ACTA ARITHMETICA
180.4 (2017)

# Estimating class numbers over metabelian extensions

by

Antonio Lei (Québec)

## 1. Introduction

**1.1. Setup and notation.** Throughout this article we fix an odd prime $p$ and an integer $d \geq 2$. Let $K$ be a number field that admits a unique prime $\mathfrak{p}$ lying above $p$. Let $K_{\infty,\infty}$ be a $d$-dimensional $p$-adic Lie extension of $K$ in which only finitely many primes of $K$ ramify and $\mathfrak{p}$ is totally ramified. Furthermore, we fix a $\mathbb{Z}_p$-extension $K^{\mathrm{c}}/K$ contained inside $K_{\infty,\infty}$ and assume that

- $\mathrm{Gal}(K_{\infty,\infty}/K^{\mathrm{c}})$ is torsion-free and abelian;
- Every prime of $K$ that ramifies in $K_{\infty,\infty}$ decomposes into finitely many primes in $K^c$.

For example, when $d = 2$, we may take $K = \mathbb{Q}(\mu_p)$, $K^{\mathrm{c}} = \mathbb{Q}(\mu_{p^\infty})$ and $K_{\infty,\infty}$ the Kummer extension $\mathbb{Q}(\mu_{p^\infty}, \sqrt[p^\infty]{\alpha})$, where $\alpha \neq 0$ is an integer such that $p \,|\, \alpha$ or $p \,\|\, \alpha^{p-1} - 1$ (such an $\alpha$ is said to be *amenable* for $p$, and this ensures that $p$ is totally ramified in $K_{\infty,\infty}$; see for example [Lee13, Proposition 2.4(i)] or [Viv04, Theorem 5.2 and Lemma 6.1]). For a general $d$, we may take $K_{\infty,\infty}$ to be the multi-Kummer extension

$$\mathbb{Q}(\mu_{p^\infty}, \sqrt[p^\infty]{\alpha_1}, \ldots, \sqrt[p^\infty]{\alpha_{d-1}}),$$

where $\alpha_i \neq 0$ are integers whose images in $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^p$ are linearly independent over $\mathbb{F}_p$ and the products $\alpha_1^{n_1} \cdots \alpha_{d-1}^{n_{d-1}}$, $0 \leq n_i \leq p-1$, are all amenable (this implies that $p$ totally ramifies in all cyclic subextensions of $K_{\infty,\infty}/K^c$).

We consider the Galois groups $G = \mathrm{Gal}(K_{\infty,\infty}/K)$, $H = \mathrm{Gal}(K_{\infty,\infty}/K^{\mathrm{c}})$ and $\Gamma = \mathrm{Gal}(K^{\mathrm{c}}/K)$. In particular, we have the isomorphisms $G \cong H \rtimes \Gamma$, $H \cong \mathbb{Z}_p^{\oplus(d-1)}$ and $\Gamma \cong \mathbb{Z}_p$.

2010 *Mathematics Subject Classification*: Primary 11R29; Secondary 11R23, 11R20.
*Key words and phrases*: non-commutative Iwasawa theory, class numbers, metabelian extensions.
Received 16 February 2017; revised 30 March 2017.
Published online 28 September 2017.

DOI: 10.4064/aa170216-27-4  

For $0 \leq m, n \leq \infty$, we denote $H_m = H^{p^m}$, $\Gamma_n = \Gamma^{p^n}$, $G_{n,m} = H_m \rtimes \Gamma_n \leq G$ and $K_{n,m} = K_{\infty,\infty}^{G_{n,m}}$. We define $\mathcal{X}_{n,m}$ to be the Hilbert $p$-class group of $K_{n,m}$ and write $e_{n,m}$ for the $p$-exponent of $\#\mathcal{X}_{n,m}$.

For any $p$-adic Lie group $L$, we shall write $\Lambda(L)$ for the Iwasawa algebra

$$\mathbb{Z}_p[[L]] = \varprojlim_{N \trianglelefteq_o L} \mathbb{Z}_p[L/N].$$

If $\mathcal{G}$ is a pro-$p$ group and $x_1, \ldots, x_r \in \mathcal{G}$, we shall write $\langle x_1, \ldots, x_r \rangle$ for the $p$-adic completion of the subgroup generated by $x_1, \ldots, x_r$. Similarly, if $X_1, \ldots, X_r \subset \mathcal{G}$, then $\langle X_1, \ldots, X_r \rangle$ denotes the closed subgroup generated by $X_1, \ldots, X_r$.

**1.2. Main results.** Let $\mathcal{X}$ (respectively $\mathcal{X}'$) be the Galois group of the maximal abelian pro-$p$ extension of $K_{\infty,\infty}$ that is unramified everywhere (respectively unramified outside $p$). When $K_{\infty,\infty}/K$ is a $\mathbb{Z}_p$-extension, a classical result of Iwasawa [Iwa73a] says that $\mathcal{X}$ is torsion over $\Lambda(\Gamma)$. Our first result is a generalization of this result.

THEOREM (Theorem 2.11). *The $\Lambda(G)$-module $\mathcal{X}$ is torsion.*

On studying the structure of $\mathcal{X}$ as a $\Lambda(H)$-module, we shall prove an asymptotic formula for $e_{n,m}$ with $n$ fixed and $m \to \infty$.

THEOREM (Corollary 3.4). *For a fixed integer $n$, there exist integers $\mu_n$ and $\lambda_n$ such that*

$$e_{n,m} = \mu_n p^{(d-1)m} + \lambda_n m p^{(d-2)m} + O(p^{(d-2)m})$$

*for $m \gg 0$.*

In other words, this gives us the asymptotic growth of the class numbers in the $H$-direction. In the example above, this tells us how the size of the $p$-primary part of the ideal class group of the extension

$$\mathbb{Q}(\mu_{p^n}, \sqrt[p^m]{\alpha_1}, \cdots, \sqrt[p^m]{\alpha_{d-1}})$$

varies as $m \to \infty$. In particular, these extensions are not Galois in general. This is analogous to the main result of [CM81] for Galois extensions of number fields whose Galois groups are isomorphic to direct sums of $\mathbb{Z}_p$. In fact, our proof relies heavily on the analysis of torsion $\Lambda(H)$-modules in Cuoco and Monsky's work.

Let $\mathfrak{M}_H(G)$ be the category of finitely generated $\Lambda(G)$-modules $M$ such that $M/M(p)$ is finitely generated over $\Lambda(H)$, where $M(p)$ denotes the submodule of $\mathbb{Z}_p$-torsions inside $M$. In non-commutative Iwasawa theory studied by Coates, Fukaya, Kakde, Kato, Ochi, Ritter, Sujatha, Venjakob, Weiss and many others [CFK$^+$05, Kak13, OV02, RW11, Ven02, Ven03b], $\mathcal{X}'$ is conjectured to be inside $\mathfrak{M}_H(G)$ for totally real fields. Since $\mathcal{X}$ is a quotient of $\mathcal{X}'$, this would imply that $\mathcal{X} \in \mathfrak{M}_H(G)$ as well. When $K^c/K$ is the cyclotomic

$\mathbb{Z}_p$-extension, Iwasawa [Iwa73a, Iwa73b] conjectured that the $\mu$-invariant associated to this extension vanishes (this is a theorem of Ferrero–Washington [FW79] when $k/\mathbb{Q}$ is an abelian extension). This conjecture turns out to be equivalent to $\mathcal{X}$ itself (not just $\mathcal{X}/\mathcal{X}(p)$) being finitely generated over $\Lambda(H)$ (see Theorem 2.13 below as well as [MF16, Lemma 3.3] and [CS05, Lemma 3.2] for the same result in different settings).

Our second result is an asymptotic formula for $e_{n,n}$ as $n \to \infty$ when $d = 2$ and $\mathcal{X}$ is finitely generated over $\Lambda(H)$.

THEOREM (Corollary 5.3). *Suppose that $d = 2$ and $\mathcal{X}$ is finitely generated over $\Lambda(H)$. If the unique prime of $K$ above $p$ is totally ramified in $K_{\infty,\infty}$, then*

$$e_{n,n} = \tau n p^n + O(p^n),$$

*where $\tau = \operatorname{rank}_{\Lambda(H)} \mathcal{X}$.*

We remark that our theorem *always* applies when $K_{\infty,\infty} = \mathbb{Q}(\mu_{p^\infty}, \sqrt[p^\infty]{\alpha})$ for some integer $\alpha$ that is amenable for $p$ since the theorem of Ferrero–Washington tells us that our hypothesis on $\mathcal{X}$ holds. In particular, it confirms the prediction made by Venjakob [Ven03a, §8] for the extension $\mathbb{Q}(\mu_{p^\infty}, \sqrt[p^\infty]{p})$. Our result can also be seen as a generalization of the classical result of Iwasawa [Iwa73a] on $\mathbb{Z}_p$-extensions in the special case that the $\mu$-invariant vanishes. If $G$ is abelian, that is, $G \cong \mathbb{Z}_p^2$, we recover the main result of [CM81] again in the case when the $\mu$-invariant is 0 (denoted by $m_0$ in *loc. cit.*).

Perbet [Per11] studied the variation of class numbers when $G$ is a general $d$-dimensional $p$-adic Lie group with no $p$-torsion, without our assumption on $\mathcal{X}$ being finitely generated over $\Lambda(H)$ or any assumption on the ramification of $p$. More precisely, if $\tilde{e}_{n,n}$ denotes the $p$-exponent of $\#\mathcal{X}_{n,n}/p^n$ (rather than $\mathcal{X}_{n,n}$ itself), Perbet showed that

$$\tilde{e}_{n,n} = \rho n p^{dn} + \mu p^{dn} + O(n p^{(d-1)n}), \tag{1.1}$$

where $\rho = \operatorname{rank}_{\Lambda(G)} \mathcal{X}$ and $\mu$ is the $\mu$-invariant of $\mathcal{X}$ as defined in [Ven02]. Under our assumption that $\mathcal{X}$ is finitely generated over $\Lambda(H)$, both $\rho$ and $\mu$ vanish. In this case, the formula of Perbet becomes simply $O(n p^{(d-1)n})$. Our formula in Corollary 5.3 is therefore slightly more precise. We shall show at the end of this article that our method yields an upper bound of $\tilde{e}_{n,n}$ in the case $d = 2$ and $\mathcal{X} \in \mathfrak{M}_H(G)$ (the constant $\rho$ would be 0, but $\mu$ may be non-zero).

THEOREM (Corollary 6.2). *If $d = 2$ and $\mathcal{X} \in \mathfrak{M}_H(G)$, then*

$$\tilde{e}_{n,n} \leq \mu p^{2n} + \tau n p^n + O(p^n),$$

*where $\tau = \operatorname{rank}_{\Lambda(H)} \mathcal{X}/\mathcal{X}(p)$.*

## 2. Preliminary results

**2.1. Ramification groups and class groups.** Let $\Sigma$ be the set of primes of $K$ that ramify in $K_{\infty,\infty}$. In particular, $\mathfrak{p} \in \Sigma$. Since $\mathfrak{p}$ is assumed to be totally ramified in $K_{\infty,\infty}$, its (unique) decomposition group inside $G$ is $G$ itself.

If $\nu \in \Sigma$, we have assumed that there are only finitely many primes in $K^{\mathrm{c}}$ lying above $\nu$. On replacing $K$ by $K_{n,0}$ if necessary, we may assume that $\nu$ is inert in $K^{\mathrm{c}}$. In particular, if $\nu_1$ and $\nu_2$ are two primes of $K_{\infty,\infty}$ lying above $\nu$, then they differ by an element in $H$.

Let $\mathcal{M}$ be the maximal unramified abelian pro-$p$ extension of $K_{\infty,\infty}$ and write $\mathcal{X} = \mathrm{Gal}(\mathcal{M}/K_{\infty,\infty})$ and $\mathcal{Y} = \mathrm{Gal}(\mathcal{M}/K)$. Note that $\mathcal{X}$ is normal in $\mathcal{Y}$ with $\mathcal{Y}/\mathcal{X} \cong G$. For each $g \in G$, let $\tilde{g} \in \mathcal{Y}$ be a lifting of $g$. If $x \in \mathcal{X}$, we have the action $x^g = \tilde{g}^{-1}x\tilde{g}$. This turns $\mathcal{X}$ into a $\Lambda(G)$-module. We recall from [Per11, Proposition 3.1] that $\mathcal{X}$ is a finitely generated $\Lambda(G)$-module.

For each $\nu \in \Sigma$, we fix a prime $\bar{\nu}$ of $\mathcal{M}$ above $\nu$ and write $I_\nu$ for the inertia group of $\bar{\nu}$ inside $\mathcal{Y}$. We note that $I_{\mathfrak{p}}$ is isomorphic to $G$ since we assume that $\mathfrak{p}$ is totally ramified in $K_{\infty,\infty}$ and it is unramified in $\mathcal{M}$. In particular,

$$\mathcal{Y} \cong \mathcal{X} \rtimes G, \tag{2.1}$$

where we identify $G$ with $I_{\mathfrak{p}}$. Each element of $\mathcal{Y}$ may be written as $(x, g)$ for some $x \in \mathcal{X}$ and $g \in G$. Note in particular that under this identification,

$$I_{\mathfrak{p}} = \{(1, g) : g \in G\}. \tag{2.2}$$

For $0 \le m, n \le \infty$, we define $\mathcal{Y}_{n,m} = \mathrm{Gal}(\mathcal{M}/K_{n,m})$. For each $\nu \in \Sigma$, we write $I_{\nu_{n,m}}$ for the inertia group of our choice of $\bar{\nu}$ inside $\mathcal{Y}_{n,m}$, and $\bar{I}_{\nu_{n,m}}$ for its image under the natural projection $\mathcal{Y}_{n,m} \to G_{n,m}$. We note that $\bar{I}_{\nu_{n,m}} \cong I_{\nu_{n,m}}$ since the extension $\mathcal{M}/K_{\infty,\infty}$ is unramified.

Since $\mathcal{X}$ is normal in $\mathcal{Y}$, it is also normal in $\mathcal{Y}_{n,m}$. Consequently, $[\mathcal{X}, \mathcal{Y}_{n,m}]$ is normal in $\mathcal{Y}_{n,m}$ and we may consider the quotient $\mathcal{Y}_{n,m}/[\mathcal{X}, \mathcal{Y}_{n,m}]$.

LEMMA 2.1. *The image of $I_{\mathfrak{p}_{n,m}}$ in $\mathcal{Y}_{n,m}/[\mathcal{X}, \mathcal{Y}_{n,m}]$ is normal. That is,*

$$\langle [\mathcal{X}, \mathcal{Y}_{n,m}], I_{\mathfrak{p}_{n,m}} \rangle / [\mathcal{X}, \mathcal{Y}_{n,m}] \trianglelefteq \mathcal{Y}_{n,m}/[\mathcal{X}, \mathcal{Y}_{n,m}].$$

*Proof.* Let $(1, g) \in I_{\mathfrak{p}_{n,m}}$ (which makes sense thanks to (2.2)) and $(x, h) \in \mathcal{Y}_{n,m}$. Then

$$(x, h)^{-1}(1, g)(x, h) = (x^{(g-1)h^{-1}}, h^{-1}gh).$$

Note that $x^{g-1} = x^{-1}\tilde{g}^{-1}x\tilde{g} \in [\mathcal{X}, \mathcal{Y}_{n,m}]$, hence the result. ∎

Let $C_{n,m}$ be the subgroup of $\mathcal{Y}_{n,m}$ generated by $[\mathcal{Y}_{n,m}, \mathcal{Y}_{n,m}]$ and by all the inertia groups $I^{\sigma}_{\nu_{n,m}}$ for $\nu \in \Sigma$ and $\sigma \in \mathcal{X} \rtimes H$. This contains all the inertia groups inside $\mathcal{Y}_{n,m}$ since any two primes of $\mathcal{M}$ lying above $\nu$ differ by an element in $\mathcal{X} \rtimes H$. Finally, we define $B_{n,m} = C_{n,m} \cap \mathcal{X}$. Recall from the

introduction that $\mathcal{X}_{n,m}$ is defined to be the Hilbert $p$-class group of $K_{n,m}$. It may be described as follows.

LEMMA 2.2. *We have the isomorphism* $\mathcal{X}_{n,m} \cong \mathcal{X}/B_{n,m}$.

*Proof.* Class field theory tells us that

$$\mathcal{X}_{n,m} \cong \mathcal{Y}_{n,m}/C_{n,m}.$$

By the isomorphism theorem, we have $\mathcal{X}/B_{n,m} \cong \mathcal{X}C_{n,m}/C_{n,m}$. This gives the short exact sequence

$$1 \to \mathcal{X}/B_{n,m} \to \mathcal{X}_{n,m} \to \mathcal{Y}_{n,m}/\mathcal{X}C_{n,m} \to 1.$$

Recall that $\mathcal{Y}_{n,m}/\mathcal{X} \cong G_{n,m}$, the last term of the short exact sequence can be described by

$$\mathcal{Y}_{n,m}/\mathcal{X}C_{n,m} \cong G_{n,m}/\langle [G_{n,m}, G_{n,m}], \bar{I}^{\sigma}_{\nu_{n,m}} : \nu \in \Sigma, \sigma \in H\rangle.$$

But $\mathfrak{p} \in \Sigma$ and $\bar{I}_{\mathfrak{p}_{n,m}} = G_{n,m}$ since $\mathfrak{p}$ is totally ramified in $K_{\infty,\infty}$. Hence, this quotient is trivial and the result follows. ∎

In particular, this gives us the following short exact sequence:

$$0 \to B_{n,m}/I_{G_{n,m}}\mathcal{X} \to \mathcal{X}/I_{G_{n,m}}\mathcal{X} \to \mathcal{X}_{n,m} \to 0. \tag{2.3}$$

**2.2. Description of $B_{n,m}$.** We write $I_{G_{n,m}}$ for the augmentation ideal of $G_{n,m}$ in $\Lambda(G)$, that is, the ideal generated by $g-1$ for $g \in G_{n,m}$. We have the following description.

LEMMA 2.3. *We have the equality*

$$[\mathcal{X}, \mathcal{Y}_{n,m}] = I_{G_{n,m}}\mathcal{X}.$$

*Proof.* Let $x \in \mathcal{X}$ and $y \in \mathcal{Y}_{n,m}$. We write $\bar{y}$ for the image of $y$ in $G_{n,m}$. Then

$$[x, y] = x^{-1}y^{-1}xy = x^{\bar{y}-1}.$$

Hence the result. ∎

COROLLARY 2.4. *The augmentation ideal $I_{G_{n,m}}\mathcal{X}$ is a normal subgroup of $\mathcal{Y}_{n,m}$.*

*Proof.* As we have seen in Lemma 2.1, $[\mathcal{X}, \mathcal{Y}_{n,m}]$ is normal in $\mathcal{Y}_{n,m}$. Hence, the result follows from Lemma 2.3. ∎

The augmentation ideal allows us to describe the commutator subgroup of $\mathcal{Y}_{n,m}$ as follows.

PROPOSITION 2.5. *We have the equality*

$$[\mathcal{Y}_{n,m}, \mathcal{Y}_{n,m}] = \big\langle I_{G_{n,m}}\mathcal{X}, [I_{\mathfrak{p}_{n,m}}, I_{\mathfrak{p}_{n,m}}]\big\rangle.$$

*Proof.* Recall that $\mathcal{X}$ is normal in $\mathcal{Y}_{n,m}$, $\mathcal{Y}_{n,m}/\mathcal{X} \cong G_{n,m}$ and $I_{\mathfrak{p}_{n,m}}\mathcal{X}/\mathcal{X} \cong G_{n,m}$. Hence, every element of $\mathcal{Y}_{n,m}$ can be written as $x \cdot b$ for some $x \in \mathcal{X}$

and $b \in I_{\mathfrak{p}_{n,m}}$. Let $x_1b_1, x_2b_2$ be any two elements of $\mathcal{Y}_{n,m}$ written in this way. We have the commutator identity

$$[x_1b_1, x_2b_2] = [x_1, x_2b_2]^{b_1}[b_1, x_2b_2] = [x_1, x_2b_2]^{b_1}[b_1, b_2][b_1, x_2]^{b_2}.$$

On the one hand, $[b_1, b_2] \in [I_{\mathfrak{p}_{n,m}}, I_{\mathfrak{p}_{n,m}}]$ by definition. On the other hand, both $[x_1, x_2b_2]$ and $[b_1, x_2]$ are inside $[\mathcal{X}, \mathcal{Y}_{n,m}]$, which is equal to $I_{G_{n,m}}\mathcal{X}$ by Lemma 2.3. Hence the result. ∎

Corollary 2.6. *We have*

$$C_{n,m} = \langle I_{G_{n,m}}\mathcal{X}, I^{\sigma}_{\nu_{n,m}} : \nu \in \Sigma,\, \sigma \in \mathcal{X} \rtimes H\rangle,$$
$$B_{n,m} = I_{G_{n,m}}\mathcal{X} + \langle I^{\sigma}_{\nu_{n,m}} : \nu \in \Sigma,\, \sigma \in \mathcal{X} \rtimes H\rangle \cap \mathcal{X}.$$

*Proof.* By definition $[\mathcal{Y}_{n,m}, \mathcal{Y}_{n,m}] \subset C_{n,m}$ and $I_{G_{n,m}}\mathcal{X} \subset \mathcal{X}$, so we see from Proposition 2.5 that

$$I_{G_{n,m}}\mathcal{X} \subset B_{n,m}.$$

Furthermore, Corollary 2.4 says that $I_{G_{n,m}}\mathcal{X}$ is normal in $\mathcal{Y}_{n,m}$. Therefore, the second equality follows from the first.

Recall that $C_{n,m}$ is defined to be

$$\langle [\mathcal{Y}_{n,m}, \mathcal{Y}_{n,m}], I^{\sigma}_{\nu_{n,m}} : \nu \in \Sigma,\, \sigma \in \mathcal{X} \rtimes H\rangle.$$

Therefore, the first equality follows from the description of $[\mathcal{Y}_{n,m}, \mathcal{Y}_{n,m}]$ in Proposition 2.5 and the fact that $[I_{\mathfrak{p}_{n,m}}, I_{\mathfrak{p}_{n,m}}]$ is contained in $I_{\mathfrak{p}_{n,m}}$. ∎

Proposition 2.7. *The quotient $B_{n,m}/I_{G_{n,m}}\mathcal{X}$ is a $\Lambda(H)$-module generated by the elements $x \in \mathcal{X}$ with the property that $(x, h) \in I_{\nu_{n,m}}$ for some $\nu \in \Sigma \setminus \{\mathfrak{p}\}$ and $h \in H_m$.*

*Proof.* Suppose that $(x, h) \in I_{\nu_{n,m}}$ for some $h \in H_m$ and $\nu \in \Sigma \setminus \{\mathfrak{p}\}$. Then $(1, h) \in I_{\mathfrak{p}_{n,m}}$ thanks to (2.2). Consequently, $(x, 1) = (x, h)(1, h)^{-1} \in C_{n,m} \cap \mathcal{X} = B_{n,m}$.

Recall from Lemma 2.1 that the image of $I_{\mathfrak{p}_{n,m}}$ in $\mathcal{Y}_{n,m}/[\mathcal{X}, \mathcal{Y}_{n,m}]$ is a normal subgroup. By Lemma 2.3, we have $[\mathcal{X}_{n,m}, \mathcal{Y}_{n,m}] = I_{G_{n,m}}\mathcal{X}$. Hence,

$$\langle I_{G_{n,m}}\mathcal{X}, I_{\mathfrak{p}_{n,m}}\rangle/I_{G_{n,m}}\mathcal{X} \trianglelefteq C_{n,m}/I_{G_{n,m}}\mathcal{X}.$$

From Corollary 2.6, we deduce that every element in $C_{n,m}/I_{G_{n,m}}\mathcal{X}$ may be written as a product $\alpha\beta$ for some $\alpha \in \langle I^{\sigma}_{\nu_{n,m}} : \nu \in \Sigma \setminus \{\mathfrak{p}\}, \sigma \in \mathcal{X} \rtimes H\rangle$ and $\beta \in I_{\mathfrak{p}_{n,m}}$.

Suppose that an element $\alpha\beta$ as above is contained in $B_{n,m}/I_{G_{n,m}}\mathcal{X}$. Then $\alpha$ is a product of elements of the form $(x_\nu, h_\nu)^\sigma \in I_{\nu_{n,m}}$, where $\sigma = (x_\sigma, h_\sigma) \in \mathcal{X} \rtimes H$. We have in fact

$$(x_\nu, h_\nu)^\sigma = (x_\sigma^{(h_\nu - 1)h_\sigma^{-1}} x_\nu^{h_\sigma^{-1}}, h_\nu)$$

given that $H$ is abelian. But $x_\sigma^{(h_\nu - 1)h_\sigma^{-1}} \in [\mathcal{X}, \mathcal{X} \rtimes H_m] \subset I_{G_{n,m}}\mathcal{X}$ by Lemma 2.3 and the fact that $h_\nu \in H_m$. Furthermore, we have the iden-

tity $(x_\nu, h_\nu)(x_{\nu'}, h_{\nu'}) = (x_\nu x_{\nu'}^{h_\nu}, h_\nu h_{\nu'})$, which implies that $\alpha = (x, h)$ for some $x \in \mathcal{X}$ is inside the $\Lambda(H)$-module generated by the elements $x_\nu$ as described in the statement of the proposition and $h \in H_m$ with $\beta = (1, h^{-1})$. Hence the result. ∎

**2.3. The $\mathbb{Z}_p$-rank of $B_{n,m}/I_{G_{n,m}}\mathcal{X}$.** In the previous section, we showed in Proposition 2.7 that we may find explicit generators for the quotient $B_{n,m}/I_{G_{n,m}}\mathcal{X}$. We shall now bound its $\mathbb{Z}_p$-rank.

The aforementioned quotient is generated by the "projection" of $I^h_{\nu_{n,m}}$ in $\mathcal{X}$, where $\nu \in \Sigma \setminus \{\mathfrak{p}\}$ and $h \in H$. But the map $\mathcal{Y} \to \mathcal{X}$, $(x, g) \mapsto x$, is not a group homomorphism a priori. However, if $(x, g), (y, h) \in \mathcal{Y}_{n,m}$, we have

$$(x, g) \cdot (y, h) = (xy^g, gh),$$

and

$$xy^g \equiv xy \bmod [\mathcal{X}, \mathcal{Y}_{n,m}] = I_{G_{n,m}}\mathcal{X}$$

by Lemma 2.3. Therefore, the map

$$\mathcal{Y}_{n,m}/I_{G_{n,m}}\mathcal{X} \to \mathcal{X}/I_{G_{n,m}}\mathcal{X}, \quad (x, g) \mapsto x,$$

is a well-defined group homomorphism.

LEMMA 2.8. *The quotient $B_{n,m}/I_{G_{n,m}}\mathcal{X}$ is a finitely generated $\mathbb{Z}_p$-module. Furthermore, its rank is bounded by $r_{n,m}$, where $r_{n,m}$ is the number of places of $K_{n,m}$ above $\Sigma \setminus \{\mathfrak{p}\}$.*

*Proof.* As discussed above, the quotient is generated by the projections of $I^h_{\nu_{n,m}}$ in $\mathcal{X}$, where $\nu \in \Sigma \setminus \{\mathfrak{p}\}$ and $h \in H$, which corresponds to all the inertia groups of the places of $\mathcal{M}$ lying above $\Sigma \setminus \{\mathfrak{p}\}$.

If two primes of $\mathcal{M}$ differ by an element in $\mathcal{Y}_{n,m}$, then their inertia groups coincide modulo $I_{G_{n,m}}\mathcal{X}$, as we have seen in the proof of Proposition 2.7. Therefore, if for each prime of $K_{n,m}$ lying above $\Sigma \setminus \{\mathfrak{p}\}$, we pick one prime in $\mathcal{M}$ lying above this prime, the resulting inertia groups generate the quotient $B_{n,m}/I_{G_{n,m}}\mathcal{X}$.

Our result then follows from the fact that each of these inertia groups has $\mathbb{Z}_p$-rank at most 1. Indeed, all primes in $\Sigma \setminus \{\mathfrak{p}\}$ are coprime to $p$ by assumption, so the maximal pro-$p$ extension of $K_\nu$ is isomorphic to $\mathbb{Z}_p \rtimes \mathbb{Z}_p$, which is of dimension 2, as given by [Ser63, II.§5.6 Exercices]. Since $K_\nu$ admits a one-dimensional unramified $\mathbb{Z}_p$-extension, the inertia group has dimension at most 1. ∎

LEMMA 2.9. *Let $r_{n,m}$ be as defined in Lemma* 2.8. *Then*

(i) *for $n$ sufficiently large, $r_{n,m}$ depends only on $m$;*
(ii) *$r_{n,m} = O(p^{(d-2)m})$ for $m \gg 0$.*

*Proof.* Since there are a finite number of primes in $K_{\infty,m}$ lying above each prime of $\Sigma \setminus \{\mathfrak{p}\}$, part (i) follows.

We now prove (ii). Fix a prime $\bar{\nu}$ of $K_{\infty,\infty}$ above $\nu \in \Sigma \setminus \{\mathfrak{p}\}$. As we have seen in the proof of Lemma 2.8, the inertia group of $\bar{\nu}$ is a $p$-adic Lie group of dimension one. Furthermore, $\nu$ is inert over $K^{\mathrm{c}}/K_{n,0}$ for $n$ sufficiently large. Therefore, the decomposition group of $\bar{\nu}$ is of dimension two.

Let $\varpi$ be a prime of $K_{n,m}$ above $\nu$. Let $G_\varpi$ be the decomposition group of $\varpi$ in the extension $K_{n,m}/K$. Our observation on the dimension of the decomposition group of $\bar{\nu}$ tells us that there exists a constant $C > 0$ such that $|G_\varpi| \geq Cp^{n+m}$ for all $\varpi$. But

$$p^{n+(d-1)m} = |G : G_{n,m}| = \sum_{\varpi|\nu} |G_\varpi|.$$

If $r_{n,m,\nu}$ denotes the number of places of $K_{n,m}$ above $\nu$, then

$$r_{n,m,\nu} \leq p^{n+(d-1)m}/(Cp^{n+m}) = p^{(d-2)m}/C,$$

which gives (ii). ∎

By combining these two lemmas, we deduce:

Corollary 2.10. *The quotient $B_{n,m}/I_{G_{n,m}}\mathcal{X}$ is a finitely generated $\mathbb{Z}_p$-module with*

$$\mathrm{rank}_{\mathbb{Z}_p} B_{n,m}/I_{G_{n,m}}\mathcal{X} = O(p^{(d-2)m})$$

*for $m \gg 0$ (and independent of $n$).*

**2.4. Algebraic structure of $\mathcal{X}$.** Our analysis of $B_{n,m}$ allows us to study the structure of $\mathcal{X}$ as a $\Lambda(G)$-module. In particular, we prove the following.

Theorem 2.11. *The $\Lambda(G)$-module $\mathcal{X}$ is torsion.*

*Proof.* As we have recalled above, $\mathcal{X}$ is finitely generated over $\Lambda(G)$ by [Per11, Proposition 3.1]. In particular, if $\rho$ denotes its rank, [Har00, Theorem 1.10] tells us that

$$\mathrm{rank}_{\mathbb{Z}_p} \mathcal{X}/I_{G_{n,n}}\mathcal{X} = \rho p^{dn} + O(p^{(d-1)n}).$$

By (2.3), together with Corollary 2.10 and the finiteness of $\mathcal{X}_{n,n}$, we have in fact

$$\mathrm{rank}_{\mathbb{Z}_p} \mathcal{X}/I_{G_{n,n}}\mathcal{X} = O(p^{(d-2)n}).$$

This implies that $\rho = 0$, and hence the result. ∎

This allows us to eliminate the most dominant term of Perbet's formula (1.1).

Corollary 2.12. *Let $\tilde{e}_{n,n}$ denote the $p$-exponent of $\#\mathcal{X}_{n,n}/p^n$. Then*

$$\tilde{e}_{n,n} = \mu p^{dn} + O(np^{(d-1)n})$$

*for some integer $\mu$.*

Under an additional hypothesis on $\mathcal{X}_{\infty,0}$, we can in fact show more:

THEOREM 2.13. *The $\Lambda(\Gamma)$-module $\mathcal{X}_{\infty,0}$ is finite if and only if $\mathcal{X}$ is finitely generated over $\Lambda(H)$. In particular, when this holds, $\mathcal{X}$ belongs to the $\mathfrak{M}_H(G)$-category.*

*Proof.* The short exact sequence (2.3) becomes

$$0 \to B_{\infty,0}/I_H\mathcal{X} \to \mathcal{X}/I_H\mathcal{X} \to \mathcal{X}_{\infty,0} \to 0$$

if we take $m = 0$ and $n = \infty$. Corollary 2.10 tells us that the first term of the short exact sequence is finite over $\mathbb{Z}_p$. Therefore, the second term is finite over $\mathbb{Z}_p$ if and only the last term is. Suppose that $\mathcal{X}$ is finite over $\Lambda(H)$. Then $\mathcal{X}/I_H\mathcal{X}$ is finite over $\mathbb{Z}_p$, which gives one implication of the theorem. If on the other hand $\mathcal{X}_{\infty,0}$ is finite over $\mathbb{Z}_p$, then so is $\mathcal{X}/I_H\mathcal{X}$. Consequently, Nakayama's Lemma (see [CH01, Lemma 2.6] or [BH97]) implies that $\mathcal{X}$ is finite over $\Lambda(H)$, which gives the other implication. ∎

**3. Growth in the $H$-direction.** In this section, we fix an integer $n \geq 0$ and estimate the growth in $e_{n,m}$ as $m \to \infty$. Our strategy is to make use of our estimation on $B_{n,m}/I_{G_{n,m}}$ from §2.2, in conjunction with the short exact sequence (2.3).

Recall that $\mathcal{X}$ is finitely generated over $\Lambda(G)$. Consequently, $\mathcal{X}_{\Gamma_n}$ is a finitely generated $\Lambda(H)$-module. In fact, we can say more:

LEMMA 3.1. *The $\Lambda(H)$-module $\mathcal{X}_{\Gamma_n}$ is torsion.*

*Proof.* Let $M$ be a finitely generated $\Lambda(H)$-module. If $\operatorname{rank}_{\Lambda(H)} M = r$, then

$$\operatorname{rank}_{\mathbb{Z}_p} M_{H_m} = rp^{(d-1)m} + O(p^{(d-2)m})$$

(see [Har00, Theorem 1.10]).

The $H_m$-coinvariant of $\mathcal{X}_{\Gamma_n}$ is nothing but $\mathcal{X}/I_{G_{n,m}}\mathcal{X}$. Since $\mathcal{X}_{n,m}$ is finite, (2.3) tells us that $\mathcal{X}/I_{G_{n,m}}\mathcal{X}$ has the same $\mathbb{Z}_p$-rank as $B_{n,m}/I_{G_{n,m}}\mathcal{X}$. Hence the result by Corollary 2.10. ∎

We recall the following definition from [CM81, §4]. Let $M$ be a finitely generated torsion $\Lambda(H)$-module. A structure $\mathcal{S}$ on $M$ consists of a fixed integer $m_0$ together with a finite set of pairs $(\tau_i, M_i)$, where $\tau_i \in H \setminus H_1$ and $M_i$ is a submodule of $M$. For every structure of $M$, we define, for $m \geq m_0$,

$$A_m(\mathcal{S}) = I_{H_m}M + \sum_i \Phi_{m/m_0}(\tau_i)M_i,$$

where $\Phi_{m/m_0}(X)$ denotes the polynomial $(X^{p^m} - 1)/(X^{p^{m_0}} - 1)$. Such a structure is said to be *admissible* if $\operatorname{rank}_{\mathbb{Z}_p} M/A_m(\mathcal{S}) = O(p^{(d-3)n})$ (for $d \geq 3$) or $\operatorname{rank}_{\mathbb{Z}_p} M/A_m(\mathcal{S}) = O(1)$ (for $d = 2$).

Let $M$ be a finitely generated $\mathbb{Z}_p$-module. We shall write $M_t$ for the torsion submodule of $M$ and $e(M)$ for the $p$-exponent of the order of $M_t$. The following result is proved in [CM81].

THEOREM 3.2. *Let $M$ be a finitely generated torsion $\Lambda(H)$-module and $\mathcal{S}$ an admissible structure on $M$. Then*

$$e(M/A_m(\mathcal{S})) = \mu_H(M) \times p^{(d-1)m} + \lambda_H(M) \times mp^{(d-2)m} + O(p^{(d-2)m})$$

*for some non-negative integers $\mu(M)$ and $\lambda(M)$ that are independent of $m$ and $\mathcal{S}$.*

*Proof.* This is [CM81, Lemma 4.9 and Theorem 4.13] when $d \geq 3$. For the case $d = 2$, we have $H = \mathbb{Z}_p$ and the result follows from the classical results of [Iwa73a]. ∎

LEMMA 3.3. *There exists an admissible structure $\mathcal{S}$ on $\mathcal{X}_{\Gamma_n}$ such that $\mathcal{X}_{n,m} = \mathcal{X}_{\Gamma_n}/A_m(\mathcal{S})$ for $m \gg 0$.*

*Proof.* Let $\nu \in \Sigma \setminus \{\mathfrak{p}\}$. Then $\bar{I}_{\nu_{n,m}}$ is a subgroup of $H_m$. Therefore, there exists an integer $m_0$ such that $H_m/\bar{I}_{\nu_{n,m}}$ is torsion-free for all $m \geq m_0$. Since $\Sigma$ is finite, we may assume that $m_0$ is an integer satisfying this property for all $\nu$.

Recall from the proof of Lemma 2.8 that each $\bar{I}_{\nu_{n,m}}$ is of dimension 1. Suppose that $I_{\nu_{n,m_0}} = \langle (x_\nu, h_\nu) \rangle$. Then $h_\nu \in H_{m_0} \setminus H_{m_0+1}$. In particular, we may write $h_\nu = k_\nu^{p^{m_0}}$ for some $k_\nu \in H \setminus H_1$. Furthermore, for all $m \geq m_0$, we have

$$I_{\nu_{n,m}} = \langle (x_\nu, h_\nu)^{p^{m-m_0}} \rangle = \langle (x_\nu^{\Phi_{m/m_0}(k_\nu)}, k_\nu^{p^m}) \rangle.$$

Therefore, Proposition 2.7 tells us that

$$B_{n,m} = I_{G_{n,m}} \mathcal{X} + \sum_\nu \Phi_{m/m_0}(k_\nu) \Lambda(H) x_\nu.$$

Hence, if we take $\mathcal{S} = \{m_0, (k_\nu, \Lambda(H) \cdot x_\nu) : \nu \in \Sigma \setminus \{\mathfrak{p}\}\}$, then $B_{n,m} = A_m(\mathcal{S})$ as $\mathcal{X}_{n,m} \cong \mathcal{X}/B_{n,m}$ by Lemma 2.2. Finally, the structure is admissible because $\mathcal{X}_{n,m}$ is finite by definition. ∎

COROLLARY 3.4. *For a fixed $n$, we have the formula*

$$e_{n,m} = \mu_H(\mathcal{X}_{\Gamma_n}) p^{(d-1)m} + \lambda_H(\mathcal{X}_{\Gamma_n}) mp^{(d-2)m} + O(p^{(d-2)m}).$$

*Proof.* This follows from combining Theorem 3.2 with Lemmas 3.1 and 3.3. ∎

**4. Interlude: review on $\Lambda(\Gamma)$-modules.** We identify $\Lambda(\Gamma)$ with the power series ring $\mathbb{Z}_p[[X]]$ by choosing a topological generator $\gamma$ of $\Gamma$ and identifying $\gamma - 1$ with $X$. We write $\omega_n = (1+X)^{p^n} - 1$ for $n \geq 0$ and $\Phi_n = \omega_n/\omega_{n-1}$ denotes the cyclotomic polynomial of order $p^n$ in $1 + X$ for

$n \geq 1$. We fix a primitive $p^n$th root of unity $\zeta_{p^n}$ and write $\epsilon_n = \zeta_{p^n} - 1$. Finally, we write $\Phi_{n/n_0} = \omega_n/\omega_{n_0}$ for $n \geq n_0$ as in §3.

Let $F \in \Lambda(\Gamma)$. The Weierstrass Preparation Theorem tells us that there exists a factorization $F = up^\mu g$, where $u \in \Lambda(\Gamma)^\times$, $\mu \in \mathbb{Z}_{\geq 0}$ and $g$ is a distinguished polynomial. We shall write $\mu_\Gamma(F) = \mu$ and $\lambda_\Gamma(F) = \deg(g)$.

If $M$ is a finitely generated torsion $\Lambda(\Gamma)$-module, it is known that there exist $F_1, \ldots, F_r \in \Lambda(\Gamma)$ and an injective $\Lambda(\Gamma)$-morphism

$$\phi : M/M' \to \bigoplus_{i=1}^{r} \Lambda(\Gamma)/(F_i),$$

where $M'$ denotes the maximal pseudo-null $\Lambda(\Gamma)$-submodule of $M$ and the cokernel of $\phi$ is pseudo-null. Note that a pseudo-null $\Lambda(\Gamma)$-module is simply a module over $\Lambda(\Gamma)$ with finite cardinality.

The $\Lambda(\Gamma)$-ideal generated by the product $\prod_{i=1}^r F_i$ is called the *characteristic ideal* of $M$. We write $\mu_\Gamma(M) = \sum \mu_\Gamma(F_i)$ and $\lambda_\Gamma(M) = \sum \lambda_\Gamma(F_i)$. We remark that the condition that $\mathcal{X}_{\infty,0}$ be finitely generated over $\mathbb{Z}_p$ in Theorem 2.13 is equivalent to $\mu_\Gamma(\mathcal{X}_{\infty,0}) = 0$.

The following result of Iwasawa in [Iwa73a] is well-known.

THEOREM 4.1. *Let $M$ be a finitely generated torsion $\Lambda(\Gamma)$-module. Then there exist constants $\nu_\Gamma(M)$ and $n_0$ such that $M_{\Phi_{n/n_0}}$ is finite with*

$$e(M_{\Phi_{n/n_0}}) = \mu_\Gamma(M)p^n + \lambda_\Gamma(M)n + \nu_\Gamma(M)$$

*for all $n \geq n_0$.*

This result has been reproved in many different places, e.g. in [Kob03, §10.2], [NSW08, §5.3] and [Was97, §13.3]. We shall give a sketch proof in the special case where the characteristic ideal of $M$ is coprime to $\omega_n$ for all $n$. In doing so, we shall be able to say how large $n$ needs to be to ensure that the formula for $e(M_{\Phi_{n/n_0}})$ holds and give information on $\nu_\Gamma(M)$.

LEMMA 4.2. *Let $n \geq 1$ and $F \in \Lambda(\Gamma)$ with $\gcd(F, \omega_n) = 1$. Consider the projection map*

$$\pi_n : \Lambda(\Gamma)/(F, \omega_n) \to \Lambda(\Gamma)/(F, \omega_{n-1}).$$

*We have*

(i) $\operatorname{rank}_{\mathbb{Z}_p} \Lambda(\Gamma)/(F, \omega_n) = \operatorname{rank}_{\mathbb{Z}_p} \Lambda(\Gamma)/(F, \omega_{n-1}) = 0$;
(ii) $\ker \pi_n$ *is finite and* $e(\ker \pi_n) = \operatorname{ord}_{\epsilon_n} F(\epsilon_n)$.

*Proof.* This is well-known (see e.g. [Was97, §13.3] or [Kob03, Lemma 10.5]). ∎

COROLLARY 4.3. *In the notation of Lemma 4.2, if*

$$F = up^\mu \prod_{i=1}^{r} F_i,$$

*where* $u \in \Lambda(\Gamma)^\times$, $\mu = \mu_\Gamma(F)$ *and* $F_i$ *are distinguished polynomials of degree* $d_i$, *then*

$$e(\ker \pi_n) = \mu p^{n-1}(p-1) + \lambda_\Gamma(F)$$

*whenever* $p^{n-1}(p-1) > d_i$ *for* $i = 1, \dots, r$.

*Proof.* Firstly, it is immediate that $\mathrm{ord}_{\epsilon_n}(u) = 0$ and $\mathrm{ord}_{\epsilon_n} p^\mu = \mu \times p^{n-1}(p-1)$. Secondly, for each $i$, we may write $F_i$ as $X^{d_i} + pG_i$ for some polynomial $G_i$ defined over $\mathbb{Z}_p$ with degree $< d_i$. As

$$d_i = \mathrm{ord}_{\epsilon_n}(\epsilon_n^{d_i}) < p^{n-1}(p-1) \le \mathrm{ord}_{\epsilon_n}(pG_i(\epsilon_n)),$$

we have $\mathrm{ord}_{\epsilon_n} F_i(\epsilon_n) = \deg F_i$. Hence the result. ∎

Corollary 4.4. *Suppose that* $F$ *is as in Corollary* 4.3. *Then*

$$e(\Lambda(\Gamma)/(F, \omega_n)) - e(\Lambda(\Gamma)/(F, \omega_{n_0})) = \mu(p^n - p^{n_0}) + \lambda_\Gamma(F)(n - n_0)$$

*for all* $n \ge n_0$, *where* $n_0$ *is a fixed integer satisfying* $p^{n_0-1}(p-1) > d_i$ *for* $i = 1, \dots, r$.

*Proof.* For $m \in \{n, n-1, \dots n_0 + 1\}$, Lemma 4.2(ii) tells us that

$$e(\ker \pi_m) = e(\Lambda(\Gamma)/(F, \omega_m)) - e(\Lambda(\Gamma)/(F, \omega_{m-1})).$$

Hence the result by Corollary 4.3. ∎

Lemma 4.5. *Let* $M$ *be a finitely generated torsion* $\Lambda(\Gamma)$*-module, with maximal pseudo-null submodule* $M'$. *Let* $\phi : M/M' \to \Lambda/(F)$ *be an injective* $\Lambda(\Gamma)$*-morphism with finite cokernel. Suppose that* $\gcd(F, \omega_m) = 1$ *for all* $m \ge 1$. *Then* $M_{\Gamma_n}$ *is finite and*

$$e(M_{\Gamma_n}) = e(\Lambda/(F, \omega_n)) + e(M'_{\Gamma_n}) \quad \text{for all } n \ge 1.$$

*Proof.* Let $C$ be the cokernel of $\phi$. Our assumption on $F$ implies that

$$\Lambda(\Gamma)/(F) \xrightarrow{\omega_n} \Lambda(\Gamma)/(F)$$

is injective. Applying the snake lemma to the short exact sequence $0 \to M/M' \to \Lambda/(F) \to C \to 0$, we have the exact sequence

$$0 \to C^{\Gamma_n} \to (M/M')_{\Gamma_n} \to \Lambda/(F, \omega_n) \to C_{\Gamma_n} \to 0.$$

Since $C$ is finite, the first and the last terms above have the same cardinality. Since $F$ is coprime to $\omega_n$, $\Lambda/(F, \omega_n)$ is finite and hence has the same cardinality as $(M/M')_{\Gamma_n}$.

Since $M/M'$ injects into $\Lambda(\Gamma)/(F)$, the fact that multiplication by $\omega_n$ is injective on $\Lambda(\Gamma)/(F)$ means that it is also injective on $M/M'$. Therefore, if we apply the snake lemma to $0 \to M' \to M \to M/M' \to 0$, we obtain

$$e(M_{\Gamma_n}) = e((M/M')_{\Gamma_n}) + e((M')_{\Gamma_n}),$$

which implies the result. ∎

We note that $M'_{\Gamma_n} = M'$ for $n \gg 0$ (see e.g. [NSW08, Lemma 5.3.14(v)]).

PROPOSITION 4.6. *Let $M$ be a finitely generated $\Lambda(\Gamma)$-module. Let $F \in \Lambda(\Gamma)$ be a generator of its characteristic ideal. Suppose that* $\gcd(F, \omega_m) = 1$ *for all integers $m \geq 1$. Let $n_0$ be an integer such that every irreducible distinguished polynomial that divides $F$ has degree $< p^{n_0-1}(p-1)$. Then*

$$e(M_{\Gamma_n}) - e(M_{\Gamma_{n_0}}) = \mu_\Gamma(M)(p^n - p^{n_0}) + \lambda_\Gamma(M)(n-n_0) + e(M'_{\Gamma_n}) - e(M'_{\Gamma_{n_0}})$$

*for all $n \geq n_0$.*

*Proof.* This is an immediate consequence of Corollary 4.4 and Lemma 4.5. ∎

**5. Estimating the growth of $e_{n,n}$ when $d = 2$.** Throughout this section, we assume that $d = 2$. Let $m, n \geq 0$ be integers and consider the $\Lambda(\Gamma)$-module

$$M_m := \mathcal{X}_{\infty,m} \cong \mathcal{X}/B_{\infty,m},$$

where $B_{\infty,m}$ is as defined in §2.2. By definition, this is the Galois group of the maximal pro-$p$ unramified extension of $K_{\infty,m}$. Then, by taking $\Gamma_n$-coinvariants, we have

$$(M_m)_{\Gamma_n} = \mathcal{X}/\langle I_{\Gamma_n}\mathcal{X}, B_{\infty,m}\rangle \cong \mathcal{X}_{n,m}$$

thanks to Lemma 2.2. As $\mathcal{X}_{n,m}$ is finite, $M_m$ is a finitely generated $\Lambda(\Gamma)$-module whose characteristic ideal is coprime to $\omega_n$ for all $n \geq 1$. We deduce from Proposition 4.6 that for a fixed $m$, there exists an integer $n_m$ such that for all $n \geq n_m$,

$$e_{n,m} - e_{n_m,m} = \mu_\Gamma(M_m)(p^n - p^{n_m}) + \lambda_\Gamma(M_m)(n-n_m) + e'_{n,m} - e'_{n_m,m}, \tag{5.1}$$

where $e'_{n,m} = e((M'_m)_{\Gamma_n})$, with $M'_m$ being the maximal pseudo-null submodule of $M_m$. We shall study how $\lambda_\Gamma(M_m)$, $\mu_\Gamma(M_m)$, $e(M'_m)$ and $n_m$ vary in $m$.

**5.1. Estimating Iwasawa invariants.** In this section, we assume that $\mathcal{X} \in \mathfrak{M}_H(G)$, where $\mathfrak{M}_H(G)$ is the category as defined in the introduction. Let us recall the definition of $\mu$-invariants of finitely generated $\Lambda(G)$-modules. Let $M$ be a finitely generated $\Lambda(G)$-module that is $\mathbb{Z}_p$-torsion. It is proved in [Ven02] that $M$ is pseudo-isomorphic to

$$\bigoplus_i \Lambda(G)/p^{n_i}$$

for some integers $n_i$. We have the $\mu$-invariant $\mu_G(M) := \sum n_i$. More generally, if $M$ is a finitely generated $\Lambda(G)$-module, we define $\mu_G(M) := \mu_G(M(p))$.

We shall write $\tilde{\mathcal{X}}$ for the quotient $\mathcal{X}/\mathcal{X}(p)$, which is finitely generated over $\Lambda(H)$ by our $\mathfrak{M}_H(G)$-hypothesis. Let $\tau_{\mathcal{X}}$ denote the $\Lambda(H)$-rank of $\tilde{\mathcal{X}}$.

We have the short exact sequence

$$0 \to \mathcal{X}(p) \to \mathcal{X} \to \tilde{\mathcal{X}} \to 0. \tag{5.2}$$

PROPOSITION 5.1. *We have*

$$\lambda_\Gamma(\mathcal{X}_{H_m}) = \tau_{\mathcal{X}} p^{(d-1)m} + O(1), \qquad \mu_\Gamma(\mathcal{X}_{H_m}) = \mu_G(\mathcal{X}) p^m.$$

*Proof.* From (5.2), there is a long exact sequence

$$H_1(H_m, \tilde{\mathcal{X}}) \to \mathcal{X}(p)_{H_m} \to \mathcal{X}_{H_m} \to \tilde{\mathcal{X}}_{H_m} \to 0.$$

Since $\mathcal{X}(p)$ is $\mathbb{Z}_p$-torsion, this tells us that

$$\operatorname{rank}_{\mathbb{Z}_p} \mathcal{X}_{H_m} = \operatorname{rank}_{\mathbb{Z}_p} \tilde{\mathcal{X}}_{H_m}.$$

But the latter is equal to $\tau_{\mathcal{X}} p^m + O(1)$ by [Har00, Theorem 1.10]. This gives the formula for $\lambda_\Gamma(H_m)$.

We now turn to the $\mu$-invariant. Since $\tilde{\mathcal{X}}$ is finitely generated over $\Lambda(H)$ and hence over $\Lambda(H_m)$, the homology groups $H_i(H_m, \tilde{\mathcal{X}})$ are finitely generated over $\mathbb{Z}_p$ for all $i \geq 0$. Therefore, the same long exact sequence tells us that

$$\mu_\Gamma(\mathcal{X}(p)_{H_m}) = \mu_\Gamma(\mathcal{X}_{H_m}).$$

Following [CK13, Lemma 5.2], we have

$$\mu_{H_m \rtimes \Gamma}(\mathcal{X}) = \mu_\Gamma\left(\mathcal{X}(p)_{H_m}\right).$$

But $[G : H_m \rtimes \Gamma] = p^m$, so the formula [CS05, (4)]) tells us that

$$\mu_{H_m \rtimes \Gamma}(\mathcal{X}) = \mu_G(\mathcal{X}) p^m.$$

Now the result follows by combining the last three equalities. ∎

**5.2. Estimating maximal finite submodules and $e_{n,n}$.** In this section, we assume that the hypothesis $\mu_\Gamma(M_0) = 0$ holds. We recall from Theorem 2.13 that this is equivalent to $\mathcal{X}$ being finitely generated over $\Lambda(H)$. This allows us to deduce the following estimates.

PROPOSITION 5.2. *If $M'_m$ is the maximal finite $\Lambda(\Gamma)$-submodule of $M_m$, then*

$$e(M'_m) = O(p^m).$$

*Proof.* We recall from §3 that there exist an integer $m_0$, $x_\nu \in \mathcal{X}$ and $k_\nu \in H \setminus H^p$ for each $\nu \in \Sigma \setminus \{\mathfrak{p}\}$ such that

$$B_{\infty,m} = I_{H_m} \mathcal{X} + \sum_\nu \Phi_{m/m_0}(k_\nu) \Lambda(H) \cdot x_\nu$$

for all $m \geq m_0$. Since we are assuming that $d = 2$ here, we may in fact assume that $k_\nu = h$ for all $\nu$, where $h$ is some fixed topological generator of $H$. In particular, we have

$$B_{\infty,m} = \Phi_{m/m_0}(h) B_{\infty,m_0}.$$

Since we are assuming that $\mathcal{X}$ is finitely generated over $\Lambda(H)$ and $H \cong \mathbb{Z}_p$, the structure theorem for finitely generated $\Lambda(H)$-modules tells us that

$$B_{\infty,m_0} \sim \Lambda(H)^r \oplus T,$$

where $\sim$ signifies pseudo-isomorphism, $r = \operatorname{rank}_{\Lambda(H)} B_{\infty,m_0}$ and $T$ is a torsion $\Lambda(H)$-module. Therefore,

$$e(B_{\infty,m_0}/B_{\infty,m}) = e((B_{\infty,m_0})_{\Phi_{m/m_0}(h)}) = e(T_{\Phi_{m/m_0}(h)}) = O(p^m),$$

as given by Theorem 4.1 (with $H$ replacing $\Gamma$).

The isomorphism theorem gives us the short exact sequence

$$0 \to B_{\infty,m_0}/B_{\infty,m} \to M_m \to M_{m_0} \to 0.$$

Hence $e(M_m) \le e(B_{\infty,m_0}/B_{\infty,m}) + e(M_{m_0})$, which finishes the proof. ∎

Corollary 5.3. *If $\mu_\Gamma(M_0) = 0$, then*

$$e_{n,n} = \tau_{\mathcal{X}} n p^n + O(p^n).$$

*Proof.* Under our assumption on $\mathcal{X}$, [DL17, Corollary A.4] tells us that there exists an integer $\rho$ such that the $\Lambda(\Gamma)$-characteristic ideal of $\mathcal{X}_{H_m}$ factorises into polynomials whose degrees are bounded by $\rho$. The same can be said about $M_m$ given that it is a quotient of $\mathcal{X}_{H_m}$. In particular, by Proposition 4.6, the estimates in (5.1) hold whenever $p^{n-1}(p-1) > \rho$. Hence, we may choose $n_m = n_0$ for some fixed $n_0$ that is independent of $m$.

We recall from Corollary 3.4 that $e_{n_0,m} = O(p^m)$. Furthermore, if $\mathcal{X}$ is finitely generated over $\Lambda(H)$, then $\mu_G(\mathcal{X}) = 0$. Hence, our result follows by combining (5.1) with Propositions 5.1 and 5.2. ∎

**6. Bounding $\tilde{e}_{n,n}$ in the case $d = 2$.** In this section, we assume that $d = 2$ and $\mathcal{X} \in \mathfrak{M}_H(G)$. Since $X$ is torsion over $\mathfrak{M}_H(G)$ in this setting, we have already seen in Corollary 2.12 that the asymptotic formula of Perbert can be improved to

$$\tilde{e}_{n,n} = \mu p^{2n} + O(np^n).$$

However, the error term is larger than that of Corollary 5.3. We now show that we may obtain an upper bound on $\tilde{e}_{n,n}$ with the same error term under our assumption $\mathcal{X} \in \mathfrak{M}_H(G)$.

Proposition 6.1. *Assume that $\mathcal{X} \in \mathfrak{M}_H(G)$ and write $\tilde{\mathcal{X}} = \mathcal{X}/\mathcal{X}(p)$. Then*

$$e(\mathcal{X}_{G_{n,n}}) \le \mu_G(\mathcal{X}) p^{2n} + \tau_{\mathcal{X}} n p^n + O(p^n),$$

*where $\tau_{\mathcal{X}} = \operatorname{rank}_{\Lambda(H)} \tilde{\mathcal{X}}$.*

*Proof.* From (5.2), we obtain the long exact sequence

$$\cdots \to \mathcal{X}(p)_{G_{n,n}} \to \mathcal{X}_{G_{n,n}} \to \tilde{\mathcal{X}}_{G_{n,n}} \to 0. \tag{6.1}$$

We shall use $e(\tilde{\mathcal{X}}_{G_{n,n}})$ and $e(\mathcal{X}(p)_{G_{n,n}})$ to bound $e(\mathcal{X}_{G_{n,n}})$.

Since $\tilde{\mathcal{X}}$ is finitely generated over $\Lambda(H)$, we have already seen in the proofs of Propositions 5.1 and 5.2 that $\tilde{\mathcal{X}}_{H_n}$ is a finitely generated $\Lambda(\Gamma)$-module with

$$\mu_\Gamma(\tilde{\mathcal{X}}_{H_n}) = 0, \quad \lambda_\Gamma(\tilde{\mathcal{X}}_{H_n}) = \tau_{\mathcal{X}} p^n + O(1), \quad e(\tilde{\mathcal{X}}'_{H_n}) = O(p^n).$$

Consequently, $e(\tilde{\mathcal{X}}_{G_{n,n}}) = \tau_{\mathcal{X}} n p^n + O(p^n)$ by Theorem 4.1.

Since $\mathcal{X}(p)$ is $\mathbb{Z}_p$-torsion and finitely generated over $\Lambda(G)$, it follows that $\mathcal{X}(p)_{G_{n,n}}$ is finite. Recall that there is a pseudo-isomorphism of $\Lambda(G)$-modules

$$\mathcal{X}(p) \sim \bigoplus_i \Lambda(G)/p^{n_i}$$

for some integers $n_i$. In general, if $M$ and $N$ are pseudo-isomorphic $\Lambda(G)$-modules that are both $\mathbb{Z}_p$-torsion, then [DL17, Lemma 4.2] tells us that

$$\#M_{G_{n,n}} = (\#N_{G_{n,n}}) p^{O(p^n)}$$

under our assumptions. Therefore,

$$\#\mathcal{X}(p)_{G_{n,n}} = \Big(\#\bigoplus_i \mathbb{Z}_p[G/G_{n,n}]/p^{n_i}\Big) p^{O(p^n)},$$

and hence

$$e(\mathcal{X}(p)_{G_{n,n}}) = p^{2n} \sum_i n_i + p^n = \mu_G(\mathcal{X}) p^{2n} + O(p^n).$$

This finishes our proof. ∎

Corollary 6.2. *We have the upper bound*

$$\tilde{e}_{n,n} \leq \mu_G(\mathcal{X}) p^{2n} + \tau_{\mathcal{X}} n p^n + O(p^n).$$

*Proof.* First of all, we observe that $\tilde{e}_{n,n} \leq e(\mathcal{X}_{G_{n,n}}/p^n)$ thanks to the short exact sequence (2.3). Therefore, it is enough to bound $e(\mathcal{X}_{G_{n,n}}/p^n)$.

Since $\mathcal{X}_{G_{n,n}}$ is a finitely generated $\mathbb{Z}_p$-module, it is isomorphic to

$$\mathbb{Z}_p^{\oplus a_n} \oplus T_n$$

for some integer $a_n \geq 0$ and some finite $\mathbb{Z}_p$-module $T_n$. This gives an isomorphism of abelian groups

$$\mathcal{X}_{G_{n,n}}/p^n \cong (\mathbb{Z}/p^n)^{a_n} \times T_n/p^n.$$

In particular, this tells us that

$$e(\mathcal{X}_{G_{n,n}}/p^n) = a_n n + e(T_n/p^n) \leq a_n n + e(T_n).$$

Since we are assuming $d = 2$, Corollary 2.10 tells us that $a_n = O(1)$. Hence we are done by the bound on $e(T_n)$ given in Proposition 6.1. ∎

**Acknowledgements.** We would like to thank Daniel Delbourgo, Dohyeong Kim and Bharathwaj Palvannan for very informative discussions during the preparation of this paper. We are also indebted to the anonymous referees for their valuable comments and suggestions which led to many improvements in the paper.

The author's research is supported by FRQNT's Établissement de nouveaux chercheurs universitaires program 188809.

## References

[BH97] P. N. Balister and S. Howson, *Note on Nakayama's lemma for compact $\Lambda$-modules*, Asian J. Math. 1 (1997), 224–229.

[CFK+05] J. Coates, T. Fukaya, K. Kato, R. Sujatha, and O. Venjakob, *The* $\mathrm{GL}_2$ *main conjecture for elliptic curves without complex multiplication*, Publ. Math. Inst. Hautes Études Sci. 101 (2005), 163–208.

[CH01] J. Coates and S. Howson, *Euler characteristics and elliptic curves. II*, J. Math. Soc. Japan 53 (2001), 175–235.

[CK13] J. Coates and D. Kim, *Introduction to the work of M. Kakde on the noncommutative main conjectures for totally real fields*, in: Noncommutative Iwasawa Main Conjectures over Totally Real Fields, Springer Proc. Math. Statist. 29, Springer, Heidelberg, 2013, 1–22.

[CM81] A. A. Cuoco and P. Monsky, *Class numbers in* $\mathbb{Z}_p^d$*-extensions*, Math. Ann. 255 (1981), 235–258.

[CS05] J. Coates and R. Sujatha, *Fine Selmer groups of elliptic curves over p-adic Lie extensions*, Math. Ann. 331 (2005), 809–839.

[DL17] D. Delbourgo and A. Lei, *Estimating the growth in Mordell–Weil ranks and Shafarevich–Tate groups over Lie extensions*, Ramanujan J. 43 (2017), 29–68.

[MF16] L. M. Fai, *Fine Selmer groups of congruent Galois representations*, arXiv: 1603.08640 (2016).

[FW79] B. Ferrero and L. C. Washington, *The Iwasawa invariant* $\mu_p$ *vanishes for abelian number fields*, Ann. of Math. (2) 109 (1979), 377–395.

[Har00] M. Harris, *Correction to: "p-adic representations arising from descent on abelian varieties" [Compos. Math. 39 (1979), 177–245]*, Compos. Math. 121 (2000), 105–108.

[Iwa73a] K. Iwasawa, *On* $\mathbb{Z}_l$*-extensions of algebraic number fields*, Ann. of Math. (2) 98 (1973), 246–326.

[Iwa73b] K. Iwasawa, *On the* $\mu$*-invariants of* $\mathbb{Z}_\ell$*-extensions*, in: Number Theory, Algebraic Geometry and Commutative Algebra, in honor of Yasuo Akizuki, Kinokuniya, Tokyo, 1973, 1–11.

[Kak13] M. Kakde, *The main conjecture of Iwasawa theory for totally real fields*, Invent. Math. 193 (2013), 539–626.

[Kob03] S.-I. Kobayashi, *Iwasawa theory for elliptic curves at supersingular primes*, Invent. Math. 152 (2003), 1–36.

[Lee13] C.-Y. Lee, *Non-commutative Iwasawa theory of elliptic curves at primes of multiplicative reduction*, Math. Proc. Cambridge Philos. Soc. 154 (2013), 303–324.

[NSW08] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of Number Fields*, 2nd ed., Grundlehren Math. Wiss. 323, Springer, Berlin, 2008.

[OV02] Y. Ochi and O. Venjakob, *On the structure of Selmer groups over p-adic Lie extensions*, J. Algebraic Geom. 11 (2002), 547–580.

[Per11] G. Perbet, *Sur les invariants d'Iwasawa dans les extensions de Lie p-adiques*, Algebra Number Theory 5 (2011), 819–848.

[RW11] J. Ritter and A. Weiss, *On the "main conjecture" of equivariant Iwasawa theory*, J. Amer. Math. Soc. 24 (2011), 1015–1050.

[Ser63] J.-P. Serre, *Cohomologie galoisienne*, Lecture Notes in Math. 5, Springer, Berlin, 1962/1963.

[Ven02] O. Venjakob, *On the structure theory of the Iwasawa algebra of a p-adic Lie group*, J. Eur. Math. Soc. 4 (2002), 271–311.

[Ven03a] O. Venjakob, *A non-commutative Weierstrass preparation theorem and applications to Iwasawa theory* (with an appendix by D. Vogel), J. Reine Angew. Math. 559 (2003), 153–191.

[Ven03b] O. Venjakob, *On the Iwasawa theory of p-adic Lie extensions*, Compos. Math. 138 (2003), 1–54.

[Viv04] F. Viviani, *Ramification groups and Artin conductors of radical extensions of* $\mathbb{Q}$, J. Théor. Nombres Bordeaux 16 (2004), 779–816.

[Was97] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Grad. Texts in Math. 83, Springer, New York, 1997.

Antonio Lei
Département de mathématiques et de statistique
Université Laval
Pavillon Alexandre-Vachon
1045 avenue de la Médecine
Québec QC, Canada G1V 0A6
E-mail: antonio.lei@mat.ulaval.ca