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

MIKHAIL ERSHOV

Abstract. Let F be a p-adic field, that is, a finite extension of $\mathbb{Q}_p$. Let D be a finite dimensional 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[Ma] proved this result for F-split groups, and the case of F-quasi-split groups is due to Deodhar [De] and Deligne (unpublished). Almost all remaining cases were handled in [PR1], and finally the complete answer was obtained in [PRp]. [3]

Date: March 5th, 2008.

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. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation.

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

[2] Recently, a very short proof of this fact was found by Prasad [Pr1].

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

If $\mathbb{G}$ is anisotropic over F, then by Tits' classification G is isomorphic to $SL_1(D)$ for some finite-dimensional 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 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^2th *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 Prasad-Raghunathan's theorem. Indeed, if $F = \mathbb{Q}_p(\sqrt[n]{1})$ 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 [We], who extended the above correspondence to the classes of powerful p-central pro-p groups and Lie algebras (see Section 2 for definitions).

Now consider the congruence subgroup $H = SL_1^{de+1}(D)$ where d is the dergee 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 $H^2(H, \mathbb{Z}/p^k\mathbb{Z})$. First we prove that $\mathbf{res}_{G|H}$ has small kernel (see Proposition 4.8). Next we show that any cohomology class lying in the image of $\mathbf{res}_{G|H}$ is represented by a (central) extension $1 \to \mathbb{Z}/p^k\mathbb{Z} \to \widehat{H} \to H \to 1$ where $\widehat{H}$ is powerful and p-central (see Lemma 5.3). 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 Section 6 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 $H^2(G/G_m, \mathbb{Z}/p^k\mathbb{Z}) \to H^2(G, \mathbb{Z}/p^k\mathbb{Z})$ 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 $H^2(SL_1(D), \mathbb{R}/\mathbb{Z}) \to H^2(SL_1(D_0), \mathbb{R}/\mathbb{Z})$ 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 Section 2 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 relationship between (second) cohomology of pro-p groups and Lie algebras belonging to those classes. In Section 3 we review basic facts about division algebras over p-adic fields. In Section 4 we study group-theoretic properties of central extensions of $SL_1(D)$ where D is a division algebra over a p-adic field. In Section 5 we deduce parts (a) and (b) of Theorem 1.1 from certain results on Lie algebra cohomology which, in turn, are proved in Section 6. Finally, in Section 7 we prove Theorem 1.1(c).

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 $\{[a, b] \colon a \in A, b \in B\}$, where $[a, b] = a^{-1}b^{-1}ab$.

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 also very thankful to Thomas Weigel for sending me his unpublished manuscript [We] and helpful e-mail communications.

2. Preliminaries

2.1. **Exp-log correspondence.** In this subsection we will discuss natural correspondence between certain classes of $\mathbb{Z}_p$-Lie algebras, as defined below, and corresponding classes of p-adic analytic pro-p groups. All pro-p groups considered in this section are assumed to be finitely generated (without further mention).

Definition. We say that L is a *$\mathbb{Z}_p$-Lie algebra* if L is a topological Lie algebra over $\mathbb{Z}_p$ which is finitely generated as a $\mathbb{Z}_p$-module. We do not assume that L is a free $\mathbb{Z}_p$-module, that is, L is allowed to have torsion elements.

Let $\mathfrak{L}_{\mathbb{Z}_p}$ (resp. $\mathfrak{G}_{\mathbb{Z}_p}$) be the category whose objects are $\mathbb{Z}_p$-Lie algebras (resp. compact p-adic analytic groups) and whose morphisms are continuous Lie ring (resp. group) homomorpshims. 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 $\exp : \mathfrak{L} \to \mathfrak{G}$ and $\log : \mathfrak{G} \to \mathfrak{L}$ such that the compositions $\exp\circ\log$ and $\log\circ\exp$ 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):

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 (resp. powerful torsion-free pro-p groups).

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 (resp. powerful p-central pro-p groups) and $p \geq 5$.

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 [LM]. For a detailed account of the theory of poweful groups the reader is referred to an 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 [LM] and is easily deduced from results in [La2].

Theorem 2.1. *A finitely generated pro-p group is p-adic analytic if and only if it contains a finite index powerful subgroup. Furthermore, every powerful pro-p group contains a finite index subgroup which is powerful and torsion-free.*

The book [DDMS] contains a full proof of Theorem 2.1 "from scratch" as well as an explicit proof of equivalence $\mathfrak{G}_{ptf} \cong \mathfrak{L}_{ptf}$ between the categories of powerful torsion-free pro-p groups and $\mathbb{Z}_p$-Lie algebras. 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 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 [We], [4] 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 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 $L \in \mathfrak{L}_{<p}$ or $L \in \mathfrak{L}_{ppc}$. While there exist distinct ways to define $\exp(L)$ formally, they are all based on the Baker-Cambell-Hausdorff (BCH) formula.

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

Theorem 2.2. *The Baker-Campbell-Hausdorff (BCH) series Φ lies in the $\mathbb{Q}$-Lie subalgebra of 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*

$$p^{[(k-1)/(p-1)]}\lambda_c \in \mathbb{Z}_p \text{ for any } c \in S \quad \text{ and } \quad \lambda_c \in \mathbb{Z}_p \text{ if } wt(c) < p.$$

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 2.2 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 the set of formal symbols $\{\exp(u) : u \in L\}$ with the group operation

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

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 $\mathfrak{L} = \mathfrak{L}_{ppc}$.

[4] In 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.

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 $wt(c) \geq p$ where $wt(c)$ is the weight of the commutator c. 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 2.2). 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: $\mathfrak{L} = \mathfrak{L}_{ppc}$. Once again, let $c = [x_{i_1}, x_{i_2}, \dots, x_{i_k}]$ be a left-normed commutator, and define $c(u_1, u_2)$ as in case 1. Since L is powerful, there exists $v_1 \in L$ such that $[u_{i_1}, u_{i_2}] = pv_1$. Now assume that $k \geq 3$ and set $\frac{1}{p}c(u_1, u_2) = [v_1, u_{i_3}, \dots, u_{i_k}]$. 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. Similarly, there is a well defined element $\frac{1}{p^l}c(u_1, u_2)$ for all $l \leq k-2$. Since $p^{[(k-1)/(p-1)]}\lambda_c \in \mathbb{Z}_p$ by Theorem 2.2, 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 $\sum_{c \in S} \lambda_c c(u_1, u_2)$ converges in L, and we let $\Phi(u_1, u_2)$ be its sum.

It is now clear how to define the functor $\exp : \mathfrak{L} \to \mathfrak{G}$ 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 $f : L_1 \to L_2$ is a Lie algebra homomorphism, the corresponding group homomorphism $f_* : \exp(L_1) \to \exp(L_2)$ is given by $f_*(\exp(u)) = \exp(f(u))$ for $u \in L_1$.

Constructing the functor $\log : \mathfrak{G} \to \mathfrak{L}$ is a more demanding task. A "naive" approach is to imitate the above construction of the exp functor, replacing the BCH series by its functional inverse; however, formalizing such construction requires a lot of technical machinery. We refer the reader to [We] for the formal definition of the log functor. All properties of log that will be used in this paper are collected in the following proposition.

Proposition 2.3. *Let $(\mathfrak{G}, \mathfrak{L}) = (\mathfrak{G}_{<p}, \mathfrak{L}_{<p})$ or $(\mathfrak{G}_{ppc}, \mathfrak{L}_{ppc})$. There exists a functor* $\log : \mathfrak{G} \to \mathfrak{L}$ *which induces categorical equivalence $\mathfrak{G} \cong \mathfrak{L}$ and satisfies the following properties:*

(a) *Let $G \in \mathfrak{G}$ and let* $\log(G) \in \mathfrak{L}$ *be the corresponding Lie algebra. The underlying set of* $\log(G)$ *is the set of formal symbols $\{\log(g) : g \in G\}$.*

(b) *Let $\varphi : G \to H$ be a morphism in $\mathfrak{G}$, and let $\varphi^* : \log(G) \to \log(H)$ be the corresponding morphism in $\mathfrak{L}$. Then $\varphi^*(\log(g)) = \log(\varphi(g))$ for any $g \in G$.*

(c) *Let $G_1, G_2 \in \mathfrak{G}$. Then $G_1 \times G_2 \in \mathfrak{G}$, and the Lie algebra* $\log(G_1 \times G_2)$ *is isomorphic to* $\log(G_1) \times \log(G_2)$ *via the map* $\log((g_1, g_2)) \mapsto (\log(g_1), \log(g_2))$.

(d) *If* $K, G, H \in \mathfrak{G}$ *and* $1 \to K \xrightarrow{\iota} G \xrightarrow{\varphi} H \to 1$ *is an exact sequence, then the sequence* $0 \to \log(K) \xrightarrow{\iota^*} \log(G) \xrightarrow{\varphi^*} \log(H) \to 0$ *is also exact.*

(e) *Let* G, H *be objects of* $\mathfrak{G}$*, and let* $\iota : H \to G$ *be a monomorphism. Then* $\iota(H)$ *lies in the center of* G *if and only if* $\iota^*(\log(H))$ *lies in the center of* $\log(G)$*.*

2.2. **Central extensions and cohomology.** Let H be a profinite group and let A be an abelian profinite group, considered as a trivial H-module. Then there exists a canonical isomorphism of abelian groups $H^2(H, A) \cong \mathrm{Ext}(H, A)$ where $H^2(H, A)$ is the second continuous [5] cohomology group and $\mathrm{Ext}(H, A)$ is the group of equivalence classes of topological central extensions of H by A. Recall that the isomorphism is constructed as follows:

Given $C \in H^2(H, A)$, let $Z : H \times H \to A$ 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 $(h_1, a_1) \cdot (h_2, a_2) = (h_1h_2, a_1 + a_2 + Z(h_1, h_2))$. The central extension corresponding to C is

$$1 \to A \xrightarrow{\iota} \widehat{H} \xrightarrow{\varphi} H \to 1 \quad \text{or, in abbreviated form,} \quad A \overset{\iota}{\hookrightarrow} \widehat{H} \overset{\varphi}{\twoheadrightarrow} H,$$

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 $\mathrm{Ext}(C)$.

Conversely, let $\mathcal{E} = (1 \to A \xrightarrow{\iota} \widehat{H} \xrightarrow{\varphi} H \to 1)$ be an element of $\mathrm{Ext}(H, A)$. Let $\psi : H \to \widehat{H}$ be a continuous section of φ, that is, a continuous map $H \to \widehat{H}$ such that $\varphi \circ \psi = \mathrm{id}_H$, and define $Z : H \times H \to A$ by

$$Z(h_1, h_2) = \iota^{-1}(\psi(h_1h_2)^{-1}\psi(h_1)\psi(h_2)).$$

Then Z is 2-cocycle, and $\mathrm{Ext}([Z]) = \mathcal{E}$.

The relationship between central extensions and cohomology in the case of Lie rings is more delicate. Let $\mathfrak{h}$ be a profinite Lie ring, and let $\mathfrak{a}$ be an abelian profinite Lie ring, considered as a trivial $\mathfrak{h}$-module. Then there exists a canonical embedding $H^2(\mathfrak{h}, \mathfrak{a}) \to \mathrm{Ext}(\mathfrak{h}, \mathfrak{a})$, but not necessarily an isomorphism.

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

Conversely, if $\mathcal{E} \in \mathrm{Ext}(\mathfrak{h}, \mathfrak{a})$ and $\mathcal{E} = (0 \to \mathfrak{a} \xrightarrow{\iota} \widehat{\mathfrak{h}} \xrightarrow{\varphi} \mathfrak{h} \to 0)$, then $\mathcal{E} = \mathrm{Ext}(c)$ for some $c \in H^2(\mathfrak{h}, \mathfrak{a})$ if and only if there exists a continuous linear section $\psi : \mathfrak{h} \to \widehat{\mathfrak{h}}$. If such ψ exists, then $\mathcal{E} = \mathrm{Ext}([z])$ where

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

However, a linear section need not exist, e.g. if

$$\mathcal{E} = (0 \to \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p^{s+1}\mathbb{Z} \to \mathbb{Z}/p^s\mathbb{Z} \to 0).$$

[5] If continuous cohomology is replaced by measurable cohomology, the assertion holds for any topological group H

2.3. **Central extensions and** exp-log **correspondence.** Throughout this subsection $\mathfrak{G}$ (resp. $\mathfrak{L}$) will denote either $\mathfrak{G}_{ppc}$ (resp. $\mathfrak{L}_{ppc}$) or $\mathfrak{G}_{<p}$ (resp. $\mathfrak{L}_{<p}$).

Given $H \in \mathfrak{G}$ and $A \in \mathfrak{G}$, with A abelian, we define $\mathrm{Ext}_{\mathfrak{G}}(H, A)$ to be the subset of $\mathrm{Ext}(H, A)$ consisting of extensions $A \hookrightarrow \widehat{H} \twoheadrightarrow H$ such that $\widehat{H} \in \mathfrak{G}$ as well. We define $\mathrm{Ext}_{\mathfrak{L}}(\mathfrak{h}, \mathfrak{a})$ for $\mathfrak{h}, \mathfrak{a} \in \mathfrak{L}$, with $\mathfrak{a}$ abelian, in the analogous way.

Proposition 2.4. *Let $\mathfrak{L}$ and $\mathfrak{G}$ be as above. Let $H, A \in \mathfrak{G}$ where A is abelian, and let $\mathfrak{h} = \log(H)$, $\mathfrak{a} = \log(A)$.*

(a) There exists a natural bijection $\mathrm{Log} : \mathrm{Ext}_{\mathfrak{G}}(H, A) \to \mathrm{Ext}_{\mathfrak{L}}(\mathfrak{h}, \mathfrak{a})$.

(b) Suppose that $\mathfrak{G} = \mathfrak{G}_{<p}$, or $\mathfrak{G} = \mathfrak{G}_{ppc}$ and H is torsion-free. Then

(i) $\mathrm{Ext}_{\mathfrak{G}}(H, A)$ *is a subgroup of* $\mathrm{Ext}(H, A)$

(ii) $\mathrm{Ext}_{\mathfrak{L}}(\mathfrak{h}, \mathfrak{a})$ *is a subgroup of* $\mathrm{Ext}(\mathfrak{h}, \mathfrak{a})$

(iii) *The map* $\mathrm{Log} : \mathrm{Ext}_{\mathfrak{G}}(H, A) \to \mathrm{Ext}_{\mathfrak{L}}(\mathfrak{h}, \mathfrak{a})$ *is an isomorphism of abelian groups.*

Proof. (a) Let $\mathcal{E} = (1 \to A \xrightarrow{\iota} \widehat{H} \xrightarrow{\varphi} H \to 1)$ be an element of $\mathrm{Ext}_{\mathfrak{G}}(H, A)$. By Proposition 2.3(d), the sequence

$$0 \to \mathfrak{a} \xrightarrow{\iota^*} \log(\widehat{H}) \xrightarrow{\varphi^*} \mathfrak{h} \to 0 \tag{2.1}$$

is exact. Since $\iota(A)$ is central in $\widehat{H}$, Proposition 2.3(e) implies that $\iota^*(\mathfrak{a})$ is central in $\log(\widehat{H})$. It follows that (2.1) is a central extension of $\mathfrak{h}$ by $\mathfrak{a}$, which we denote by $\mathrm{Log}(\mathcal{E})$. Thus we constructed a map $\mathrm{Log} : \mathrm{Ext}_{\mathfrak{G}}(H, A) \to \mathrm{Ext}_{\mathfrak{L}}(\mathfrak{h}, \mathfrak{a})$. Similarly, one uses the exp functor to construct the inverse map $\mathrm{Exp} : \mathrm{Ext}_{\mathfrak{L}}(\mathfrak{h}, \mathfrak{a}) \to \mathrm{Ext}_{\mathfrak{G}}(H, A)$, whence $\mathrm{Log} : \mathrm{Ext}_{\mathfrak{G}}(H, A) \to \mathrm{Ext}_{\mathfrak{L}}(\mathfrak{h}, \mathfrak{a})$ is a bijection.

(b) Let $\mathcal{E}_1 = (A \overset{\iota_1}{\hookrightarrow} \widehat{H}_1 \overset{\varphi_1}{\twoheadrightarrow} H)$ and $\mathcal{E}_2 = (A \overset{\iota_2}{\hookrightarrow} \widehat{H}_2 \overset{\varphi_2}{\twoheadrightarrow} H)$ be two elements of $\mathrm{Ext}_{\mathfrak{G}}(H, A)$. By definition of addition in $\mathrm{Ext}(H, A)$ we have

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

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

To prove (i) we need to show that $\widehat{H}/\widehat{N} \in \mathfrak{G}$. If $\mathfrak{G} = \mathfrak{G}_{<p}$, this is obvious since $\widehat{H}_1, \widehat{H}_2 \in \mathfrak{G}_{<p}$ 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 2.5. *A 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

$$[x, y] = [(x_1, x_2), (y_1, y_2)] = ([x_1, y_1], [x_2, y_2]) = (z_1^p, z_2^p) = (z_1, z_2)^p \tag{2.2}$$

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 (2.2) and Lemma 2.5. The proof of (i) is complete.

The proof of (ii) is analogous to (and easier than) the proof of (i). Finally, to prove (iii) we need to show that $\mathrm{Log}(\mathcal{E}_1 + \mathcal{E}_2) = \mathrm{Log}(\mathcal{E}_1) + \mathrm{Log}(\mathcal{E}_2)$. We have $\mathrm{Log}(\mathcal{E}_i) = (\mathfrak{a} \overset{\iota_i^*}{\hookrightarrow} \widehat{\mathfrak{h}}_i \overset{\varphi_i^*}{\twoheadrightarrow} \mathfrak{h})$ for $i = 1, 2$ where $\widehat{\mathfrak{h}}_i = \log(\widehat{H}_i)$ and

$$\mathrm{Log}(\mathcal{E}_1 + \mathcal{E}_2) = (\mathfrak{a} \overset{\iota^*}{\hookrightarrow} \log(\widehat{H}/\widehat{N}) \overset{\varphi^*}{\twoheadrightarrow} \mathfrak{h}).$$

Now let $\widehat{\mathfrak{h}} = \{(u_1, u_2) \in \widehat{\mathfrak{h}}_1 \times \widehat{\mathfrak{h}}_2 : \varphi_1^*(u_1) = \varphi_2^*(u_2)\}$ and $\widehat{\mathfrak{n}} = \{(\iota_1^*(a), \iota_2^*(-a)) : a \in \mathfrak{a}\}$. By Proposition 2.3(a), $\log(\widehat{H}/\widehat{N}) = \{\log((\hat{h}_1, \hat{h}_2)\widehat{N}) : (\hat{h}_1, \hat{h}_2) \in \widehat{H}\}$ as a set. We claim that the map

$$\theta : \log(\widehat{H}/\widehat{N}) \to \widehat{\mathfrak{h}}/\widehat{\mathfrak{n}} \text{ given by } \theta(\log((\hat{h}_1, \hat{h}_2)\widehat{N})) = (\log \hat{h}_1, \log \hat{h}_2) + \widehat{\mathfrak{n}}$$

is a Lie algebra isomorphism. This follows from Proposition 2.3(c)(d) since each of the groups $\widehat{H}_1 \times \widehat{H}_2$, $\widehat{H}$ and $\widehat{H}/\widehat{N}$ is powerful and p-central. Thus $\mathrm{Log}(\mathcal{E}_1 + \mathcal{E}_2)$ is equivalent to the extension $(\mathfrak{a} \overset{\theta\iota^*}{\hookrightarrow} \widehat{\mathfrak{h}}/\widehat{\mathfrak{n}} \overset{\varphi^*\theta^{-1}}{\twoheadrightarrow} \mathfrak{h})$, and it is easy to see that

$$(\mathfrak{a} \overset{\theta\iota^*}{\hookrightarrow} \widehat{\mathfrak{h}}/\widehat{\mathfrak{n}} \overset{\varphi^*\theta^{-1}}{\twoheadrightarrow} \mathfrak{h}) = \mathrm{Log}(\mathcal{E}_1) + \mathrm{Log}(\mathcal{E}_2). \quad \square$$

Equivariant extensions and cohomology classes. Let H and A be as above, and suppose that G is another group which acts on both H and A. An extension $A \overset{\iota}{\hookrightarrow} \widehat{H} \overset{\varphi}{\twoheadrightarrow} H$ will be called **G-equivariant** if there exists an action of G on $\widehat{H}$ which is compatible with the G-action on H and A, that is,

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

We will denote the subset of G-equivariant extensions by $\mathrm{Ext}(H, A)^G$, and we set $\mathrm{Ext}_{\mathfrak{G}}(H, A)^G = \mathrm{Ext}_{\mathfrak{G}}(H, A) \cap \mathrm{Ext}(H, A)^G$.

An element $c \in H^2(H, A)$ will be called G-equivariant if $\mathrm{Ext}(c) \in \mathrm{Ext}(H, A)^G$, 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 easy to see that G-equivariant cohomology classes are invariant under the G-action of $H^2(H, A)$, but the converse is not necessarily true.

Similarly, if $\mathfrak{h}, \mathfrak{a} \in \mathfrak{L}$, with $\mathfrak{a}$ abelian, and both $\mathfrak{h}$, $\mathfrak{a}$ are G-modules, we define abelian groups $\mathrm{Ext}(\mathfrak{h}, \mathfrak{a})^G$, $\mathrm{Ext}_{\mathfrak{L}}(\mathfrak{h}, \mathfrak{a})^G$ and $H^2(\mathfrak{h}, \mathfrak{a})^G$ in the analogous way.

Proposition 2.6. *Let H, A and G be as above, and define $\mathfrak{h} = \log(H)$, $\mathfrak{a} = \log(A)$. Then there exists a canonical action of G on $\mathfrak{h}$ given by*

$$\log(h)^g = \log(h^g) \textit{ for any } h \in H \textit{ and } g \in G, \tag{2.3}$$

and the map Log *defined in Proposition 2.4 maps* $\mathrm{Ext}_{\mathfrak{G}}(H,A)^G$ *onto* $\mathrm{Ext}_{\mathfrak{L}}(\mathfrak{h},\mathfrak{a})^G$.

Proof. The action of G on H determines a homomorphism $G \to \mathrm{Aut}\,(H)$. By Proposition 2.3(a)(b), there exists a canonical isomorphism $I : \mathrm{Aut}\,(H) \to \mathrm{Aut}\,(\mathfrak{h})$ given by $(I\varphi)(\log h) = \log \varphi(h)$ for $h \in H$ and $\varphi \in \mathrm{Aut}\,(H)$. Thus, we obtain a canonical action of G on $\mathfrak{h}$ which is clearly given by (2.3).

Let $\mathcal{E} = (A \hookrightarrow \widehat{H} \twoheadrightarrow H)$ be an element of $\mathrm{Ext}_{\mathfrak{G}}(H,A)^G$ and let $(\mathfrak{a} \hookrightarrow \widehat{\mathfrak{h}} \twoheadrightarrow \mathfrak{h}) = \mathrm{Log}(\mathcal{E})$. Repeating the above argument with $\mathfrak{h}$ replaced by $\widehat{\mathfrak{h}}$, we obtain a canonical action of G on $\widehat{\mathfrak{h}}$, and it is straightforward to check that the extension $\mathfrak{a} \hookrightarrow \widehat{\mathfrak{h}} \twoheadrightarrow \mathfrak{h}$ is G-equivariant. Thus, Log sends $\mathrm{Ext}_{\mathfrak{G}}(H,A)^G$ to $\mathrm{Ext}_{\mathfrak{L}}(\mathfrak{h},\mathfrak{a})^G$. Similarly, one shows that the inverse map $\mathrm{Exp} = \mathrm{Log}^{-1}$ sends $\mathrm{Ext}_{\mathfrak{L}}(\mathfrak{h},\mathfrak{a})^G$ to $\mathrm{Ext}_{\mathfrak{G}}(H,A)^G$. □

Proposition 2.7. *Suppose that* $\mathfrak{G} = \mathfrak{G}_{ppc}$, $\mathfrak{L} = \mathfrak{L}_{ppc}$. *Let H be powerful torsion-free, let A be an abelian pro-p group, and let* $\mathfrak{h} = \log(H)$ *and* $\mathfrak{a} = \log(A)$. *The following hold:*

(a) The canonical embedding $H^2(\mathfrak{h},\mathfrak{a}) \to \mathrm{Ext}(\mathfrak{h},\mathfrak{a})$ *is an isomorphism.*

(b) Let $H^2_{\mathfrak{G}}(H,A)$ *be the preimage of* $\mathrm{Ext}_{\mathfrak{G}}(H,A)$ *under the canonical isomorphism* $H^2(H,A) \to \mathrm{Ext}(H,A)$, *and define* $H^2_{\mathfrak{L}}(\mathfrak{h},\mathfrak{a})$ *in a similar way. Then there exists a natural isomorphsim* $H^2_{\mathfrak{G}}(H,A) \to H^2_{\mathfrak{L}}(\mathfrak{h},\mathfrak{a})$.

Proof. (a) Since H is a torsion-free group, $\mathfrak{h}$ is a torsion-free $\mathbb{Z}_p$-Lie algebra, which means that $\mathfrak{h}$ is a free $\mathbb{Z}_p$-module. Thus for any central extension $\mathcal{E} = \mathfrak{a} \overset{\iota}{\hookrightarrow} \widehat{\mathfrak{h}} \overset{\varphi}{\twoheadrightarrow} \mathfrak{h}$, there exists a (continuous) linear map $\psi : \mathfrak{h} \to \widehat{\mathfrak{h}}$ such that $\varphi\psi = \mathrm{id}$, and therefore $\mathcal{E} = \mathrm{Ext}(c)$ for some $c \in H^2(\mathfrak{h},\mathfrak{a})$.

(b) This follows directly from (a) and Proposition 2.4(b). □

Definition. Let $c \in H^2(G,A)$ (for some G and A) and $A \overset{\iota}{\hookrightarrow} \widehat{G} \overset{\varphi}{\twoheadrightarrow} G = \mathrm{Ext}(c)$. The map $\varphi : \widehat{G} \to G$ will be called the *covering map* corresponding to c, and $\widehat{G}$ will be called the *covering group* of G corresponding to c.

3. The norm one group of a p-adic division algebra.

General notation. If K is a discrete valuation ring (not necessarily commutative), we will denote the ring of integers of K by O_K and the maximal ideal of O_K by $\mathfrak{m}_K$.

Division algebras over p-adic fields. Let F be a p-adic field, i.e. a finite extension of $\mathbb{Q}_p$. Let D be a finite-dimensional central division algebra over F, and let d be the degree of D. Let W be a maximal unramified extension of F inside D (note that $[W : F] = d$). Then there exist a uniformizer π of D and a generator σ of the Galois group $\mathrm{Gal}\,(W/F)$ such that

$$\pi w \pi^{-1} = \sigma(w) \text{ for all } w \in W. \tag{3.1}$$

Note that $\tau = \pi^d$ is a uniformizer of F, so $\mathfrak{m}_D = \pi O_D$, $\mathfrak{m}_D \cap W = \mathfrak{m}_W = \tau O_W$ and $\mathfrak{m}_D \cap F = \mathfrak{m}_F = \tau O_F$.

The norm one group $SL_1(D)$. Let $\mathrm{N}_{\mathrm{red}}$ (resp. $\mathrm{T}_{\mathrm{red}}$) denote the reduced norm (resp. reduced trace) map from D to F. Recall that if $a \in D$, then $\mathrm{N}_{\mathrm{red}}(a)$ (resp. $\mathrm{T}_{\mathrm{red}}(a)$) is equal to the determinant (resp. trace) of the endomorphism of the left W-vector space D given by $x \mapsto xa$. The restriction of $\mathrm{N}_{\mathrm{red}}$ (resp. $\mathrm{T}_{\mathrm{red}}$) to W coincides with the norm (resp. trace) map of the extension W/F.

Let $G = SL_1(D)$ be the group of elements of reduced norm one in D. For $n \geq 1$ let $G_n = SL_1^n(D) = \{g \in G : g \equiv 1 \mod \mathfrak{m}_D^n\}$. Note that each G_n is a finite index pro-p subgroup of G. The following properties are well known:

Proposition 3.1. *The following hold:*

(a) *G is a semi-direct product of G_1 and the group Δ 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 $i, j \geq 1$. If $p \neq 2$ or $d \neq 2$, then*

$$[G_i, G_j] = \begin{cases} G_{i+j} & \text{if } d \nmid i \text{ or } d \nmid j \\ G_{i+j+1} & \text{otherwise} \end{cases} ; \quad \text{in particular, } G_i = \gamma_i G_1 \text{ for } i \geq 1.$$

(c) *Let e be the ramification index of F and let $i > de/(p-1)$. Then $G_i^p = G_{i+dp}$. Moreover, if $g \in G_i \backslash G_{i+1}$, then $g^p \in G_{i+dp} \backslash G_{i+dp+1}$.*

Lie algebras of congruence subgroups. Using (3.1), it is easy to deduce a formula for the commutator bracket on D:

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

For each $n \geq 1$ we set $\mathfrak{g}_n = \mathfrak{sl}(\pi^n O_D)$, where $\mathfrak{sl}$ stands for the set of elements of reduced trace zero. It is easy to see that for $a \in W$ and $i \in \mathbb{Z}$,

$$\mathrm{T}_{\mathrm{red}}(a\pi^i) = 0 \quad \text{if and only if} \quad d \nmid i \text{ or } \mathbf{tr}_{W/F}(a) = 0.$$

There is a natural "conjugation" action of G on $\mathfrak{g}_n$ given by

$$u^g = g^{-1}ug \text{ for } u \in \mathfrak{g}_n \text{ and } g \in G \tag{3.2}$$

Note also that (3.2) induces an action of G on each quotient $\mathfrak{g}_n/\mathfrak{g}_m$.

If $n > de$, the group G_n is powerful and torsion-free by Proposition 3.1(b)(c), so we can consider the Lie algebra $\log(G_n)$. It is easy to see that $\log(G_n)$ is isomorphic to $\mathfrak{g}_n$ via the map $\log(h) \mapsto \sum_{i=1}^{\infty} \frac{(-1)^{i-1}(h-1)^i}{i!}$ where the product and sum on the right-hand side are taken in O_D.

Similarly, if $m, n \in \mathbb{N}$ are such that $n \leq m \leq (p-1)n$, then $G_n/G_m \in \mathfrak{G}_{<p}$, and $\log(G_n/G_m)$ is isomorphic to $\mathfrak{g}_n/\mathfrak{g}_m$ via the map $\log(hG_m) \mapsto \sum_{i=1}^{p-1} \frac{(-1)^{i-1}(h-1)^i}{i!} + \mathfrak{g}_m$.

Now let $H = G_n$ and $\mathfrak{h} = \mathfrak{g}_n$ for some $n > de$, or $H = G_n/G_m$ and $\mathfrak{h} = \mathfrak{g}_n/\mathfrak{g}_m$, with $n \leq m \leq (p-1)n$. The conjugation action of G on H yields a canonical action of G on $\log(H)$ given by (2.3). It is easy to see that this action on $\log(H)$ corresponds to the action of G on $\mathfrak{h}$ given by (3.2) under the above isomorphism between $\log(H)$ and $\mathfrak{h}$.

More on local fields. We finish this section with an elementary fact which will come very handy when we compute cohomology of $\mathfrak{h}$ in Section 6.

Claim 3.2. *Given a local field K, let $\overline{K}$ be the abelian group K/O_K.*

a) *$\overline{K}$ is an O_K-module where $(a+O_K)b = ab + O_K$ for $a \in K$ and $b \in O_K$.*
b) *Any field automorphism $\varphi : K \to K$ induces a ring automorphism $\bar{\varphi} : \overline{K} \to \overline{K}$*
c) *If L/K is an unramified extension and $\varphi \in \mathrm{Gal}\,(L/K)$, then $\alpha \in \overline{L}$ is fixed by $\bar{\varphi}$ if and only if $\alpha \in \overline{K}$.*
d) *If L/K is an unramified extension, there is a well-defined map $\mathbf{tr}_{\overline{L}/\overline{K}} : \overline{L} \to \overline{K}$ such that $\mathbf{tr}_{\overline{L}/\overline{K}}(a + O_L) = \mathbf{tr}_{L/K}(a) + O_K$ for any $a \in L$.*

4. 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 Section 3. Recall that $G = SL_1(D)$, d is the degree of D and e is the ramification index of F. From now on 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 $\le p^n$ 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 embeddings $A_1 \subset A_2 \subset A_3 \dots$ induce a sequence of homomorphisms

$$H^2(G, A_1) \xrightarrow{\iota_1} H^2(G, A_2) \xrightarrow{\iota_2} \dots$$

Since $G/[G,G]$ is a finite group of order prime to p, it is easy to see that each ι_k is injective and moreover $H^2(G, A_k)$ can be identified with the subgroup of elements of order $\le p^k$ in $H^2(G, A_\infty)$ (see [PR2, 2.2]). The main result of [PR2] asserts that $H^2(G, A_\infty)$ is a finite cyclic group. Therefore, if $H^2(G, A_\infty)$ has order p^N, then $H^2(G, A_\infty) \cong H^2(G, A_k)$ for any $k \ge N$.

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 $n \ge 1$ 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 $n \ge 1$.

The following proposition describes basic power-commutator structure in covering groups of G:

Proposition 4.1. *Let $c \in H^2(G, A)$ with $\mathrm{Ext}(c) = A \overset{\iota}{\hookrightarrow} \widehat{G} \overset{\varphi}{\twoheadrightarrow} G$. 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 $k \ge 1$ 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* $x \in G_k \backslash G_{k+1}$ *for some* $k > \frac{pde}{p-1}$*, and choose any* $\hat{x} \in \gamma_k \widehat{S}$ *such that* $\varphi(\hat{x}) = x$*. Then* $\hat{x}^{p^n} \in \gamma_{k+nde}\widehat{S} \backslash \gamma_{k+1+nde}\widehat{S}$ *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 $[U, W] = [V, W]$.

(a) Using the Hall-Petrescu formula we have

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

$$(\gamma_k \widehat{S})^p \subseteq [(\gamma_{k-1}\widehat{S})^p, \widehat{S}]\, \gamma_{p(k-1)+1}\widehat{S}. \tag{4.1}$$

By Proposition 3.1, $(\gamma_{k-1}S)^p = G_{k-1}^p = G_{k+de-1} = \gamma_{k+de-1}S$. 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 (4.1) 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 Hall-Petrescu formula we have

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

Since $p(k-1) + 1 > k + de$, we conclude that $[(\gamma_{k-1}\widehat{S})^p, \widehat{S}] \subseteq (\gamma_k\widehat{S})^p$.

(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 3.1(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,

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

(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 3.1(c) since $x \notin G_{k+1}$ by assumption. □

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 4.2 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 $\mathrm{Ext}(c) = A \overset{\iota}{\hookrightarrow} \widehat{G} \overset{\varphi}{\twoheadrightarrow} G$. Let $\widehat{S} = \varphi^{-1}(S)$.

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

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

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

Proposition 4.2. *For any $c \in H^2(G, A)$ we have* $\mathrm{infdep}(c) = \mathrm{comdep}(c)$.

Before proving Proposition 4.2, we need to establish several auxiliary results.

Lemma 4.3. *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 $H^2(G, A_r) \to H^2(G, A_s)$, then c and c' have the same set of commutator breaks. In particular,* $\mathrm{comdep}(c') = \mathrm{comdep}(c)$.

Proof. Let $\widehat{G} \overset{\varphi}{\to} G$ and $\widehat{G}' \overset{\varphi'}{\to} G$ be the covering maps determined by c and c' respectively, let $\widehat{S} = \varphi^{-1}(S)$ and $\widehat{S}' = \varphi'^{-1}(S)$. Since $\widehat{S} = A_r \times S$ and $\widehat{S}' = A_s \times S$ as sets, we can think of $\widehat{S}$ as a subgroup of $\widehat{S}'$. It is easy to see that $\gamma_m \widehat{S}' = \gamma_m \widehat{S}$ for $m \geq 2$, and $\mathrm{Ker}\,\varphi' \cap \gamma_2 \widehat{S}' = \mathrm{Ker}\,\varphi \cap \gamma_2 \widehat{S}$. It follows that $\mathrm{Ker}\,\varphi' \cap \gamma_m \widehat{S}' = \mathrm{Ker}\,\varphi \cap \gamma_m \widehat{S}$ for any $m \geq 2$, so c and c' have the same commutator breaks. □

The key information about inflation depth is provided by the following lemma from [PR2].

Lemma 4.4. *If F has no primitive p^{th} root of unity, the group $H^2(G, A_1)$ is trivial. Otherwise, $H^2(G, A_1)$ is cyclic of order p, and for any nonzero $c \in H^2(G, A_1)$ one has* $\mathrm{infdep}(c) = pde/(p-1)$. □

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

If $H^2(G, A_1) = 0$, then $H^2(G, \mathbb{Q}_p/\mathbb{Z}_p)$ is trivial by the discussion at the beginning of this section, and there is nothing to study. Thus, from now on we assume that $H^2(G, A_1)$ is cyclic of order p.

Corollary 4.5. *Let c be a non-trivial element of $H^2(G, A_s)$ for some s. Then*

$$\mathrm{infdep}(c) \geq pde/(p-1).$$

Proof. By Lemma 4.3, after making s smaller if necessary, we can assume that c does not lie in the image of the natural map $H^2(G, A_{s-1}) \to H^2(G, A_s)$. The short exact sequence $1 \to A_{s-1} \to A_s \xrightarrow{\times p^{s-1}} A_1 \to 1$ yields the long exact sequence of cohomology groups

$$\cdots \to H^2(G, A_{s-1}) \to H^2(G, A_s) \to H^2(G, A_1) \to \cdots$$

Let $\bar{c}$ be the image of c in $H^2(G, A_1)$. Then $\bar{c} \neq 0$ since c does not come from $H^2(G, A_{s-1})$. By Lemma 4.4 we have $\mathrm{infdep}(\bar{c}) = pde/(p-1)$. It remains to show that $\mathrm{infdep}(c) \geq \mathrm{infdep}(\bar{c})$.

Let $m = \mathrm{infdep}(c)$, and let $c_1 \in H^2(G/G_m, A_s)$ be an element which maps to c. If $\bar{c}_1$ is the image of c_1 in $H^2(G/G_m, A_1)$, then clearly $\bar{c}_1$ maps to $\bar{c}$ under the inflation $H^2(G/G_m, A_1) \to H^2(G, A_1)$. Therefore, $\mathrm{infdep}(\bar{c}) \leq m$. □

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 4.6. *Let Γ be a group, N a normal subgroup of Γ, and let M be a trivial Γ-module. Fix $c \in H^2(\Gamma, M)$ with $\operatorname{Ext}(c) = (1 \to M \xrightarrow{\iota} \widehat{\Gamma} \xrightarrow{\varphi} \Gamma \to 1)$. Let $\inf : H^2(\Gamma/N, M) \to H^2(\Gamma, M)$ be the inflation map.*

(a) *Suppose that $c = \inf(c')$ for some $c' \in H^2(\Gamma/N, M)$. Then there exists a section ψ of φ (i.e. a map $\psi : \Gamma \to \widehat{\Gamma}$ with $\varphi\psi = \mathrm{id}_\Gamma$) such that $\psi(N)$ is a normal subgroup of $\widehat{\Gamma}$.*

(b) *Conversely, suppose that φ has a section ψ such that $\psi(N)$ is a normal subgroup of $\widehat{\Gamma}$. Let $c' \in H^2(\Gamma/N, M)$ be the cohomology class corresponding to the extension*

$$\mathcal{E}' = (1 \to M \xrightarrow{\iota'} \widehat{\Gamma}/\psi(N) \xrightarrow{\varphi'} \Gamma/N \to 1)$$

where ι' and φ' are induced by ι and φ, respectively. Then $c = \inf(c')$. The element c' will be called the **deflation** *of c.*

Proof. (a) Let $\Gamma' = \Gamma/N$, $\pi : \Gamma \to \Gamma'$ the natural surjection, and let $(M \overset{\iota'}{\hookrightarrow} \widehat{\Gamma'} \overset{\varphi'}{\twoheadrightarrow} \Gamma') = \operatorname{Ext}(c')$. Then clearly $\operatorname{Ext}(c) \cong (M \overset{\iota}{\hookrightarrow} \Delta \overset{\varphi}{\twoheadrightarrow} \Gamma)$ where Δ is the pullback of the diagram

$$\begin{tikzcd} \widehat{\Gamma'} \arrow[r, "\varphi'"] & \Gamma' & \Gamma \arrow[l, "\pi"'] \end{tikzcd}$$

that is, $\Delta = \{(x, y) \in \widehat{\Gamma'} \times \Gamma \mid \varphi'(x) = \pi(y)\}$, and ι and φ are defined by $\iota(m) = (\iota'(m), 1)$ for any $m \in M$ and $\varphi(x, y) = y$ for any $y \in \Gamma$.

Now choose a section $\psi' : \Gamma' \to \widehat{\Gamma'}$ of φ' such that $\psi'(1) = 1$, and define $\psi : \Gamma \to \Delta$ by $\psi(y) = (\psi'(\pi(y)), y)$. Clearly, ψ is a section of φ, and $\psi(N) = \{(1, y) : y \in N\}$ is easily seen to be a normal subgroup of Δ.

(b) First we will contruct a section $\theta : \Gamma \to \widehat{\Gamma}$ of φ such that $\theta = \psi$ on N and $\theta(xn) = \theta(x)\theta(n)$ for any $x \in \Gamma$ and $n \in N$. Let S be a transversal for N in Γ such that $1 \in S$. Define $\theta : S \to \widehat{\Gamma}$ to be any map such that $\varphi(\theta(s)) = s$ for $s \in S$, and $\theta(1) = 1$. Finally, extend θ to Γ by setting $\theta(sn) = \theta(s)\theta(n)$ for $s \in S$ and $n \in N$. Clearly θ has required properties since $\psi(n_1 n_2) = \psi(n_1)\psi(n_2)$ for any $n_1, n_2 \in N$.

Now let $\widehat{N} = \psi(N) = \theta(N)$, and define $\theta' : \Gamma/N \to \widehat{\Gamma}/\widehat{N}$ by $\theta'(xN) = \theta(x)\widehat{N}$. Then θ' is well-defined since $\theta(xn) = \theta(x)\theta(n)$ for $x \in \Gamma$ and $n \in N$, and clearly θ' is a section of φ'. The elements $c \in H^2(\Gamma, M)$ and $c' \in H^2(\Gamma/N, M)$ are represented by the cocycles $Z : \Gamma \times \Gamma \to M$ and $Z' : \Gamma/N \times \Gamma/N \to M$, respectively, where

$$Z(x, y) = \iota^{-1}(\theta(xy)^{-1}\theta(x)\theta(y)) \text{ and } Z'(x', y') = \iota'^{-1}((\theta'(x'y'))^{-1}\theta'(x')\theta'(y')).$$

It is clear that $Z(x, y) = Z'(xN, yN)$ for any $x, y \in \Gamma$, and therefore, c is the inflation image of c'. □

Proof of Proposition 4.2. Let $m = \operatorname{comdep}(c)$. First we will show that that $m \geq \operatorname{infdep}(c) - 1$. By definition of commutator depth, we have $\operatorname{Ker}\varphi \cap \gamma_{m+1}\widehat{S} = \{1\}$, whence φ maps $\gamma_{m+1}\widehat{S}$ isomorphically onto $\gamma_{m+1}S = G_{m+1}$. Therefore, φ has a 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 $\mathrm{infdep}(c) \leq m+1$ by Lemma 4.6(b). Thus, we showed that $m \geq \mathrm{infdep}(c) - 1$.

If $c = 0$, Proposition 4.2 is trivially true, so from now on we assume that $c \neq 0$. By Corollary 4.5 we have $m \geq \frac{pde}{p-1} - 1$, whence $(\gamma_m\widehat{S})^p \subseteq \gamma_{m+1}\widehat{S}$ by Proposition 4.1(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 $G/S \cong \widehat{G}/\widehat{S}$. Let $\overline{K}$ be the subspace $(\gamma_m\widehat{S} \cap \operatorname{Ker}\varphi)\gamma_{m+1}\widehat{S}/\gamma_{m+1}\widehat{S}$ 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 L be an arbitrary lift of $\overline{L}$ in $\gamma_m\widehat{S}$, and let H be the subgroup of $\widehat{S}$ generated by L and $\gamma_{m+1}\widehat{S}$. 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 in normal in $\widehat{G}$. By construction, $H \cap \operatorname{Ker}\varphi = \{1\}$ and $\varphi(H) = \gamma_m S$. Applying Lemma 4.6(b) and arguing as before, we conclude that $\mathrm{infdep}(c) \leq m = \mathrm{comdep}(c)$.

Now we prove the reverse inequality $\mathrm{comdep}(c) \leq \mathrm{infdep}(c)$. Let $n = \mathrm{infdep}(c)$. Then c is represented by a cocycle $Z : G \times G \to A$ such that

$$Z(G, G_n) = Z(G_n, G) = \{0\}.$$

Recall that $\widehat{G}$ is the set of pairs $\{(g,a) : g \in G, a \in A\}$ with multiplication $(g,a)(h,b) = (gh, a+b+Z(g,h))$. For each $g \in G$ we set $\hat{g} = (g, 0) \in \widehat{G}$.

Let $g \in S$ and $h \in G_n$. Since Z vanishes on $G \times G_n$ and $G_n \times G$, we have

$$[\hat{g},\hat{h}] = \hat{g}^{-1}\hat{h}^{-1}\hat{g}\hat{h} = (\hat{h}\hat{g})^{-1}\hat{g}\hat{h} = (\widehat{hg})^{-1}\widehat{gh} =$$
$$(\widehat{gh[h,g]})^{-1}\widehat{gh} = (\widehat{gh}\widehat{[h,g]})^{-1}\widehat{gh} = \widehat{[h,g]}^{-1} = \widehat{[h,g]^{-1}} = \widehat{[g,h]}.$$

Similarly, if we are given elements $\{g_i, h_i\}_{1 \leq i \leq s}$ such that $g_i \in G$ and $h_i \in G_n$ for each i, then

$$\prod[\widehat{g_i},\widehat{h_i}] = \widehat{\prod[g_i,h_i]}.$$

Since $\operatorname{Ker}\varphi$ does not contain non-trivial elements of the form $\hat{g}$, with $g \in G$, it follows that $\operatorname{Ker}\varphi \cap \gamma_{n+1}\widehat{S} = \{1\}$, whence $\mathrm{comdep}(c) \leq n$. □

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

Proposition 4.7. *Let $c \in H^2(G, A_s)$ for some $s \in \mathbb{N}$. Let $b_1 < \ldots < b_n$ be the commutator breaks of c. Then $b_i = de(i + \frac{1}{p-1})$ for $1 \leq i \leq n$. Moreover, ord$(c) = p^n$.*

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

Proof. By Lemma 4.3, we can assume that c does not come from $H^2(G, A_{s-1})$, so the image $\bar{c}$ of c in $H^2(G, A_1)$ is nontrivial. Let $A_s \xhookrightarrow{\iota} \widehat{G} \overset{\varphi}{\twoheadrightarrow} G = \mathrm{Ext}(c)$. Then $\mathrm{Ext}(\bar{c}) = A_1 \xhookrightarrow{\bar{\iota}} \widehat{G}/\iota(A_{s-1}) \overset{\bar{\varphi}}{\twoheadrightarrow} G$, and $\bar{\iota}(A_1) = \iota(A_s)/\iota(A_{s-1})$. It follows easily that $b_1 = \mathrm{comdep}(\bar{c})$. Therefore, $b_1 = \frac{pde}{p-1}$ by Lemma 4.4.

From now on we set $A = A_s$. We know that $\iota(A) \subset \gamma_{b_1}\widehat{S}$. For any $i \geq 1$ we have $\iota(A^{p^{i-1}}) \subseteq (\gamma_{b_1}\widehat{S})^{p^{i-1}} \subseteq \gamma_{b_1+(i-1)de}\widehat{S}$, where the last inclusion holds by Proposition 4.1(a). Since A is a cyclic group, it follows that $b_i \geq b_1 + (i-1)de = (i + \frac{1}{p-1})de$ for $1 \leq i \leq n$.

Now suppose that $b_m > \frac{de}{p-1} + mde$ for some $m \geq 2$, and let m be minimal with this property. Let x be a generator of $\iota(A^{p^{m-1}})$; then $x \in \gamma_{b_m}\widehat{S}$. Since $b_m > 2de$, we have $\gamma_{b_m}\widehat{S} = (\gamma_{b_m-de}\widehat{S})^p$ by Proposition 4.1(a). Moreover, $\gamma_{b_m-de}\widehat{S}$ is powerful, so $x = y^p$ for some $y \in \gamma_{b_m-de}\widehat{S}$.

We claim that $y \in \iota(A)$. Indeed, $\varphi(y)^p = \varphi(y^p) = \varphi(x) = 1$ since $x \in \iota(A)$. On the other hand, $\varphi(y) \in G_{b_m-de}$, and G_{b_m-de} is torsion-free by Proposition 3.1. Therefore, $\varphi(y) = 1$, whence $y \in \iota(A)$.

Since x is a generator of $\iota(A^{p^{m-1}})$, we have $y \notin \iota(A^{p^{m-1}})$, whence $y \notin \gamma_{b_{m-1}+1}\widehat{S}$. Thus, $b_{m-1} + 1 > b_m - de$, whence $b_{m-1} \geq b_m - de > \frac{de}{p-1} + (m-1)de$, contrary to the choice of m.

Finally, we prove that $ord(c) = p^n$. Since c is an element of $H^2(G, A_s)$ which does not come from $H^2(G, A_{s-1})$, the discussion at the beginning of this section implies that $ord(c) = p^s$. Since $\iota(A) \cap \gamma_{b_i}\widehat{S} \neq \iota(A) \cap \gamma_{b_i+1}\widehat{S}$ for any $1 \leq i \leq n$, it is clear that $n \leq s$. On the other hand, if $n < s$, then for some i we have $|\iota(A) \cap \gamma_{b_i}\widehat{S}/\iota(A) \cap \gamma_{b_i+1}\widehat{S}| \geq p^2$. This would imply that the group $\gamma_{b_i}\widehat{S}/\gamma_{b_i+1}\widehat{S}$ contains an element of order $\geq p^2$ contrary to Proposition 4.1(a). □

The final result of this section is concerned with the kernel of the restriction map $H^2(G, A) \to H^2(G_n, A)$.

Proposition 4.8. *Let $n \in \mathbb{N}$. Let K be the kernel of the restriction map $H^2(G, A) \to H^2(G_n, A)$, 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 $\widehat{G} \xrightarrow{\varphi} G$ be the covering map determined by c and $\widehat{G}_n = \varphi^{-1}(G_n)$. Since $c \in K$, the extension $A \overset{\iota}{\hookrightarrow} \widehat{G}_n \overset{\varphi}{\twoheadrightarrow} G_n$ 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 4.1(c), whence $\gamma_{2n+2}\widehat{S} \cap \iota(A) = \{1\}$, and therefore $b_m \leq 2n+1$ where b_m is the mth commutator break of c (note that c has m commutator breaks by the last assertion of Proposition 4.7). Also by Proposition 4.7 we get $2n + 1 \geq (m + \frac{1}{p-1})de$, whence $m \leq \frac{2n+1}{de} - \frac{1}{p-1}$. □

5. Reduction to Lie algebras

Notations. Recall that A_s denotes the cylcic 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.

The following two results on Lie algebra cohomology will be established in the next section.

Theorem 5.1. *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 the ramification index of F.*

Theorem 5.2. *Suppose that $n \equiv l \equiv 1 \mod d$, $n > \frac{de}{p-1}$ 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 $ord(c_1) \leq p^{w+1}$. 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 $ord(c_2) \leq p^{w+1}$ and c_2 maps to c_1 under the inflation map $H^2(\mathfrak{g}_l/\mathfrak{g}_m, \mathfrak{a}) \to H^2(\mathfrak{g}_l, \mathfrak{a})$.*

In this section we will deduce parts (a) and (b) of Theorem 1.1 from Theorem 5.1 and Theorem 5.2, respectively. We start with the less technical proof of part (a).

Lemma 5.3. *Suppose that $n \geq de + 1$, and let $H^2(G_n, A)^{\#}$ be the image of the restriction map $H^2(G, A) \to H^2(G_n, A)$. Then $H^2(G_n, A)^{\#} \subseteq H^2_{\mathfrak{G}}(G_n, A)^G$ where $\mathfrak{G} = \mathfrak{G}_{ppc}$.*

Proof. Let $H = G_n$. Take any $c \in H^2(G, A)$, let $c_1 \in H^2(H, A)$ be the restriction of c, and let $(A \hookrightarrow \widehat{H} \overset{\varphi}{\twoheadrightarrow} H) = \mathrm{Ext}(c_1)$. We need to prove that $\mathrm{Ext}(c_1) \in \mathrm{Ext}_{\mathfrak{G}}(H, A)^G$ which amounts to showing that $\widehat{H} \in \mathfrak{G}$ and $\mathrm{Ext}(c_1)$ is G-equivariant.

Let $\widehat{S} = \varphi^{-1}(S)$. By Proposition 4.1(b)(c) we have $\widehat{H}^p = \gamma_{n+de}\widehat{S}$ and $\gamma_2\widehat{H} \subseteq \gamma_{2n}\widehat{S}$. Since $n \geq de$, we conclude that $\gamma_2\widehat{H} \subseteq \widehat{H}^p$, so $\widehat{H}$ is powerful. Since H is torsion-free, $\widehat{H}$ is automatically p-central, so $\widehat{H} \in \mathfrak{G}$. Finally, G-equivariance of $\mathrm{Ext}(c)$ is clear: the desired action of G on $\widehat{H}$ is induced by the conjugation action of $\widehat{G}$. □

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

Theorem 1.1(a). *Suppose that $|H^2(G, \mathbb{Q}_p/\mathbb{Z}_p)| = p^N$, and let p^w be the highest power dividing e. Then $N \leq w + 6$.*

Proof. Let $A = A_N$, $\mathfrak{a} = \log(A)$, and let $C \in H^2(G, A)$ be an element of order p^N. Let $n = de + 1$, and let C_1 be the image of C under the restriction map $H^2(G, A) \to H^2(G_n, A)$. By Proposition 4.8 we have $ord(C_1) \geq p^{N-2}$.

By Lemma 5.3, $C_1 \in H^2_{\mathfrak{G}}(G_n, A)^G$ where $\mathfrak{G} = \mathfrak{G}_{ppc}$. Since G_n is torsion-free, $\mathrm{Ext}_{\mathfrak{G}}(G_n, A)^G$ is a subgroup of $\mathrm{Ext}_{\mathfrak{G}}(G_n, A)$ by Proposition 2.4(b)(i) and thus $H^2_{\mathfrak{G}}(G_n, A)^G \cong \mathrm{Ext}_{\mathfrak{G}}(G_n, A)^G$ as abelian groups. Furthermore, $\mathrm{Ext}_{\mathfrak{G}}(G_n, A)^G \cong \mathrm{Ext}_{\mathfrak{L}}(\mathfrak{g}_n, \mathfrak{a})^G$ by Proposition 2.6, and $\mathrm{Ext}_{\mathfrak{L}}(\mathfrak{g}_n, \mathfrak{a})^G \cong H^2_{\mathfrak{L}}(\mathfrak{g}_n, \mathfrak{a})^G$ by Propositions 2.7.

Thus, $H^2_{\mathfrak{G}}(G_n, A)^G$ is isomorphic to a subgroup of $H^2(\mathfrak{g}_n, \mathfrak{a})^G$. By Theorem 5.1, $H^2(\mathfrak{g}_n, \mathfrak{a})^G$ has exponent $\leq p^{w+4}$. Hence, $ord(C_1) \leq p^{w+4}$, whence $N-2 \leq w+4$. □

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 5.4. *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*

$$\mathrm{Log}_{n,m} : \mathrm{Ext}(G_n/G_m, A) \to \mathrm{Ext}(\mathfrak{g}_n/\mathfrak{g}_m, \mathfrak{a})$$

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

Proof. Since $m \leq (p-1)n$, the nilpotency class of the group G_n/G_m is at most $p-2$. Thus, if $1 \to A \to \widehat{H} \to G_n/G_m \to 1$ is any central extension, then $\widehat{H}$ has nilpotency class $\leq p-1$. It follows that $\mathrm{Ext}(G_n/G_m, A) = \mathrm{Ext}_{\mathfrak{G}}(G_n/G_m, A)$ where $\mathfrak{G} = \mathfrak{G}_{<p}$, and similarly $\mathrm{Ext}(\mathfrak{g}_n/\mathfrak{g}_m, \mathfrak{a}) = \mathrm{Ext}_{\mathfrak{L}}(\mathfrak{g}_n/\mathfrak{g}_m, \mathfrak{a})$ where $\mathfrak{L} = \mathfrak{L}_{<p}$. It is now clear that Lemma 5.4 follows from Propositions 2.4 and 2.6. □

Unlike the case of torsion-free Lie algebras, the map $H^2(\mathfrak{g}_n/\mathfrak{g}_m, \mathfrak{a}) \to \mathrm{Ext}(\mathfrak{g}_n/\mathfrak{g}_m, \mathfrak{a})$ is never surjective, so there is no direct analogue of Proposition 2.7(a). Lemma 5.5 below provides a technical substitute for the latter.

Definition. Let $m, n \in \mathbb{N}$, with $n < m$. An element $C' \in H^2(G_n/G_m, A)$ will be called **good** if there exists $C \in H^2(G_n, A)$ such that

(i) C' is equal to the deflation of C in the terminology of Lemma 4.6;
(ii) C lies in the image of the restriction map $H^2(G, A) \to H^2(G_n, A)$.

The subgroup of $H^2(G_n/G_m, A)$ generated by good elements will be denoted by $H^2(G_n/G_m, A)_{good}$.

Lemma 5.5. *Suppose that $n < m \leq (p-1)n$ and $n > \frac{de}{p-1}$. Then there exists a natural monomorphism* $\log : H^2(G_n/G_m, A)_{good} \to H^2(\mathfrak{g}_n/\mathfrak{g}_m, \mathfrak{a})$.

Proof. Let $C \in H^2(G_n/G_m, A)_{good}$, let $\mathcal{E} = \mathrm{Ext}(C) \in \mathrm{Ext}(G_n/G_m, A)$, and let $\mathrm{Log} = \mathrm{Log}_{m,n} : \mathrm{Ext}(G_n/G_m, A) \to \mathrm{Ext}(\mathfrak{g}_n/\mathfrak{g}_m, \mathfrak{a})$ be the isomorphism defined in Lemma 5.4. To prove Lemma 5.5, we need to show that $\mathrm{Log}(\mathcal{E}) = \mathrm{Ext}(c)$ for some $c \in H^2(\mathfrak{g}_n/\mathfrak{g}_m, \mathfrak{a})$.

By linearity, it suffices to consider the case when C itself is good (not just a sum of good elements). Then there exists a central extension $A \overset{\iota}{\hookrightarrow} \widehat{G} \overset{\varphi}{\twoheadrightarrow} G$ such that $\mathcal{E} = A \overset{\iota'}{\hookrightarrow} \widehat{G}_n/\gamma_m\widehat{S} \overset{\varphi'}{\twoheadrightarrow} G_n/G_m$ where $\widehat{S} = \varphi^{-1}(S)$ and $\widehat{G}_n = \varphi^{-1}(G_n)$.

Choose elements $x_1, \ldots, x_k \in \mathfrak{g}_n/\mathfrak{g}_m$ such that $\mathfrak{g}_n/\mathfrak{g}_m = \langle x_1 \rangle \oplus \ldots \oplus \langle x_k \rangle$ as an abelian group. Then every element of $\mathfrak{g}_n/\mathfrak{g}_m$ can be uniquely written in the form $n_1x_1 + \ldots + n_kx_k$ where $0 \leq n_i < ord(x_i)$ for each i.

Let $\exp : \mathfrak{g}_n/\mathfrak{g}_m \to G_n/G_m$ be Lazard's exponential map (where $\mathfrak{g}_n/\mathfrak{g}_m$ is identified with $\log(G_n/G_m)$ as described in Section 3). For $1 \leq i \leq k$ we set $X_i = \exp(x_i)$. By Proposition 4.1(c), there exist lifts $\widehat{X}_1, \ldots, \widehat{X}_k \in \gamma_n\widehat{S}/\gamma_m\widehat{S}$ such that $ord(\widehat{X}_i) = ord(X_i)$ for each i. Finally, let $\hat{x}_i = \log(\widehat{X}_i) \in \log(\widehat{G}_n/\gamma_m\widehat{S})$.

By Proposition 2.3(a) we have $ord(x_i) = ord(X_i)$ and $ord(\widehat{X}_i) = ord(\hat{x}_i)$, and thus $ord(x_i) = ord(\hat{x}_i)$. Thus, we can define a linear map $\psi : \mathfrak{g}_n/\mathfrak{g}_m \to \log(\widehat{G}_n/\gamma_m\widehat{S})$ by setting

$$\psi\left(\sum_{i=1}^{k} n_i x_i\right) = \sum_{i=1}^{k} n_i \hat{x}_i.$$

Clearly, ψ is a linear section for the extension $\log(\mathcal{E}) = (\mathfrak{a} \hookrightarrow \log(\widehat{G}_n/\gamma_m\widehat{S}) \twoheadrightarrow \mathfrak{g}_n/\mathfrak{g}_m)$, and therefore $\log(\mathcal{E}) = \mathrm{Ext}(c)$ for some $c \in H^2(\mathfrak{g}_n/\mathfrak{g}_m, \mathfrak{a})$. □

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 $4w+15 \le p$. Then $|H^2(G,A)| \le p^{w+1}$.*

Proof. Throughout the proof we 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 5.2, that is, $n \equiv l \equiv 1 \mod d$, $n > \frac{de}{p-1}$, $l > 2n$ and $m \ge l + (w+1)de$, and

(ii) $2l < \frac{pde}{p-1}$, $m \le n(p-1)$ and $m \ge (w + 2 + \frac{1}{p-1})de$.

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

$$m \ge de\left(\frac{p}{4} - \frac{3(p-1)}{2e}\right) \ge de\left(w + \frac{15}{4} - \frac{3(p-1)}{2e}\right).$$

Since e divides $p-1$ and $p > 5$, we have $\frac{15}{4} - \frac{3(p-1)}{2e} \ge \frac{15}{4} - \frac{3}{2} = \frac{9}{4} \ge 2 + \frac{1}{p-1}$. Thus all inequalities in part (ii) hold. The remaining inequalities $n > \frac{de}{p-1}$ and $m \ge l + (w+1)de$ in part (i) are easily seen to hold as well.

Now consider the following commutative diagram. All vertical arrows are restriction maps, horizontal arrows without labels are inflation maps, and the two labeled arrows denote $\log$ maps defined in Lemma 5.5.

$$\begin{tikzcd}
 & & H^2(G/G_m)_{good} \arrow[r] \arrow[d] & H^2(G) \arrow[d] \\
H^2(\mathfrak{g}_n) \arrow[d] & H^2(\mathfrak{g}_n/\mathfrak{g}_m) \arrow[l] \arrow[d] & H^2(G_n/G_m)_{good} \arrow[l, "\log"'] \arrow[r] \arrow[d] & H^2(G_n) \arrow[d] \\
H^2(\mathfrak{g}_l) & H^2(\mathfrak{g}_l/\mathfrak{g}_m) \arrow[l] & H^2(G_l/G_m)_{good} \arrow[l, "\log"'] \arrow[r] & H^2(G_l)
\end{tikzcd} \tag{5.1}$$

Step 2: Assume that $|H^2(G)| \ge p^{w+2}$, and let $C \in H^2(G)$ be an element of order p^{w+2}. Then by our choice of m and Proposition 4.8, C is the inflation image of some $C_1 \in H^2(G/G_m, A)_{good}$, so we have $ord(C_1) \ge ord(C) \ge p^{w+2}$. Now let $C_2 \in H^2(G_n/G_m)_{good}$, $C_5 \in H^2(G_l/G_m)_{good}$, $C_3 \in H^2(G_n)$ and $C_4 \in H^2(G_l)$ be the images of C_1 in the commutative diagram (5.1). Since $2l < \frac{pde}{p-1}$, the map $H^2(G) \to H^2(G_l)$ is injective by Proposition 4.8. Therefore, $ord(C_2) \ge ord(C_5) \ge ord(C_4) = p^{w+2}$.

$$\begin{tikzcd}
 & & C_1 \arrow[r] \arrow[d] & C \arrow[d] \\
c_3 \arrow[d] & c_2 \arrow[l] \arrow[d] & C_2 \arrow[l, "\log"'] \arrow[r] \arrow[d] & C_3 \arrow[d] \\
c_4 & c_5 \arrow[l] & C_5 \arrow[l, "\log"'] \arrow[r] & C_4
\end{tikzcd}$$

Step 3: Let $c_2 = \log(C_2)$ and $c_5 = \log(C_5)$ where log is the map defined in Lemma 5.5. Since log is a monomorphism, we have $ord(c_2) \geq ord(c_5) \geq p^{w+2}$. 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 (5.1).

Clearly, C_2 is G-equivariant. Therefore, c_2 is G-equivariant by Proposition 2.6, whence c_3, c_5 and c_4 are also G-equivariant being inflation or restriction images of c_2.

Step 4: By Theorem 5.2, 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 $\leq p^{w+1}$. It follows that $ord(c_4) \leq p^{w+1}$ and there exist $c_5' \in H^2(\mathfrak{g}_l/\mathfrak{g}_m)$ such that $ord(c_5') \leq p^{w+1}$, and c_5' and c_5 inflate to the same element c_4.

Step 5: Let K be the kernel of the inflation map $H^2(\mathfrak{g}_l/\mathfrak{g}_m, \mathfrak{a}) \to H^2(\mathfrak{g}_l, \mathfrak{a})$ where $\mathfrak{a} = \log(A)$. According to the Lyndon-Hochschild-Serre spectral sequence, K is equal to the transgression image of $H^1(\mathfrak{g}_m, \mathfrak{a})^{\mathfrak{g}_l} = \operatorname{Hom}(\mathfrak{g}_m/[\mathfrak{g}_m, \mathfrak{g}_l], \mathfrak{a})$. The latter group has exponent p since $[\mathfrak{g}_m, \mathfrak{g}_l] \supseteq p\,\mathfrak{g}_m$. On the other hand, K contains the element $c_5 - c_5'$ which has order p^{w+2} by Steps 3 and 4. The obtained contradiction finishes the proof. □

6. 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 $\mathfrak{a}_\infty = \cup_{n=1}^{\infty}\mathfrak{a}_n$.

The goal of this section is to prove Theorems 5.1 and 5.2. The main part of the proof consists of describing $\mathfrak{a}_\infty$-valued G-invariant cocycles of Lie algebras $\mathfrak{g}_n$ for $n \equiv 1 \mod d$. Once this is achieved, both Theorems 5.1 and 5.2 follow very easily.

For the rest of this section we fix $f \in \mathbb{N}$, and let $\mathfrak{h} = \mathfrak{g}_{df+1}$. Let $\mathcal{E} = (\mathfrak{a} \overset{\iota}{\hookrightarrow} \widehat{\mathfrak{h}} \twoheadrightarrow \mathfrak{h})$ be an element of $\operatorname{Ext}(\mathfrak{h}, \mathfrak{a})$. Given a (linear) section $\psi : \mathfrak{h} \to \widehat{\mathfrak{h}}$, 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 becomes

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

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 Section 3) which, as we recall here, consists of roots of unity in $W^* \cap G$ of order prime to p.

Proposition 6.1. *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 $g \in \Delta$.*

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

Now define $\psi' : \mathfrak{h} \to \widehat{\mathfrak{h}}$ 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, $\psi'(u^g) = \psi'(u)^g$ for any $u \in \mathfrak{h}$ and $g \in \Delta$, and it follows that $Z_{\psi'}$ is Δ-invariant. □

Our next goal is to determine all bilinear Δ-invariant maps from $\mathfrak{g}_{df+1} \times \mathfrak{g}_{df+1}$ to $\mathfrak{a}_{\infty}$ (since $\mathfrak{g}_{df+1}$ 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 new notations.

Let σ and π be as in Section 3. For a subset U of W, we set

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

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

Let O be the ring of integers of W_{ur}. Given $n \geq df + 1$, define the Δ-module O_n as follows:

$$O_n = \begin{cases} O & \text{if } d \nmid n \\ \mathfrak{sl}(O) & \text{if } d \mid n \end{cases} \quad \text{as a set,} \tag{6.1}$$

and the Δ-action is given by

$$\alpha^g = \alpha \frac{g}{\sigma^n(g)} \text{ for any } \alpha \in O_n \text{ and } g \in \Delta.$$

It is easy to see that the map from O_n to $\mathfrak{g}_{df+1}$ given by $\alpha \mapsto \alpha\pi^n$ is a monomorphism of Δ-modules.

Definition. Let $C : \mathfrak{g}_{df+1} \times \mathfrak{g}_{df+1} \to \mathfrak{a}_{\infty}$ be a bilinear map. Given $i, j \geq df + 1$, define $C_{i,j} : O_i \times O_j \to \mathfrak{a}_{\infty}$ by $C_{i,j}(\alpha, \beta) = C(\alpha\pi^i, \beta\pi^j)$.

Note that a bilinear map $C : \mathfrak{g}_{df+1} \times \mathfrak{g}_{df+1} \to \mathfrak{a}_{\infty}$ 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 $\mathfrak{a}_{\infty}$ is given by the following proposition. In order to state this and all subsequent results, we use the maps introduced in Claim 3.2 as well as the following shortcut notations: $\mathbf{w} = W_{ur}/O_{W_{ur}}$, $\mathbf{f} = F_{ur}/O_{F_{ur}}$, $\mathbf{Tr} = \mathbf{tr}_{\mathbf{w}/\mathbf{f}}$ and $\mathbf{tr} = \mathbf{tr}_{\mathbf{w}/\mathfrak{q}_p}$, where $\mathfrak{q}_p = \mathbb{Q}_p/\mathbb{Z}_p$

Proposition 6.2. *Fix $i, j \geq df + 1$ and let $E : O_i \times O_j \to \mathfrak{a}_{\infty}$ be a bilinear Δ-invariant map.*

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

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

Proof. 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 (as a set $\mathfrak{o}_n$ can be identified with the residue field of W). Define the map $\overline{E} : \mathfrak{o}_i \times \mathfrak{o}_j \to \frac{1}{p}\mathbb{Z}_p/\mathbb{Z}_p$ by setting $\overline{E}(\alpha + pO_i, \beta + pO_j) = p^{k-1}E(\alpha, \beta)$. Clearly, $\overline{E}$ is Δ-invariant as well. According to [PR2, 1.5(iii) and 3.8], there exists $\mu \in \frac{1}{p}O/O$ such that $\overline{E}(\alpha, \beta) = \mathbf{tr}\,(\mu\alpha\sigma^i(\beta))$ for any $\alpha \in O_i$ and $\beta \in O_j$. Moreover, $\mu = 0$ if $d \nmid (i+j)$.

Now choose $\lambda \in \mathbf{w}$ such that $p^{k-1}\lambda = \mu$ (if $\mu = 0$, set $\lambda = 0$). Define $E_1 : O_i \times O_j \to \mathfrak{a}_k$ 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 $\alpha^g\sigma^i(\beta)^g = \alpha\frac{g}{\sigma^i(g)}\sigma^i(\beta)\sigma^i\left(\frac{g}{\sigma^j(g)}\right) = \alpha\sigma^i(\beta)$.

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 $\lambda_1 \in \mathbf{w}$, hence E has the desired form. □

Definition. Let $C : \mathfrak{g}_{df+1} \times \mathfrak{g}_{df+1} \to \mathfrak{a}_\infty$ be a bilinear map. A pair of integers (i, j), with $i, j \geq df + 1$, will be called *regular* for C if there exists $\lambda \in \mathbf{w}$ such that

$$C_{i,j}(\alpha, \beta) = \mathbf{tr}\,(\lambda\alpha\sigma^i(\beta)) \text{ for all } \alpha \in O_i \text{ and } \beta \in O_j. \tag{6.2}$$

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

One may ask if equation (6.2) determines λ uniquely. The answer is yes, unless $d = 2$, $d \mid i$ and $d \mid j$. In the latter case the set of all λ satisfying (6.2) is either empty or has the form $\lambda_0 + \mathfrak{sl}(\mathbf{w})$ for some λ_0; since $p \neq 2$ when $d = 2$ 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 (6.2) 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 (6.2) holds.

Proposition 6.2 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 6.3. *Let C be a Δ-invariant cocycle of $\mathfrak{g}_{df+1}$. 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) [6] $\lambda_{i,j} = -\sigma^i(\lambda_{j,i})$

[6] For simplicity, the automorphism of $\mathbf{w}$ induced by σ will also be denoted by σ and not $\bar{\sigma}$

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

(b) Let $i \geq 2df + d$, $j \geq df + d$, *with* $d \mid i$ *and* $d \mid j$. *Then* $(i, j) \in I_{reg}(C)$ *provided there exist* $k, l > df$, *with* $k + l = i$ *and* $d \nmid k$, *such that* $\lambda_{k,l+j} + \sigma^k(\lambda_{l,k+j}) \in \mathbf{f}$. *(***)*

Moreover, condition (***) automatically holds if $p \nmid d$.

Proof. **(a)** Relation (R1) follows easily from skew-symmetry of C, so we will only prove (R2).

First note that if $d \nmid (i + j + k)$, then all expressions in (R2) vanish by Proposition 6.2a). So, from now 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

$$\text{(6.3)}\quad \mathbf{tr}\,\Big(\Big(\lambda_{i+j,k} + \sigma^i(\lambda_{j+k,i}) + \sigma^{-k}(\lambda_{k+i,j})\Big)\,\alpha\sigma^i(\beta)\sigma^{-k}(\gamma) - \Big(\lambda_{i+j,k} + \sigma^{-k}(\lambda_{j+k,i}) + \sigma^j(\lambda_{k+i,j})\Big)\,\beta\sigma^j(\alpha)\sigma^{-k}(\gamma)\Big) = 0$$
$$\text{whenever } \alpha\pi^i, \beta\pi^j, \gamma\pi^k \in \mathfrak{g}_{df+1}.$$

Let $\mu = \lambda_{i+j,k} + \sigma^i(\lambda_{j+k,i}) + \sigma^{-k}(\lambda_{k+i,j})$ 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 $\nu = \lambda_{i+j,k} - \sigma^j(\lambda_{i,j+k}) - \lambda_{j,i+k}$, so all we have to show is that $\mu = \nu = 0$.

If neither i nor j nor k are divisible by d, we can choose arbitrary α, β and γ in (6.3), and it follows easily that $\mu = \nu = 0$. Since we assume that d divides $(i+j+k)$, but not each of i, j and k, the only remaining case is when exactly one of i, j and k is divisible by d. By symmetry, it is enough to consider the case $d \mid i$.

So, we have $d \mid i$, $d \nmid j$ and $d \nmid k$. The only restriction on α, β and γ in (6.3) is that $\alpha \in \mathfrak{sl}(O)$. Since γ can be chosen arbitrarily, it follows that $\mu\alpha\sigma^i(\beta) - \nu\beta\sigma^j(\alpha) = 0$ for any $\alpha \in \mathfrak{sl}(O)$ and $\beta \in O$.

Now suppose that $(\mu, \nu) \neq (0, 0)$. Then the above equation implies that both μ and ν are nonzero and $\frac{\mu}{\nu} = \frac{\beta\sigma^j(\alpha)}{\alpha\sigma^i(\beta)} = \frac{\sigma^j(\alpha)}{\alpha}$ since $d \mid i$. Thus, the quotient $\frac{\sigma^j(\alpha)}{\alpha}$ is the same for all nonzero α with $\mathbf{Tr}_{W/F}(\alpha) = 0$. A simple counting argument shows that the latter is possible only if $d = 2$, in which case $\mathbf{Tr}_{W/F}(\alpha) = 0$ if and only if $\frac{\sigma^j(\alpha)}{\alpha} = -1$ (since j is odd).

We proceed with the case $d = 2$. So far, we only showed that $\mu = -\nu$. But recall that in this case 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. Therefore, $\mu - \nu = \sigma^{-k}(\lambda_{k+i,j}) - \sigma^j(\lambda_{k+i,j}) = 0$ (since $-k \equiv j \mod d$). Thus, we finally showed that $\mu = \nu = 0$.

(b) Let $k, l > df$ be such that $k + l = i$ and $k \equiv 1 \mod d$ (since $i \geq 2df + d$, at least one such pair (k, l) exists). 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 6.2, after simplifications we get

$$\text{(6.4)}\qquad C((\alpha - \sigma^{-1}(\alpha))\pi^i, \gamma\pi^j) = \mathbf{tr}\,(\gamma(\sigma^{-1}(\nu\alpha) - \nu\alpha)),$$

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, (6.4) 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 $\alpha \in O$. Therefore, by definition $(i,j) \in I_{reg}(C)$.

It remains to prove that $\nu \in \mathbf{f}$ if $p \nmid d$. Replace α by $\alpha + 1$ in (6.4). 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 $\sigma^{-1}(\nu) - \nu \in \mathbf{f}$. 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 $\nu \in \mathbf{f}$. □

New notations.

1. For $m, n \in \mathbb{N}$, with $m \leq n$, we set $[m, n] = \{k \in \mathbb{N} \colon m \leq k \leq n\}$.
2. For $f \in \mathbb{N}$ and $n \geq 2f + 1$, let $I_{n,f} = [df + 1, dn - (df + 1)]$.
3. (taken from [PR2]). Given $\lambda \in \mathbf{w}$ and $i \geq 0$, let $\lambda(i) = \lambda + \sigma(\lambda) + \ldots + \sigma^{i-1}(\lambda)$. Note that $\lambda(i) + \sigma^i(\lambda(j)) = \lambda(i + j)$.

Proposition 6.4. *Let C be a Δ-invariant cocycle and set $\lambda_{i,j} = \lambda_{i,j}(C)$ for $(i,j) \in I_{reg}(C)$. Let $n \geq 4f + 2$. The following hold:*

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

Proof. First we make some preparations. Given i such that $(i, dn - i) \in I_{reg}(C)$, set $\mu_i = \lambda_{i,dn-i}(C)$. By Proposition 6.2, μ_i is defined whenever $i \in I_{n,f}$ and $d \nmid i$. Relation (R2) of Proposition 6.3 implies that

$$\mu_{i+j} = \mu_i + \sigma^i(\mu_j) = \mu_j + \sigma^j(\mu_i) \text{ unless } d \mid i \text{ and } d \mid j. \tag{6.5}$$

Claim 6.5. *Assume that $d \neq 2$. Then $\mu_k - \mu_{df+1}(k) \in \mathbf{f}$ for any $k \in I_{n,f}$ with $k \equiv \pm 1 \mod d$.*

Proof. Let $\mu = \mu_{df+1}$ and $S = \{k \in I_{n,f} : \mu_k - \mu(k) \in \mathbf{f}\}$. We proceed in several steps.

Step 1: $k \in S$ if $df + 1 \leq k \leq n - (2df + 2)$ and $k \equiv 1 \mod d$.
Subproof: The restrictions on k imply that $k + df + 1 \in I_{n,f}$. By (6.5) we have $\mu_{df+(k+1)} = \mu_{df+1} + \sigma(\mu_k) = \mu_k + \sigma^k(\mu_{df+1})$. Therefore, $\sigma(\mu_k) - \mu_k = \sigma^k(\mu_{df+1}) - \mu_{df+1} = \sigma(\mu_{df+1}(k)) - \mu_{df+1}(k)$, whence $\mu_k - \mu_{df+1}(k) \in \mathbf{f}$ by Claim 3.2(c).

Step 2: $k \in S$ if $2df + 2 \leq k \leq n - (df + 1)$ and $k \equiv -1 \mod d$.
Subproof: By step 1, $dn - k \in S$, so $\mu_{dn-k} - \mu(dn - k) \in \mathbf{f}$. By Proposition 6.3(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 $k \in S$.

Step 3: if $i, j \in I_{n,f}$ are such that $i \equiv j \equiv \pm 1 \mod d$ and $i + j \in I_{n,f}$, then $i \in S$ if and only if $j \in S$.
Subproof: Since $i \equiv j \equiv \pm 1 \mod d$, we have $\sigma^i = \sigma^j = \sigma^{\pm 1}$, and (6.5) 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 $k \equiv \pm 1 \mod d$.
Subproof: Let $i = df + (d - 1)$ and $j = 2df + (d - 1)$. By step 2 we have $j \in S$. Since $i + j = d(3f + 2) - 2 \leq dn - df - 2$ by assumptions on n, 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 $k \equiv -1 \mod d$. Combining this result with step 2, we conclude that $k \in S$ for any $k \in I_{n,f}$ with $k \equiv -1 \mod d$.

Step 5: $k \in S$ for any $k \equiv I_{n,f}$ with $k \in \pm 1 \mod d$.
Subproof: This follows from Step 4 and equality $\mu_k = -\sigma^k(\mu_{dn-k})$ by the same argument as in Step 2. □

Proof of Proposition 6.4(a). We already know that $(i, dn-i) \in I_{reg}(C)$ if $d \nmid i$. If $d = 2$, then by our assumptions $p > 2$, and the assertion in the case $d \mid i$ follows from Proposition 6.3(b). Thus we can assume that $d > 2$. 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 $k + l = i$, $l \equiv 1 \mod d$ (hence $k \equiv -1 \mod d$). 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 6.3b).

By Claim 6.5, 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, $\mu_k + \sigma^k(\mu_l) - (\mu(k) + \sigma^k(\mu(l))) \in \mathbf{f}$. Since $\mu(k) + \sigma^k(\mu(l)) = \mu(k+l) = \mu(i) = \frac{i}{d}\mathbf{Tr}\,(\mu) \in \mathbf{f}$, the proof is complete.

Once we established part a), we know that μ_i is defined for all $i \in I_{n,f}$. Thus, we can state a stronger version of Claim 6.5 (the proof remains nearly identical):

Claim 6.6. *For each $k \in I_{n,f}$ we have $\mu_k - \mu_{df+1}(k) \in \mathbf{f}$.* □

Proof of Proposition 6.4(b). For $k \in I_{n,f}$ let $\nu_k = \mu_k - \mu_{df+1}(k)$. Equation (6.5) implies that

$$\nu_{i+j} = \nu_i + \nu_j \text{ whenever } d \nmid i \text{ or } d \nmid j. \tag{6.6}$$

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 (6.6), 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 (6.5).

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

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

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. □

The assertions of Propositions 6.2 and 6.4 motivate the following definition.

Definition. A bilinear map $C : \mathfrak{g}_{df+1} \times \mathfrak{g}_{df+1} \to \mathfrak{a}_\infty$ 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 (obviously each κ_n is uniquely determined).

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

Claim 6.7. *Let C be a Δ-invariant cocycle of $\mathfrak{g}_{df+1}$. The following hold:*

(a) *Let $n = dm+1$ with $m \geq 2f+1$. Then the restriction of C to $\mathfrak{g}_n \times \mathfrak{g}_n$ is a regular cocycle.*

(b) *Assume that $f \leq e$. Then p^3C is a regular cocycle of $\mathfrak{g}_{df+1}$.*

Proof. (a) is a direct consequence of Proposition 6.4(b).

(b) Let $D = p^3C$. Clearly, D is Δ-invariant as well, so $\lambda_{i,j}(D) = 0$ if $d \nmid (i+j)$ by Proposition 6.2. It remains to show that for any $n \geq 2f+1$ and $i \in I_{n,f}$ there exists $\kappa'_n \in \mathbf{w}$ such that $\lambda_{i,dn-i}(C) = \kappa'_n(i)$.

By Proposition 6.4, for any $m \geq 4f+2$ there exists $\kappa_m \in \mathbf{w}$ such that for any $i \in I_m$ we have $C(\alpha\pi^i, \beta\pi^{dm-i}) = \mathbf{tr}\,(\kappa_m \alpha\sigma^i(\beta))$.

Recall that $\tau = \pi^d$ is a uniformizer of F. Since $e = [F : F_{ur}]$, there exist $\{d_k\} \in O_{F_{ur}}$ 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

$$D(\alpha\pi^i, \beta\pi^{dn-i}) = C(\alpha\pi^i, p^3\beta\pi^{dn-i}) = \sum_{k=3e}^{4e-1} C(\alpha\pi^i, \beta d_k \pi^{dn-i+dk}) =$$

$$\sum_{k=3e}^{4e-1} \mathbf{tr}\,(\kappa_{n+k}(i)\alpha\sigma^i(\beta)d_k) = \mathbf{tr}\,(\kappa'_n(i)\alpha\sigma^i(\beta)),$$

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

We are now ready to give a full characterization of regular Δ-invariant cocycles. This characterization involves coefficients of the minimal polynomial of τ over F_{ur}.

Definition. Let $\{c_k \in O_{F_{ur}}\}_{k=0}^{e-1}$ be defined by the relation $\tau^e = p\sum_{k=0}^{e-1} c_k \tau^k$. A sequence $\{\kappa_n \in \mathbf{w}\}_{n=2f+1}^{\infty}$ will be called *compatible* if for any $n \geq 2f+1$ we have

(C1) $\kappa_{n+e} = p\sum_{k=0}^{e-1} c_k \kappa_{n+k}$ and

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

Theorem 6.8. *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 6.3 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 $C(\alpha\pi^i,\beta\pi^{d(n+e)-i})=C(\alpha\pi^i,\beta\pi^{dn-i}\tau^e)=C(\alpha\pi^i,\beta\pi^{dn-i}\cdot p\sum\limits_{k=0}^{e-1}c_k\tau^k)=p\sum\limits_{k=0}^{e-1}C(\alpha\pi^i,c_k\beta\pi^{d(n+k)-i})$. Hence, $\mathbf{tr}\,(\kappa_{n+e}(i)\alpha\sigma^i(\beta))=p\sum\limits_{k=0}^{e-1}\mathbf{tr}\,(\kappa_{n+k}(i)c_k\alpha\sigma^i(\beta))$, 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 $d\nmid(i+j)$. Condition (C1) ensures that there exists a bilinear map $C:\mathfrak{g}_{df+1}\times\mathfrak{g}_{df+1}\to\mathfrak{a}_\infty$ such that $C_{i,j}(\alpha,\beta)=\mathbf{tr}\,(\lambda_{i,j}\alpha\sigma^i(\beta))$ for all $i,j\geq df+1$, $\alpha\in O_i$ and $\beta\in O_j$. Obviously, C is Δ-invariant. Finally, (C2) implies that $\{\lambda_{i,j}\}$ satisfy relations (R1) and (R2) of Proposition 6.3, whence C is a cocycle. □

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 6.9. *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 m indeed exists and moreover $m\leq 2f+e$ since $\mu_n=p\sum\limits_{k=0}^{e-1}c_k\mu_{n-e+k}$ for $n\geq 2f+e+1$. We know that $m\mu_m=0$, so p^l divides m.

Now consider the equality $\mu_{m+e}=p\sum\limits_{k=0}^{e-1}c_k\mu_{m+k}$ The element $\sum\limits_{k=0}^{e-1}c_k\mu_{m+k}$ 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, $l\leq w+1$. □

Proposition 6.10. *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 are cohomologous in $H^2(\mathfrak{h},\mathfrak{a}_v)$*

(b) *If $\{\alpha_n\}$ is the defining sequence of C_1, then $p^{w+1}\alpha_n=0$ 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 $n\geq 2f+1$. It is easy to see that $\mathbf{Tr}\,(\frac{1}{p^k}O/O)=\frac{1}{p^k}O_{F_{ur}}/O_{F_{ur}}$ for any $k\geq 0$. For any $n\geq 2f+1$ we have

$\mathbf{Tr}\,(\kappa_n) \in \frac{1}{p^{w+1}} O_{F_{ur}}/O_{F_{ur}}$, whence there exists $\alpha_n \in \mathbf{w}$ such that $\mathbf{Tr}\,(\alpha_n) = \mathbf{Tr}\,(\kappa_n)$ and $p^{w+1}\alpha_n = 0$.

We claim that the sequence $\{\alpha_n\}$ can be chosen compatible. First we choose α_n satisfying the above conditions for $n \in [2f+1, 2f+e]$. Then there exists a unique way to choose the remaining α_n so that (C1) holds. Since $\{\kappa_n\}$ satisfies (C1) as well, it follows that $\mathbf{Tr}\,(\alpha_n) = \mathbf{Tr}\,(\kappa_n)$ for all n, whence $\{\alpha_n\}$ satisfies (C2). It remains to show that $p^{w+1}\alpha_n = 0$ for all $n \geq 2f+1$. The latter is true for $n \in [2f+1, 2f+e]$ by construction, and follows from (C1) for $n \geq 2f+e+1$.

Since $\{\alpha_n\}$ is compatible, there exists a regular cocycle C_1 whose defining sequence is $\{\alpha_n\}$. It is also clear that $C_1(\mathfrak{h}, \mathfrak{h}) \subseteq \mathfrak{a}_{w+1} \subseteq \mathfrak{a}_v$. It remains to prove the following claim:

Claim 6.11. *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 $\kappa'_n = \kappa_n - \alpha_n$, whence $\mathbf{Tr}\,(\kappa'_n) = 0$. Hence, 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).

Now define a linear function $h : \mathfrak{h} \to \mathfrak{a}_v$ by setting

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

In general such a definition would be ambiguous since the elements $\{\pi^n : n \in \mathbb{N}\}$ are not linearly independent over O. This problem does not arise here since $\{\mu_n\}$ satisfies (C1).

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 6.10.

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

$$B(u,v) = \sum_{i,j} B(\alpha_i\pi^i, \beta_j\pi^j) = \sum_{n=2f+1}^{\infty} \sum_{i+j=dn} \mathbf{tr}\,(\kappa'_n(i)\alpha_i\sigma^i(\beta_j)) =$$

$$\sum_{n=2f+1}^{\infty} \sum_{i+j=dn} \mathbf{tr}\,((\mu_n - \sigma^i(\mu_n))\alpha_i\sigma^i(\beta_j)) = \sum_{n=2f+1}^{\infty} \sum_{i+j=dn} \mathbf{tr}\,\left(\mu_n(\alpha_i\sigma^i(\beta_j) - \sigma^{-i}(\alpha)\beta_j)\right) =$$

$$\sum_{n=2f+1}^{\infty} \sum_{i+j=dn} h([\alpha_i\pi^i, \beta_j\pi^j]) = \sum_{i,j} h([\alpha_i\pi^i, \beta_j\pi^j]) = h([u,v]).$$

□

Proof of Theorem 5.2. Let l and n be as in the statement of Theorem 5.2. Since $c \in H^2(\mathfrak{g}_n, \mathfrak{a})^G$, 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 6.7(a), C_1 is a regular cocycle of $\mathfrak{g}_l$. Therefore, by Proposition 6.10, there exists a cocylce C'_1 of $\mathfrak{g}_l$, cohomologous to C in $H^2(\mathfrak{g}_l, \mathfrak{a})$ and such that $p^{w+1}C'_1 = 0$. 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, $ord(c_2) \leq ord(C_1') = p^{w+1}$, and the inflation image of c_2 in $H^2(\mathfrak{g}_l, \mathfrak{a})$ is equal to $[C_1'] = c_1$. □

Proof of Theorem 5.1. 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 6.7(a), p^3C is a regular cocycle, so by the same argument as above, $[p^3C] \in H^2(\mathfrak{g}_n, \mathfrak{a})$ has order at most p^{w+1}. Therefore, $[C]$ has order at most p^{w+4}. □

7. 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 7.1. *Assume that $p \geq 19$. Let F be a p-adic field containing primitive p^2th 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 7.2. *Let K'/K be an extension of p-adic 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 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 $E_{K,K'} : Br(K) \to Br(K')$ 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. This yields both assertions of the proposition. □

Cohomology of SL_d over p-adic fields.

Let F be a p-adic field, and let μ_F be the group of roots of unity in F. 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 $c_F : SL_d(F) \times SL_d(F) \to \mu_F$ 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

$$c_F(\operatorname{diag}(\lambda_1, \ldots, \lambda_d), \operatorname{diag}(\mu_1, \ldots, \mu_d)) = \prod_{i \geq j} (\lambda_i, \mu_j)_F, \tag{7.1}$$

where $(\cdot,\cdot)_F$ is the norm-residue symbol on F^* of order $|\mu_F|$.

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

By properties of the norm-residue symbols, for any $\alpha, \beta \in F^*$ we have $(\alpha,\beta)_F^{n/q} = (\alpha,\beta)_{q,F}$ where $(\cdot,\cdot)_{q,F}$ is the norm-residue symbol on F^* of order q. Thus, the restriction of $c_F^{n/q}$ to $T \times T$ is given by

$$c_F^{n/q}(\operatorname{diag}(\lambda_1,\ldots,\lambda_d), \operatorname{diag}(\mu_1,\ldots,\mu_d)) = \prod_{i\geq j}(\lambda_i,\mu_j)_{q,F}. \tag{7.2}$$

Remark: By [Rp, Lemma 3], the restriction map $H^2(SL_d(F)) \to H^2(T)$ is injective if $d \geq 3$ and has kernel of order 2 if $d = 2$. Thus, (7.2) determines the cohomology class $[c_F^{n/q}]$ uniquely unless $p = d = 2$.

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

Lemma 7.3. *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 $r_{W,D} : H^2(SL_d(W)) \to H^2(SL_1(D))$ be the natural restriction map. Then $|\operatorname{Im} r_{W,D}| = |\mu_{F,wild}|$, and therefore $r_{W,D}$ is injective on $H^2(SL_d(W))_{wild}$.* □

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 7.4. *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 $r_{D',D} : H^2(SL_1(D')) \to H^2(SL_1(D))$ be the restriction map. Let p^s be the largest power of p dividing l, and assume that $|\mu_{K,wild}| \geq p^{s+1}$. Then $|\operatorname{Ker} r_{D',D}| = p^s$.*

Proof. Let W be a maximal unramified extension of K contained in D. Then it is easy to see that $W' = D \otimes_K K'$ is a maximal unramified extension of K' in D', and we have the following commutative diagram:

$$\begin{tikzcd}
H^2(SL_d(W'))_{wild} \arrow[r, "r_{W',D'}"] \arrow[d, "r_{W',W}"] & H^2(SL_1(D')) \arrow[d, "r_{D',D}"] \\
H^2(SL_d(W))_{wild} \arrow[r, "r_{W,D}"] & SL_1(D)
\end{tikzcd}$$

We claim that it is sufficient to show that $|\operatorname{Ker} r_{W',W}| = p^s$. Indeed, this would imply that the map $r_{W',W} : H^2(SL_d(W'))_{wild} \to H^2(SL_d(W))_{wild}$ is non-trivial since $|\mu_{W',wild}| \geq |\mu_{K,wild}| \geq p^{s+1}$. Since horizontal arrows in the above diagram are injective and both groups $H^2(SL_1(D'))$ and $H^2(SL_1(D))$ are cyclic of p-power order, it would follow that

$$|\operatorname{Ker} r_{D',D}| = |\operatorname{Ker} r_{W',W}| = p^s. \tag{7.3}$$

Now 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 (7.1). 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 of the norm-residue symbol we have

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

which by (7.2) 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, $\operatorname{Ker} r_{W',W}$ is generated by $([c']^{q'/q})^{q/p^s} = [c']^{q'/p^s}$. Since $ord([c']) = q'$, we conclude that $|\operatorname{Ker} r_{W',W}| = p^s$. □

Proof of Theorem 7.1. Let $d = \deg(D)$. Write $d = d_1 d_2$ where d_1 is relatively prime to p and d_2 is a power of p. By our assumption, $d_1 \neq 1$.

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. According to [PR2, 4.6], D' is a central division algebra of degree d_1 over K, and the restriction map $H^2(SL_1(D)) \to H^2(SL_1(D'))$ 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. 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. This means that $[L:\mathbb{Q}_p]$ is relatively prime to p and $|K:L| = p^w$. Since K contains primitive pth root of unity, so does L.

Since K/L is Galois and $\operatorname{Gal}(K/L)$ is a p-group, there is a tower of fields $L = L_0 \subset L_1 \subset \ldots \subset L_w = K$ such that $[L_{i+1}:L_i] = p$ for each i. Furthermore, since $|\mu_{K,wild}| \geq p^2$ by hypotheses of the theorem, we can assume that $|\mu_{L_1,wild}| = p^2$. By Proposition 7.2(b), there exists a division algebra D_0 over L such that $D_0 \otimes_L K \cong D'$, and 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 $|\mu_{L_i,wild}| \geq p^2$, Proposition 7.4 yields $|\operatorname{Ker}\{H^2(SL_1(D_{i+1})) \to H^2(SL_1(D_i))\}| \leq p$, whence $|H^2(SL_1(D_{i+1}))| \leq p \cdot |H^2(SL_1(D_i))| \leq p \cdot p^{i+1} = p^{i+2}$. □

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.

[Er] M. Ershov, *Finite presentability of $SL_1(D)$,* Israel J. Math 158 (2007), 297-347.

[Fe] I. Fesenko, S. Vostokov, *Local fields and their extensions,* With a foreword by I. R. Shafarevich. Second edition. Translations of Mathematical Monographs, 121. American Mathematical Society, Providence, RI, 2002.

[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 Ètudes Sci. Publ. Math. No. 26 (1965), 389–603.

[LM] 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.

[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 tudes Sci. Publ. Math. No. 84 (1996), 91–187 (1997).

[Ra] M. S. Raghunathan, *On the congruence subgroup problem.* Inst. Hautes Etudes 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* $\mathfrak{p}$*-adic division algebra.* Amer. J. of Math. 92 (1970), no. 2, 499-523.

[We] 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
E-mail address: ershov@virginia.edu