ESTIMATING CLASS NUMBERS OVER METABELIAN EXTENSIONS

ANTONIO LEI

Abstract. Let \( p \) be an odd prime and \( K_{\infty, \infty}/K \) a \( p \)-adic Lie extension whose Galois group is of the form \( \mathbb{Z}_d^{d-1} \rtimes \mathbb{Z}_p \). Under certain assumptions on the ramification of \( p \) and the structure of an Iwasawa module associated to \( K_{\infty, \infty} \), we study the asymptotic behaviours of the size of the \( p \)-primary part of the ideal class groups over certain finite subextensions inside \( K_{\infty, \infty}/K \). This generalizes the classical result of Iwasawa and Cuoco-Monsky in the abelian case and gives a more precise formula than a recent result of Perbet in the non-commutative case when \( d = 2 \).

1. Introduction

1.1. Setup and notation. We fix throughout this article 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 \( K_c/K \) contained inside \( K_{\infty, \infty} \) and assume that

- \( \text{Gal}(K_{\infty, \infty}/K_c) \) 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 \( K = \mathbb{Q}(\mu_p) \), \( K_c = \mathbb{Q}(\mu_{p^\infty}) \) and \( K_{\infty, \infty} \) the Kummer extension \( \mathbb{Q}(\mu_p^{\infty}, \sqrt[\infty]{\alpha}) \), where \( \alpha \neq 0 \) is an integer such that \( p^r | \alpha^p - 1 \) (such \( \alpha \) 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

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

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 that the products \( \alpha_1^{n_1} \cdots \alpha_{d-1}^{n_{d-1}} \), \( 0 \leq n_i \leq p - 1 \), are all amenable (as this implies that \( p \) totally ramifies in all cyclic sub-extensions of \( K_{\infty, \infty}/K_c \)).

We denote the Galois groups \( G = \text{Gal}(K_{\infty, \infty}/K) \), \( H = \text{Gal}(K_{\infty, \infty}/K_c) \) and \( \Gamma = \text{Gal}(K_c/K) \). 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. 11R29 (primary), 11R23 (secondary).

Key words and phrases. Non-commutative Iwasawa theory, class numbers, metabelian extensions.

The author’s research is supported by FRQNT’s Établissement de nouveaux chercheurs universitaires program 188809.
For $0 \leq m, n \leq \infty$, we denote $H_m = H^{p^m}$, $\Gamma_n = \Gamma^{p^n}$, $G_{n,m} = H_m \times \Gamma_n \leq G$ and $K_{n,m} = K^{p^\infty}$. We define $X_{n,m}$ to be the Hilbert $p$-class group of $K_{n,m}$ and write $e_{n,m}$ for the $p$-exponent of $\#X_{n,m}$.

For any $p$-adic Lie group $L$, we shall write $\Lambda(L)$ for the Iwasawa algebra
\[ \mathbb{Z}_p[[L]] = \lim_{N \to \infty} \mathbb{Z}_p[L/N]. \]
If $G$ is a pro-$p$ group and $x_1, \ldots, x_r \in G$, we shall write $(x_1, \ldots, x_r)$ for the $p$-adic completion of the subgroup generated by the elements $x_1, \ldots, x_r$. Similarly, if $X_1, \ldots, X_r \subseteq G$, $(X_1, \ldots, X_r)$ denotes the closed subgroup generated by $X_1, \ldots, X_r$.

1.2. Main results. Let $X$ (respectively $X'$) 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 $X$ is torsion over $\Lambda(\Gamma)$. Our first result is a generalization of this result.

Theorem (Theorem 2.11). The $\Lambda(G)$-module $X$ is torsion.

On studying the structure of $X$ 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
\[ e_{n,m} = \mu_n \times p^{(d-1)m} + \lambda_n \times mp^{(d-2)m} + O(p^{d-2}m) \]
gequation 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
\[ \mathbb{Q} \left( \mu_{p^n}, \sqrt[p]{\alpha_1}, \ldots, \sqrt[p]{\alpha_{d-1}} \right) \]
varies as $m \to \infty$. In particular, these extensions are not Galois in general. This is analogous to the main result of [CMS03] 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 (c.f. [CFK05, Kak13, OV02, RW11, Ven02, Ven03]), $X'$ is conjectured to be inside $\mathfrak{M}_H(G)$ for totally real fields. Since $X$ is a quotient of $X'$, this would imply that $X \subseteq \mathfrak{M}_H(G)$ 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 $X'$ itself (not just $X/X(p)$) 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 $X$ is finitely generated over $\Lambda(H)$. 
Theorem (Corollary 5.3). Suppose that \(d = 2\) and \(X\) is finitely generated over \(\Lambda(H)\). If the unique prime of \(K\) above \(p\) is totally ramified in \(K_{\infty,\infty}\), then
\[
\epsilon_{n,n} = \tau \times np^n + O(p^n),
\]
where \(\tau = \text{rank}_{\Lambda(H)} X\).

We remark that our theorem always applies when \(K_{\infty,\infty} = \mathbb{Q}(\mu_{p^\infty}, \sqrt[p]{\alpha})\) for some integer \(\alpha\) that is amenable for \(p\) since the theorem of Ferrero-Washington tells us that our hypothesis on \(X\) holds. In particular, it confirms the prediction made by Venjakob \cite{Ven02} for the extension \(\mathbb{Q}(\mu_{p^\infty}, \sqrt[p]{\alpha})\). Our result can also be seen as a generalization of the classical result of Iwasawa \cite{Iwa73} 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 \cite{CM81} again in the case when the \(\mu\)-invariant is 0 (denoted by \(m_0\) in loc. cit.).

In \cite{Per11}, Perbet 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 \(X\) being finitely generated over \(\Lambda(H)\) nor any assumption on the ramification of \(p\). More precisely, if \(\tilde{\epsilon}_{n,n}\) denotes the \(p\)-exponent of \(#X_{n,n}/p^n\) (rather than \(X_{n,n}\) itself), Perbet showed that
\[
(1.1) \quad \tilde{\epsilon}_{n,n} = \rho \times np^{dn} + \mu \times p^{dn} + O(np^{(d-1)n}),
\]
where \(\rho = \text{rank}_{\Lambda(G)} X\) and \(\mu\) is the \(\mu\)-invariant of \(X\) as defined in \cite{Ven02}. Under our assumption that \(X\) is finitely generated over \(\Lambda(H)\), both \(\rho\) and \(\mu\) vanish. In this case, the formula of Perbet becomes simply \(O(np^{(d-1)n})\). 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 \(\tilde{\epsilon}_{n,n}\) in the case \(d = 2\) and \(X \in \mathfrak{M}_H(G)\) (the constant \(\rho\) would be 0, but \(\mu\) may be non-zero).

Theorem (Corollary 6.2). If \(d = 2\) and \(X \in \mathfrak{M}_H(G)\), then
\[
\epsilon_{n,n} \leq \mu \times p^{2n} + \tau \times np^n + O(p^n),
\]
where \(\tau = \text{rank}_{\Lambda(H)} X/\mathcal{X}(p)\).

Acknowledgment. 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.

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, \(p \in \Sigma\). Since \(p\) 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 \(K^c\) lying above \(\nu\). On replacing \(K\) by \(K_{\nu,0}\) if necessary, we may assume that \(\nu\) is inert in \(K^c\). 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 \(X = \text{Gal}(\mathcal{M}/K_{\infty,\infty})\) and \(\mathcal{Y} = \text{Gal}(\mathcal{M}/K)\). Note that \(X\) is normal in \(\mathcal{Y}\) with \(\mathcal{Y}/X \cong G\). For each \(g \in G\), let \(\tilde{g} \in \mathcal{Y}\) be a lifting of \(g\). If \(x \in X\), 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 $\tilde{\nu}$ a prime of $\mathcal{M}$ above $\nu$ and write $I_{\nu}$ for the inertia group of $\tilde{\nu}$ inside $\mathcal{Y}$. We note that $I_p$ is isomorphic to $G$ since we assume that $p$ is totally ramified in $K_{\infty,\infty}$ and it is unramified in $\mathcal{M}$. In particular, we have the isomorphism

\begin{equation}
\mathcal{Y} \cong \mathcal{X} \rtimes G,
\end{equation}

where we identify $G$ with $I_p$. 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, we have the equality

\begin{equation}
I_p = \{(1, g) : g \in G\}.
\end{equation}

For $0 \leq m, n \leq \infty$, we define $\mathcal{Y}_{n,m} = \text{Gal}(\mathcal{M}/K_{n,m})$. For each $\nu \in \Sigma$, we write $I_{\nu_{n,m}}$ for the inertia group of our choice of $\tilde{\nu}$ inside $\mathcal{Y}_{n,m}$ and $I_{\nu_{n,m}}$ its image under the natural projection $\mathcal{Y}_{n,m} \to G_{n,m}$. We note that $I_{\nu_{n,m}} \cong I_{\nu_{n,m}}$ 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 $I_{\nu_{n,m}}$ in the quotient $\mathcal{Y}_{n,m}/[\mathcal{X}, \mathcal{Y}_{n,m}]$ is normal. That is, 

$$
([\mathcal{X}, \mathcal{Y}_{n,m}], I_{\nu_{n,m}})/[\mathcal{X}, \mathcal{Y}_{n,m}] \trianglelefteq \mathcal{Y}_{n,m}/[\mathcal{X}, \mathcal{Y}_{n,m}].
$$

**Proof.** Let $(1, g) \in I_{\nu_{n,m}}$ (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 $x^g = x^{-1}\tilde{g}^{-1}x\tilde{g} \in [\mathcal{X}, \mathcal{Y}_{n,m}]$, hence the result. \qed

Let $C_{n,m}$ the subgroup of $\mathcal{Y}_{n,m}$ generated by $[\mathcal{Y}_{n,m}, \mathcal{Y}_{n,m}]$ and all the inertia groups $I_{\nu_{n,m}}$ 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 $X_{n,m}$ 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 $X_{n,m} \cong \mathcal{X}/B_{n,m}$.

**Proof.** Class field theory tells us that

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

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

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

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

$$\mathcal{Y}_{n,m}/\mathcal{X}C_{n,m} \cong G_{n,m}/(\langle G_{n,m}, G_{n,m} \rangle, I_{\nu_{n,m}} : \nu \in \Sigma, \sigma \in H).$$ 

But $p \in \Sigma$ and $I_{\nu_{n,m}} = G_{n,m}$ since $p$ is totally ramified in $K_{\infty,\infty}$. Hence, this quotient is trivial and the result follows. \qed
In particular, this gives us the following short exact sequence:

\[ 0 \to B_{n,m} / I_{G_{n,m}} \to X / I_{G_{n,m}} X \to X_{n,m} \to 0. \]

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 \( g - 1 \), \( g \in G_{n,m} \). We have the following description.

**Lemma 2.3.** We have the equality

\[ [X, Y_{n,m}] = I_{G_{n,m}} X. \]

**Proof.** Let \( x \in X \) and \( y \in Y_{n,m} \). We write \( \bar{y} \) for the image of \( y \) in \( G_{n,m} \). Then,

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

Hence the result. \( \square \)

**Corollary 2.4.** The augmentation ideal \( I_{G_{n,m}} X \) is a normal subgroup of \( Y_{n,m} \).

**Proof.** As we have seen in Lemma 2.1 \([X, Y_{n,m}]\) is normal in \( Y_{n,m} \). Hence, the result follows from Lemma 2.3. \( \square \)

The augmentation ideal allows us to describe the commutator subgroup of \( Y_{n,m} \) as follows.

**Proposition 2.5.** We have the equality

\[ [Y_{n,m}, Y_{n,m}] = \langle I_{G_{n,m}} X, [I_{p_{n,m}}, I_{p_{n,m}}] \rangle. \]

**Proof.** Recall that \( X \) is normal in \( Y_{n,m} \), \( Y_{n,m} / X \cong G_{n,m} \) and \( I_{p_{n,m}} X / X \cong G_{n,m} \). Hence, every element of \( Y_{n,m} \) can be written as \( x \cdot b \) for some \( x \in X \) and \( b \in I_{p_{n,m}} \). Let \( x_1 b_1, x_2 b_2 \) be any two elements of \( Y_{n,m} \) written in this way. We have the commutator identity

\[ [x_1 b_1, x_2 b_2] = [x_1, x_2 b_2]^{b_1} [b_1, x_2 b_2] = [x_1, x_2 b_2]^{b_1} [b_1, x_2]^{b_2}. \]

On the one hand, \([b_1, b_2] \in [I_{p_{n,m}}, I_{p_{n,m}}]\) by definition. On the other hand, both \([x_1, x_2 b_2] \) and \([b_1, x_2]\) are inside \([X, Y_{n,m}]\), which is equal to \( I_{G_{n,m}} X \) by Lemma 2.3. Hence the result. \( \square \)

**Corollary 2.6.** We have

\[ C_{n,m} = \langle I_{G_{n,m}} X, I_{p_{n,m}}^\sigma : \nu \in \Sigma, \sigma \in X \rtimes H \rangle; \]

\[ B_{n,m} = I_{G_{n,m}} X + (I_{p_{n,m}}^\sigma : \nu \in \Sigma, \sigma \in X \rtimes H) \cap X. \]

**Proof.** By definition \([Y_{n,m}, Y_{n,m}] \subset C_{n,m} \) and \( I_{G_{n,m}} X \subset X \), so we see from Proposition 2.5 that \( I_{G_{n,m}} X \subset B_{n,m} \).

Furthermore, Corollary 2.4 says that \( I_{G_{n,m}} X \) is normal in \( Y_{n,m} \). Therefore, the second equality follows from the first.

Recall that \( C_{n,m} \) is defined to be

\[ \langle [Y_{n,m}, Y_{n,m}], I_{p_{n,m}}^\sigma : \nu \in \Sigma, \sigma \in X \rtimes H \rangle. \]

Therefore, the first equality follows from the description of \([Y_{n,m}, Y_{n,m}] \) in Proposition 2.5 and the fact that \([I_{p_{n,m}}, I_{p_{n,m}}]\) is contained in \( I_{p_{n,m}} \). \( \square \)
Proposition 2.7. The quotient $B_{n,m}/IG_{n,m} \mathcal{X}$ is a $\Lambda(H)$-module generated by the elements $x \in \mathcal{X}$ satisfying the property that $(x, h) \in I_{\nu_n,m}$ for some $\nu \in \Sigma \setminus \{p\}$ and $h \in H_m$.

Proof. Suppose that $(x, h) \in I_{\nu_n,m}$ for some $h \in H_m$ and $\nu \in \Sigma \setminus \{p\}$, then $(1, h) \in I_{\nu_n,m}$ 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 we may find explicit generators for the quotient $I_{\nu_n,m} / (\mathcal{X} \cap I_{\nu_n,m})$ is a normal subgroup. By Lemma 2.3, we have $[\mathcal{X}_{\nu_n,m}, \mathcal{Y}_{\nu_n,m}] = IG_{n,m} \mathcal{X}$. Hence,

$$\langle I_{\nu_n,m} \mathcal{X}, I_{p_n,m} / IG_{n,m} \mathcal{X} \rangle \cong C_{n,m} / IG_{n,m} \mathcal{X}.$$ 

On applying Corollary 2.6 we deduce that every element in $C_{n,m} / IG_{n,m} \mathcal{X}$ may be written as a product $\alpha \beta$ for some $\alpha \in \langle I_{\nu_n,m} : \nu \in \Sigma \setminus \{p\}, \sigma \in \mathcal{X} \times H \rangle$ and $\beta \in I_{\nu_n,m}$.

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

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

given that $H$ is abelian. But $x_{\sigma}^{(h_{\nu})^{-1}h_{\sigma}^{-1}} \in [\mathcal{X}, \mathcal{X} \times H_m] \subset IG_{n,m} \mathcal{X}$ by Lemma 2.3 and the fact that $h_{\nu} \in H_m$. Furthermore, we have the identity $(x_{\nu}, h_{\nu})(x_{\nu'}, h_{\nu'}) = (x_{\nu, h_{\nu}^{-1}h_{\nu'}}, h_{\nu}h_{\nu'})$, 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. \[\square\]

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

The aforementioned quotient is generated by the “projection” of $I_{\nu_n,m}^h$ in $\mathcal{X}$, where $\nu \in \Sigma \setminus \{p\}$ 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

$$xy^g \equiv xy \mod [\mathcal{X}, \mathcal{Y}_{n,m}] = IG_{n,m} \mathcal{X}$$

by Lemma 2.3. Therefore, the map

$$\mathcal{Y}_{n,m} / IG_{n,m} \mathcal{X} \to \mathcal{X} / IG_{n,m} \mathcal{X}$$

$$(x, g) \mapsto x$$

is a well-defined group homomorphism.

Lemma 2.8. The quotient $B_{n,m} / IG_{n,m} \mathcal{X}$ 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 $\Sigma \setminus \{p\}$.

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

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

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 \( \Sigma \setminus \{ p \} \) 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 is a finite number of primes in \( K_{\infty,m} \), part (i) follows.

We now prove part (ii). Fix a prime \( \bar{\nu} \) of \( K_{\infty,\infty} \) above \( \nu \in \Sigma \setminus \{ p \} \). 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 \( K^c/K_{n,0} \) for \( n \) sufficiently large. Therefore, the decomposition group of \( \bar{\nu} \) is of dimension two.

Let \( \bar{\sigma} \) be a prime of \( K_{n,m} \) above \( \nu \). Let \( G_{\bar{\sigma}} \) be the decomposition group of \( \bar{\sigma} \) 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

\[
|G_{\bar{\sigma}}| \geq C \times p^{n+m}
\]

for all \( \bar{\sigma} \). But

\[
p^{n+(d-1)m} = |G : G_{n,m}| = \sum_{\bar{\sigma} \mid \nu} |G_{\bar{\sigma}}|.
\]

If \( r_{n,m,\nu} \) denotes the number of places of \( K_{n,m} \) above \( \nu \). Then,

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

which gives (ii). □

On combining these two lemmas, we deduce:

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

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

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

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

**Theorem 2.11.** The \( \Lambda(G) \)-module \( X \) is torsion.

**Proof.** As we have recalled above, \( X \) 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

\[
\text{rank}_{\mathbb{Z}_p} X/I_{G_{n,n}}X = \rho \times p^{dn} + O(p^{(d-1)n}).
\]

By [2.8], together with Corollary 2.10 and the finiteness of \( X_{n,n} \), we have in fact

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

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 \( \#X_{n,n}/p^n \). Then,
\[
\tilde{e}_{n,n} = \mu \times p^{dn} + O(np^{(d-1)n}),
\]
for some integer \( \mu \).

Under an additional hypothesis on \( X_{\infty,0} \), we can in fact show more:

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

Proof. The short exact sequence (2.3) becomes
\[
0 \to B_{\infty,0}/I_H X \to X/I_H X \to X_{\infty,0} \to 0
\]
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 \( X \) is finite over \( \Lambda(H) \), then \( X/I_H X \) is finite over \( \mathbb{Z}_p \), which gives one implication of the theorem. If on the other hand \( X_{\infty,0} \) is finite over \( \mathbb{Z}_p \), then so is \( X/I_H X \). Consequently, Nakayama’s Lemma (c.f. [CH01, Lemma 2.6] or [BH97]) implies that \( X \) is finite over \( \Lambda(H) \), which gives the other implication as claimed. \( \Box \)

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 \( X \) is finitely generated over \( \Lambda(G) \). Consequently, \( X_{\Gamma_n} \) is a finitely generated \( \Lambda(\Gamma) \)-module. In fact, we can say more:

Lemma 3.1. The \( \Lambda(\Gamma) \)-module \( X_{\Gamma_n} \) is torsion.

Proof. Let \( M \) be a finitely generated \( \Lambda(\Gamma) \)-module. If \( \text{rank}_{\Lambda(H)} M = r \), then
\[
\text{rank}_{\mathbb{Z}_p} M_{H_m} = r \times p^{(d-1)m} + O(p^{(d-2)m})
\]
(c.f. [Har00, Theorem 1.10]).

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

We recall the following definition from [CMS1, §4]. Let \( M \) be a finitely generated torsion \( \Lambda(H) \)-module. A structure \( S \) 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 \( M_i \) submodules of \( M \). For every structure of \( M \), we define for \( m \geq m_0 \)
\[
A_m(S) = I_{H_m} M + \sum_i \Phi_{m/m_0}(\tau_i) \cdot M_i,
\]
where \( \Phi_{m/m_0}(X) \) denotes the polynomial \( (X^{p^n} - 1)/(X^{p^{m_0}} - 1) \). Such a structure is said to be admissible if \( \text{rank}_{\mathbb{Z}_p} M/A_m(S) = O(p^{(d-3)n}) \) (for \( d \geq 3 \)) or \( \text{rank}_{\mathbb{Z}_p} M/A_m(S) = O(1) \) (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 loc. cit.
Theorem 3.2. Let $M$ be a finitely generated torsion $\Lambda(H)$-module and $S$ an admissible structure on $M$. Then,

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

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

Proof. This is Lemma 4.9 and Theorem 4.13 in op. cit. 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 $S$ on $X_{\Gamma_n}$ such that $X_{n,m} = X_{\Gamma_n}/A_m(S)$ for $m \gg 0$.

Proof. Let $\nu \in \Sigma \setminus \{p\}$. Then $I_{\nu,m}$ is a subgroup of $H_m$. Therefore, there exists an integer $m_0$ such that $H_m/I_{\nu,m}$ 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 $I_{\nu,m}$ is of dimension 1. Suppose that $I_{\nu,m_0} = \langle (x_{\nu}, h_{\nu}) \rangle$. 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

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

Therefore, Proposition 2.7 tells us that

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

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

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

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

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 $\mathbb{Z}_p[[X]]$ on 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 shall fix a primitive $p^n$-th root of unity $\zeta_{p^n}$ and write $\epsilon_n = \zeta_{p^n} - 1$.

Finally, we write $\Phi_{n/m_0} = \omega_n/\omega_{m_0}$ for $n \geq m_0$ as in [K].

Let $F \in \Lambda(\Gamma)$. Weierstrass Preparation Theorem tells us that there exists a factorization $F = u \times p^{\mu} \times g$, 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 $X_{\infty,0}$ being finitely generated over $\mathbb{Z}_p$ in Theorem 2.13 is equivalent to $\mu_{\Gamma}(X_{\infty,0}) = 0$.

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 $n_{\Gamma}(M)$ and $n_0$ such that $M_{\Phi_n/n_0}$ is finite with

$$e(M_{\Phi_n/n_0}) = \mu_{\Gamma}(M) \times p^n + \lambda_{\Gamma}(M) \times n + n_{\Gamma}(M)$$

for all $n \geq n_0$.

This result has been reproved in many different places, e.g. [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 $n_{\Gamma}(M)$.

**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) $\text{rank}_{\mathbb{Z}_p} \Lambda(\Gamma)/(F, \omega_n) = \text{rank}_{\mathbb{Z}_p} \Lambda(\Gamma)/(F, \omega_{n-1}) = 0$;

(ii) $\ker \pi_n$ is finite and $e(\ker \pi_n) = \text{ord}_{\epsilon_n} F(\epsilon_n)$.

**Proof.** This is well-known. See for example [Was97, §13.3] or [Kob03 Lemma 10.5].

**Corollary 4.3.** Under the same notation as Lemma 4.2, if

$$F = u \times p^\mu \times \prod_{i=1}^{r} F_i,$$

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

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

whenever $p^n(p-1) > d_i$ for $i = 1, \ldots, r$.

**Proof.** Firstly, it is immediate that $\text{ord}_{\epsilon_n}(u) = 0$ and $\text{ord}_{\epsilon_n} p^\mu = \mu \times p^{n-1}(p-1)$. 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

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

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

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

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

for all $n \geq n_0$, where $n_0$ is a fixed integer satisfying $p^{n_0-1}(p-1) > d_i$ for $i = 1, \ldots, r$. 
Proof. For \( m \in \{ n, n-1, \ldots, n_0 + 1 \} \), Lemma 4.3(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.
\[ \square \]

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 \( m \geq 1 \). Then, \( M_{\Gamma_n} \) is finite and
\[
e(M_{\Gamma_n}) = e(\Lambda/(F, \omega_n)) + e(M_{\Gamma_n}')
\]
for any integer \( n \geq 1 \).

Proof. Let \( C \) be the cokernel of \( \phi \). Our assumption on \( F \) implies that
\[
\Lambda(\Gamma)/(F) \overset{\omega_n}{\longrightarrow} \Lambda(\Gamma)/(F)
\]
is injective. On 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 of the exact sequence have the same cardinality. Since \( F \) is coprime to \( \omega_n \), \( \Lambda/(F, \omega_n) \) is finite and hence have 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 have
\[
e(M_{\Gamma_n}) = e((M/M')_{\Gamma_n}) + e((M')_{\Gamma_n}),
\]
which implies the result.
\[ \square \]

We note that \( M_{\Gamma_n}' = M' \) for \( n \gg 0 \) (see for example [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 all the irreducible distinguished polynomials that divide \( F \) have degree \(< p^{n_0-1}(p-1) \). Then,
\[
e(M_{\Gamma_n}) - e(M_{\Gamma_{n_0}}) = \mu_{\Gamma}(M) \times (p^n - p^{n_0}) + \lambda_{\Gamma}(M) \times (n - n_0) + e(M'_{\Gamma_n}) - e(M'_{\Gamma_{n_0}})
\]
for all \( n \geq n_0 \).

Proof. This is an immediate consequence of Corollary 4.1 and Lemma 4.5.
\[ \square \]

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, on taking \( \Gamma_n \)-coinvariant, we have
\[
(M_m)_{\Gamma_n} = \mathcal{X}/(M_n \mathcal{X}, B_{\infty,m}) \cong \mathcal{X}_{n,m}
\]
thanks to Lemma 2.2. As $X_{n,m}$ 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 $n \geq n_m$,

\begin{equation}
(5.1) \quad e_{n,m} - e_{n_m,m} = \mu_\Gamma(M_m) \times (p_n - p_{n_m}) + \lambda_\Gamma(M_m) \times (n - n_m) + e'_{n,m} - e'_{n_m,m},
\end{equation}

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 $\lambda_\Gamma(M_m)$, $\mu_\Gamma(M_m)$, and $e(M'_m)$ and $n_m$ vary in $m$.

### 5.1. Estimating Iwasawa invariants.

In this section, we assume that $X \in \mathcal{M}_H(G)$, where $\mathcal{M}_H(G)$ 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 $\tilde{X}$ for the quotient $X/X(p)$, which is finitely generated over $\Lambda(H)$ by our $\mathcal{M}_H(G)$-hypothesis. Let $\tau_X$ denote the $\Lambda(H)$-rank of $\tilde{X}$. We have the following short exact sequence

\begin{equation}
(5.2) \quad 0 \to X(p) \to X \to \tilde{X} \to 0.
\end{equation}

**Proposition 5.1.** We have

\[ \lambda_\Gamma(X_{H_m}) = \tau_X \times p^{(d-1)m} + O(1), \quad \mu_\Gamma(X_{H_m}) = \mu_G(X) \times p^m \]

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

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

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

$$
\text{rank}_{\mathbb{Z}_p} X_{H_m} = \text{rank}_{\mathbb{Z}_p} \tilde{X}_{H_m}.
$$

But the latter is equal to $\tau_X \times p^m + O(1)$ as given by [Har00] Theorem 1.10. This gives the formula for $\lambda_\Gamma(H_m)$.

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

$$
\mu_\Gamma(X_{H_m}) = \mu_\Gamma(X_{H_m}).
$$

Following [CK03] Lemma 5.2], we have the equation

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

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

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

Hence the result follows on combining the last three equations. \qed
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 $X$ 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 $m_0$, $x_\nu \in X$ and $k_\nu \in H \setminus H^p$ for each $\nu \in \Sigma \setminus \{p\}$ such that 
\[ B_{\infty,m} = I_{H,m}X + \sum_\nu \Phi_{m/m_0}(k_\nu)\Lambda(H) \cdot x_\nu \]
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 the equation 
\[ B_{\infty,m} = \Phi_{m/m_0}(h)B_{\infty,m_0}. \]

Since we are assuming that $X$ 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 a pseudo-isomorphism, $r = \text{rank}_{\Lambda(H)} B_{\infty,m_0}$ 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 $e(M_m) \leq e(B_{\infty,m_0}/B_{\infty,m}) + e(M_{m_0})$, which finishes the proof. \(\square\)

**Corollary 5.3.** If $\mu_\Gamma(M_0) = 0$, then 
\[ e_{n,n} = \tau_X \times np^n + O(p^n). \]

**Proof.** Under our assumption on $X$, Corollary A.4 tells us that there exists an integer $\rho$ such that the $\Lambda(\Gamma)$-characteristic ideal of $X_{H_m}$ factorises into polynomials whose degrees are bounded by $\rho$. The same can be said about $M_m$ given that it is a quotient of $X_{H_m}$. 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 $X$ is finitely generated over $\Lambda(H)$, then $\mu_G(X) = 0$. Hence, our result follows on combining (5.1) with Propositions 5.1 and 5.2. \(\square\)
In this section, we assume that $d = 2$ and $X \in M_H(G)$. Since $X$ is torsion over $M_H(G)$ in this setting, we have already seen in Corollary 2.12 that the asymptotic formula of Perbert can be improved to

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

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 $X \in M_H(G)$.

**Proposition 6.1.** Assume that $X \in M_H(G)$ and write $\tilde{X} = X/X(p)$. Then,

$$
e(X_{G,n,n}) \leq \mu_G(X) \times p^{2n} + \tau_X \times np^n + O(p^n),
$$

where $\tau_X = \text{rank}_{\Lambda(H)} \tilde{X}$.

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

$$
\cdots \to X(p)G_{n,n} \to X_{G,n,n} \to \tilde{X}_{G,n,n} \to 0.
$$

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

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

$$
\mu_{\Gamma}(\tilde{X}_{H,n}) = 0, \quad \lambda_{\Gamma}(\tilde{X}_{H,n}) = \tau_X \times p^n + O(1), \quad e(\tilde{X}_{H,n}) = O(p^n).
$$

Consequently, $e(\tilde{X}_{G,n,n}) = \tau_X \times np^n + O(p^n)$ by Theorem 4.1.

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

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

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 [DL16, Lemma 4.2] tells us that

$$
\# MG_{n,n} = \# NG_{n,n} \times p^{O(p^n)}
$$

under our assumptions. Therefore,

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

and hence

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

This finishes our proof.

**Corollary 6.2.** We have the upper bound

$$
\tilde{e}_{n,n} \leq \mu_G(X) \times p^{2n} + \tau_X \times np^n + O(p^n)
$$

**Proof.** First of all, we observe that $\tilde{e}_{n,n} \leq e(X_{G,n,n})/p^n$ thanks to the short exact sequence (5.2). Therefore, it is enough to bound $e(X_{G,n,n})/p^n$.

Since $X_{G,n,n}$ 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

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

In particular, this tells us that

\[
e((\mathcal{X}_{G,n})/p^n) = a_n \times n + e(T_n/p^n) \leq a_n \times n + e(T_n).
\]

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.

\[\square\]

**References**

[BH97] P. N. Balister and S. Howson, *Note on Nakayama’s lemma for compact \(\Lambda\)-modules*, Asian J. Math. 1 (1997), no. 2, 224–229.

[CFK+05] John Coates, Takako Fukaya, Kazuya Sujatha, and Otmart Venjakob, *The \(GL_2\) main conjecture for elliptic curves without complex multiplication*, Publ. Math. Inst. Hautes Études Sci. 101 (2005), 163–208.

[CH01] John Coates and Susan Howson, *Euler characteristics and elliptic curves. II*, J. Math. Soc. Japan 53 (2001), no. 1, 175–235.

[CK13] John Coates and Dohyeong Kim, *Introduction to the work of M. Kakde on the noncommutative main conjectures for totally real fields*, Noncommutative Iwasawa main conjectures over totally real fields, Springer Proc. Math. Stat., vol. 29, Springer, Heidelberg, 2013, pp. 1–22.

[CM81] Albert A. Cuoco and Paul Monsky, *Class numbers in \(\mathbb{Z}_d/p\)-extensions*, Math. Ann. 255 (1981), no. 2, 235–258.

[CS05] J. Coates and R. Sujatha, *Fine Selmer groups of elliptic curves over \(p\)-adic Lie extensions*, Math. Ann. 331 (2005), no. 4, 809–839.

[DL16] Daniel Delbourgo and Antonio Lei, *Estimating the growth in Mordell-Weil ranks and Shafarevich-Tate groups over Lie extensions*, to appear in Ramanujan J., 2016.

[FW79] Bruce Ferrero and Lawrence C. Washington, *The Iwasawa invariant \(\mu_p\) vanishes for abelian number fields*, Ann. of Math. (2) 109 (1979), no. 2, 377–395.

[Har00] Michael Harris, *Correction to: “\(p\)-adic representations arising from descent on abelian varieties”* [Compositio Math. 39 (1979), no. 2, 177–245], Compositio Math. 121 (2000), no. 1, 105–108.

[Iwa73a] Kenkichi Iwasawa, *On \(\mathbb{Z}_l\)-extensions of algebraic number fields*, Ann. of Math. (2) 98 (1973), 246–262.

[Iwa73b] ———, *On the \(\mu\)-invariants of \(\mathbb{Z}_l\)-extensions*, Number theory, algebraic geometry and commutative algebra, in honor of Yasuo Akizuki, Kinokuniya, Tokyo, 1973, pp. 1–11.

[Kak13] Mahesh Kakde, *The main conjecture of Iwasawa theory for totally real fields*, Invent. Math. 193 (2013), no. 3, 539–626.

[Kob03] Shin-ichi Kobayashi, *Iwasawa theory for elliptic curves at supersingular primes*, Invent. Math. 152 (2003), no. 1, 1–36.

[Lee13] Chern-Yang Lee, *Non-commutative Iwasawa theory of elliptic curves at primes of multiplicative reduction*, Math. Proc. Cambridge Philos. Soc. 154 (2013), no. 2, 303–324.

[MF16] Lim Meng Fai, *Fine Selmer groups of congruent Galois representations*, 2016, arXiv:1603.08640.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, second ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2008.

[OV02] Yoshihiro Ochi and Otmart Venjakob, *On the structure of Selmer groups over \(p\)-adic Lie extensions*, J. Algebraic Geom. 11 (2002), no. 3, 547–580.

[Per11] Guillaume Perbet, *Sur les invariants d’Iwasawa dans les extensions de Lie \(p\)-adiques*, Algebra Number Theory 5 (2011), no. 6, 819–848.

[RW11] Jürgen Ritter and Alfred Weiss, *On the “main conjecture” of equivariant Iwasawa theory*, J. Amer. Math. Soc. 24 (2011), no. 4, 1015–1050.

[Ser63] Jean-Pierre Serre, *Cohomologie galoisienne*, Cours au Collège de France, vol. 1962, Springer-Verlag, Berlin-Heidelberg-New York, 1962/1963.
[Ven02] Otmar Venjakob, *On the structure theory of the Iwasawa algebra of a p-adic Lie group*, J. Eur. Math. Soc. (JEMS) 4 (2002), no. 3, 271–311.

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

[Ven03b] _______, *On the Iwasawa theory of p-adic Lie extensions*, Compositio Math. 138 (2003), no. 1, 1–54.

[Viv04] Filippo Viviani, *Ramification groups and Artin conductors of radical extensions of Q*, J. Théor. Nombres Bordeaux 16 (2004), no. 3, 779–816.

[Was97] Lawrence C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, 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 address: antonio.lei@mat.ulaval.ca