ISRAEL JOURNAL OF MATHEMATICS **158** (2007), 297–347
DOI: 10.1007/s11856-007-0015-9

FINITE PRESENTABILITY OF $SL_1(D)$

BY

Mikhail Ershov*

School of Mathematics, Institute for Advanced Study
Einstein Drive 1, Princeton NJ 08540, USA
e-mail: ershov@math.ias.edu

ABSTRACT

Let D be a finite dimensional division algebra over a local field of characteristic p and let $SL_1(D)$ denote the group of elements of reduced norm 1 in D. In this paper we prove that $SL_1(D)$ is finitely presented as a profinite group.

1. Introduction

Let F be a local field of (positive) characteristic p. Let D be a finite dimensional central division algebra over F, and let $SL_1(D)$ denote the group of elements of reduced norm 1 in D. The goal of this paper is to prove the following result.

Theorem 1.1: *The group $SL_1(D)$ is finitely presented as a profinite group.*

The notion of finite presentability for profinite groups is defined in the usual sense of category theory, but in general is hard to analyze. Things become easier if one considers pro-p groups instead of profinite groups, in which case a simple cohomological criterion is available (see [Wil]).

Theorem 1.2: *A finitely generated pro-p group G is finitely presented (as a pro-p group) if and only if $H^2(G, \mathbb{F}_p)$ is finite.*[1]

* This work is part of the author's Ph.D. Thesis at Yale University.

1 Here $\mathbb{F}_p$ is a finite field with p elements, considered as a trivial G-module, and cohomology is based on continuous cochains. Recall that $H^2(G, \mathbb{F}_p)$ is in bijective correspondence with equivalence classes of topological central extensions of G by $\mathbb{F}_p$.

Received September 21, 2005

Remark: By a theorem of Lubotzky [Lu1], a pro-p group is finitely presented as a pro-p group if and only if it is finitely presented as a profinite group.

Just as in the case of abstract groups, finite presentability of profinite groups is a commensurability invariant (recall that two groups are called commensurable if they have isomorphic subgroups of finite index). Since $SL_1(D)$ contains a finite index pro-p subgroup, the assertion of Theorem 1.1 is equivalent to finiteness of $H^2(G, \mathbb{F}_p)$ for some (hence arbitrary) open pro-p subgroup G of $SL_1(D)$.

In [PR], Prasad and Raghunathan established vanishing of $H^2(SL_1(D), \mathbb{Q}/\mathbb{Z})$ (where $\mathbb{Q}/\mathbb{Z}$ is given discrete topology and the action of $SL_1(D)$ is trivial), which immediately implies that $H^2(SL_1(D), \mathbb{F}_p) = 0$. The assertion of Theorem 1.1 does not follow from this result, since finiteness of cohomology is not necessarily preserved under the passage to a finite index subgroup. Still, many ideas from [PR] are used in the present paper, although they are often expressed in different language.

Theorem 1.1 settles the last open case of the following question posed by Yiftach Barnea.

QUESTION: *Let G be a connected, simply-connected, (absolutely almost) simple algebraic group defined over a (non-archimedean) local field F. If U is an open compact subgroup of $G(F)$, is U finitely presented as a profinite group?*

If F has characteristic zero, then U must be p-adic analytic and hence finitely presented (see [DDMS]). Recently, Lubotzky [Lu2] answered the above question affirmatively for all **isotropic** groups. Finally, if G is a connected simply-connected simple algebraic group defined and **anisotropic** over a local field F, then by Tits' classification $G(F)$ is isomorphic to $SL_1(D)$ for some division algebra D. Since $SL_1(D)$ is compact, its open subgroups are of finite index and hence finitely presented by Theorem 1.1.

The proof of Theorem 1.1 is based on certain relations between cohomology of pro-p groups and associated graded Lie algebras. Our method[2] is described in detail in Section 3; here we just explain how Lie algebras come into play and motivate some of the later definitions. Some notations and terminology below are introduced for expository purposes and will not be used in the rest of the paper.

Given a finitely generated pro-p group G, let $L(G)$ be the Lie algebra of G

2 A somewhat similar method was used in [Er], but the language in that paper is different.

with respect to the lower central series. The following result was suggested to the author by Efim Zelmanov.

PROPOSITION 1.3: *If $L(G)$ is finitely presented (as a Lie algebra over the ring of p-adic integers), then G is finitely presented (as a pro-p group).*

Unfortunately, we do not know any interesting examples where the hypothesis of Proposition 1.3 holds. Nevertheless, we would like to sketch a proof of this result. We give not the shortest argument, but the one which will lead us to a suitable generalization.

By Theorem 1.2, a finitely generated pro-p group G is finitely presented if and only if G has only finitely many (non-equivalent) topological central extensions by $\mathbb{F}_p$; we will call such extensions *elementary*. With each elementary extension $\mathcal{E} = 1 \to \mathbb{F}_p \to \hat{G} \to G \to 1$ one can associate an elementary extension of Lie algebras $L(\mathcal{E}) := 0 \to \mathbb{F}_p \to L(\hat{G}) \to L(G) \to 0$. The correspondence $\mathcal{E} \mapsto L(\mathcal{E})$ is not injective; however extensions $L(\mathcal{E})$ and $L(\mathcal{E}')$ are non-equivalent provided $\mathcal{E}$ and $\mathcal{E}'$ have different depths. The depth of an extension $1 \to \mathbb{F}_p \to \hat{G} \xrightarrow{\phi} G \to 1$ is defined to be the largest integer n such that $\operatorname{Ker}\phi \subseteq \gamma_n \hat{G}$. Now suppose that G is not finitely presented. Then it is easy to show that G has elementary extensions of arbitrarily large depth. It follows from the above argument that $L(G)$ has infinitely many elementary extensions and therefore $L(G)$ is not finitely presented. This finishes the sketch of a proof of Proposition 1.3.

Let us say that an elementary extension of $L(G)$ is *integrable*, if it is of the form $L(\mathcal{E})$ for some extension $\mathcal{E}$ of G. Now suppose that G is finitely presented, while $L(G)$ is not. This means that $L(G)$ has infinitely many elementary extensions, but only finitely many integrable ones. So, if we want to prove that G is finitely presented by classifying extensions of $L(G)$, we need to find necessary conditions for an extension of $L(G)$ to be integrable. The latter seems to be a hard task.

The problem can be resolved by considering Lie algebras with respect to filtrations other than the lower central series. One natural choice is the "e-step lower central series" (where e is a fixed positive integer), i.e. the series $\gamma_e G \supset \gamma_{2e} G \supset \gamma_{3e} G \supset \cdots$. Let $L^e(G)$ be the corresponding Lie algebra. As above, there is a correspondence $\mathcal{E} \mapsto L^e(\mathcal{E})$ between elementary extensions of G and elementary extensions of $L^e(G)$, and we can define the notion of an integrable extension. The new feature is that $L^e(G)$ is acted on by G in a non-trivial way (for $e > 1$). As a result, one can write down easily verifiable conditions which must hold for every integrable extension of $L^e(G)$. "Ideally", one would like to find e such that only finitely many extensions of $L^e(G)$ satisfy those

conditions. However, even if we are unable to do that, we may still be able to prove finite presentability of G as follows:

a) for every $e \in \mathbb{N}$ classify elementary extensions of $L^e(G)$;

b) show that for any sufficiently large n there exists $e = e(n)$ with the following property: if an elementary extension of $L^e(G)$ is of the form $L^e(\mathcal{E})$, then the depth of $\mathcal{E}$ cannot be equal to n (hence G has no elementary extensions of depth n).

The point is that if $\mathcal{E}$ is an elementary extension of G, then $L^e(\mathcal{E})$ carries some information about the depth of $\mathcal{E}$. So, even if we cannot show directly that $L^e(G)$ has only finitely many integrable extensions, we may still be able to establish b).

As far as part a) is concerned, note that in general not all elementary extensions of $L^e(G)$ are accounted for by the cohomology group $H^2(L^e(G), \mathbb{F}_p)$, since some of those extensions do not split even on the level of abelian groups. However, if G is the first congruence subgroup of $SL_1(D)$ (which is our case of interest), this problem does not arise: we will show that for any central extension $1 \to \mathbb{F}_p \to \hat{G} \to G \to 1$, both $L^e(G)$ and $L^e(\hat{G})$ are $\mathbb{F}_p$-Lie algebras for a suitable choice of e, whence every integrable extension of $L^e(G)$ is represented by some element of $H^2(L^e(G), \mathbb{F}_p)$.

Final remark: The filtrations we will use in the actual proof of Theorem 1.1 are not "e-step lower central series", but their truncated versions (which we call **basic filtrations**). This minor technical modification does not affect the idea of the proof.

Organization: In Section 2 we recall basic facts about filtrations in pro-p groups and associated Lie algebras. The general method used to prove Theorem 1.1 is described in Section 3. In Section 4 we review the structure of division algebras over local fields. Section 5 is concerned with computation of the second cohomology of Lie algebras associated with basic filtrations of $SL_1^1(D)$. In Section 6 we use the obtained information to complete the proof of Theorem 1.1. In the cases $p = 2$, $d = 4$, and $p = d = 3$ (where d is the degree of D over F), some of the results of Section 5 require different proofs — these are given in Sections 7. The proof of Theorem 1.1 in the case $p = d = 2$ (which requires more serious modifications) is given in Section 8.

Acknowledgements: I am extremely grateful to Alex Lubotzky for posing the problem and to Efim Zelmanov for proposing the use of Lie methods for finite presentability questions. I would like to thank Alex Lubotzky, Gregory

Margulis and Gopal Prasad for very interesting conversations and useful remarks on earlier versions of this paper, and Uzi Vishne for suggesting good references on finite fields.

Basic notations: Throughout the paper $\mathbb{Z}$ will stand for integers, and $\mathbb{N}$ for positive integers. A finite field of order q will be denoted by $\mathbb{F}_q$, and the ring of p-adic integers by $\mathbb{Z}_p$. If x is real number, then $[x]$ is the largest integer which does not exceed x. Finally, we will write $a \equiv_n b$ for $a \equiv b \bmod n$.

2. Filtrations of pro-p groups and associated graded Lie algebras

Let G be a pro-p group. As usual, given $g, h \in G$, we set $(g,h) = g^{-1}h^{-1}gh$. If A and B are subsets of G, let (A,B) be the closed subgroup generated by the set $\{(a,b) \mid a \in A, b \in B\}$. The n^{th} term of the lower central series of G is denoted by $\gamma_n G$.

Let $\omega = \{\omega_1 G \supseteq \omega_2 G \supseteq \cdots\}$ be a descending chain of closed normal subgroups of a pro-p group G. We will call ω a **filtration** of G if $(\omega_i G, \omega_j G) \subseteq \omega_{i+j} G$ for all $i, j > 0$. Note that our definition does not include standard requirements a) $\omega_1 G = G$, b) $\bigcap \omega_i G = \{1\}$ and c) $\omega_i G$ is open in G.

The **graded Lie algebra** of G associated with the filtration ω will be denoted by $L^\omega(G)$. As a graded abelian group, $L^\omega(G) = \bigoplus_{n=1}^{\infty} \omega_n G/\omega_{n+1} G$, and the bracket is defined as follows: given $g \in \omega_i G \backslash \omega_{i+1} G$ and $h \in \omega_j G \backslash \omega_{j+1} G$, set $[g\omega_{i+1}G, h\omega_{j+1}G] = (g,h)\omega_{i+j+1}G$. For each $n \geq 1$, the quotient $\omega_n G/\omega_{n+1} G$ has the structure of a right G-module with respect to the "conjugation" action. More precisely, given $g \in \omega_n G$ and $h \in G$, we set $(g\omega_{n+1}G)^h := g^h \omega_{n+1} G$ where $g^h = h^{-1}gh$. Extending by linearity, we obtain a grading-preserving action of G on $L^\omega(G)$, which respects the Lie bracket. Note that if $\omega_1 G = G$, this action is necessarily trivial.

Since G is pro-p, for every $g \in G$ and $a \in \mathbb{Z}_p$, there is a well-defined element g^a; it follows that $L^\omega(G)$ has the structure of a Lie algebra over $\mathbb{Z}_p$. If $(\omega_i G)^p \subseteq \omega_{i+1} G$ for all i, ω will be called a p-**filtration**; in this case $pL^\omega(G) = 0$, so $L^\omega(G)$ becomes a Lie algebra over $\mathbb{F}_p$.

Once again, fix a filtration $\omega = \{\omega_i G\}$ of a pro-p group G. Let $g \in G$. If $g \in \omega_n G \backslash \omega_{n+1} G$ for some n, the coset $g\omega_{n+1}G$ (which can be thought of as an element of $L^\omega(G)$) will be called the ω-**leading term** of g and denoted by $\mathrm{LT}_\omega(g)$. The number n will be referred to as the ω-**degree** of g and denoted by $\deg_\omega(g)$. If $g \in \bigcap_{i \geq 1} \omega_i G$, we set $\mathrm{LT}_\omega(g) = 0$ and $\deg_\omega(g) = \infty$. If $g \notin \omega_1 G$, both the ω-degree and the ω-leading term will be undefined.

Given a subgroup H of G, the Lie subalgebra of $L^\omega(G)$ corresponding to H is $L^\omega_G(H) := \bigoplus_{i=1}^\infty (H \cap \omega_i G)\omega_{i+1}G/\omega_{i+1}G$. Since $(H \cap \omega_i G)\omega_{i+1}G/\omega_{i+1}G$ is naturally isomorphic to $(H \cap \omega_i G)/(H \cap \omega_{i+1}G)$ for all i, we can identify $L^\omega_G(H)$ with the Lie algebra of H associated with the filtration $\{\omega_i G \cap H\}_{i=1}^\infty$.

3. Lie algebras as a tool for proving finite presentability of pro-p groups

3.1 Finite presentations and covering maps. Finiteness of the second cohomology group $H^2(G, \mathbb{F}_p)$ is one of several conditions that are equivalent to finite presentability of a pro-p group G. In order to state the other conditions we introduce the following definition.

Definition: Let G be a pro-p group. A **cover** of G is a pair $(\hat{G}, \phi)$, where $\hat{G}$ is another pro-p group and $\phi\colon \hat{G} \to G$ is a surjective homomorphism. We say that

a) $(\hat{G}, \phi)$ is a **non-trivial** cover, if $\operatorname{Ker}\phi \neq 1$,

b) $(\hat{G}, \phi)$ is an **elementary** cover, if $\operatorname{Ker}\phi \cong \mathbb{F}_p$.

The **depth** of a non-trivial cover $(\hat{G}, \phi)$ is the largest integer n such that $\operatorname{Ker}\phi \subseteq \gamma_n \hat{G}$. We will write $\operatorname{dep}(\hat{G}, \phi) = n$.

Note that if $(\hat{G}, \phi)$ is an elementary cover, then $\operatorname{Ker}\phi$ is central in $\hat{G}$. Indeed, the order of the group $A = \operatorname{Aut}(\mathbb{F}_p)$ is not divisible by p, so there is no non-trivial homomorphism from $\hat{G}$ to A.

Remark: The difference between an elementary cover and an elementary extension (extension of G by $\mathbb{F}_p$) is that in the definition of an elementary cover we do not specify the embedding of $\mathbb{F}_p$ into $\hat{G}$. Thus, each elementary cover corresponds to $(p-1)$ non-equivalent elementary extensions.

Proposition 3.1: *Let G be a finitely generated pro-p group. The following are equivalent:*

a) *G is finitely presented;*

b) *$H^2(G, \mathbb{F}_p)$ is finite;*

c) *G has finitely many equivalence classes of elementary extensions;*

d) *The depths of all non-trivial covers of G are uniformly bounded;*

e) *The depths of all elementary covers of G are uniformly bounded.*

Proof: The equivalence of a), b) and c) is well known (see [Wil]), and it is clear that c) implies e). So, it is enough to show that e) implies d) and d) implies a).

e)⇒ d) Let N be a bound for the depths of elementary covers of G. Let $(\hat{G}, \phi)$ be a non-trivial cover of G, let $n = \mathrm{dep}(\hat{G}, \phi)$, and let $K = \operatorname{Ker}\phi$. We know that $K \subseteq \gamma_n\hat{G}$ and $K \not\subseteq \gamma_{n+1}\hat{G}$, so there exists a subgroup H of K such that $K \cap \gamma_{n+1}\hat{G} \subseteq H$ and $|K : H| = p$. It is easy to see that H is a normal subgroup of $\hat{G}$, and $(\hat{G}/H, \bar{\phi})$ is an elementary cover of G (where $\bar{\phi}$ is defined in an obvious way). Therefore, $\mathrm{dep}(\hat{G}/H, \bar{\phi}) \leq N$ by assumption. On the other hand, we have $\mathrm{dep}(\hat{G}/H, \bar{\phi}) \geq n$ since $\operatorname{Ker}\bar{\phi} \subseteq \gamma_n\hat{G}/H = \gamma_n(\hat{G}/H)$. Hence, $n \leq N$.

d)⇒ a) Since G is finitely generated, it has a presentation

$$\langle x_1, \ldots, x_m \mid r_1, r_2, \ldots \rangle$$

with the following property: for every $n > 0$ all but finitely many relators $\{r_i\}$ lie in $\gamma_n F$, where F is the free pro-p group on $\{x_1, x_2, \ldots, x_m\}$ (this is true because each quotient $\gamma_n F/\gamma_{n+1}F$ is a finitely generated $\mathbb{Z}_p$-module).

Now let N be a bound for the depths of non-trivial covers of G, and let $r_1, \ldots, r_l$ be all defining relators in the above presentation which do NOT lie in $\gamma_{N+1}F$. Clearly, the group $\hat{G} = \langle x_1, \ldots, x_m \mid r_1, \ldots, r_l \rangle$ is a cover of G of depth at least $N + 1$. Therefore, G is isomorphic to $\hat{G}$ and hence finitely presented. ∎

3.2 Central extensions: from pro-p groups to Lie algebras. Let G be a pro-p group whose finite presentability we are trying to establish. For the rest of this section we fix an elementary cover $(\hat{G}, \phi)$ of G, and let $N = \mathrm{dep}(\hat{G}, \phi)$. We will describe a Lie algebra method which can be used to show that no such cover exists for sufficiently large N (and hence G is finitely presented by Proposition 3.1).

In this subsection we define a suitable filtration of G and an $\mathbb{F}_p$-valued 2-cocycle of the associated Lie algebra $L^\omega(G)$ which carries a lot of useful information about the cover $(\hat{G}, \phi)$. At some point we will need to assume that $\hat{G}$ satisfies certain condition, which holds automatically if $(\gamma_i G)^p \subseteq \gamma_{pi}G$ for all i.

Fix a positive integer e such that $e \leq N$, and let $c = [N/e]$. Given a pro-p group H, let $\{\omega_i H\}$ be the filtration of H defined by setting $\omega_i H = \gamma_{ei}H$ for $i \leq c$ and $\omega_i H = \gamma_{N+1}H$ for $i > c$. In what follows, we refer to this filtration as the **basic filtration of type** (N, e). Let $L^\omega(H) = \bigoplus_{i=1}^{\infty} L_i^\omega(H)$ be the associated graded Lie algebra. Note that $L_i^\omega(H) = 0$ for $i > c$.

Recall that we have a "conjugation" action of $\hat{G}$ on $L^\omega(\hat{G})$ and of G on $L^\omega(G)$. Since $\operatorname{Ker}\phi$ is central in $\hat{G}$, $\operatorname{Ker}\phi$ acts trivially on $L^\omega(\hat{G})$. Hence both $L^\omega(\hat{G})$

and $L^\omega(G)$ are G-modules. Moreover, the G-submodules $L_i^\omega(G)$ and $L_i^\omega(\hat{G})$ are isomorphic for $i < c$, since $\mathrm{dep}(\hat{G}, \phi) > ce$.

From now on we use shortcut notations $L = L^\omega(G)$, $\hat{L} = L^\omega(\hat{G})$ and $L_i^\omega = L_i^\omega(G)$, $\hat{L}_i^\omega = L_i^\omega(\hat{G})$ for $i \in \mathbb{N}$ (of course, $L_i^\omega = 0$ and $\hat{L}_i^\omega = 0$ for $i > c$).

Define $\phi_*\colon L \to \hat{L}$ by setting $\phi_*(\hat{g}\omega_{i+1}\hat{G}) = \phi(\hat{g})\omega_{i+1}G$ for $\hat{g} \in \omega_i\hat{G}$. Let ϕ_i be the restriction of ϕ_* to $\hat{L}_i^\omega$. Clearly, ϕ_* is a Lie algebra homomorphism preserving the G-action, ϕ_i is surjective for all i and injective for $i \neq c$, while $\mathrm{Ker}\,\phi_c \cong \mathbb{F}_p$.

In order to proceed we need the following technical lemma.

LEMMA 3.2: *Let G, $\hat{G}$ and N be as above. Let $f\colon \mathbb{N} \to \mathbb{N}$ be a function such that $(\gamma_i G)^p \subseteq \gamma_{f(i)}G$. Then for all $i \in \mathbb{N}$ we have $(\gamma_i\hat{G})^p \subseteq \gamma_{\min(f(i),N)}\hat{G}$ and $(\gamma_i\hat{G})^p \subseteq \gamma_{\min(p(i-1)+1,f(i-1)+1)}\hat{G}$.*

Proof: The first half of the statement is clear since $\mathrm{Ker}\,\phi \subseteq \gamma_N\hat{G}$. The second half can be proved using the following well-known congruence (see [LM]):

$$(x^p, y) \equiv (x, y)^p \bmod K(x, (x, y)),$$

where $K(a, b)$ is the normal closure of $\gamma_p\langle a, b\rangle \cdot (\gamma_2\langle a, b\rangle)^p$ in $\langle x, y\rangle$.

We omit the details and refer the reader to [Er, Lemma 4.2], where a very similar statement is proved. ∎

COROLLARY 3.3: *Suppose that $c \geq 2$ and $(\gamma_i G)^p \subseteq \gamma_{pi}G$ for all $i \geq 1$. Then $\{\omega_i\hat{G}\}$ is a p-filtration, i.e. $(\omega_i\hat{G})^p \subseteq \omega_{i+1}\hat{G}$ for all i.*

From now on we will assume that the conclusion (not necessarily the hypothesis) of Corollary 3.3 holds. It follows that $\hat{L}$ is a Lie algebra over $\mathbb{F}_p$ (and so is L). After choosing an isomorphism between $\mathrm{Ker}\,\phi_*$ and $\mathbb{F}_p$, we obtain a central extension of graded $\mathbb{F}_p$-Lie algebras:

$$0 \to \mathbb{F}_p \to \hat{L} \xrightarrow{\phi_*} L \to 0. \tag{3.1}$$

This extension splits on the level of graded $\mathbb{F}_p$-vector spaces. In other words, there exists a linear map $f\colon L \to \hat{L}$, such that $\phi_* f = \mathrm{id}$ and $f(L_i^\omega) \subseteq \hat{L}_i^\omega$ for $1 \leq i \leq c$. We shall call such map an ω-**graded splitting** or simply an ω-**splitting**. Note that the restriction of an ω-splitting to L_i^ω is uniquely determined for $i \neq c$.

Next we introduce two functions which encode the above central extension. Given f as above, define $\mathfrak{z}_f\colon G \times L \to \hat{L}$ as follows:

$$\mathfrak{z}_f(g, u) = f(u)^g - f(u^g).$$

Note that

$$\phi_*(\mathfrak{z}_f(g,u)) = \phi_*(f(u)^g) - \phi_*(f(u^g)) = (\phi_* f(u))^g - \phi_* f(u^g) = u^g - u^g = 0,$$

whence $\mathrm{Im}(\mathfrak{z}_f) \subseteq \mathrm{Ker}\,\phi_*$. Now define $Z_f\colon L \times L \to \hat{L}$ by setting

$$Z_f(u,v) = f([u,v]) - [f(u), f(v)].$$

Once again, we have $\mathrm{Im}(Z_f) \subseteq \mathrm{Ker}\,\phi_*$.

Of course, Z_f is a 2-cocycle of L with values in the trivial L-module $\mathbb{F}_p$, and the cohomology class of Z_f in $H^2(L, \mathbb{F}_p)$ does not depend on the choice of f. Any 2-cocycle cohomologous to Z_f is equal to $Z_{f'}$ for another splitting f'; however f' is not necessarily an ω-splitting. It is important to know when the latter is the case.

Let us say that a map $C\colon L \times L \to \hat{L}$ is ω-graded if $C(L_i^\omega, L_j^\omega) \subseteq \hat{L}_{i+j}^\omega$ for $i, j \in \mathbb{N}$. Under the chosen identification of $\mathbb{F}_p$ with $\mathrm{Ker}\,\phi_*$, a map $C\colon L \times L \to \mathbb{F}_p$ is ω-graded if and only if $C(L_i^\omega, L_j^\omega) = 0$ whenever $i + j \neq c$ (since $\mathrm{Ker}\,\phi_* \subseteq \hat{L}_c^\omega$). Clearly, Z_f is an ω-graded 2-cocycle. Now define the graded cohomology group[3] $H^2_{gr}(L, \mathbb{F}_p)$ to be the quotient space of ω-graded 2-cocycles modulo ω-graded 2-coboundaries. It is easy to see that a 2-cocycle C is equal to $Z_{f'}$ for some ω-splitting f' if and only if

a) C is ω-graded,

b) C and Z_f represent the same class in $H^2_{gr}(L, \mathbb{F}_p)$.

Cohomological interpretation of $\mathfrak{z}_f$ will not be needed, but let us state it anyway. Define the left G-module structure on $\mathrm{Hom}(L, \mathbb{F}_p)$ in the usual way: given $l\colon L \to \mathbb{F}_p$ and $u \in L$, set $(g * l)(u) = l(u^g)$. One can check that the function from G to $\mathrm{Hom}(L, \mathbb{F}_p)$ given by $g \mapsto (u \mapsto \mathfrak{z}_f(g,u))$ is a 1-cocycle, and its cohomology class $[\mathfrak{z}_f] \in H^1(G, \mathrm{Hom}(L, \mathbb{F}_p))$ does not depend on f.

Definition: Let $C\colon L \times L \to \mathbb{F}_p$ and $\mathfrak{c}\colon G \times L \to \mathbb{F}_p$ be any maps. We will say that C and $\mathfrak{c}$ are **compatible** if

$$\mathfrak{c}(g, [u,v]) = C(u,v) - C(u^g, v^g), \quad \text{for any } g \in G \text{ and } u, v \in L. \tag{3.2}$$

The key relation between Lie algebra and group cohomology is provided by the following result.

3 This notion is introduced for expository purposes only. In the actual proof we will always work with cocycles and not their cohomology classes.

PROPOSITION 3.4: *The maps Z_f and $\mathfrak{z}_f$ are compatible.*

Proof: Note that G acts trivially on $\operatorname{Ker}\phi_*$, whence $Z_f(u,v)^g = Z_f(u,v)$ for all $u, v \in L$. Thus the right-hand side of (3.2) is equal to

$$\begin{aligned} Z_f(u,v)^g - Z_f(u^g, v^g) &= f([u,v])^g - [f(u), f(v)]^g - f([u^g, v^g]) + [f(u^g), f(v^g)] \\ &= f([u,v])^g - [f(u)^g, f(v)^g] - f([u,v]^g) + [f(u^g), f(v^g)] \\ &= \mathfrak{z}_f(g, [u,v]) - [f(u)^g, f(v)^g] + [f(u^g), f(v^g)]. \end{aligned}$$

Now $f(w)^g - f(w^g) \in \operatorname{Ker}\phi_*$ for any $w \in L$, and $\operatorname{Ker}\phi_*$ lies in the center of L. Therefore, $[f(u)^g, f(v)^g] = [f(u^g), f(v^g)]$, and we are done. ∎

The following simple observation is recorded here for future use.

CLAIM 3.5: *Let Ω be a subset of $L \times L$ such that if $(u,v) \in \Omega$, then*

$$(u^g, v^g) \in \Omega \quad \text{for any } g \in G.$$

If $C\colon L \times L \to \mathbb{F}_p$ and $\mathfrak{c}\colon G \times L \to \mathbb{F}_p$ are compatible, then the values of C on Ω determine the values of $\mathfrak{c}$ on $G \times \Omega'$, where $\Omega' = \{[u,v] \mid (u,v) \in \Omega\}$.

3.3 COMPUTING THE GROUP 1-COCYCLE $\mathfrak{z}_f$. Suppose now that we explicitly constructed ω-graded 2-cocycles $C_1, \dots, C_k$ whose cohomology classes form a basis for $H^2_{gr}(L, \mathbb{F}_p)$. Then for a suitable ω-splitting f we have $Z_f = \sum \lambda_i C_i$ for some $\lambda_i \in \mathbb{F}_p$. Proposition 3.4 enables us to write a formula for $\mathfrak{z} = \mathfrak{z}_f$ (or rather its restriction to $G \times [L,L]$) in terms of $\{\lambda_i\}$.

The next step is to find restrictions on the values of λ_i. These can be obtained by finding suitable pairs of commuting elements of G.

LEMMA 3.6: *Let g and h be commuting elements of G. Assume that $\deg_\omega(h^p) = c$ and let $u = \mathrm{LT}_\omega(h^p) \in L^\omega_c$. Then $\mathfrak{z}(g,u) = 0$.*

Proof: It is enough to show that $f(u)^g = f(u)$. Indeed, this would imply that $u^g = (\phi_* f(u))^g = \phi_*(f(u)^g) = \phi_*(f(u)) = u$, whence $f(u^g) = f(u)$.

Choose $\hat{g}, \hat{h} \in \hat{G}$ such that $\phi(\hat{h}) = h$ and $\phi(\hat{g}) = g$, and let $\hat{u} = \mathrm{LT}_\omega(\hat{h}^p)$. Clearly, $\hat{u} - f(u) \in \operatorname{Ker}\phi_*$. Since G acts trivially on $\operatorname{Ker}\phi_*$, $f(u)^g = f(u)$ if and only if $\hat{u}^g = \hat{u}$. The latter holds if and only if $(\hat{h}^p, \hat{g}) \in \gamma_{N+1}\hat{G}$. Let $k = (\hat{h}, \hat{g})$. It follows from the Hall-Petrescu formula (see [DDMS, Appendix A]) that $(\hat{h}^p, \hat{g}) = k^p w$ where w is a product of elements of the form $\{(k,s) \mid s \in \hat{G}\}$. Since g and h commute, $k \in \operatorname{Ker}\phi$. But $\operatorname{Ker}\phi$ is central in $\hat{G}$ and has order p. Therefore $k^p = w = 1$, whence $(\hat{h}^p, \hat{g}) = 1$. ∎

The objective is to find enough restrictions on the $\{\lambda_i\}$ to conclude that $\mathfrak{z}$ vanishes on $G \times U$, where $U = \gamma_{N-1}G/\gamma_{N+1}G \subset L_c^\omega$. The latter would contradict the following lemma.

LEMMA 3.7: *Let $U = \gamma_{N-1}G/\gamma_{N+1}G$, $V = \gamma_N G/\gamma_{N+1}G$, $\hat{U} = \gamma_{N-1}\hat{G}/\gamma_{N+1}\hat{G}$, $\hat{V} = \gamma_N\hat{G}/\gamma_{N+1}\hat{G}$ (note that $V \subset U \subset L_c^\omega$ and $\hat{V} \subset \hat{U} \subset \hat{L}_c^\omega$). The following hold:*

a) *$\hat{V}$ is the linear span of elements of the form $f(u)^g - f(u)$, where $u \in U$ and $g \in G$.*

b) *The restriction of $\mathfrak{z}$ to $G \times U$ is non-trivial.*

c) *The restriction of $\mathfrak{z}$ to $G \times V$ is trivial.*

Proof: a) First observe that $f(u)^g - f(u) \in \hat{V}$ for any $u \in U$ and $g \in G$, since $f(U) \subset \hat{U}$ and $\hat{u}^g - \hat{u} \in \hat{V}$ for any $\hat{u} \in \hat{U}$.

Given $\hat{v} \in \hat{V}$, let $h \in \gamma_N\hat{G}$ be such that $\mathrm{LT}_\omega(h) = \hat{v}$. There exist elements $h_i \in \gamma_{N-1}\hat{G}$ and $k_i \in \hat{G}$ such that $h \equiv \prod(h_i, k_i) \bmod \gamma_{N+1}\hat{G}$. Since $(h_i, k_i) = h_i^{-1}h_i^{k_i}$, we have

$$\hat{v} = \mathrm{LT}_\omega(h) = \sum(\hat{u}_i^{k_i} - \hat{u}_i) \quad \text{where } \hat{u}_i = \mathrm{LT}_\omega(h_i) \in \hat{U}.$$

Now let $u_i = \phi_*(\hat{u}_i) \in U$. Clearly, $\hat{u}_i - f(u_i) \in \operatorname{Ker}\phi_*$. Since $\hat{G}$ acts trivially on $\operatorname{Ker}\phi_*$, we conclude that $\hat{u}_i^{k_i} - \hat{u}_i = f(u_i)^{k_i} - f(u_i)$ which takes care of a).

b) Suppose that $\mathfrak{z}$ vanishes on $G \times U$. Then for any $u \in U$ and $g \in G$ we have $f(u)^g = f(u^g)$, whence $f(u)^g - f(u) = f(u^g - u)$. Since $u^g - u \in V$ for any $u \in U$, part a) implies that $\hat{V} \subseteq f(V)$. Since $\hat{V} \supset \operatorname{Ker}\phi_*$ and $\operatorname{Im} f \cap \operatorname{Ker}\phi_* = 0$, we conclude that $\operatorname{Ker}\phi_* = 0$, which is impossible.

c) This is very easy and left to the reader. ∎

Remark: The method we just described may fail or succeed depending on the choice of the number e (appearing in the definition of ω). In general, the larger e is, the more relations between $\{\lambda_i\}$ Lemma 3.6 yields. However, the dimension of the group $H^2(L, \mathbb{F}_p)$ also grows with increasing e. The optimal choice of e depends largely on G, but the basic guideline is that neither e nor N/e should be too small. As a rule, the larger N is, the easier it is to find a suitable value of e.

4. The group $SL_1(D)$

We start by reviewing the structure of division algebras over local fields. For more details the reader is referred to a paper of Riehm [Ri].

Let F be a local field of characteristic p. Let D be a finite-dimensional central division algebra over F and let d be the degree of D over F. Then there exists an unramified extension W of F of degree d, a generator σ of the Galois group $\mathrm{Gal}(W/F)$ and a uniformizer π of D such that

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

Denote by O_F, O_W and O_D the valuation rings of F, W and D, and by $\mathfrak{m}_F$, $\mathfrak{m}_W$, $\mathfrak{m}_D$ the corresponding maximal ideals. It is easy to see that $\tau := \pi^d$ is a uniformizer of F, so we have $\mathfrak{m}_D = \pi O_D$, $\mathfrak{m}_F = \tau O_F$ and $\mathfrak{m}_W = \tau O_W$.

Let $\mathbf{w}$ (resp. $\mathbf{f}$) be the residue field of W (resp. F). So $\mathbf{f} \cong \mathbb{F}_q$, where q is a power of p, and $\mathbf{w} \cong \mathbb{F}_{q^d}$. Let $\mathbf{f}_0$ be the prime subfield of $\mathbf{f}$ (so $\mathbf{f}_0 \cong \mathbb{F}_p$). We will denote the trace map of the extension $\mathbf{w}/\mathbf{f}$ (resp. $\mathbf{w}/\mathbf{f}_0$) by $\mathbf{tr}$ (resp. $\mathbf{tr}_0$).

Since F has characteristic p, we can canonically identify $\mathbf{f}$ (resp. $\mathbf{w}$) with a subfield of F (resp. W). We will also identify the Galois groups $\mathrm{Gal}(W/F)$ and $\mathrm{Gal}(\mathbf{w}/\mathbf{f})$ via the restriction map (which is an isomorphism). So we can write $F = \mathbf{f}((\tau))$, $W = \mathbf{w}((\tau))$, $O_F = \mathbf{f}[[\tau]]$ and $O_W = \mathbf{w}[[\tau]]$. Similarly, D can be identified (as a set) with Laurent series $\mathbf{w}((\pi))$. Using (4.1), it is easy to see that multiplication in D is given by the formula

$$\alpha\pi^i \cdot \beta\pi^j = \alpha\sigma^i(\beta)\pi^{i+j}, \quad \text{for } \alpha, \beta \in \mathbf{w} \text{ and } i, j \in \mathbb{Z}.$$

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 $GL_1^1(D) = \{g \in D^* \mid g \equiv 1 \bmod \mathfrak{m}_D\}$ and let $SL_1(D)$ be the group of elements of reduced norm one in D. The group $SL_1^1(D) = GL_1^1(D) \cap SL_1(D)$, which is an open pro-$p$ subgroup of $SL_1(D)$, will be our main object of study. For the rest of the paper we denote $SL_1^1(D)$ by G and $GL_1^1(D)$ by U. Let $\{U_i\}$ (resp. $\{G_i\}$) be the congruence filtration of U (resp. G), that is, set $U_i = \{g \in U \mid g \equiv 1 \bmod \mathfrak{m}_D^i\}$ and $G_i = G \cap U_i$. It is known that

$$\text{a) } G_i^p \subseteq G_{pi} \text{ for all } i \geq 1, \quad \text{b) } G_i = \gamma_i G \text{ for all } i \geq 1 \text{ unless } d = p = 2. \tag{4.2}$$

Let $\mathrm{Lie}(U)$ be the Lie algebra of U with the respect to the congruence filtration. It is easy to see that $\mathrm{Lie}(U)$ can be identified with the subalgebra $\mathbf{w}[\pi] \subset O_D$ via the map $\mathrm{LT}(1+\alpha\pi^i) \mapsto \alpha\pi^i$. Therefore, the Lie bracket on $\mathrm{Lie}(U)$ is given by the formula

$$[\lambda\pi^i, \mu\pi^j] = (\lambda\sigma^i(\mu) - \mu\sigma^j(\lambda))\pi^{i+j}.$$

The subalgebra $\mathrm{Lie}_U(G) = \bigoplus_{n=1}^{\infty}(G \cap U_n)U_{n+1}/U_{n+1}$ consists of elements of reduced trace zero in $\mathbf{w}[\pi]$. More explicitly, $\mathrm{Lie}_U(G) = \bigoplus_{n=1}^{\infty} M_n$, where $M_n = \mathbf{w}\pi^n$ if $d \nmid n$, and $M_n = \{\lambda\pi^n \mid \mathbf{tr}(\lambda) = 0\}$ if $d \mid n$.

Our next goal is to describe the Lie algebras of G with respect to various basic filtrations. These Lie algebras are similar to $\mathrm{Lie}_U(G)$, and they can be nicely embedded into certain associative algebras, which are defined below.

Fix integers N and e such that $1 \le e \le N$. Let $A = A(N,e)$ be the $\mathbb{F}_p$-vector space $\bigoplus_{i=0}^{N} \mathbf{w}x^i$ (where x is a formal variable) with the associative multiplication defined as follows. Given $i \in \mathbb{N}$, let $\varepsilon(i)$ be the remainder of i modulo e. For any $\alpha, \beta \in \mathbf{w}$ and $i, j \in \mathbb{N}$ we set

$$\alpha x^i \cdot \beta x^j = \begin{cases} \alpha\sigma^i(\beta)x^{i+j} & \text{if } \varepsilon(i)+\varepsilon(j) < e \text{ and } i+j \le N, \\ 0 & \text{otherwise.} \end{cases} \tag{4.3}$$

The associative algebra A has two natural gradings:

- thin grading $A = \bigoplus_{i=0}^{\infty} A_i$, where $A_i = \mathbf{w}x^i$ for $i \le N$ and $A_i = 0$ for $i \ge N$;
- thick grading $A = \bigoplus_{i=0}^{\infty} A_i^{\omega}$, where $A_i^{\omega} = \bigoplus_{j=ei}^{e(i+1)-1} A_j$.

Given $a \in A$, we write $\deg(a) = i$ (resp. $\deg_{\omega}(a) = i$) if $a \in A_i$ (resp. $a \in A_i^{\omega}$).

Below we list some of the key properties of A. Their proofs are straightforward and left to the reader. Recall that $\mathbf{tr}$ (resp. $\mathbf{tr}_0$) denotes the trace map of $\mathbf{w}/\mathbf{f}$ (resp. $\mathbf{w}/\mathbf{f}_0$).

(P1) The map $^-\colon O_D \to A$, defined by

$$g = \sum_{i=0}^{\infty} \alpha_i\pi^i \mapsto \overline{g} := \sum_{i=0}^{e-1} \alpha_i x^i,$$

is a homomorphism of associative algebras. Therefore, we can define an action of U on A by setting $a^g = \overline{g}^{-1}a\overline{g}$ for $a \in A$ and $g \in U$.

(P2) Let $I = \{i \in \mathbb{N} \mid i \le N \text{ and } d \mid i\}$. For every $i \in I$ define the function $\mathbf{T}_i\colon A \to \mathbb{F}_p$ as follows: if $a = \sum_{j=0}^{N} \alpha_j x^j$, set $\mathbf{T}_i(a) = \mathbf{tr}_0(\alpha_i)$. Each $\mathbf{T}_i$ is a *trace form*, that is, $\mathbf{T}_i(a+b) = \mathbf{T}_i(a) + \mathbf{T}_i(b)$ and $\mathbf{T}_i(ab) = \mathbf{T}_i(ba)$ for $a, b \in A$.

(P3) Consider A as a Lie algebra (with the usual bracket $[a,b]=ab-ba$). The subset $\mathfrak{sl}(A) := \{\sum_{i=0}^{N}\alpha_i x^i \mid \mathbf{tr}(\alpha_i)=0 \text{ for all } i \text{ divisible by } d\}$ is a Lie subalgebra of A, which is invariant under the action of U.

Now consider the filtrations $\{\omega_i U\}_{i=1}^{\infty}$ of U and $\{\omega_i G\}_{i=1}^{\infty}$ of G defined by setting $\omega_i U = U_{\min(ei,N+1)}$ and $\omega_i G = G_{\min(ei,N+1)}$. Let $L^{\omega}(G)$ (resp. $L^{\omega}(U)$) be the associated Lie algebra of G (resp. U). Clearly, $\omega_i G = \omega_i U \cap G$ for all i, and therefore, $L^{\omega}(G)$ can be canonically identified with a subalgebra of $L^{\omega}(U)$. Note that if $p \neq 2$ or $d \neq 2$, then $\{\omega_i G\}$ is the basic filtration of type (N,e) by (4.2)b).

PROPOSITION 4.1: *Let $A^+ = \bigoplus_{i=1}^{c} A_i^{\omega}$ and $\mathfrak{sl}(A)^+ = \mathfrak{sl}(A)\cap A^+$. Let $\psi : A^+ \to L^{\omega}(U)$ be the unique linear map such that $\psi(\alpha x^i) = \mathrm{LT}_{\omega}(1+\alpha\pi^i)$ for all $\alpha \in \mathbf{w}$ and $i \geq e$. Then ψ is an isomorphism of Lie algebras, which preserves the action of U. Moreover, $\psi(A_i^{\omega}) = \omega_i U/\omega_{i+1}U$ for all $i \geq 1$, and $\psi(\mathfrak{sl}(A)^+) = L^{\omega}(G)$.*

Proof: First we prove that ψ is a homomorphism. Take any $\alpha,\beta \in \mathbf{w}$ and $i,j \in \mathbb{N}$, with $e \leq i,j \leq N$. Let $u = \psi(\alpha x^i) = \mathrm{LT}_{\omega}(1+\alpha\pi^i)$ and $v = \psi(\beta x^j) = \mathrm{LT}_{\omega}(1+\beta\pi^j)$. Note that $u \in L_k^{\omega}(U)$ and $v \in L_l^{\omega}(U)$ where $k = [i/e]$ and $l = [j/e]$. By definition, $[u,v] = [\psi(\alpha x^i), \psi(\beta x^j)] = (1+\alpha\pi^i, 1+\beta\pi^j)\omega_{k+l+1}U$. It is easy to see that

$$(1+\alpha\pi^i, 1+\beta\pi^j) \equiv 1 + (\alpha\sigma^i(\beta) - \beta\sigma^j(\alpha))\pi^{i+j} \bmod U_{\min(i+2j,j+2i)}. \tag{4.4}$$

Since $i = ke+\varepsilon(i)$ and $j = le+\varepsilon(j)$, it is clear that $U_{\min(i+2j,j+2i)} \subseteq \omega_{k+l+1}U$.

Now $[u,v] \neq 0$ if and only if $(1+\alpha\pi^i, 1+\beta\pi^j) \notin \omega_{k+l+1}U$. By (4.4), the latter happens if and only if $\varepsilon(i)+\varepsilon(j) < e$, $i+j \leq N$ and $\alpha\sigma^i(\beta) - \beta\sigma^j(\alpha) \neq 0$. By (4.3), the last three conditions hold precisely when $[\alpha x^i, \beta x^j] \neq 0$. Thus $[u,v] = 0$ if and only if $[\alpha x^i, \beta x^j] = 0$. If $[u,v] \neq 0$, then $[u,v] = \mathrm{LT}_{\omega}(1 + (\alpha\sigma^i(\beta) - \beta\sigma^j(\alpha))\pi^{i+j})$ by (4.4). In either case, we conclude that $[u,v] = \psi([\alpha x^i, \beta x^j])$. So, ψ: $A^+ \to L^{\omega}(U)$ is a homomorphism of Lie algebras. Clearly ψ is bijective, since every element of $\omega_1 U$ is uniquely expressible in the form $\prod_{i\geq e}(1+\alpha_i\pi^i)$ for some $\alpha_i \in \mathbf{w}$. The facts that ψ preserves the U-action and $\psi(A_i^{\omega}) = \omega_i U/\omega_{i+1}U$ for $i \geq 1$ follow directly from definitions.

Now let us prove that ψ maps $\mathfrak{sl}(A)^+$ to $L^{\omega}(G)$. Fix $i \in \mathbb{N}$ and $\alpha \in \mathbf{w}$ such that $\alpha x^i \in \mathfrak{sl}(A)^+$. It will be enough to show that there exists $g = g(i,\alpha)$ of reduced norm 1 such that $g \equiv 1+\alpha\pi^i \bmod U_{2i}$.

First assume that $d \nmid i$. Let $h = 1+\alpha\pi^i$. A direct computation shows that $\mathrm{N}_{\mathrm{red}}(h) \equiv 1 \bmod U_m$, where m is the least common multiple of i and d; in particular, $m \geq 2i$. Since W/F is unramified, we have $\mathbf{N}_{W/F}(W \cap U_i) = F \cap U_i$

for all $i \geq 1$, where $\mathbf{N}_{W/F}$ is the norm map of W/F. Therefore, there exists $k \in W \cap U_m$ such that $\mathrm{N}_{\mathrm{red}}(k) = \mathrm{N}_{\mathrm{red}}(h)$, whence $g = hk^{-1}$ has the desired properties.

Now consider the case $d \mid i$. This time the assumption $\alpha x^i \in \mathfrak{sl}(A)^+$ yields $\mathbf{tr}(\alpha) = 0$. So, $\alpha = \sigma(\lambda) - \lambda$ for some $\lambda \in \mathbf{w}$. Let $h = 1 + \lambda\pi^i = 1 + \lambda\tau^{i/d}$, and let $g = \sigma(h)h^{-1} = (1 + \sigma(\lambda)\pi^i)(1 + \lambda\pi^i)^{-1}$. Since $h \in W$, we have $\mathrm{N}_{\mathrm{red}}(g) = \mathbf{N}_{W/F}(\sigma(h)h^{-1}) = 1$. On the other hand, $g \equiv 1 + (\sigma(\lambda) - \lambda)\pi^i \bmod U_{2i}$.

It remains to show $\psi(\mathfrak{sl}(A)^+)$ is the entire $L^\omega(G)$. If this was not the case, there would exist $g \in G$ such that $g \equiv 1 + \alpha\pi^i \bmod U_{i+1}$, where $d \mid i$ and $\mathbf{tr}(\alpha) \neq 0$. This is impossible since $\mathrm{N}_{\mathrm{red}}(U_{i+1}) \subseteq U_{i+1}$, $\mathrm{N}_{\mathrm{red}}(1 + \alpha\pi^i) = \mathbf{N}_{W/F}(1 + \alpha\pi^i)$ (as $d \mid i$) and $\mathbf{N}_{W/F}(1 + \alpha\pi^i) \equiv 1 + \mathbf{tr}(\alpha)\pi^i \bmod U_{i+1}$. ∎

5. Lie algebra cohomology

Our ultimate goal (which will be accomplished at the end of Section 6) is to prove the following theorem using the method described in Section 3:

THEOREM 5.1: *The depth of any elementary cover of $G = SL_1^1(D)$ does not exceed $100p^3d$.*

Throughout this section some restrictions on p and d will be made. The case $p = d = 2$ is excluded from our considerations here and will be dealt with in Section 8. When $p = d = 3$, or $p = 2$ and $d = 4$, the general scheme of the proof remains the same as in the "regular" case, but a couple of key results require different arguments. The proofs of those results in these exceptional cases are given in Section 7. Throughout the proof we shall use several facts about extensions of finite fields. These facts are collected in Section 9.

Fix an elementary cover $(\hat{G}, \phi)$ of G. Let $N = \mathrm{dep}(\hat{G}, \phi)$, and fix[4] a positive integer $e < N$. Let $\omega = \{\omega_i\}$ be the basic filtration of type (N, e), and let $c = [N/e]$. Throughout this section we write $L = L^\omega(G)$, $\hat{L} = L^\omega(\hat{G})$, and for $i \leq c$ we set $L_i^\omega = L_i^\omega(G) = \omega_i G/\omega_{i+1}G$ and $\hat{L}_i^\omega = L_i^\omega(\hat{G}) = \omega_i\hat{G}/\omega_{i+1}\hat{G}$. Given an ω-graded splitting $f\colon L \to \hat{L}$, let Z_f (resp. $\mathfrak{z}_f$) be the corresponding $\mathbb{F}_p$-valued 2-cocycle of L (resp. $\mathrm{Hom}(L, \mathbb{F}_p)$-valued 1-cocycle of G), as defined in Section 3. The goal of this section is to find an explicit formula for the restriction of Z_f to some large subset of $L \times L$ (under the assumption $N \geq 100p^3d$), and then use compatibility equation (3.2) to find a formula for $\mathfrak{z}_f$. In the next section we will show that the obtained formula leads to a contradiction using Lemma 3.6 and Lemma 3.7.

4 We will impose certain restrictions on the choice of e later in this section.

5.1 Cocycle descriptions. Let $A = A(N, e)$ be defined as in the previous section, and identify L with $\mathfrak{sl}^+(A)$ as in Proposition 4.1. For $e \le i \le N$ let $L_i = \mathbf{w}x^i \cap L$, that is,

$$L_i = \begin{cases} \mathbf{w}x^i & \text{if } d \nmid i; \\ \{\alpha x^i \mid \mathbf{tr}(\alpha) = 0\} & \text{if } d \mid i. \end{cases}$$

We also set $L_i = 0$ for $i > N$ and $i < e$. Note that

$$L_i = \{\mathrm{LT}_\omega(g) \mid g \in \gamma_i G \backslash \gamma_{i+1} G\} \cup \{0\} \quad \text{for } e \le i \le N. \tag{5.1}$$

Given a non-negative integer $n \le N$, let $\mathrm{d}_\omega(n) := [n/e]$. If $n > N$, set $\mathrm{d}_\omega(n) = \infty$. Then for $1 \le i \le c$ we have

$$L_i^\omega = \bigoplus_{\mathrm{d}_\omega(j) = i} L_j.$$

As in the previous section, let $\varepsilon(n)$ be the remainder of n modulo e. Thus, $\varepsilon(n) = n - \mathrm{d}_\omega(n)e$ for $0 \le n \le N$. It is natural to introduce the following definition.

Definition: A pair of non-negative integers (i, j) is **regular** if $i + j \le N$ and the following equivalent conditions hold:

a) $\mathrm{d}_\omega(i + j) = \mathrm{d}_\omega(i) + \mathrm{d}_\omega(j)$; b) $\varepsilon(i + j) = \varepsilon(i) + \varepsilon(j)$; c) $\varepsilon(i) + \varepsilon(j) < e$; d) $\varepsilon(i + j) \ge \varepsilon(i)$; e) $\varepsilon(i + j) \ge \varepsilon(j)$.

In view of (4.3), the formula for the Lie bracket in L can be written as follows:

$$[\alpha x^i, \beta x^j] = \begin{cases} (\alpha\sigma^i(\beta) - \beta\sigma^j(\alpha))x^{i+j} & \text{if } (i, j) \text{ is regular,} \\ 0 & \text{otherwise.} \end{cases}$$

Claim 5.2: *If the pair (i, j) is regular and j is prime to d, then $[L_i, L_j] = L_{i+j}$. If (i, j) is not regular, then $[L_i, L_j] = 0$.*

Proof: The first assertion follows from Lemma 9.4 if $d \nmid (i + j)$ and from Lemma 9.1 if $d \mid (i + j)$. The second assertion is obvious. ∎

Now recall that a bilinear map $C\colon L \times L \to \mathbb{F}_p$ is a 2-**cocycle**, if it satisfies the following two conditions:

$$C(u, u) = 0 \quad \text{for all } u \in L, \tag{5.2}$$

$$C([u, v], w) = C(u, [v, w]) - C(v, [u, w]) \quad \text{for all } u, v, w \in L. \tag{5.3}$$

A cocycle $B\colon L \times L \to \mathbb{F}_p$ is a **coboundary**, if there exists a linear function $h\colon L \to \mathbb{F}_p$ such that $B(x, y) = h([x, y])$ for all $x, y \in L$.

Definition: A bilinear map satisfying (5.3), but not necessarily (5.2), will be called a **semi-cocycle**.[5] We will refer to (5.3) as *the semi-cocycle identity.*

Next we introduce more auxiliary definitions.

Definition: Let $C\colon L \times L \to \mathbb{F}_p$ be a bilinear map.

a) Let I be a subset of $\mathbb{N}$. We will say that C is **supported on** I, if C vanishes on $L_i \times L_j$ whenever $i + j \notin I$. If C is supported on $\{n\}$ for some n, we will say that C is **homogeneous of weight** n (or simply of weight n).

b) C is **regular,** if C vanishes on $L_i \times L_j$ whenever (i, j) is NOT regular.

c) C is **admissible,** if there exists a function $\mathfrak{c}\colon G \times L \to \mathbb{F}_p$ linear in the second argument such that C and $\mathfrak{c}$ are compatible in the sense of (3.2).

Remark: Every coboundary is a regular map, since $[L_i, L_j] = 0$ whenever (i, j) is not regular.

Definition: Let $C\colon L \times L \to \mathbb{F}_p$ be a bilinear map. For every positive integer $n \leq N$ let $C_{|n}\colon L \times L \to \mathbb{F}_p$ be the unique bilinear map such that

$$C_{|n}(\alpha x^i, \beta x^j) = \begin{cases} C(\alpha x^i, \beta x^j) & \text{if } i + j = n \\ 0 & \text{if } i + j \neq n. \end{cases}$$

We will call $C_{|n}$ the **weight** n **component of** C.

Note that $C = \sum_{n=2e}^{N} C_{|n}$ and $C_{|n}$ is of weight n for every n. Moreover, C is a semi-cocycle (resp. cocycle, regular cocycle) if and only if each $C_{|n}$ is a semi-cocycle (resp. cocycle, regular cocycle). On the other hand, if C is admissible, $C_{|n}$ need not be admissible.

Claim 5.3: *Let f be an ω-splitting. Then Z_f is an admissible regular cocycle supported on the set $[ce, N] := \{i \mid ce \leq i \leq N\}$.*

Proof: Admissibility of Z_f is an immediate consequence of Proposition 3.4. Next we claim that $Z_{f_{|n}} = 0$ for $n < ce$. Indeed, let $u \in L_i$, $v \in L_j$, where $i+j < ce$. Then $Z_f(u, v) = f([u, v]) - [f(u), f(v)] \in \hat{L}^{\omega}_k$, where $k = \mathrm{d}_{\omega}(i+j) < c$. On the other hand, $Z_f(u, v) \in \operatorname{Ker} \phi_*$. Since $\operatorname{Ker} \phi_* \subset \hat{L}^{\omega}_c$, we conclude that $Z_f(u, v) = 0$.

It remains to prove that $Z_f(L_i, L_j) = 0$ whenever (i, j) is not regular (this will also imply that $Z_{f_{|n}} = 0$ for $n > N$). If $i > N$ (resp. $j > N$), then $L_i = 0$

5 The reason for using such terminology will be clear shortly.

(resp. $L_j = 0$), and there is nothing to prove. So, fix a pair (i, j) which is NOT regular, with $i, j \le N$, and set $k = \mathrm{d}_\omega(i)$ and $l = \mathrm{d}_\omega(j)$.

Let $u \in L_i$, $v \in L_j$. Choose $\hat{g}, \hat{h} \in \hat{G}$ such that $f(u) = \hat{g}\omega_{k+1}\hat{G}$ and $f(v) = \hat{h}\omega_{l+1}\hat{G}$, and let $g = \phi(\hat{g})$, $h = \phi(\hat{h})$. Then $u = \phi_*(\hat{g}\omega_{k+1}\hat{G}) = g\omega_{k+1}G$ and $v = h\omega_{l+1}H$. So, $\mathrm{LT}_\omega(g) \in L_i$ and $\mathrm{LT}_\omega(h) \in L_j$, whence $g \in \gamma_i G$ and $h \in \gamma_j G$ by (5.1). Since $\operatorname{Ker}\phi \subset \gamma_N\hat{G}$ (and $i, j \le N$), we have $\hat{g} \in \gamma_i\hat{G}$ and $\hat{h} \in \gamma_j\hat{G}$.

We are trying to prove that

$$f([u, v]) = [f(u), f(v)].$$

Since $[u, v] = \phi_*([f(u), f(v)])$, it will be enough to show that $[f(u), f(v)] = 0$. By definition,

$$[f(u), f(v)] = [\hat{g}\omega_{k+1}\hat{G}, \hat{h}\omega_{l+1}\hat{G}] = (\hat{g}, \hat{h})\omega_{k+l+1}\hat{G}.$$

Now $(\hat{g}, \hat{h}) \in \gamma_{i+j}\hat{G} \subseteq \omega_{\mathrm{d}_\omega(i+j)}\hat{G}$. Since (i, j) is not regular, $\mathrm{d}_\omega(i + j) \ge \mathrm{d}_\omega(i) + \mathrm{d}_\omega(j) + 1 = k + l + 1$. Therefore, $[f(u), f(v)] = 0$. ∎

So, we should try to describe regular homogeneous cocycles of weights in $[ce, N]$. The following proposition gives a method of constructing Lie algebra *semi-cocycles*.

PROPOSITION 5.4: *Let $\mathfrak{d}$ be a derivation of A, that is, $\mathfrak{d}(ab) = a\mathfrak{d}(b) + \mathfrak{d}(a)b$ for all $a, b \in A$. Let $n \le N$ be divisible by d. Then the function*

$$C = C_{\mathfrak{d},n} \colon L \times L \to \mathbb{F}_p$$

defined by $C(a, b) = \mathbf{T}_n(\mathfrak{d}(a)b)$ is a homogeneous semi-cocycle of weight n.

Proof: The assertion follows directly from the facts that $\mathbf{T}_n$ is linear and $\mathbf{T}_n(ab) = \mathbf{T}_n(ba)$ for all $a, b \in A$. ∎

The following notation is taken from [PR]: given $\lambda \in \mathbf{w}$ and $i \in \mathbb{Z}_{\ge 0}$, we set $\lambda(i) := \lambda + \sigma(\lambda) + \cdots + \sigma^{i-1}(\lambda)$. Now define two families $\{\mathfrak{d}_\lambda\}_{\lambda\in\mathbf{w}}$ and $\{\mathfrak{e}_\mu\}_{\mu\in\mathbf{f}}$ of derivations of A by setting

$$\mathfrak{d}_\lambda(\alpha x^i) = \lambda(i)\alpha x^i \quad \text{and} \quad \mathfrak{e}_\mu(\alpha x^i) = \alpha\mu\,\mathrm{d}_\omega(i)x^i.$$

For convenience we give special names to the corresponding semi-cocycles: $\mathcal{D}_{\lambda,n} = C_{\mathfrak{d}_\lambda,n}$ and $\mathcal{E}_{\mu,n} = C_{\mathfrak{e}_\mu,n}$. It is clear that

$$\mathcal{D}_{\lambda,n}(\alpha x^i, \beta x^j) = \begin{cases} \mathbf{tr}_0(\lambda(i)\alpha\sigma^i(\beta)) & \text{if } i + j = n \text{ and } (i, j) \text{ is regular} \\ 0 & \text{otherwise,} \end{cases}$$

$$\mathcal{E}_{\mu,n}(\alpha x^i, \beta x^j) = \begin{cases} \mathbf{tr}_0(\mu\,\mathrm{d}_\omega(i)\alpha\sigma^i(\beta)) & \text{if } i + j = n \text{ and } (i, j) \text{ is regular} \\ 0 & \text{otherwise.} \end{cases}$$

The next result tells us which of the above semi-cocycles are cocycles.

PROPOSITION 5.5: *Fix an integer n divisible by d, with $2e \le n \le N$. Assume, in addition, that $\varepsilon(n) \ge 2$. The following hold:*

a) *If $pd \mid n$, then $\mathcal{D}_{\lambda,n}$ is a cocycle for every $\lambda \in \mathbf{w}$. Moreover, if $\mathbf{tr}(\lambda) = \mathbf{tr}(\mu)$, then $\mathcal{D}_{\lambda,n} - \mathcal{D}_{\mu,n}$ is a coboundary.*

b) *If $pd \nmid n$, then $\mathcal{D}_{\lambda,n}$ is a cocycle if and only if $\mathbf{tr}(\lambda) = 0$. Every such cocycle is a coboundary.*

c) *$\mathcal{E}_{\mu,n}$ is a cocycle if and only if $\mathrm{d}_\omega(n)$ is divisible by p or $\mu = 0$.*

Proof: a) First assume that $p \ne 2$. Fix $\lambda \in \mathbf{w}$, and let $C = \mathcal{D}_{\lambda,n}$. To prove that C is a cocycle, it suffices to show that $C(u,v) + C(v,u) = 0$ for all $u, v \in L$ such that $u = \alpha x^i$, $v = \beta x^{n-i}$, where $\alpha, \beta \in \mathbf{w}$ and the pair $(i, n-i)$ is regular. We have

(5.4)

$$\begin{aligned} C(u,v) + C(v,u) &= \mathbf{tr}_0(\lambda(i)\alpha\sigma^i(\beta)) + \mathbf{tr}_0(\lambda(n-i)\beta\sigma^{n-i}(\alpha)) \\ &= \mathbf{tr}_0(\lambda(i)\alpha\sigma^i(\beta)) + \mathbf{tr}_0(\sigma^i(\lambda(n-i))\sigma^i(\beta)\sigma^n(\alpha)) \\ &\qquad\qquad \text{since } \mathbf{tr}_0 \text{ is } \sigma\text{-invariant} \\ &= \mathbf{tr}_0((\lambda(i) + \sigma^i(\lambda(n-i)))\alpha\sigma^i(\beta)) \\ &\qquad\qquad \text{since } \sigma^n(\alpha) = \alpha \text{ (as } d \mid n). \end{aligned}$$

Now $\lambda(i) + \sigma^i(\lambda(n-i)) = \lambda(n) = n/d\ \mathbf{tr}(\lambda) = 0$ since n/d is divisible by p. Thus we proved the first assertion.

Now assume that $\mathbf{tr}(\lambda) = 0$. Then $\lambda = \nu - \sigma(\nu)$ for some ν, and therefore $\lambda(i) = \nu - \sigma^i(\nu)$. We have

$$C(u,v) = C(\alpha x^i, \beta x^{n-i}) = \mathbf{tr}_0((\nu - \sigma^i(\nu))\alpha\sigma^i(\beta)) = \mathbf{tr}_0(\nu(\alpha\sigma^i(\beta) - \sigma^{-i}(\alpha)\beta)).$$

On the other hand, $[u,v] = (\alpha\sigma^i(\beta) - \sigma^{n-i}(\alpha)\beta)x^n$. Thus $C(u,v) = h([u,v])$, where $h(a)$ is equal to $\mathbf{f}_0$-trace of the coefficient of x^n in νa. Therefore, C is a coboundary.

Finally, if $\lambda, \mu \in \mathbf{w}$ are arbitrary and $\mathbf{tr}(\lambda) = \mathbf{tr}(\mu)$, then $\mathcal{D}_{\lambda,n} - \mathcal{D}_{\mu,n} = \mathcal{D}_{\lambda-\mu,n}$ is a coboundary by the above argument.

Now consider the case $p = 2$ (in which case the identity $C(u,v) + C(v,u) = 0$ does not imply that $C(u,u) = 0$). Since C is bilinear and has weight n, it suffices to show that $C(u,u) = 0$ for $u \in L_{n/2}$. Recall that $n = 2dm$ for some m. If $u \in L_{n/2}$, then $u = \alpha x^{dm}$, where $\mathbf{tr}(\alpha) = 0$. Therefore,

$$\begin{aligned} C(u,u) &= \mathbf{tr}_0(\lambda(dm)\alpha\sigma^{dm}(\alpha)) = \mathbf{tr}_0(m\mathbf{tr}(\lambda)\alpha^2) = \mathbf{tr}_{\mathbf{f}/\mathbf{f}_0}(\mathbf{tr}(m\mathbf{tr}(\lambda)\alpha^2)) \\ &= \mathbf{tr}_{\mathbf{f}/\mathbf{f}_0}(m\mathbf{tr}(\lambda)\mathbf{tr}(\alpha^2)) = 0 \quad \text{since } \mathbf{tr}(\alpha^2) = (\mathbf{tr}\alpha)^2. \end{aligned}$$

b) The assertion follows immediately from the calculations in the proof of part a). Here is where we use the assumption $\varepsilon(n) \geq 2$ — it ensures that there exists a regular pair $(i, n-i)$ with $d \nmid i$ and $d \nmid (n-i)$, whence one can use arbitrary α and β in (5.4). The case $p = 2$ does not require special consideration.

c) Let $C = \mathcal{E}_{\mu,n}$. Let $u = \alpha x^i$, $v = \beta x^{n-i}$, where $(i, n-i)$ is regular. Since $\mu \in \mathbf{f}$, we have

$$\begin{aligned} C(u,v) + C(v,u) &= \mathbf{tr}_0(\mu\, \mathrm{d}_\omega(i)\alpha\sigma^i(\beta)) + \mathbf{tr}_0(\mu\, \mathrm{d}_\omega(n-i)\beta\sigma^{n-i}(\alpha)) \\ &= \mathbf{tr}_0(\mu(\mathrm{d}_\omega(i) + \mathrm{d}_\omega(n-i))\alpha\sigma^i(\beta)) = \mathbf{tr}_0(\mu\, \mathrm{d}_\omega(n)\alpha\sigma^i(\beta)). \end{aligned}$$

The above expression vanishes for all α, β and i if and only if $p \mid \mathrm{d}_\omega(n)$ or $\mu = 0$, so we are done if $p \neq 2$. If $p = 2$, we can use the same argument as in the proof of part a). ∎

From now on we assume that $N \geq 100p^3d$ and e satisfies the conclusion of the following claim (whose verification is left to the reader).

Claim 5.6: *If $N \geq 100p^3d$, we can choose e so that the following conditions hold:* a) $pd \mid e$, b) $[N/e] = 4p$ *(that is, $c = 4p$) and* c) $\varepsilon(N) \geq p + 100$.

Let $I_{good} = [2e, (c-1)e - 1] = \{i \in \mathbb{N} \mid 2 \leq \mathrm{d}_\omega(i) \leq c-2\}$, and let $L_{good} = \bigoplus_{i \in I_{good}} L_i = \bigoplus_{k=2}^{c-2} L_k^\omega$. The main part of this section will be devoted to the proof of the following result.

Theorem 5.7: *Fix n such that $ce + 2 \leq n \leq N$, and let C be a regular cocycle of weight n. If the pair (p, d) is equal to $(2, 4)$ or $(3, 3)$, assume in addition that $n \geq N - p$ and C is the weight n component of some regular admissible cocycle Z.*

a) *If $d \nmid n$, there exists a coboundary B of weight n which coincides with C on $L_{good} \times L_{good}$.*

b) *If $d \mid n$, there exist $\mu \in \mathbf{w}$ and $\nu \in \mathbf{f}$ such that C and $\mathcal{D}_{\mu,n} + \mathcal{E}_{\nu,n}$ coincide on $L_{good} \times L_{good}$.*

5.2 Proof of Theorem 5.7a). We will use the following shortcut notations:

$$C_i(\alpha, \beta) = C(\alpha x^i, \beta x^{n-i}) \quad \text{for } e \leq i \leq n - e$$

and

$$\lambda[i] = \sigma^i(\lambda) - \lambda \quad \text{for } \lambda \in \mathbf{w}, i \in \mathbb{Z}.$$

Fix $\eta_0 \in \mathbf{w}$ such that $\mathbf{tr}(\eta_0) = 0$ and η_0 generates $\mathbf{w}$ as a field over $\mathbf{f}$ (such η_0 exists by Lemma 9.1). We claim that the map $\alpha x^{n-e} \mapsto [\alpha x^{n-e}, \eta_0 x^e]$ from

L_{n-e} to L_n is injective. Indeed,

$$[\alpha x^{n-e}, \eta_0 x^e] = \Big(\alpha\sigma^{n-e}(\eta_0) - \sigma^e(\alpha)\eta_0\Big)x^n = \alpha(\sigma^n(\eta_0) - \eta_0)x^n$$
$$= \alpha \cdot \eta_0[n]x^n \quad (\text{as } d \mid e)$$

and $\eta_0[n] \neq 0$ since $d \nmid n$. Therefore, there exists a coboundary B of weight n such that $C(\alpha x^{n-e}, \eta_0 x^e) = B(\alpha x^{n-e}, \eta_0 x^e)$ for all $\alpha \in \mathbf{w}$. Clearly, it is enough to prove the theorem for $C - B$ instead of C (note that $C - B$ is also regular since every coboundary is regular). Thus, after replacing C by $C - B$, we can assume that

$$C(\alpha x^{n-e}, \eta_0 x^e) = 0 \quad \text{for all } \alpha \in \mathbf{w}. \tag{5.5}$$

We are going to deduce from (5.5) that C vanishes on $L_{good} \times L_{good}$.

CLAIM 5.8: *Suppose that $d \mid i$ and $1 \leq \mathrm{d}_\omega(i) \leq c-2$. Then C_i is identically zero.*

Proof: First of all, we can assume that $(i, n-i)$ is regular (otherwise $C_i = 0$ because C is regular). Since $\mathrm{d}_\omega(i) \leq c-2$, we have $\mathrm{d}_\omega(n-i) = \mathrm{d}_\omega(n) - \mathrm{d}_\omega(i) \geq 2$, whence $n - i - e \geq e$. Thus given $\alpha, \beta \in \mathbf{w}$, with $\mathbf{tr}(\alpha) = 0$, we have

$$C_i(\alpha, \beta) = C(\alpha x^i, \beta x^{n-i}) = C\Big(\alpha x^i, \Big[\frac{\beta}{\eta_0[n-i]}x^{n-i-e}, \eta_0 x^e\Big]\Big)$$
$$= C\Big(\Big[\alpha x^i, \frac{\beta}{\eta_0[n-i]}x^{n-i-e}\Big], \eta_0 x^e\Big) + C\Big(\frac{\beta}{\eta[n-i]}x^{n-i-e}, [\alpha x^i, \eta_0 x^e]\Big)$$
$$= 0.$$

The first summand in the last expression is equal to zero by (5.5), and the second summand is zero because $[\alpha x^i, \eta_0 x^e] = 0$ (as $d \mid i$). ∎

Note that if $i \in I_{good}$, then $1 \leq \mathrm{d}_\omega(n-i) \leq c-2$. Since C is skew-symmetric, it follows from Claim 5.8 that $C_i = 0$ whenever $i \in I_{good}$ and either $d \mid (n-i)$ or $d \mid i$. It remains to prove that $C_i = 0$ for every $i \in I_{good}$ such that $d \nmid i$, $d \nmid (n-i)$.

LEMMA 5.9: *The following hold:*

a) *Let $i \in I_{good}$, and let $\alpha, \beta, \eta \in \mathbf{w}$, with $\mathbf{tr}(\eta) = 0$. Then*

$$C_i(\alpha \cdot \eta[i], \beta) = -C_i(\alpha, \beta \cdot \eta[n-i]). \tag{5.6}$$

b) *Let $i, i' \in \mathbb{N}$ be such that $i' \equiv_d i$. Assume in addition that $e \leq i < i' \leq n-e$, $d \nmid i$, $d \nmid (n-i)$ and $\varepsilon(i) \leq \varepsilon(i') \leq \varepsilon(n)$. Then $C_i = C_{i'}$.*

First we will prove an auxiliary statement:

CLAIM 5.10: *Let i and i' satisfy the hypotheses of Lemma 5.9b), and assume that $\mathrm{d}_\omega(i'-i)>0$. Then for any $\alpha,\beta,\eta\in\mathbf{w}$, with $\mathbf{tr}(\eta)=0$, we have*

$$C_{i'}(\alpha\cdot\eta[i],\beta)=C_i(\alpha,-\beta\cdot\eta[n-i]). \tag{5.7}$$

Proof: Applying the semi-cocycle identity we have

$$C([\alpha x^i,\eta x^{i'-i}],\beta x^{n-i'})=C(\alpha x^i,[\eta x^{i'-i},\beta x^{n-i'}])-C(\eta x^{i'-i},[\alpha x^i,\beta x^{n-i'}]). \tag{5.8}$$

Since $\varepsilon(i)\le\varepsilon(i')\le\varepsilon(n)$, the pairs $(i,n-i)$, $(i',n-i')$ and $(i,i'-i)$ are regular. Since $d\mid(i'-i)$, we have $[\alpha x^i,\eta x^{i'-i}]=\alpha\cdot\eta[i]x^{i'}$ and $[\eta x^{i'-i},\beta x^{n-i'}]=-\beta\cdot\eta[n-i]x^{n-i}$. The second summand on the right-hand side of (5.8) vanishes by Claim 5.8, and (5.7) follows. ∎

Proof of Lemma 5.9: a) We can assume that $(i,n-i)$ is regular (otherwise the result is trivial). Applying (5.7) three times, we get

$$C_i(\alpha\cdot\eta[i],\beta)=-C_{i+e}(\alpha,\beta\cdot\eta[n-i])=C_{i-e}(\alpha\cdot\eta[i],\beta)=-C_i(\alpha,\beta\cdot\eta[n-i]).$$

b) If $\mathrm{d}_\omega(i'-i)>0$ and either $i\in I_{good}$ or $i'\in I_{good}$, the result follows immediately from (5.6) and (5.7) (since $d\nmid i$ and $d\nmid(n-i)$, there exists η, with $\mathbf{tr}(\eta)=0$, such that $\eta[i]\ne0$ and $\eta[n-i]\ne0$).

In the general case, choose $a\ne0$ such that $i-ae\in I_{good}$. If $a>0$, we have $C_i=C_{i-ae}=C_{i'}$ by the above argument. If $a<0$, we have $C_i=C_{i'-ae}=C_{i'}$. ∎

Conclusion of the proof of Theorem 5.7a): From now on we fix $i\in I_{good}$ such that $d\nmid i$, $d\nmid(n-i)$ and $(i,n-i)$ is regular. Let $D=C_i$. We want to prove that $D=0$. The cases $p=2$ and $p>2$ will be treated in slightly different ways. Both arguments are based on the same idea, but the one in the case $p=2$ requires more computations. The exceptional cases $(p,d)=(3,3)$ or $(2,4)$ will be considered in Section 7.

CASE 1: $p>2$. Let $\eta_1,\eta_2\in\mathbf{w}$ be such that $\mathbf{tr}(\eta_1)=\mathbf{tr}(\eta_2)=0$ and η_2 generates $\mathbf{w}/\mathbf{f}$ (so that $\eta_2[j]\ne0$ if $d\nmid j$). By (5.6) we have

$$D\Big(\alpha\cdot\frac{\eta_1[i]}{\eta_2[i]},\beta\Big)=-D\Big(\frac{\alpha}{\eta_2[i]},\beta\cdot\eta_1[n-i]\Big)=D\Big(\alpha,\beta\cdot\frac{\eta_1[n-i]}{\eta_2[n-i]}\Big). \tag{5.9}$$

By Lemma 9.2, we can choose η_1,η_2 as above and $\eta\in\mathbf{w}$ such that $\eta-\eta_2\in\mathbf{f}$ and $\eta^2-\eta_1\in\mathbf{f}$. For every j not divisible by d we have $\eta_1[j]=\eta^2[j]$, $\eta_2[j]=\eta[j]$, and so $\eta_1[j]/\eta_2[j]=\sigma^j(\eta)+\eta$. Equation (5.9) can now be written as

$$D(\alpha(\sigma^i(\eta)+\eta),\beta)=D(\alpha,\beta(\sigma^{n-i}(\eta)+\eta)).$$

Lemma 5.9a) yields

$$D(\alpha(\sigma^i(\eta)-\eta),\beta) = -D(\alpha,\beta(\sigma^{n-i}(\eta)-\eta)).$$

Taking half-sum and half-difference of the last two equations, we get

$$D(\alpha\sigma^i(\eta),\beta) = D(\alpha,\beta\eta), \tag{5.10}$$

$$D(\alpha\eta,\beta) = D(\alpha,\beta\sigma^{n-i}(\eta)). \tag{5.11}$$

It is easy to see that if η, η_1, η_2 are replaced by $\sigma^i(\eta), \sigma^i(\eta_1), \sigma^i(\eta_2)$, respectively, the whole argument can be repeated. Replacing η by $\sigma^i(\eta)$ in (5.11), we have

$$D(\alpha\sigma^i(\eta),\beta) = D(\alpha,\beta\sigma^n(\eta)). \tag{5.12}$$

Subtracting (5.10) from (5.12), we get

$$D(\alpha,\beta\cdot\eta[n]) = 0.$$

Now $\eta[n] \neq 0$ since $d \nmid n$, and it follows that D is identically zero. The proof in the case $p > 2$ is complete.

Case 2: $p = 2$. Let

$$\mathfrak{R} = \{(\lambda,\mu) \in \mathbf{w}\times\mathbf{w} \mid D(\alpha\lambda,\beta) = D(\alpha,\beta\mu) \text{ for all } \alpha,\beta \in \mathbf{w}\}.$$

Clearly, $\mathfrak{R}$ is a subring of $\mathbf{w}\times\mathbf{w}$. Moreover, if $(\lambda,\mu) \in \mathfrak{R}$, $(\lambda',\mu') \in \mathfrak{R}$, with $\lambda,\mu \neq 0$, then $(\lambda'/\lambda, \mu'/\mu) \in \mathfrak{R}$. Lemma 5.9a) implies that $(\eta[i],\eta[n-i]) \in \mathfrak{R}$ if $\mathbf{tr}(\eta) = 0$. It follows that $(\lambda,\lambda) \in \mathfrak{R}$ for all $\lambda \in \mathbf{f}$.

Now fix $\eta,\eta_1,\eta_2 \in \mathbf{w}$ such that $\eta-\eta_1 \in \mathbf{f}, \eta^{-1}-\eta_2 \in \mathbf{f}$, $\mathbf{tr}(\eta_1) = \mathbf{tr}(\eta_2) = 0$ and η generates $\mathbf{w}/\mathbf{f}$ (existence of such elements is proved in Lemma 9.2). Since $\eta[j] = \eta_1[j]$, $\eta^{-1}[j] = \eta_2[j]$ for all j, Lemma 5.9a) yields $(\eta[i],\eta[n-i]) \in \mathfrak{R}$ and $(\eta^{-1}[i],\eta^{-1}[n-i]) \in \mathfrak{R}$, whence $(\frac{\eta[i]}{\eta^{-1}[i]}, \frac{\eta[n-i]}{\eta^{-1}[n-i]}) \in \mathfrak{R}$. But $\frac{\eta[j]}{\eta^{-1}[j]} = \frac{\eta+\sigma^j(\eta)}{\eta^{-1}+\sigma^j(\eta^{-1})} = \eta\sigma^j(\eta)$ if $d \nmid j$. Therefore, $(\eta\sigma^i(\eta),\eta\sigma^{n-i}(\eta)) \in \mathfrak{R}$, that is,

$$D(\alpha\eta\sigma^i(\eta),\beta) = D(\alpha,\eta\sigma^{n-i}(\eta)\beta) \quad \text{for all } \alpha,\beta \in \mathbf{w}. \tag{5.13}$$

Now let $E(\alpha,\beta) = D(\alpha\eta,\beta) - D(\alpha,\eta\beta)$. We shall first prove that E is identically zero and then deduce that $D = 0$ unless $i \equiv_d (n-i)$. Rewrite (5.6) as follows:

$$D(\alpha\sigma^i(\eta),\beta) - D(\alpha\eta,\beta) = D(\alpha,\beta\sigma^{n-i}(\eta)) - D(\alpha,\beta\eta).$$

Therefore,

$$E(\alpha,\beta) = D(\alpha\eta,\beta) - D(\alpha,\beta\eta) = D(\alpha\sigma^i(\eta),\beta) - D(\alpha,\beta\sigma^{n-i}(\eta))$$
$$= D(\alpha\sigma^i(\eta),\beta) - D(\alpha\eta\sigma^i(\eta),\beta/\eta) = E(\alpha\sigma^i(\eta),\beta/\eta),$$

where we used (5.13) at the next to last step. So, for all $\alpha,\beta \in \mathbf{w}$ we have

$$E(\alpha,\eta\beta) = E(\alpha\sigma^i(\eta),\beta). \tag{5.14}$$

Similarly, one can show that

$$E(\alpha\eta,\beta) = E(\alpha,\sigma^{n-i}(\eta)\beta). \tag{5.15}$$

Now let $\mathfrak{S} = \{\xi \in \mathbf{w} \mid E(\alpha,\beta\xi) = E(\alpha\sigma^i(\xi),\beta) \text{ for all } \alpha,\beta \in \mathbf{w}\}$. Clearly, $\mathfrak{S}$ is an $\mathbf{f}$-subalgebra of $\mathbf{w}$. Formula (5.14) implies that $\eta \in \mathfrak{S}$, and since η generates $\mathbf{w}/\mathbf{f}$, we have $\mathfrak{S} = \mathbf{w}$.

It follows that $E(\alpha,\beta)$ depends only on $\alpha\sigma^i(\beta)$. Since the map $(\mu,\nu) \mapsto \mathbf{tr}_0(\mu\nu)$ is a non-degenerate $\mathbb{F}_p$-valued bilinear form on $\mathbf{w}\times\mathbf{w}$, we conclude that $E(\alpha,\beta) = \mathbf{tr}_0(\lambda\alpha\sigma^i(\beta))$ for some $\lambda \in \mathbf{w}$. Similarly, (5.15) implies that $E(\alpha,\beta) = \mathbf{tr}_0(\lambda'\alpha\sigma^{i-n}(\beta))$ for some $\lambda' \in \mathbf{w}$.

Setting $\beta = 1$ in the above formulas, we have $\mathbf{tr}_0(\lambda\alpha) = \mathbf{tr}_0(\lambda'\alpha)$ for all $\alpha \in \mathbf{w}$, whence $\lambda = \lambda'$. Therefore, $\mathbf{tr}_0(\lambda\alpha(\sigma^i(\beta) - \sigma^{i-n}(\beta))) = 0$ for all $\alpha,\beta \in \mathbf{w}$. Since $d \nmid n$, there exists $\beta \in \mathbf{w}$ such that $\sigma^i(\beta) - \sigma^{i-n}(\beta) \neq 0$. Therefore, $\lambda = 0$ and E is identically zero.

Thus, we proved that

$$D(\alpha\eta,\beta) = D(\alpha,\eta\beta) \quad \text{for all } \alpha,\beta \in \mathbf{w}. \tag{5.16}$$

Combining this with (5.13), we get

$$D(\alpha\sigma^i(\eta),\beta) = D(\alpha,\sigma^{n-i}(\eta)\beta) \quad \text{for all } \alpha,\beta \in \mathbf{w}. \tag{5.17}$$

Arguing as in the case $p > 2$, we conclude from (5.16) and (5.17) that $D = 0$ unless $i \equiv_d (n-i)$.

Suppose now that $i \equiv_d (n-i)$. Using Lemma 5.9b), we can assume that $\varepsilon(i) > d$. Let $j = 1$ or $d-1$ be such that $d \nmid 2(j-i)$ (such j exists unless $d = 2$ or $d = 4$). The commutator map $L_{i-e-j} \times L_{e+j} \to L_i$ is surjective by Claim 5.2, since $j \equiv_d \pm 1$ and $(i-e-j, e+j)$ is regular. According to the semi-cocycle identity (5.3), C vanishes on $L_i \times L_{n-i}$ as long as C vanishes on $L_{i-e-j} \times L_{n-i+e+j}$ and on $L_{e+j} \times L_{n-e-j}$. The latter holds, as we just proved, unless $(i-j) \equiv_d (n-i+j)$ or $j \equiv_d (n-j)$. Either of the last two conditions would contradict our assumptions. The proof is complete. ∎

5.3 Proof of Theorem 5.7b).

Remark: Apart from the cases $p = d = 3$ and $p = 2$, $d = 4$, we will never use skew-symmetry of C, so the assertion of Theorem 5.7b) holds if C is only assumed to be a semi-cocycle.

Lemma 5.11: *Let* $I_{reg} = \{i \in \mathbb{N} \mid e \le i \le n-e, (i, n-i)$ *is regular and* $d \nmid i\}$.

a) *Let* $i, j \in I_{reg}$, *and assume that* $i < j$, $\varepsilon(i) \le \varepsilon(j)$, $pd \mid (j-i)$ *and* $p \mid \mathrm{d}_\omega(j-i)$. *Then* $C_i = C_j$.

b)[6] *For every* $i \in I_{reg}$, *with* $i \equiv_d 1$, *there exists* $\lambda_i \in \mathbf{w}$ *such that*

$$C_i(\alpha, \beta) = \mathbf{tr}_0(\lambda_i \alpha\sigma(\beta)) \quad \textit{for all } \alpha, \beta \in \mathbf{w}.$$

Proof: a) Let k and l be such that

$$(5.18)\quad d \mid l,\ k \equiv_d i,\ e \le k, l, n-k-l,\ \varepsilon(k)+\varepsilon(l) = \varepsilon(k+l) \text{ and } \varepsilon(k+l) < \varepsilon(n)$$

(the last two conditions imply that the pairs (k, l), $(k, n-k-l)$ and $(l, n-k-l)$ are regular). Applying the semi-cocycle identity to the triple αx^k, ηx^l and βx^{n-k-l} (where $\mathbf{tr}(\eta) = 0$) and simplifying, we have

$$(5.19)\qquad C_{k+l}(\alpha\eta[i], \beta) = C_k(\alpha, (-\eta[-i])\beta)) + C_l(\eta, \{\alpha\sigma^i(\beta)\}[-i]).$$

Let $\xi = -\eta[-i]$. Then $\eta[i] = \sigma^i(\xi)$, and the last equation can be rewritten as follows:

$$(5.20)\qquad C_{k+l}(\alpha\sigma^i(\xi), \beta) = C_k(\alpha, \beta\xi) + C_l(\eta, \{\alpha\sigma^i(\beta)\}[-i]).$$

Now suppose that $i \le n - 3e$. Applications of (5.20) yield

$$\begin{aligned} C_{i+2e}(\alpha(\sigma^i(\xi))^2, \beta/\xi) &= C_i(\alpha\sigma^i(\xi), \beta) + C_{2e}(\eta, \{\alpha\sigma^i(\beta)\}[-i]) \quad \text{and} \\ C_{i+2e}(\alpha(\sigma^i(\xi))^2, \beta/\xi) &= C_{i+e}(\alpha\sigma^i(\xi), \beta) + C_e(\eta, \{\alpha\sigma^i(\beta)\}[-i]) \\ &= C_i(\alpha, \beta\xi) + 2C_e(\eta, \{\alpha\sigma^i(\beta)\}[-i]). \end{aligned}$$

Combining these formulas, we conclude that

$$C_i(\alpha\sigma^i(\xi), \beta) = C_i(\alpha, \beta\xi) + R(\alpha\sigma^i(\beta)) \quad \text{for some function } R\colon \mathbf{w} \to \mathbb{F}_p.$$

Replacing α by $\alpha\sigma^i(\xi)$, we get

$$C_i(\alpha(\sigma^i(\xi))^2, \beta) = C_i(\alpha\sigma^i(\xi), \beta\xi) + R(\alpha\sigma^i(\beta\xi)) = C_i(\alpha, \beta\xi^2) + 2R(\alpha\sigma^i(\beta\xi)).$$

6 In the cases $p = d = 3$ and $p = 2, d = 4$, the assertion of Lemma 5.11b) will be proved in Section7.

By induction we have $C_i(\alpha\sigma^i(\xi^m),\beta) = C_i(\alpha,\beta\xi^m) + mR(\alpha\sigma^i(\beta\xi^{m-1}))$ for any $m \geq 1$. Setting $m = q^d = \mathrm{card}(\mathbf{w})$ and noting that $\xi^m = \xi$, we get

$$C_i(\alpha\sigma^i(\xi),\beta) = C_i(\alpha,\beta\xi). \tag{5.21}$$

Case 1: $\mathrm{d}_\omega(i) < \mathrm{d}_\omega(j)$. Our assumptions imply that $i \leq j-pe \leq n-(p+1)e \leq n-3e$, whence (5.21) holds. Now let $k = i$ and $l = (j-i)/p$. It is easy to check that conditions (5.18) are satisfied. Applying (5.20) and combining the result with (5.21), we get

$$C_{i+l}(\alpha\sigma^i(\xi),\beta) = C_i(\alpha\sigma^i(\xi),\beta) + C_l(\eta,\{\alpha\sigma^i(\beta)\}[-i]). \tag{5.22}$$

Arguing as before, we have

$$C_{i+pl}(\alpha\sigma^i(\xi),\beta) = C_i(\alpha\sigma^i(\xi),\beta) + pC_l(\eta,\{\alpha\sigma^i(\beta)\}[-i]) = C_i(\alpha\sigma^i(\xi),\beta).$$

Now recall that $\xi = \eta - \sigma^{-i}(\eta)$. Since $d \nmid i$, we can choose η so that $\xi \neq 0$. Thus we showed that $C_{i+pl} = C_i$.

Case 2: $\mathrm{d}_\omega(i) = \mathrm{d}_\omega(j)$. If $\mathrm{d}_\omega(i) \geq p+2$, it follows from case 1 that $C_i = C_{i-pe}$ and $C_{i-pe} = C_j$. If $\mathrm{d}_\omega(i) < p+2$, we have $C_i = C_{j+pe} = C_j$.

b) Let $\Lambda = \{\lambda \in \mathbf{w} \mid C_i(\alpha\sigma(\lambda),\beta) = C_i(\alpha,\beta\lambda) \text{ for all } \alpha,\beta \in \mathbf{w}\}$. Clearly, Λ is a subring of $\mathbf{w}$. Since $i \equiv_d 1$, (5.21) implies that Λ contains all elements of the form $\sigma(\eta) - \eta$, with $\mathbf{tr}(\eta) = 0$. Since $(p,d) \neq (3,3)$ or $(2,4)$, we have $\Lambda = \mathbf{w}$ by Lemma 9.3.[7] Therefore, $C_i(\alpha,\beta)$ depends only on $\alpha\sigma(\beta)$, which implies the assertion of part b). ∎

Note that if $i \equiv_{pd} 1$, then $\lambda(i) = \lambda$, whence $\mathcal{D}_{\lambda,n}(\alpha x^i, \beta x^{n-i}) = \mathbf{tr}_0(\lambda\alpha\sigma(\beta))$ (provided $i \in I_{reg}$). Thus Lemma 5.11b) asserts that C coincides with $\mathcal{D}_{\lambda_i,n}$ on $L_i \times L_{n-i}$ whenever $i \in I_{reg}$ and $i \equiv_{pd} 1$.

Now let $\{\lambda_k\}$ be as in the conclusion of Lemma 5.11b). For the rest of the proof, set $\mu_i = \lambda_{ie+1}$ (for $i = 1,2,\ldots,c-1$). Note that $\mu_i = \mu_j$ if $i \equiv_p j$ by Lemma 5.11b).

Proposition 5.12: *Let $i \in \mathbb{N}$ be such that $e \leq i \leq n-e$, $(i,n-i)$ is regular and $0 < \varepsilon(i) < p$. Let $a \in \{1,2,\ldots,p\}$ be such that $\mathrm{d}_\omega(i) \equiv_p ia$. Then $C_i(\alpha,\beta) = \mathbf{tr}_0(\mu_a(i)\alpha\sigma^i(\beta))$. In other words, C coincides with $\mathcal{D}_{\mu_a,n}$ on $L_i \times L_{n-i}$.*

First we state a simple technical lemma which follows directly from Claim 5.2.

7 This is the only place in the proof where we use that $(p,d) \neq (3,3)$ or $(2,4)$.

LEMMA 5.13: *Let S_1 and S_2 be two semi-cocycles of L. Let $J = \{i \in \mathbb{N} \mid e \leq i \leq n-e$ and S_1 coincides with S_2 on $L_i \times L_{n-i}\}$. Suppose that $j, k \in J$ and $k \equiv_d 1$.*

a) *If (k, j) is regular and $\mathrm{d}_\omega(k+j) \leq c-1$, then $j+k \in J$.*

b) *If $j - k \geq e$ and $(n-j, k)$ is regular, then $j - k \in J$.*

Proof of Proposition 5.12: Let $J = \{j \in \mathbb{N} \mid 1 \leq \mathrm{d}_\omega(j) \leq c-1$ and C coincides with $\mathcal{D}_{\mu_a,n}$ on $L_j \times L_{n-j}\}$. We will show that $i \in J$ by induction on $\varepsilon(i)$.

The case $\varepsilon(i) = 1$ is clear. Indeed, if $i = ue + 1$, then $a \equiv_p u$, whence

$$C_{ue+1}(\alpha, \beta) = C_{ae+1}(\alpha, \beta) = \mathbf{tr}_0(\mu_a \alpha\sigma(\beta)) = \mathbf{tr}_0(\mu_a(i)\alpha\sigma^i(\beta)).$$

Now suppose that $1 < \varepsilon(i) < p$. If $\mathrm{d}_\omega(i) > p$, let $j = i - ae - 1$. Then $\varepsilon(j) < \varepsilon(i) < p$ and $\mathrm{d}_\omega(j) = \mathrm{d}_\omega(i) - a \equiv_p ja$, whence $j \in J$ by induction. Note that $i - j = ae + 1$ lies in J by definition of μ_a. So, $i \in J$ by Lemma 5.13a).

If $\mathrm{d}_\omega(i) \leq p$ and $d \nmid i$, apply the above argument to $i + pe$ and use the facts that $C_{i+pe} = C_i$ (by Lemma 5.11a)) and $\mu_a(i) = \mu_a(i + pe)$.

Finally, suppose that $\mathrm{d}_\omega(i) \leq p$ and $d \mid i$. Let $j = i + (p-a)e - 1$. We have $\varepsilon(j) < \varepsilon(i) < p$ and $\mathrm{d}_\omega(j) = \mathrm{d}_\omega(i) + p - a \equiv_p ja$, so by induction $j \in J$. Applying Lemma 5.13a), we see that $j + ae + 1 \in J$ and $j + 2ae + 2 \in J$. Now $j + 2ae + 2 = i + (a+p)e + 1 \leq (3p+1)e \leq n - e$. Since $d \nmid (i + (a+p)e + 1)$, Lemma 5.11a) implies that $i + ae + 1 \in J$, whence $i \in J$ by Lemma 5.13b). ∎

Next we establish a relation between the numbers $\{\mu_a\}$.

LEMMA 5.14: *There exist $\mu \in \mathbf{w}$ and $\nu \in \mathbf{f}$ such that $\mu_a = \mu + a\nu$ for all a.*

Proof: Assume first that $p > 2$. Fix $i, j \in \{1, 2, \ldots, p\}$ and apply the semi-cocycle identity to the triple $\alpha x^{ie+1}, \beta x^{je+1}, \gamma x^{n-(i+j)e-2}$, where $\alpha, \beta, \gamma \in \mathbf{w}$. If $d > 2$, α, β and γ can be chosen arbitrarily; if $d = 2$, we must have $\mathbf{tr}(\gamma) = 0$ since in this case $d \mid (n - (i+j)e - 2)$. We have

$$C_{(i+j)e+2}(\alpha\sigma(\beta) - \beta\sigma(\alpha), \gamma) = C_{ie+1}(\alpha, \beta\sigma(\gamma) - \gamma\sigma^{-2}(\beta)) - C_{je+1}(\beta, \alpha\sigma(\gamma) - \gamma\sigma^{-2}(\alpha)).$$

By Proposition 5.12, the right-hand side is equal to

$$\mathbf{tr}_0(\mu_i\alpha(\sigma(\beta)\sigma^2(\gamma) - \sigma(\gamma)\sigma^{-1}(\beta)) - \mu_j\beta(\sigma(\alpha)\sigma^2(\gamma) - \sigma(\gamma)\sigma^{-1}(\alpha))) = \mathbf{tr}_0((\mu_i + \sigma(\mu_j))\alpha\sigma(\beta)\sigma^2(\gamma) - (\sigma(\mu_i) + \mu_j)\beta\sigma(\alpha)\sigma^2(\gamma))$$

while the left-hand side equals

$$\mathbf{tr}_0(\mu_{\frac{i+j}{2}}(2)(\alpha\sigma(\beta)-\beta\sigma(\alpha))\sigma^2(\gamma))$$

(by $\mu_{\frac{i+j}{2}}$ we mean μ_a where $a\in\{1,\dots,p\}$ is such that $2a\equiv_p(i+j)$).

Therefore,

$$\mathbf{tr}_0(u\alpha\sigma(\beta)\sigma^2(\gamma)-v\beta\sigma(\alpha)\sigma^2(\gamma)\Big)=0, \tag{5.23}$$

where $u=\mu_{\frac{i+j}{2}}(2)-\mu_i-\sigma(\mu_j)$ and $v=\mu_{\frac{i+j}{2}}(2)-\mu_j-\sigma(\mu_i)$.

Applying (5.23) with various values of $\alpha,\beta,\gamma\in\mathbf{w}$, one can show that $u=v=0$. If $d>2$, the argument is straightforward (since α,β,γ can be chosen arbitrarily). If $d=2$, we note that $v=\sigma(u)$ and $\sigma(\gamma)=-\gamma$ (as $\mathbf{tr}(\gamma)=0$). Therefore,

$$\begin{aligned}0&=\mathbf{tr}_0(u\alpha\sigma(\beta)\sigma^2(\gamma)-v\beta\sigma(\alpha)\sigma^2(\gamma))\\&=\mathbf{tr}_0(u\alpha\sigma(\beta)\sigma^2(\gamma)-\sigma(v\beta\sigma(\alpha)\sigma^2(\gamma)))=\mathbf{tr}_0(2u\alpha\sigma(\beta)\gamma),\end{aligned}$$

and we conclude that $u=0$ (whence $v=0$). So, we showed that

$$\mu_{\frac{i+j}{2}}(2)=\mu_i+\sigma(\mu_j)\quad\text{and}\quad\mu_{\frac{i+j}{2}}(2)=\mu_j+\sigma(\mu_i). \tag{5.24}$$

It follows immediately that $\mu_i-\mu_j=\sigma(\mu_i-\mu_j)$, whence $\mu_i-\mu_j\in\mathbf{f}$. Now let $\mu=\mu_p$ and $\nu_i=\mu_i-\mu_p$ for $1\le i\le p$. Since $\nu_i\in\mathbf{f}$ for all i, (5.24) yields

$$2\nu_{\frac{i+j}{2}}=\nu_i+\nu_j. \tag{5.25}$$

To finish the proof it remains to show that $\nu_k=k\nu_1$ for $1\le k\le p$. The assertion is trivially true for $k=1$ and $k=p$. If $1<k<p$, applying (5.25) with $i=k-1$ and $j=k+1$, we get $\nu_k-\nu_{k-1}=\nu_{k+1}-\nu_k$.

So, the difference $\delta:=\nu_k-\nu_{k-1}$ is the same for $1<k<p$, whence $\nu_k=\nu_1+(k-1)\delta$ for $1\le k\le p$. On the other hand, we know that $\nu_p=0$, whence $\delta=\nu_1$. This finishes the proof in the case $p>2$.

Now assume that $p=2$. Note that in this case we only have to prove that $\mu_1-\mu_2\in\mathbf{f}$. Formula (5.24) still holds if we assume that both i and j have the same parity. Taking $i=1$ and $j=3$, we get $\mu_2(2)=\mu_1+\sigma(\mu_1)$. Therefore, $\mu_2-\mu_1=\sigma(\mu_2-\mu_1)$, whence $\mu_1-\mu_2\in\mathbf{f}$. ∎

Conclusion of the proof of Theorem 5.7b): Let μ and ν be as in the conclusion of Lemma 5.14. Let $J=\{j\in\mathbb{N}\mid C$ coincides with $\mathcal{D}_{\mu,n}+\mathcal{E}_{\nu,n}$ on $L_j\times L_{n-j}\}$. Since both C and $\mathcal{D}_{\mu,n}+\mathcal{E}_{\nu,n}$ are homogeneous of weight n, it is enough to show that $J\supseteq I_{good}$.

Fix $i \in I_{good}$. We can assume that $(i, n-i)$ is regular for otherwise both C and $\mathcal{D}_{\mu,n} + \mathcal{E}_{\nu,n}$ vanish on $L_i \times L_{n-i}$.

CASE 1: $0 < \varepsilon(i) < p$. Let $a := \mathrm{d}_\omega(i)/i \in \mathbb{F}_p$. According to Proposition 5.12 and Lemma 5.14, we have

$$\begin{aligned} C(\alpha x^i, \beta x^{n-i}) &= \mathbf{tr}_0(\{\mu + a\nu\}(i)\alpha\sigma^i(\beta)) = \mathbf{tr}_0((\mu(i) + \nu a i)\alpha\sigma^i(\beta)) \\ &= \mathbf{tr}_0((\mu(i) + \nu\,\mathrm{d}_\omega(i))\alpha\sigma^i(\beta)) \\ &= \mathcal{D}_{\mu,n}(\alpha x^i, \beta x^{n-i}) + \mathcal{E}_{\nu,n}(\alpha x^i, \beta x^{n-i}). \end{aligned}$$

CASE 2: $\varepsilon(i) = 0$. (i.e. $e \mid i$) We know that $e+1 \in J$ and $i+e+1 \in J$ since $\varepsilon(e+1) = \varepsilon(i+e+1) = 1$, whence $i \in J$ by Lemma 5.13b).

CASE 3: $\varepsilon(i) \geq p$. In this case we use induction on $\theta(i) = 3\varepsilon(i) - 2\,\mathrm{d}_\omega(i)$ (it is clear that possible values of $\theta(i)$ are bounded from below).

If $\mathrm{d}_\omega(i) \geq 3$, let $k = e+1$ and $j = i-k$. Then $k \in J$ since $\varepsilon(k) = 1 < p$, and $j \in J$ by induction since $\theta(j) = \theta(i) - 1$. Therefore, $i \in J$ by Lemma 5.13a).

If $\mathrm{d}_\omega(i) = 2$ and $\varepsilon(i) < e-1$, apply Lemma 5.13b) with $j = i + pe + 1$ and $k = pe + 1$. Finally, if $\varepsilon(i) = e-1$, then $(i, n-i)$ cannot be regular (as $d \mid n$). ∎

5.4 FORMULAS FOR Z_f AND $\mathfrak{z}_f$. Theorem 5.7 can be applied to the weight n component of Z_f (where $n \geq N-p$) for any ω-splitting $f\colon L \to \hat{L}$. If we choose the splitting in the "right" way, a stronger statement can be made:

COROLLARY 5.15: *Let $I_{great} = \{i \in \mathbb{N} \mid N-p \leq i \leq N\}$. Fix $\lambda \in \mathbf{w}$ with $\mathbf{tr}(\lambda) \neq 0$. Then there exists an ω-splitting f such that for every $i \in I_{great}$ we have*

(5.26)

$$Z_{f\,|i\ \ L_{good}\times L_{good}} = \begin{cases} 0 & \text{if } d \nmid i, \\ \mathcal{E}_{\nu_i,i} \text{ for some } \nu_i \in \mathbf{f} & \text{if } d \mid i \text{ but } pd \nmid i, \\ \mathcal{D}_{\lambda_i,i} + \mathcal{E}_{\nu_i,i} \text{ for some } \nu_i \in \mathbf{f} \text{ and } \lambda_i \in \mathbf{f}\lambda & \text{if } pd \mid i. \end{cases}$$

(recall that $Z_{f\,|i}$ is the weight i component of Z_f).

Proof: Let f_0 be some ω-splitting. As mentioned in Section 3, if B is a coboundary, then $Z_{f_0} + B = Z_f$ for another splitting f; moreover, f is an ω-splitting if and only if $B(L_i^\omega, L_j^\omega) = 0$ whenever $i + j \neq c$. The latter holds if and only if B is supported on $[ce, N]$ (we leave verification of this fact to the reader).

Since $I_{great} \subset [ce, N]$, Theorem 5.7 immediately implies that there exists an ω-splitting f_1 such that for every $i \in I_{great}$,

$$Z_{f_1\,|i\ \ L_{good}\times L_{good}} = \begin{cases} 0 & \text{if } d \nmid i \\ \mathcal{D}_{\mu_i,i} + \mathcal{E}_{\nu_i,i} \text{ for some } \nu_i \in \mathbf{f} \text{ and } \mu_i \in \mathbf{w} & \text{if } d \mid i. \end{cases}$$

It remains to show that for every $i \in I_{great}$ with $d \mid i$ there exists $\lambda_i \in \mathbf{f}\lambda$ such that $B_i := \mathcal{D}_{\lambda_i,i} - \mathcal{D}_{\mu_i,i}$ is a coboundary and $\lambda_i = 0$ if $pd \nmid i$. This will finish the proof since then $Z_{f_1} + \sum_{i \in I_{great}, d|i} B_i = Z_f$ for some ω-splitting f, and (5.26) clearly holds.

First let $i \in I_{great}$ with $d \mid i$ and $pd \nmid i$. We claim that $\mathbf{tr}(\mu_i) = 0$. Indeed, $\mathcal{E}_{\nu_i,i}$ is a cocycle by Proposition 5.5c), since p divides $c = \mathrm{d}_\omega(i)$. Therefore, $Z_{f_1|_i} - \mathcal{E}_{\nu_i,i}$ is also a cocycle. On the other hand, $\mathcal{D}_{\mu_i,i}$ is NOT a cocycle unless $\mathbf{tr}(\mu_i) = 0$ by Proposition 5.5b). We know that $Z_{f_1|_i} - \mathcal{E}_{\nu_i,i}$ coincides with $\mathcal{D}_{\mu_i,i}$ on $L_{good} \times L_{good}$. Even though $Z_{f_1|_i} - \mathcal{E}_{\nu_i,i}$ and $\mathcal{D}_{\mu_i,i}$ may not coincide on $L \times L$, the argument of Proposition 5.5b) still implies that $\mathbf{tr}(\mu_i) = 0$.

Now we are ready to finish the proof. Given $i \in I_{great}$ with $d \mid i$, let $\lambda_i = \frac{\mathbf{tr}(\mu_i)}{\mathbf{tr}(\lambda)}\lambda$. Clearly, $\lambda_i \in \mathbf{f}\lambda$ and $\mathbf{tr}(\lambda_i) = \mathbf{tr}(\mu_i)$. If $pd \nmid i$, then $\lambda_i = 0$ since $\mathbf{tr}(\mu_i) = 0$. Finally, $B_i := \mathcal{D}_{\lambda_i,i} - \mathcal{D}_{\mu_i,i}$ is a coboundary by Proposition 5.5a). ∎

In order to derive a formula for the group 1-cocycle $\mathfrak{z}_f$ we use the following result.

PROPOSITION 5.16: *Let $n \le N$, with $d \mid n$, and let $\mathfrak{d}$ be a derivation of A. Recall that $C_{\mathfrak{d},n}(a,b) = \mathbf{T}_n(\mathfrak{d}(a)b)$ for every $a, b \in A$. Define*[8] *$\mathfrak{c}_{\mathfrak{d},n}\colon G \times L \to \mathbb{F}_p$ by setting $\mathfrak{c}_{\mathfrak{d},n}(g,b) = \mathbf{T}_n(\mathfrak{d}(\overline{g})\overline{g}^{-1}b)$ (recall that the map $g \mapsto \overline{g}$ was defined in Section 4). Then $\mathfrak{c}_{\mathfrak{d},n}$ and $C_{\mathfrak{d},n}$ are compatible in the sense of (3.2).*

Proof: Let $\mathfrak{c} = \mathfrak{c}_{\mathfrak{d},n}$ and $C = C_{\mathfrak{d},n}$. Fix $g \in G$ and let $k = \overline{g} \in A$. Recall that $u^g = k^{-1}uk$ for every $u \in A$. Therefore for any $u, v \in L$ we have

$$\begin{aligned} C(u,v) - C(u^g, v^g) =& \mathbf{T}_n(\mathfrak{d}(u)v) - \mathbf{T}_n(\mathfrak{d}(k^{-1}uk)k^{-1}vk) \\ =& \mathbf{T}_n(\mathfrak{d}(u)v) - \mathbf{T}_n((\mathfrak{d}(k^{-1})uk + k^{-1}\mathfrak{d}(u)k \\ &+ k^{-1}u\mathfrak{d}(k))k^{-1}vk). \end{aligned}$$

Since $\mathfrak{d}(k^{-1}) = -k^{-1}\mathfrak{d}(k)k^{-1}$, $\mathbf{T}_n(ab) = \mathbf{T}_n(ba)$ and $\mathbf{T}_n(k^{-1}ak) = \mathbf{T}_n(a)$, we have

$$\begin{aligned} C(u,v) - C(u^g, v^g) &= \mathbf{T}_n(\mathfrak{d}(u)v) - \mathbf{T}_n(-\mathfrak{d}(k)k^{-1}uv + \mathfrak{d}(u)v + u\mathfrak{d}(k)k^{-1}v) \\ &= \mathbf{T}_n(\mathfrak{d}(k)k^{-1}uv - \mathfrak{d}(k)k^{-1}vu) \\ &= \mathbf{T}_n(\mathfrak{d}(k)k^{-1}[u,v]) = \mathfrak{c}(g,[u,v]). \qquad ∎ \end{aligned}$$

Let $L_{great} = \bigoplus_{i \in I_{great}} L_i$, where $I_{great} = \{i \in \mathbb{N} \mid N - p \le i \le N\}$ as before. We are now ready to give a formula for the restriction of $\mathfrak{z}_f$ to $G \times L_{great}$.

8 This notation will be used for the rest of this section

PROPOSITION 5.17: *If I_{great} does not contain multiples of pd, then $\mathfrak{z}_f$ vanishes on $G \times L_{great}$ for some ω-splitting f. Otherwise, let N_0 be the unique multiple of pd lying in I_{great}. Then there exist an ω-splitting f and $\lambda_0 \in \mathbf{w}$ such that $\mathfrak{z}_f$ coincides with $\mathfrak{c}_{\mathfrak{d}_{\lambda_0},N_0}$ on $G \times L_{great}$. Moreover, given $\lambda \in \mathbf{w}$, with $\mathbf{tr}(\lambda) \neq 0$, we can always choose f so that $\lambda_0 \in \mathbf{f}\lambda$.*

Proof: Let f, $\{\lambda_i\}$ and $\{\nu_i\}$ be as in the conclusion of Corollary 5.15. Let $I_1 = \{i \in I_{great} \mid pd \text{ divides } i\}$, $I_2 = \{i \in I_{great} \mid d \text{ divides } i\}$ and let $C = \sum_{i\in I_1} \mathcal{D}_{\lambda_i,i} + \sum_{i\in I_2} \mathcal{E}_{\nu_i,i}$. Let $S = \{(i,j) \in I_{good} \times I_{good} \mid i + j \geq N - p\}$ and let Ω be the linear span of the set $\bigcup_{(i,j)\in S} L_i \times L_j$ in $L \times L$.

By Corollary 5.15, Z_f coincides with C on Ω. We know that Z_f is compatible with $\mathfrak{z}_f$ (by Proposition 3.4). By Proposition 5.16, $\mathcal{D}_{\lambda_i,i}$ (resp. $\mathcal{E}_{\nu_i,i}$) is compatible with $\mathfrak{c}_{\mathfrak{d}_{\lambda_i},i}$ (resp. $\mathfrak{c}_{\mathfrak{e}_{\nu_i},i}$) whence C is compatible with $\sum_{i\in I_1} \mathfrak{c}_{\mathfrak{d}_{\lambda_i},i} + \sum_{i\in I_2} \mathfrak{c}_{\mathfrak{e}_{\nu_i},i}$.

It is easy to see that Ω is invariant under the diagonal action of G on $L \times L$ and the set $\{[u,v] \mid (u,v) \in \Omega\}$ spans L_{great}. Therefore, by Claim 3.5 we have

$$\mathfrak{z}_f = \sum_{i\in I_1} \mathfrak{c}_{\mathfrak{d}_{\lambda_i},i} + \sum_{i\in I_2} \mathfrak{c}_{\mathfrak{e}_{\nu_i},i} \text{ on } G \times L_{great}.$$

The proof will be finished if we show that $\mathfrak{c}_{\mathfrak{e}_{\nu_i},i}$ is identically zero for all i. It suffices to show that $\mathfrak{e}_\nu(\overline{g}) = 0$ for any $g \in G$ and $\nu \in \mathbf{f}$. The latter holds since $\overline{g} \in \bigoplus_{i=0}^{c-1} \mathbf{w}x^i$ for any $g \in G$ and $\mathfrak{e}_\nu(\mathbf{w}x^i) = 0$ for $0 \leq i \leq c-1$. ∎

CHANGE OF NOTATION. In the next section we will write $\mathfrak{c}_{\lambda,n}$ for $\mathfrak{c}_{\mathfrak{d}_\lambda,n}$.

6. Proof of finite presentability in the case $(p,d) \neq (2,2)$

We retain all notations from the previous section. Fix an ω-splitting f for which the assertion of Proposition 5.17 holds, and let $Z = Z_f$, $\mathfrak{z} = \mathfrak{z}_f$. Throughout the section λ_0 and N_0 will be as in the conclusion of Proposition 5.17.

We are trying to reach a contradiction with Lemma 3.7, which asserts that $\mathfrak{z}$ does not vanish on $G \times U$, where $U = \gamma_{N-1}G/\gamma_{N+1}G = L_{N-1} \oplus L_N \subset L_{great}$. We already know that $\mathfrak{z}$ vanishes on $G \times L_{great}$ (and hence on $G \times U$), if I_{great} does not contain multiples of pd.

Next we show that $\mathfrak{z}$ vanishes on $G \times U$, if N is not a multiple of pd. Indeed, let $u \in U$ and $g \in G$. By Proposition 5.17, $\mathfrak{z}(g,u) = \mathfrak{c}_{\lambda_0,N_0}(g,u)$ (where $N - p \leq N_0 \leq N$ and N_0 is a multiple of pd). So, $\mathfrak{z}(g,u)$ is equal to the $\mathbf{f}_0$-trace of the coefficient of x^{N_0} in $\mathfrak{d}_{\lambda_0}(\overline{g})\overline{g}^{-1}u$. Since $\mathfrak{d}_{\lambda_0}(\overline{g})$ has zero constant term and

$u \in U = L_{N-1} \oplus L_N \subseteq x^{N-1}A$, the above coefficient is equal to zero unless $N_0 = N$.

Finally, consider the case $N = pdM$ for some M. In this case vanishing of $\mathfrak{z}$ on $G \times U$ will be proved using Lemma 3.6. The underlying computations have direct analogues in [PR]; however, due to many differences in terminology and notations, it seems more appropriate to reproduce the arguments from the above paper rather than give vague references to it. For the reader's convenience, throughout the section we shall indicate which part of [PR] we are following.

To prove that $\mathfrak{z}$ vanishes on $G \times U$ we must show that $\lambda_0 = 0$. By Proposition 5.17, λ_0 is an $\mathbf{f}$-multiple of some element with non-zero $\mathbf{f}$-trace, so it suffices to prove that $\mathbf{tr}(\lambda_0) = 0$.

Case 1: $p \nmid d$ (see [PR, pp. 682–683]). It will be enough to show that $\mathbf{tr}_0(\lambda_0\theta) = 0$ for any $\theta \in \mathbf{f}$. Indeed, if this is the case, then for any $\theta \in \mathbf{f}$ we have $\mathbf{tr}_{\mathbf{f}/\mathbf{f}_0}(\mathbf{tr}_{\mathbf{w}/\mathbf{f}}(\lambda_0)\theta) = \mathbf{tr}_{\mathbf{f}/\mathbf{f}_0}(\mathbf{tr}_{\mathbf{w}/\mathbf{f}}(\lambda_0\theta)) = \mathbf{tr}_0(\lambda_0\theta) = 0$. Since $\mathbf{tr}_{\mathbf{f}/\mathbf{f}_0}$ is a non-degenerate bilinear form on $\mathbf{f} \times \mathbf{f}$, we conclude that $\mathbf{tr}_{\mathbf{w}/\mathbf{f}}(\lambda_0) = 0$.

Fix $\theta \in \mathbf{f}$. Since $p \nmid d$, G is isomorphic to the quotient of $U = GL_1^1(D)$ modulo its center $Z(U) = U \cap F^*$. Therefore, there exist $\alpha, \beta \in \mathfrak{m}_F$ such that the elements $g := (1+\pi)(1+\alpha)$ and $h := (1+\theta\pi^{dM-1})(1+\beta)$ lie in G. Moreover, it is easy to see that $\beta \in \mathfrak{m}_F^M$, that is, $\beta = \sum_{i \geq M} \beta_i \pi^{di}$ for some $\beta_i \in \mathbf{f}$. Now let $u = \mathrm{LT}_\omega(h^p)$. Since $h^p = (1+\theta^p\pi^{N-p})(1+\beta^p)$, we have $u = \theta^p x^{N-p} + \beta_M^p x^N \in L_{great}$. Clearly, g and h commute, so $\mathfrak{z}(g,u) = 0$ by Lemma 3.6. Therefore, $\mathbf{T}_N(\mathfrak{d}_{\lambda_0}(\overline{g})\overline{g}^{-1}u) = \mathfrak{z}(g,u) = 0$.

Since $p \nmid d$, the restriction of the trace map $\mathbf{tr}$ to $\mathbf{f}$ is non-zero, so by Proposition 5.17 we can assume that λ_0 lies in $\mathbf{f}$. Let $\mathfrak{d} = \mathfrak{d}_{\lambda_0}$. We have $\overline{g} = (1+x)(1+\bar{\alpha})$, whence $\mathfrak{d}(\overline{g}) = \lambda_0 x(1+\bar{\alpha}) + (1+x)\mathfrak{d}(\bar{\alpha})$. Since $\alpha \in \mathfrak{m}_F$ and $\lambda_0 \in \mathbf{f}$, both $\bar{\alpha}$ and $\mathfrak{d}(\bar{\alpha})$ belong to $\mathbf{f}[x^d]$ and hence lie in the center of A. Hence, $\mathfrak{d}(\overline{g})\overline{g}^{-1} = \lambda_0 x(1+x)^{-1} + \gamma$ where $\gamma = \mathfrak{d}(\bar{\alpha})(1+\bar{\alpha})^{-1} \in x^d\mathbf{f}[x^d]$. We have

$$\begin{aligned}\mathfrak{d}(\overline{g})\overline{g}^{-1}u &= (\lambda_0 x(1+x)^{-1} + \gamma)(\theta^p x^{N-p} + \beta_M^p x^N) \\ &= \lambda_0\theta^p x^{N-p+1}(1+x)^{-1} + \gamma\theta^p x^{N-p}\end{aligned}$$

since $x^N \cdot x^i = 0$ if $i > 0$. We are interested in the $\mathbf{f}_0$-trace of the coefficient of x^N in the above expression. The second summand has zero coefficient of x^N since $\gamma \in \mathbf{f}[x^d]$, pd divides N, and p does not divide d. The coefficient of x^N in the first summand is equal to $\lambda_0\theta^p$. Hence, $\mathbf{tr}_0(\lambda_0\theta^p) = \mathbf{T}_N(\mathfrak{d}(\overline{g})\overline{g}^{-1}u) = 0$, and we are done.

Case 2: $p \mid d$ and $p > 2$ (see [PR, pp. 684–685] and [PR, 4.7, 4.8]). Let $K = \mathbf{f}((\pi^p))$ and let D_1 be the centralizer of K in D. Let $\mathbf{v} \subseteq \mathbf{w}$ be the

(unique) extension of $\mathbf{f}$ of degree p. Then $D_1 = \mathbf{v}((\pi))$ is a division algebra of degree p over its center K. Let $H = SL_1^1(D_1) \subseteq G$.

The following computational result is proved in [PR, p. 684].

LEMMA 6.1 ([PR]): *Let $\theta \in \mathbf{f}$ and $s \in \mathbb{N}$, and assume that $p > 2$. There exist commuting elements $g, h \in H$ such that*

$$h^p \equiv 1 + \theta^p \pi^{p^2 s - p} + \theta^p \pi^{p^2 s - 1} \bmod \pi^{p^2 s} O_{D_1}$$

and

$$g \equiv 1 + \pi - \xi \pi^p \bmod \pi^{p+1} O_{D_1},$$

where $\xi \in \mathbf{v}$ and $\mathbf{tr}_{\mathbf{v}/\mathbf{f}}(\xi) = 1$.

Note that $N = pdM$ is divisible by p^2. Let $s = N/p^2$, let $\theta \in \mathbf{f}$ be arbitrary, and let $g, h \in H$ be as in the conclusion of Lemma 6.1. As before, we have the equation $\mathfrak{z}(g, u) = 0$ where $u := \mathrm{LT}_\omega(h^p) = \theta^p x^{N-p} + \theta^p x^{N-1} + \delta x^N$ for some $\delta \in \mathbf{v}$. Computing $\mathfrak{z}(g, u)$ as in case 1, we conclude that

$$\mathbf{tr}_{\mathbf{w}/\mathbf{f}_0}((2\lambda_0 - \xi\lambda_0(p))\theta^p) = 0.$$

Since $\mathbf{tr}_{\mathbf{w}/\mathbf{f}_0}(\alpha\theta^p) = \mathbf{tr}_{\mathbf{f}/\mathbf{f}_0}(\mathbf{tr}_{\mathbf{w}/\mathbf{f}}(\alpha)\theta^p)$ for any $\alpha \in \mathbf{w}$, we get

$$\mathbf{tr}_{\mathbf{w}/\mathbf{f}}(2\lambda_0 - \xi\lambda_0(p)) = 0. \tag{6.1}$$

We have $\mathbf{tr}_{\mathbf{w}/\mathbf{f}}(\xi\lambda_0(p)) = \mathbf{tr}_{\mathbf{v}/\mathbf{f}}(\mathbf{tr}_{\mathbf{w}/\mathbf{v}}(\lambda_0(p))\xi)$. The Galois group $\mathrm{Gal}(\mathbf{w}/\mathbf{v})$ is generated by σ^p, whence

$$\mathbf{tr}_{\mathbf{w}/\mathbf{v}}(\lambda_0(p)) = \sum_{i=0}^{d/p-1} \sigma^{pi}\left(\sum_{j=0}^{p-1} \sigma^j(\lambda_0)\right) = \sum_{i=0}^{d-1} \sigma^i(\lambda_0) = \mathbf{tr}_{\mathbf{w}/\mathbf{f}}(\lambda_0).$$

Therefore $\mathbf{tr}_{\mathbf{w}/\mathbf{f}}(\xi\lambda_0(p)) = \mathbf{tr}_{\mathbf{v}/\mathbf{f}}(\xi\mathbf{tr}_{\mathbf{w}/\mathbf{f}}(\lambda_0)) = \mathbf{tr}_{\mathbf{v}/\mathbf{f}}(\xi)\mathbf{tr}_{\mathbf{w}/\mathbf{f}}(\lambda_0) = \mathbf{tr}_{\mathbf{w}/\mathbf{f}}(\lambda_0)$. Combining this with (6.1), we finally conclude that $\mathbf{tr}_{\mathbf{w}/\mathbf{f}}(\lambda_0) = 0$.

CASE 3: $p = 2$ and d is even (see [PR, 5.6,6.6]). Let $K, D_1, \mathbf{v}$ and H be as in Case 2. Let $s = N/4$. Fix $\theta \in \mathbf{f}$. By Lemma 8.2 (stated later in the paper) there exist $g, h \in H$ such that

$$h \equiv 1 + \pi^{2s-1} \bmod \pi^{4s-2} O_{D_1} \quad \text{and} \quad g \equiv 1 + \theta\pi + \beta\pi^2 \bmod \pi^3 O_{D_1},$$

where $\mathbf{tr}_{\mathbf{v}/\mathbf{f}}(\beta) = \theta^2$. It is easy to see that $(g, h) \equiv 1 + \theta^2 \pi^{2s+1} \bmod \pi^{2s+2} O_{D_1}$.

Now let $\hat{g}$ and $\hat{h}$ be any lifts of g and h in $\hat{G}$. We shall use the identity

$$(\hat{g}, \hat{h}^2) = (\hat{g}, \hat{h})^2((\hat{g}, \hat{h}), \hat{h}). \tag{6.2}$$

Since $(g,h) \in \gamma_{2s+1}G$ (see above) and $\mathrm{dep}(\hat{G},\phi) = N > 2s+1$, we have $(\hat{g},\hat{h}) \in \gamma_{2s+1}\hat{G}$. Hence, $(\hat{g},\hat{h})^2 \in \gamma_{N+1}\hat{G}$ by Lemma 3.2.

Let

$$\begin{array}{lll} \hat{u} = \mathrm{LT}_\omega(\hat{h}^2), & \hat{v} = \mathrm{LT}_\omega((\hat{g},\hat{h})), & \hat{w} = \mathrm{LT}_\omega(\hat{h}), \\ u = \mathrm{LT}_\omega(h^2), & v = \mathrm{LT}_\omega((g,h)), & w = \mathrm{LT}_\omega(h). \end{array}$$

It is easy to see that $w = x^{N/2-1}$, $u = x^{N-2}$ and $v = \theta^2 x^{N/2+1} + \cdots$.

It follows from (6.2) that

$$(\hat{h}^{-2})^{\hat{g}} \cdot \hat{h}^2 \equiv ((\hat{g},\hat{h}),\hat{h}) \bmod \omega_{c+1}\hat{G} (= \gamma_{N+1}\hat{G}).$$

Since $\mathrm{d}_\omega(\hat{h}) = \mathrm{d}_\omega((\hat{g},\hat{h})) = c/2$ and $\mathrm{d}_\omega(\hat{h}^2) = c$, projecting both sides of the above equation to $\omega_c\hat{G}/\omega_{c+1}\hat{G}$, we get $\hat{u} - \hat{u}^g = [\hat{w},\hat{v}]$. It is clear that the elements $\hat{u} - f(u)$, $\hat{v} - f(v)$ and $\hat{w} - f(w)$ lie in $\hat{V} = \gamma_N\hat{G}/\gamma_{N+1}\hat{G}$. Since $\hat{V}$ is central in $\hat{L}$, and is acted trivially on by G, we have $\hat{u} - f(u) = \hat{u}^g - f(u)^g$ and $[\hat{w},\hat{v}] = [f(w),f(v)]$. Hence,

$$f(u) - f(u)^g = [f(w),f(v)]. \tag{6.3}$$

Applying the map $f\phi_*$ to both sides of (6.3) and subtracting the result from (6.3), we get

$$\mathfrak{z}(g,u) = Z(w,v). \tag{6.4}$$

Now let $\lambda = \lambda_0$. Since $u \in L_{great}$, we have $\mathfrak{z}(g,u) = \mathfrak{c}_{\lambda,N}(g,u) = \mathbf{T}_N(\mathfrak{d}_\lambda(\overline{g}) \cdot \overline{g}^{-1}u)$. Clearly, $\overline{g} = 1 + \theta x + \beta x^2 + \cdots$, whence $\mathfrak{d}_\lambda(\overline{g}) = \theta\lambda x + \beta\lambda(2)x^2 + \cdots$. We have

$$\mathfrak{d}_\lambda(\overline{g}) \cdot \overline{g}^{-1}u = \theta\lambda x^{N-1} + (\beta\lambda(2) - \theta^2\lambda)x^N = \theta\lambda x^{N-1} + (\beta\sigma(\lambda) - \sigma(\beta)\lambda)x^N,$$

where at the last step we used that $\theta^2 = \beta + \sigma(\beta)$. So, $\mathfrak{z}(g,u) = \mathbf{tr}_0(\beta\sigma(\lambda) - \sigma(\beta)\lambda)$. But $\beta \in \mathbf{v}$, whence $\sigma^2(\beta) = \beta$. Therefore, $\mathbf{tr}_0(\beta\sigma(\lambda) - \sigma(\beta)\lambda) = \mathbf{tr}_0(\sigma(\sigma(\beta)\lambda) - \sigma(\beta)\lambda) = 0$. Thus, $\mathfrak{z}(g,u) = 0$.

Finally, $Z(w,v) = \mathbf{T}_N(\mathfrak{d}_\lambda(w)v) = \mathbf{tr}_0(\lambda(N/2-1)\theta^2)$. Now $\lambda(N/2-1) = \lambda(dM-1) = M\mathbf{tr}(\lambda) - \sigma^{-1}(\lambda)$. Since $\mathbf{tr}(M\mathbf{tr}(\lambda)) = dM\mathbf{tr}(\lambda) = 0$, we have $\mathbf{tr}_0(M\mathbf{tr}(\lambda)\theta^2) = 0$. Therefore, (6.4) implies that $\mathbf{tr}_0(\sigma^{-1}(\lambda)\theta^2) = 0$. The last equality holds for any $\theta \in \mathbf{f}$, and we conclude that $\mathbf{tr}(\lambda) = \mathbf{tr}(\sigma^{-1}(\lambda)) = 0$. ∎

7. Exceptional cases

7.1 Preliminaries. In this section we will finish the proof of Theorem 5.7 in the cases $p = d = 3$ and $p = 2$, $d = 4$. The main difference with the regular case is that we will only be able to classify admissible cocycles. Recall that the only results that require different arguments are Lemma 5.11b) and the conclusion of the proof of Theorem 5.7a) (the part following Lemma 5.9). We retain all notations introduced in Section 5.

A key role in the proof will be played by the following formula, describing the action of elements of W^* on $L = L^\omega(G)$. Note that $W^* \cap G$ is generated by elements of the form $(1+h)^{-1}\sigma(1+h)$, where $h = \lambda\tau^s$ for some $\lambda \in \mathbf{w}$ and $s \in \mathbb{N}$.

Proposition 7.1 (W-action formula): *Let $\lambda \in \mathbf{w}$, $s \in \mathbb{N}$, and let*

$$g = g(\lambda, s) = (1+\lambda\tau^s)^{-1}(1+\sigma(\lambda)\tau^s) \quad \textit{where } \tau = \pi^d.$$

Let $\alpha \in \mathbf{w}$, $k \geq e$ and let $u = \alpha x^k$. We have

$$u^g = u + \sum_{\substack{n\geq 1,\\ \mathrm{d}_\omega(k+dn)=\mathrm{d}_\omega(k)}} \alpha F_n(\lambda) x^{k+dns},$$

where

$$\begin{aligned} F_n(\lambda) =& \sigma(\lambda^{n-1})(\sigma(\lambda)-\lambda) + \sigma^k(\lambda^{n-1})(\sigma^k(\lambda)-\sigma^{k+1}(\lambda)) \\ &+ \sum_{\substack{i+j=n-2,\\ i,j\geq 0}} \sigma(\lambda^i)\sigma^k(\lambda^j)(\sigma(\lambda)-\lambda)(\sigma^k(\lambda)-\sigma^{k+1}(\lambda)). \end{aligned}$$

Proof: Direct computation. ∎

It will also be convenient to introduce one more definition.

Definition: Let $\mathbf{k}$ be a subfield of $\mathbf{w}$. A map $C\colon \mathbf{w}\times\mathbf{w} \to \mathbb{F}_p$ is called **$\mathbf{k}$-balanced**,[9] if $C(\kappa\alpha, \beta) = C(\alpha, \kappa\beta)$ for all $\alpha, \beta \in \mathbf{w}$ and $\kappa \in \mathbf{k}$.

Notations: Throughout the section n, C, Z are fixed and assumed to satisfy the hypotheses of Theorem 5.7. Recall that Z is a regular admissible cocycle, and C is the weight n component of Z.

We will use shortcut notations

$$Z_{i,j}(\alpha,\beta) := Z(\alpha x^i, \beta x^j) \quad \text{and} \quad C_i(\alpha,\beta) := C(\alpha x^i, \beta x^{n-i}) = Z_{i,n-i}(\alpha,\beta).$$

9 I am thankful to Gopal Prasad for suggesting this term

Recall that $\eta[i] = \sigma^i(\eta) - \eta$ (where $\eta \in \mathbf{w}$ and $i \in \mathbb{Z}$).

Finally, we will write $\mathrm{d}_\omega(i,j)$ for the pair $(\mathrm{d}_\omega(i), \mathrm{d}_\omega(j))$.

7.2 The case $p = d = 3$.

Proof of Theorem 5.7a): Recall that $C_i = 0$ if either $3 \mid i$ or $3 \mid (n-i)$ (by Claim 5.8). So we can assume that $3 \nmid i$ and $3 \nmid (n-i)$ (which implies that $i \equiv_3 n-i$). It is easy to see that there exists $\eta \in \mathbf{w}$ such that $\eta[i] = \eta[n-i] = 1$. Applying (5.6), we have $C_i(\alpha,\beta) = C_i(\alpha,-\beta)$ for all $\alpha,\beta \in \mathbf{w}$, whence C_i is identically zero. ∎

Proof of Lemma 5.11b): First of all, let us explicitly write down W-action formula for the case $p = d = 3$.

Given $k, s \in \mathbb{N}$, $\alpha, \lambda \in \mathbf{w}$, let $u = \alpha x^k$ and $g = g(\lambda, s)$ be as in Proposition 7.1. If $k \equiv_3 1$, then

$$u^g = \alpha(x^k - \mathbf{tr}(\lambda)x^{k+3s} + \mathbf{tr}(\lambda\sigma(\lambda))x^{k+6s} + (\sigma(\lambda^3) - \mathbf{N}(\lambda)x^{k+9s}) + \cdots)$$

If $k \equiv_3 2$, then

$$u^g = \alpha(x^k + \mathbf{tr}(\lambda)x^{k+3s} + \mathbf{tr}(\lambda^2 + \lambda\sigma(\lambda))x^{k+6s} + (\mathbf{tr}(\lambda)\mathbf{tr}(\lambda^2) - \lambda^3 + \mathbf{N}(\lambda))x^{k+9s} + \cdots)$$

Here $\mathbf{N}$ denotes the norm map of the extension $\mathbf{w}/\mathbf{f}$.

We claim that it suffices to prove Lemma 5.11b) for all i such that $\varepsilon(i) \leq 27$. Indeed, if $\varepsilon(i) > 27$, then $\mathrm{d}_\omega(i) = \mathrm{d}_\omega(i-27)$ and $i - 27 \in I_{reg}$, so by Lemma 5.11a) we have $C_i = C_{i-27}$. Hence, we can replace i by $i-27$ and repeat the process several times if needed. Note that if $\varepsilon(i) \leq 27$, then $\mathrm{d}_\omega(i, n-i) = \mathrm{d}_\omega(i+27, n-i-27)$, since $\varepsilon(i) + 27 \leq 54 < e$ and $\varepsilon(n-i) = \varepsilon(n) - \varepsilon(i) \geq \varepsilon(N) - 3 - 27 \geq 73 > 27$.

So, from now on we fix $i \in I_{reg}$ and assume that $\mathrm{d}_\omega(i, n-i) = \mathrm{d}_\omega(i+27, n-i-27)$. Take any $\lambda \in \mathbf{w}$, and let $g = g(\lambda, 3)$ be defined as above.

Given $\alpha, \beta \in \mathbf{w}$, let $u = \alpha x^i$, $v = \beta x^{n-i-27}$. Let $\mathfrak{c}\colon G \times L \to \mathbb{F}_p$ be a map compatible with Z. We have

$$Z(u,v) - Z(u^g, v^g) = \mathfrak{c}(g, [u,v]) = \mathfrak{c}(g, (\alpha\sigma(\beta) - \beta\sigma^{-1}(\alpha))x^{n-27}). \tag{7.1}$$

Note that the right-hand side of (7.1) depends only on $\alpha\sigma(\beta)$ (if we keep λ fixed).

Now compute u^g and v^g using W-action formula (note that $i \equiv_3 1$ and $n-i \equiv_3 2$). The left-hand side of (7.1) can then be expanded by bilinearity. Note that $Z_{k,j}=0$ when $k+j>n+3$, since $n \geq N-3$. Using this fact we get

(7.2)

$$\begin{aligned}
&Z_{i+9,n-i-27}(\mathbf{tr}(\lambda)\alpha,\beta) - Z_{i,n-i-18}(\alpha,\mathbf{tr}(\lambda)\beta) - Z_{i+18,n-i-27}(\mathbf{tr}(\lambda\sigma(\lambda))\alpha,\beta)\\
&\quad + Z_{i+9,n-i-18}(\mathbf{tr}(\lambda)\alpha,\mathbf{tr}(\lambda)\beta) - Z_{i,n-i-9}(\alpha,\mathbf{tr}(\lambda\sigma(\lambda)+\lambda^2)\beta)\\
&\quad - Z_{i+27,n-i-27}((\sigma(\lambda^3)-\mathbf{N}(\lambda))\alpha,\beta) - Z_{i+18,n-i-18}(\mathbf{tr}(\lambda\sigma(\lambda))\alpha,\mathbf{tr}(\lambda)\beta)\\
&\quad + Z_{i+9,n-i-9}(\mathbf{tr}(\lambda)\alpha,\mathbf{tr}(\lambda\sigma(\lambda)+\lambda^2)\beta)\\
&\quad - Z_{i,n-i}(\alpha,(\mathbf{tr}(\lambda)\mathbf{tr}(\lambda^2)-\lambda^3+\mathbf{N}(\lambda))\beta)\\
&\qquad = R(\alpha\sigma(\beta)) \quad \text{for some function } R\colon \mathbf{w}\to\mathbb{F}_p.
\end{aligned}$$

Now let j,k be such that $k,j \geq e$, (j,k) is regular and $ce < k+j \leq N$. Let $m=j+k$. Applying the regular case argument of Lemma 5.11b) to the cocycle $Z_{|m}$, we have

$$Z_{j,k}(\alpha,\eta\beta) = Z_{j,k}(\eta\alpha,\beta) \text{ for all } \eta\in\Lambda,$$

where Λ is the ring generated by $\{\sigma(\eta)-\eta \mid \mathbf{tr}(\eta)=0\}$. In the case $p=d=3$ it is easy to see that $\Lambda=\mathbf{f}$, so $Z_{j,k}$ is $\mathbf{f}$-balanced. We also know that $Z_{j,k}=Z_{j+9,k-9}$ if $\mathrm{d}_\omega(j,k)=\mathrm{d}_\omega(j+9,k-9)$ (Lemma 5.11a)).

Since $\mathrm{d}_\omega(i,n-i)=\mathrm{d}_\omega(i+27,n-i-27)$, we have

$$Z_{i,n-i}=Z_{i+9,n-i-9}=Z_{i+18,n-i-18}=Z_{i+27,n-i-27},$$

$$Z_{i,n-i-9}=Z_{i+9,n-i-18}=Z_{i+18,n-i-27}$$

and

$$Z_{i,n-i-18}=Z_{i+9,n-i-27}.$$

Using these observations and the fact that $\mathbf{tr}(\lambda\sigma(\lambda))=\mathbf{tr}(\lambda^2)-(\mathbf{tr}\lambda)^2$, we can simplify the left-hand side of (7.2). After setting $D=C_i(=Z_{i,n-i})$, we get

$$D(\alpha,\lambda^3\beta)-D(\sigma(\lambda^3)\alpha,\beta)=R(\alpha\sigma(\beta)).$$

Now let $\alpha'=\sigma(\lambda^3)\alpha$ and $\beta'=\beta/\lambda^3$. Clearly, $\alpha'\sigma(\beta')=\alpha\sigma(\beta)$, whence

$$D(\sigma(\lambda^3)\alpha,\beta)-D(\sigma(\lambda^6)\alpha,\beta/\lambda^3)=R(\alpha\sigma(\beta)).$$

Similarly, we have

$$D(\sigma(\lambda^6)\alpha,\beta/\lambda^3)-D(\sigma(\lambda^9)\alpha,\beta/\lambda^6)=R(\alpha\sigma(\beta)).$$

Adding the last three equations, we get

$$D(\alpha, \lambda^3\beta) = D(\sigma(\lambda^9)\alpha, \beta/\lambda^6).$$

Since λ can be chosen arbitrarily, we conclude that $D(\alpha, \beta)$ depends only on $\alpha\sigma(\beta)$, whence $D(\alpha, \beta) = \mathbf{tr}_0(\mu\alpha\sigma(\beta))$ for some $\mu \in \mathbf{w}$. ∎

7.3 The case $p = 2$, $d = 4$. Let $\mathbf{k}$ be the unique field lying strictly between $\mathbf{f}$ and $\mathbf{w}$ (so that $[\mathbf{k} : \mathbf{f}] = [\mathbf{w} : \mathbf{k}] = 2$). It is easy to show that $\mathbf{tr} = \mathbf{tr}_{\mathbf{w/f}}$ vanishes on $\mathbf{k}$, and $\mathbf{k} = \{\sigma(\eta) - \eta \mid \mathbf{tr}(\eta) = 0\}$.

Proof of Theorem 5.7a): First assume that n is odd, in which case the result is an easy consequence of Lemma 5.9a). Indeed, let η be any element of $\mathbf{k}\backslash\mathbf{f}$. If $i \in I_{good}$ is even, then $\eta[i] = 0$, while $\eta[n - i] \neq 0$ since $n - i$ is prime to $d = 4$. It follows from (5.6) that $C_i = 0$. The case of odd i is similar.

Now assume that n is even. Since $4 \nmid n$, we must have $n \equiv_4 2$. Preliminary information about C is given by the following result.

Lemma 7.2: *Fix an integer i such that $e \leq i \leq n - e$.*

a) *If i is even, then $C_i = 0$.*

b) *If i is odd, then C_i is $\mathbf{k}$-balanced and symmetric, that is, $C_i(\alpha, \beta) = C_i(\beta, \alpha)$.*

Proof: a) If i is even, then either $4 \mid i$ or $4 \mid (n - i)$, so $C_i = 0$ by Claim 5.8.

b) The fact that C_i is $\mathbf{k}$-balanced follows from (5.6) since $\mathbf{k} = \{\sigma(\eta) - \eta \mid \mathbf{tr}(\eta) = 0\}$. Showing that C_i is symmetric is equivalent to showing that $C_i = C_{n-i}$. Note that $i \equiv_4 (n - i)$ since i is odd and $n \equiv_4 2$. If $i > n - i$ and $\varepsilon(i) \geq \varepsilon(n-i)$ (or $i < n-i$ and $\varepsilon(i) \leq \varepsilon(n-i)$), then $C_i = C_{n-i}$ by Lemma 5.9b). If $i > n - i$ and $\varepsilon(i) < \varepsilon(n - i)$ (or vice versa), use the fact that $C_i = C_{i+ae}$ for $1 - \mathrm{d}_\omega(i) \leq a \leq c - 1 - \mathrm{d}_\omega(i)$ and apply the above argument. ∎

Next we use W-action formula. Given $\alpha, \lambda \in \mathbf{w}$ and $k \geq e$, let $g = g(\lambda, s)$ and $u = \alpha x^k$.

If $k \equiv_4 1$, then

$$u^g = \alpha(x^k + (\lambda + \sigma^2(\lambda))x^{k+4s} + (\sigma(\lambda^2) + \lambda\sigma^2(\lambda))x^{k+8s} + \cdots).$$

If $k \equiv_4 3$, then

$$u^g = \alpha(x^k + (\sigma(\lambda) + \sigma^3(\lambda))x^{k+4s} + (\mathbf{tr}(\lambda^2) + \sigma^2(\lambda^2) + \sigma(\lambda)\sigma^3(\lambda))x^{k+8s} + \cdots).$$

Fix i such that $e \leq i \leq n - e$ and assume that $i \equiv_4 1$. As in the case $p = d = 3$, we can assume that $\mathrm{d}_\omega(i, n - i) = \mathrm{d}_\omega(i + 16, n - i - 16)$. Now let

$\mathfrak{c}\colon G \times L \to \mathbb{F}_p$ be a map which is compatible with Z and linear in the second argument (unlike the case $p = d = 3$, the last condition will be used). We shall apply the compatibility equation $Z(u,v) - Z(u^g, v^g) = \mathfrak{c}(g, [u,v])$ to the elements $u = \alpha x^i$, $v = \beta x^{n-i-16}$ and $g = g(\lambda, 2)$, where λ, α, β are arbitrary elements of $\mathbf{w}$.

Since $\mathbf{k} = \{\sigma(\eta) - \eta \mid \mathbf{tr}(\eta) = 0\}$, it follows from Lemma 5.9a) that $Z_{k,j}$ is $\mathbf{k}$-balanced whenever $k, j \geq e$, $ce \leq k + j \leq N$, (k,j) is regular, k and j are odd, and $k \equiv_4 j$. Computing u^g and v^g by W-action formula and simplifying the expression $Z(u,v) - Z(u^g, v^g)$ using the above observation, we get

$$\begin{aligned} &Z_{i,n-i}(\alpha, \beta(\sigma(\lambda^2) + \lambda\sigma^2(\lambda))) + Z_{i+8,n-i-8}(\alpha(\lambda + \sigma^2(\lambda)), \beta(\lambda + \sigma^2(\lambda))) \\ &+ Z_{i+16,n-i-16}(\alpha(\sigma(\lambda^2) + \lambda\sigma^2(\lambda)), \beta) = R(\lambda, \alpha\sigma(\beta) - \beta\sigma(\alpha)), \end{aligned} \tag{7.3}$$

where R is linear in the second argument. Let $D = C_i (= Z_{i,n-i} = Z_{i+8,n-i-8} = Z_{i+16,n-i-16})$. Writing μ for $\sigma(\lambda^2)$ in (7.3) and simplifying further, we get

$$D(\alpha\mu, \beta) + D(\alpha, \beta\sigma^2(\mu)) + D(\alpha, \beta \cdot \mathbf{tr}(\mu)) = R(\sigma^{-1}(\sqrt{\mu}), \alpha\sigma(\beta) - \beta\sigma(\alpha)). \tag{7.4}$$

Before proving that $D = 0$, we establish an auxiliary result.

Claim 7.3: *The following hold:*
(i) *D vanishes on $\mathbf{k}\upsilon \times \mathbf{k}\upsilon$ for any $\upsilon \in \mathbf{w}$.*
(ii) *There exists $\lambda \in \mathbf{k}$ such that $D(\alpha, \beta) = \mathbf{tr}_0(\lambda\alpha\sigma^2(\beta))$ for all $\alpha, \beta \in \mathbf{w}$.*

Proof: Let $\mu \in \mathbf{w}$ be such that $\sigma^2(\mu) = \mu + 1$. It is clear that $\mathbf{tr}(\mu) = 0$. Applying (7.4) with this value of μ and $\alpha = \beta$, we get

$$D(\alpha\mu, \alpha) + D(\alpha, \alpha\mu) + D(\alpha, \alpha) = 0.$$

Since D is symmetric, we conclude that $D(\alpha, \alpha) = 0$ for all $\alpha \in \mathbf{w}$.

Now fix $\upsilon \in \mathbf{w}$. Given $\lambda, \mu \in \mathbf{k}\upsilon$, let $\alpha = \sqrt{\lambda\mu}$ and $\kappa = \sqrt{\lambda/\mu}$. Since $\kappa \in \mathbf{k}$ and D is $\mathbf{k}$-balanced, we have $D(\lambda, \mu) = D(\alpha\kappa, \frac{\alpha}{\kappa}) = D(\alpha, \alpha) = 0$. So, we proved (i).

Part (ii) will be proved by dimension counting. Fix $\upsilon \in \mathbf{w}$ such that $\mathbf{w} = \mathbf{k} \oplus \mathbf{k}\upsilon$. Let V be the space of bilinear maps from $\mathbf{w} \times \mathbf{w}$ to $\mathbb{F}_p$ that are $\mathbf{k}$-balanced, symmetric and vanish on $\mathbf{k} \times \mathbf{k}$ and $\mathbf{k}\upsilon \times \mathbf{k}\upsilon$. Clearly, a map from V is uniquely determined by its values on $\{(1, \kappa\upsilon) \mid \kappa \in \mathbf{k}\}$. Therefore, $\dim_{\mathbb{F}_p} V \leq [\mathbf{k} : \mathbf{f}_0]$ (recall that $\mathbf{f}_0 \cong \mathbb{F}_p$). On the other hand, every map of the form $(\alpha, \beta) \mapsto \mathbf{tr}_0(\lambda\alpha\sigma^2(\beta))$, with $\lambda \in \mathbf{k}$, lies in V since $\mathbf{k}$ is the fixed field of σ^2. Clearly, the subspace of these trace maps has dimension $[\mathbf{k} : \mathbf{f}_0]$, so we are done. ∎

An immediate consequence of part (ii) of the above claim is that

$$D(\alpha\mu, \beta) = D(\alpha, \beta\sigma^2(\mu)) \quad \text{for all } \alpha, \beta, \mu \in \mathbf{w}.$$

Thus (7.4) simplifies to

$$D(\alpha, \beta \cdot \mathbf{tr}(\mu)) = R(\sigma^{-1}(\sqrt{\mu}), \alpha\sigma(\beta) - \beta\sigma(\alpha)).$$

Now fix μ, with $\mathbf{tr}(\mu) = 1$, and let $F(x) = R(\sigma^{-1}(\sqrt{\mu}), x)$. Thus, $D(\alpha, \beta) = F(\alpha\sigma(\beta) - \beta\sigma(\alpha))$ for all $\alpha, \beta \in \mathbf{w}$, where $F\colon \mathbf{w} \to \mathbb{F}_p$ is linear.

Choose $\kappa \in \mathbf{k}$ with $\sigma(\kappa) = \kappa + 1$. By Claim 7.3(i) for any $\alpha \in \mathbf{w}$ we have

$$0 = D(\alpha, \alpha\kappa) = F(\alpha\sigma(\alpha)(\sigma(\kappa) - \kappa)) = F(\alpha\sigma(\alpha)).$$

Since F is linear, for any $\alpha, \beta \in \mathbf{w}$ we have

$$F(\alpha\sigma(\beta) + \beta\sigma(\alpha)) = F((\alpha + \beta)\sigma(\alpha + \beta)) - F(\alpha\sigma(\alpha)) - F(\beta\sigma(\beta)) = 0.$$

Hence, D is identically zero. Thus we showed that $C_i = 0$ if $i \equiv_4 1$. The case $i \equiv_4 3$ can be done in a similar way, but it can also be deduced from the case $i \equiv_4 1$ using the semi-cocycle identity. ∎

Proof of Lemma 5.11b): Arguing as in the regular case, we have

$$Z_{i,n-i}(\alpha\sigma(\eta), \beta) = Z_{i,n-i}(\alpha, \eta\beta) \quad \text{for all } \alpha, \beta \in \mathbf{w} \text{ and } \eta \in \mathbf{k}. \tag{7.5}$$

We must now prove the above formula for $\eta \notin \mathbf{k}$. Once again, we can assume that $\mathrm{d}_\omega(i, n-i) = \mathrm{d}_\omega(i+16, n-i-16)$. Arguing as before and taking (7.5) into account, we get

$$D(\alpha\sigma(\lambda^2), \beta) + D(\alpha, \beta\lambda^2) = R(\alpha\sigma(\beta)) \quad \text{for any } \alpha, \beta, \lambda \in \mathbf{w}, \tag{7.6}$$

where $D = Z_{i,n-i} = Z_{i+8,n-i-8} = Z_{i+16,n-i-16}$ and R is some function. Now arguing as in the case $p = d = 3$, we conclude that $D(\alpha\sigma(\lambda^4), \beta/\lambda^2) = D(\alpha, \beta\lambda^2)$, and the assertion of the Lemma follows. ∎

8. The case $p = d = 2$

This is the most demanding case. The main problem here is that the Lie algebra of G with respect to any basic filtration (as defined in section 3) is solvable, and while its second cohomology is computable, it does not yield enough information about group cocycles via the compatibility equation.

The filtration we use in this case is less natural, the associated Lie algebra has more complex structure, and the corresponding associative algebras cannot be defined at all. The proof becomes more technical, although it is based on similar ideas.

As before, let G_n be the n^{th} congruence subgroup of G, and let $E_n = W^* \cap G_n$. The following relations are easy to check.

LEMMA 8.1: *The following hold:*

a) $G_n^2 \subseteq G_{2n}$ *for all* $n \geq 1$;
b) $\gamma_n G = G_{2n-2}$ *for all* $n \geq 4$;
c) $(E_n, E_m) = 1$ *for all* $n, m \geq 1$;
d) $(E_n, G_m) \subseteq G_{m+2n}$ *for all* $n, m \geq 1$.

As in the regular case, fix an elementary cover $(\hat{G}, \phi)$ of G and let $N = \operatorname{dep}(\hat{G}, \phi)$. We shall assume that $N \geq 100p^3d = 1600$ and reach a contradiction.

We start by defining the filtrations $\{\omega_i G\}$ of G and $\{\omega_i \hat{G}\}$ of $\hat{G}$. Choose the numbers c and e such that $4 \mid c$ and

$$(e+1)(2c-1) < N < 2ce \tag{8.1}$$

Let $\omega_1 G = \gamma_{e+1} G$ and let $\omega_1 \hat{G} = \gamma_{e+1} \hat{G}$. For $2 \leq i \leq c$, set $\omega_i G = (\omega_{i-1} G, \omega_1 G) \cdot (\omega_{i-1} G)^2$ and $\omega_i \hat{G} = (\omega_{i-1} \hat{G}, \omega_1 \hat{G}) \cdot (\omega_{i-1} \hat{G})^2$. Finally, for $i > c$, set $\omega_i G = \gamma_{N+1} G$ and $\omega_i \hat{G} = \gamma_{N+1} \hat{G}$.

The subgroups $\{\omega_i G\}_{i=1}^{c}$ can be described explicitly as follows:

$$\begin{gathered} \omega_1 G = G_{2e}, \quad \omega_2 G = G_{6e} \cdot E_{4e}, \quad \omega_3 G = G_{10e} \cdot E_{8e}, \\ \omega_k G = G_{(4k-2)e} \cdot E_{(4k-4)e+2} \text{ for } 4 \leq k \leq c, \quad \omega_{c+1} G = G_{2N}. \end{gathered} \tag{8.2}$$

While $\{\omega_i \hat{G}\}$ and $\{\omega_i G\}$ are not basic filtrations, the construction of Section 3 can still be applied. There are a few things to check though. First, we need to show that $\{\omega_i G\}$ and $\{\omega_i \hat{G}\}$ are indeed 2-filtrations of G and $\hat{G}$, respectively. Moreover, in order to apply Lemma 3.6 and Lemma 3.7, we must show that $\omega_c G \supseteq \gamma_{N-1} G$ and $\omega_c \hat{G} \supseteq \gamma_{N-1} \hat{G}$. Clearly, it suffices to verify the following inclusions:

$$\text{a) } (\omega_c G)^2 \subseteq \omega_{c+1} G \quad \text{b) } (\omega_c G, \omega_1 G) \subseteq \omega_{c+1} G \quad \text{c) } \omega_c G \supseteq \gamma_{(2c-1)e+1} G \tag{8.3}$$

$$\text{d) } (\omega_c \hat{G})^2 \subseteq \omega_{c+1} \hat{G} \quad \text{e) } (\omega_c \hat{G}, \omega_1 \hat{G}) \subseteq \omega_{c+1} \hat{G} \quad \text{f) } \omega_c \hat{G} \supseteq \gamma_{(2c-1)e+1} \hat{G}. \tag{8.4}$$

Inclusions a), b) and c) follow immediately from Lemma 8.1 and (8.2).

d) By (8.2) and Lemma 8.1 we have $\omega_c G \subseteq \gamma_{(2c-2)e+2} G$. It is clear from the definition that $\phi(\omega_c \hat{G}) = \omega_c G$, whence $\omega_c \hat{G} \subseteq \gamma_{(2c-2)e+2} \hat{G} \cdot \operatorname{Ker} \phi$. Now $\operatorname{Ker} \phi$ is

central and has order 2, so $(\omega_c\hat{G})^2 \subseteq (\gamma_{(2c-2)e+2}\hat{G})^2$. Finally, $(\gamma_{(2c-2)e+2}\hat{G})^2 \subseteq \gamma_{N+1}\hat{G}$ by Lemma 3.2 (where $f(i) = 2i-2$).

e) Let $\hat{E}_n = \phi^{-1}(E_n)$. Arguing as in d), we have $\omega_c\hat{G} \subseteq \gamma_{(2c-1)e+1}\hat{G} \cdot \hat{E}_{(4c-4)e+2}$, whence

$$(\omega_c\hat{G}, \omega_1\hat{G}) \subseteq (\gamma_{(2c-1)e+1}\hat{G}\cdot\hat{E}_{(4c-4)e+2}, \gamma_{e+1}\hat{G}) \subseteq \gamma_{2ce+2}\hat{G}\cdot(\hat{E}_{(4c-4)e+2}, \gamma_{e+1}\hat{G}).$$

By assumption $2ce > N$, so $\gamma_{2ce+2}\hat{G} \subseteq \gamma_{N+1}\hat{G} = \omega_{c+1}\hat{G}$. Now

$$(\hat{E}_{(4c-4)e+2}, \gamma_{e+1}\hat{G}) = (\hat{E}_{(4c-4)e+2}, (\gamma_e\hat{G}, \hat{G})) \subseteq$$
$$(8.5) \qquad ((\hat{E}_{(4c-4)e+2}, \hat{G}), \gamma_e\hat{G})((\hat{E}_{(4c-4)e+2}, \gamma_e\hat{G}), \hat{G}) \subseteq ((\hat{E}_{(4c-4)e+2}, \hat{G}), \hat{G}).$$

For each $n \geq 1$ we have $(E_n, G) \subseteq E_{2n+1}$ by Lemma 8.1, whence $(\hat{E}_n, \hat{G}) \subseteq \hat{E}_{2n+1}$. It follows immediately that $(\hat{E}_{(4c-4)e+2}, \hat{G}) \subseteq \gamma_{(4c-4)e+2}\hat{G} \cdot \operatorname{Ker}\phi \subseteq \gamma_N\hat{G}$, whence $(\hat{E}_{(4c-4)e+2}, \gamma_{e+1}\hat{G}) \subseteq \gamma_{N+1}\hat{G}$ by (8.5).

f) We know that $\omega_c G \supset G_{(4c-2)e} = \gamma_{(2c-1)e+1}G$, whence $\gamma_{(2c-1)e+1}\hat{G} \subseteq \omega_c\hat{G}\gamma_N\hat{G}$. Since $N > (2c-1)e+1$, a standard argument implies that

$$\gamma_{(2c-1)e+1}\hat{G} \subseteq \omega_c\hat{G}.$$

In order to describe the Lie algebra $L = L^\omega(G)$ we need the following lemma.

LEMMA 8.2: *Let $\alpha \in \mathbf{w}$ and $n \in \mathbb{N}$, and assume that $\alpha \in \mathbf{f}$ if n is even. Then there exists $g = g_{\alpha,n} \in G$ such that $g \equiv 1 + \alpha\pi^n + \beta\pi^{2n} \bmod U_{3n}$ for some $\beta \in \mathbf{w}$. Moreover, if g is of the above form, then $\mathbf{tr}(\beta) = \alpha\sigma(\alpha)$.*

Proof: The proof is similar to that of Proposition 4.1a). ∎

Remark: Since $[\mathbf{w} : \mathbf{f}] = 2$ and $p = 2$, $\alpha \in \mathbf{f}$ if and only if $\mathbf{tr}(\alpha) = 0$.

Let $S = \{(\alpha, n) \in \mathbf{w} \times \mathbb{N} \mid n \geq 2e \text{ and } \alpha \in \mathbf{f} \text{ if } n \text{ is even}\}$. For each $(\alpha, n) \in S$ choose $g_{\alpha,n} \in G$ satisfying the conclusion of Lemma 8.2. It is clear that $\mathrm{LT}_\omega(g_{\alpha,n})$ does not depend on the choice of $g_{\alpha,n}$, and $\mathrm{LT}_\omega(g_{\alpha,n}) + \mathrm{LT}_\omega(g_{\beta,n}) = \mathrm{LT}_\omega(g_{\alpha+\beta,n})$.

Now we can identify L with a subspace of $\mathfrak{L} = \bigoplus_{i=2e}^{2N-1} \mathbf{w}x^i$ via the linear map defined by $\mathrm{LT}_\omega(g_{\alpha,n}) \mapsto \alpha x^n$. Under this identification the ω-homogeneous components $\{L_i^\omega\}_{i=1}^c$ are given as follows:

$$L_1^\omega = \bigoplus_{i=e}^{2e-1} \mathbf{f}x^{2i} \oplus \bigoplus_{i=e}^{3e-1} \mathbf{w}x^{2i+1}$$

$$L_2^\omega = \bigoplus_{i=2e}^{4e-1} \mathbf{f}x^{2i} \oplus \bigoplus_{i=3e}^{5e-1} \mathbf{w}x^{2i+1}$$
$$L_3^\omega = \bigoplus_{i=4e}^{6e} \mathbf{f}x^{2i} \oplus \bigoplus_{i=5e}^{7e-1} \mathbf{w}x^{2i+1}$$
$$L_k^\omega = \bigoplus_{i=(2k-2)e+1}^{2ke} \mathbf{f}x^{2i} \oplus \bigoplus_{i=(2k-1)e}^{(2k+1)e-1} \mathbf{w}x^{2i+1} \quad \text{for } 4 \le k \le c-1$$
$$L_c^\omega = \bigoplus_{i=(2c-2)e+1}^{N-1} \mathbf{f}x^{2i} \oplus \bigoplus_{i=(2c-1)e}^{N-1} \mathbf{w}x^{2i+1}.$$

Given $n \in \mathbb{N}$, with $2e \le n \le 2N-1$, let $\mathrm{d}_\omega(n)$ be the unique number k such that $x^n \in L_k^\omega$. If $n > 2N-1$, set $\mathrm{d}_\omega(n) = \infty$.

Unlike the regular case, it is not true in general that $[L \cap \mathbf{w}x^n, L \cap \mathbf{w}x^m] \subseteq L \cap \mathbf{w}x^{n+m}$ (although this is true if $\mathrm{d}_\omega(n) \ge 2$ and $\mathrm{d}_\omega(m) \ge 2$), so there is no direct analogue of the "thin" grading on L. We will go around this problem by considering the smaller algebra $L^{\mathrm{good}} := \bigoplus_{i=e}^{N-1} \mathbf{f}x^{2i} \oplus \bigoplus_{i=2e}^{N-1} \mathbf{w}x^{2i+1}$. The Lie bracket on L^{good} is given by the following formulas:

$$[\alpha x^{2i+1}, \beta x^{2j}] = \alpha\beta^2 x^{2(i+2j)+1}, \quad \text{if } \mathrm{d}_\omega(2i+1)+1 = \mathrm{d}_\omega(2i+4j+1)),$$
$$[\alpha x^{2i+1}, \beta x^{2j+1}] = (\alpha\sigma(\beta) - \beta\sigma(\alpha))x^{2(i+j+1)},$$
$$\text{if } \mathrm{d}_\omega(2i+1) + \mathrm{d}_\omega(2j+1) = \mathrm{d}_\omega(2(i+j+1)),$$

and all other commutators of the form $[\alpha x^k, \beta x^l]$ are equal to zero.

Moreover, L^{good} is invariant under the action of G. Finally, L^{good} admits another grading $\bigoplus_{i=4e}^{2N-1} L_i$, where

$$L_n = \begin{cases} \mathbf{f}x^n \oplus \mathbf{f}x^{n/2} & \text{if } 4 \mid n \text{ and } 4e \le n \le 8e-4 \\ L \cap \mathbf{w}x^n, & \text{otherwise.} \end{cases} \tag{8.6}$$

If C is a cocycle of L and $n \ge 8e$, we define $C_{|n}$ (the weight n component of C) to be the cocycle of L^{good} (not the entire L) given as follows. If $u \in L_i$ and $v \in L_j$, set

$$C_{|n}(u,v) = \begin{cases} C(u,v) & \text{if } i+j = n \\ 0 & \text{if } i+j \ne n. \end{cases}$$

Finally, as before we set $C_{i,j}(\alpha,\beta) = C(\alpha x^i, \beta x^j)$.

8.1 Cocycle descriptions. In this subsection we obtain partial information about homogeneous cocycles of L^{good}. Fix n such that $\mathrm{d}_\omega(n) = c$. If n is even,

assume in addition that $n \geq (4c-2)e+14$ (note that $2N-2 \geq (4c-2)e+14$ by (8.1)). Let C be the weight n component of some admissible cocycle of L.

Case 1: *n is odd.* We claim that C is a coboundary. Replacing C by $C-B$ for some coboundary B, we can assume that $C(x^{2e}, \beta x^{n-4e}) = 0$ for all $\beta \in \mathbf{w}$. Under this assumption, we shall prove that $C = 0$.

It is enough to show that $C(\alpha x^{n-m}, \beta x^m) = 0$ for all odd m such that $\alpha x^{n-m}, \beta x^m \in L^{\mathrm{good}}$. Assume first that $3 \leq \mathrm{d}_\omega(m)$. Then we have

$$\begin{aligned} C(\alpha x^{n-m}, \beta x^m) &= C(\alpha x^{n-m}, [\beta x^{m-4e}, x^{2e}]) \\ &= C([\alpha x^{n-m}, \beta x^{m-4e}], x^{2e}) + C([\alpha x^{n-m}, x^{2e}], \beta x^{m-4e}). \end{aligned} \tag{8.7}$$

In the last expression the first term is equal to zero by assumption, while the second term is zero since $[\alpha x^{n-m}, x^{2e}] = 0$ (as both $n-m$ and $2e$ are even).

If $\mathrm{d}_\omega(m) \leq 2$, write αx^{n-m} in the form $[\alpha_1 x^k, \alpha_2 x^l]$, where k and l are both odd and $k, l \geq 4e+1$, and use semi-cocycle identity.

Case 2: *n is even (recall that $(4c-2)e+14 \leq n \leq 2N-2$ by our assumption).* In this case we will use W-action formula. When $p = d = 2$, it gives the following. Assume that $k \geq e$ is odd, $\alpha, \lambda \in \mathbf{w}$, $s \geq 1$. Let $u = \alpha x^k$ and $g = g(\lambda, s)$. Then

$$u^g = \alpha(x^k + \mathbf{tr}(\lambda^2)x^{k+4s} + \sigma(\lambda^2)\mathbf{tr}(\lambda^2)x^{k+8s} + \cdots). \tag{8.8}$$

An argument similar to the ones we used in other exceptional cases yields the following. Let $I_{reg} := \{i \in \mathbb{N} \mid 4e \leq i \leq N-4e \text{ and } i \text{ is odd}\}$. If $m \geq (4c-2)e+14$ is even and $i \in I_{reg}$, then

$$C_{i,m-i} = C_{i+4,m-i-4} \text{ if } \mathrm{d}_\omega(i, m-i) = \mathrm{d}_\omega(i+4, m-i-4); \tag{8.9}$$

$$C_{i,m-i} \text{ is } \mathbf{f}\text{-balanced}. \tag{8.10}$$

From now on we write C_i for $C_{i,n-i}$. Let $r = n-(4c-2)e$. Note that by our assumptions on n we have $14 \leq r < 2e$.

Claim 8.3: *Suppose that $i = (4a+2)e + (2b+1)$, where $1 \leq a \leq c-2$ and $0 \leq b < e + r/2$. Then there exists $\lambda_i \in \mathbf{w}$ such that $C_i(\alpha, \beta) = \mathbf{tr}_0(\lambda_i \alpha \sigma(\beta))$ for all $\alpha, \beta \in \mathbf{w}$. Moreover, λ_i depends only on the parity of a and b.*

Proof: First we will show that if a is fixed, then C_i depends only on the parity of b. Indeed, let $i = (4a+2)e + (2b+1)$ and $i' = (4a+2)e + (2b'+1)$, where b and b' have the same parity and $0 \leq b, b' < e + r/2$. Then $n - i =$

$(4(c-a-2)+2)e+(2e-2b-1+r)$ and $n-i' = (4(c-a-2)+2)e+(2e-2b'-1+r)$, so clearly $\mathrm{d}_\omega(i, n-i) = \mathrm{d}_\omega(i', n-i')$, whence $\lambda_i = \lambda_{i'}$ by (8.9).

Now fix b. To prove that C_i depends only on the parity of a, we must show that $C_i = C_{i+8e}$ or, equivalently, $C_{i+4e} - C_i = C_{i+8e} - C_{i+4e}$. We have

$$\begin{aligned} C_{i+4e}(\alpha,\beta) - C_i(\alpha,\beta) &= C([\alpha x^i, x^{2e}], \beta x^{n-i-4e}) - C(\alpha x^i, [\beta x^{n-i-4e}, x^{2e}]) \\ &= C([\alpha x^i, \beta x^{n-i-4e}], x^{2e}) \\ &= C((\alpha\sigma(\beta) - \beta\sigma(\alpha))x^{n-4e}, x^{2e}). \end{aligned}$$

The last expression is independent of i, and we are done.

Now we establish the first assertion of the claim. Since $C_i = C_{(4a+2)e+(2b+1)}$ depends only the parity of a and b, we can assume that $0 < b < 2$, in which case $\mathrm{d}_\omega(i, n-i-8) = \mathrm{d}_\omega(i+8, n-i)$. Let $\mathfrak{c}$ be a map compatible with C. Given $\alpha, \beta, \mu \in \mathbf{w}$, we use the compatibility equation (3.2) with $u = \alpha x^i$, $v = \beta x^{n-i-8}$ and $g = g(\sqrt{\mu}, 1)$. Applying W-action formula and using (8.9) and (8.10), we get

$$D(\alpha, \sigma(\mu)\mathbf{tr}(\mu)\beta) + D(\mathbf{tr}(\mu)\alpha, \mathbf{tr}(\mu)\beta) + D(\alpha\sigma(\mu)\mathbf{tr}(\mu), \beta) = R(\alpha\sigma(\beta)),$$

where $D = C_i$ and R is some function. Since $\mathbf{tr}(\mu) = \mu + \sigma(\mu)$ and D is $\mathbf{f}$-balanced, we have

$$D(\alpha, \sigma(\mu)\mathbf{tr}(\mu)\beta) + D(\mu\mathbf{tr}(\mu)\alpha, \beta) = R(\alpha\sigma(\beta)).$$

Arguing as in other exceptional cases, we conclude that $D(\alpha, \beta) = \mathbf{tr}(\lambda_i \alpha\sigma(\beta))$ for some $\lambda_i \in \mathbf{w}$. ∎

For the rest of the section, we set

$$\mu_{k,l} = \lambda_{(4k+2)e+(2l+1)}, \quad \text{where } 1 \le k < c \text{ and } 0 \le l < e + r/2.$$

According to Claim 8.3, $\mu_{k,l}$ depends only on the parity of k and l.

LEMMA 8.4: *Let k, l be as above.*

a) *If $n \equiv_4 2$, then $\mu_{k,l} \in \mathbf{f}$.*

b) *If $4 \mid n$, then $\mu_{k,l} = \sigma(\mu_{k,l+1})$.*

Proof: a) Let $i = (4k+2)e + (2l+1)$ and let $r = n - (4c-2)e$ as before. Since $C_i(\alpha, \beta) = C_{n-i}(\beta, \alpha)$, we have

$$\mathbf{tr}_0(\lambda_{(4k+2)e+(2l+1)}\alpha\sigma(\beta)) = \mathbf{tr}_0(\lambda_{((4(c-k-2)+2)e+2e+r-(2l+1)}\beta\sigma(\alpha)),$$

whence $\mu_{k,l} = \sigma(\mu_{c-k-2,e-l-1+r/2})$. Since c and e are even, $\mu_{c-k-2,e-l-1+r/2} = \mu_{k,e-l-1+r/2} = \mu_{k,r/2+1+l}$. Since $n \equiv_4 2$, $r/2+1$ is even. We get $\mu_{k,l} = \sigma(\mu_{k,l})$, whence $\mu_{k,l} \in \mathbf{f}$.

Proof of b) is analogous. ∎

8.2 Proof of Theorem 5.1. Let $Z = Z_f$ and $\mathfrak{z} = \mathfrak{z}_f$ be defined as in Section 3. Recall that by Lemma 3.7, $\mathfrak{z}$ does not vanish on $G \times U$, where $U = \gamma_{N-1}G/\gamma_{N+1}G$. On the other hand, $\mathfrak{z}$ vanishes on $G \times V$, where $V = \gamma_N G/\gamma_{N+1}G$. Since $U = V \oplus \mathbf{w}x^{2N-3} \oplus \mathbf{f}x^{2N-4}$, there exists $\alpha \in \mathbf{w}$ and $g \in G$ such that either $\mathfrak{z}(g, \alpha x^{2N-4}) \neq 0$ or $\mathfrak{z}(g, \alpha x^{2N-3}) \neq 0$. We are going to construct an ω-splitting f for which the above assertion does not hold, thus reaching a contradiction.

We start with a simple observation.

Claim 8.5: *Let n be even, with $\mathrm{d}_\omega(n) = c$, and let $\lambda \in \mathbf{f}$. Define $\mathcal{D}_{\lambda,n}\colon L^{\mathrm{good}} \times L^{\mathrm{good}} \to \mathbb{F}_p$ by setting*

$$\mathcal{D}_{\lambda,n}(\alpha x^i, \beta x^j) = \begin{cases} \mathbf{tr}_0(\lambda\alpha\sigma(\beta)) & \text{if } i+j=n, \mathrm{d}_\omega(i)+\mathrm{d}_\omega(j)=c \text{ and } i \text{ is odd,} \\ 0 & \text{otherwise.} \end{cases}$$

Then $\mathcal{D}_{\lambda,n}$ is a coboundary.

Proof: Note that the above definition of $\mathcal{D}_{\lambda,n}$ is essentially the same as the one used in Section 5 (we simplified the formula using the fact that $\lambda(i) = i\lambda$ for $\lambda \in \mathbf{f}$). Thus we can simply adjust the argument of Proposition 5.5b). ∎

Now let f be some ω-splitting, and let $Z = Z_f$. For the rest of the section we set $C = Z_{|2N-2}$, and let $\lambda_k, \mu_{k,l}$ be as in the conclusion of Claim 8.3 applied to C.

Proposition 8.6: *We can choose f so that the following conditions are satisfied:*

a) *$Z_{|n} = 0$ for all odd n, with $\mathrm{d}_\omega(n) = c$.*

b) *Either $\mu_{1,2} = 0$ or $\mu_{1,2} \notin \mathbf{f}$.*

Proof: a) In the last subsection we showed that $Z_{|n}$ is a coboundary (of L^{good}) for any choice of f. Therefore, by changing f, we can assume that $Z_{|n} = 0$.

b) This is a direct consequence of Claim 8.5. ∎

From now we assume that f satisfies the conclusion of Proposition 8.6. Note that $Z = Z_f$ vanishes on $L_i \times L_j$ if either

A) $i+j$ is odd and $\mathrm{d}_\omega(i+j) = c$ or

B)[10] $i + j \geq 2N$.

Indeed, A) holds by Proposition 8.6a). If both i and j are odd, B) can be proved in the same way as Claim 5.3. Finally, B) in the case of i and j even follows from B) in the case of i and j odd and the semi-cocycle identity.

Now let $g \in G$ and $\alpha \in \mathbf{w}$ be arbitrary. Write g in the form $1 + a\pi + b\pi^2 + \cdots$, where $a, b \in \mathbf{w}$. By Lemma 8.2, we have $\mathbf{tr}(b) = a\sigma(a)$. If m is odd and $u = \alpha x^m$, direct computation shows that

$$u^g = \alpha x^m + \mathbf{tr}(a\sigma(\alpha))x^{m+1} + a^2\sigma(\alpha)x^{m+2} + \cdots.$$

It is also easy to see that

$$(x^{2e})^g = x^{2e} + ax^{4e+1}.$$

Using properties A) and B) above we have

$$\begin{aligned}
\mathfrak{z}(g, \alpha x^{2N-3}) &= \mathfrak{z}(g, [\alpha x^{2N-3-4e}, x^{2e}]) \\
&= Z((\alpha x^{2N-3-4e})^g, (x^{2e})^g) - Z(\alpha x^{2N-3-4e}, x^{2e}) \\
&= Z(\alpha x^{2N-3-4e} + \mathbf{tr}(a\sigma(\alpha))x^{2N-2-4e}, x^{2e} + ax^{4e+1}) \\
&\quad - Z(\alpha x^{2N-3-4e}, x^{2e}) \\
&= Z(\alpha x^{2N-3-4e}, ax^{4e+1}) + Z(\mathbf{tr}(a\sigma(\alpha))x^{2N-2-4e}, x^{2e}) \\
&= Z([\alpha x^{2N-3-8e}, x^{2e}], ax^{4e+1}) + Z([ax^{4e+1}, \alpha x^{2N-3-8e}], x^{2e}) \\
&= Z([x^{2e}, ax^{4e+1}], \alpha x^{2N-3-8e}) = Z(ax^{8e+1}, \alpha x^{2N-3-8e}) \\
&= \mathbf{tr}_0(\mu_{1,2} a\sigma(\alpha)). \qquad (8.11)
\end{aligned}$$

Next we compute $\mathfrak{z}(g, \alpha x^{2N-4})$ (this time $\alpha \in \mathbf{f}$). Choose odd numbers k and l such that $k + l = 2N - 4$ and $\mathrm{d}_\omega(k) = \mathrm{d}_\omega(l) = c/2$. Choose $\beta, \gamma \in \mathbf{w}$ such that $\alpha = \mathbf{tr}(\beta\sigma(\gamma))$. We have

$$\begin{aligned}
\mathfrak{z}(g, \alpha x^{2N-4}) = \mathfrak{z}(g, [\beta x^k, \gamma x^l]) &= Z(\beta x^k + \mathbf{tr}(a\sigma(\beta))x^{k+1} + a^2\sigma(\beta)x^{k+2}, \\
\gamma x^l + \mathbf{tr}(a\sigma(\gamma))x^{l+1} + a^2\sigma(\gamma)x^{l+2}) &- Z(\beta x^k, \gamma x^l) \\
&= Z(\beta x^k, a^2\sigma(\gamma)x^{l+2}) + Z(a^2\sigma(\beta)x^{k+2}, \gamma x^l) \\
&= \mathbf{tr}_0((\lambda_k + \lambda_l)\beta\gamma\sigma(a^2)). \qquad (8.12)
\end{aligned}$$

We are now ready to prove that $\mathfrak{z}$ vanishes on $G \times (\mathbf{w}x^{2N-3} \oplus \mathbf{f}x^{2N-4})$.

10 Note that x^{2e} lies in L_{4e}, not in L_{2e}, according to (8.6).

CASE 1: *N is odd.* First of all, we claim that $\mathfrak{z}(g, \alpha x^{2N-4}) = 0$ for all $\alpha \in \mathbf{f}$ and $g \in G$. Indeed, if k and l are as in (8.12), then $k \equiv_4 l$, whence $\lambda_k = \lambda_l$.

Now let $\theta \in \mathbf{f}$, and let $g = 1 + \theta\pi + \cdots$. Arguing as in Section 6 (case 3), we conclude that $Z(x^{N-2}, \theta^2 x^N) = \mathfrak{z}(g, x^{2N-4})$ (see (6.4)). We just showed that $\mathfrak{z}(g, x^{2N-4}) = 0$. Therefore, $\mathbf{tr}_0(\lambda_N \theta^2) = Z(x^{N-2}, \theta^2 x^N) = 0$ for all $\theta \in \mathbf{f}$, whence $\mathbf{tr}(\lambda_N) = 0$, i.e., $\lambda_N \in \mathbf{f}$. Now $N = (4(c/2-1)+2)e + r$ where $e < r < 2e$. Since $4 \mid c$, we have $\lambda_N = \lambda_{c/2-1,r} = \mu_{1,1}$ or $\mu_{1,2}$. Since C has weight $2N-2$ and $4 \mid (2N-2)$, $\mu_{1,2} = \sigma(\mu_{1,1})$ by Lemma 8.4b). Therefore, $\mu_{1,2} = \mu_{1,1} \in \mathbf{f}$. By Proposition 8.6b) we have $\mu_{1,2} = 0$, so according to (8.11), $\mathfrak{z}(g, \alpha x^{2N-3}) = 0$ for all $\alpha \in \mathbf{w}$ and $g \in G$.

CASE 2: *N is even.* We apply the procedure described in [PR, 7.3]. Let $\omega \in D$ be such that

$$\omega^2 + \omega\pi^2 = \pi^2. \tag{8.13}$$

Then $\omega \in \mathfrak{m}_D$; moreover, $\omega = \pi + \xi\pi^2 + \cdots$, where $\mathbf{tr}(\xi) = 1$, and $1 + \omega \in G$. Note that $\omega^2/(1-\omega) = \pi^2$, whence $K := \mathbf{f}((\omega))$ is an extension of $F = \mathbf{f}((\pi^2))$ of degree 2. Now $\omega/(1-\omega)$ is also a root of (8.13), whence there exists $A \in \mathrm{Gal}(K/F)$ such that $A(\omega) = \omega/(1-\omega)$.

Fix $\theta \in \mathbf{f}$. Let $b := (1 + \theta\omega^{N-3})^{-1} A(1 + \theta\omega^{N-3})$. Note that $\mathbf{N}_{K/F}(b) = 1$, whence $b \in G$. An easy computation shows that $b \equiv 1 + \theta\omega^{N-2} \bmod \omega^{N-1}\mathbf{f}[[\omega]]$ and $b^2 \equiv 1 + \theta^2\pi^{2N-4} \bmod \pi^{2N-2}O_D$, so

$$\mathrm{LT}_\omega(b^2) = \theta^2 x^{2N-4} + v, \quad \text{where } v \in V = \gamma_N G/\gamma_{N+1}G.$$

Let $h = 1 + \omega$. Note that h and b both lie in K and therefore commute, so $\mathfrak{z}(h, \mathrm{LT}_\omega(b^2)) = 0$ by Lemma 3.6. Since $v \in \gamma_N\hat{G}/\gamma_{N+1}\hat{G}$, $\mathfrak{z}(h, v) = 0$ by Lemma 3.7c). Therefore, $\mathfrak{z}(h, \theta^2 x^{2N-4}) = 0$.

Now let $\alpha = \theta^2$ and fix $\xi \in \mathbf{w}$ such that $\mathbf{tr}(\xi) = 1$. Then $\alpha = \mathbf{tr}(\beta\sigma(\gamma))$ where $\beta = 1$ and $\gamma = \theta^2\xi$, and (8.12) yields

$$\mathfrak{z}(h, \theta^2 x^{2N-4}) = \mathbf{tr}_0((\mu_{1,2} + \mu_{1,1})\theta^2\xi). \tag{8.14}$$

Since $(2N-2) \equiv_4 2$, Lemma 8.4a) implies that $\mu_{1,1}, \mu_{1,2} \in \mathbf{f}$. By Proposition 8.6b), the latter implies that $\mu_{1,2} = 0$.

It follows from (8.14) that

$$0 = \mathbf{tr}_0(\mu_{1,1}\theta^2\xi) = \mathbf{tr}_{\mathbf{f}/\mathbf{f}_0}(\mu_{1,1}\theta^2\mathbf{tr}(\xi)) = \mathbf{tr}_{\mathbf{f}/\mathbf{f}_0}(\mu_{1,1}\theta^2).$$

Since the above equality holds for all $\theta \in \mathbf{f}$, we conclude that $\mu_{1,1} = 0$.

So, we showed that $\mu_{1,1} = \mu_{1,2} = 0$. Therefore, $\mathfrak{z}(g, \alpha x^{2N-4}) = 0$ for all $\alpha \in \mathbf{f}$ and $g \in G$ by (8.12), and $\mathfrak{z}(g, \alpha x^{2N-3}) = 0$ for all $\alpha \in \mathbf{w}$ and $g \in G$ by (8.11). ∎

9. Some properties of finite fields

Here we collect several properties of extensions of finite fields, which are used for computation of Lie algebra cohomology. We retain all notations from previous sections. Recall that $\mathbf{f} \cong \mathbb{F}_q$ and $\mathbf{w} \cong \mathbb{F}_{q^d}$.

LEMMA 9.1 (see [Ri, Lemma 4]): *If $p \neq 2$ or $d \neq 2$, then there exists $\eta \in \mathbf{w}$, with $\mathbf{tr}(\eta) = 0$, such that η generates $\mathbf{w}$ over $\mathbf{f}$ (as a field).*

LEMMA 9.2: *Assume that the pair (p, d) is different from $(2, 2)$, $(2, 4)$ and $(3, 3)$. Let $k = 2$, if $p > 2$, and let $k = -1$ if $p = 2$. Then there exist elements $\eta, \eta_1, \eta_2 \in \mathbf{w}$ such that $\mathbf{tr}(\eta_1) = \mathbf{tr}(\eta_2) = 0$, $\eta - \eta_1 \in \mathbf{f}$, $\eta^k - \eta_2 \in \mathbf{f}$ and η generates $\mathbf{w}$ over $\mathbf{f}$.*

Proof:

CASE 1: $p \nmid d$. In this case for any $\mu \in \mathbf{w}$ there exists $\lambda \in \mathbf{f}$ such that $\mathbf{tr}(\lambda + \mu) = 0$ since $\mathbf{tr}(\lambda + \mu) = d\lambda + \mathbf{tr}(\mu)$ when $\lambda \in \mathbf{f}$, and the assertion of the Lemma follows trivially.

CASE 2: $p \mid d$ *and* $p > 2$. Note that in this case $d \geq 5$, since we assume $(p, d) \neq (3, 3)$. By a result of Cohen and Mills [CM], for any $a, b \in \mathbb{F}_q$, there exists a primitive polynomial $f(x) \in \mathbb{F}_q[x]$ of degree d such that $f(x) = x^d + ax^{d-1} + bx^{d-2} + \cdots$ (f is said to be primitive if it is irreducible and any of its roots generates the multiplicative group of $\mathbb{F}_{q^d}$). If we set $a = b = 0$ and let η be any root of $f(x)$, then clearly $\mathbf{tr}(\eta) = \mathbf{tr}(\eta^2) = 0$ and η generates $\mathbf{w}$ over $\mathbf{f}$.

CASE 3: $p \mid d$ *and* $p = 2$. In this case we use a result of Chou and Cohen [CC], which says that if $d \geq 5$ and the pair (q, d) is different from $(4, 5)$, $(2, 6)$ and $(3, 6)$, there exists a primitive polynomial $f(x) \in \mathbb{F}_q[x]$ of degree d whose coefficients of x and x^{d-1} are both zero. If η is a root of $f(x)$, then obviously $\mathbf{tr}(\eta) = \mathbf{tr}(\eta^{-1}) = 0$.

Since q is a power of 2 and d is even, the only remaining pair is $q = 2$, $d = 6$. In this case we let η be any root of the polynomial $x^6 + x^3 + 1$, which is easily seen to be irreducible over $\mathbb{F}_2$. ∎

LEMMA 9.3: *Let* $S = \{\sigma(\eta) - \eta \mid \mathbf{tr}(\eta) = 0\}$ *and let* Λ *be the subring(=subfield) of* $\mathbf{w}$ *generated by* S. *Then* $\Lambda = \mathbf{w}$ *with the exception of the cases* $p = d = 3$, $p = d = 2$ *and* $p = 2$, $d = 4$.

Proof: Given $\lambda \in \mathbf{w}$, let $\lambda S = \{\lambda s \mid s \in S\}$. Note that if $\lambda \neq 0$, then λS is an $\mathbf{f}$-subspace of $\mathbf{w}$ which has codimension 1 if $p \nmid d$ and codimension 2 if $p \mid d$. Since $\mathbf{w}$ is a d-dimensional space over $\mathbf{f}$, we conclude that $\lambda S \cap S \neq 0$ as long as $d > 2$ and $p \nmid d$, or $d > 4$. This implies that every element of $\mathbf{w}$ is a ratio of two elements of S unless $d = 2$ or $p = d = 3$ or $p = 2$, $d = 4$.

It remains to prove the Lemma in the case $d = 2$, $p > 2$, which is very easy. Indeed, Λ is a subfield of $\mathbf{w}$ containing $\mathbf{f}$, and since $[\mathbf{w} : \mathbf{f}] = 2$, $\Lambda = \mathbf{w}$ or $\Lambda = \mathbf{f}$. The latter is clearly impossible since $\mathrm{card}(\Lambda) \geq \mathrm{card}(S) = \mathrm{card}(\mathbf{f})$ and $\mathbf{f}$ does not contain non-zero elements of zero trace. ∎

LEMMA 9.4: *Let* i *and* j *be integers. Let* $\Lambda_{i,j}$ *be the linear span of the set* $S_{i,j} = \{\alpha\sigma^i(\beta) - \sigma^j(\alpha)\beta \mid \alpha, \beta \in \mathbf{w}\}$. *Assume that* j *is prime to* d. *Then*

$$\Lambda_{i,j} = \begin{cases} \mathbf{w} & \text{if } d \nmid (i+j) \\ \{\eta \in \mathbf{w} \mid \mathbf{tr}(\eta) = 0\} & \text{if } d \mid (i+j). \end{cases}$$

Proof: It is clear that $\Lambda_{i,j}$ is a σ-invariant $\mathbf{f}$-subspace of $\mathbf{w}$. Setting $\beta = 1$, we see that $S_{i,j}$ contains all elements of the form $\alpha - \sigma^j(\alpha)$. Since j is prime to d, there exists k such that $jk \equiv_d 1$. Then $\alpha - \sigma(\alpha) = \sum_{i=0}^{k-1} \sigma^{ji}(\alpha - \sigma^j(\alpha)) \in \Lambda_{i,j}$, whence $\Lambda_{i,j}$ contains all elements of zero trace.

If $d \mid (i+j)$, it is clear that every element of $S_{i,j}$ has zero trace. On the other hand, if $d \nmid (i+j)$, at least one element of $S_{i,j}$ has non-zero trace. Since elements of zero trace form an $\mathbf{f}$-subspace of codimension 1, it follows that $\Lambda_{i,j} = \mathbf{w}$. ∎

References

[CC] W.-S. Chou and S. Cohen, *Primitive elements with zero traces,* Finite Fields and Applications **7** (2001), 125–141.

[CM] S. Cohen and D. Mills, *Primitive polynimials with first and second coefficients prescribed,* Finite Fields and Applications **9** (2003), 334–350.

[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, *The Nottingham group is finitely presented,* Journal of the London Mathematical Society **71** (2005), 362–378.

[LM] C. R. Leedham-Green and S. McKay, *The Structure of Groups of Prime Power Order,* London Mathematical Society Monographs. New Series, 27, Oxford Science Publications, Oxford University Press, Oxford, 2002.

[Lu1] A. Lubotzky, *Profinite presentations,* Journal of Algebra **242** (2001), 672–690.

[Lu2] A. Lubotzky, *Finite presentations of adelic groups, the congruence kernel and cohomology of finite simple groups,* Pure and Applied Mathematics Quarterly **1** (2005), 241–256.

[PR] G. Prasad, M. S. Raghunathan, *Topological central extensions of $SL_1(D)$,* Inventiones Mathematicae **92** (1988), 645–689.

[Ri] C. Riehm, *The norm 1 group of $\mathfrak{p}$-adic division algebra,* American Journal of Mathematics **92** (1970), 499–523.

[Wil] J. Wilson, *Profinite groups,* London Mathematical Society Monographs, New Series, 19, The Clarendon Press, Oxford University Press, New York, 1998.