l-1} .

On the other hand, $(m+e)\mu_{m+e} = 0$. Since p^{l-1} divides m , p^{l-1} must divide e as well. Therefore, $l \leq w + 1$. \square

Proposition 7.11. *Let $\mathfrak{h} = \mathfrak{g}_{df+1}$ for some f , let C be a regular Δ -invariant cocycle of \mathfrak{h} and let $\{\kappa_n\}_{n \geq 2f+1}$ be the defining sequence of C . Let v be any integer such that $C(\mathfrak{h}, \mathfrak{h}) \subseteq \mathfrak{a}_v$ or, equivalently, any integer such that $p^v \kappa_n = 0$ for all $n \geq 2f + 1$. Then there exists a regular cocycle C_1 of \mathfrak{h} such that*

- (a) C and C_1 represent the same class in $H^2(\mathfrak{h}, \mathfrak{a}_v)$
- (b) If $\{\theta_n\}$ is the defining sequence of C_1 , then $p^{w+1} \theta_n = 0$ for all $n \geq 2f + 1$.

Proof. If $v \leq w + 1$, we can simply set $C_1 = C$, so we will assume that $v > w + 1$.

We already know that $p^{w+1} \mathbf{Tr}(\kappa_n) = 0$ for all $n \geq 2f + 1$. Hence $\mathbf{Tr}(\kappa_n) \in \frac{1}{p^{w+1}} O_{F_{ur}} / O_{F_{ur}}$, and therefore by Claim 4.5(d) there exists $\theta_n \in \mathfrak{w}$ such that $\mathbf{Tr}(\theta_n) = \mathbf{Tr}(\kappa_n)$ and $p^{w+1} \theta_n = 0$.

We claim that the sequence $\{\theta_n\}$ can be chosen compatible. We start by choosing any θ_n such that $\mathbf{Tr}(\theta_n) = \mathbf{Tr}(\kappa_n)$ and $p^{w+1} \theta_n = 0$ for $n \in [2f + 1, 2f + e]$. Then there exists a unique way to choose the remaining θ_n so that (C1) holds, that is,

$$\theta_{n+e} = p \sum_{k=0}^{e-1} c_k \theta_{n+k}.$$

Since $\{\kappa_n\}$ satisfies (C1) as well, it follows that $\mathbf{Tr}(\theta_n) = \mathbf{Tr}(\kappa_n)$ for all n , whence $\{\theta_n\}$ satisfies (C2). It remains to show that $p^{w+1} \theta_n = 0$ for all $n \geq 2f + 1$. The latter is true for $n \in [2f + 1, 2f + e]$ by construction, and follows from (C1) for $n \geq 2f + e + 1$.

We proceed with the proof. Since $\{\theta_n\}$ is compatible, there exists a regular cocycle C_1 whose defining sequence is $\{\theta_n\}$. Since $p^{w+1} \theta_n = 0$ for all n , we have $C_1(\mathfrak{h}, \mathfrak{h}) \subseteq \mathfrak{a}_{w+1} \subseteq \mathfrak{a}_v$. It remains to prove the following claim:

Claim 7.12. *The cocycles C and C_1 represent the same class in $H^2(\mathfrak{h}, \mathfrak{a}_v)$.*

Proof. Let $B = C - C_1$ and let $\{\kappa'_n\}$ be the defining sequence of B . Then $\kappa'_n = \kappa_n - \theta_n$, whence $\mathbf{Tr}(\kappa'_n) = 0$. Hence by Claim 4.5(c) there exists $\{\mu_n\}_{n=2f+1}^\infty$ such that $\kappa'_n = \mu_n - \sigma(\mu_n)$. Since $p^v \kappa'_n = 0$, we can assume that $p^v \mu_n = 0$. Similarly, since κ'_n satisfies (C1), we can assume that $\{\mu_n\}$ satisfies (C1).

Let $h : \mathfrak{h} \rightarrow \mathfrak{a}_v$ be the unique \mathbb{Z}_p -linear function such that

$$h(\alpha\pi^n) = \begin{cases} \mathbf{tr}(\alpha\mu_{n/d}) & \text{if } d \mid n \\ 0 & \text{if } d \nmid n \end{cases} \quad \text{for } df + 1 \leq n \leq df + de \text{ and } \alpha \in O_n.$$

Since $\{\mu_n\}$ satisfies (C1), the above formula for $h(\alpha\pi^n)$ holds for all $n \geq df + 1$.

We claim that $B(u, v) = h([u, v])$ for any $u, v \in \mathfrak{h}$. This would imply that B is a coboundary and thus finish the proof of the claim and Proposition 7.11.

Let $u = \sum \alpha_i \pi^i$ and $v = \sum \beta_i \pi^i$ (where $\alpha_i, \beta_i \in O_i$ for all i). Then

$$\begin{aligned} B(u, v) &= \sum_{i,j} B(\alpha_i \pi^i, \beta_j \pi^j) = \sum_{n=2f+1}^{\infty} \sum_{i+j=dn} \mathbf{tr}(\kappa'_n(i) \alpha_i \sigma^i(\beta_j)) = \\ &= \sum_{n=2f+1}^{\infty} \sum_{i+j=dn} \mathbf{tr}((\mu_n - \sigma^i(\mu_n)) \alpha_i \sigma^i(\beta_j)) = \sum_{n=2f+1}^{\infty} \sum_{i+j=dn} \mathbf{tr}(\mu_n(\alpha_i \sigma^i(\beta_j) - \sigma^{-i}(\alpha) \beta_j)) \\ &= \sum_{n=2f+1}^{\infty} \sum_{i+j=dn} h([\alpha_i \pi^i, \beta_j \pi^j]) = \sum_{i,j} h([\alpha_i \pi^i, \beta_j \pi^j]) = h([u, v]). \quad \square \end{aligned}$$

We are now ready to prove Theorems 6.2 and 6.1 whose statements are recalled below. Recall that p^w is the largest power of p dividing e .

Theorem 6.2. *Let $p \geq 3$ with $(p, d, |\overline{F}|) \neq (3, 2, 3)$, and assume that $n \equiv l \equiv 1 \pmod{d}$ and $l > 2n$. Let $c \in H^2(\mathfrak{g}_n, \mathfrak{a})^G$ and let c_1 be the image of c in $H^2(\mathfrak{g}_l, \mathfrak{a})$. Then $\text{ord}(c_1) \leq p^{w+1}$. Furthermore, if $m \geq l + (w+1)de$, there exists $c_2 \in H^2(\mathfrak{g}_l/\mathfrak{g}_m, \mathfrak{a})$ such that $\text{ord}(c_2) \leq p^{w+1}$ and c_2 maps to c_1 under the inflation map $H^2(\mathfrak{g}_l/\mathfrak{g}_m, \mathfrak{a}) \rightarrow H^2(\mathfrak{g}_l, \mathfrak{a})$.*

Proof. Since $c \in H^2(\mathfrak{g}_n, \mathfrak{a})^G$, by Proposition 7.1 it is represented by some Δ -invariant cocycle C of \mathfrak{g}_n . Let C_1 be the restriction of C to $\mathfrak{g}_l \times \mathfrak{g}_l$. By Claim 7.8(a), C_1 is a regular cocycle of \mathfrak{g}_l . Therefore, by Proposition 7.11, there exists a cocycle C'_1 of \mathfrak{g}_l , such that C_1 and C'_1 represent the same cohomology class in $H^2(\mathfrak{g}_l, \mathfrak{a})$ and $p^{w+1}C'_1 = 0$. This implies that $c_1 = [C_1] = [C'_1]$ has order at most p^{w+1} .

Now let $m \geq l + (w+1)de$. Define the \mathfrak{a} -valued 2-cocycle C_2 of $\mathfrak{g}_l/\mathfrak{g}_m$ by setting $C_2(u + \mathfrak{g}_m, v + \mathfrak{g}_m) = C'_1(u, v)$. Then C_2 is well-defined since $p^{w+1}C'_1 = 0$ and $\mathfrak{g}_m \subseteq \mathfrak{g}_{l+(w+1)de} = p^{w+1}\mathfrak{g}_l$. Let $c_2 = [C_2] \in H^2(\mathfrak{g}_l/\mathfrak{g}_m, \mathfrak{a})$. By construction, $\text{ord}(c_2) \leq \text{ord}(C'_1) \leq p^{w+1}$, and the inflation image of c_2 in $H^2(\mathfrak{g}_l, \mathfrak{a})$ is equal to $[C'_1] = c_1$. \square

Theorem 6.1. *Let $p \geq 3$ with $(p, d, |\overline{F}|) \neq (3, 2, 3)$, and let $n = de + 1$. Then the group $H^2(\mathfrak{g}_n, \mathfrak{a})^G$ has exponent $\leq p^{w+4}$.*

Proof. Let $c \in H^2(\mathfrak{g}_n, \mathfrak{a})^G$, and let C be a Δ -invariant cocycle of \mathfrak{g}_n representing c . By Claim 7.8(b), p^3C is a regular cocycle, so arguing as in the proof of Theorem 6.2, we conclude that $[p^3C] \in H^2(\mathfrak{g}_n, \mathfrak{a})$ has order at most p^{w+1} . Therefore, $[C]$ has order at most p^{w+4} . \square

8. REDUCTION TO THE SMALL FIELD CASE

The purpose of this section is to prove part (c) of Theorem 1.1 whose statement is recalled below. The author is grateful to Gopal Prasad for suggesting several ideas used in the proof.

Theorem 8.1. *Assume that $p \geq 19$. Let F be a p -adic field containing a primitive p^2 th root of unity and such that the extension F/\mathbb{Q}_p is Galois. Let D be a central division algebra over F whose degree is not a power of p , and let $G = SL_1(D)$. Then $|H^2(G, \mathbb{R}/\mathbb{Z})| \leq p^{w+1}$ where p^w is the largest power of p dividing the ramification index of F .*

Notation: Throughout this section we set $H^2(G) = H^2(G, \mathbb{R}/\mathbb{Z})$ for any group G .

We start with a simple fact about division algebras over local fields.

Proposition 8.2. *Let K'/K be an extension of local fields, let $n = [K' : K]$, and let $d \in \mathbb{N}$ be coprime to n . The following hold:*

- (a) *Let D be a central division algebra over K of degree d . Then $D \otimes_K K'$ is a central division algebra over K' (also of degree d).*
- (b) *Conversely, if D' is a central division algebra over K' of degree d , then $D' \cong D \otimes_K K'$ for some central division algebra D over K .*

Proof. If F is a local field, the Brauer group $Br(F)$ is canonically isomorphic to \mathbb{Q}/\mathbb{Z} . Under this isomorphism, division algebras of degree d over F correspond to generators of the subgroup $\frac{1}{d}\mathbb{Z}/\mathbb{Z}$ of \mathbb{Q}/\mathbb{Z} . The map $E_{K,K'} : Br(K) \rightarrow Br(K')$ given by $D \mapsto D \otimes_K K'$ corresponds to multiplication by $n = [K' : K]$ under the above identification. Since n is coprime to d , $E_{K,K'}$ maps $\frac{1}{d}\mathbb{Z}/\mathbb{Z}$ onto itself (and sends generators to generators). This yields both assertions of the proposition. \square

Cohomology of SL_d over p -adic fields.

We start by recalling the definition of norm-residue symbols. Let F be a p -adic field, and let μ_F be the group of roots of unity in F . Let F^{ab} be the maximal abelian extension of F , and let $\rho_F : F^* \rightarrow Gal(F^{ab}/F)$ be the (local) Artin map.⁹

Now let $n \in \mathbb{N}$ be any divisor of $|\mu_F|$. The *norm-residue symbol on F^* of order n* is the map $(\cdot, \cdot)_{n,F} : F^* \times F^* \rightarrow \mu_F$ given by

$$(8.1) \quad (a, b)_{n,F} = \frac{\rho_F(a)(\sqrt[n]{b})}{\sqrt[n]{b}}.$$

Note that F contains primitive n^{th} root of unity by assumption, so $\sqrt[n]{b} \in F^{ab}$ and the right-hand side of (8.1) is independent of the choice of $\sqrt[n]{b}$.

We will need the following 3 properties of norm-residue symbols. In all statements below n is a divisor of $|\mu_F|$.

- (NR1) $(a, b)_{n,F}$ is bi-multiplicative, that is, $(ab, c) = (a, c)(b, c)$ and $(a, bc) = (a, b)(a, c)$ for all $a, b, c \in F^*$.
- (NR2) For any m dividing n we have $(a, b)_{m,F} = (a, b)_{n,F}^{n/m}$.

⁹The map ρ_F itself is frequently called the norm-residue symbol.

(NR3) If K/F is a finite extension, then $(a, b)_{n, K} = (N_{K/F}(a), b)_{n, F}$ for all $a \in K^*$ and $b \in F^*$.

(NR1) and (NR2) follow immediately from the definition, and (NR3) follows from a basic result in local class field theory which asserts that $\rho_K(a)|_{F^{ab}} = \rho_F(N_{K/F}(a))$ (see, e.g., [Iw, Theorem 6.9]).

To simplify our notations below we will denote $(\cdot, \cdot)_{|\mu_F|, F}$, the norm-residue symbol on F^* of maximal possible order, simply by $(\cdot, \cdot)_F$.

We now turn to the discussion of the second cohomology groups. Moore [Mo1] showed that $H^2(SL_d(F))$ is isomorphic to μ_F . Elements of $H^2(SL_d(F))$ can be explicitly described as follows [Rp, Theorem B]. Let T be the diagonal subgroup of $SL_d(F)$. Then there is a canonical cocycle $c_F : SL_d(F) \times SL_d(F) \rightarrow \mu_F$ such that

- (i) the cohomology class $[c_F]$ generates $H^2(SL_d(F))$
- (ii) the restriction of c_F to $T \times T$ is given by

$$(8.2) \quad c_F(\text{diag}(\lambda_1, \dots, \lambda_d), \text{diag}(\mu_1, \dots, \mu_d)) = \prod_{i \geq j} (\lambda_i, \mu_j)_F.$$

Now let $\mu_{F, \text{wild}}$ be the p -primary component of μ_F and $H^2(SL_d(F))_{\text{wild}}$ the corresponding subgroup of $H^2(SL_d(F))$. If $n = |\mu_F|$ and $q = |\mu_{F, \text{wild}}|$, then clearly $H^2(SL_d(F))_{\text{wild}}$ is generated by $[c_F]^{n/q} = [c_F^{n/q}]$.

Thus, by property (NR2) above, the restriction of $c_F^{n/q}$ to $T \times T$ is given by

$$(8.3) \quad c_F^{n/q}(\text{diag}(\lambda_1, \dots, \lambda_d), \text{diag}(\mu_1, \dots, \mu_d)) = \prod_{i \geq j} (\lambda_i, \mu_j)_{q, F}.$$

Remark: By [Rp, Lemma 3], the restriction map $H^2(SL_d(F)) \rightarrow H^2(T)$ is injective if $d \geq 3$ and has kernel of order 2 if $d = 2$. Thus, (8.3) determines the cohomology class $[c_F^{n/q}]$ uniquely unless $p = d = 2$.

The following result is established in [PR2, 8.2]:

Lemma 8.3. *Let F be a p -adic field, D a central division algebra over F whose degree is not divisible by p . Let W be a maximal unramified extension of F in D , and let $r_{W, D} : H^2(SL_d(W)) \rightarrow H^2(SL_1(D))$ be the natural restriction map. Then $|\text{Im } r_{W, D}| = |\mu_{F, \text{wild}}|$, and therefore $r_{W, D}$ is injective on $H^2(SL_d(W))_{\text{wild}}$. \square*

Using this lemma and the above description of cohomology of SL_n , we can relate the cohomology groups $H^2(SL_1(D))$ and $H^2(SL_1(D'))$ when D' is obtained from D by a field extension.

Proposition 8.4. *Let K'/K be an extension of p -adic fields and $l = [K' : K]$. Let D be a central division algebra over F whose degree d is coprime to both l and p , let $D' = D \otimes_K K'$, and let $r_{D', D} : H^2(SL_1(D')) \rightarrow H^2(SL_1(D))$ be the restriction map. Let p^s be the largest power of p dividing l , and assume that $|\mu_{K, \text{wild}}| \geq p^{s+1}$. Then $|\text{Ker } r_{D', D}| = p^s$.*

Proof. First, since d is coprime to l , by Proposition 8.2(a) $D' = D \otimes_K K'$ is a central division algebra of degree d over K' . Let W be a maximal unramified extension of K

contained in D . Then $[W : K] = d$ and $W' = W \otimes_K K'$ is an unramified extension of K' of degree d , so W' is a maximal unramified extension of K' in D' . Moreover we have the following commutative diagram:

$$\begin{array}{ccc} H^2(SL_d(W'))_{wild} & \xrightarrow{r_{W',D'}} & H^2(SL_1(D')) \\ \downarrow r_{W',W} & & \downarrow r_{D',D} \\ H^2(SL_d(W))_{wild} & \xrightarrow{r_{W,D}} & H^2(SL_1(D)) \end{array}$$

We claim that it is sufficient to show that

$$(8.4) \quad |\text{Ker } r_{W',W}| = p^s.$$

Indeed, assume that (8.4) holds. Both maps $r_{W',D'}$ and $r_{W,D}$ are injective by Lemma 8.3. Thus, if $P' = \text{Im } r_{W',D'}$ and $P = \text{Im } r_{W,D}$, then

$$|P' \cap \text{Ker } r_{D',D}| = |\text{Ker } r_{W',W}| = p^s.$$

On the other hand, P' and $\text{Ker } r_{D',D}$ both lie in $H^2(SL_1(D'))$ which is cyclic of p -power order, so either $\text{Ker } r_{D',D} \subseteq P'$ or $P' \subseteq \text{Ker } r_{D',D}$. In the former case, we get $|\text{Ker } r_{D',D}| = p^s$, as desired. If $P' \subseteq \text{Ker } r_{D',D}$, then $r_{W',W}$ must be the zero map which contradicts (8.4) since $|H^2(SL_d(W'))_{wild}| = |\mu_{W',wild}| \geq |\mu_{K,wild}| \geq p^{s+1}$ by our hypotheses.

We proceed with proving (8.4). Let $n' = |\mu_{W'}|$, $n = |\mu_W|$, $q' = |\mu_{W',wild}|$ and $q = |\mu_{W,wild}|$. Let $c' = (c_{W'})^{n'/q'}$ and $c = (c_W)^{n/q}$ where $c_{W'}$ and c_W are as in (8.2). Then $H^2(SL_d(W'))_{wild}$ is generated by $[c']$ and $H^2(SL_d(W))_{wild}$ is generated by $[c]$. Given $\alpha, \beta \in W^*$, by properties (NR1)-(NR3) of the norm-residue symbols we have

$$((\alpha, \beta)_{q',W'})^{q'/q} = (\alpha, \beta)_{q,W'} = (\alpha^l, \beta)_{q,W} = ((\alpha, \beta)_{q,W})^l$$

which by (8.3) and the remark after it yields $r_{W',W}([c']^{q'/q}) = [c]^l$. The element $[c]^l$ has order $q/p^s > 1$. Therefore, $\text{Ker } r_{W',W}$ is generated by $([c']^{q'/q})^{q/p^s} = [c]^{q'/p^s}$. Since $\text{ord}([c']) = q'$, we conclude that $|\text{Ker } r_{W',W}| = p^s$. \square

Proof of Theorem 8.1. Let $d = \deg(D)$. Write $d = d_1 d_2$ where d_1 is coprime to p and d_2 is a power of p . By our assumption, $d_1 > 1$.

As before, let W be a maximal unramified extension of F in D , and let K be the unique extension of F of degree d_2 inside W . Note that K and F have the same ramification index. Let D' be the centralizer of K in D . By [PR2, 4.7], D' is a central division algebra of degree d_1 over K , and since $d_1 > 1$, by [PR2, 4.8] the restriction map $H^2(SL_1(D)) \rightarrow H^2(SL_1(D'))$ is injective. Thus it is sufficient to show that $|H^2(SL_1(D'))| \leq p^{w+1}$.

Since F/\mathbb{Q}_p is Galois and K/F is unramified, the extension K/\mathbb{Q}_p is Galois as well (this holds since any local field has a unique unramified extension of any given degree). Therefore, there exists an intermediate field $\mathbb{Q}_p \subset L \subset K$ such that L/\mathbb{Q}_p is tamely ramified and K/L is wildly ramified (specifically we let L be the fixed field of a Sylow p -subgroup of $\text{Gal}(K/K_{ur})$). Thus, $|K : L| = p^w$. Since K contains primitive p th root of unity, so does L .

Since K/L is Galois and $\text{Gal}(K/L)$ is a p -group, there is a tower of fields $L = L_0 \subset L_1 \subset \dots \subset L_w = K$ such that $[L_{i+1} : L_i] = p$ for each i . Furthermore, since $|\mu_{K, \text{wild}}| \geq p^2$ by hypotheses of the theorem, we can assume that $|\mu_{L_1, \text{wild}}| = p^2$. By Proposition 8.2(b), there exists a central division algebra D_0 of degree d_1 over L such that $D_0 \otimes_L K \cong D'$. Let $D_i = D_0 \otimes_L L_i$ for $1 \leq i \leq w$. We shall prove that $|H^2(SL_1(D_i))| \leq p^{i+1}$ for $1 \leq i \leq w$ by induction on i .

The base case $i = 1$ follows from Theorem 1.1(b) since $w(L_1) = 1$. Now suppose that $|H^2(SL_1(D_i))| \leq p^{i+1}$ for some i . Since $D_{i+1} \cong D_i \otimes_{L_i} L_{i+1}$, $[L_{i+1} : L_i] = p$ and $|\mu_{L_i, \text{wild}}| \geq p^2$, Proposition 8.4 yields $|\text{Ker}\{H^2(SL_1(D_{i+1})) \rightarrow H^2(SL_1(D_i))\}| \leq p$, whence $|H^2(SL_1(D_{i+1}))| \leq p \cdot |H^2(SL_1(D_i))| \leq p \cdot p^{i+1} = p^{i+2}$. \square

APPENDIX A. $\exp - \log$ CORRESPONDENCE FOR POWERFUL p -CENTRAL \mathbb{Z}_p -LIE ALGEBRAS AND PRO- p GROUPS

BY MIKHAIL ERSHOV AND THOMAS WEIGEL

In this appendix we provide additional details on the \exp - \log correspondence between the category \mathfrak{G}_{ppc} of finitely generated powerful p -central pro- p groups and the category \mathfrak{L}_{ppc} of powerful p -central \mathbb{Z}_p -Lie algebras of finite rank. Our main goal is to give a proof of Theorem 3.3 for the pair $(\mathfrak{L}_{ppc}, \mathfrak{G}_{ppc})$. The proof given here is based almost entirely on the results and ideas from [Weig], but the order of exposition and some of our terminology is quite different.

For the rest of this section we fix a prime $p \geq 5$ and let $\mathfrak{G} = \mathfrak{G}_{ppc}$ and $\mathfrak{L} = \mathfrak{L}_{ppc}$.

Recall that according to our convention in § 3, the functors $\exp : \mathfrak{L} \rightarrow \mathfrak{G}$ and $\log : \mathfrak{G} \rightarrow \mathfrak{L}$ act as identity on the underlying sets, that is, $\exp(L) = L$ as sets for any $L \in \text{Ob}(\mathfrak{L})$ and $\log(G) = G$ as sets for any $G \in \text{Ob}(\mathfrak{G})$. Such a definition may lead to confusion between group and Lie algebra operations defined on the same sets, most importantly, the group commutator and the Lie bracket both of which are denoted by $[\cdot, \cdot]$. To avoid such problems we will slightly change the definitions here and assume that as a set $\exp(L)$ is the set of formal symbols $\{\exp(x) : x \in L\}$, and similarly for the \log functor. Of course, this only changes the functors up to equivalence.

Notation: For a set S and $n \in \mathbb{N}$ we will denote by $S^{\times n}$ the direct product of n copies of S . We do not use the standard notation S^n here to avoid confusion with the subgroup generated by n^{th} powers.

A.1. Evaluating Lie power series in powerful p -central \mathbb{Z}_p -Lie algebras. Let $X = \{x_1, \dots, x_d\}$ be a finite set. Let $\mathbb{Q}_p\langle X \rangle$ (resp. $\mathbb{Q}_p\langle\langle X \rangle\rangle$) be the associative \mathbb{Q}_p -algebra of polynomials (resp. power series) in non-commuting variables x_1, \dots, x_d . Let $A(X)$ (resp. $\mathcal{A}(X)$) be the subalgebras of $\mathbb{Q}_p\langle x_1, \dots, x_d \rangle$ (resp. $\mathbb{Q}_p\langle\langle x_1, \dots, x_d \rangle\rangle$) consisting of polynomials (resp. power series) with zero constant term. For each $n \in \mathbb{N}$ let $\mathcal{A}^{(n)}(X)$ be the set of all power series in $\mathcal{A}(X)$ which have no terms of degree $< n$. By the *degree topology* on $\mathcal{A}(X)$ we will mean the unique translation-invariant topology such that $\{\mathcal{A}^{(n)}(X)\}$ is a base of neighborhoods of 0.

Let $L(X)$ be the \mathbb{Q}_p -Lie subalgebra of $A(X)$ generated by X , and let $\mathcal{L}(X)$ be the \mathbb{Q}_p -Lie subalgebra of $\mathcal{A}(X)$ consisting of power series all of whose homogeneous components lie in $L(X)$. Thus, $\mathcal{A}(X) \cap \mathbb{Q}_p\langle X \rangle = A(X)$, $\mathcal{L}(X) \cap \mathbb{Q}_p\langle X \rangle = L(X)$, and $A(X)$ (resp. $L(X)$) is dense in $\mathcal{A}(X)$ (resp. $\mathcal{L}(X)$) in the degree topology. It is well known that $L(X)$ is a free \mathbb{Q}_p -Lie algebra on X .

The following terminology is non-standard, but very convenient for our purposes:

Definition.

- A *monic X -commutator of weight 1* is just an element of X .
- For an integer $k \geq 2$, we define *monic X -commutators of weight k* inductively as formal expressions $[c, d]$ where c and d are monic X -commutators of weight $< k$ with $wt(c) + wt(d) = k$.
- An *X -commutator of weight k* is a formal expression λc where c is a monic X -commutator of weight k and $\lambda \in \mathbb{Q}_p$. We define the *p -adic valuation $\nu_p(\lambda c)$* to be the p -adic valuation of λ , that is, the unique $k \in \mathbb{Z}$ such that $\lambda \in p^k \mathbb{Z}_p \setminus p^{k+1} \mathbb{Z}_p$.

We will usually think of X -commutators as elements of $\mathcal{L}(X)$; however there are two advantages of defining them as formal expressions. First, we will sometimes need to distinguish between distinct commutators which represent the same element of $\mathcal{L}(X)$ (e.g. $[[x_1, x_2], x_3]$ and $[x_3, [x_2, x_1]]$); second we will occasionally need to consider X -commutators as elements of the algebras of polynomials or power series over other coefficient rings.

We will now introduce an important class of \mathbb{Z}_p -Lie subalgebras of $\mathcal{L} = \mathcal{L}(X)$. Fix a function $\gamma : \mathbb{N} \rightarrow \mathbb{Z}_{\geq 0}$.

Definition.

- (a) A commutator w of weight k will be called *γ -integral* if $\nu_p(w) \geq \gamma(k)$. In other words, γ -integral commutators of weight k are precisely elements of the form $\frac{\lambda}{p^{\gamma(k)}}c$ where c is a monic X -commutator of weight k and $\lambda \in \mathbb{Z}_p$.
- (b) We define $\mathcal{L}_\gamma^{full} = \mathcal{L}_\gamma^{full}(X)$ to be the \mathbb{Z}_p -subspace of $\mathcal{L}(X)$ consisting of all infinite sums of γ -integral commutators which converge in the degree topology. In other words, $w \in \mathcal{L}_\gamma^{full}$ if and only if w can be written as $\sum_{i=1}^{\infty} w_i$ where each w_i is a γ -integral X -commutator and $wt(w_i) \rightarrow \infty$ as $i \rightarrow \infty$.
- (c) An element of $\mathcal{L}_\gamma^{full}$ will be called *γ -integral* if it can be written as $\sum_{i=1}^{\infty} \lambda_i w_i$ where each w_i is a γ -integral X -commutator, $wt(w_i) \rightarrow \infty$ as $i \rightarrow \infty$, each $\lambda_i \in \mathbb{Z}_p$ and $\lambda_i \rightarrow 0$ in \mathbb{Z}_p . The set of all γ -integral elements (which is a clearly a \mathbb{Z}_p -submodule) will be denoted by $\mathcal{L}_\gamma = \mathcal{L}_\gamma(X)$.

In general neither $\mathcal{L}_\gamma^{full}$ nor \mathcal{L}_γ is a subalgebra of $\mathcal{L}(X)$. It is easy to see that $\mathcal{L}_\gamma^{full}$ is a subalgebra if and only if \mathcal{L}_γ is a subalgebra if and only if γ is super-additive, that is, $\gamma(i + j) \geq \gamma(i) + \gamma(j)$ for all $i, j \in \mathbb{N}$. We will be interested in a slightly more restrictive condition on γ which guarantees that $\mathcal{L}_\gamma^{full}$ and \mathcal{L}_γ are also *substitution-closed*.

Definition. A subset S of \mathcal{L} will be called *substitution-closed* if for any $f, f_1, \dots, f_d \in S$ (recall that $d = |X|$) the element $f(f_1, \dots, f_d)$ also lies in S . Here $f(f_1, \dots, f_d)$ is defined to be the image of f under the unique continuous \mathbb{Q}_p -Lie algebra endomorphism of \mathcal{L} which sends x_i to f_i for all i .

The following result can be proved by direct verification.

Lemma A.1. *The following are equivalent:*

- (i) $\gamma(i_1 + \dots + i_k) \geq \gamma(i_1) + \dots + \gamma(i_k) + \gamma(k)$ for any finite sequence $i_1, \dots, i_k \in \mathbb{N}$
- (ii) $\mathcal{L}_\gamma^{full}$ is a substitution-closed subalgebra of \mathcal{L}
- (iii) \mathcal{L}_γ is a substitution-closed subalgebra of \mathcal{L}

Now let $m \in \mathbb{N}$ and define the function $\gamma_m : \mathbb{N} \rightarrow \mathbb{Z}_{\geq 0}$ by $\gamma_m(k) = \max\{0, k - m\}$. We define

$$\mathcal{L}_m^{full}(X) = \mathcal{L}_{\gamma_m}^{full}(X) \text{ and } \mathcal{L}_m(X) = \mathcal{L}_{\gamma_m}(X)$$

It is straightforward to check that γ_m satisfies condition (i) of Lemma A.1, so $\mathcal{L}_m^{full}(X)$ and $\mathcal{L}_m(X)$ are both substitution-closed subalgebras.

We will refer to elements of $\mathcal{L}_m(X)$ as *m-integral*. In particular, if c is a monic X -commutator of weight k and $\lambda \in \mathbb{Z}_p$, then λc is m -integral if and only if $k \leq m$ and $\lambda \in \mathbb{Z}_p$ or $k > m$ and $p^{k-m}\lambda \in \mathbb{Z}_p$.

We also let $\mathcal{L}_\infty(X) = \bigcap_{m=1}^{\infty} \mathcal{L}_m(X)$. It is easy to see that $\mathcal{L}_\infty(X) = \mathcal{L}(X) \cap \mathbb{Z}_p\langle\langle X \rangle\rangle$, that is, $\mathcal{L}_\infty(X)$ consists of all elements $w \in \mathcal{L}(X)$ such that all coefficients of w (considered as a power series in X) lie in \mathbb{Z}_p . We will refer to elements of $\mathcal{L}_\infty(X)$ as *integral*.

Topologies on \mathcal{L}_γ . Note that \mathcal{L}_γ is never complete with respect to the degree topology. However, \mathcal{L}_γ is complete with respect to the *p-adic topology* where the sets $\{p^n \mathcal{L}_\gamma\}_{n=1}^{\infty}$ form a base of neighborhoods of 0. All continuity statements involving \mathcal{L}_γ will be made with respect to the *p-adic topology* unless mentioned otherwise. It is clear that for any $m \leq n$, the topology on $\mathcal{L}_m(X)$ induced from the *p-adic topology* on $\mathcal{L}_n(X)$ coincides with the *p-adic topology* on $\mathcal{L}_m(X)$.

We now turn to the central problem of this subsection. Given an element $w \in \mathcal{L}(X)$ and a Lie algebra $L \in \text{Ob}(\mathfrak{L})$, we want to define a function $w_L : L^{\times d} \rightarrow L$ such that $w_L(u_1, \dots, u_d)$ can be reasonably interpreted as the value of w under the substitution $x_i \mapsto u_i$ for $1 \leq i \leq d$.

Case 1: As a warm-up, let us start with the case where $w \in \mathcal{L}_\infty$, that is, w is integral. In this case we can proceed in an obvious way. Indeed, since L is powerful, it is clear that for any d -tuple $\mathbf{u} = (u_1, \dots, u_d)$, there exists a unique continuous homomorphism $\varphi_{\mathbf{u}} : \mathcal{L}_\infty \rightarrow L$ which sends x_i to u_i for each i . We define $w_L(\mathbf{u}) = \varphi_{\mathbf{u}}(w)$.

Case 2: Next consider the case where w is a 1-integral X -commutator. In this case we define w_L using certain choices in L , but such that the value of w_L modulo Ω does not depend on these choices where $\Omega = \{z \in L : pz = 0\}$ (recall that $\Omega \subseteq Z(L)$)

since L is p -central). Here and throughout the appendix, given an element $v \in pL$, by $\frac{1}{p}v$ we will denote any element $v' \in L$ satisfying $pv' = v$.

We proceed by induction on the weight of w . If $wt(w) = 1$, then w is integral, and w_L is already defined (no choices needed here). Now fix $k \geq 2$ and a 1-integral X -commutator w of weight k , and assume we already defined v_L for any 1-integral X -commutator v of weight k such that v_L is choice-independent modulo Ω .

Since w is 1-integral, by definition $w = \frac{\lambda}{p^{k-1}}[y, z]$ where y and z are monic X -commutators of weights i and j with $i + j = k$ and $\lambda \in \mathbb{Z}_p$. Note that $\frac{1}{p^{i-1}}y$ and $\frac{1}{p^{j-1}}z$ are 1-integral, so we can define $w_L(\mathbf{u}) = \lambda \cdot \frac{1}{p}[\frac{1}{p^{i-1}}y(\mathbf{u}), \frac{1}{p^{j-1}}z(\mathbf{u})]$. Since L is p -central and powerful and the values $\frac{1}{p^{i-1}}y(\mathbf{u})$ and $\frac{1}{p^{j-1}}z(\mathbf{u})$ are well-defined modulo Ω , the element $v = [\frac{1}{p^{i-1}}y(\mathbf{u}), \frac{1}{p^{j-1}}z(\mathbf{u})]$ lies in pL and does not depend on any choices. Thus, $w_L(\mathbf{u}) = \lambda(\frac{1}{p}v)$ is well defined modulo Ω , as desired.

Case 3: Next assume that w is a 2-integral X -commutator. In this case the scalar λ in the previous paragraph must lie in $p\mathbb{Z}_p$, and therefore the function w_L we just defined does not involve any choices in L .

We can now define $w_L : L^{\times d} \rightarrow L$ for any $w \in \mathcal{L}_2(X)$ as follows: write $w = \sum_{i=1}^{\infty} \lambda_i w_i$ where w_i is a 2-integral X -commutator and $\lambda_i \rightarrow 0$ in \mathbb{Z}_p and define

$$(A.1) \quad w_L(\mathbf{u}) = \sum_{i=1}^{\infty} (\lambda_i w_i)_L(\mathbf{u}).$$

The series on the right of (A.1) converges since L has finite rank and $\lambda_i \rightarrow 0$ in \mathbb{Z}_p .

The obtained function w_L does not involve any choices in L , but it may depend on the expansion of w as a sum $\sum_{i=1}^{\infty} \lambda_i w_i$. As we will see shortly (see Corollary A.3 below), this issue will not arise if we assume that $w \in \mathcal{L}_3(X)$. The following is the key result in this subsection:

Theorem A.2. *Let $X = \{x_1, \dots, x_d\}$ for some $d \in \mathbb{N}$. Let $L \in \text{Ob}(\mathfrak{L})$ or $L = \mathcal{L}_3(X)$ and $\mathbf{u} = (u_1, \dots, u_d)$ any d -tuple in L . Then there exists a unique continuous Lie algebra homomorphism $f = f_{\mathbf{u}} : \mathcal{L}_3(X) \rightarrow L$ such that $f(c) = c_L(\mathbf{u})$ for every 3-integral commutator c . In particular, $f(x_i) = u_i$ for all $1 \leq i \leq d$.*

The uniqueness of f is clear since by definition 3-integral commutators form a dense subset of $\mathcal{L}_3(X)$. If $L = \mathcal{L}_3(X)$, the existence is also immediate – we just start with the substitution homomorphism $\tilde{f} : \mathcal{L}(X) \rightarrow \mathcal{L}(X)$ given by $\tilde{f}(v(x_1, \dots, x_d)) = v(u_1, \dots, u_d)$ (recall that $\mathcal{L}(X)$ is a \mathbb{Q}_p -Lie algebra, so \tilde{f} is clearly well-defined) and let f be the restriction of \tilde{f} to $\mathcal{L}_3(X)$. Since $\mathcal{L}_3(X)$ is substitution closed, we have $f(\mathcal{L}_3(X)) \subseteq \mathcal{L}_3(X)$.

The proof of the existence part of Theorem A.2 for $L \in \text{Ob}(\mathfrak{L})$ is fairly long and will be postponed till the last subsection of this Appendix.

Corollary A.3. *Let $w \in \mathcal{L}_3(X)$ and write $w = \sum_{i=1}^{\infty} \lambda_i w_i$ where each w_i is a 3-integral commutator and $\lambda_i \rightarrow 0$ as $i \rightarrow \infty$. Then for any $L \in \text{Ob}(\mathfrak{L})$, the function*

w_L defined by (A.1) (relative to the chosen expansion) depends only on w and not on the expansion $\sum \lambda_i w_i$.

Proof. Let $\mathbf{u} = (u_1, \dots, u_d)$ be any d -tuple in L , and let $f = f_{\mathbf{u}} : \mathcal{L}_3 \rightarrow L$ be the homomorphism from Theorem A.2. Then $w_L(\mathbf{u}) = \sum_{i=1}^{\infty} (\lambda_i w_i)_L(\mathbf{u}) = \sum_{i=1}^{\infty} f(\lambda_i w_i) = f(\sum_{i=1}^{\infty} \lambda_i w_i) = f(w)$, so w_L is determined entirely by w . \square

Note that a continuous homomorphism $f : \mathcal{L}_3(X) \rightarrow L$ need not be uniquely determined by its values on X since the \mathbb{Z}_p -Lie subalgebra generated by X is not dense in $\mathcal{L}_3(X)$. Nevertheless we will prove the following:

Proposition A.4. *Let $L \in \text{Ob}(\mathfrak{L})$ or $L = \mathcal{L}_3(X)$, let $\mathbf{u} = (u_1, \dots, u_d)$ be a d -tuple in L , and let $f : \mathcal{L}_3(X) \rightarrow L$ be a continuous Lie algebra homomorphism such that $f(x_i) = u_i$ for all i . Then $f(w) = w_L(\mathbf{u})$ for any $w \in \mathcal{L}_4(X)$. In particular, the restriction of f to $\mathcal{L}_4(X)$ is completely determined by \mathbf{u} .*

Proof. Let C be the set of elements of the form $\frac{1}{p^{\max\{k-4, 0\}}}c$ where c is a monic left-normed X -commutator of length k . Since every monic X -commutator is a \mathbb{Z} -linear combination of monic left-normed commutators of the same weight, the \mathbb{Z}_p -submodule generated by C is dense in $\mathcal{L}_4(X)$. Thus, it suffices to prove that $f(z) = f_{\mathbf{u}}(z)$ for every $z \in C$ (where $f_{\mathbf{u}}$ is the homomorphism from Theorem A.2).

We argue by induction on $k = wt(c)$. If $k \leq 4$, the result follows directly from the assumption that f is a Lie algebra homomorphism.

Let us assume that $k \geq 5$ and take any $z \in C$ with $wt(z) = k$. Then $z = \frac{1}{p^{k-4}}[y_1, \dots, y_k]$ where each $y_i = x_{n_i}$ for some $n_i \in \{1, \dots, d\}$.

Let $w = \frac{1}{p^{k-4}}[y_1, \dots, y_{k-1}]$, so that $z = [w, y_k]$. Clearly, $w \in \mathcal{L}_3$, so

$$f(z) = [f(w), f(y_k)] = [\frac{1}{p}f(pw), f(y_k)] = [\frac{1}{p}f(pw), f_{\mathbf{u}}(y_k)]$$

Note that $pw \in C$ and $wt(pw) = k - 1$, so by the induction hypothesis $f(pw) = f_{\mathbf{u}}(pw)$. Hence $f(z) = [\frac{1}{p}f_{\mathbf{u}}(pw), f_{\mathbf{u}}(y_k)] = [f_{\mathbf{u}}(w), f_{\mathbf{u}}(y_k)] = f_{\mathbf{u}}([w, y_k]) = f_{\mathbf{u}}(z)$. \square

Corollary A.5. *Let $X = \{x_1, \dots, x_d\}$ for some d . Assume that $L \in \text{Ob}(\mathfrak{L})$ or $L = \mathcal{L}_3(X)$, let $M \in \text{Ob}(\mathfrak{L})$, $\varphi : L \rightarrow M$ be a continuous \mathbb{Z}_p -Lie algebra homomorphism and $w \in \mathcal{L}_4(X)$. Then φ commutes with w , that is, $\varphi(w_L(u_1, \dots, u_d)) = w_M(\varphi(u_1), \dots, \varphi(u_d))$ for any d -tuple $\mathbf{u} = (u_1, \dots, u_d)$ in L .*

Proof. Choose any continuous Lie algebra homomorphism $f : \mathcal{L}_3(X) \rightarrow L$ such that $f(x_i) = u_i$ for $1 \leq i \leq d$ (such f exists by Theorem A.2). Applying Proposition A.4 to the maps $f : \mathcal{L}_3(X) \rightarrow L$ and $\varphi \circ f : \mathcal{L}_3(X) \rightarrow M$, we get that $\varphi(w_L(u_1, \dots, u_d)) = \varphi(f(w)) = w_M(\varphi \circ f(x_1), \dots, \varphi \circ f(x_d)) = w_M(\varphi(u_1), \dots, \varphi(u_d))$, as desired. \square

A.2. The exp functor. Let $X = \{x_1, x_2\}$. Recall from Theorem 3.2 that the Baker-Campbell-Hausdorff (BCH) series $\Phi \in \mathcal{L}(X)$ can be written as $\Phi = \sum_c \lambda_c c$ where c ranges over all left-normed monic X -commutators and for any such c we

have $p^{\delta(wt(c))}\lambda_c \in \mathbb{Z}_p$ where $\delta(k) = \lfloor \frac{k-1}{p-1} \rfloor$ for $k \in \mathbb{N}$. Note that $\delta(k) \leq \gamma_{p-1}(k) = \max\{0, k - (p-1)\}$ and $\lim_{k \rightarrow \infty} \gamma(k) - \delta(k) = \infty$. Hence by definition $\Phi \in \mathcal{L}_{p-1}(X)$ and in particular $\Phi \in \mathcal{L}_4(X)$ for $p \geq 5$.

Let us now take any $L \in \text{Ob}(\mathfrak{L})$. By Corollary A.3, Φ defines a function from $L^{\times 2}$ to L which does not involve any choices in L and does not depend on representation of Φ as a convergent sum of 3-integral commutators. For simplicity of notation this function will also be denoted by Φ rather than Φ_L .

We already defined the group $\exp(L)$ in § 3. Recall (with our new convention) that $\exp(L) = \{\exp(u) : u \in L\}$, and the group operation on $\exp(L)$ is defined by

$$\exp(u) \cdot \exp(v) = \exp \Phi(u, v).$$

Define the topology on $\exp(L)$ simply by transferring the topology from L via the map $u \mapsto \exp(u)$. It is straightforward to check that $\exp(L)$ is a topological group.

Also recall that for any morphism $\varphi : L \rightarrow M$ in \mathfrak{L} , the corresponding morphism $\exp(\varphi) : \exp(L) \rightarrow \exp(M)$ is given by $(\exp(\varphi))(\exp(u)) = \exp(\varphi(u))$.

We need to prove the following:

Proposition A.6.

- (1) *The operation \cdot satisfies the group axioms.*
- (2) *If $L, M \in \text{Ob}(\mathfrak{L})$ and $\varphi : L \rightarrow M$ is a homomorphism of \mathbb{Z}_p -Lie algebras, then $\exp(\varphi) : \exp(L) \rightarrow \exp(M)$ is a group homomorphism.*
- (3) *For any $L \in \text{Ob}(\mathfrak{L})$ the group $\exp(L)$ is an object of \mathfrak{G} , that is, $\exp(L)$ is a finitely generated powerful p -central pro- p group.*

Proof. We start by observing that $\exp(0)$ is clearly the identity element with respect to \cdot and $\exp(u + v) = \exp(u)\exp(v)$ whenever u and v commute; in particular, $\exp(nu) = \exp(u)^n$ for all $n \in \mathbb{Z}$. Also since the BCH series Φ is 4-integral, (2) follows directly from Corollary A.5 (applied with $w = \Phi$).

(1) Let us now prove that \cdot is associative. First recall that for any $a, b \in \mathcal{L}(X)$ we have

$$\text{Exp}(a) \cdot \text{Exp}(b) = \text{Exp}(\Phi(a, b))$$

where $\text{Exp}(a) = 1 + a + \frac{a^2}{2} + \dots$ and the product on the left-hand side is taken in $\mathcal{A}(X)$. Since multiplication in $\mathcal{A}(X)$ is associative, for any $a, b, c \in \mathcal{L}(X)$ we have the equality $\Phi(a, \Phi(b, c)) = \Phi(\Phi(a, b), c)$.

Now take any $u_1, u_2, u_3 \in L$ and set $X = \{x_1, x_2, x_3\}$. By Theorem A.2 there exists a continuous Lie algebra homomorphism $f : \mathcal{L}_3(X) \rightarrow L$ such that $f(x_i) = u_i$ for $1 \leq i \leq 3$. By Corollary A.5 applied to $w = \Phi$ and $\varphi = f$ we have $f(\Phi(a, b)) = \Phi(f(a), f(b))$ for all $a, b \in \mathcal{L}_3(X)$.

Hence

$$\begin{aligned} (u_1 \cdot u_2) \cdot u_3 &= \Phi(\Phi(u_1, u_2), u_3) = \Phi(\Phi(f(x_1), f(x_2)), f(x_3)) \\ &= \Phi(f(\Phi(x_1, x_2)), f(x_3)) = f(\Phi(\Phi(x_1, x_2), x_3)). \end{aligned}$$

Similarly $u_1 \cdot (u_2 \cdot u_3) = f(\Phi(x_1, \Phi(x_2, x_3)))$. Since $\Phi(\Phi(x_1, x_2), x_3) = \Phi(x_1, \Phi(x_2, x_3))$, we proved that $(u_1 \cdot u_2) \cdot u_3 = u_1 \cdot (u_2 \cdot u_3)$, as desired.

(3) Finally, let us prove that $\exp(L)$ is an object of \mathfrak{G} . First, the sets $\{p^n L\}_{n=1}^\infty$ form a base of neighborhoods of 0 for the topology on L . It is straightforward to check that each $\exp(p^n L)$ is a normal subgroup of p -power index in $G = \exp(L)$. Thus, G (considered with the same topology as L) is a topological group which has a base of neighborhoods consisting of normal subgroups of p -power index, so by definition G is a pro- p group.

Next observe that for any $u, v \in L$ we have $[\exp(u), \exp(v)] = \exp \Psi(u, v)$ where $\Psi \in \mathcal{L}(\{x_1, x_2\})$ is the series defined by

$$\Psi = \Phi(-x_1, \Phi(-x_2, \Phi(x_1, x_2))).$$

Since Φ is $(p-1)$ -integral and \mathcal{L}_{p-1} is substitution-closed, Ψ is also $(p-1)$ -integral. Also, by a simple direct computation Ψ has no linear terms (the leading term of Ψ is $[x_1, x_2]$). Hence $\Psi(u, v)$ is equal to a convergent sum $\sum_{i=1}^\infty h_i$ where each $h_i = [a_i, b_i]$ for some $a_i, b_i \in L$. Since L is powerful, $[a_i, b_i] = pc_i$ for some $c_i \in L$; moreover, we can assume that the sequence $\{c_i\}$ is also convergent. Thus, if we let $c = \sum_{i=1}^\infty c_i$, then $\Psi(u, v) = pc$ whence $[\exp(u), \exp(v)] = \exp pc = (\exp c)^p \in G^p$. Thus, we proved that G is powerful.

Next we prove that G is a finitely generated. It is well known that for a pro- p group G the minimal number of generators is equal to $\dim_{\mathbb{F}_p} G/[G, G]G^p$. We already proved that $[G, G]G^p = G^p$ and $G^p = \exp(pL)$. Moreover, it is easy to see that \exp maps additive cosets of pL to multiplicative cosets of G^p . Thus, $|G/[G, G]G^p| = |L/pL|$, and $|L/pL|$ is finite since L is finitely generated as \mathbb{Z}_p -module (in fact, since L is powerful, its minimal number of generators is equal to $\dim_{\mathbb{F}_p} L/pL$, so we actually proved that G and L have the same minimal number of generators).

It remains to prove that G is p -central. Suppose that $\exp(u) \in G$ is an element of order p . Since $\exp(u)^p = \exp(pu)$, it follows that $pu = 0$. Since L is p -central, $u \in Z(L)$. It is clear from definitions that $\Phi(u, v) = u + v = \Phi(v, u)$ for any $v \in L$, so $\exp(u) \in Z(G)$. Thus, we proved that G is p -central. \square

A.3. The log functor. The functor $\log : \mathfrak{G} \rightarrow \mathfrak{L}$ will be defined quite similarly to \exp , although both its definition and justification of its basic properties involve extra technicalities.

First we claim that for any integer $1 \leq m \leq p-1$, the set $\mathcal{G}_m(X) = \text{Exp}(\mathcal{L}_m(X))$ is a group (with respect to the usual multiplication on $\mathcal{A}(X)$). Indeed, for any $y, z \in \mathcal{L}_m(X)$ we have $\text{Exp}(y) \cdot \text{Exp}(z) = \text{Exp}(\Phi(y, z))$ (by Theorem 3.2) and $\Phi(y, z) \in \mathcal{L}_m(X)$ since Φ is $(p-1)$ -integral (and hence m -integral) and $\mathcal{L}_m(X)$ is substitution-closed.

We define the topology on $\mathcal{G}_m(X)$ by transferring the topology from $\mathcal{L}_m(X)$ via the map $u \mapsto \text{Exp}(u)$. It is easy to check that the subgroups $\{\mathcal{G}_m(X)^{p^n}\}_{n \in \mathbb{N}}$ form a base of neighborhoods of 1 for this topology.

It is also easy to show that the group $\mathcal{G}_1(X)$ is powerful – this can be verified directly or deduced from the fact that the Lie algebra $\mathcal{L}_1(X)$ is powerful (the latter is immediate from the definition). Similarly to the Lie algebra case, the group $\mathcal{G}_3(X)$ will play the role of a free-like object for the category \mathfrak{G} .

Recall that in the Lie algebra case we showed that every element $w \in \mathcal{L}_3(X)$ naturally defines a function $w_L : L^{\times d} \rightarrow L$ (where $d = |X|$) for every $L \in \text{Ob}(\mathfrak{L})$. In the group case we will take a slightly different approach. Instead of turning elements of $\mathcal{G}_3(X)$ into functions, we introduce certain formal expressions $\{H_c\}$ and $\{R_c\}$ (see the definitions below) which can be interpreted as functions $G^{\times d} \rightarrow G$ for all $G \in \text{Ob}(\mathfrak{G})$ as well as for $G = \mathcal{G}_m(X)$ for certain m . This approach will lead to a more ad hoc, but also more intuitive, definition of the *log* functor.

Consider a new set of formal variables $\{t_k\}_{k=1}^{\infty}$. For each monic X -commutator c we define the expression H_c as follows:

- If $wt(c) = 1$, so $c = x_i$ for some i , we let $H_c = t_i$.
- If $wt(c) = k > 1$, so $c = [d, e]$ for some monic X -commutators d and e with $wt(d) + wt(e) = k$, we define H_c inductively as $H_c = \sqrt[p]{[H_d, H_e]}$.

For instance, if $c = [x_1, [x_2, x_3]]$, then $H_c = \sqrt[p]{t_1, \sqrt[p]{[t_2, t_3]}}$. One should think of H_c as a multiplicative analogue of the 1-integral commutator $\frac{1}{p^{wt(c)-1}}c$.

Now assume that c is a monic *left-normed* X -commutator. Define the expression $\{R_c\}$ as follows:

- If $wt(c) \leq 4$, so $c = [x_{i_1}, \dots, x_{i_k}]$ for some $1 \leq k \leq 4$, let $R_c = [t_{i_1}, \dots, t_{i_k}]$.
- If $wt(c) = k \geq 5$ and $c = [d, x_j]$ (where d is a monic left-normed X -commutator of weight $k-1$), we let $R_c = [\sqrt[p]{R_d}, t_j]$.

For instance, if $c = [x_1, x_2, x_3, x_4, x_5]$, then $R_c = [\sqrt[p]{[t_1, t_2, t_3, t_4]}, t_5]$. One should think of R_c as a multiplicative analogue of the 4-integral commutator $\frac{1}{p^{\max\{wt(c)-4, 0\}}}c$.

The expressions $\{R_c\}$ will be called *root-commutators* (this name is equally applicable to the elements $\{H_c\}$, and our choice is dictated by the fact that we will work with R_c more frequently).

Similarly to the Lie algebra case, the expressions H_c and R_c naturally define functions $G^{\times d} \rightarrow G$ for certain groups G . We claim the following:

- (i) If $G \in \text{Ob}(\mathfrak{G})$, each H_c defines a function whose values are well-defined modulo $\Omega = \{g \in G : g^p = 1\}$ (recall that $\Omega \subseteq Z(G)$ since G is p -central), and each R_c defines a function not involving any choices.
- (ii) If $G = \mathcal{G}_1(X)$, then G is powerful and torsion-free, so each H_c and R_c becomes a well-defined function on G . Moreover for each $1 \leq m \leq p-1$, the subgroup $\mathcal{G}_m(X)$ of G is invariant under these functions.

To justify (i) we need the following results which will be discussed below in § A.5:

- (a) (see Lemma A.12(b)(i)) Let G be a finitely generated powerful pro- p group. Then every element of G^p is equal to g^p for some $g \in G$.
- (b) (see Lemma A.16) Let $G \in \text{Ob}(\mathfrak{G})$. If $x^p = y^p$ for some $x, y \in G$, then $(x^{-1}y)^p = 1$.

Property (ii) can be established by a straightforward computation. We will need a slightly stronger version of (ii) in the special case $m = 3$:

Lemma A.7. *Let c be a monic X -commutator of weight ≥ 2 and $g_1, \dots, g_m \in \mathcal{G}_3(X)$. Then $R_c(g_1, \dots, g_m) \in \mathcal{G}_4(X)$.*

Remark: Note that $p^{\min\{3, wt(c)-1\}} \cdot \frac{1}{p^{wt(c)-1}} c = \frac{1}{p^{\max\{wt(c)-4, 0\}}} c$, so one should expect the elements $R_c(\text{Exp}(x_1), \dots, \text{Exp}(x_d))$ and $H_c^{p^{\min\{3, wt(c)-1\}}}(\text{Exp}(x_1), \dots, \text{Exp}(x_d))$ of $\mathcal{G}_3(X)$ to be related. If $wt(c) \geq 3$, these elements are distinct but have the same leading term.

Proof. We argue by induction on $k = wt(c)$. As before, define the series $\Psi \in \mathcal{L}(\{x_1, x_2\})$ by $\Psi = \Phi(-x_1, \Phi(-x_2, \Phi(x_1, x_2)))$. In the base case $k = 2$, Lemma A.7 is equivalent to the assertion

$$(A.2) \quad \Psi(u, v) \in \mathcal{L}_4(X) \text{ for all } u, v \in \mathcal{L}_3(X).$$

which can be verified by direct computation.

Let us proceed with the induction step. Suppose that $k = wt(c) > 2$, and write $c = [d, x_j]$ where $wt(d) = k - 1$. Below we will give an argument for $k \geq 5$ (the cases $k = 3, 4$ are similar and easier). By definition of R_c we have

$$(A.3) \quad R_c(g_1, \dots, g_m) = [\sqrt[p]{R_d(g_1, \dots, g_m)}, g_j]$$

By assumption $g_j = \text{Exp}(v_j)$ for some $v_j \in \mathcal{L}_3(X)$, and by the induction hypothesis $R_d(g_1, \dots, g_m) = \text{Exp}(u)$ for some $u \in \mathcal{L}_4(X)$. Also it is clear that u has no terms of degree $\leq wt(d) = k - 1$. Since $k - 1 \geq 4$ and $u \in \mathcal{L}_4(X)$, we have $\frac{1}{p}u \in \mathcal{L}_3(X)$ and therefore $\Psi(\frac{1}{p}u, v_j) \in \mathcal{L}_4(X)$ by (A.2).

On the other hand, from (A.3) we get $R_c(g_1, \dots, g_m) = \text{Exp}(\Psi(\frac{1}{p}u, v_j))$, and thus $R_c(g_1, \dots, g_m) \in \mathcal{G}_4(X)$, as desired. \square

Our next result (Proposition A.8) asserts that the addition and the Lie bracket on $\mathcal{L}_3(X)$ can be expressed as convergent products of integer powers of the root-commutators $\{R_c\}$ in $\mathcal{G}_3(X)$. This result, which should be thought of as a formal inversion of the Baker-Campbell-Hausdoff formula, is well known, but we are not aware of a reference where it is stated exactly in this form.

Let $X = \{x_1, x_2\}$. For each $n \in \mathbb{N}$ let C_n be the set of all left-normed monic X -commutators of weight n .

Proposition A.8. *There exist formal expressions $\{a_n\}_{n=2}^\infty$ and $\{b_n\}_{n=3}^\infty$ in the variables $\{t_1, t_2\}$ and an integer sequence $\{\delta_n\}$ with $\delta_n \rightarrow \infty$ satisfying the following conditions:*

(a) Each $a_n = \prod_{c \in C_n} R_c^{\lambda_c p^{\delta_n}}$ for some $\lambda_c \in \mathbb{Z}_p$.

(b) $\text{Exp}(x_1 + x_2) = \text{Exp}(x_1)\text{Exp}(x_2)S_A(x_1, x_2)$ where

$$S_A(x_1, x_2) = \prod_{n=2}^{\infty} a_n(\text{Exp}(x_1), \text{Exp}(x_2))$$

(c) Each $b_n = \prod_{c \in C_n} R_c^{\mu_c p^{\delta_n}}$ for some $\mu_c \in \mathbb{Z}_p$.

(d) $\text{Exp}([x_1, x_2]) = [\text{Exp}(x_1), \text{Exp}(x_2)]S_B(x_1, x_2)$ where

$$S_B(x_1, x_2) = \prod_{n=3}^{\infty} b_n(\text{Exp}(x_1), \text{Exp}(x_2))$$

Remark: Recall that for each $n \in \mathbb{N}$ and $c \in C_n$, the root-commutator R_c defines a function $G^{\times 2} \rightarrow G$ for any $G \in \text{Ob}(\mathfrak{G})$ and also for $G = \mathcal{G}_1(X)$. Hence each a_n and b_n also naturally defines a function on any of these groups. Also note that since $\delta_n \rightarrow \infty$, the products in (b) and (d) converge in the p -adic topology on $\mathcal{G}_1(X)$.

Proof. We will prove parts (a) and (b) of Proposition A.8 dealing with the addition operation. The proof of (c) and (d) which deal with the Lie bracket is analogous. It will be convenient to prove a slightly stronger and more precise version of Proposition A.8 (which in particular will include a precise formula for δ_n). To state it we need some additional notations.

Define the function $\gamma : \mathbb{N} \rightarrow \mathbb{Z}_{\geq 0}$ by $\gamma(k) = \lfloor \frac{k-1}{p-1} \rfloor$. It is straightforward to check that γ satisfies condition (i) in Lemma A.1, so \mathcal{L}_γ is substitution-closed. Also note that $\Phi \in \mathcal{L}_\gamma$ by Theorem 3.2 and therefore $\mathcal{G}_\gamma = \text{Exp} \mathcal{L}_\gamma$ is a group. For each $n \in \mathbb{N}$ define

$$\delta_n = \gamma_4(n) - \gamma(n) = \max\{0, n - 4\} - \lfloor \frac{n-1}{p-1} \rfloor.$$

Clearly, $\delta_n \geq 0$ and $\delta_n \rightarrow \infty$ as $n \rightarrow \infty$.

We will now prove that there exists a sequence $\{a_n\}_{n=1}^\infty$ with $a_1 = t_1 t_2$ such that

- (i) each a_n satisfies (a) in Proposition A.8 and $a_n(\text{Exp}(x_1), \text{Exp}(x_2))$ lies in $\mathcal{G}_\gamma(X)$
- (ii) for each n the series $\text{Exp}(x_1 + x_2)$ and $\prod_{k=1}^n a_k(\text{Exp}(x_1), \text{Exp}(x_2))$ coincide up to (and including) degree n (and hence (b) in Proposition A.8 holds as well)

We will prove (i) and (ii) by simultaneous induction on n . In the base case $n = 1$ (i) and (ii) obviously hold by definition of a_1 .

Now fix $n \geq 2$ and assume that (i) and (ii) hold for all $m < n$. Then the element $g = \left(\prod_{k=1}^{n-1} a_k(\text{Exp}(x_1), \text{Exp}(x_2)) \right)^{-1} \cdot \text{Exp}(x_1 + x_2)$ has no terms of positive degree $< n$ and lies in $\mathcal{G}_\gamma(X)$. Thus, the degree n term of g has the form $\sum_{c \in C_n} \frac{\lambda_c}{p^{\gamma(n)}} c$ for some $\lambda_c \in \mathbb{Z}_p$.

Now define $a_n = \prod_{c \in C_n} R_c^{\lambda_c p^{\delta_n}}$. Then (a) in Proposition A.8 holds (we will verify the second part of condition (i) later). Let $r_c = R_c(\text{Exp}(x_1), \text{Exp}(x_2))$, so

$$r_c = 1 + \frac{1}{p^{\gamma_4(n)}} c + \text{higher order terms.}$$

Hence the series $\left(\prod_{k=1}^{n-1} a_k(\text{Exp}(x_1), \text{Exp}(x_2)) \right)^{-1} \cdot \text{Exp}(x_1 + x_2)$ and $a_n(\text{Exp}(x_1), \text{Exp}(x_2))$ both have no terms of positive degree $< n$ and the same term of degree n (since $\delta_n - \gamma_4(n) = -\gamma(n)$) and hence $\text{Exp}(x_1 + x_2)$ and $\prod_{k=1}^n a_k(\text{Exp}(x_1), \text{Exp}(x_2))$ coincide up to (and including) degree n , so (ii) holds for n .

It remains to show that $a_n(\text{Exp}(x_1), \text{Exp}(x_2))$ lies in $\mathcal{G}_\gamma(X)$. Note that $r_c = R_c(\text{Exp}(x_1), \text{Exp}(x_2)) \in \mathcal{G}_4(X)$ by Lemma A.7, so $r_c = \text{Exp}(v_c)$ for some $v_c \in$

$\mathcal{L}_4(X)$. Then $r_c^{\lambda_c p^{\delta_n}} = \text{Exp}(\lambda_c p^{\delta_n} v_c)$. For each $m \in \mathbb{N}$ the degree m coefficients of v_c lie in $\frac{1}{p^{\gamma_4(m)}} \mathbb{Z}_p$ and hence the degree m coefficients of $\lambda_c p^{\delta_n} v_c$ lie in $p^{\delta_n - \gamma_4(m)} \mathbb{Z}_p$.

Recall that v_c has no terms of positive degree $< n$. Also it is clear from the definitions of γ_4 and γ that for $n \geq m$ we have $\gamma_4(n) - \gamma_4(m) \geq \gamma(n) - \gamma(m)$ and hence $\delta_n - \gamma_4(m) = \gamma_4(n) - \gamma(n) - \gamma_4(m) \geq -\gamma(m)$. It follows that $\lambda_c p^{\delta_n} v_c \in \mathcal{L}_\gamma(X)$ whence $r_c^{\lambda_c p^{\delta_n}} \in \mathcal{G}_\gamma(X)$ for each $c \in C_n$ and hence $a_n(\text{Exp}(x_1), \text{Exp}(x_2)) \in \mathcal{G}_\gamma(X)$ as well. \square

We can now use Proposition A.8 to define the log functor. Let $G \in \text{Ob}(\mathfrak{G})$, that is, G is a finitely generated powerful p -central pro- p group. We define $L = \log(G)$ to be the set of formal symbols $\{\log(g) : g \in G\}$. Given any $g, h \in G$, we set $S_A(g, h) = \prod_{n=2}^{\infty} a_n(g, h)$ and $S_B(g, h) = \prod_{n=3}^{\infty} b_n(g, h)$ where a_n and b_n come from Proposition A.8, and define

$$(A.4) \quad \log(g) + \log(h) = \log(gh S_A(g, h)) \text{ and } [\log(g), \log(h)] = \log([g, h] S_B(g, h))$$

Also, similarly to \exp , for any morphism $\varphi : G \rightarrow H$ in \mathfrak{G} , the corresponding morphism $\log(\varphi) : \log(G) \rightarrow \log(H)$ is defined by $(\log(\varphi))(\log(g)) = \log(\varphi(g))$.

Remark: The expressions S_A and S_B in Proposition A.8 are not uniquely determined as a_n and b_n are not uniquely determined; however, our definition of \log does not depend on these choices. The latter is not clear at this point and will be established in the next subsection once we prove that the compositions $\exp \circ \log$ and $\log \circ \exp$ are equivalent to the identity functor.

The following theorem is a (weaker) group-theoretic counterpart of Theorem A.2. Its proof is analogous (albeit slightly more technical) and will also be given in the last subsection.

Theorem A.9. *Let $X = \{x_1, \dots, x_d\}$ and $G \in \text{Ob}(\mathfrak{G})$ or $G = \mathcal{G}_3(X)$. For any finite subset $\{g_1, \dots, g_d\}$ of G there exists a continuous group homomorphism $f : \mathcal{G}_3(X) \rightarrow G$ such that $f(\text{Exp}(x_i)) = g_i$ for all i .*

We proceed with the rest of the proof of the Lie algebra axioms for $L = \log(G)$ (where $G \in \text{Ob}(\mathfrak{G})$ is arbitrary). Let $\{g_1, \dots, g_d\}$ be any finite generating set for G , let $X = \{x_1, \dots, x_d\}$, and let $f : \mathcal{G}_3(X) \rightarrow G$ be the homomorphism from Theorem A.9. We claim that f preserves all root-commutators:

Proposition A.10. *Let c be a left-normed monic X -commutator. Then for any $u_1, \dots, u_d \in \mathcal{G}_3(X)$ we have*

$$(A.5) \quad f(R_c(u_1, \dots, u_d)) = R_c(f(u_1), \dots, f(u_d))$$

Proof. This is proved by induction on $wt(c)$ similarly to Proposition A.4. The full power of Lemma A.7 (which we have not used so far) is needed to complete the induction step. \square

Since the functions S_A and S_B are convergent products of root-commutators, we conclude from Proposition A.10 that

$$f(S_A(g, h)) = S_A(f(g), f(h)) \text{ and } f(S_B(g, h)) = S_B(f(g), f(h)) \text{ for all } g, h \in \mathcal{G}_3(X).$$

As in the construction of the exp functor (see the last paragraph in the proof of Proposition A.6(1)), we deduce that L is a Lie ring. Moreover, we can turn L into a \mathbb{Z}_p -Lie algebra by setting $\lambda \log(g) = \log(g^\lambda)$ for $\lambda \in \mathbb{Z}_p$ (the expression g^λ is well defined since G is a pro- p group).

To finish proving that $\log : \mathfrak{L} \rightarrow \mathfrak{G}$ is a functor, we need to check the following:

- (i) Let $G_1, G_2 \in \text{Ob}(\mathfrak{G})$ and let $\varphi : G_1 \rightarrow G_2$ be a group homomorphism. Then $\log(\varphi) : \log(G_1) \rightarrow \log(G_2)$ is a \mathbb{Z}_p -Lie algebra homomorphism.
- (ii) For any $G \in \text{Ob}(\mathfrak{L})$, the Lie algebra $L = \log(G)$ is finitely generated, powerful and p -central.

These are direct analogues of Proposition A.6(2)(3) and are proved by nearly identical arguments.

A.4. Why exp and log are mutually inverse. We have now constructed both functors $\exp : \mathfrak{L} \rightarrow \mathfrak{G}$ and $\log : \mathfrak{G} \rightarrow \mathfrak{L}$, and parts (a)-(f) of Proposition 3.4 (which are stated for \log) and their analogues for \exp clearly hold by construction. Proposition 3.4 also asserts that \exp and \log are mutually inverse, but of course this is based on the convention that $\exp(L) = L$ and $\log(G) = G$ as sets for any $L \in \text{Ob}(\mathfrak{L})$ and $G \in \text{Ob}(\mathfrak{G})$. With the different convention adopted in this appendix, the latter statement translates as follows:

Proposition A.11.

- (1) For any $G \in \text{Ob}(\mathfrak{G})$ the map $G \rightarrow \exp(\log(G))$ given by $g \mapsto \exp(\log(g))$ is a group homomorphism.
- (2) For any $L \in \text{Ob}(\mathfrak{L})$ the map $L \rightarrow \log(\exp(L))$ given by $u \mapsto \log(\exp(u))$ is a Lie algebra homomorphism.

Below we will prove (1). The proof of (2) is similar.

Proof of Proposition A.11(1). Take any $G \in \text{Ob}(\mathfrak{G})$, let $L = \log(G)$ and $G' = \exp(\log(G))$. By Theorem A.9 there exists a finite set X and a continuous surjective homomorphism $f : \mathcal{G}_3(X) \rightarrow G$. Define $f_* : \mathcal{L}_3(X) \rightarrow L$ by

$$\begin{aligned} f_*(u) &= \log f(\text{Exp}(u)) \text{ for } u \in \mathcal{L}_3(X) \text{ or, equivalently,} \\ f_*(\text{Log}(y)) &= \log(f(y)) \text{ for } y \in \mathcal{G}_3(X) \end{aligned}$$

The two expressions for f_* are indeed equivalent since Exp and Log are mutually inverse.

Clearly f_* is continuous. We claim that f_* is a Lie algebra homomorphism. Indeed, take any $u, v \in \mathcal{L}_3(X)$, and let $g = f(\text{Exp}(u))$ and $h = f(\text{Exp}(v))$ (both g and h lie in G). By Proposition A.8(b),

$$\begin{aligned} f_*(u + v) &= \log f(\text{Exp}(u + v)) = \log f(\text{Exp}(u) \cdot \text{Exp}(v) \cdot S_A(\text{Exp}(u), \text{Exp}(v))) \\ &= \log(f(\text{Exp}(u)) \cdot f(\text{Exp}(v)) \cdot f(S_A(\text{Exp}(u), \text{Exp}(v)))) . \end{aligned}$$

By Proposition A.10, f preserves all root commutators and hence commutes with S_A , so the last expression is equal to

$$\log(f(\text{Exp}(u)) \cdot f(\text{Exp}(v)) \cdot S_A(f(\text{Exp}(u)), f(\text{Exp}(v)))) = \log(g \cdot h \cdot S_A(g, h)).$$

By the definition of addition in $L = \log(G)$ (see (A.4)), the obtained expression is equal to $\log(g) + \log(h) = f_*(u) + f_*(v)$, as desired. Similarly one checks that f_* preserves the Lie bracket.

Now define $f' : \mathcal{G}_3(X) \rightarrow G'$ by

$$(A.6) \quad f'(y) = \exp f_*(\text{Log}(y)) = \exp \log f(y).$$

We will prove that f' is a group homomorphism (which is obviously continuous) arguing similarly to the previous paragraph. Take any $y_1, y_2 \in \mathcal{G}_3(X)$, and let $u_i = \text{Log}(y_i) \in \mathcal{L}_3(X)$ for $i = 1, 2$. Note that $y_1 y_2 = \text{Exp}(u_1) \text{Exp}(u_2) = \text{Exp} \Phi(u_1, u_2)$, so $\text{Log}(y_1 y_2) = \Phi(u_1, u_2)$.

Since $f_* : \mathcal{L}_3(X) \rightarrow L$ is a continuous Lie algebra homomorphism, it preserves all the 4-integral commutators by Corollary A.5. In particular, it commutes with Φ , so $f_*(\Phi(u_1, u_2)) = \Phi(f_*(u_1), f_*(u_2))$. Putting everything together we get

$$\begin{aligned} f'(y_1) f'(y_2) &= \exp f_*(\text{Log}(y_1)) \exp f_*(\text{Log}(y_2)) = \exp f_*(u_1) \exp f_*(u_2) \\ &= \exp \Phi(f_*(u_1), f_*(u_2)) = \exp f_*(\Phi(u_1, u_2)) = \exp f_*(\text{Log}(y_1 y_2)) = f'(y_1 y_2). \end{aligned}$$

Denote the map $g \mapsto \exp(\log(g))$ from G to G' by ι . Then $f' = \iota \circ f$. We just proved that f' is a homomorphism. Since f is a surjective homomorphism, it follows that ι is a homomorphism, as desired. \square

A.5. (λ, p) -groups and p -complete Lie algebras. In this subsection we introduce the notions of (λ, p) -groups (called λ -groups in [Weig]) and their Lie-theoretic counterparts called p -complete Lie algebras and state some results about them. These results will be used to prove Theorem A.2 and A.9.

Definition. Let p be a fixed prime and let G be a group.

- (a) The *lower p -series* $\{\lambda_n(G)\}_{n \geq 1}$ of G is defined by $\lambda_1(G) = G$ and $\lambda_n(G) = \lambda_{n-1}(G)^p [\lambda_{n-1}(G), G]$ for $n \geq 2$ (note that the quotients $\lambda_{n-1}(G)/\lambda_n(G)$ are \mathbb{F}_p -vector spaces).
- (b) The *(λ, p) -topology* on G is the unique translation-invariant topology on G in which $\{\lambda_n(G)\}$ is a base of neighborhoods of identity (since $\lambda_n(G)$ are normal, this turns G into a topological group). The completion of G with respect to its (λ, p) -topology will be called the *(λ, p) -completion*.
- (c) G is called a *(λ, p) -group* if G is a complete Hausdorff group with respect to its (λ, p) -topology.

Definition. Let L be a topological \mathbb{Z}_p -Lie algebra. We will say that L is *p -complete* if its additive group $(L, +)$ is a (λ, p) -group.

It is easy to see that any (λ, p) -group G is a \mathbb{Z}_p -powered group (that is, for any $\mu \in \mathbb{Z}_p$ there exists a group homomorphism $g \mapsto g^\mu$ from G to G such that $g^\mu \cdot g^\nu = g^{\mu+\nu}$, $(g^\mu)^\nu = g^{\mu\nu}$ and $g^\mu = \lim g^{\mu_n}$ for any integer sequence $\{\mu_n\}$ such that $\mu_n \rightarrow \mu$ in \mathbb{Z}_p).

It is not hard to show that finitely generated (λ, p) -groups are exactly finitely generated pro- p groups, but in the infinitely generated case neither of the two classes contains the other. For instance, the group $\mathcal{G}_1(X)$ considered in this appendix and

the additive group of $\mathcal{L}_1(X)$ are (λ, p) -groups but not pro- p groups while \mathbb{Z}_p^∞ with product topology is a pro- p group but not a (λ, p) -group.

In § 3 we defined the property of being *powerful* only for pro- p groups. The definition actually makes sense for an arbitrary topological (possibly discrete) group, but we should keep in mind that the definition depends on p .

Lemma A.12 (see Proposition VI.1.3 in [Weig]). *Let G be a powerful (λ, p) -group (with respect to a prime p). The following hold for all $n \in \mathbb{N}$:*

- (a) $\lambda_n(G) = G^{p^{n-1}}$.
- (b) (i) *Every element of G^{p^n} is equal to g^{p^n} for some $g \in G$.*
- (ii) *Moreover, for any $g_1, \dots, g_k \in G$ there exists $g \in G$ such that $\prod_{i=1}^k g_i^{p^n} = g^{p^n}$ and $g \equiv \prod_{i=1}^k g_i \pmod{\lambda_2(\langle g_1, \dots, g_k \rangle)}$.*

Parts (a) and (b)(i) are well known for finitely generated pro- p groups (for example, see Theorem 1.3 and Proposition 1.7 in [LM1]) and can be proved quite similarly for arbitrary (λ, p) -groups. Part (b)(ii) follows easily from the proof of (b)(i) given in [LM1].

As an immediate consequence of Lemma A.12(b)(i) and its analogue for p -complete Lie algebras (which is trivially true), we obtain the following corollary.

Corollary A.13. *Any homomorphism φ between powerful (λ, p) -groups or p -complete Lie algebras is continuous. If φ is surjective, it is also an open map.*

We will also need several results dealing with p -central groups and Lie algebras.

Lemma A.14. *Let A be a group (resp. Lie ring). Then A admits the unique largest p -central quotient, that is, there exists a normal subgroup (resp. ideal) N of A such that A/N is p -central and any homomorphism from A to a p -central group (resp. Lie ring) factors through A/N .*

Proof. This follows directly from the obvious fact that the class of p -central groups (resp. Lie rings) is closed under subgroups (resp. subrings) and direct products. \square

Before stating the next result, we need to define the notion of Ω -subgroups/ideals.

Definition. Again let p be a fixed prime.

- (a) Let L be a topological Lie ring. For each $k \in \mathbb{N}$ define $\Omega_k(L) = \{z \in L : p^k z = 0\}$ (obviously $\Omega_k(L)$ is an ideal of L).
- (b) Let G be a topological group. For each $k \in \mathbb{N}$ define $\Omega_k(G)$ to be the closed subgroup generated by $\{g \in G : g^{p^k} = 1\}$.

Note that by definition a topological group G (resp. a topological Lie algebra L) is p -central if and only if $\Omega_1(G) \subseteq Z(G)$ (resp. $\Omega_1(L) \subseteq Z(L)$). The next result provides some information about the sets Ω_k in p -central (λ, p) -groups and Lie algebras.

Lemma A.15.

- (a) Let L be a p -central topological Lie algebra. Then $[\Omega_k(L), L] \subseteq \Omega_{k-1}(L)$ for all $k \geq 2$.
- (b) Let G be a powerful p -central (λ, p) -group. Then $[\Omega_2(G), G] \subseteq \Omega_1(G)G^{p^2}$.

Proof. (a) Take any $x \in \Omega_k(L)$. Then $p^{k-1}x \in \Omega_1(L)$. Since L is p -central, for any $y \in L$ we have $p^{k-1}[x, y] = [p^{k-1}x, y] = 0$ and hence $[x, y] \in \Omega_{k-1}(L)$.

(b) Using the commutator identity $[h_1h_2, g] = [h_1, g]^{h_2}[h_2, g]$, we are reduced to showing that $[h, g] \in \Omega_1(G)G^{p^2}$ whenever $h^{p^2} = 1$.

So let us assume that $h^{p^2} = 1$ and take any $g \in G$. Since G is p -central, we have $[h^p, g] = 1$. On the other hand, by (5.1) (which is a direct consequence of the Hall-Petrescu formula) we have $[h^p, g] \equiv [h, g]^p \pmod{\lambda_4 G}$ (since $p \geq 3$). Since G is powerful, parts (a) and (b)(i) of Lemma A.12 imply that $[h, g]^p = z^{p^3}$ for some $z \in G$. On the other hand, by Lemma A.12(b)(ii) we have $1 = [h, g]^p(z^{-p^2})^p = ([h, g]z^{-p^2}r)^p$ for some $r \in \lambda_2(\lambda_2(G)) = \lambda_3(G) = G^{p^2}$. Thus, $[h, g]z^{-p^2}r \in \Omega_1(G)$ and so $[h, g] \in \Omega_1(G)G^{p^2}$, as desired. \square

Lemma A.16. *Let G be a powerful p -central (λ, p) -group, let $x, y \in G$, and suppose that $x^p = y^p$. Then $x^{-1}y \in \Omega_1(G)$, that is, $(x^{-1}y)^p = 1$.*

Proof. Since $\Omega_1(G)$ is closed with respect to the (λ, p) -topology on G , it suffices to prove that $x^{-1}y \in \lambda_k(G)\Omega_1(G)$ for each $k \in \mathbb{N}$. We will argue by induction on k , with the base case $k = 1$ being obvious.

Suppose now that $x^{-1}y \in \lambda_k(G)\Omega_1(G)$ for some k . Thus, $y = xwz$ where $w \in \lambda_k(G)$ and $z \in \Omega_1(G)$. Since $z^p = 1$ and z is central in G , we have $y^p = (xw)^p$, and by the Hall-Petrescu formula $(xw)^p \equiv x^p w^p \pmod{\lambda_{k+2}(G)}$ (since $w \in \lambda_k G$).

Since $x^p = y^p$ by assumption and G is powerful, Lemma A.12(b)(i) implies that $w^p = h^{p^{k+1}}$ for some h in G . By Lemma A.12(b)(ii), $(wh^{-p^k}r)^p = 1$ for some $r \in \lambda_2(\langle w, h^{p^k} \rangle) \subseteq \lambda_{k+1}(G)$. Thus, $w \in r^{-1}h^{p^k}\Omega_1(G) \subseteq \lambda_{k+1}(G)\Omega_1(G)$, which completes the induction step. \square

A.6. Constructing homomorphisms from $\mathcal{L}_3(X)$ and $\mathcal{G}_3(X)$. In our last subsection we will prove Theorem A.2 and its group-theoretic counterpart Theorem A.9. The proofs of these results will be quite similar to each other, but the group case will involve some additional technicalities. Thus we will give a complete proof of Theorem A.2 and then explain which steps require non-trivial modifications in the group case.

We start by recalling the statement of Theorem A.2.

Theorem A.2. *Let $X = \{x_1, \dots, x_d\}$ for some $d \in \mathbb{N}$. Let $L \in \text{Ob}(\mathfrak{L})$ or $L = \mathcal{L}_3(X)$ and $\mathbf{u} = (u_1, \dots, u_d)$ any d -tuple in L . Then there exists a unique continuous Lie algebra homomorphism $f = f_{\mathbf{u}} : \mathcal{L}_3(X) \rightarrow L$ such that $f(c) = c_L(\mathbf{u})$ for every 3-integral commutator c . In particular, $f(x_i) = u_i$ for all $1 \leq i \leq d$.*

Proof. Recall that we only need to prove the existence of f in the case $L \in \text{Ob}(\mathfrak{L})$ (the other parts of the statement are easy and have already been established). The proof will be divided into several steps.

Step 0: a brief outline. For a monic X -commutator c we set $\bar{c} = \frac{1}{p^{wt(c)-1}}c$, and let $S \subseteq \mathcal{L}_1(X)$ be the set of all elements of the form \bar{c} . Thus,

$$S = X \cup \left\{ \frac{1}{p}[x_i, x_j] \right\} \cup \left\{ \frac{1}{p^2}[[x_i, x_j], x_k], \frac{1}{p^2}[x_i, [x_j, x_k]] \right\} \cup \dots$$

Since each \bar{c} is 1-integral, it yields the corresponding function $\bar{c}_L : L^{\times d} \rightarrow L$ which is well defined up to $\Omega_1(L) = \{z \in L : pz = 0\}$. From now on we fix such a function for each $\bar{c} \in S$. If $wt(c) = 1$, so $\bar{c} = c = x_i$ for some i , we naturally require that $\bar{c}((v_1, \dots, v_d)) = v_i$. Define the function $f_0 : S \rightarrow L$ by

$$f_0(s) = s_L(\mathbf{u}) \text{ for all } s \in S.$$

Note that the \mathbb{Z}_p -span of S is dense in $\mathcal{L}_1(X)$. If it were possible to extend f_0 to a Lie algebra homomorphism $f : \mathcal{L}_1(X) \rightarrow L$, then the restriction of f to $\mathcal{L}_3(X)$ would be a map with desired properties; however, one can show that in general it is not even possible to extend f_0 to a \mathbb{Z}_p -linear map on $\mathcal{L}_1(X)$. We will overcome this problem as follows.

We will construct a \mathbb{Z}_p -Lie algebra $\mathcal{F}(X)$ generated by a set \widehat{S} and continuous Lie algebra homomorphisms $\tilde{f} : \mathcal{F}(X) \rightarrow L$ and $\pi : \mathcal{F}(X) \rightarrow \mathcal{L}_1(X)$ such that $\pi(\widehat{S} \cup -\widehat{S}) = S$ and $f_0(\pi(s)) = \tilde{f}(s)$ for all $s \in \widehat{S}$. The Lie algebra $\mathcal{F}(X)$ will be obtained from a certain Lie algebra defined by generators and relations by first taking the (λ, p) -completion and then considering its largest p -central quotient.

We will then show that there exists an open subalgebra $\mathcal{F}_3(X)$ of $\mathcal{F}(X)$ such that π is injective on $\mathcal{F}_3(X)$ and maps $\mathcal{F}_3(X)$ onto $\mathcal{L}_3(X)$. Thus, there exists a Lie algebra isomorphism $\pi^{-1} : \mathcal{L}_3(X) \rightarrow \mathcal{F}_3(X)$, and π^{-1} is automatically continuous. since π is open by Corollary A.13. It is now straightforward to check that $f = \tilde{f} \circ \pi^{-1} : \mathcal{L}_3(X) \rightarrow L$ is a homomorphism with desired properties.

Step 1: Construction of $\mathcal{F}(X)$. Choose any total ordering on the set of monic X -commutators such that a longer commutator is always larger than a shorter one. Let T be the unique set of monic X -commutators such that $X \subseteq T$ and an X -commutator c of weight ≥ 2 lies in T if and only if $c = [t, t']$ with $t, t' \in T$ and $t > t'$.

Let \widehat{S} be the set of formal symbols $\{s_t : t \in T\}$, and let $F(X)$ be the \mathbb{Z}_p -Lie algebra generated by \widehat{S} subject to relations $ps_{[c,d]} = [s_c, s_d]$ whenever $c, d, [c, d] \in T$.

Recall that if e is a monic X -commutator, then $\bar{e} = \frac{1}{p^{wt(e)-1}}e$. Note that $p[\bar{c}, \bar{d}] = [\bar{c}, \bar{d}]$ and $p[\bar{c}, \bar{d}]_L = [\bar{c}_L, \bar{d}_L]$ (as functions on L) for all monic X -commutators c, d . Hence there exist (unique) Lie algebra homomorphisms $\pi : F(X) \rightarrow \mathcal{L}_1(X)$ and $\tilde{f} : F(X) \rightarrow L$ such that $\pi(s_t) = \bar{t}$ and $\tilde{f}(s_t) = \bar{t}_L(\mathbf{u}) = f_0(\bar{t})$ for all $t \in T$.

We define $\mathcal{F}(X)$ as the Lie algebra obtained from $F(X)$ by taking first the (λ, p) -completion and then the largest p -central quotient (see Lemma A.14). Since L and $\mathcal{L}_1(X)$ are both p -complete Lie algebras, the homomorphisms $\pi : F(X) \rightarrow \mathcal{L}_1(X)$ and $\tilde{f} : F(X) \rightarrow L$ induce the corresponding homomorphisms from $\mathcal{F}(X)$. For simplicity of notations we will denote these induced homomorphisms by the same symbols π and \tilde{f} , and the image of \widehat{S} in $\mathcal{F}(X)$ will also be denoted by \widehat{S} .

Note that $\mathcal{F}(X)$ is p -central (by construction) and powerful since $F(X)$ is powerful (also by construction).

Step 2: Let $S_X = \{s_x \in \widehat{S} : x \in X\}$ be the subset of \widehat{S} corresponding to X . Let $\langle S_X \rangle$ be the abstract \mathbb{Z}_p -Lie subalgebra of $\mathcal{F}(X)$ generated by S_X . Let $\mathcal{F}_3(X) = p^2\mathcal{F}(X) + \langle S_X \rangle$. We claim that

- (i) π is injective on $p^2\mathcal{F}(X)$
- (ii) π is injective on $\langle S_X \rangle$
- (iii) $\pi(p^2\mathcal{F}(X) \cap \langle S_X \rangle) = \pi(p^2\mathcal{F}(X)) \cap \pi(\langle S_X \rangle)$
- (iv) $\pi(\mathcal{F}_3(X)) = \mathcal{L}_3(X)$.

We will need the following elementary result:

Lemma A.17. *Let $\varphi : C \rightarrow D$ be a homomorphism of groups, and let A and B be subgroups of C such that φ is injective on both A and B and $\varphi(A \cap B) = \varphi(A) \cap \varphi(B)$. Then φ is injective on AB .*

Remark: Lemma A.17 automatically applies to homomorphisms of Lie rings as well.

Proof. Suppose $\varphi(ab) = 1$ for some $a \in A$, $b \in B$. Then $\varphi(a) = \varphi(b^{-1}) \in \varphi(A) \cap \varphi(B) = \varphi(A \cap B)$. Since φ is injective on A and B , it follows that $a, b \in A \cap B$ whence $ab \in A \cap B$, so $\varphi(ab) = 1$ forces $ab = 1$. \square

If we prove (i)-(iv), it would follow from Lemma A.17 that $\mathcal{F}_3(X) = p^2\mathcal{F}(X) + \langle S_X \rangle$ satisfies all the requirements described in Step 0 and thus finish the proof.

It is clear that $\pi(\langle S_X \rangle) = \langle X \rangle$ (the abstract \mathbb{Z}_p -Lie subalgebra of $\mathcal{L}_1(X)$ generated by X). This immediately implies (ii) since $\langle X \rangle$ is free on X and $|S_X| = |X|$. Conditions (iii) and (iv) can be checked by an easy direct computation. Both sides of (iii) consist of all elements of $\langle X \rangle$ in which the coefficients of all degree 1 monomials are divisible by p^2 and the coefficients of all degree 2 monomials are divisible by p . Thus, it remains to prove (i).

Step 3: In this step we reduce condition (i) from Step 2 to showing that π induces an injective (and hence bijective) map $\pi_2 : p^2\mathcal{F}(X)/p^3\mathcal{F}(X) \rightarrow p^2\mathcal{L}_1(X)/p^3\mathcal{L}_1(X)$.

For each $k \in \mathbb{N}$ we have a commutative diagram

$$(A.7) \quad \begin{array}{ccc} p^k\mathcal{F}(X)/p^{k+1}\mathcal{F}(X) & \xrightarrow{\pi_k} & p^k\mathcal{L}_1(X)/p^{k+1}\mathcal{L}_1(X) \\ \downarrow \theta_k & & \downarrow \theta'_k \\ p^{k+1}\mathcal{F}(X)/p^{k+2}\mathcal{F}(X) & \xrightarrow{\pi_{k+1}} & p^{k+1}\mathcal{L}_1(X)/p^{k+2}\mathcal{L}_1(X) \end{array}$$

where the horizontal maps π_k and π_{k+1} are induced by π and the vertical maps θ_k and θ'_k are induced by multiplication by p .

The maps θ_k and θ'_k are automatically surjective. Moreover, θ'_k is also injective since $\mathcal{L}_1(X)$ is torsion-free. Therefore, (A.7) shows that injectivity of π_k for some k implies injectivity of π_{k+1} . Thus if we know that π_3 is injective, then π_k is injective for all $k \geq 3$ and since $\bigcap_k p^k\mathcal{F}(X) = 0$ (as $\mathcal{F}(X)$ is a p -complete Lie algebra), it follows that π is injective on $p^2\mathcal{F}(X)$, as desired.

Step 4: We are now reduced to proving that the map

$$\pi_2 : p^2\mathcal{F}(X)/p^3\mathcal{F}(X) \rightarrow p^2\mathcal{L}_1(X)/p^3\mathcal{L}_1(X)$$

from Step 3 is injective.

Let B be Hall's set of basic X -commutators. We will recall the definition of B in Step 5 below; at this point all we need to know is that $B \subseteq T$ and B forms a basis for the free \mathbb{Z} -Lie algebra on X (and hence also a basis for the free R -Lie algebra on X for any commutative ring R with 1).

Let M be the abstract \mathbb{Z}_p -submodule of $\mathcal{F}(X)$ generated by $\{s_b : b \in B\}$. The image of p^2M in $p^2\mathcal{F}(X)/p^3\mathcal{F}(X)$ is an \mathbb{F}_p -vector space spanned by $\{p^2s_b + p^3\mathcal{F}(X) : b \in B\}$ and $\pi_2(p^2s_b) = \frac{1}{p^{wt(b)-3}}b + p^3\mathcal{L}_1(X)$ for all $b \in B$.

The elements $\{\frac{1}{p^{wt(b)-3}}b + p^3\mathcal{L}_1(X) : b \in B\}$ are clearly linearly independent (in fact, if $\text{Lie}_{\mathbb{F}_p}(X)$ is the free \mathbb{F}_p -Lie algebra on X , then $\text{Lie}_{\mathbb{F}_p}(X) \cong p^2\mathcal{L}_1(X)/p^3\mathcal{L}_1(X)$ as \mathbb{F}_p -vector spaces via the map $b \mapsto \frac{1}{p^{wt(b)-3}}b + p^3\mathcal{L}_1(X)$ for all $b \in B$), so π_2 is injective on $(p^2M + p^3\mathcal{F}(X))/p^3\mathcal{F}(X)$. Thus, to finish the proof it suffices to show that $p^2\mathcal{F}(X) = p^2M + p^3\mathcal{F}(X)$ (where only the inclusion " \subseteq " needs to be justified).

Step 5: For $k \in \mathbb{N}$ let $\Omega_k = \Omega_k(\mathcal{F}(X)) = \{z \in \mathcal{F}(X) : p^kz = 0\}$. In this step we will prove the inclusion

$$(A.8) \quad \mathcal{F}(X) \subseteq M + \Omega_2 + p\mathcal{F}(X).$$

Multiplying both sides of (A.8) by p^2 , we get $p^2\mathcal{F}(X) \subseteq p^2M + p^3\mathcal{F}(X)$, which would finish the proof by Step 4.

Since $\mathcal{F}(X)$ is powerful, to prove (A.8) it suffices to show that $s_t \in M + \Omega_2 + p\mathcal{F}(X)$ for any $t \in T$. We will split the proof into two parts.

Substep 1: First we will show that $s_t \in M + \Omega_2$ for all $t \in T$ such that $t = [b, c]$ for some $b, c \in B$ (our assumptions on T imply that $b > c$).

Recall that B is Hall's set of basic X -commutators (relative to the chosen ordering on the set of all monic X -commutators) which are defined as follows:

- (i) B contains X (all monic X -commutators of weight 1).
- (ii) Suppose $k > 1$ and we already defined which monic X -commutators of weight $< k$ lie in B . Then a monic X -commutator c of weight k lies in B if $c = [y, z]$ where $y, z \in B$, $y > z$ and either $wt(y) = 1$ or $y = [v, w]$ with $w \leq z$.

By construction $B \subseteq T$ and all elements of T of weight ≤ 2 lie in B , so we only need to prove the assertion of Substep 1 for t with $wt(t) \geq 3$.

So assume that $t = [b, c]$ with $b, c \in B$, $b > c$ and $wt(t) = wt(b) + wt(c) \geq 3$. Then $wt(b) > 1$, so $b = [d, e]$ for some $d, e \in B$ with $d > e$. We consider 3 cases. In Case 3 below we will argue by downward induction on $wt(c)$. It is clear that Case 3 can only occur if $wt(c) \leq \frac{k}{3}$, so all c with $wt(c) > \frac{k}{3}$ are covered by Cases 1, 2 and 2' where we give a direct argument.

Case 1: $e \leq c$. In this case $t = [b, c] = [d, e, c] \in B$, so $s_t \in M$.

Case 2: $e > c$ and $[e, c] > d$. In this case $[e, c, d] \in B$ and $[d, c, e] \in B$, so $s_{[e,c,d]}, s_{[d,c,e]} \in M$. Moreover, since $[d, e, c]$, $[e, c, d]$ and $[d, c, e]$ all lie in T , we have

$$\begin{aligned} 0 &= [s_d, s_e, s_c] + [s_e, s_c, s_d] + [s_c, s_d, s_e] \\ &= [s_d, s_e, s_c] + [s_e, s_c, s_d] - [s_d, s_c, s_e] = p^2(s_{[d,e,c]} + s_{[e,c,d]} - s_{[d,c,e]}). \end{aligned}$$

Hence, $s_{[d,e,c]} + s_{[e,c,d]} - s_{[d,c,e]} \in \Omega_2$, so

$$s_t = s_{[d,e,c]} = s_{[d,c,e]} - s_{[e,c,d]} + (s_{[d,e,c]} + s_{[e,c,d]} - s_{[d,c,e]}) \in M + \Omega_2.$$

Case 2': $e > c$ and $[e, c] = d$. In this case $[e, c, d] = 0$ and $[s_e, s_c, s_d] = p[s_{[e,c]}, s_d] = 0$. We can essentially repeat the argument from Case 2 (just delete $s_{[e,c,d]}$ from the above calculations).

Case 3: $e > c$ and $[e, c] < d$. In this case $[d, c, e] \in B$ and $[d, [e, c]] \in T$, so

$$\begin{aligned} 0 &= [s_d, s_e, s_c] + [s_e, s_c, s_d] + [s_c, s_d, s_e] \\ &= [s_d, s_e, s_c] - [s_d, [s_e, s_c]] - [s_d, s_c, s_e] = p^2(s_{[d,e,c]} - s_{[d,[e,c]]} - s_{[d,c,e]}) \end{aligned}$$

and thus $s_{[d,e,c]} - s_{[d,[e,c]]} - s_{[d,c,e]} \in \Omega_2$. We also have $s_{[d,c,e]} \in M$. While $s_{[d,[e,c]]}$ may not lie in M , since $wt([e, c]) > wt(c)$, we know that $s_{[d,[e,c]]} \in M + \Omega_2$ by the induction hypothesis, and we are done as in case 2.

Thus, we have now proved that $s_t \in M + \Omega_2$ for all $t \in T$ such that $t = [b, c]$ for some $b, c \in B$.

Substep 2: Let us now prove that $s_t \in M + \Omega_2 + p\mathcal{F}(X)$ for all $t \in T$ by induction on $k = wt(t)$.

As in substep 1, there is nothing to prove for $k \leq 2$. So fix $k \geq 3$, $t \in T$ with $wt(t) = k$ and suppose that $s_{t'} \in M + \Omega_2 + p\mathcal{F}(X)$ for all $t' \in T$ with $wt(t') < k$.

Write $t = [t_1, t_2]$ with $t_1, t_2 \in T$ and $t_1 > t_2$. By the induction hypothesis we can write $s_{t_1} = \sum_{b \in B} n_b s_b + p y_1 + r_1$ and $s_{t_2} = \sum_{b \in B} m_b s_b + p y_2 + r_2$ where $n_b, m_b \in \mathbb{Z}_p$, $y_1, y_2 \in \mathcal{F}(X)$ and $r_1, r_2 \in \Omega_2$. Therefore (using again that $\mathcal{F}(X)$ is powerful) we have

$$\begin{aligned} \text{(A.9)} \quad p s_t &= [s_{t_1}, s_{t_2}] = \sum_{b, b' \in B} n_b m_{b'} [s_b, s_{b'}] + p^2 y + p z \\ &= \sum_{b > b' \in B} (n_b m_{b'} - m_b n_{b'}) p s_{[b, b']} + p^2 y + p z. \end{aligned}$$

where $y \in \mathcal{F}(X)$ and $p z \in [\Omega_2, \mathcal{F}(X)]$.

Equation (A.9) implies that $s_t - (\sum_{b > b' \in B} (n_b m_{b'} - m_b n_{b'}) s_{[b, b']} + p y + z) \in \Omega_1$. By Substep 1, $s_{[b, b']} \in M + \Omega_2$ for all $b, b' \in B$ with $b > b'$. Finally, by Lemma A.15(a) $p z \in \Omega_1$, so $z \in \Omega_2$. Thus, $s_t \in M + \Omega_2 + p\mathcal{F}(X)$, as desired.

The proof of Theorem A.2 is now complete. \square

Let us finally prove Theorem A.9. As with Theorem A.2, we recall the statement.

Theorem A.9. *Let $X = \{x_1, \dots, x_d\}$ and $G \in \text{Ob}(\mathfrak{G})$ or $G = \mathcal{G}_3(X)$. For any finite subset $\{g_1, \dots, g_d\}$ of G there exists a continuous group homomorphism $f : \mathcal{G}_3(X) \rightarrow G$ such that $f(\text{Exp}(x_i)) = g_i$ for all i .*

Proof. As we already mentioned, this proof is very similar to that of Theorem A.2. We will briefly go over the argument concentrating on the non-obvious changes.

The role of $\mathcal{L}_1(X)$ will be played by the group $\mathcal{G}_1(X)$. Recall that $\mathcal{G}_1(X)$ is powerful and torsion-free, and moreover any element of $\mathcal{G}_1(X)^p$ has a unique p^{th} root.

For each monic X -commutator c let $h_c = H_c(\text{Exp}(x_1), \dots, \text{Exp}(x_d)) \in \mathcal{G}_1(X)$ where H_c is defined as at the beginning of § A.3.

Step 1: We define T exactly as in the Lie algebra case, and again we let $\widehat{S} = \{s_t : t \in T\}$. We define $F(X)$ to be the abstract group generated by \widehat{S} subject to relations $s_{[c,d]}^p = [s_c, s_d]$ whenever $c, d, [c, d] \in T$.

As in the Lie algebra case, we have (unique) homomorphisms with dense images $\pi : F(X) \rightarrow \mathcal{G}_1(X)$ and $\tilde{f} : F(X) \rightarrow G$ such that $\pi(s_t) = h_t$ and $\tilde{f}(s_t) = H_t(g_1, \dots, g_d)$ for all $t \in T$ (recall from § A.3 that the values of $H_t : G^{\times d} \rightarrow G$ are well defined modulo $\Omega_1(G)$).

If $\mathcal{F}(X)$ is the group obtained from $F(X)$ by taking first the (λ, p) -completion and then taking the largest p -central quotient, we obtain induced continuous surjective homomorphisms $\pi : \mathcal{F}(X) \rightarrow \mathcal{G}_1(X)$ and $\tilde{f} : \mathcal{F}(X) \rightarrow G$.

Step 2: Let $\mathcal{F}_3(X) = \mathcal{F}(X)^{p^2} \langle S_X \rangle$ where S_X is the abstract subgroup generated by $S_X = \{s_x : x \in X\}$. As in the Lie algebra case we reduce Theorem A.9 first to showing that π is injective on $\mathcal{F}_3(X)$ and then to showing that π is injective on $\mathcal{F}(X)^{p^2}$.

Step 3: Now we reduce to proving that the induced map $\pi_2 : \mathcal{F}(X)^{p^2} / \mathcal{F}(X)^{p^3} \rightarrow \mathcal{G}_1(X)^{p^2} / \mathcal{G}_1(X)^{p^3}$ is injective. Similarly to the Lie algebra case this is done via the commutative diagram

$$(A.10) \quad \begin{array}{ccc} \mathcal{F}(X)^{p^k} / \mathcal{F}(X)^{p^{k+1}} & \xrightarrow{\pi_k} & \mathcal{G}_1(X)^{p^k} / \mathcal{G}_1(X)^{p^{k+1}} \\ \downarrow \theta_k & & \downarrow \theta'_k \\ \mathcal{F}(X)^{p^{k+1}} / \mathcal{F}(X)^{p^{k+2}} & \xrightarrow{\pi_{k+1}} & \mathcal{G}_1(X)^{p^{k+1}} / \mathcal{G}_1(X)^{p^{k+2}} \end{array}$$

where the horizontal maps π_k and π_{k+1} are induced by π and the vertical maps θ_k and θ'_k are induced by raising to power p . Since $\mathcal{F}(X)$ and $\mathcal{G}_1(X)$ are powerful (λ, p) -groups, the maps θ_k and θ'_k are surjective by Lemma A.12. Since every element of $\mathcal{G}_1(X)^p$ has a unique p^{th} -root, Lemma A.12 also implies that θ'_k is injective.

Step 4: Define M to be the abstract subgroup generated by $\{s_b : b \in B\}$ (where B is still Hall's set of basic X -commutators). We claim that π_2 is injective on $M^{p^2} \mathcal{F}(X)^{p^3} / \mathcal{F}(X)^{p^3}$. This reduces to the corresponding result in the Lie algebra case using the simple observation that the exponential map $\text{Exp} : \mathcal{L}_1(X) \rightarrow \mathcal{G}_1(X)$ induces an isomorphism of \mathbb{F}_p -vector spaces $p^k \mathcal{L}_1(X) / p^{k+1} \mathcal{L}_1(X) \rightarrow \mathcal{G}_1(X)^{p^k} / \mathcal{G}_1(X)^{p^{k+1}}$.

Step 5: As in the Lie algebra case (this time using the fact that $\mathcal{F}(X)$ and $\mathcal{G}_1(X)$ are powerful), we reduce Theorem A.9(a) to showing that

$$(A.11) \quad \mathcal{F}(X) \subseteq M \cdot \Omega_2 \cdot \mathcal{F}(X)^p.$$

where $\Omega_2 = \Omega_2(\mathcal{F}(X)) = \{g \in \mathcal{F}(X) : g^{p^2} = 1\}$ (the order of the product on the right-hand side of (A.11) is irrelevant since Ω_2 and $\mathcal{F}(X)^p$ are both normal).

The argument from the Lie algebra case carries over without any changes until Case 2 of Substep 1 where in the group case we have the equality

$$[s_d, s_e, s_c] \cdot [s_e, s_c, s_d] \cdot [s_d, s_c, s_e]^{-1} = s_{[d,e,c]}^{p^2} s_{[e,c,d]}^{p^2} (s_{[d,c,e]}^{-1})^{p^2}.$$

It is still true that $[e, c, d], [d, c, e] \in B$, so $s_{[e,c,d]}, s_{[d,c,e]} \in M$. Unlike the Lie algebra counterpart of this equality, the left-hand side need not be trivial; however the element $y = [s_d, s_e, s_c] \cdot [s_e, s_c, s_d] \cdot [s_d, s_c, s_e]^{-1}$ still lies in $\gamma_4 \mathcal{F}(X)$ by basic commutator identities, and hence by Lemma A.12(b)(i) $y = w^{p^3}$ for some $w \in \mathcal{F}(X)$. Thus, $s_{[d,e,c]}^{p^2} s_{[e,c,d]}^{p^2} (s_{[d,c,e]}^{-1})^{p^2} (w^{-p})^{p^2} = 1$, and applying the Lemma A.12(b)(ii) we get that there exists $r \in \lambda_2 \mathcal{F}(X) = \mathcal{F}(X)^p$ such that $(s_{[d,e,c]} s_{[e,c,d]} s_{[d,c,e]}^{-1} w^{-p} r)^{p^2} = 1$, whence $s_{[d,e,c]} \in s_{[d,c,e]} s_{[e,c,d]}^{-1} \mathcal{F}(X)^p \Omega_2 \subseteq M \cdot \mathcal{F}(X)^p \cdot \Omega_2$, as desired.

Making similar modifications in Case 3 of Substep 1 and in Substep 2, we complete the proof of Theorem A.9. \square

REFERENCES

- [De] V. V. Deodhar, *On central extensions of rational points of algebraic groups*. Amer. J. Math. 100 (1978), no. 2, 303–386.
- [DDMS] J. D. Dixon, M. P. F. du Sautoy, A. Mann and D. Segal, *Analytic pro- p groups*. Second edition. Cambridge Studies in Advanced Mathematics, 61. Cambridge University Press, Cambridge, 1999.
- [HZ] M. Horn, S. Zandi, *Second cohomology of Lie rings and the Schur multiplier*. Int. J. Group Theory 3 (2014), no. 2, 9–20.
- [Iw] K. Iwasawa, *Local class field theory*. Oxford Science Publications. Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, 1986. viii+155
- [K] B. Klopsch, *On the Lie theory of p -adic analytic groups*. Math. Z. 249 (2005), no. 4, 713–730.
- [La1] M. Lazard, *Sur les groupes nilpotents et les anneaux de Lie*. (French) Ann. Sci. École Norm. Sup. (3) 71 (1954), 101–190.
- [La2] M. Lazard, *Groupes analytiques p -adiques*. (French) Inst. Hautes Études Sci. Publ. Math. No. 26 (1965), 389–603.
- [LM1] A. Lubotzky, A. Mann, *Powerful p -groups. I. Finite groups*. J. Algebra 105 (1987), no. 2, 484–505.
- [LM2] A. Lubotzky, A. Mann, *Powerful p -groups. II. p -adic analytic groups*. J. Algebra 105 (1987), no. 2, 506–515.
- [Ma] H. Matsumoto, *Sur les sous-groupes arithmétiques des groupes semi-simples déployés*. (French) Ann. Sci. École Norm. Sup. (4) no. 2 (1969), 1–62.
- [Mo1] C. C. Moore, *Group extensions of p -adic and adelic linear groups*. Inst. Hautes Etudes Sci. Publ. Math. No. 35 (1968), 157–222.
- [Mo2] C. C. Moore, *Group extensions and cohomology for locally compact groups. IV*. Trans. Amer. Math. Soc. 221 (1976), no. 1, 35–58.
- [NS1] N. Nikolov, D. Segal, *On finitely generated profinite groups. I. Strong completeness and uniform bounds*. Ann. of Math. (2) 165 (2007), no. 1, 171–238.

- [NS2] N. Nikolov, D. Segal, *On finitely generated profinite groups. II. Products in quasisimple groups*. Ann. of Math. (2) 165 (2007), no. 1, 239–273.
- [Pr1] G. Prasad, *On some work of Raghunathan*. Algebraic groups and arithmetic, 25–40, Tata Inst. Fund. Res., Mumbai, 2004.
- [Pr2] G. Prasad, *Deligne’s topological central extension is universal*. Adv. Math. 181 (2004), no. 1, 160–164.
- [PR1] G. Prasad, M. S. Raghunathan, *Topological central extensions of semisimple groups over local fields I, II*. Ann. of Math. (2) 119 (1984), no. 1, 143–201 and no. 2, 203–268.
- [PR2] G. Prasad, M. S. Raghunathan, *Topological central extensions of $SL_1(D)$* . Invent. Math. 92 (1988), 645–689.
- [PRp] G. Prasad, A. Rapinchuk, *Computation of the metaplectic kernel*. Inst. Hautes Études Sci. Publ. Math. No. 84 (1996), 91–187 (1997).
- [Ra] M. S. Raghunathan, *On the congruence subgroup problem*. Inst. Hautes Études Sci. Publ. Math. No. 46 (1976), 107–161.
- [Rp] A. Rapinchuk, *The multiplicative arithmetic of division algebras over number fields and the metaplectic problem*. Math. USSR-Izv. 31 (1988), no. 2, 349–379.
- [Ri] C. Riehm, *The norm 1 group of p -adic division algebra*. Amer. J. of Math. 92 (1970), no. 2, 499–523.
- [Se] J.-P. Serre, *Local fields*. Translated from the French by Marvin Jay Greenberg. Graduate Texts in Mathematics, 67. Springer-Verlag, New York-Berlin, 1979.
- [Weib] C. Weibel, *An introduction to homological algebra*. Cambridge Studies in Advanced Mathematics, 38. Cambridge University Press, Cambridge, 1994. xiv+450 pp.
- [Weig] T. Weigel, *Exp and log functors for the categories of powerful p -central groups and Lie algebras*, Habilitationsschrift, Freiburg, 1994.
- [Wil] J. Wilson, *Profinite groups*, London Mathematical Society Monographs. New Series, 19. The Clarendon Press, Oxford University Press, New York, 1998.

UNIVERSITY OF VIRGINIA

Email address: ershov@virginia.edu