Iwasawa theory over solvable three-dimensional p-adic Lie extensions

A thesis
submitted in partial fulfilment
of the requirements for the Degree
of
Doctor of Philosophy
at the
University of Waikato

by

Chao Qin

THE UNIVERSITY OF
WAIKATO
Te Whare Wānanga o Waikato

University of Waikato

2018

Abstract

Iwasawa theory is a powerful tool which describes the mysterious relationship between arithmetic objects (motives) and the special values of L-functions. A precise form of this relationship is neatly encoded in the so-called "Iwasawa Main Conjecture". Classically the Main Conjecture (as formulated by Iwasawa himself) involved the behaviour of ideal class groups over cyclotomic $\mathbb{Z}_p$-extensions, and related this to the Kubota-Leopoldt p-adic zeta-function. During the last two decades, the main conjecture has been greatly generalized to admissible p-adic Lie extensions, and provides a conjectural relationship between L-values of motives and their associated Selmer groups.

A key component of the "Non-commutative Iwasawa Main Conjecture" in [CFK$^+$05] predicts the existence of an analytic p-adic L-function $\mathcal{L}_M^{\mathrm{an}}$ inside $\mathrm{K}_1\big(\mathbb{Z}_p[\![\mathcal{G}_\infty]\!]_{\mathcal{S}^*}\big)$. To establish the existence of such an object, we need to be able to do two things: (1) describe $\mathrm{K}_1\big(\mathbb{Z}_p[\![\mathcal{G}_\infty]\!]_{\mathcal{S}^*}\big)$ in terms of the Artin representations factoring through $\mathcal{G}_\infty$ using p-adic congruences, and then (2) show for each motive that the abelian fragments satisfy these congruences.

This thesis provides a complete answer to the first task (1), in the specific situation where the pro-p-group $\mathcal{G}_\infty$ has dimension ≤ 3 and is torsion-free. We completely describe $\mathrm{K}_1(\mathbb{Z}_p[\![\mathcal{G}_\infty]\!])$ and its localisations by using an infinite family of p-adic congruences, where $\mathcal{G}_\infty$ is any solvable p-adic Lie group of dimension 3. This builds on earlier work of Kato when $\dim(\mathcal{G}_\infty) = 2$, and of Daniel Delbourgo and Lloyd Peters when $\mathcal{G}_\infty \cong \mathbb{Z}_p^\times \ltimes \mathbb{Z}_p^d$ with a scalar action of $\mathbb{Z}_p^\times$. The method exploits the classification of 3-dimensional p-adic Lie groups due to González-Sánchez and Klopsch, as well as the fundamental ideas of Kakde, Burns, etc. in non-commutative Iwasawa theory.

We also undertake a short study of elliptic curves over $\mathrm{GL}_2(\mathbb{F}_p)$-extensions, and compile some numerical evidence in support of the first layer congruences predicted by Kakde [Kak17] for non-CM curves.

Acknowledgements

First and foremost, I would like to express my sincere gratitude to my supervisor, Associate Professor Daniel Delbourgo, for endless amounts of time and energy which he has devoted to me over the last four years. It would not have been possible to finish this thesis without him. He has been a helpful mentor and a role model both academically and personally; what I learned from him will definitely benefit me for my whole life. I appreciate his patience and encouragement.

I am grateful to my co-supervisor, Dr Ian Hawthorn, for his friendly guidance and continuous encouragement during the hard times.

I would also like to thank the graduate students in the Department of Mathematics and Statistics at Waikato University, especially Hamish Gilmore, for numerous mathematical discussions and for being in the same boat with me. I would like to send, as well, a big thank you to Lloyd Peters for providing his MAGMA code.

I greatly appreciate the University of Waikato for providing me the Doctoral scholarship during the first three years of the PhD program.

Last, but not least, I am hugely indebted to my family for their love and support.

Contents

Chapter 1

Introduction

Over the last twenty years, the study of non-commutative Iwasawa theory for motives has progressed rapidly, due to the work of many mathematicians [Bur15, BV11, CFK$^+$05, Kak13, Kak17, Kat05, Kat06, RW06]. Fix an odd prime p, and an infinite algebraic extension F_∞/F of some number field F. We assume that $G_\infty = \mathrm{Gal}(F_\infty/F)$ is a p-adic Lie group with no element of order p; we further suppose that F_∞ contains the cyclotomic $\mathbb{Z}_p$-extension F^{cyc} of the base field F. Clearly if $H_\infty = \mathrm{Gal}\big(F_\infty/F^{\mathrm{cyc}}\big)$, then the quotient $\Gamma = G_\infty/H_\infty$ will be isomorphic to an open subgroup of $1 + p\mathbb{Z}_p$, under the p-th cyclotomic character 'κ_F'.

For a motive M with good ordinary reduction at p, the work of Coates et al [CFK$^+$05] associates (under the $\mathfrak{M}_H(G)$-conjecture) a characteristic element $\xi_M \in K_1\big(\mathbb{Z}_p[\![G_\infty]\!]_{\mathcal{S}^*}\big)$, where $K_1(-)$ denotes the first algebraic K-group, the subscript '${}_{\mathcal{S}^*}$' means the localisation at the set $\mathcal{S}^* = \bigcup_{n\geq 0} p^n\mathcal{S}$, and here $\mathcal{S}$ indicates the canonical choice of Ore set

$$\mathcal{S} := \left\{ f \in \mathbb{Z}_p[\![G_\infty]\!] \;\middle|\; \mathbb{Z}_p[\![G_\infty]\!]/\mathbb{Z}_p[\![G_\infty]\!]f \text{ is a finitely-generated } \mathbb{Z}_p[\![H_\infty]\!]\text{-module} \right\}.$$

The "Non-commutative Iwasawa Main Conjecture" predicts that there exists an element $\mathcal{L}_M^{\mathrm{an}} \in K_1\big(\mathbb{Z}_p[\![G_\infty]\!]_{\mathcal{S}^*}\big)$ of the exact form $\mathcal{L}_M^{\mathrm{an}} = \mathfrak{u} \cdot \xi_M$ with $\mathfrak{u}$ in the image of $K_1\big(\mathbb{Z}_p[\![G_\infty]\!]\big)$; for any Artin representation $\rho : G_\infty \to \mathrm{GL}(V)$, its evaluation at $\rho \otimes \kappa_F^k$ should then satisfy

$$\mathcal{L}_M^{\mathrm{an}}\big(\rho\kappa_F^k\big) \;=\; \text{the value of the } p\text{-adic } L\text{-function } \mathbf{L}_p(M, \rho, s) \text{ at } s = k,$$

as the variable k ranges over the p-adic integers. Note that the existence of $\mathbf{L}_p(M,\rho,s)$ is in most cases still conjectural, although its interpolation properties are easy to describe.

Remark: The strategy of Burns and Kato [Bur15, Kat06] reduces this conjecture to the following: (1) prove the abelian Iwasawa Main Conjectures for M over all finite layers; (2) describe $K_1\big(\mathbb{Z}_p[\![G_\infty]\!]_{\mathcal{S}^*}\big)$ via a system of non-commutative congruences; and (3) show that each of the abelian fragments, $\mathbf{L}_p(M,\rho,-)$, in combination satisfy this system of congruences.

There seem to be two approaches to (2), either using congruences modulo trace ideals [Bou10, Kak13, Kat06, Kim15, RW06], or instead by deriving p-adic congruences [DP15, DW08, DW10, Har10, Kak17, Kat05]. Naturally both approaches should be equivalent to one another.

To illustrate precisely what is meant by the terminology 'p-adic congruences' above, for the moment suppose that G_∞ is a two-dimensional p-adic Lie group of the form

$$G_\infty \;\cong\; \mathbb{Z}_p^\times \ltimes \mathbb{Z}_p \;\cong\; \big(\mathbb{F}_p^\times \times \Gamma\big) \ltimes \mathbb{Z}_p$$

where $\Gamma = 1 + p\mathbb{Z}_p$, and the first factor $\mathbb{Z}_p^\times$ acts on the second $\mathbb{Z}_p$ via scalar multiplication.

Let $\varphi : \mathbb{Z}_p[\![\Gamma]\!] \to \mathbb{Z}_p[\![\Gamma]\!]$, $\varphi : \gamma \mapsto \gamma^p$ denote the linear extension of the p-power map on Γ. At integers $m \geq m' \geq 0$, we also write $\mathcal{N}_{m',m} : \mathbb{Z}_p[\![\Gamma^{p^{m'}}]\!] \to \mathbb{Z}_p[\![\Gamma^{p^m}]\!]$ for the norm map.

Kato's Theorem. *([Kat05, 8.12]) A sequence $\big(\mathbf{y}_m\big) \in \prod_{m\geq 0} \mathbb{Z}_p\big[\big[\Gamma^{p^m}\big]\big]^\times_{(p)}$ arises from an element in $K_1\big(\mathbb{Z}_p[\![G_\infty]\!]_{\mathcal{S}}\big)$ only if the system of p-adic congruences*

$$\prod_{m'=1}^{m} \mathcal{N}_{m',m}\left(\frac{\mathbf{y}_{m'}}{\varphi\big(\mathbf{y}_{m'-1}\big)}\cdot\frac{\varphi\big(\mathcal{N}_{0,m'-1}\big(\mathbf{y}_0\big)\big)}{\mathcal{N}_{0,m'}\big(\mathbf{y}_0\big)}\right)^{p^{m'}} \equiv\; 1 \quad \mathrm{mod}\ p^{2m}\cdot\mathbb{Z}_p\big[\big[\Gamma^{p^m}\big]\big]_{(p)}$$

hold at every integer $m \geq 1$.

Kato has obtained similar congruences when G_∞ is replaced by any of the groups $\Gamma^{p^s} \ltimes \mathbb{Z}_p$. His work completely describes the two-dimensional situation, since any non-commutative torsion-free pro-p-group G with $\dim(G) = 2$ is isomorphic to $\Gamma^{p^s} \ltimes \mathbb{Z}_p$ for some $s \geq 0$.

Question. *Can the analogue of Kato's p-adic congruences be proven when* $\dim(G) > 2$*?*

Our goal here is to give a positive answer when $\dim(G) = 3$ and $G \ncong \mathrm{SL}_2(\mathbb{Z}_p)$, and $G \ncong \mathrm{SL}_1(\mathbb{D}_p)$ where $\mathbb{D}_p$ is a certain division algebra of rank four over $\mathbb{Z}_p$. We exclude the two insolvable cases as the representation theory is unpleasant, although recent work of Kakde [Kak17] provides hope that an answer for $\mathrm{GL}_2(\mathbb{Z}_p)$ is not too far away.

We shall also give some fragmentary numerical evidence supporting Mahesh Kakde's modulo p congruences in [Kak17], which are formulated for elliptic curves over $\mathrm{GL}_2(\mathbb{F}_p)$-extensions. These calculations are undertaken using MAGMA, but for efficiency reasons we considered only $p = 3$ in Chapter 8.

Chapter 2

Background

Iwasawa theory is a powerful tool to study the hidden secrets contained in zeta values. Almost 100 years after Dirichlet's celebrated class number formula, Iwasawa theory gave a new way to study the connection between analytic objects and arithmetic objects, by interpreting the class number formula in terms of Galois actions on towers of ideal class groups.

There has been much interest in the study of non-commutative Iwasawa theory over the last decade, in particular due to the GL_2-Main Conjecture formulated by Coates et al [CFK$^+$05]. Coates et al associated in *op. cit.* a characteristic element to a certain class of finitely generated $\Lambda(G)$-modules, where G is a p-torsion free p-adic Lie group. In this chapter, we will briefly recall the background material necessary to set up this Main Conjecture, in the context of elliptic curves.

2.1 The Birch and Swinnerton-Dyer Conjecture

We start this section by recalling some basic facts on elliptic curves; see Silverman's book for more details [Sil09].

Definition 2.1 *An elliptic curve E over a field K is a non-singular projective curve of genus one, equipped with a specified K-rational point.*

As a consequence of the Riemann-Roch theorem, the elliptic curve can be also described as a cubic Weierstrass equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with $a_i \in K$, where $O_E = [0, 1, 0]$ is the point at infinity. If the characteristic of K is different from 2, we can simplify the equation above by changing the coordinate $y \mapsto \frac{1}{2(y-a_1x-a_3)}$, which gives a new equation of the form

$$E: \;\; y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

where $b_2 = a_1^2 + 4a_4, b_4 = 2a_4 + a_1a_3$, and $b_6 = a_3^2 + 4a_6$. We define the quantities,

$$\begin{aligned}
b_8 &= a_1^2a_6 + 4a_2a_6 - a_2a_3^2 - a_4^2,\\
c_4 &= b_2^2 - 2b_4,\\
c_6 &= -b_2^3 + 36b_2b_4 - 216b_6,\\
\Delta &= b_2^2b_8 - 8b_4^3 + 9b_2b_4b_6,\\
j &= c_4^3/\Delta,\\
\omega &= dx/(2y + a_1x + a_3) = dy/(3x^2 + 2a_2x + a_4 - a_1y)
\end{aligned}$$

In particular, note that

$$4b_8 = b_2b_6 - b_4^2 \quad \text{and} \quad 1728\Delta = c_4^3 - c_6^2.$$

If the characteristic of K is different from 2 and 3, again we change the coordinate via $(x, y) \mapsto (x - 3b_2/36, y/108)$, thus providing the short Weierstrass form

$$y^2 = x^3 + Ax + B$$

where $A = 27c_4, B = -54c_6$ and $\Delta = -16(4A^3 + 27B^2)$.

Remark: Note that Δ[1] is called the discriminant of E over K, which is an important invariant of the Weierstrass form. Since E is non-singular, thus $\Delta \neq 0$ and $x^3 + Ax + B$ has three distinct roots. The quantity j defined above

[1] Clearly Δ depends on the choice of Weierstrass model $E: \;\; y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$.

is called the j-invariant of the elliptic curve, and ω is called the invariant differential associated to the Weierstrass equation.

A natural question to ask about elliptic curves is, given two points on the elliptic curve, is there a way to produce a third point? The answer is positive, since an elliptic curve has a group structure.

Define $E(K)$ to be the set of points on the elliptic curve E

$$E(K) = \{P = (x, y) \in K \times K : y^2 = x^3 + Ax + B\} \cup \{O_E\}$$

where O_E is the point of infinity. The set $E(K)$ forms an abelian group, with the following properties:

1. O_E is the identity element

2. If $P, Q \in E(K)$ and $P \neq O_E, Q \neq O_E$, and $R = (x, y)$ is the intersection between the elliptic curve and the line passing through P and Q, then the point $P + Q = (x, -y) \in E(K)$

3. If $P = (x, y) \in E(K), P \neq O_E$ then the inverse of P is $(x, -y.)$

From now, we assume K is a number field (i.e. a finite extension of $\mathbb{Q}$). The first deep result concerning the group $E(K)$ is the Mordell-Weil Theorem, which appeared in 1922.

Theorem 2.1 *(Mordell-Weil) The abelian group $E(K)$ is finitely generated.*

It follows that there is an isomorphism

$$E(K) \cong \mathbb{Z}^{r_K} \oplus T_K$$

where $r_K = \text{rank}_{\mathbb{Z}}(E(K))$ is called the rank of E, and $T_K = E(K)_{tor}$ is a finite abelian group (the torsion group of E).

For a non-archimedean prime v of K, let k_v denote the residue field at v. We say that E has good reduction at v if v does not divide the discriminant $\Delta = -16(4A^3 + 27B^2)$. For each finite place v, we write $\tilde{E}$ for the reduction of E at v (which may or may not be a non-singular curve over k_v), and then define

$$a_v(E) := q_v + 1 - \#\tilde{E}(k_v)$$

where q_v is the size of the finite field k_v.

Definition 2.2 *The local L-factor of the Hasse-Weil L-function of E at v is the polynomial defined by*

$$L_v(E/K,X) = \begin{cases} 1 - a_v(E)X + q_vX^2 & \textit{if } E \textit{ has good reduction at } v \\ 1 - X & \textit{if } E \textit{ is split multiplicative at } v \\ 1 + X & \textit{if } E \textit{ is non-multiplicative at } v \\ 1 & \textit{if } E \textit{ has additive reduction at } v. \end{cases}$$

The Hasse-Weil L-function of E over K has the Euler product form

$$L(E/K,s) = \prod_v L_v(E/K, q_v^{-s})^{-1} \qquad \text{for } Re(s) \gg 0$$

where the product varies over all non-archimedean primes of K. By Hasse's theorem, if v is a prime of E/K of good reduction and

$$1 - a_v(E)X + q_vX^2 = (1 - \alpha X)(1 - \beta X)$$

then $|\alpha| = |\beta| = \sqrt{q_v}$, and $a_v(E) \leq 2|\sqrt{q_v}|$. Furthermore, this result implies that the Euler product converges in the right half plane $Re(s) \geq 3/2$.

The L-series $L(E/K,s)$ satisfies a functional equation relating the value at s with its value at $2-s$. More precisely, define the completed L-series as

$$\Lambda(E/K,s) = L(E/K,s)L_\infty(E/K,s),$$

where $L_\infty(E/K,s) = N^{s/2}((2\pi)^{-s}\Gamma(s))^{[K:\mathbb{Q}]}$, with N being the conductor of E over K. Then

$$\Lambda(E/K,s) = \omega_{E/K}\Lambda(E/K,2-s), \text{ with } \omega_{E/K} = \pm 1.$$

The L-series of E can also be defined in terms of the torsion points on E, which is quite important when defining the Selmer group of E, and also in the proof of Mordell-Weil theorem. Let l be a rational prime, and define

$$T_l(E) = \lim_{\leftarrow} E_{l^n}, \qquad V_l(E) = T_l(E) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l, \qquad H_l^1(E) = \mathrm{Hom}(V_l(E), \mathbb{Q}_l)$$

where the inverse limit is taken with respect to multiplication by l. Here $T_l(E)$ is called the l-adic Tate module, and $V_l(E)$ denotes the l-adic Galois representation of E.

The trace of the Frobenius morphism is equal to the coefficient $a_v(E)$ we defined above. It follows that the factor at v could be also written as

$$det\Big(1 - Frob_v^{-1} X | H_l^1(E)^{I_v}\Big)\Big|_{X=q_v^{-s}}$$

whence

$$L(E/K, s) = \prod_v det\Big(1 - Frob_v^{-1} X | H_l^1(E)^{I_v}\Big)^{-1}\Big|_{X=q_v^{-s}}.$$

This description is quite useful when we define p-adic L-functions later on.

For a field K, we write $\mathcal{M}_K$ for the set of places of K, and K_v denotes the completion of K at a place v; let us define

$$G_K := Gal(\bar{K}/K) \quad \text{and} \quad G_{K_v} := Gal(\bar{K}_v/K_v).$$

Note that both of G_K and G_{K_v} are equipped with the profinite topology, and G_{K_v} can be realised as a subgroup of G_K.

Now consider the Galois module

$$E_m := \{P \in E(\bar{K}) : mP = O_E\},$$

equipped with the discrete topology. There is an exact sequence of discrete G_K-modules

$$0 \to E_m \to E(\bar{K}) \xrightarrow{[m]} E(\bar{K}) \to 0$$

where $[m]$ denotes the morphism of multiplication by m on E. This induces a short exact sequence in G_K-cohomology

$$0 \to E(K)/mE(K) \xrightarrow{\delta} H^1(G_K, E_m) \to H^1(G_K, E(\bar{K}))_m \to 0,$$

where $H^1(G_K, E(\bar{K}))_m$ is the m-torsion in $H^1(G_K, E(\bar{K}))$, and δ indicates the coboundary map.

Definition 2.3 *1. The m-Selmer group of E/K is given by*

$$Sel_m(E/K) = ker\Big(H^1(G_K, E_m) \mapsto \prod_v H^1(G_{K_v}, E(\bar{K_v}))_m\Big)$$

where the product is over all places of K.

2. The Shafarevich-Tate group of E/K equals

$$Ш(E/K) := ker\big(H^1(G_K, E(\bar{K})) \mapsto \prod_v H^1(G_{K_v}, E(\bar{K_v}))\big).$$

Hence, one obtains the short exact descent sequence

$$0 \rightarrow E(K)/mE(K) \rightarrow Sel_m(E/K) \rightarrow Ш(E/K)_m \rightarrow 0.$$

We now introduce various terms appearing the BSD conjecture. First a height function is defined on affine points $P = (x, y)$ in $E(K)$, with $x = r/s$ such that $(r, s) = 1$, by setting

$$h(P) = log(\max\{|r|, |s|\}).$$

Also note that $h(O_E) = 0$. Now, we exploit the naive height function to produce a truly quadratic function, the so-called Néron-Tate height, by the formula

$$\hat{h}_{NT}(P) = \frac{1}{2}\lim_{n\to\infty} 4^{-n}h(2^nP).$$

The Néron-Tate height plays an important role in the statement of Birch and Swinnerton-Dyer conjecture, and it satisfies the following properties:

1. $2\hat{h}_{NT}(P) = h(P) + O(1)$;

2. $\hat{h}_{NT}(P) \geq 0$ for all P;

3. $\hat{h}_{NT}(P) = 0$ if and only if P is a torsion point;

4. $\hat{h}_{NT}(mP) = m^2\hat{h}_{NT}(P)$.

One constructs the bilinear Néron-Tate non-degenerate pairing

$$\langle\ ,\ \rangle_{NT} : E(K)/E(K)_{tors} \times E(K)/E(K)_{tors} \mapsto \mathbb{R},$$

via the formula $\langle P, Q\rangle_{NT} = \hat{h}_{NT}(P + Q) - \hat{h}_{NT}(P) - \hat{h}_{NT}(Q)$.

Definition 2.4 *With $\{P_1, \cdots, P_r\}$ a $\mathbb{Z}$-basis for $E(K)/E(K)_{tor}$, the regulator $Reg(E/K)$ of E is the discriminant of the Néron-Tate pairing, ie.*

$$Reg(E/K) := det(\langle P_i, P_j \rangle_{NT}).$$

If the elliptic curve E has the Weierstrass form

$$E: \; y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

then the archimedean period of E over K is the non-zero complex number

$$\Omega_{E/K} := \prod_{i=1}^{s} \int_{E(\mathbb{R})} |\omega^{\sigma_i}| \times \prod_{j=1}^{t} 2 \int_{E(\mathbb{C})} \omega^{\tau_j} \wedge \bar{\omega^{\tau_j}}$$

where $\omega = dx/(2y + a_1x + a_3)$ is the Néron differential associated to a global minimal Weierstrass equation, and σ_i and τ_j range over the real/complex embeddings of K.

Definition 2.5 *For each place v of K, the Tamagawa number at v is defined to be*

$$c_v := \#(E(K_v)/E_0(K_v))$$

where $E_0(K_v)$ is the subgroup of $E(K_v)$ which consists of points which reduce to non-singular points at v. Thus $c_v(E) = 1$ if $v \not| N$.

Conjecture 2.2 *(Birch, Swinnerton-Dyer) For a number field K and an elliptic curve E over K,*

1. *$ord_{s=1}L(E/K, s) = r_K(E)$;*

2. *the Shafarevich-Tate group $Ш(E/K)$ is finite;*

3. *the following equality holds*
$$\lim_{s \to 1} \frac{L(E/K, s)}{(s-1)^{r_K(E)}} = \frac{\Omega_{E/K} \times Reg(E/K) \times \#Ш(E/K) \prod_v c_v}{(\#E(K)_{tor})^2} \times \sqrt{disc_K}$$

Some special cases of the BSD conjectures have been proven, due to the work of Coates-Wiles, Gross-Zagier, Kolyvagin, Rubin, and many others.

Theorem 2.3 *(Coates-Wiles)[CW77] If E is an elliptic curve defined over a quadratic imaginary extension K over $\mathbb{Q}$, and if E has complex multiplication by K with $L(E/K, s)$ is non-zero at 1, then $E(K)$ is finite.*

Theorem 2.4 *(Kolyvagin,Gross-Zagier)[KL89, Kol07, GZ86] Let $K = \mathbb{Q}$. Then*

1. *If $L(E/\mathbb{Q}) \neq 0$, then both $E(\mathbb{Q})$ and $\text{Ш}(E/\mathbb{Q})$ are finite.*
2. *If $order_{s=1}L(E/\mathbb{Q}, s) = 1$, then $\text{Ш}(E/\mathbb{Q})$ is finite and $E(\mathbb{Q})$ has rank one.*

2.2 Iwasawa theory over $\mathbb{Z}_p$-extensions

The class number formula, obtained by Dirichlet and Dedekind, was considered as the first example of a deep interplay between zeta functions and ideal class groups. In fact Iwasawa theory, which was developed in the middle of 20th century, is actually an upgraded version of Dirichlet's class number formula!

Iwasawa constructed the p-adic zeta function as an element of the Iwasawa algebra, and thereby formulated the classical Iwasawa Main Conjecture, which was then proven by Mazur and Wiles twenty years later. Over the last thirty years, versions of the Iwasawa Main Conjecture have been formulated for arbitrary motives over $\mathbb{Q}$. In this section, we will introduce the Iwasawa theory of both Tate motives and elliptic curves, over $\mathbb{Z}_p$-extensions at least.

Historically, the p-adic L-function was first constructed by Kubota and Leopoldt in the 1950's by interpolating the Riemann zeta function $\zeta(s)$ p-adically. Recall that a multiplicative homomorphism $\chi : (\mathbb{Z}/M\mathbb{Z})^\times \mapsto \mathbb{C}^\times$ is called a Dirichlet character modulo M. Then the χ-twisted L-function attached to χ is given by

$$L(s, \chi) = \sum_{n=1}^{\infty} \chi(n)n^{-s}, \quad Re(s) > 1.$$

Recall also the Bernoulli numbers are defined by the Taylor series expansion

$$\frac{t}{e^t - 1} = \sum_{m=0}^{\infty} B_m \frac{t^m}{m!},$$

and the generalized Bernoulli numbers by

$$\sum_{j=1}^{M} \frac{\chi(j)te^{jt}}{e^{nt} - 1} = \sum_{m=0}^{\infty} B_{m,\chi} \frac{t^m}{m!}.$$

The generalized Bernoulli numbers are related to the special values of χ-twisted L-functions, as follows. For every integer $m \geq 1$, we have

$$L(1-m, \chi) = -\frac{B_{m,\chi}}{m}.$$

Upon interpolating these values through a fixed embedding $\iota : \bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_p$, Kubota and Leopoldt then obtained:

Theorem 2.5 *([Was97] Theorem 5.11) Let χ be a Dirichlet character. There exists a p-adic meromorphic function (analytic if $\chi \neq 1$) $\mathcal{L}_p(s, \chi)$ defined on $\{s \in \mathbb{C}_p : |s| < p^{1-\frac{1}{p-1}}\}$ such that*

$$\mathcal{L}_p(1-n, \chi) = -(1 - \chi\omega^{-n}(p)p^{n-1})\frac{B_{n,\chi\omega^{-n}}}{n}, \quad \textit{for all } n \geq 1.$$

In particular, for every $n \geq 1$ we therefore have

$$\mathcal{L}_p(1-n, \chi) = (1 - \chi\omega^{-n}(p)p^{n-1})L(1-n, \chi\omega^{-n}),$$

where $\omega : \mathbb{F}_p^\times \mapsto \mu_{p-1}$ is the Teichmüller character mod p, and $\chi\omega^{-n}$ means the associated primitive character. Iwasawa showed that such a p-adic L-function belongs to an Iwasawa algebra, and he formulated his main conjecture in this setting.

Definition 2.6 *1. A Galois extension F_∞ of F is called a $\mathbb{Z}_p$-extension if $Gal(F_\infty/F) \cong \mathbb{Z}_p$.*

2. If $\Gamma = Gal(F_\infty/F) \cong \mathbb{Z}_p$, then the Iwasawa algebra $\Lambda(\Gamma) = \mathbb{Z}_p[[\Gamma]]$ is defined to be the inverse limit $\varprojlim_m \mathbb{Z}_p\left[\Gamma/\Gamma^{p^m}\right]$.

As an example, consider $G_\infty = Gal(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$, where $\mathbb{Q}(\zeta_{p^\infty}) = \cup_{n\geq 1}\mathbb{Q}(\zeta_{p^n})$. Then $\Lambda(G_\infty) = \mathbb{Z}_p[[G_\infty]]$, which is isomorphic to $p-1$ copies of $\mathbb{Z}_p[[T]]$, the ring of formal power series over $\mathbb{Z}_p$. Let us henceforth abbreviate $\Lambda(\Gamma)$ just by Λ.

Proposition 2.6 *Let X be a finitely generated Λ-module. Then there exists $e, s, t, n_j, m_i \in \mathbb{Z}$, and irreducible distinguished polynomials $f_j(T) \in \mathbb{Z}_p[T]$, such that*

$$X \sim \Lambda^r \oplus \Big(\bigoplus_{i=1}^{s} \Lambda/p^{m_i}\Lambda\Big) \oplus \Big(\bigoplus_{j=1}^{t} \Lambda/f_j^{\,n_j}\Lambda\Big)$$

where $\sim$ means a pseudo-isomorphism of Λ-modules.

A proof of this proposition can be found in Washington's book [Was97].

The rank of X is just written as $rank_\Lambda(X) = r$. The μ-invariant equals $\mu(X) = \sum_{i=1}^{s} m_i$, and the λ-invariant is given by $\lambda(X) = \sum_{j=1}^{t} n_j \cdot deg(f_j)$. Lastly, the characteristic power series of X is defined to be

$$Char_\Lambda(X) = p^{\mu(X)} \cdot \prod_{j=1}^{t} f_j^{n_j},$$

which is well-defined up to an element of $\Lambda^\times$, of course.

Main Conjecture If $\mathcal{X} = Hom_{cont}(Gal(M_\infty/\mathbb{Q}(\zeta_{p^\infty})), \mathbb{Q}_p/\mathbb{Z}_p)$, where M_∞ is the maximal abelian pro-p-extension of $\mathbb{Q}(\zeta_{p^\infty})$ unramified outside p, then the characteristic power series of the ω^i-eigenspace for $\mathcal{X}$, i.e.

$$\mathcal{X}^{(\omega^i)} \;=\; \frac{1}{p-1} \sum_{\sigma \in Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})} \omega^{-i}(\sigma) \cdot \mathcal{X}\big|\sigma,$$

equals the p-adic zeta-function $\mathcal{L}_p(\omega^{1-i})$ for each i, up to an element of $\Lambda^\times$. This conjecture was proved by Mazur and Wiles in 1984 [MW84]. Wiles then extended the proof to totally real fields in 1990 [Wil90]. Around the same time, Rubin gave an easier proof by using the properties of Euler systems [Rub91].

We now switch to studying elliptic curves; indeed the BSD conjecture can be considered as an elliptic curve version of Dirichlet's class number formula. In the early 1970s, Mazur studied the Iwasawa theory of these curves over cyclotomic $\mathbb{Z}_p$-extensions, and formulated an Iwasawa main conjecture for elliptic curves over $\mathbb{Q}$.

Let E be an elliptic curve over $\mathbb{Q}$. For the number field $\mathbb{Q}(\zeta_{p^n})$, we have the following exact sequence

$$0 \to E(\mathbb{Q}(\zeta_{p^n})) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to Sel_{p^\infty}(E/\mathbb{Q}(\zeta_{p^n})) \to \text{Ш}_{p^\infty}(E/\mathbb{Q}(\zeta_{p^n})) \to 0,$$

where $Sel_{p^\infty}(E/\mathbb{Q}(\zeta_{p^n})) = \varinjlim_m Sel_{p^m}(E/\mathbb{Q}(\zeta_{p^n}))$.

Definition 2.7 *The Pontrjagin dual of the Selmer group over* $\mathbb{Q}(\zeta_{p^\infty})$ *is denoted by*

$$X_E = Hom(Sel_{p^\infty}(E/\mathbb{Q}(\zeta_{p^\infty})), \mathbb{Q}_p/\mathbb{Z}_p)$$

where $Sel_{p^\infty}(E/\mathbb{Q}(\zeta_{p^\infty})) = \varinjlim_n Sel_{p^\infty}(E/\mathbb{Q}(\zeta_{p^n}))$.

Here X_E naturally has the structure of a finitely generated $\Lambda(G_\infty)$-module. Mazur conjectured it to be a torsion $\Lambda(G_\infty)$-module, and this was subsequently proven by Kato [K$^+$05].

In order to formulate a p-adic version of the BSD conjecture, Mazur, Tate and Teitelbaum considered a p-adic analogue of the Hasse-Weil function $L(E,s)$ in [MTT86]. We briefly describe their construction, for the newform f_E of weight two associated to E. Let r be any rational number. Then one defines

$$\lambda^+(r) = -\pi i \cdot (\int_r^{i\infty} f_E(\tau) d\tau + \int_{-r}^{i\infty} f_E(\tau) d\tau) \quad \in \mathbb{R}.$$

For all $r \in \mathbb{Q}$, the modular symbol $[r]^+$ is given by

$$[r]^+ = \frac{\lambda^+(r)}{\Omega_E},$$

where Ω_E is a Néron period for E over $\mathbb{Z}$.

Let p be a prime of good ordinary reduction for E, and let a_p be the trace of Frobenius, so that $N_p = p + 1 - a_p$ is the number of points in $\tilde{E}(\mathbb{F}_p)$. Write $X^2 - a_p X + p$ for the characteristic polynomial of Frobenius, and α will denote a root such that $ord_p(\alpha) \leq \frac{1}{2}$. To construct the p-adic L-function as in [MTT86], we define a measure μ_α on $\mathbb{Z}_p^\times$ by

$$\mu_\alpha(a + p^k \mathbb{Z}_p) = \frac{1}{\alpha^k} \cdot [\frac{a}{p^k}]^+ - \frac{1}{\alpha^{k+1}} \cdot [\frac{1}{p^{k-1}}]^+$$

for any $k \geq 1$ and $a \in \mathbb{Z}_p^\times$.

Definition 2.8 *The analytic p-adic L-function is given by the Mazur-Mellin transform*

$$L_\alpha(E,s) = \int_{\mathbb{Z}_p^\times} \langle x \rangle^{s-1} d\mu_\alpha(x) \quad \textit{for all } s \in \mathbb{Z}_p,$$

where $\langle x\rangle^{s-1} = exp_p\big((s-1)\cdot log_p(\langle x\rangle)\big)$, and exp_p and log_p are the p-adic exponential and logarithm, and $\langle - \rangle : \mathbb{Z}_p^\times \twoheadrightarrow 1+p\mathbb{Z}_p$.

If $G_\infty = Gal(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ again, then $\kappa : G_\infty \mapsto \mathbb{Z}_p^\times$ denotes the p^{th}-cyclotomic character. We can choose a topological generator γ in $\Gamma = G_\infty^{p-1}$, so that $\kappa(\gamma)$ will be a generator of $1+p\mathbb{Z}_p$. Now, we can convert the function $L_\alpha(E,s)$ into a p-adic power series as follows.

Definition 2.9 *We define $\mathcal{L}_\alpha(E,T)$ in $\mathbb{Q}_p(\alpha)[[T]]$ to be the power series*

$$\mathcal{L}_\alpha(E,T) = \int_{\mathbb{Z}_p^\times} (1+T)^{\frac{log_p(\langle x\rangle)}{log_p(\kappa(\gamma))}} d\mu_\alpha(x).$$

Since p is a prime of good reduction, we shall denote the p-adic multiplier by

$$\epsilon_p = (1-\frac{1}{\alpha})^2.$$

Note the p-adic L-function 2.9 can be seen to p-adically interpolate the complex L-function. For example,

$$\mathcal{L}_\alpha(E,0) = \int_{\mathbb{Z}_p^\times} d\mu_\alpha = \epsilon_p \cdot \frac{L(E,1)}{\Omega_E}.$$

In general, if $\chi \neq 1$ is a character on Γ sending γ to ζ_{p^n}, then

$$\mathcal{L}_\alpha(E,\zeta-1) = \frac{1}{\alpha^{n+1}}\cdot\frac{p^{n+1}}{G(\chi^{-1})}\cdot\frac{L(E,\chi,1)}{\Omega_E^{sign(\chi)}},$$

where $G(\chi^{-1})$ is the Gauss sum, and $L(E,\chi^{-1},1)$ is the Hasse-Weil L-function of E twisted by χ^{-1}.

If we further assume that the elliptic curve has good ordinary reduction at p, then in fact

$$\mathcal{L}_\alpha(E,T) \in \mathbb{Z}_p[[T]][\frac{1}{p}].$$

Mazur's version of the Main Conjecture predicts the following:

Conjecture 2.7 *If E has good ordinary reduction at p, then the p-adic L-function $\mathcal{L}_\alpha(E,T)$ is a generator for the characteristic ideal $Char_\Lambda(X^{\omega^0})$, i.e. there exists an element $u(T)\in\Lambda^\times$ such that $\mathcal{L}_\alpha(E,T) = u(T)\times Char_\Lambda(X^{\omega^0})$.*

This conjecture has now been proved in many cases, thanks to the work of Kato, Rubin, Greenberg and Skinner-Urban [K$^+$05, Rub91, Gre94, SU14].

2.3 Algebraic K-theory

In this section, we introduce the formal definition of the Grothendieck group K_0, and of the Whitehead group K_1.

Definition 2.10 *For a ring R with identity element 1_R, the* **Grothendieck group** *$K_0(R)$ is the free abelian group generated by the isomorphism classes $[P]$ of finitely generated projective left R-modules P, modulo the subgroup generated by the classes*

$$[P] + [Q] - [P \oplus Q].$$

Note that two isomorphism classes $[P]$ and $[Q]$ are equal in $K_0(R)$, if and only if P and Q are stably isomorphic, namely $P \oplus R^n \cong Q \oplus R^n$ for some $n \in \mathbb{N}$.

Recall that a nonzero R-submodule I of $Quot(R)$ is called a **fractional ideal** of R if there exists some non-zero $a \in R$ with $aI \lhd R$. A ring R is a **Dedekind domain** if the fractional ideals form a group under multiplication.

Example 2.8 1. *If R is a local ring or PID, then $K_0(R) = \mathbb{Z}$.*

2. *If R is a Dedekind domain, then there is a natural isomorphism*

$$K_0(R) \cong \mathbb{Z} \oplus Cl(R),$$

where $Cl(R)$ is the class group of R.

Let R be a ring, and $I \subset R$ a two-sided ideal. The **double of R along I** is the subring of the Cartesian product $R \times R$ given by

$$D(R, I) := \{(x, y) \in R \times R : x - y \in I\}.$$

If p_1 denotes the projection onto the first coordinate, then there is a short exact sequence

$$0 \to I \to D(R, I) \xrightarrow{p_1} R \to 0,$$

where I embeds into $D(R, I)$ via the map $x \mapsto (0, x)$.

Definition 2.11 *The* **relative K_0 group** *of a ring R and an ideal I is defined to be*

$$K_0(R,I) := ker\big((p_1)_*:\ K_0(D(R,I)) \to K_0(R)\big).$$

Again let R be a ring and $I \subset R$ an ideal. Then there exists a short exact sequence

$$K_0(R,I) \to K_0(R) \xrightarrow{q_*} K_0(R/I),$$

where q_* is induced by the quotient map $q : R \to R/I$, and the map $K_0(R,I) \to K_0(R)$ is induced by p_1. The idea behind relative K-theory is to lift a matrix over R/I to a matrix over R, in the situation where R is not necessarily commutative.

Lemma 2.9 *If $A \in GL_n(R/I)$, then the $2n \times 2n$ matrix $\begin{pmatrix} A & 0 \\ 0 & A^{-1} \end{pmatrix}$ lifts to a matrix in $GL_{2n}(R)$*

Proof. First note that

$$\begin{pmatrix} A & 0 \\ 0 & A^{-1} \end{pmatrix} = \begin{pmatrix} I_n & A \\ 0 & I_n \end{pmatrix} \begin{pmatrix} I_n & 0 \\ -A^{-1} & I_n \end{pmatrix} \begin{pmatrix} I_n & A \\ 0 & I_n \end{pmatrix} \begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix}.$$

Clearly the matrix $\begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix}$ lifts to an invertible matrix over R. Let B and C be any two matrices in $M_n(R)$ lifting A and A^{-1} respectively. Then

$$\begin{pmatrix} I_n & B \\ 0 & I_n \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} I_n & 0 \\ -C & I_n \end{pmatrix}$$

are both invertible, and lift

$$\begin{pmatrix} I_n & A \\ 0 & I_n \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} I_n & 0 \\ -A^{-1} & I_n \end{pmatrix} \quad \text{respectively.}$$

Then the result follows after taking the product of these lifts. □

For $M \in GL_n(R)$, we define an injection

$$\begin{aligned}\iota : GL_n(R) &\mapsto GL_{n+1}(R)\\ M &\mapsto \begin{pmatrix} M & 0 \\ 0 & 1 \end{pmatrix}\end{aligned}$$

and call $GL(R) := \varinjlim_n GL_n(R)$ the **înfinite general linear group**.

Definition 2.12 *The abelian group $K_1(R)$ is defined as the abelianization of the infinite general linear group $GL(R)$, namely*

$$K_1(R) = \frac{GL(R)}{\big[GL(R), GL(R)\big]}.$$

Let $E_n(R)$ be the subgroup of $GL_n(R)$ which is generated by all elementary matrices

$$E_{ij}(a) = I_n + ae_{ij},$$

where $1 \leq i \neq j \leq n$, $a \in R$, and e_{ij} denotes the standard matrix with a 1 on the i^{th}-row and j^{th}-column and 0 everywhere else.

If $E(R) = \varinjlim_n E_n(R)$, then one can show that

$$E(R) = \big[GL(R), GL(R)\big]$$

and therefore as a corollary,

$$K_1(R) = GL(R)/E(R).$$

Now, whenever the ring R is commutative, taking the determinant yields a group homomorphism from $GL(R)$ onto the abelian group $R^\times$, and so induces a surjective map

$$det : K_1(R) \mapsto R^\times.$$

The kernel of the map is defined to be the abelian subgroup $SK_1(R)$.

Example 2.10 *1. Let R be a commutative ring. Then*

$$K_1(R) \cong R^\times \oplus (SL(R)/E(R)) \cong R^\times \oplus SK_1(R).$$

2. If $R = \mathcal{K}$ is a field or a division ring, then

$$K_1(\mathcal{K}) \cong \mathcal{K}^\times.$$

3. If $R = R_1 \times R_2$, then $K_1(R) = K_1(R_1) \oplus K_1(R_2)$.

Note that if $R = \mathbb{Z}$, then $SL(\mathbb{Z}) = E(\mathbb{Z})$, so we have $K_1(\mathbb{Z}) \cong \mathbb{Z}^\times = \{-1, 1\}$. Similarly $K_1(\mathbb{Z}[i]) \cong \{1, -1, i, -i\}$ and $K_1(\mathbb{Z}[\frac{-1+\sqrt{3}i}{2}]) \cong \mu_6$.

There is also a homological interpretation of $K_1(R)$ given by

$$K_1(R) = H_1(GL(R), \mathbb{Z}),$$

where the right hand side denotes the first homology group of $GL(R)$ with integer coefficients. Just as we did with K_0, we want to relate K_1 of the quotient ring R/I to $K_1(R)$.

Definition 2.13 *Let R be a ring with unit, and let I be a two-sided ideal in R. The* **relative K_1 group** *of a ring R and an ideal I is defined by*

$$K_1(R, I) := ker\big((p_1)_* : \ K_1(D(R, I)) \to K_1(R)\big).$$

We define $GL(R, I)$ to be the kernel of the map $GL(R) \mapsto GL(R/I)$ induced by the quotient map $R \mapsto R/I$. We also denote by $E(R, I)$ the smallest normal subgroup of $E(R)$ containing the elementary matrices $E_{ij}(a)$, for all $a \in I$.

Clearly as each such elementary matrix is congruent to the identity matrix modulo I, thus $E(R, I) \subset GL(R, I)$.

Remark: The subgroup $E(R, I)$ is normal in $GL(R, I)$, and

$$GL(R, I)/E(R, I) \cong K_1(R, I),$$

In fact, $GL(R, I)/E(R, I)$ is the center of $GL(R)/E(R, I)$, and furthermore, $E(R, I) = [E(R), E(R, I)] = [GL(R), E(R, I)]$ (see [Ros95, Theorem 2.5.3]).

Theorem 2.11 *Let R be a ring and $I \subset R$ an ideal. Then there exists a long exact sequence*

$$K_1(R, I) \to K_1(R) \xrightarrow{q_*} K_1(R/I) \xrightarrow{\partial} K_0(R, I) \to K_0(R) \xrightarrow{q_*} K_0(R/I),$$

where q_* is induced by the quotient map $q : R \to R/I$, and the maps $K_j(R, I) \to K_j(R)$ are induced by p_1.

2.4 Iwasawa algebras of p-adic Lie groups

Iwasawa algebras are completed group algebras of compact p-adic Lie groups, so we will introduce the latter first. (We already met them in Section 2.2 in the special case $G \cong \mathbb{Z}_p$.)

Definition 2.14 *(i) A* **profinite group** *is a compact Hausdorff topological group G whose open subgroups form a base for the open neighbourhoods of the identity.*
(ii) The group G is said to be topologically finitely generated if $G = \overline{\langle X \rangle}$ for some finite subset X of G. Here X is said to be a topological generating set for G, and $d(G)$ will denote the minimal cardinality of such an X.

A **pro-p group** is a profinite group whose open subgroups each have index equal to some power of p.

Definition 2.15 *Let G be a pro-p group. Define the subgroups*

$$P_1(G) = G_1 = G \text{ and } P_{i+1}(G) = G_{i+1} = \overline{P_i(G)^p[P_i(G), G]}, \text{ for } i \geq 1.$$

The decreasing chain of subgroups $G = P_1(G) \geq P_2(G) \geq \cdots \geq P_k(G) \geq \cdots$ is called the lower p-series of G. Furthermore,

1. *G is* **powerful** *if p is odd and $G/\overline{G^p}$ is abelian, or if $p = 2$ and $G/\overline{G^4}$ is abelian.*

2. *G is* **uniform** *if G is powerful, finitely generated and $[G : P_2(G)] = [P_i(G) : P_{i+1}(G)]$ for all $i \geq 1$.*

Recall from [DDSMS03] that a topological group G is a **compact p-adic Lie group**, if and only if G contains a normal open uniformly powerful pro-p-subgroup of finite index. If G is a compact p-adic Lie group, then its Iwasawa algebra is given by the inverse limit

$$\Lambda(G) = \mathbb{Z}_p\big[[G]\big] := \varprojlim_U \mathbb{Z}_p\big[G/U\big]$$

where U runs over all open normal subgroups of G.

Lastly, let T be a multiplicative closed subset consisting of nonzero divisors in $\Lambda(G)$, such that for each $s \in T$ and $a \in \Lambda(G)$ there exist $t_1, t_2 \in T$ and $b_1, b_2 \in \Lambda(G)$ satisfying

$$sb_1 = at_1, b_2s = t_2a.$$

Then one can always form the Ore localisation '$\Lambda(G)_T$' at the multiplicatively closed set T. We now further assume that G has a quotient $\Gamma \cong \mathbb{Z}_p$, and let H denote the kernel of the surjection $G \twoheadrightarrow \Gamma$, so that $G/H \xrightarrow{\cong} \mathbb{Z}_p$.

Definition 2.16 *Let S denote the set of all $f \in \Lambda(G)$ such that $\Lambda(G)/\Lambda(G)f$ is a finitely generated $\Lambda(H)$-module; we call S a left and right* **Ore set** *in $\Lambda(G)$.*

If M is a finitely generated left and right $\Lambda(G)$-module, then M is S-torsion if and only if M is finitely generated over $\Lambda(H)$. Moreover, the set S is multiplicatively closed, and all elements of S are non-zero divisors in $\Lambda(G)$ (see [CFK$^+$05, Section 2]).

2.5 The non-commutative Iwasawa Main Conjecture

In this section, we shall focus on the non-commutative Main Conjecture formulated by Coates et al in [CFK$^+$05] for $GL_2(\mathbb{Z}_p)$, but in the setting of general p-adic Lie groups. Henceforth let G denote a compact p-adic Lie group which is torsion-free.

2.5.1 Akashi series and Euler characteristics

To make explicit the connection between p-adic L-functions and Selmer groups, it is not so easy to directly interpolate the complex zeta function inside a non-commutative ring.

Recall that $S = \{s \in \Lambda | \Lambda/\Lambda s \text{ is a finitely generated } \Lambda(H) - \text{module}\}$. Let $S^* = \cup_{n\geq 0} p^n S$ be its p-saturation.

Lemma 2.12 *[CFK+05] A $\Lambda(G)$-module M is S^*-torsion if and only if $M/M(p)$ is finitely generated over $\Lambda(H)$, where $M(p)$ denotes the submodule of M consisting of all elements of p-power order.*

We write $\Lambda(G)_S, \Lambda(G)_{S^*}$ for the localization of $\Lambda(G)$ at S and S^* respectively, so that

$$\Lambda(G)_{S^*} = \Lambda(G)_S[1/p].$$

We also write $\mathfrak{M}_H(G)$ for the category of all finitely generated $\Lambda(G)$-modules which are S^*-torsion.

We say that a $\Lambda(G)$-module M has finite Euler characteristic if $H_i(G, M)$ is finite for all i. If M has finite Euler characteristic, we define

$$\chi(G, M) = \prod_{i\geq 0} |H_i(G, M)|^{(-1)^i} = \prod_{i\geq 0} |Tor_n^{\Lambda(G)}(M, \mathbb{Z}_p)|^{(-1)^i}.$$

Theorem 2.13 *[CFK+05, Lemma 3.1] For each M in $\mathfrak{M}_H(G)$, the homology groups $H_i(H, M)$ for $i \geq 0$ are all finitely generated torsion $\Lambda(G)$-modules. If G has no element of order p, then $H_i(H, M) = 0$ for $i \geq d$, where d is the dimension of the p-adic Lie group G.*

Let $\rho : G \mapsto GL_n(\mathcal{O})$ be a continuous representation, where $\mathcal{O}$ is the ring of integers of a finite extension L of $\mathbb{Q}_p$. We define $M_n(\mathcal{O})$ to be the ring of matrices with coefficients inside $\mathcal{O}$, and set $\Lambda_{\mathcal{O}}(\Gamma) := \mathcal{O}[\![\Gamma]\!]$ to be the associated completed group algebra. Then ρ induces two homomorphisms

$$\rho : \Lambda(G) \mapsto M_n(\mathcal{O}) \quad \text{and} \quad \Phi_\rho : \Lambda(G) \mapsto M_n(\Lambda_{\mathcal{O}}(\Gamma)).$$

If $Q_{\mathcal{O}}(\Gamma)$ is the fraction field of the Iwasawa algebra $\Lambda_{\mathcal{O}}(\Gamma)$, then Φ_ρ can be extended to a map

$$\Phi_\rho : \Lambda(G)_{S^*} \mapsto M_n(Q_{\mathcal{O}}(\Gamma))$$

which (on the level of K-groups) induces

$$\Phi'_\rho : K_1(\Lambda(G)_{S^*}) \mapsto K_1(M_n(\Lambda_{\mathcal{O}}(\Gamma))) \cong \Lambda_{\mathcal{O}}(\Gamma)^\times.$$

Let us write $\varphi : \Lambda_{\mathcal{O}}(\Gamma) \mapsto \mathcal{O}$ for the augmentation map (sending a topological generator γ of Γ to the value 1), and set $\mathfrak{p} = Ker(\varphi)$. Clearly φ extends to a homomorphism

$$\varphi : \Lambda_{\mathcal{O}}(\Gamma)_{\mathfrak{p}} \mapsto L.$$

Now let ξ be any element in $K_1(\Lambda(G)_{S^*})$. We can compose Φ'_ρ and φ together, so one defines the 'evaluation of ξ at ρ' by

$$\xi(\rho) = \begin{cases} \varphi(\Phi'_\rho(\xi) & \text{if } \xi \in \Lambda_{\mathcal{O}}(\Gamma)_{\mathfrak{p}} \\ \infty & \text{if } \xi \notin \Lambda_{\mathcal{O}}(\Gamma)_{\mathfrak{p}}. \end{cases}$$

This map allows us to send element from $K_1(\Lambda(G)_{S^*})$ to $L \cup \{\infty\}$. One defines the boundary map

$$\partial_G : K_1(\Lambda(G)_{S^*}) \longrightarrow K_0(\mathfrak{M}_H(G))$$

to be the connecting map in the long exact sequence

$$\cdots \to K_1(\Lambda(G)) \to K_1(\Lambda(G)_{S^*}) \xrightarrow{\partial_G} K_0(\mathfrak{M}_H(G)) \to K_0(\Lambda(G)) \to K_0(\Lambda(G)_{S^*}) \to 0 \tag{2.1}$$

from [CFK$^+$05, Eqn (24)]. Furthermore, if G has no element of order p then ∂_G is surjective [CFK$^+$05, Proposition 3.4]; henceforth we assume that G has no element of order p.

Definition 2.17 *For each M in $\mathfrak{M}_H(G)$, a characteristic element of M is any lift $\xi_M \in K_1(\Lambda(G)_{S^*})$, such that*

$$\partial_G(\xi_M) = [M].$$

2.5.2 Non-commutative Main Conjecture

We now assume E is an elliptic curve over $\mathbb{Q}$ with good ordinary reduction at p. Let $\rho : G_{\mathbb{Q}} \to GL(V_\rho)$ be an Artin representation.

Definition 2.18 *The complex Artin L-function is defined to be*

$$L(\rho, s) = \prod_q P_q(\rho, q^{-s})^{-1}$$

where $P_q(\rho, T)$ is the polynomial

$$P_q(\rho, T) = det(1 - Frob_q^{-1} X | V_\rho^{I_q}).$$

Conjecturally, this L-function has a meromorphic continuation to the whole of $\mathbb{C}$. For a prime l, recall that

$$T_l(E) = \lim_{\leftarrow} E_{l^n}, \qquad V_l(E) = T_l(E) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l, \qquad H_l^1(E) = \mathrm{Hom}(V_l(E), \mathbb{Q}_l).$$

The complex L-function of E twisted by the Artin representation ρ is defined by the Euler product

$$L_R(E, \rho, s) = \prod_{q \notin R} P_q(E, \rho, q^{-s})^{-1}$$

where $P_q(E, \rho, X)$ is the polynomial

$$P_q(E, \rho, X) = det(1 - Frob_q^{-1} X | (H_l^1(E) \otimes_{\mathbb{Q}_l} V_{\rho,\lambda})^{I_q}) \quad \text{for } Re(s) \gg 0.$$

Here λ is a place lying over l, and R is the finite set of primes that ramify in the extension $F_\infty/\mathbb{Q}$.

Let L be any algebraic extension of $\mathbb{Q}$. Recall again that the classical Selmer group $S(E/L)$ is defined by

$$Sel(E/L) := ker\big(H^1(L, E_{p^\infty}) \mapsto \prod_\omega H^1(L_\omega, E(\bar{L}_\omega))\big)$$

where ω runs over all the non-Archimedean places of L, and L_ω denotes the union of the completions at ω of all finite extensions of $\mathbb{Q}$ contained in L. One then denotes by

$$X(E/L) := Hom(Sel(E/L), \mathbb{Q}_p/\mathbb{Z}_p)$$

the Pontrjagin dual of the discrete abelian group $Sel(E/L)$.

The following is a non-commutative generalisation of Conjecture 2.7.

Conjecture 2.14 *[CFK+05] Assume that E has good ordinary reduction at p, let $G = Gal(F_\infty/\mathbb{Q})$ be a p-adic Lie group without p-torsion, and assume that F_∞ contains the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}^{cyc}$ of $\mathbb{Q}$, with $\Gamma = Gal(\mathbb{Q}^{cyc}/\mathbb{Q}) \cong \mathbb{Z}_p$. Then*

1. *$X(E/F_\infty)$ belongs to $\mathfrak{M}_H(G)$;*

2. *there exists $\mathcal{L}_E \in K_1(\Lambda(G)_{S^*})$ such that for all Artin representations ρ factoring through $F_\infty/\mathbb{Q}$,*

$$\Phi_\rho(\mathcal{L}_E) = \frac{L_R(E,\rho,1)}{\Omega_+(E)^{d^+(\rho)}\Omega_-(E)^{d^-(\rho)}} \cdot e_p(\rho) \cdot \frac{P_p(\hat{\rho},u^{-1})}{P_p(\rho,\omega^{-1})} \cdot {\alpha_p}^{-f_\rho},$$

where R is the set of primes that ramifies in $F_\infty/\mathbb{Q}$;

3. *$\partial_G(\mathcal{L}_E) = [X(E/F_\infty)]$.*

2.5.3 A special case when $G = \Gamma$

In this subsection, we focus on the special case where $G = \Gamma \cong \mathbb{Z}_p$. Let $G = Gal(\mathbb{Q}^{cyc}/\mathbb{Q}) = \Gamma$, so that $H = \{1\}$. Then the long exact sequence (2.1) becomes

$$\cdots \to K_1(\Lambda(\Gamma)) \to K_1(\Lambda(\Gamma)_{S^*}) \xrightarrow{\partial_G} K_0(\mathfrak{M}_H(\Gamma)) \to K_0(\Lambda(\Gamma)) \to K_0(\Lambda(\Gamma)_{S^*}) \to 0$$

where $K_1(\Lambda(\Gamma)) = \Lambda(\Gamma)^\times$, and $K_1(\Lambda(\Gamma)_{S^*}) \cong \Lambda(\Gamma)_{(p)}[\frac{1}{p}]^\times$. One makes the key observation that $X(\widetilde{E/\mathbb{Q}^{cyc}}) \in \Lambda(\Gamma)_{(p)}[\frac{1}{p}]^\times$ where $X(\widetilde{E/\mathbb{Q}^{cyc}})$ is a lift of $[X(E/\mathbb{Q}^{cyc})]$, and so it well-defined up to an element $u \in K_1(\Lambda(\Gamma)) \cong \Lambda(\Gamma)^\times$.

In particular, when $G \cong \mathbb{Z}_p$ the Main Conjecture of Coates et al. collapses back down to the version of the Iwasawa Main Conjecture formulated by Mazur for elliptic curves.

Conjecture 2.15 *1. There exists $\mathcal{L}_\alpha(E,T) \in \mathbb{Z}_p[[T]][\frac{1}{p}] \cong \Lambda(\Gamma)[\frac{1}{p}]$, such that for each $\chi : \Gamma \mapsto \bar{\mathbb{Q}}_p^\times$ of finite order*

$$\mathcal{L}_\alpha(E,\chi(\gamma)-1) = \begin{cases} \epsilon \cdot \frac{L(E,1)}{\Omega_E} & \text{if } \chi = 1 \\ \frac{1}{\alpha^{n+1}} \cdot \frac{p^{n+1}}{G(\chi^{-1})} \cdot \frac{L(E,\chi,1)}{\Omega_E^{sign(\chi)}} & \text{if } \chi \neq 1, \text{ and } cond(\chi) = p^n. \end{cases}$$

2. *The p-adic L-function $\mathcal{L}_\alpha(E,\gamma-1)$ is a characteristic element of $X(E/F_\infty)$, i.e.*

$$\partial_\Gamma(\mathcal{L}_\alpha(E,\gamma-1)) = [X(E/\mathbb{Q}^{cyc})].$$

Equivalently, $\mathcal{L}_\alpha(E,\gamma-1) = Char_{\Lambda(\Gamma)}(X(E/\mathbb{Q}^{cyc}) \times u$, where u is an element of $\Lambda(\Gamma)^\times$.

Chapter 3

The Main Results

In order to explain our main research question, we start by introducing some necessary notations. Then we will give statements for two of the major theorems in this thesis. Lastly, various applications of our theorems will be discussed at the end of the chapter, in terms of specific arithmetic situations.

3.1 Preliminaries

Fix a number field F and a prime number $p \neq 2$. We shall assume that F_∞ denotes a p-adic Lie extension of F satisfying:

(i) $\mathrm{Gal}(F_\infty/F)$ is a pro-p-group without any p-torsion;

(ii) F_∞ contains the cyclotomic $\mathbb{Z}_p$-extension F^{cyc} of F.

The examples we have in mind here are solvable three-dimensional Galois groups arising from algebraic geometry, or alternatively the direct product of a two-dimensional Galois group with a group of diamond operators (in the context of Hida's deformation theory). We therefore suppose that either

(iiia) $\mathcal{G}_\infty = \mathrm{Gal}(F_\infty/F)$ where $\dim\big(\mathrm{Gal}(F_\infty/F)\big) = 3$ and $\mathcal{G}_\infty \ncong \mathrm{SL}_2(\mathbb{Z}_p), \mathrm{SL}_1(\mathbb{D}_p)$;

or (iiib) $\mathcal{G}_\infty = \mathrm{Gal}(F_\infty/F) \times \mathcal{W}_\infty$ where $\dim\big(\mathrm{Gal}(F_\infty/F)\big) = 2$ and $\mathcal{W}_\infty \cong \mathbb{Z}_p$.

In both (iiia) and (iiib), the p-adic Lie group $\mathcal{G}_\infty$ is three-dimensional and also solvable; in fact $\mathcal{G}_\infty$ is a semi-direct product of $\mathbb{Z}_p$ with an abelian subgroup $\mathcal{H}_\infty$ of $\mathbb{Z}_p$-rank two. The following result classifies such groups.

Classification Theorem. *(González-Sánchez and Klopsch [GSK09]) If the pro-p-group $\mathcal{G}_\infty$ is solvable and torsion-free with $\dim(\mathcal{G}_\infty) = 3$, then $\mathcal{G}_\infty$ must be isomorphic to one of the following possibilities:*

(I) the abelian group $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$;

(II) an open subgroup of the p-adic Heisenberg group, i.e. a group given by the presentation $\left\langle \gamma, h_1, h_2 : [h_1, h_2] = 1, [h_1, \gamma] = 1, [h_2, \gamma] = h_1^{p^s} \right\rangle$ for some $s \in \mathbb{N}_0$;

(III) the group $\left\langle \gamma, h_1, h_2 : [h_1, h_2] = 1, [h_1, \gamma] = h_1^{p^s}, [h_2, \gamma] = h_2^{p^s} \right\rangle$ for some $s \in \mathbb{N}$;

(IV) $\left\langle \gamma, h_1, h_2 : [h_1, h_2] = 1, [h_1, \gamma] = h_1^{p^s} h_2^{p^{s+r}d}, [h_2, \gamma] = h_1^{p^{s+r}} h_2^{p^s} \right\rangle$ for some $s, r \in \mathbb{N}$ with $d \in \mathbb{Z}_p$;

(V) $\left\langle \gamma, h_1, h_2 : [h_1, h_2] = 1, [h_1, \gamma] = h_2^{p^s d}, [h_2, \gamma] = h_1^{p^s} h_2^{p^{s+r}} \right\rangle$ where $s, r \in \mathbb{N}_0$ and $d \in \mathbb{Z}_p$, such that either $s \geq 1$, or instead $r \geq 1$ and $d \in p\mathbb{Z}_p$;

(VI) either one of the groups:

$$\begin{aligned} &(a) \quad \left\langle \gamma, h_1, h_2 : [h_1, h_2] = 1, [h_1, \gamma] = h_2^{p^{s+r}}, [h_2, \gamma] = h_1^{p^s} \right\rangle \\ \text{or} \quad &(b) \quad \left\langle \gamma, h_1, h_2 : [h_1, h_2] = 1, [h_1, \gamma] = h_2^{p^{s+r}t}, [h_2, \gamma] = h_1^{p^s} \right\rangle \end{aligned}$$

where $s, r \in \mathbb{N}_0$ such that $s + r \geq 1$, and $t \in \mathbb{Z}_p^\times$ is not a square modulo p.

Let $\Gamma = \left\{ \gamma^z \mid z \in \mathbb{Z}_p \right\}$ where γ is as in the previous theorem (if $\mathcal{G}_\infty = \text{Gal}(F_\infty/F)$ satisfies condition (iiia) above, we shall identify its quotient $\text{Gal}(F^{\text{cyc}}/F) \cong \mathbb{Z}_p$ with Γ). One defines a decreasing sequence of normal subgroups for $\mathcal{G}_\infty$ by

$$\mathcal{U}_m := \Gamma^{p^m} \ltimes \mathcal{H}_\infty \quad \text{at each } m \geq 0.$$

Recall from [Ser12, Prop 25], every irreducible $\mathcal{G}_\infty$-representation with finite image is of the form $\psi \otimes \text{Ind}_{\mathcal{U}_m}^{\mathcal{G}_\infty}(\chi)$ for some $m \geq 0$, with characters $\chi : \mathcal{U}_m^{\text{ab}} \to \mu_{p^\infty}$ and $\psi : \Gamma^{p^m} \to \overline{\mathbb{Q}}_p^\times$.

If G is a pro-p-group, then we write $\Lambda(G) = \varprojlim_P \mathbb{Z}_p[G/P]$ for its Iwasawa algebra where the inverse limit runs over open subgroups $P \lhd G$. If $\mathcal{O}$ contains $\mathbb{Z}_p$ as a subring then $\Lambda_{\mathcal{O}}(G) := \Lambda(G) \otimes_{\mathbb{Z}_p} \mathcal{O}$. Lastly for a canonical Ore set $\mathcal{S}$, we use $\Lambda(G)_{\mathcal{S}}$ and $\Lambda(G)_{\mathcal{S}^*}$ for the localisation of $\Lambda(G)$ at $\mathcal{S}$, and at its p-saturation $\mathcal{S}^* = \bigcup_{n \geq 0} p^n \mathcal{S}$, respectively.

Remark: We shall use $\mathcal{O}_\chi$ to indicate the finite integral extension of $\mathbb{Z}_p$ generated by the values of χ. Let us also write $\mathcal{N}_{\mathcal{U}_m} : \Lambda(\mathcal{G}_\infty) \to \Lambda(\mathcal{U}_m)$ for the norm mapping on Iwasawa algebras. If $\big[\mathcal{U}_m, \mathcal{U}_m\big]$ denotes the commutator subgroup of $\mathcal{U}_m$, there is a commutative diagram

$$\begin{tikzcd}
K_1\big(\Lambda(\mathcal{G}_\infty)\big) \arrow[r, "\prod \mathcal{N}_{\mathcal{U}_m}(-) \bmod [\mathcal{U}_m,\mathcal{U}_m]"] \arrow[d] & \prod\limits_{m\geq 0} K_1\big(\Lambda(\mathcal{U}_m^{\mathrm{ab}})\big) \arrow[r, "\prod \chi_*"] \arrow[d] & \prod\limits_{m\geq 0} \prod\limits_{\rho_\chi} \Lambda_{\mathcal{O}_\chi}\big(\Gamma^{p^m}\big)^\times \arrow[d, hook] \\
K_1\big(\Lambda(\mathcal{G}_\infty)_{\mathcal{S}}\big) \arrow[r, "\prod \mathcal{N}_{\mathcal{U}_m}(-) \bmod [\mathcal{U}_m,\mathcal{U}_m]"] \arrow[d] & \prod\limits_{m\geq 0} K_1\big(\Lambda(\mathcal{U}_m^{\mathrm{ab}})_{\overline{\mathcal{S}}}\big) \arrow[r, "\prod \chi_*"] \arrow[d] & \prod\limits_{m\geq 0} \prod\limits_{\rho_\chi} \Lambda_{\mathcal{O}_\chi}\big(\Gamma^{p^m}\big)^\times_{(p)} \arrow[d, hook] \\
K_1\big(\Lambda(\mathcal{G}_\infty)_{\mathcal{S}^*}\big) \arrow[r, "\prod \mathcal{N}_{\mathcal{U}_m}(-) \bmod [\mathcal{U}_m,\mathcal{U}_m]"] & \prod\limits_{m\geq 0} K_1\big(\Lambda(\mathcal{U}_m^{\mathrm{ab}})_{\overline{\mathcal{S}}^*}\big) \arrow[r, "\prod \chi_*"] & \prod\limits_{m\geq 0} \prod\limits_{\rho_\chi} \mathrm{Quot}\big(\Lambda_{\mathcal{O}_\chi}(\Gamma^{p^m})\big)^\times
\end{tikzcd}$$

where the vertical arrows are induced from the inclusions $\Lambda(\mathcal{G}_\infty) \hookrightarrow \Lambda(\mathcal{G}_\infty)_{\mathcal{S}} \hookrightarrow \Lambda(\mathcal{G}_\infty)_{\mathcal{S}^*}$, and the right-most products range over *irreducible* non-isomorphic $\mathcal{G}_\infty$-representations. Here we have used $\overline{\mathcal{S}}$ as a generic symbol, indicating the image of the set $\mathcal{S}$ under each mapping $\prod \mathcal{N}_{\mathcal{U}_m}(-) \bmod [\mathcal{U}_m, \mathcal{U}_m]$ above.

One can then define three separate theta-maps $\Theta_{\infty,\underline{\chi}}$, $\Theta_{\infty,\underline{\chi},\mathcal{S}}$ and $\Theta_{\infty,\underline{\chi},\mathcal{S}^*}$ by composing (respectively) the first, second and third rows in the above diagram, so that

$$\begin{aligned}
\Theta_{\infty,\underline{\chi}} : K_1\big(\Lambda(\mathcal{G}_\infty)\big) &\longrightarrow \prod_{\rho_\chi} \Lambda_{\mathcal{O}_\chi}\big(\Gamma^{\dim(\rho_\chi)}\big)^\times, \\
\Theta_{\infty,\underline{\chi},\mathcal{S}} : K_1\big(\Lambda(\mathcal{G}_\infty)_{\mathcal{S}}\big) &\longrightarrow \prod_{\rho_\chi} \Lambda_{\mathcal{O}_\chi}\big(\Gamma^{\dim(\rho_\chi)}\big)^\times_{(p)} \\
\text{and} \qquad \Theta_{\infty,\underline{\chi},\mathcal{S}^*} : K_1\big(\Lambda(\mathcal{G}_\infty)_{\mathcal{S}^*}\big) &\longrightarrow \prod_{\rho_\chi} \mathrm{Quot}\big(\Lambda_{\mathcal{O}_\chi}(\Gamma^{\dim(\rho_\chi)})\big)^\times.
\end{aligned}$$

The Main Goal. *To describe the images of $\Theta_{\infty,\underline{\chi}}$, $\Theta_{\infty,\underline{\chi},\mathcal{S}}$ and $\Theta_{\infty,\underline{\chi},\mathcal{S}^*}$ by using a family of p-adic congruences linking together the abelian fragments $\mathbf{y}_{\rho_\chi} \in \mathrm{Quot}\big(\Lambda_{\mathcal{O}_\chi}(\Gamma^{p^{\mathbf{m}_\chi}})\big)^\times$.*

Note that Case (I) is devoid of any content since $\mathcal{G}_\infty \cong \Gamma \times \mathcal{H}_\infty$ is abelian, in which case

$$K_1\big(\Lambda(\mathcal{G}_\infty)\big) \;=\; K_1\big(\Lambda(\Gamma \times \mathcal{H}_\infty)\big) \;\cong\; \Lambda(\Gamma \times \mathcal{H}_\infty)^\times$$

by Morita invariance. **Hence one may ignore Case (I) completely, since there are no non-abelian congruences to consider here.**

3.2 The non-abelian congruences

In order to describe the congruences in each of the non-empty Cases (II-VI), we first need some means to keep track of those Artin representations induced from characters on $\mathcal{H}_\infty$. If χ is a finite order character on $\mathcal{H}_\infty$ then χ extends naturally to $\mathrm{Stab}_\Gamma(\chi) \ltimes \mathcal{H}_\infty$, hence

$$\rho_\chi \;:=\; \mathrm{Ind}^{\mathcal{G}_\infty}_{\mathrm{Stab}_\Gamma(\chi)\ltimes\mathcal{H}_\infty}(\chi)$$

is an irreducible $\mathcal{G}_\infty$-representation of dimension $p^{\mathbf{m}_\chi}$, where $\mathbf{m}_\chi = \mathrm{ord}_p\big([\Gamma : \mathrm{Stab}_\Gamma(\chi)]\big)$. In all cases $\star \in \{\text{II,III,IV,V,VI}\}$, one constructs characters $\chi_{1,n},\ \chi_{2,n} : \mathcal{H}_\infty \to \mu_{p^\infty}$ via

$$\chi_{1,n}\big(h_1^x h_2^y\big) \;=\; \exp\big(2\pi\sqrt{-1}\, x/p^n\big) \quad \text{and} \quad \chi_{2,n}\big(h_1^x h_2^y\big) \;=\; \exp\big(2\pi\sqrt{-1}\, y/p^n\big)$$

for each $x, y \in \mathbb{Z}_p$. In particular, $\chi_{1,n}$ and $\chi_{2,n}$ together generate a basis for $\mathrm{Hom}(\mathcal{H}_\infty, \mu_{p^n})$.

Case (II). For simplicity, let us initially assume we are in Case (II). Then for each character $\chi = \chi_{2,n}^a \cdot \chi_{1,s+m'}^b$ and group element $h = h_1^x h_2^y \in \mathcal{H}_\infty$, one defines $\mathbf{e}^*_{\chi,h} \in \mathbb{Z}[\mu_{p^n}]$ by the formula

$$\mathbf{e}^*_{\chi,h} \;:=\; \begin{cases} \chi^{-1}(\overline{h}) \cdot p^{\max\{0,m'-\mathrm{ord}_p(b)\}} & \text{if } p^{m'} \mid by \\ 0 & \text{if } p^{m'} \nmid by. \end{cases}$$

Theorem 3.1 *If we are in Case (II), then a sequence* $\big(\mathbf{y}_{\rho_\chi}\big) \in \prod_{\rho_\chi} \Lambda_{\mathcal{O}_\chi}\big(\Gamma^{p^{\mathbf{m}_\chi}}\big)^\times_{(p)}$ *belongs to the image of* $\Theta_{\infty,\underline{\chi},\mathcal{S}}$ *only if*

$$\prod_{m'=0}^{m} \prod_{a=1}^{p^{n-m'}} \prod_{\substack{b\,=\,1, \\ p\,\nmid\, b \text{ if } m'>0}}^{p^{s+m'}} \mathcal{N}_{\mathbf{m}_\chi,m}\left(\frac{\mathbf{y}_{\rho_\chi}}{\varphi\big(\mathbf{y}_{\rho_{\chi^p}}\big)} \cdot \frac{\varphi\big(\mathcal{N}_{0,\mathbf{m}_\chi-1}(\mathbf{y_1})\big)}{\mathcal{N}_{0,\mathbf{m}_\chi}(\mathbf{y_1})}\right)^{\mathbf{e}^*_{\chi,h}} \Bigg|_{\chi=\chi^a_{2,n}\cdot\chi^b_{1,s+m'}}$$

$$\equiv\; 1 \mod p^{s+m+n+\mathrm{ord}_p(y)} \cdot \mathbb{Z}_p\big[\big[\Gamma^{p^m}\big]\big]_{(p)} \qquad (3.1)$$

for all integer pairs $m, n \geq 0$ with $m \leq n - s$, and at every choice of $h = h_1^x h_2^y \in \mathcal{H}_\infty$ with $x \in \{1, \ldots, p^n\}$ and $y \in \{1, \ldots, p^m\}$.

We should point out that, a priori, it is not clear whether the p-adic power $\mathcal{N}_{\mathbf{m}_\chi,m}(\ldots)^{\mathbf{e}^*_{\chi,h}}$ above should even exist, as the exponent $\mathbf{e}^*_{\chi,h} \in \mathbb{Z}[\mu_{p^n}]$ is frequently not a rational integer!

Remarks: (i) For any function $f(X) \in 1 + p \cdot \mathcal{O}_{\mathbb{C}_p}[\![X]\!]$, and provided that $s \in \mathbb{C}_p$ is chosen to lie inside the disk $\big|s\big|_p < p^{(p-2)/(p-1)}$, the p-adic power series defined as

$$f(X)^s \;:=\; \exp_p\big(s \log_p\big(f(X)\big)\big)$$

converges to an element of $1 + p \cdot \mathcal{O}_{\mathbb{C}_p}[\![X]\!]$. In particular, if $s \in \mathbb{Z}$ then $f(X)^s$ coincides with the standard definition of the s-th power.

(ii) Furthermore, this construction extends after localisation at the multiplicatively closed set $\mathcal{O}_{\mathbb{C}_p}[\![X]\!] - p \cdot \mathcal{O}_{\mathbb{C}_p}[\![X]\!]$, i.e. if $f(X) \in 1 + p \cdot \mathcal{O}_{\mathbb{C}_p}[\![X]\!]_{(p)}$ then $f(X)^s \in 1 + p \cdot \mathcal{O}_{\mathbb{C}_p}[\![X]\!]_{(p)}$.

(iii) Although not explicitly stated, it is nevertheless inbuilt into Theorem 3.1 that each of the fractions $\frac{\mathbf{y}_{\rho_\chi}}{\varphi(\mathbf{y}_{\rho_\chi p})} \cdot \frac{\varphi(\mathcal{N}_{0,\mathbf{m}_\chi - 1}(\mathbf{y_1}))}{\mathcal{N}_{0,\mathbf{m}_\chi}(\mathbf{y_1})}$ belongs to the multiplicative group $1 + p \cdot \mathcal{O}_\chi[\![\Gamma^{p^m}]\!]_{(p)}$. In light of this discussion, one deduces that each term $\mathcal{N}_{\mathbf{m}_\chi, m}(\dots)^{\mathbf{e}^*_{\chi,h}}$ in the above theorem exists as a well-defined element of the multiplicative group $1 + p \cdot \mathcal{O}_{\mathbb{C}_p}[\![\Gamma^{p^m}]\!]_{(p)}$.

Cases (III)-(VI). Let us now instead suppose we are in Case $(\star)$ with $\star \in$ {III,IV,V,VI}. We define a non-negative integer $\epsilon_{\star,p}$ by the rule

$$\epsilon_{\star,p} \;=\; \begin{cases} 0 & \text{if } \star = \text{(III) or (IV)} \\ \mathrm{ord}_p(d) & \text{if } \star = \text{(V)} \\ r + \mathrm{ord}_p(t) & \text{if } \star = \text{(VI).} \end{cases}$$

It will be shown (in Proposition 4.4) that the abelianization of $\mathcal{U}_m$ yields the tricyclic group

$$\mathcal{U}_m^{\mathrm{ab}} \;:=\; \frac{\mathcal{U}_m}{[\mathcal{U}_m, \mathcal{U}_m]} \;\;\cong\;\; \Gamma^{p^m} \times C_{p^{s+m+\epsilon_{\star,p}}} \times C_{p^{s+m}}$$

where C_d denotes the cyclic group of order d.

Note that the commutator $[\mathcal{U}_m\ ,\ \mathcal{U}_m]$ is actually a subgroup of $\mathcal{H}_\infty$, while Γ acts on $\mathcal{U}_m^{\mathrm{ab}}$ through the finite quotient Γ/Γ^{p^m}; we can then partition

$$\overline{\mathcal{H}}_\infty^{(m)} \;:=\; \frac{\mathcal{H}_\infty}{[\mathcal{U}_m\ ,\ \mathcal{U}_m]} \;\;\cong\;\; C_{p^{s+m+\epsilon_{\star,p}}} \times C_{p^{s+m}}$$

into a finite disjoint union of its Γ-orbits. Similarly, the dual group $\mathrm{Hom}\big(\overline{\mathcal{H}}_\infty^{(m)}, \mathbb{C}^\times\big)$

also has an action of Γ/Γ^{p^m}; let '$\mathfrak{R}_m$' denote a set of representatives for its Γ-orbits.

For each orbit $\varpi_{\overline{h}} = \{\gamma^{-j}\overline{h}\gamma^j \mid j \in \mathbb{Z}/p^m\mathbb{Z}\}$, $\overline{h} \in \overline{\mathcal{H}}_\infty^{(m)}$ and character $\chi : \overline{\mathcal{H}}_\infty^{(m)} \to \mathbb{C}^\times$, we generalise the definition of $\mathbf{e}^*_{\chi,h}$ by computing the trace of $\overline{h}$ over the orbits of χ:

$$\mathbf{e}^*_{\chi,\varpi_{\overline{h}}} \;=\; \mathrm{Tr}(\mathrm{Ind}\chi^*)\big(\varpi_{\overline{h}}\big) \;:=\; \sum_{\chi'\in\{\chi^g \mid g\in\Gamma\}} (\chi')^{-1}(\overline{h}).$$

In fact, it is easy to check that $\mathbf{e}^*_{\chi,\varpi_{\overline{h}}}$ depends only on the representative for χ within the set $\mathfrak{R}_m$ and on the orbit $\varpi_{\overline{h}}$ generated by $\overline{h}$, but not on the individual choices of χ and $\overline{h}$. Although these quantities might seem abstract, they are all computable (see Lemma 7.3).

Theorem 3.2 *If we are in Cases (III)–(VI), then a sequence* $\big(\mathbf{y}_{\rho_\chi}\big) \in \prod_{\rho_\chi} \Lambda_{\mathcal{O}_\chi}\big(\Gamma^{p^{\mathbf{m}_\chi}}\big)^\times_{(p)}$ *belongs to the image of* $\Theta_{\infty,\underline{\chi},\mathcal{S}}$ *only if*

$$\prod_{\chi\in\mathfrak{R}_m} \mathcal{N}_{\mathbf{m}_\chi,m}\left(\frac{\mathbf{y}_{\rho_\chi}}{\varphi\big(\mathbf{y}_{\rho_{\chi^p}}\big)}\cdot\frac{\varphi\big(\mathcal{N}_{0,\mathbf{m}_\chi-1}\big(\mathbf{y_1}\big)\big)}{\mathcal{N}_{0,\mathbf{m}_\chi}\big(\mathbf{y_1}\big)}\right)^{\mathbf{e}^*_{\chi,\varpi}} \equiv\; 1 \mod p^{2s+3m+\epsilon_{\star,p}-\mathrm{ord}_p(\#\varpi)}\cdot\mathbb{Z}_p\big[\big[\Gamma^{p^m}\big]\big]_{(p)} \quad (3.2)$$

for every $m \geq 0$*, and over all* Γ*-orbits* ϖ *inside the group* $\overline{\mathcal{H}}_\infty^{(m)} \cong C_{p^{s+m+\epsilon_{\star,p}}} \times C_{p^{s+m}}$*.*

Note in both of these theorems, if one additionally knows that $\big(\mathbf{y}_{\rho_\chi}\big) \in \prod_{\rho_\chi} \Lambda_{\mathcal{O}_\chi}\big(\Gamma^{p^{\mathbf{m}_\chi}}\big)^\times$, the modified statement should read: '$\big(\mathbf{y}_{\rho_\chi}\big) \in \mathrm{Im}\big(\Theta_{\infty,\underline{\chi}}\big)$ **if and only if** the same congruences in (3.1), (3.2) hold after replacing $p^\bullet\cdot\mathbb{Z}_p[[\Gamma^{p^m}]]_{(p)}$ with its unlocalised version $p^\bullet\cdot\mathbb{Z}_p[[\Gamma^{p^m}]]$'.

We also remark that Burns and Venjakob [BV11, Prop 3.4] have constructed a splitting

$$K_1\big(\Lambda(\mathcal{G}_\infty)_{\mathcal{S}^*}\big) \;\cong\; K_1\big(\Lambda(\mathcal{G}_\infty)_{\mathcal{S}}\big)\oplus K_0\big(\mathbb{F}_p[[\mathcal{G}_\infty]]\big)$$

so one can reduce the existence of elements in $K_1\big(\Lambda(\mathcal{G}_\infty)_{\mathcal{S}^*}\big)$ to those in $K_1\big(\Lambda(\mathcal{G}_\infty)_{\mathcal{S}}\big)$, combined with a precise growth formula for the μ-invariant of the individual $\mathbf{y}_{\rho_\chi}$'s.

3.3 Some arithmetic examples

Before explaining the strategy to prove our two main theorems, we first discuss some applications to non-commutative Iwasawa theory that arise from these K_1-congruences.

Totally real extensions. Let us initially suppose that F is a totally real field, and further:

- $F_\infty = \bigcup_{n\geq 1} F_n$ is a union of totally real fields;
- only finitely many primes of F ramify inside F_∞/F;
- F_∞ contains the cyclotomic $\mathbb{Z}_p$-extension F^{cyc} of F;
- the cyclotomic μ-invariant of $F\big(e^{2\pi i/p}\big)$ vanishes.

We denote by Σ the primes ramifying inside F_∞/F. One also defines $F^{(m)}$ to be the unique extension of degree p^m contained in F^{cyc}, so that $\Gamma = \mathrm{Gal}\big(F^{\mathrm{cyc}}/F\big) \cong \varprojlim_m \mathrm{Gal}\big(F^{(m)}/F\big)$.

Let $\mathcal{G}_\infty = \mathrm{Gal}\big(F_\infty/F\big)$, and write $\kappa_F : \Gamma \to \mathbb{Z}_p^\times$ for the p-th cyclotomic character. By seminal work of Burns, Kakde and Ritter-Weiss [Bur15, Kak13, RW06], there exists an element $\zeta_{F_\infty/F} \in K_1\big(\Lambda(\mathcal{G}_\infty)_{\mathcal{S}^*}\big)$ such that, at any Artin representation $\rho : \mathcal{G}_\infty \to \mathrm{GL}(V)$, one has

$$\zeta_{F_\infty/F}\big(\rho\kappa_F^k\big) \;=\; L_\Sigma(\rho, 1-k)$$

for each $k \in \mathbb{N}$ satisfying $k \equiv 0 \pmod{[F(\mu_p) : F]}$. By deforming the k-variable p-adically, the above values interpolate to the Iwasawa function $L_{p,\Sigma}(\rho, -) : \mathbb{Z}_p \to \overline{\mathbb{Q}}_p$ constructed by Cassou-Noguès and Deligne-Ribet [CN79, DR80].

Corollary 3.3 *Let F_∞/F be an infinite solvable Lie extension as above, with $\dim(\mathcal{G}_\infty) = 3$. If the representation $\rho_\chi = \mathrm{Ind}^{\mathcal{G}_\infty}_{\mathrm{Stab}_\Gamma(\chi)\ltimes\mathcal{H}_\infty}(\chi)$ has dimension equal to $p^{\mathbf{m}_\chi}$ say, then write $\mathbf{L}^{\text{D-R}}_{p,\Sigma}\big(\rho_\chi\big) \in \mathrm{Quot}\big(\Lambda_{\mathcal{O}_\chi}(\Gamma^{p^{\mathbf{m}_\chi}})\big)^\times$ for the unique element satisfying*

$$\kappa_F^k \circ \mathbf{L}^{\text{D-R}}_{p,\Sigma}\big(\rho_\chi\big) \;=\; L_{p,\Sigma}(\rho_\chi, 1-k) \quad \textit{for all } k \in \mathbb{Z}_p.$$

(a) If we are in Case (II), then the system of congruences (3.1) holds for $\mathbf{y}_{\rho_\chi} = \mathbf{L}^{\text{D-R}}_{p,\Sigma}\big(\rho_\chi\big)$.

(b) In Case $(\star)$ *with* $\star \in \{$*III,IV, V, VI*$\}$*, the congruences (3.2) hold for* $\mathbf{y}_{\rho_\chi} = \mathbf{L}^{\text{D-R}}_{p,\Sigma}\big(\rho_\chi\big)$.

Proof. Note that the infinite sequence $\big(\mathbf{L}^{\text{D-R}}_{p,\Sigma}(\rho_\chi)\big) \in \prod_{\rho_\chi} \text{Quot}\big(\Lambda_{\mathcal{O}_\chi}(\Gamma^{p^{\mathbf{m}_\chi}})\big)^\times$ coincides with $\Theta_{\infty,\underline{\chi},\mathcal{S}^*}\big(\zeta_{F_\infty/F}\big)$, as they both interpolate the same L-values. Therefore the necessity of the congruences (3.1) and (3.2) follows directly from Theorems 3.1 and 3.2, respectively. □

Let us now digress momentarily, and assume we are given a congruence of the form

$$\frac{F(X)}{G(X)} \;\equiv\; 1 \quad \text{mod } p^v \cdot \mathbb{Z}_p[\![X]\!]_{(p)} \quad \text{with } F, G \in \mathcal{O}_{\mathbb{C}_p}[\![X]\!] \text{ and } v \geq 1.$$

Then $\frac{F(X)}{G(X)} = 1 + p^v \cdot \frac{R(X)}{T(X)}$ for some $R, T \in \mathbb{Z}_p[\![X]\!]$ where the μ-invariant of T equals zero. It follows that $F \cdot T = G \cdot (T + p^v \cdot R)$, and one works out that

$$\mu(F) \;=\; \mu(F \cdot T) \;=\; \mu(G) + \mu(T + p^v \cdot R) \;=\; \mu(G) + 0,$$

i.e. $\mu(F) = \mu(G)$. Also $F = G + \frac{p^v \cdot RG}{T} \in \mathcal{O}_{\mathbb{C}_p}[\![X]\!]$ so that $T\big|RG$, whence $F \equiv G \;(\text{mod } p^v)$. Certainly if $\mu(F) = \mu(G) = 0$, then the leading terms of F and G are congruent mod p^v. However even if $\mu(F) = \mu(G) > 0$, their leading terms must still be congruent modulo p^v, as one can repeat the above argument with $\tilde{F} = p^{-\mu(F)} \cdot F$ and $\tilde{G} = p^{-\mu(F)} \cdot G$ instead.

Conclusion: If $\frac{F(X)}{G(X)} \equiv 1 \text{ mod } p^v \cdot \mathbb{Z}_p[\![X]\!]_{(p)}$, the leading terms of F, G agree modulo p^v.

We are going to apply this to the congruences (3.1) and (3.2) at the trivial orbit $\varpi = \{\text{id}\}$: specifically, F will denote the numerator of (3.1) and (3.2) while G will be the denominator, so that $\frac{F(X)}{G(X)} \equiv 1 \text{ mod } p^v \cdot \mathbb{Z}_p[\![X]\!]_{(p)}$ with $X = \gamma^{p^m} - 1$, and $v = s + 2m + n$ when $\star =$II whilst $v = 2s + 3m + \epsilon_{\star,p}$ when $\star \neq$II.

To individually describe the leading terms, if $r(\rho, x_0) = \text{order}_{x=x_0}\big(L_{p,\Sigma}(\rho, x)\big)$ then

$$L_{\Sigma}^{(p)}(\rho, 1-k) \ := \ \begin{cases} L_{\Sigma}(\rho, 1-k) & \text{if } r(\rho, 1-k) = 0 \\ \lim_{x \to 1-k} \big(x^{-r(\rho,1-k)} \cdot L_{p,\Sigma}(\rho, x)\big) & \text{if } r(\rho, 1-k) > 0 \end{cases}$$

yields the p-adic residue of $L_{p,\Sigma}(\rho, x)$ at the non-positive critical value $x = 1-k$.

Notations: (i) At integers $m \geq m' \geq 0$, let us define $\mathbf{r}_{m',m} = \text{Ind}_{F^{(m)}}^{F^{(m')}}(\mathbf{1})$ to be the regular representation for $\text{Gal}\big(F^{(m)}/F^{(m')}\big)$.
(ii) Furthermore, we shall write $\mathbf{r}_{0,m}^{(m')}$ as an abbreviation for $\text{Ind}_{F^{(m'-1)}}^{F}\Big(\psi_p \circ \mathbf{r}_{m',m}\Big|_{F^{(m')}}\Big)$, where ψ_p is the p-th Adams operator (strictly speaking ψ_p only acts on the trace of a virtual representation, but the abuse of notation makes sense in the context of ζ-functions).
(iii) Lastly set $\rho_{\chi}^{(m)} := \text{Ind}_{F^{(m)}}^{F}\big(\chi\big|_{F^{(m)}}\big)$ and $\rho_{\chi^p}^{(m)} := \text{Ind}_{F^{(\mathbf{m}_\chi - 1)}}^{F}\Big(\psi_p \circ \text{Ind}_{F^{(m)}}^{F^{(\mathbf{m}_\chi)}}\big(\chi\big|_{F^{(m)}}\big)\Big)$.

Theorem 3.4 *Let F_∞/F be as above, with* $\dim(\mathcal{G}_\infty) = 3$ *and also* $\zeta_{F_\infty/F} \in K_1\big(\Lambda(\mathcal{G}_\infty)_{\mathcal{S}}\big)$.
(a) If we are in Case (II), then for every $m, n, k \in \mathbb{N}$:

$$\prod_{m'=0}^{m} \prod_{a=1}^{p^{n-m'}} \prod_{\substack{b\,=\,1, \\ p \,\nmid\, b \text{ if } m' > 0}}^{p^{s+m'}} \Big(L_{\Sigma}^{(p)}\big(\rho_{\chi}^{(m)}, 1-k\big) \cdot L_{\Sigma}^{(p)}\big(\mathbf{r}_{0,m}^{(\mathbf{m}_\chi)}, 1-k\big)\Big)^{p^{\mathbf{m}_\chi}} \Bigg|_{\chi = \chi_{2,n}^{a} \cdot \chi_{1,s+m'}^{b}}$$

$$\equiv \ \prod_{m'=0}^{m} \prod_{a=1}^{p^{n-m'}} \prod_{\substack{b\,=\,1, \\ p \,\nmid\, b \text{ if } m' > 0}}^{p^{s+m'}} \Big(L_{\Sigma}^{(p)}\big(\rho_{\chi^p}^{(m)}, 1-k\big) \cdot L_{\Sigma}^{(p)}\big(\mathbf{r}_{0,m}, 1-k\big)\Big)^{p^{\mathbf{m}_\chi}} \Bigg|_{\chi = \chi_{2,n}^{a} \cdot \chi_{1,s+m'}^{b}}$$

modulo p^{s+2m+n}.
(b) In Case ($\star$) with $\star \in \{III, IV, V, VI\}$, for every $m, k \in \mathbb{N}$:

$$\prod_{\chi \in \mathfrak{R}_m} \Big(L_{\Sigma}^{(p)}\big(\rho_{\chi}^{(m)}, 1-k\big) \cdot L_{\Sigma}^{(p)}\big(\mathbf{r}_{0,m}^{(\mathbf{m}_\chi)}, 1-k\big)\Big)^{p^{\mathbf{m}_\chi}}$$

$$\equiv \ \prod_{\chi \in \mathfrak{R}_m} \Big(L_{\Sigma}^{(p)}\big(\rho_{\chi^p}^{(m)}, 1-k\big) \cdot L_{\Sigma}^{(p)}\big(\mathbf{r}_{0,m}, 1-k\big)\Big)^{p^{\mathbf{m}_\chi}} \quad \text{mod } p^{2s+3m+\epsilon_{\star,p}}.$$

Because p-adic zeta-functions of totally real fields do not vanish at odd negative integers, a nice consequence is that whenever $k \equiv 0 \pmod{[F(\mu_p) : F]}$, these congruences actually involve bona fide *complex zeta-values*, not simply their p-adic residues.

Heisenberg extensions. Let us now suppose we are in Case (II) with the parameter $s \geq 0$, in which case $\mathcal{G}_\infty$ is an open subgroup of the Heisenberg group, i.e.

$$\mathcal{G}_\infty \ \lhd \ H_3(\mathbb{Z}_p) := \begin{pmatrix} 1 & \mathbb{Z}_p & \mathbb{Z}_p \\ 0 & 1 & \mathbb{Z}_p \\ 0 & 0 & 1 \end{pmatrix} \quad \text{where} \ \ \big[H_3(\mathbb{Z}_p) : \mathcal{G}_\infty\big] = p^s.$$

In an unpublished preprint [Kat06], Kato derives different but equivalent congruences to (3.1), as ideal congruences in the group algebras associated to finite sub-quotients of $H_3(\mathbb{Z}_p)$. Thus Theorem 3.4(a) gives a concrete description for the most basic of these ideal relations, as a congruence modulo p^{s+2m+n} connecting the special values of Artin L-functions.

False-Tate extensions. Fix an integer $s \geq 1$. We shall now set $F = \mathbb{Q}(\mu_{p^s})$ and $F_\infty = \mathbb{Q}\big(\mu_{p^\infty}, q_1^{1/p^\infty}, q_2^{1/p^\infty}\big)$ where $q_1, q_2 > 1$ are distinct p-power free integers satisfying $\gcd(p, q_1q_2) = \gcd(q_1, q_2) = 1$. Then $\mathcal{G}_\infty = \mathrm{Gal}\big(F_\infty/F\big)$ is a three-dimensional pro-p-group, which corresponds precisely to Case (III) covered by the Classification Theorem (note that F_∞ is **not** a union of totally real fields so there is no element $\zeta_{F_\infty/F} \in K_1\big(\Lambda(\mathcal{G}_\infty)_{\mathcal{S}^*}\big)$ available, and therefore no Iwasawa Main Conjecture can be formulated for Tate motives here).

Now if $s = 1$, the congruences (3.2) specialise down to yield the congruences labelled $(1.1)_{m,\underline{\mathfrak{h}}}$ and $(1.2)_m$ in [DP15, p3]. If $E_{/\mathbb{Q}}$ denotes a semistable elliptic curve with good ordinary reduction at p, then p-adic L-functions $\mathbf{L}_p(E, \rho_\chi) \in \Lambda\big(\Gamma^{p^{\mathbf{m}_\chi}}\big)\big[1/p\big]$ interpolating the algebraic part of $L_{\{pq_1q_2\}}(E, \rho_\chi, 1)$ have been constructed in Theorem 1.5 of *op. cit.* Furthermore, there are three 'first layer congruences' to check for each tuple (E, p, q_1, q_2). These were verified numerically for the elliptic curves 11a3, 77c1, 19a3 and 56a1 using MAGMA at the primes $p = 3, 5$ and at small values of q_1 and q_2, in §6 of *op. cit.*

On the algebraic side, let us further assume that q_1 and q_2 are both chosen to be primes of non-split multiplicative reduction for E, such that

$$(-1)^{(p-1)/2} \times \prod_{l|\mathrm{cond}(E),\ l\neq q_1,q_2} \left(\frac{l}{p}\right) \;=\; -1$$

where $\left(\frac{-}{p}\right)$ denotes the Legendre symbol at p. Then if the cyclotomic λ-invariant of $\mathrm{Sel}_{p^\infty}\big(E/\mathbb{Q}(\mu_{p^\infty})\big)$ equals one and if $\mathrm{Sel}_{p^\infty}(E/F_\infty)^\wedge$ belongs to the category $\mathfrak{M}_{\mathcal{H}_\infty}(\mathcal{G}_\infty)$, it is shown in [DL17, Corollary 2.6] that

$$\mathrm{rank}_{\mathbb{Z}}\big(E(F_n)\big) \;=\; p^{2n-1} \text{ or } p^{2n},$$

provided the p-Sylow subgroup of $\text{Ш}(E/F_n)$ is finite at each layer $F_n = \mathbb{Q}\big(\mu_{p^n}, q_1^{1/p^n}, q_2^{1/p^n}\big)$. Alternatively, by studying the λ-invariants of each χ-part $\mathrm{Sel}_{p^\infty}(E/F_n(\mu_{p^\infty}))^\wedge \otimes_{\mathbb{Z}_p,\chi} \mathcal{O}_\chi$ using the congruences in Theorem 3.2, one can produce the same estimate for the rank (current work of the first named author [Del18]).

Heegner-type extensions. Consider an imaginary quadratic field $k = \mathbb{Q}\big(\sqrt{-D}\big)$ and let us suppose k_∞ denotes its $\mathbb{Z}_p^2$-extension, so that $\mathrm{Gal}(k_\infty/k) \cong \Gamma \times \mathcal{H}_{1,\infty}$ where $\mathcal{H}_{1,\infty}$ is the Galois group of the anticyclotomic $\mathbb{Z}_p$-extension of k. For any choice of odd prime $q \neq p$ with $q \nmid D$, one may set $F = \mathbb{Q}\big(\sqrt{-D}, \mu_p\big)$ and $F_\infty = k_\infty\big(\mu_p, q^{1/p^\infty}\big)$, in which case

$$\mathcal{G}_\infty := \mathrm{Gal}(F_\infty/F) \;\cong\; \Gamma \ltimes \big(\mathcal{H}_{1,\infty} \times \mathcal{H}_{2,\infty}\big) \;\cong\; \big(\Gamma \times \mathcal{H}_{1,\infty}\big) \ltimes \mathcal{H}_{2,\infty}.$$

Here h_1 acts trivially on $\mathcal{H}_{2,\infty} = \overline{\langle h_2 \rangle} = \mathrm{Gal}\big(F_\infty/k_\infty(\mu_p)\big)$, while γ acts on h_2 through multiplication by $1+p$ (we must therefore be in Case (V) with $s = d = 0$ and $r = 1$).

Let $E_{/\mathbb{Q}}$ be a semistable elliptic curve with ordinary reduction at p, split multiplicative reduction at q, and with non-split multiplicative reduction at all other primes dividing the conductor of E. We also suppose that q generates $\big(\mathbb{Z}/p^2\mathbb{Z}\big)^\times$ so that q is inert in $\mathbb{Q}(\mu_{p^\infty})$, and that the various Heegner conditions **(DT1)**–**(DT7)** described in [DL17, Sect 2.4] hold. Then it is shown in Proposition 2.14 of *op. cit.* that for $n \gg 0$,

$$p^{2n} \cdot \left(1 - \frac{2p^2+2p+1}{(p+1)^3}\right) \;\leq\; \mathrm{rank}_{\mathbb{Z}}\big(E(F_n)\big) \;\leq\; p^{2n} + 4$$

with no hypotheses whatsoever on the finiteness of $Ш(E/F_n)[p^\infty]$.

The upper bound essentially comes from a growth formula for the λ-invariant of $\mathrm{Sel}_{p^\infty}(E/F_n(\mu_{p^\infty}))^\wedge$ as n becomes large. In fact if one exploits the congruences (3.2), this yields another way to obtain the upper bound on $\mathrm{rank}_{\mathbb{Z}}\big(E(F_n)\big)$, and establishes finer bounds on the χ-part of $E(F_n)$. However the lower bound relies heavily on the properties of Heegner points, following the same approach as Darmon and Tian [DT10] in dimension 2.

p^n-division fields of CM curves. Let $E_{/\mathbb{Q}}$ be an elliptic curve with complex multiplication by $k = \mathbb{Q}\big(\sqrt{-D}\big)$, and select a good ordinary prime $p \neq 2$ for E which splits inside $\mathbb{Z}\big(\sqrt{-D}\big)$. If one takes $F = \mathbb{Q}\big(\sqrt{-D}, \mu_p\big)$, $F_n = \mathbb{Q}\big(E[p^n], q^{1/p^n}\big)$ and $F_\infty = \bigcup_{n\geq 1} F_n$ for an auxiliary prime q not dividing $\mathrm{cond}(E)$, then $\mathcal{G}_\infty := \mathrm{Gal}(F_\infty/F)$ corresponds to Case (V) with $s = d = 0$ and $r = 1$ again. By using the congruences (3.2) to study the λ-invariants of $\mathrm{Sel}_{p^\infty}(E/F_n)^\wedge$, one can bound the rank of $E(F_n)$ from above by p^{2n} if the cyclotomic λ-invariant is one. Whilst Heegner points are no longer useful here, a lower bound on the $\mathbb{Z}$-rank of $E(F_n)$ of the form $c_p \times p^{2n}$ (with $c_p \neq 0$ and $c_p \sim 1$ if $p \gg 0$) should still be feasible, if one exploits the non-triviality of the Euler system of elliptic units in place of the Heegner points.

Chapter 4

Representation Theory for Dimension Three

We begin by reviewing some representation theory for the three-dimensional group $\mathcal{G}_\infty$. We next calculate the stabilizer of a character χ on a case-by-case basis. We shall also need a nice system of subgroups on which to realize our theta-maps, so we define such a system. Finally, following the blueprint of Kakde's seminal paper [Kak13], we introduce the transfer map Ver, the shift map π, the trace map and the norm map.

4.1 The general set-up in dimension three

Observe that $\mathcal{H}_\infty = \mathcal{H}_{1,\infty} \times \mathcal{H}_{2,\infty} \cong \mathbb{Z}_p \times \mathbb{Z}_p$ is generated by $h_1 = (1,0)^T$ and $h_2 = (0,1)^T$ topologically. The action of each $g = \gamma^z \in \Gamma$ on an arbitrary element $(x,y)^T = h_1^x h_2^y \in \mathcal{H}_\infty$ can be described through a 2×2-matrix of the form $I_2 + M$:

$$\gamma^z\big((x,y)^T\big) \;=\; \gamma^{-z}\big(h_1^x h_2^y\big)\gamma^z \;=\; \big(I_2 + M\big)^z \begin{pmatrix} x \\ y \end{pmatrix} \qquad \text{for all } g = \gamma^z \in \Gamma$$

where $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the identity, and $M \in \mathrm{Mat}_{2\times 2}\big(\mathbb{Z}_p\big)$ is topologically nilpotent.

Proposition 4.1 *Applying the Classification Theorem for $\mathcal{G}_\infty$, the matrix M equals*

$$\begin{pmatrix} 0 & p^s \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} p^s & 0 \\ 0 & p^s \end{pmatrix}, \begin{pmatrix} p^s & p^{s+r} \\ p^{s+r}d & p^s \end{pmatrix}, \begin{pmatrix} 0 & p^s \\ p^sd & p^{s+r} \end{pmatrix} \text{ and } \begin{pmatrix} 0 & p^s \\ p^{s+r}t & 0 \end{pmatrix} \tag{4.1}$$

in Cases (II), (III), (IV), (V) and (VI) respectively (note in Case (VIa) we have set $t = 1$).

Proof. Let us treat these on a case-by-case basis. We shall switch between group notation and vector notation throughout.

In Case (II),

$$\gamma^{-1}\big(h_1^x h_2^y\big)\gamma \;= h_1^{x+p^sy}h_2^y = \begin{pmatrix} x+p^sy \\ y \end{pmatrix} = \begin{pmatrix} 1 & p^s \\ 0 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix},$$

hence $I_2 + M = \begin{pmatrix} 1 & p^s \\ 0 & 1 \end{pmatrix}$.

In Case (III),

$$\gamma^{-1}\big(h_1^x h_2^y\big)\gamma \;= (h_1^x h_2^y)^{(1+p^s)} = \begin{pmatrix} (1+p^s)x \\ (1+p^s)y \end{pmatrix} = \begin{pmatrix} 1+p^s & 0 \\ 0 & 1+p^s \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix},$$

hence $I_2 + M = \begin{pmatrix} 1+p^s & 0 \\ 0 & 1+p^s \end{pmatrix}$.

In Case (IV),

$$\gamma^{-1}\big(h_1^x h_2^y\big)\gamma \;= h_1^{(1+p^s)x+p^{s+r}y}h_2^{p^{s+r}dx+(1+p^s)y} = \begin{pmatrix} 1+p^s & p^{s+r} \\ p^{s+r}d & 1+p^s \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix},$$

hence $I_2 + M = \begin{pmatrix} 1+p^s & p^{s+r} \\ p^{s+r}d & 1+p^s \end{pmatrix}$.

In Case (V),

$$\gamma^{-1}\big(h_1^x h_2^y\big)\gamma \;= h_1^{x+p^sy}h_2^{p^sdx+(1+p^{s+r})y} = \begin{pmatrix} 1 & p^s \\ p^sd & 1+p^{s+r} \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix},$$

hence $I_2 + M = \begin{pmatrix} 1 & p^s \\ p^s d & 1 + p^{s+r} \end{pmatrix}$.

In Case (VI),

$$\gamma^{-1}\big(h_1^x h_2^y\big)\gamma \;=\; h_1^{x+p^s y} h_2^{p^{s+r}tx+y} \;=\; \begin{pmatrix} 1 & p^s \\ p^{s+r}t & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix},$$

hence $I_2 + M = \begin{pmatrix} 1 & p^s \\ p^{s+r}t & 1 \end{pmatrix}$.

□

4.1.1 Determining the stabilizer of a character on $\mathcal{H}_\infty$

Note each element $g \in \Gamma$ acts naturally (on the left) on each $\chi \in \mathrm{Hom}(\mathcal{H}_\infty, \mu_{p^\infty})$ by sending $\chi \mapsto g \star \chi$, where $g \star \chi(h) := \chi(g^{-1}hg)$ for all $h \in \mathcal{H}_\infty$. The Γ-stabilizer of χ is given by the subgroup

$$\mathrm{Stab}_\Gamma(\chi) \;:=\; \Big\{ g \in \Gamma \;\Big|\; \chi\big(g^{-1}(h_1^x h_2^y) g\big) = \chi\big(h_1^x h_2^y\big) \;\text{ for all } h = h_1^x h_2^y \in \mathcal{H}_\infty \Big\}.$$

Proposition 4.2 *If* $\chi = \chi_{1,n}^{e_1} \times \chi_{2,n}^{e_2} : \mathcal{H}_\infty \twoheadrightarrow \mu_{p^n}$ *is a surjective character, then*

$$\big[\Gamma : \mathrm{Stab}_\Gamma(\chi)\big] = p^{\max\{0, \boldsymbol{m}_\chi\}}$$

where, using the case-by-case description in the Classification Theorem, one has:

(II) $\boldsymbol{m}_\chi = n - s - \mathrm{ord}_p(\boldsymbol{e}_1)$; *(III)* $\boldsymbol{m}_\chi = n - s$; *(IV)* $\boldsymbol{m}_\chi = n - s$;
(V) $\boldsymbol{m}_\chi = n - s - \min\big\{\mathrm{ord}_p(\boldsymbol{e}_2) + \mathrm{ord}_p(d), \mathrm{ord}_p(\boldsymbol{e}_1 + p^r\boldsymbol{e}_2)\big\}$; *and*
(VI) $\boldsymbol{m}_\chi = n - s - \min\big\{r + \mathrm{ord}_p(\boldsymbol{e}_2), \mathrm{ord}_p(\boldsymbol{e}_1)\big\}$.

Proof. Firstly, let us denote by ζ_{p^n} the primitive p^n-th root of unity $\exp(2\pi\sqrt{-1}/p^n)$.

Case (II). Here $I_2 + M = \begin{pmatrix} 1 & p^s \\ 0 & 1 \end{pmatrix}$, so that $\gamma^{-p^i}(h_1^x h_2^y)\gamma^{p^i} = h_1^{x+p^{s+i}y} h_2^y$.

Consequently

$$\chi\left(\gamma^{-p^i}(h_1^x h_2^y)\gamma^{p^i}\right) \;=\; \chi_{1,n}\big(h_1^{x+p^{s+i}y} h_2^y\big)^{\mathbf{e}_1} \times \chi_{2,n}\big(h_1^{x+p^{s+i}y} h_2^y\big)^{\mathbf{e}_2} \;=\; \zeta_{p^n}^{\mathbf{e}_1 x + (\mathbf{e}_2 + \mathbf{e}_1 \times p^{s+i})y}$$

equals $\chi\big(h_1^x h_2^y\big) = \zeta_{p^n}^{\mathbf{e}_1 x + \mathbf{e}_2 y}$ for all $x, y \in \mathbb{Z}$, if and only if $\mathbf{e}_1 \times p^{s+i} \equiv 0 \ (\bmod\ p^n)$.

Case (III). Here $I_2 + M = \begin{pmatrix} 1+p^s & 0 \\ 0 & 1+p^s \end{pmatrix}$ with repeated eigenvalue $\lambda_{III,\pm} = 1 + p^s$, and it follows that

$$\chi\left(\gamma^{-p^i}(h_1^x h_2^y)\gamma^{p^i}\right) \ = \ \chi(h_1^x h_2^y)^{(1+p^s)^{p^i}} \ = \ \zeta_{p^n}^{(\mathbf{e}_1 x + \mathbf{e}_2 y)\times(1+p^s)^{p^i}}.$$

However $(1+p^s)^{p^i} \equiv 1 \ (\bmod\ p^{s+i})$ but $(1+p^s)^{p^i} \not\equiv 1 \ (\bmod\ p^{s+i+1})$, in which case $\chi\left(\gamma^{-p^i}(h_1^x h_2^y)\gamma^{p^i}\right)$ equals $\chi(h_1^x h_2^y) = \zeta_{p^n}^{\mathbf{e}_1 x + \mathbf{e}_2 y}$ for all $x, y \in \mathbb{Z}$, if and only if

$$\mathrm{ord}_p\big((1+p^s)^{p^i} - 1\big) = s + i \ \geq \ n, \qquad \text{i.e. if and only if } \ i \ \geq \ n - s.$$

Case (IV). Here $I_2 + M = \begin{pmatrix} 1+p^s & p^{s+r} \\ p^{s+r}d & 1+p^s \end{pmatrix}$; let $\lambda_{IV,\pm} := 1 + p^s \pm p^{s+r}\sqrt{d}$ be the two distinct eigenvalues of $I_2 + M$, so that

$$I_2 + M = P_{IV} D_{IV} P_{IV}^{-1} \quad \text{with } \ D_{IV} = \begin{pmatrix} \lambda_{IV,+} & 0 \\ 0 & \lambda_{IV,-} \end{pmatrix} \text{and } P_{IV} = \begin{pmatrix} 1 & 1 \\ \sqrt{d} & -\sqrt{d} \end{pmatrix}.$$

Since $(I_2 + M)^{p^i} = P_{IV} D_{IV}^{p^i} P_{IV}^{-1}$, one readily computes

$$\begin{aligned}
\gamma^{-p^i}\big(h_1^x h_2^y\big)\gamma^{p^i} &= \begin{pmatrix} 1+p^s & p^{s+r} \\ p^{s+r}d & 1+p^s \end{pmatrix}^{p^i} \begin{pmatrix} x \\ y \end{pmatrix} \\
&= \begin{pmatrix} 1 & 1 \\ \sqrt{d} & -\sqrt{d} \end{pmatrix} \begin{pmatrix} \lambda_{IV,+} & 0 \\ 0 & \lambda_{IV,-} \end{pmatrix}^{p^i} \begin{pmatrix} 1 & 1 \\ \sqrt{d} & -\sqrt{d} \end{pmatrix}^{-1} \begin{pmatrix} x \\ y \end{pmatrix} \\
&= \begin{pmatrix} \frac{\lambda_{IV,+}^{p^i} + \lambda_{IV,-}^{p^i}}{2} & \frac{\lambda_{IV,+}^{p^i} - \lambda_{IV,-}^{p^i}}{2\sqrt{d}} \\ \frac{\lambda_{IV,+}^{p^i} - \lambda_{IV,-}^{p^i}}{2}\sqrt{d} & \frac{\lambda_{IV,+}^{p^i} + \lambda_{IV,-}^{p^i}}{2} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \\
&= h_1^{\left(\frac{\lambda_{IV,+}^{p^i} + \lambda_{IV,-}^{p^i}}{2}\right)x + \left(\frac{\lambda_{IV,+}^{p^i} - \lambda_{IV,-}^{p^i}}{2\sqrt{d}}\right)y} h_2^{\left(\frac{\lambda_{IV,+}^{p^i} - \lambda_{IV,-}^{p^i}}{2}\right)\sqrt{d}\,x + \left(\frac{\lambda_{IV,+}^{p^i} + \lambda_{IV,-}^{p^i}}{2}\right)y}
\end{aligned} \tag{4.2}$$

To study both $\frac{\lambda_{IV,+}^{p^i} + \lambda_{IV,-}^{p^i}}{2}$ and $\frac{\lambda_{IV,+}^{p^i} - \lambda_{IV,-}^{p^i}}{2}$, note that

$$\lambda_{IV,\pm}^p \ = \ \big(1 + p^s(1 \pm p^r\sqrt{d})\big)^p \ = \ 1 + \begin{pmatrix} p \\ 1 \end{pmatrix} p^s(1 \pm p^r\sqrt{d}) + \sum_{j=2}^{p} \begin{pmatrix} p \\ j \end{pmatrix} p^{sj}(1 \pm p^r\sqrt{d})^j$$

and $(1 \pm p^r\sqrt{d})^j = 1 \pm jp^r\sqrt{d} + O\big(p^{2r+\delta_p}\big)$ where $\delta_p = \mathrm{ord}_p(d)$, hence

$$\begin{aligned}\lambda^p_{IV,\pm} &= 1 + p^{s+1} \pm p^{s+r+1}\sqrt{d} + \sum_{j=2}^{p} \begin{pmatrix} p \\ j \end{pmatrix} p^{sj} \pm p^r\sqrt{d}\ \sum_{j=2}^{p} \begin{pmatrix} p \\ j \end{pmatrix} jp^{sj} + O\big(p^{2s+2r+1+\delta_p}\big) \\ &= \ 1 + p^{s+1} \pm p^{s+r+1}\sqrt{d} + \Big((1+p^s)^p - 1 - p^{s+1}\Big) \pm O\big(p^{2s+r+1+\delta_p/2}\big) + O\big(p^{2s+2r+1+\delta_p}\big).\end{aligned}$$

It follows that $\frac{\lambda^p_{IV,+}+\lambda^p_{IV,-}}{2}$ will equal $1 + p^{s+1} + \Big((1 + p^s)^p - 1 - p^{s+1}\Big) + O\big(p^{2s+r+1+\delta_p/2}\big)$, or less accurately $\frac{\lambda^p_{IV,+}+\lambda^p_{IV,-}}{2} = 1 + p^{s+1} + O\big(p^{2s+1}\big)$; applying an induction argument:

$$\frac{\lambda^{p^i}_{IV,+} + \lambda^{p^i}_{IV,-}}{2} \ = \ 1 + p^{s+i} + O\big(p^{2s+i}\big). \tag{4.3}$$

On the other hand, the difference term $\frac{\lambda^p_{IV,+}-\lambda^p_{IV,-}}{2}$ equals $p^{s+r+1}\sqrt{d} + O\big(p^{2s+r+1+\delta_p/2}\big)$, and therefore $\frac{\lambda^p_{IV,+}-\lambda^p_{IV,-}}{2\sqrt{d}} = p^{s+r+1} + O\big(p^{2s+r+1}\big)$; applying induction again:

$$\frac{\lambda^{p^i}_{IV,+} - \lambda^{p^i}_{IV,-}}{2\sqrt{d}} \ = \ p^{s+r+i} + O\big(p^{2s+r+i}\big). \tag{4.4}$$

Recalling the chosen character $\chi = \chi^{\mathbf{e}_1}_{1,n} \times \chi^{\mathbf{e}_2}_{2,n}$, from Equation (4.2) one obtains

$$\begin{aligned}\chi\left(\gamma^{-p^i}(h_1^x h_2^y)\gamma^{p^i}\right) \ &= \ \chi_{1,n}\left(\gamma^{-p^i}(h_1^x h_2^y)\gamma^{p^i}\right)^{\mathbf{e}_1} \times \chi_{2,n}\left(\gamma^{-p^i}(h_1^x h_2^y)\gamma^{p^i}\right)^{\mathbf{e}_2} \\ &= \ \zeta_{p^n}^{\left(\mathbf{e}_1\left(\frac{\lambda^{p^i}_{IV,+}+\lambda^{p^i}_{IV,-}}{2}\right)+\mathbf{e}_2\left(\frac{\lambda^{p^i}_{IV,+}-\lambda^{p^i}_{IV,-}}{2}\right)\sqrt{d}\right)x+\left(\mathbf{e}_1\left(\frac{\lambda^{p^i}_{IV,+}-\lambda^{p^i}_{IV,-}}{2\sqrt{d}}\right)+\mathbf{e}_2\left(\frac{\lambda^{p^i}_{IV,+}+\lambda^{p^i}_{IV,-}}{2}\right)\right)y}.\end{aligned}$$

As a corollary of our estimates in (4.3) and (4.4), $\gamma^{p^i}\star\chi(h_1^x h_2^y) = \chi\left(\gamma^{-p^i}(h_1^x h_2^y)\gamma^{p^i}\right)$ equals $\chi(h_1^x h_2^y) = \zeta_{p^n}^{\mathbf{e}_1 x + \mathbf{e}_2 y}$ for all $x, y \in \mathbb{Z}$, if and only if

$$\mathbf{e}_1 p^{s+i} + \mathbf{e}_2 p^{s+r+i} d \equiv 0 \ (\bmod p^n) \quad \text{and} \quad \mathbf{e}_1 p^{s+r+i} + \mathbf{e}_2 p^{s+i} \equiv 0 \ (\bmod p^n),$$

i.e. if and only if $i \ \geq \ n - s - \min\big\{\mathrm{ord}_p(\mathbf{e}_1 + p^r d\mathbf{e}_2)\ , \mathrm{ord}_p(p^r\mathbf{e}_1 + \mathbf{e}_2)\big\} = n - s$.

Case (V). Here $I_2 + M = \begin{pmatrix} 1 & p^s \\ p^s d & 1 + p^{s+r} \end{pmatrix}$; let $\lambda_{V,\pm} := 1 + \frac{p^{s+r}}{2} \pm p^s\sqrt{\Delta_V}$ with $\Delta_V = d + p^{2r}/4$ denote the eigenvalues of $I_2 + M$. Indeed for all $i \geq 0$, one may write

$$(I_2 + M)^{p^i} \ = \ P_V \begin{pmatrix} \lambda^{p^i}_{V,+} & 0 \\ 0 & \lambda^{p^i}_{V,-} \end{pmatrix} P_V^{-1}$$

where $P_V = \begin{pmatrix} 1 & 1 \\ \frac{p^r}{2} + \sqrt{\Delta_V} & \frac{p^r}{2} - \sqrt{\Delta_V} \end{pmatrix}$, and its inverse $P_V^{-1} = \frac{1}{2} \begin{pmatrix} 1 - \frac{p^r}{2\sqrt{\Delta_V}} & \frac{1}{\sqrt{\Delta_V}} \\ 1 + \frac{p^r}{2\sqrt{\Delta_V}} & -\frac{1}{\sqrt{\Delta_V}} \end{pmatrix}$. Using this decomposition, we next deduce

$$\begin{aligned}
\gamma^{-p^i}\big(h_1^x h_2^y\big)\gamma^{p^i} &= \begin{pmatrix} 1 & p^s \\ p^s d & 1 + p^{s+r} \end{pmatrix}^{p^i} \begin{pmatrix} x \\ y \end{pmatrix} \\
&= \begin{pmatrix} 1 & 1 \\ \frac{p^r}{2} + \sqrt{\Delta_V} & \frac{p^r}{2} - \sqrt{\Delta_V} \end{pmatrix} \begin{pmatrix} \lambda_{V,+} & 0 \\ 0 & \lambda_{V,-} \end{pmatrix}^{p^i} \frac{1}{2} \begin{pmatrix} 1 - \frac{p^r}{2\sqrt{\Delta_V}} & \frac{1}{\sqrt{\Delta_V}} \\ 1 + \frac{p^r}{2\sqrt{\Delta_V}} & -\frac{1}{\sqrt{\Delta_V}} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \\
&= \begin{pmatrix} \frac{\lambda_{V,+}^{p^i} + \lambda_{V,-}^{p^i}}{2} - \frac{\lambda_{V,+}^{p^i} - \lambda_{V,-}^{p^i}}{2\sqrt{\Delta_V}} \times \frac{p^r}{2} & \frac{\lambda_{V,+}^{p^i} - \lambda_{V,-}^{p^i}}{2\sqrt{\Delta_V}} \\ \frac{\lambda_{V,+}^{p^i} - \lambda_{V,-}^{p^i}}{2\sqrt{\Delta_V}} d & \frac{\lambda_{V,+}^{p^i} + \lambda_{V,-}^{p^i}}{2} + \frac{\lambda_{V,+}^{p^i} - \lambda_{V,-}^{p^i}}{2\sqrt{\Delta_V}} \times \frac{p^r}{2} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \\
&= h_1^{\left(\frac{\lambda_{V,+}^{p^i} + \lambda_{V,-}^{p^i}}{2} - \frac{\lambda_{V,+}^{p^i} - \lambda_{V,-}^{p^i}}{2\sqrt{\Delta_V}} \times \frac{p^r}{2}\right)x + \left(\frac{\lambda_{V,+}^{p^i} - \lambda_{V,-}^{p^i}}{2\sqrt{\Delta_V}}\right)y} \\
&\quad \times h_2^{\left(\frac{\lambda_{V,+}^{p^i} - \lambda_{V,-}^{p^i}}{2\sqrt{\Delta_V}}\right)dx + \left(\frac{\lambda_{V,+}^{p^i} + \lambda_{V,-}^{p^i}}{2} + \frac{\lambda_{V,+}^{p^i} - \lambda_{V,-}^{p^i}}{2\sqrt{\Delta_V}} \times \frac{p^r}{2}\right)y} \qquad (4.5)
\end{aligned}$$

Now from the binomial theorem,

$$\lambda_{V,\pm}^p \;=\; 1 + \frac{p^{s+r+1}}{2} \pm p^{s+1}\sqrt{\Delta_V} \;+\; \sum_{j=2}^{p} \binom{p}{j} p^{sj}\Big(\frac{p^r}{2} \pm \sqrt{\Delta_V}\Big)^j.$$

- If $\mathrm{ord}_p(\sqrt{\Delta_V}) \geq r$ then $\left(\frac{p^r}{2} \pm \sqrt{\Delta_V}\right)^j = \left(\frac{p^r}{2}\right)^j \pm j\left(\frac{p^r}{2}\right)^{j-1}\sqrt{\Delta_V} + O\big(p^{r(j-2)+\delta'_p}\big)$

where $\delta'_p = \mathrm{ord}_p(\Delta_V)$, hence

$$\begin{aligned}
&\textstyle\sum_{j=2}^{p} \binom{p}{j} p^{sj}\Big(\frac{p^r}{2} \pm \sqrt{\Delta_V}\Big)^j \\
&= \textstyle\sum_{j=2}^{p} \binom{p}{j} p^{sj}\left(\left(\frac{p^r}{2}\right)^j \pm j\left(\frac{p^r}{2}\right)^{j-1}\sqrt{\Delta_V}\right) + O\big(p^{2s+1+\delta'_p}\big) \\
&= \left(1 + \tfrac{p^{r+s}}{2}\right)^p - \left(1 + \tfrac{p^{r+s+1}}{2}\right) \pm p^{s+1}\sqrt{\Delta_V} \times \left(\left(1 + \tfrac{p^{r+s}}{2}\right)^{p-1} - 1\right) \;+\; O\big(p^{2s+1+\delta'_p}\big).
\end{aligned}$$

It follows that $\frac{\lambda_{V,+}^p + \lambda_{V,-}^p}{2} = 1 + \frac{p^{s+r+1}}{2} + O\big(p^{2s+2r+1}\big)$ and $\frac{\lambda_{V,+}^p - \lambda_{V,-}^p}{2\sqrt{\Delta_V}} = p^{s+1} + O\big(p^{2s+r+1}\big)$ upon using the condition $\delta'_p \geq 2r$, so by induction:

$$\frac{\lambda_{V,+}^{p^i} + \lambda_{V,-}^{p^i}}{2} = 1 + \frac{p^{s+r+i}}{2} + O\big(p^{2s+2r+i}\big) \quad \text{and} \quad \frac{\lambda_{V,+}^{p^i} - \lambda_{V,-}^{p^i}}{2\sqrt{\Delta_V}} = p^{s+i} + O\big(p^{2s+r+i}\big). \qquad (4.6)$$

- Alternatively, if $r \geq \mathrm{ord}_p(\sqrt{\Delta_V})$ then

$$\Big(\frac{p^r}{2} \pm \sqrt{\Delta_V}\Big)^j \;=\; \Big(\pm\sqrt{\Delta_V}\Big)^j + \frac{jp^r}{2}\Big(\pm\sqrt{\Delta_V}\Big)^{j-1} + O\big(p^{\delta_p'(j-2)/2+2r}\big)$$

and arguing in an identical fashion to before, one deduces that

$$\frac{\lambda_{V,+}^{p^i} + \lambda_{V,-}^{p^i}}{2} = 1 + \frac{p^{s+r+i}}{2} + O\big(p^{2s+\delta_p'+i}\big) \quad \text{and} \quad \frac{\lambda_{V,+}^{p^i} - \lambda_{V,-}^{p^i}}{2\sqrt{\Delta_V}} = p^{s+i} + O\big(p^{2s+\delta_p'/2+i}\big). \tag{4.7}$$

Again as $\chi = \chi_{1,n}^{\mathbf{e}_1} \times \chi_{2,n}^{\mathbf{e}_2}$, this time Equation (4.5) implies

$$\chi\left(\gamma^{-p^i}(h_1^x h_2^y)\gamma^{p^i}\right) \;=\; \zeta_{p^n}^{\left(\mathbf{e}_1\left(\frac{\lambda_{V,+}^{p^i}+\lambda_{V,-}^{p^i}}{2} - \frac{\lambda_{V,+}^{p^i}-\lambda_{V,-}^{p^i}}{2\sqrt{\Delta_V}}\times\frac{p^r}{2}\right)+\mathbf{e}_2 d\left(\frac{\lambda_{V,+}^{p^i}-\lambda_{V,-}^{p^i}}{2\sqrt{\Delta_V}}\right)\right)x} \\ \times\ \zeta_{p^n}^{\left(\mathbf{e}_1\left(\frac{\lambda_{V,+}^{p^i}-\lambda_{V,-}^{p^i}}{2\sqrt{\Delta_V}}\right)+\mathbf{e}_2\left(\frac{\lambda_{V,+}^{p^i}+\lambda_{V,-}^{p^i}}{2} + \frac{\lambda_{V,+}^{p^i}-\lambda_{V,-}^{p^i}}{2\sqrt{\Delta_V}}\times\frac{p^r}{2}\right)\right)y}.$$

Exploiting our eigenvalue estimates in Equations (4.6) and (4.7) appropriately, it follows that $\chi\left(\gamma^{-p^i}(h_1^x h_2^y)\gamma^{p^i}\right)$ equals $\chi(h_1^x h_2^y) = \zeta_{p^n}^{\mathbf{e}_1 x + \mathbf{e}_2 y}$ for all $x, y \in \mathbb{Z}$, if and only if

$$\mathbf{e}_2 d \times p^{s+i} \equiv 0 \ (\bmod\ p^n) \quad \text{and} \quad \mathbf{e}_1 \times p^{s+i} + \mathbf{e}_2 \times p^{s+i+r} \equiv 0 \ (\bmod\ p^n);$$

the latter holds precisely when

$$s + i \;\geq\; n - \mathrm{ord}_p(\mathbf{e}_2 d) \quad \text{and} \quad s + i \;\geq n - \mathrm{ord}_p(\mathbf{e}_1 + \mathbf{e}_2 p^r).$$

Case (VI). Here $I_2 + M = \begin{pmatrix} 1 & p^s \\ p^{s+r}t & 1 \end{pmatrix}$; let $\lambda_{VI,\pm} := 1 \pm p^s\sqrt{p^r t}$ be its eigenvalues (note that $t = 1$ in (a) of the Classification Theorem, and $t \in \mathbb{Z}_p^\times$ is not a square in (b)). Then

$$(I_2{+}M)^{p^i} = P_{VI} D_{VI}^{p^i} P_{VI}^{-1} \quad \text{with} \ \ D_{VI} = \begin{pmatrix} \lambda_{VI,+} & 0 \\ 0 & \lambda_{VI,-} \end{pmatrix} \text{and } P_{VI} = \begin{pmatrix} 1 & 1 \\ \sqrt{p^r t} & -\sqrt{p^r t} \end{pmatrix}.$$

A straightforward calculation shows

$$\begin{aligned}
\gamma^{-p^i}\left(h_1^x h_2^y\right)\gamma^{p^i} &= \begin{pmatrix} 1 & p^s \\ p^{s+r}t & 1 \end{pmatrix}^{p^i} \begin{pmatrix} x \\ y \end{pmatrix} \\
&= \begin{pmatrix} 1 & 1 \\ \sqrt{p^r t} & -\sqrt{p^r t} \end{pmatrix} \begin{pmatrix} \lambda_{VI,+} & 0 \\ 0 & \lambda_{VI,-} \end{pmatrix}^{p^i} \begin{pmatrix} 1 & 1 \\ \sqrt{p^r t} & -\sqrt{p^r t} \end{pmatrix}^{-1} \begin{pmatrix} x \\ y \end{pmatrix} \\
&= \begin{pmatrix} \frac{\lambda_{VI,+}^{p^i}+\lambda_{VI,-}^{p^i}}{2} & \frac{\lambda_{VI,+}^{p^i}-\lambda_{VI,-}^{p^i}}{2\sqrt{p^r t}} \\ \sqrt{p^r t}\frac{\lambda_{VI,+}^{p^i}-\lambda_{VI,-}^{p^i}}{2} & \frac{\lambda_{VI,+}^{p^i}+\lambda_{VI,-}^{p^i}}{2} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \\
&= h_1^{\left(\frac{\lambda_{VI,+}^{p^i}+\lambda_{VI,-}^{p^i}}{2}\right)x+\left(\frac{\lambda_{VI,+}^{p^i}-\lambda_{VI,-}^{p^i}}{2\sqrt{p^r t}}\right)y} \times h_2^{\sqrt{p^r t}\left(\frac{\lambda_{VI,+}^{p^i}-\lambda_{VI,-}^{p^i}}{2}\right)x+\left(\frac{\lambda_{VI,+}^{p^i}+\lambda_{VI,-}^{p^i}}{2}\right)y}
\end{aligned} \tag{4.8}$$

and clearly $\lambda_{V,\pm}^p = 1 \pm p^{s+1}\sqrt{p^r t} + p^{2s+1}\left(\frac{p-1}{2}\right)p^r t + \ldots = 1 \pm p^{s+1}\sqrt{p^r t} + O\left(p^{2s+r+1}\right)$. Using a now familiar mathematical induction,

$$\frac{\lambda_{VI,+}^{p^i}+\lambda_{VI,-}^{p^i}}{2} = 1+O\left(p^{2s+r+i}\right) \quad \text{and} \quad \frac{\lambda_{VI,+}^{p^i}-\lambda_{VI,-}^{p^i}}{2\sqrt{p^r t}} = p^{s+i}+O\left(p^{2s+r/2+i}\right). \tag{4.9}$$

If the character $\chi = \chi_{1,n}^{\mathbf{e}_1} \times \chi_{2,n}^{\mathbf{e}_2}$, by Equation (4.8) the value $\chi\left(\gamma^{-p^i}(h_1^x h_2^y)\gamma^{p^i}\right)$ equals

$$\zeta_{p^n}^{\left(\mathbf{e}_1\left(\frac{\lambda_{VI,+}^{p^i}+\lambda_{VI,-}^{p^i}}{2}\right)+\mathbf{e}_2\sqrt{p^r t}\left(\frac{\lambda_{VI,+}^{p^i}-\lambda_{VI,-}^{p^i}}{2}\right)\right)x+\left(\mathbf{e}_1\left(\frac{\lambda_{VI,+}^{p^i}-\lambda_{VI,-}^{p^i}}{2\sqrt{p^r t}}\right)+\mathbf{e}_2\left(\frac{\lambda_{VI,+}^{p^i}+\lambda_{VI,-}^{p^i}}{2}\right)\right)y}.$$

Plugging Equation (4.9) into the above, one can then deduce $\chi\left(\gamma^{-p^i}(h_1^x h_2^y)\gamma^{p^i}\right) = \chi\left(h_1^x h_2^y\right)$ for all $x, y \in \mathbb{Z}$, if and only if both

$$\mathbf{e}_2 \times p^{s+i} \times \left(\sqrt{p^r t}\right)^2 \equiv 0 \pmod{p^n} \quad \text{and} \quad \mathbf{e}_1 \times p^{s+i} \equiv 0 \pmod{p^n},$$

which is itself equivalent to ensuring that

$$s+i \;\geq\; n - \mathrm{ord}_p(\mathbf{e}_2 p^r t) = n - r - \mathrm{ord}_p(\mathbf{e}_2) \quad \text{and} \quad s+i \;\geq\; n - \mathrm{ord}_p(\mathbf{e}_1).$$

□

4.1.2 How to choose a "good system" of subgroups

The theory in [CSRV12, Har10, Kak13, RW06] operates best in the setting of one-dimensional Lie groups. Throughout we choose an integer n, and work with the p-adic group $\mathcal{G}_{\infty,n} := \Gamma \ltimes \left(\frac{\mathcal{H}_\infty}{\mathcal{H}_\infty^{p^n}}\right)$. In later sections we will allow n to vary, but for the time being n is fixed.

Lemma 4.3 *If $\mathcal{Z}(G)$ denotes the centre of a group G, then*

$$\mathcal{Z}(\mathcal{G}_{\infty,n}) \;=\; \begin{cases} \Gamma^{p^{n-s}} \times \frac{\mathcal{H}_{1,\infty}\times\mathcal{H}_{2,\infty}^{p^{n-s}}}{\mathcal{H}_\infty^{p^n}} & \textit{in Case (II)} \\ \Gamma^{p^{n-s}} \times \frac{\mathcal{H}_\infty^{p^{n-s}}}{\mathcal{H}_\infty^{p^n}} & \textit{in Cases (III) and (IV)} \\ \Gamma^{p^{n-s}} \times \frac{\mathcal{H}_{1,\infty}^{p^{n-s}}\times\mathcal{H}_{2,\infty}^{p^{n-s-r}}}{\mathcal{H}_\infty^{p^n}} & \textit{in Case (V)} \\ \Gamma^{p^{n-s}} \times \frac{\mathcal{H}_{1,\infty}^{p^{n-s-r-\mathrm{ord}_p(t)}}\times\mathcal{H}_{2,\infty}^{p^{n-s}}}{\mathcal{H}_\infty^{p^n}} & \textit{in Case (VI).} \end{cases}$$

In particular, $\mathcal{Z}(\mathcal{G}_\infty) \cong \varprojlim_n \mathcal{Z}(\mathcal{G}_{\infty,n}) = \begin{cases} \mathcal{H}_{1,\infty} & \textit{in Case (II)} \\ \{1\} & \textit{otherwise.} \end{cases}$

Proof. We first note from the semi-direct product structure on $\mathcal{G}_{\infty,n}$ that

$$\mathcal{Z}(\mathcal{G}_{\infty,n}) \;=\; \mathrm{Stab}_\Gamma\left(\frac{\mathcal{H}_\infty}{\mathcal{H}_\infty^{p^n}}\right)\times\frac{\left\{h_1^x h_2^y \,\middle|\, (I_2+M)\begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} x \\ y \end{pmatrix} \mod p^n\mathbb{Z}_p^2\right\}}{\mathcal{H}_\infty^{p^n}}.$$

One then computes the right-hand side on a case-by-case basis, using the form of the matrix M listed in Equation (4.1), as follow.

Firstly in Case (II), one has

$$(I_2+M)\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & p^s \\ 0 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x+p^s y \\ y \end{pmatrix},$$

so the congruence $(I_2+M)\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}$ (mod p^n) holds if and only if $y \equiv 0$ (mod p^{n-s}).

In Case (III),

$$(I_2+M)\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1+p^s & 0 \\ 0 & 1+p^s \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} (1+p^s)x \\ (1+p^s)y \end{pmatrix}$$

and the condition $\begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} \pmod{p^{n-s}}$ ensures that $(I_2 + M) \begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} x \\ y \end{pmatrix} \pmod{p^n}$.

In Case (IV),

$$(I_2 + M) \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1+p^s & p^{s+r} \\ p^{s+r}d & 1+p^s \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + p^s x + p^{s+r} y \\ y + p^s y + p^{s+r} dx \end{pmatrix}.$$

Therefore, we deduce that $(I_2 + M) \begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} x \\ y \end{pmatrix} \pmod{p^n}$ if and only if $\begin{pmatrix} x + p^r y \\ y + p^r dx \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} \pmod{p^{n-s}}$. Since $x + p^r y \equiv 0 \pmod{p^{n-s}}$ and $y + p^r dx \equiv 0 \pmod{p^{n-s}}$, we may write

$$x = kp^{n-s} - p^r y \quad \text{for some integer } k,$$

in which case

$$\begin{aligned} y + p^r dx &= y + p^r d(kp^{n-s} - p^r y) = y - p^{2r} dy + kp^r dp^{n-s} \\ &\equiv y - p^{s+r} dy \pmod{p^{n-s}} \equiv (1 - p^{2r} d) y \equiv 0 \pmod{p^{n-s}}. \end{aligned}$$

Lastly because $1 - p^{2r} d$ is invertible, one concludes that $y \equiv 0 \pmod{p^{n-s}}$.

Next in Case (V),

$$\begin{aligned} (I_2 + M) \begin{pmatrix} x \\ y \end{pmatrix} &= \begin{pmatrix} 1 & p^s \\ p^s d & 1 + p^{s+r} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \\ &= \begin{pmatrix} x + p^s y \\ y + p^s dx + p^{s+r} y \end{pmatrix} \end{aligned}$$

and therefore one deduces that $(I_2 + M) \begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} x \\ y \end{pmatrix} \pmod{p^n}$ if and only if $\begin{pmatrix} y \\ dx + p^r y \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} \pmod{p^{n-s}}$. The later is equivalent to $x \equiv 0 \pmod{p^{n-s-ord_p(d)}}$ and $y \equiv 0 \pmod{p^{n-s}}$.

Finally in Case (VI),

$$(I_2+M)\begin{pmatrix}x\\ y\end{pmatrix} = \begin{pmatrix}1 & p^s\\ p^{s+r}t & 1\end{pmatrix}\begin{pmatrix}x\\ y\end{pmatrix} = \begin{pmatrix}x+p^sy\\ p^{s+r}tx+y\end{pmatrix}$$

Hence, $(I_2+M)\begin{pmatrix}x\\ y\end{pmatrix} \equiv \begin{pmatrix}x\\ y\end{pmatrix} \pmod{p^n}$ is equivalent to the congruence $\begin{pmatrix}y\\ p^rtx\end{pmatrix} \equiv \begin{pmatrix}0\\ 0\end{pmatrix} \pmod{p^{n-s}}$, and this becomes $x \equiv 0 \pmod{p^{n-s-r-ord_p(t)}}$ and $y \equiv 0 \pmod{p^{n-s}}$. □

Bearing in mind Kakde's subgroups should always contain the centre of $\mathcal{G}_{\infty,n}$, we define

$$\mathcal{U}_{m,n} \ := \ \Gamma^{p^m} \ltimes \left(\frac{\mathcal{H}_\infty}{\mathcal{H}_\infty^{p^n}}\right) \qquad \text{where the integer } m \in \{0,\dots,n-s\},$$

so: (i) $\mathcal{Z}(\mathcal{G}_{\infty,n}) \subset \mathcal{U}_{m,n}$, and (ii) $\Gamma^{p^{n-s}} \subset \mathrm{Stab}_\Gamma(\chi)$ for any $\chi : \mathcal{H}_\infty \twoheadrightarrow \mu_{p^m}$ by Proposition 4.2. It follows that such χ extend to $\mathcal{U}_{m,n}$ if $m \in \{\mathbf{m}_\chi,\dots,n-s\}$, and will thus factor through

$$\mathcal{U}_{m,n}^{\mathrm{ab}} \ = \ \frac{\mathcal{U}_{m,n}}{[\mathcal{U}_{m,n},\mathcal{U}_{m,n}]} \ = \ \frac{\Gamma^{p^m} \ltimes \mathcal{H}_\infty/\mathcal{H}_\infty^{p^n}}{\left\langle \left[h_1^x h_2^y \mod \mathcal{H}_\infty^{p^n},\ \gamma^{p^m}\right] \,\middle|\, x,y\in\mathbb{Z}\right\rangle}.$$

Therefore, by determining the nature of $\mathcal{U}_{m,n}^{\mathrm{ab}}$ in each case, we may calculate the number of irreducible representations $\psi \otimes \mathrm{Ind}_{\mathcal{U}_{m,n}}^{\mathcal{G}_{\infty,n}}(\chi)$ with $\psi : \Gamma \to \mathbb{C}^\times$ of finite order. (Remember that every irreducible Artin representation ρ on $\mathcal{G}_\infty$ is of this form for suitable m, n, χ, ψ.)

Proposition 4.4 *For each pair $m,n \in \mathbb{Z}$ with $0 \le m \le n-s$,*

$$\mathcal{U}_{m,n}^{\mathrm{ab}} \ \cong \ \begin{cases} \Gamma^{p^m} \times \frac{\mathcal{H}_{1,\infty}}{\mathcal{H}_{1,\infty}^{p^{s+m}}} \times \frac{\mathcal{H}_{2,\infty}}{\mathcal{H}_{2,\infty}^{p^n}} & \textit{in Case (II)} \\ \mathcal{U}_{m,s+m} & \textit{in Cases (III) and (IV)} \\ \Gamma^{p^m} \times \frac{\mathbb{Z}}{p^{\min\{n,s+m+\mathrm{ord}_p(d)\}}\mathbb{Z}} \times \frac{\mathbb{Z}}{p^{s+m}\mathbb{Z}} & \textit{in Case (V)} \\ \Gamma^{p^m} \times \frac{\mathbb{Z}}{p^{\min\{n,s+m+r+\mathrm{ord}_p(t)\}}\mathbb{Z}} \times \frac{\mathbb{Z}}{p^{s+m}\mathbb{Z}} & \textit{in Case (VI);} \end{cases}$$

in fact, the first two lines are actual equalities, not just isomorphisms.

Proof. We proceed by working through the different cases (II)–(VI) in numerical order.

Case (II). Here one simply exploits the commutator relation $\left[h_1^x h_2^y, \gamma^{p^m}\right] = (h_1^y)^{p^{s+m}}$.

Case (III). Here we use the relation $\left[h_1^x h_2^y, \gamma^{p^m}\right] = (h_1^x h_2^y)^{(1+p^s)^{p^m}-1}$ and the fact that $\mathrm{ord}_p\big((1+p^s)^{p^m}\!-1\big) = s+m$.

Case (IV). Recall from Equation 4.2 that

$$\begin{aligned}\gamma^{-p^m}(h_1^x h_2^y)\gamma^{p^m} \;&=\; h_1^{\left(\frac{\lambda_{IV,+}^{p^m}+\lambda_{IV,-}^{p^m}}{2}\right)x+\left(\frac{\lambda_{IV,+}^{p^m}-\lambda_{IV,-}^{p^m}}{2\sqrt{d}}\right)y} \times h_2^{\left(\frac{\lambda_{IV,+}^{p^m}-\lambda_{IV,-}^{p^m}}{2}\right)\sqrt{d}\,x+\left(\frac{\lambda_{IV,+}^{p^m}+\lambda_{IV,-}^{p^m}}{2}\right)y} \\ &=\; \left(h_1^{p^{s+m}+\dots} \times h_2^{p^{s+r+m}d+\dots}\right)^x \times \left(h_1^{p^{s+r+m}+\dots} \times h_2^{p^{s+m}+\dots}\right)^y \times h_1^x h_2^y\end{aligned}$$

upon using the estimates in (4.3) and (4.4); consequently

$$\frac{\mathcal{H}_\infty}{\left\langle [h_1,\gamma^{p^m}],[h_2,\gamma^{p^m}]\right\rangle} \cong \frac{\mathbb{Z}_p \,\oplus\, \mathbb{Z}_p}{\mathbb{Z}_p\cdot\left\{(p^{s+m}+\dots\;,p^{s+r+m}d+\dots),(p^{s+r+m}+\dots\;,p^{s+m}+\dots)\right\}}$$

which means $\mathcal{U}_{m,n}^{\mathrm{ab}} = \frac{\mathcal{U}_{m,n}}{\left\langle[h_1,\gamma^{p^m}],[h_2,\gamma^{p^m}]\right\rangle} \cong \Gamma^{p^m}\times\frac{\mathbb{Z}_p}{p^{s+m}\mathbb{Z}_p}\times\frac{\mathbb{Z}_p}{p^{s+m}\mathbb{Z}_p}$.

Case (V). This time Equation (4.5) combined with the estimates (4.6) and (4.7) yields

$$\begin{aligned}\gamma^{-p^m}(h_1^x h_2^y)\gamma^{p^m} \;&=\; h_1^{\left(\frac{\lambda_{V,+}^{p^m}+\lambda_{V,-}^{p^m}}{2}-\frac{\lambda_{V,+}^{p^m}-\lambda_{V,-}^{p^m}}{2\sqrt{\Delta_V}}\times\frac{p^r}{2}\right)x+\left(\frac{\lambda_{V,+}^{p^m}-\lambda_{V,-}^{p^m}}{2\sqrt{\Delta_V}}\right)y} \\ &\qquad\times h_2^{\left(\frac{\lambda_{V,+}^{p^m}-\lambda_{V,-}^{p^m}}{2\sqrt{\Delta_V}}\right)dx+\left(\frac{\lambda_{V,+}^{p^m}+\lambda_{V,-}^{p^m}}{2}+\frac{\lambda_{V,+}^{p^m}-\lambda_{V,-}^{p^m}}{2\sqrt{\Delta_V}}\times\frac{p^r}{2}\right)y} \\ &=\; \left(h_1^{\frac{p^{s+r+m}}{2}-\frac{p^{s+r+m}}{2}+\dots} \times h_2^{p^{s+m}d+\dots}\right)^x \times \left(h_1^{p^{s+m}+\dots} \times h_2^{\frac{p^{s+r+m}}{2}+\frac{p^{s+r+m}}{2}+\dots}\right)^y \times h_1^x h_2^y\end{aligned}$$

so that $\mathcal{U}_{m,n}^{\mathrm{ab}} = \frac{\mathcal{U}_{m,n}}{\left\langle[h_1,\gamma^{p^m}],[h_2,\gamma^{p^m}]\right\rangle} \cong \Gamma^{p^m}\times\frac{\mathbb{Z}_p}{p^n\mathbb{Z}_p\cup\, p^{s+m}d\mathbb{Z}_p}\times\frac{\mathbb{Z}_p}{p^{s+m}\mathbb{Z}_p}$.

Case (VI). Lastly, Equation (4.8) in tandem with the estimates in (4.9) implies

$$\begin{aligned}\gamma^{-p^m}(h_1^x h_2^y)\gamma^{p^m} = h_1^{\left(\frac{\lambda_{VI,+}^{p^m}+\lambda_{VI,-}^{p^m}}{2}\right)x+\left(\frac{\lambda_{VI,+}^{p^m}-\lambda_{VI,-}^{p^m}}{2\sqrt{p^r t}}\right)y} \times h_2^{\sqrt{p^r t}\left(\frac{\lambda_{VI,+}^{p^m}-\lambda_{VI,-}^{p^m}}{2}\right)x+\left(\frac{\lambda_{VI,+}^{p^m}+\lambda_{VI,-}^{p^m}}{2}\right)y} \\ =\; \left(h_1^{0+\dots} \times h_2^{p^{s+m+r}t+\dots}\right)^x \times \left(h_1^{p^{s+m}+\dots} \times h_2^{0+\dots}\right)^y \times h_1^x h_2^y\;,\end{aligned}$$

hence $\mathcal{U}_{m,n}^{\mathrm{ab}} = \frac{\mathcal{U}_{m,n}}{\left\langle[h_1,\gamma^{p^m}],[h_2,\gamma^{p^m}]\right\rangle} \cong \Gamma^{p^m}\times\frac{\mathbb{Z}_p}{p^n\mathbb{Z}_p\cup\, p^{s+m+r}t\mathbb{Z}_p}\times\frac{\mathbb{Z}_p}{p^{s+m}\mathbb{Z}_p}$. □

We remark in Cases (II-VI), each $\mathcal{U}_{m,n}^{\mathrm{ab}}$ has the form $\Gamma^{p^m}\times\overline{\mathcal{H}}_\infty^{(m,n)}$ where $\overline{\mathcal{H}}_\infty^{(m,n)}$ is obtained from quotienting $\mathcal{H}_\infty/\mathcal{H}_\infty^{p^n} = \langle\overline{h}_1,\overline{h}_2\rangle$ with the subgroup generated by $\left\{[\overline{h}_1,\gamma^{p^m}],[\overline{h}_2,\gamma^{p^m}]\right\}$.

Definition 4.1 *Let " $\mathrm{orb}_\Gamma\big(\overline{\mathcal{H}}_\infty^{(m,n)}\big)$ " denote the orbits under the action of Γ/Γ^{p^m} in $\overline{\mathcal{H}}_\infty^{(m,n)}$. In particular, if $\overline{h} \in \overline{\mathcal{H}}_\infty^{(m,n)}$ then $\varpi_{\overline{h}} \in \mathrm{orb}_\Gamma\big(\overline{\mathcal{H}}_\infty^{(m,n)}\big)$ consists of the set $\big\{\gamma^{-i}\overline{h}\gamma^i \;\big|\; i \in \mathbb{Z}\big\}$; we shall sometimes abuse notation, and write $\overline{h}$ in place of $\varpi_{\overline{h}}$.*

4.1.3 Maps between the abelianizations of $\mathcal{U}_{m,n}$

We now outline the various mappings that appear in the description of Ψ and Φ in [CSRV12, Kak13]. Rather than give their full definitions, we specialise them to the specific three-dimensional situation we are considering.

The conditions (A1)-(A3) and (M1)-(M4) in the exposition [CSRV12, p79-123] degenerate into some fairly simple rules, which can be expressed in terms of an explicit basis for the image of Kakde's map "$\sigma_U^{N(U)}$". In subsequent sections we will then study how these expressions transform, once the completed group algebras $\Lambda\big(\mathcal{U}_{m,n}^{\mathrm{ab}}\big)$ are evaluated at a system of characters χ on $\mathcal{H}_\infty$.

The mapping σ_m: Note that the normaliser of each subgroup $U = \mathcal{U}_{m,n} \subset \mathcal{G}_{\infty,n}$ is the whole of $\mathcal{G}_{\infty,n}$, so the $\mathbb{Z}_p$-linear map labelled $\sigma_U^{N(U)}$ in [CSRV12, p85] becomes

$$\sigma_{\mathcal{U}_{m,n}}^{\mathcal{G}_{\infty,n}} : \Lambda\big(\mathcal{U}_{m,n}^{\mathrm{ab}}\big) \longrightarrow \Lambda\big(\mathcal{U}_{m,n}^{\mathrm{ab}}\big) \quad \text{where } f \mapsto \sum_{i=0}^{p^m-1} \gamma^{-i} f \gamma^i.$$

If we use the shorthand σ_m for this linear mapping, clearly $\sigma_m(f) \in H^0\left(\Gamma, \Lambda\big(\mathcal{U}_{m,n}^{\mathrm{ab}}\big)\right)$ corresponds to the sum over the orbits of f under the action of the finite group Γ/Γ^{p^m}.

Definition 4.2 *For any $\overline{h} = h_1^x h_2^y \mod \big[\mathcal{U}_{m,n}, \mathcal{U}_{m,n}\big]$, one defines $\mathcal{A}_{\overline{h}}^{(m,n)} \in \mathbb{Z}_p\big[\mathcal{U}_{m,n}^{\mathrm{ab}}\big]$ by*

$$\mathcal{A}_{\overline{h}}^{(m,n)} := \sum_{i=0}^{p^m-1} \overline{h}_1^{x_i}\overline{h}_2^{y_i} \quad \textit{where} \begin{pmatrix} x_i \\ y_i \end{pmatrix} \equiv (I_2 + M)^i \begin{pmatrix} x \\ y \end{pmatrix} \mod p^n.$$

In fact, we could alternatively have defined $\mathcal{A}_{\overline{h}}^{(m,n)}$ to be equal to the summation $\sum_{i=0}^{p^m-1} \gamma^{-i}\overline{h}\gamma^i$ which coincides, of course, with $\sigma_m(\overline{h})$; we will see that these form a basis for $\mathrm{Im}(\sigma_m)$.

Proposition 4.5 *(i) Each element $\mathcal{A}_{\overline{h}}^{(m,n)}$ depends only on the Γ-orbit of $\overline{h}$ inside $\overline{\mathcal{H}}_\infty^{(m,n)}$;*

(ii) The image of σ_m is freely generated over $\mathbb{Z}_p\big[\big[\Gamma^{p^m}\big]\big]$ by the $\mathcal{A}_{\overline{h}}^{(m,n)}$'s, in other words

$$\mathrm{Im}\big(\sigma_m\big) \;\cong\; \mathbb{Z}_p\big[\big[\Gamma^{p^m}\big]\big] \otimes_{\mathbb{Z}_p} \mathbb{Z}_p\left\{\mathcal{A}_{\overline{h}}^{(m,n)} \;\middle|\; \overline{h} = h_1^x h_2^y \mod \big[\mathcal{U}_{m,n}, \mathcal{U}_{m,n}\big]\right\};$$

(iii) If $r_{\sigma_m}^{(n)} := \mathrm{rank}_{\mathbb{Z}_p[\![\Gamma^{p^m}]\!]}\big(\mathrm{Im}(\sigma_m)\big)$, then

$$r_{\sigma_m}^{(n)} \;=\; \begin{cases} p^{n+s-1} \times (mp + p - m) & \textit{in Case (II)} \\ p^{2s-1} \times (p^{m+1} + p^m - 1) & \textit{in Cases (III) and (IV)} \\ p^{\min\{n-m, s+\mathrm{ord}_p(d)\}+s-1} \times (p^{m+1} + p^m - 1) & \textit{in Case (V)} \\ p^{\min\{n-m, s+r+\mathrm{ord}_p(t)\}+s-1} \times (p^{m+1} + p^m - 1) & \textit{in Case (VI).} \end{cases}$$

Proof. Let $\overline{h} = h_1^x h_2^y \mod [\mathcal{U}_{m,n}, \mathcal{U}_{m,n}]$, and put $\overline{h}' = \gamma^{-j}\overline{h}\gamma^j$ for some fixed j, so that $\overline{h}'$ has the same Γ-orbit as $\overline{h}$. By definition,

$$\mathcal{A}_{\overline{h}'}^{(m,n)} = \sum_{i=0}^{p^m-1} \gamma^{-i}\overline{h}'\gamma^i = \sum_{i=0}^{p^m-1} \gamma^{-i}\gamma^{-j}\overline{h}\gamma^j\gamma^i = \sum_{i=0}^{p^m-1} \gamma^{-(i+j)}\overline{h}\gamma^{i+j}$$

so that

$$\mathcal{A}_{\overline{h}}^{(m,n)} = \sum_{i=0}^{p^m-1} \gamma^{-i}\overline{h}\gamma^i = \sum_{i=0}^{p^m-1} \gamma^{-(i+j)}\overline{h}\gamma^{i+j} = \mathcal{A}_{\overline{h}'}^{(m,n)},$$

which completes the proof for part (i).

To establish (ii), first note that $\mathcal{U}_{m,n}^{\mathrm{ab}} = \Gamma^{p^m} \times \overline{\mathcal{H}}_\infty^{(m,n)}$ where $\overline{\mathcal{H}}_\infty^{(m,n)}$ is the previous quotient of $\mathcal{H}_\infty$ equipped with the action of the group $\Gamma\big/\Gamma^{p^m}$; part (ii) now follows because $\overline{\mathcal{H}}_\infty^{(m,n)}$ is generated by $h_1^x h_2^y \mod \big[\mathcal{U}_{m,n}, \mathcal{U}_{m,n}\big]$ for $x, y \in \mathbb{Z}$.

Finally, to prove (iii) we just need to count the number of distinct $\mathcal{A}_{\overline{h}}^{(m,n)}$'s, which coincides with the total number of $\big(\Gamma/\Gamma^{p^m}\big)$-orbits inside $\overline{\mathcal{H}}_\infty^{(m,n)}$. In fact by Burnside's lemma,

$$\#\big\{\Gamma\text{-orbits in } \overline{\mathcal{H}}_\infty^{(m,n)}\big\} \;=\; \#\big(\Gamma/\Gamma^{p^m}\big)^{-1} \times \sum_{j=1}^{p^m} \#\left\{\overline{h} \in \overline{\mathcal{H}}_\infty^{(m,n)} \;\middle|\; \gamma^{-j}\overline{h}\gamma^j = \overline{h}\right\}.$$

From Proposition 4.4, in each case $\star \in \{\text{II,III,IV,V,VI}\}$ one knows

$$\overline{\mathcal{H}}_\infty^{(m,n)} \cong \frac{\mathbb{Z}}{p^{N_{\star,1}^{(m)}}\mathbb{Z}} \times \frac{\mathbb{Z}}{p^{N_{\star,2}^{(m)}}\mathbb{Z}}$$

where $N^{(m)}_{\star,1}, N^{(m)}_{\star,2} \in \mathbb{N}$ satisfy $m+s \le N^{(m)}_{\star,1} \le n$ and $m+s \le N^{(m)}_{\star,2} \le n$ in all five scenarios.

- If $\star = \mathrm{II}$ then γ acts trivially on the first direct factor in $\overline{\mathcal{H}}^{(m,n)}_{\infty}$, whence

$$\begin{aligned}
\#\big\{\Gamma\text{-orbits in } \overline{\mathcal{H}}^{(m,n)}_{\infty}\big\} &= p^{-m} \times \sum_{j=1}^{p^m} p^{N^{(m)}_{II,1}} \times p^{N^{(m)}_{II,2}+\mathrm{ord}_p(j)-m} \\
&= p^{-m} \times \sum_{j=1}^{p^m} p^{s+m} \times p^{n+\mathrm{ord}_p(j)-m} = p^{n+s-m} \times \sum_{j=0}^{p^m-1} p^{\mathrm{ord}_p(j)} \\
&= p^{n+s-m} \times \Big((p^0 \cdot \varphi(p^m) + p^1 \cdot \varphi(p^{m-1}) + \cdots + p^{m-1} \cdot \varphi(p^1) + p^m) \Big) \\
&= p^{n+s-m} \times p^{m-1}(mp - m + p) = p^{n+s-1} \times (mp + p - m).
\end{aligned}$$

- Assuming that $\star \neq \mathrm{II}$, one discovers that

$$\#\big\{\Gamma\text{-orbits in } \overline{\mathcal{H}}^{(m,n)}_{\infty}\big\} \;=\; p^{-m} \times \sum_{j=1}^{p^m} p^{N^{(m)}_{\star,1}+\mathrm{ord}_p(j)-m} \times p^{N^{(m)}_{\star,2}+\mathrm{ord}_p(j)-m}$$

Now in Cases (III) and (IV), $N^{(m)}_{II,1} = s+m$ and $N^{(m)}_{II,2} = s+m$, and it follows that

$$\begin{aligned}
\#\big\{\Gamma\text{-orbits in } \overline{\mathcal{H}}^{(m,n)}_{\infty}\big\} &= p^{-m} \times \sum_{j=1}^{p^m} p^{s+m+\mathrm{ord}_p(j)-m} \times p^{s+m+\mathrm{ord}_p(j)-m} \\
&= p^{2s-m} \times \sum_{j=0}^{p^m-1} p^{2\mathrm{ord}_p(j)} \\
&= p^{2s-m} \times \Big(p^0 \cdot \varphi(p^m) + p^2 \cdot \varphi(p^{m-1}) + \cdots + p^{2(m-1)} \cdot \varphi(p^1) + p^{2m} \Big) \\
&= p^{2s-1} \times (p^{m+1} + p^m - 1).
\end{aligned}$$

Similarly, one can also determine that the $\#\big\{\Gamma\text{-orbits in } \overline{\mathcal{H}}^{(m,n)}_{\infty}\big\}$ in Cases (V) and Case (VI) are

$$p^{\min\{n, s+m+\mathrm{ord}_p(d)\}+s-m-1} \times (p^{m+1} + p^m - 1)$$

and

$$p^{\min\{n, s+m+r+\mathrm{ord}_p(t)\}+s-m-1} \times (p^{m+1} + p^m - 1)$$

respectively. So, we conclude that for $\star \neq \mathrm{II}$,

$$\#\big\{\Gamma\text{-orbits in } \overline{\mathcal{H}}^{(m,n)}_{\infty}\big\} \;=\; p^{\left(N^{(m)}_{\star,1}-m\right)+\left(N^{(m)}_{\star,2}-m\right)-1} \times \left(p^{m+1} + p^m - 1\right)$$

where $N^{(m)}_{\star,1}$ and $N^{(m)}_{\star,2}$ can be read off from Proposition 4.4. □

Corollary 4.6 *The number of irreducible representations of the form* $\mathrm{Ind}^{\mathcal{G}_{\infty,n}}_{\mathrm{Stab}_\Gamma(\chi)\ltimes\mathcal{H}_\infty/p^n}(\chi)$ *where* χ *factors through* $\overline{\mathcal{H}}^{(m,n)}_\infty$ *but not through* $\overline{\mathcal{H}}^{(m-1,n)}_\infty$ *is given by* $r^{(n)}_{\sigma_m}-r^{(n)}_{\sigma_{m-1}}$.

Proof. Note that any two characters χ,χ' as above induce the same $\mathcal{G}_{\infty,n}$-representation, if and only if χ' belongs to the Γ-orbit of χ inside $\mathrm{Hom}\big(\overline{\mathcal{H}}^{(m,n)}_\infty,\mathbb{C}^\times\big)$; since the latter group is (non-canonically) isomorphic to $\overline{\mathcal{H}}^{(m,n)}_\infty$, its Γ-orbits are in one-to-one correspondence with the finite set $\mathrm{orb}_\Gamma\big(\overline{\mathcal{H}}^{(m,n)}_\infty\big)$. It follows immediately that

$$\text{“the no. of Ind}(\chi)\text{'s primitive on } \overline{\mathcal{H}}^{(m,n)}_\infty\text{ ”} \;=\; \#\mathrm{orb}_\Gamma\big(\overline{\mathcal{H}}^{(m,n)}_\infty\big)-\#\mathrm{orb}_\Gamma\big(\overline{\mathcal{H}}^{(m-1,n)}_\infty\big),$$

which equals $r^{(n)}_{\sigma_m}-r^{(n)}_{\sigma_{m-1}}$ because $\mathrm{Im}(\sigma_m)=\mathbb{Z}_p[\![\Gamma^{p^m}]\!]\cdot\big\{\mathcal{A}^{(m,n)}_{\overline{h}}\;\big|\;\varpi_{\overline{h}}\in\mathrm{orb}_\Gamma\big(\overline{\mathcal{H}}^{(m,n)}_\infty\big)\big\}$. □

The transfer map $\mathrm{Ver}_{m,m'}$*:* Consider the subgroups $\mathcal{U}_{m,n}\subset\mathcal{U}_{m',n}$ of $\mathcal{G}_{\infty,n}$ with $m>m'$. The transfer homomorphism (Verlagerung) $\mathrm{Ver}^{\mathcal{U}_{m',n}}_{\mathcal{U}_{m,n}}$ relative to these subgroups maps $\mathcal{U}^{\mathrm{ab}}_{m',n}\longrightarrow\mathcal{U}^{\mathrm{ab}}_{m,n}$ by sending

$$g\big[\mathcal{U}_{m',n},\mathcal{U}_{m',n}\big]\;\mapsto\;\prod_{\tau\in\mathcal{R}}c_{g,\tau}\big[\mathcal{U}_{m,n},\mathcal{U}_{m,n}\big]$$

where $\mathcal{R}$ is a fixed set of left coset representatives for $\mathcal{U}_{m',n}/\mathcal{U}_{m,n}$, and $g\tau=r_gc_{g,\tau}$ with $c_{g,\tau}\in\mathcal{U}_{m,n}$ and $r_g\in\mathcal{R}$.

Henceforth one writes $\mathrm{Ver}_{m',m}:\Lambda\big(\mathcal{U}^{\mathrm{ab}}_{m',n}\big)\to\Lambda\big(\mathcal{U}^{\mathrm{ab}}_{m,n}\big)$ for the $\mathbb{Z}_p$-linear and continuous extension of the transfer map to the completed group algebras.

Lemma 4.7 *Suppose* $g\in\mathcal{U}^{\mathrm{ab}}_{m',n}$, *and let* $\hat{g}=(\gamma^{p^{m'}})^j\cdot(h_1^xh_2^y)\in\Gamma^{p^{m'}}\ltimes\mathcal{H}_\infty$ *be any lift. Then*

$$\mathrm{Ver}_{m',m}(g)\;\equiv\;(\gamma^{p^m})^j\cdot h_1^{x'}h_2^{y'}\mod\big[\mathcal{U}_{m,n},\mathcal{U}_{m,n}\big]$$

where $(x',y')=\Big(p^{m-m'}x,\;p^{m-m'}y\Big)$ *in Case (II), and in the same notation as the proof of Proposition 4.2:*

$$\begin{pmatrix}x'\\ \\ y'\end{pmatrix}\;=\;P_\star\begin{pmatrix}\frac{\lambda_{\star,+}^{p^m}-1}{\lambda_{\star,+}^{p^{m'}}-1}&0\\ 0&\frac{\lambda_{\star,-}^{p^m}-1}{\lambda_{\star,-}^{p^{m'}}-1}\end{pmatrix}P_\star^{-1}\begin{pmatrix}x\\ \\ y\end{pmatrix}\qquad\textit{in Case }(\star),\quad\textit{with }\star\in\{\mathit{III,IV,V,VI}\}.$$

Proof. Since $\mathcal{U}_{m',n}/\mathcal{U}_{m,n} \cong \Gamma^{p^{m'}}/\Gamma^{p^m}$, its coset representatives are $\{r_0, r_1, \ldots, r_{p^{m-m'}-1}\}$ where $r_i = \gamma^{p^{m'}i}$. One can represent $\hat{g}$ in the form $\gamma^{p^{m'}j} \cdot (h_1^x h_2^y)$ for some choice of $j \in \mathbb{Z}_p$, in which case

$$\hat{g}\ r_i \ = \ \gamma^{p^{m'}j}(h_1^x h_2^y)\gamma^{p^{m'}i} \ = \ \gamma^{p^{m'}(j+i)}\left(\gamma^{-p^{m'}i}(h_1^x h_2^y)\gamma^{p^{m'}i}\right) \ = \ \gamma^{p^{m'}(j+i)} \cdot \left(h_1^{x_{p^{m'}i}} h_2^{y_{p^{m'}i}}\right)$$

where $\begin{pmatrix} x_{p^{m'}i} \\ y_{p^{m'}i} \end{pmatrix} = \left(I_2 + M\right)^{p^{m'}i} \begin{pmatrix} x \\ y \end{pmatrix}$.

In fact, if $\iota : \mathbb{Z}_p \to \{0, 1, \ldots, p^{m-m'} - 1\}$ so that $\iota(z) \equiv z \bmod p^{m-m'}$, then one has $\gamma^{p^{m'}(j+i)} = r_{\iota(j+i)} \cdot \gamma^{p^{m'}(j+i-\iota(j+i))}$; consequently

$$\hat{g}\ r_i \ = \ r_{\iota(j+i)} \left(\gamma^{p^{m'}(j+i-\iota(j+i))} \cdot \left(h_1^{x_{p^{m'}i}} h_2^{y_{p^{m'}i}}\right)\right).$$

By definition, the transfer is congruent to

$$\mathrm{Ver}_{m',m}(g) \ \equiv \ \prod_{i=0}^{p^{m-m'}-1} \gamma^{p^{m'}(j+i-\iota(j+i))} \cdot h_1^{x_{p^{m'}i}} h_2^{y_{p^{m'}i}} \quad \bmod \left[\mathcal{U}_{m,n}, \mathcal{U}_{m,n}\right]$$

and as $j+i \equiv \iota(j+i) \bmod p^{m-m'}$ clearly $\gamma^{p^{m'}(j+i-\iota(j+i))} \in \Gamma^{p^m}$, hence $\gamma^{p^{m'}(j+i-\iota(j+i))}$ and $h_1^{x_i} h_2^{y_i}$ commute modulo $\left[\mathcal{U}_{m,n}, \mathcal{U}_{m,n}\right]$. It follows that

$$\mathrm{Ver}_{m',m}(g) \ \equiv \ \gamma^{p^{m'}c} \cdot h_1^{x'} h_2^{y'} \quad \bmod \left[\mathcal{U}_{m,n}, \mathcal{U}_{m,n}\right]$$

where $c = \sum_{i=0}^{p^{m-m'}-1} j + i - \iota(j+i)$, and the vector

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} \sum x_{p^{m'}i} \\ \sum y_{p^{m'}i} \end{pmatrix} = \sum_{i=0}^{p^{m-m'}-1} \left(I_2 + M\right)^{p^{m'}i} \begin{pmatrix} x \\ y \end{pmatrix}.$$

To calculate the term c, without loss of generality assume $j \in \mathbb{Z}$, which implies

$$c \ = \ \sum_{i=0}^{p^{m-m'}-1} j + i - \iota(j+i) \ = \ p^{m-m'} \times \sum_{i=0}^{p^{m-m'}-1} \left\lfloor \frac{j+i}{p^{m-m'}} \right\rfloor.$$

The right-hand sum then yields

$$\sum_{i=0}^{p^{m-m'}-1} \left\lfloor \frac{j+i}{p^{m-m'}} \right\rfloor \ = \ p^{m-m'} \left\lfloor \frac{j}{p^{m-m'}} \right\rfloor + \sum_{i=0}^{p^{m-m'}-1} \left\lfloor \frac{\iota(j)+i}{p^{m-m'}} \right\rfloor$$

$$= \ p^{m-m'} \left\lfloor \frac{j}{p^{m-m'}} \right\rfloor + \sum_{i=0}^{p^{m-m'}-\iota(j)-1} 0 \ + \sum_{i=p^{m-m'}-\iota(j)}^{p^{m-m'}-1} 1 \ = \ p^{m-m'} \left\lfloor \frac{j}{p^{m-m'}} \right\rfloor + \iota(j) \ = \ j$$

and as an immediate consequence, $c = p^{m-m'} \times j$ so that $\gamma^{p^{m'}c} = \gamma^{p^m j}$ as required.

To compute x' and y', in Case (II) we find that

$$\sum_{i=0}^{p^{m-m'}-1} \big(I_2{+}M\big)^{p^{m'}i} = \sum_{i=0}^{p^{m-m'}-1} \left(\begin{array}{cc} 1 & p^s \times ip^{m'} \\ 0 & 1 \end{array}\right) = \left(\begin{array}{cc} p^{m-m'} & p^{s+m} \times \frac{p^{m-m'}-1}{2} \\ 0 & p^{m-m'} \end{array}\right).$$

In all other cases $\star \in \{\text{III,IV,V,VI}\}$ one has $\big(I_2{+}M\big)^{p^{m'}i} = P_\star \left(\begin{array}{cc} \lambda_{\star,+}^{p^{m'}i} & 0 \\ 0 & \lambda_{\star,-}^{p^{m'}i} \end{array}\right) P_\star^{-1}$, which means

$$\sum_{i=0}^{p^{m-m'}-1} \big(I_2 + M\big)^{p^{m'}i} \left(\begin{array}{c} x \\ y \end{array}\right) = P_\star \left(\begin{array}{cc} \sum_{i=0}^{p^{m-m'}-1} \lambda_{\star,+}^{p^{m'}i} & 0 \\ 0 & \sum_{i=0}^{p^{m-m'}-1} \lambda_{\star,-}^{p^{m'}i} \end{array}\right) P_\star^{-1}.$$

Note that $P_{III} = I_2$ because $I_2 + M$ is already diagonalised.

The result follows upon summing up the relevant geometric progression, i.e. $\sum_{i=0}^{p^{m-m'}-1} \lambda_{\star,\pm}^{p^{m'}i}$ equals $\frac{\lambda_{\star,\pm}^{p^m}-1}{\lambda_{\star,\pm}^{p^{m'}}-1}$. □

The shift $\pi_{m,m'}$: For integers $m > m'$, we now look for a reverse mapping to $\text{Ver}_{m',m}$. The commutator $[h_1^x h_2^y, \gamma^{p^m}]$ corresponds to $\Big((I_2{+}M)^{p^m} - I_2\Big) \left(\begin{array}{c} x \\ y \end{array}\right)$ as a vector in $\mathbb{Z}_p^2$; however $X^{p^m} - 1 = (X^{p^{m'}} - 1) \times \prod_{d=m'+1}^m \phi_{p^d}(X)$ where ϕ_{p^d} denotes the p^d-th cyclotomic polynomial, therefore

$$[h_1^x h_2^y, \gamma^{p^m}] \;=\; [h_1^{x''} h_2^{y''}, \gamma^{p^{m'}}] \quad \text{with} \quad \left(\begin{array}{c} x'' \\ y'' \end{array}\right) = \prod_{d=m'+1}^{m} \phi_{p^d}\big(I_2 + M\big) \left(\begin{array}{c} x \\ y \end{array}\right).$$

As a consequence, we have the containments

$$\big[\mathcal{U}_{m,n}, \mathcal{U}_{m,n}\big] \subset \big[\mathcal{U}_{m',n}, \mathcal{U}_{m',n}\big] \subset \mathcal{H}_\infty / \mathcal{H}_\infty^{p^n}.$$

The natural inclusion $\mathcal{U}_{m,n} \hookrightarrow \mathcal{U}_{m',n}$ then yields the composition

$$\pi_{m,m'} \;:\; \mathcal{U}_{m,n}^{\text{ab}} \;=\; \frac{\mathcal{U}_{m,n}}{\big[\mathcal{U}_{m,n}, \mathcal{U}_{m,n}\big]} \;\hookrightarrow\; \frac{\mathcal{U}_{m',n}}{\big[\mathcal{U}_{m,n}, \mathcal{U}_{m,n}\big]} \;\overset{\text{proj}}{\twoheadrightarrow}\; \frac{\mathcal{U}_{m',n}}{\big[\mathcal{U}_{m',n}, \mathcal{U}_{m',n}\big]} \;=\; \mathcal{U}_{m',n}^{\text{ab}}.$$

Moreover this shift homomorphism induces a map $(\pi_{m,m'})_* : \text{orb}_\Gamma\big(\overline{\mathcal{H}}_\infty^{(m,n)}\big) \to \text{orb}_\Gamma\big(\overline{\mathcal{H}}_\infty^{(m',n)}\big)$, sending each orbit $\varpi_{\overline{h}} = \big\{\gamma^{-i}\overline{h}\gamma^i \mid i \in \mathbb{Z}\big\}$ to the direct image $\varpi_{\pi_{m,m'}(\overline{h})}$.

Recall from Proposition 4.5(ii) that a typical element of $\mathrm{Im}(\sigma_m)$ has the form

$$\sum_{\varpi\in\mathrm{orb}_\Gamma(\overline{\mathcal{H}}_\infty^{(m,n)})} f_\varpi(\gamma^{p^m}-1)\cdot\mathcal{A}_\varpi^{(m,n)} \;=\; \sum_{\varpi} f_\varpi\cdot\mathcal{A}_\varpi^{(m,n)} \ \text{ say,}$$

where each $f_\varpi(X)\in\mathbb{Z}_p[\![X]\!]$ and $\mathcal{A}_\varpi^{(m,n)} := \sum_{i=0}^{p^m-1}\gamma^{-i}\overline{h}\gamma^i$ for any $\overline{h}\in\varpi$.

Lemma 4.8 *If $m>m'$, then $\pi_{m,m'}\left(\sum_\varpi f_\varpi\cdot\mathcal{A}_\varpi^{(m,n)}\right) = p^{m-m'}\times\sum_\varpi f_\varpi\cdot\mathcal{A}^{(m',n)}_{(\pi_{m,m'})_*(\varpi)}$.*

Proof. If $\overline{h}\in\varpi$ with $\varpi\in\mathrm{orb}_\Gamma\big(\overline{\mathcal{H}}_\infty^{(m,n)}\big)$, then within the algebra $\Lambda\big(\mathcal{U}^{\mathrm{ab}}_{m',n}\big)$ one has

$$\begin{aligned}\pi_{m,m'}\left(f_\varpi\cdot\sum_{i=0}^{p^m-1}\gamma^{-i}\overline{h}\gamma^i\right) &= f_\varpi(\gamma^{p^m}-1)\cdot\pi_{m,m'}\left(\sum_{i_1=0}^{p^{m-m'}-1}\sum_{i_2=0}^{p^{m'}-1}\gamma^{-p^{m'}i_1-i_2}\overline{h}\gamma^{p^{m'}i_1+i_2}\right)\\ &= f_\varpi(\gamma^{p^m}-1)\cdot\sum_{i_1=0}^{p^{m-m'}-1}\sum_{i_2=0}^{p^{m'}-1}\gamma^{-i_2}\pi_{m,m'}(\overline{h})\gamma^{i_2}\end{aligned}$$

since $\gamma^{-p^{m'}}\pi_{m,m'}(\overline{h})\gamma^{p^{m'}} = \pi_{m,m'}(\overline{h})$ inside $\mathcal{U}^{\mathrm{ab}}_{m',n}$, which gives the result. □

The norm and trace homomorphisms: We now introduce two final maps that occur in the definition of both of Kakde's groups Ψ and Φ. Firstly, if G is a group and $\mathrm{Conj}(G)$ denotes it set of conjugacy classes, then $\Lambda\big(\mathrm{Conj}(G)\big)\cong\Lambda(G)/\overline{[\Lambda(G),\Lambda(G)]}$ as an isomorphism of $\mathbb{Z}_p$-modules [CSRV12, §2]. For an integer pair m,m' with $m\geq m'$:

- the norm mapping $K_1\Big(\Lambda\big(\mathcal{U}^{\mathrm{ab}}_{m',n}\big)\Big)\longrightarrow K_1\Big(\Lambda\big(\mathcal{U}_{m,n}/[\mathcal{U}_{m',n},\mathcal{U}_{m',n}]\big)\Big)$ relative to the subgroup $\frac{\mathcal{U}_{m,n}}{[\mathcal{U}_{m',n},\mathcal{U}_{m',n}]}\subset\frac{\mathcal{U}_{m',n}}{[\mathcal{U}_{m',n},\mathcal{U}_{m',n}]}=\mathcal{U}^{\mathrm{ab}}_{m',n}$ is abbreviated by $\mathcal{N}_{m',m}$; and
- similarly, the additive trace map $\Lambda\Big(\mathrm{Conj}\big(\mathcal{U}^{\mathrm{ab}}_{m',n}\big)\Big)\longrightarrow\Lambda\Big(\mathrm{Conj}\big(\mathcal{U}_{m,n}/[\mathcal{U}_{m',n},\mathcal{U}_{m',n}]\big)\Big)$ relative to $\frac{\mathcal{U}_{m,n}}{[\mathcal{U}_{m',n},\mathcal{U}_{m',n}]}\subset\frac{\mathcal{U}_{m',n}}{[\mathcal{U}_{m',n},\mathcal{U}_{m',n}]}=\mathcal{U}^{\mathrm{ab}}_{m',n}$ is denoted by $\mathrm{Tr}_{m',m}$.

The following lemma describes the effect of the second of these maps on the image of $\sigma_{m'}$. Let $\mathrm{char}_{\Gamma^{p^m}}:\Lambda(\Gamma)\to\Lambda(\Gamma^{p^m})$ denote the $\mathbb{Z}_p$-linear and continuous extension of the map which sends $\gamma^i\mapsto\gamma^i$ if p^m divides i, and sends $\gamma^i\mapsto 0$ if p^m does not divide i.

Lemma 4.9 *For any element* $\mathbf{a}_{m'} = \sum_{\varpi} f_{\varpi}(\gamma^{p^{m'}} - 1) \cdot \mathcal{A}_{\varpi}^{(m',n)} \in \mathrm{Im}\big(\sigma_{m'}\big)$,

$$\mathrm{Tr}_{m',m}\big(\mathbf{a}_{m'}\big) \;=\; p^{m-m'} \times \sum_{\varpi} \mathrm{char}_{\Gamma^{p^m}}\left(f_{\varpi}\big(\gamma^{p^{m'}} - 1\big)\right) \cdot \mathcal{A}_{\varpi}^{(m',n)} \;\in\; \Lambda\left(\frac{\mathcal{U}_{m,n}}{[\mathcal{U}_{m',n}, \mathcal{U}_{m',n}]}\right)$$

where the sum is taken over all $\varpi \in \mathrm{orb}_{\Gamma}\big(\overline{\mathcal{H}}_{\infty}^{(m',n)}\big)$.

Proof. From [CSRV12, Rk iii], one knows

$$\mathrm{Tr}_{m',m}\big(\gamma^{p^{m'}j}\overline{h}\big) = \begin{cases} p^{m-m'} \times \gamma^{p^{m'}j}\overline{h} & \text{if } \gamma^{p^{m'}j} \in \Gamma^{p^m} \\ 0 & \text{if } \gamma^{p^{m'}j} \notin \Gamma^{p^m}, \end{cases}$$

so that for any $\overline{h} \in \varpi$:

$$\mathrm{Tr}_{m',m}\left(\gamma^{p^{m'}j} \cdot \mathcal{A}_{\varpi}^{(m',n)}\right) \;=\; \begin{cases} p^{m-m'} \times \sum_{i=0}^{p^{m'}-1} \gamma^{p^{m'}j} \cdot \big(\gamma^{-i}\overline{h}\gamma^{i}\big) & \text{if } \gamma^{p^{m'}j} \in \Gamma^{p^m} \\ 0 & \text{otherwise.} \end{cases}$$

The stated formula then follows by linearity and continuity. □

Chapter 5

The Additive Calculations

We begin by recalling Kakde's definition of the subset $\Psi \subset \prod_m \mathbb{Q}_p[[\mathcal{U}^{\mathrm{ab}}_{m,n}]]$ given in [Kak13]. For a fixed $n \geq s$, the $\mathbb{Z}_p$-module Ψ consists of sequences $\big(\mathbf{a}_m\big)$ satisfying the conditions:

(A1) $\mathrm{Tr}_{m',m}\big(\mathbf{a}_{m'}\big) = \pi_{m,m'}\big(\mathbf{a}_m\big)$ for any $m > m'$;

(A2) $\mathbf{a}_m = g\mathbf{a}_m g^{-1}$ at every $g \in \mathcal{G}_{\infty,n}$;

(A3) $\mathbf{a}_m \in \mathrm{Im}(\sigma_m)$ for each $m \in \{0, \ldots, n-s\}$.

In fact, the general definition of Ψ involves more than just this system of subquotients. However for our purposes these are sufficient, as every irreducible representation of $\mathcal{G}_{\infty,n}$ is a finite twist of a representation obtained from inducing down a character χ on $\mathcal{U}_{m,n}$, for an appropriate choice of m and χ.

5.1 The image of Ψ under the characters on $\overline{\mathcal{H}}^{(m,n)}_{\infty}$

The main task is to see how Ψ transforms if we evaluate its constituent elements at a system of characters $\underline{\chi} = \{\chi\}$ on $\mathcal{H}_\infty/\mathcal{H}_\infty^{p^n}$. In particular, we want to translate the conditions (A1)–(A3) involving the $\mathbf{a}_m$'s into equivalent conditions involving $\mathbf{a}_\chi := \chi(\mathbf{a}_{\mathbf{m}_\chi})$ instead, and thereby complete the middle square in the diagram

$$\begin{tikzcd}
K_1'\big(\mathbb{Z}_p[\![\mathcal{G}_{\infty,n}]\!]\big) \arrow[r, "\Theta_{\infty,n}"] \arrow[dr, "\mathrm{Ev}_{\underline{\chi}}"'] & \Phi \arrow[r, "\text{``twisted log''}"] \arrow[d, "\underline{\chi}"] & \Psi \arrow[r, hook] \arrow[d, "\underline{\chi}"] & \mathbb{Q} \otimes \left(\prod_{0 \leq m \leq n-s} \mathbb{Z}_p\big[\![\mathcal{U}_{m,n}^{\mathrm{ab}}]\!\big] \right) \arrow[d, "\underline{\chi}"] \\
 & \underline{\chi}(\Phi) \arrow[r, dashed, "??"] & \underline{\chi}(\Psi) \arrow[r, hook] & \mathbb{Q} \otimes \left(\prod_{m,\chi} \mathcal{O}_\chi \big[\![\mathrm{Stab}_\Gamma(\chi)]\!\big] \right)
\end{tikzcd}$$

which at this stage we make no attempt to explain in detail! The objects and maps above will be properly introduced later, although we should perhaps point out that, in general, $K_1'(-) := K_1(-)/SK_1(-)$ (see [SV10, Section 4]).

The following key result describes $\underline{\chi}(\Psi) \subset \prod_\chi \mathbb{C}_p\big[\![\mathrm{Stab}_\Gamma(\chi)]\!\big]$ using p-adic congruences.

Theorem 5.1 *A collection of elements* $\mathbf{a}_\chi \in \mathcal{O}_{\mathbb{C}_p}\big[\![\mathrm{Stab}_\Gamma(\chi)]\!\big]$ *arises from a sequence* $(\mathbf{a}_m) \in \Psi \cap \prod_{0 \leq m \leq n-s} \mathbb{Z}_p\big[\![\mathcal{U}_{m,n}^{\mathrm{ab}}]\!\big]$*, if and only if for each* $m \geq 0$ *and* $\varpi \in \mathrm{orb}_\Gamma\big(\overline{\mathcal{H}}_\infty^{(m,n)}\big)$*:*

(C1) *the compatibility* $\chi(\mathbf{a}_m) = \mathrm{Tr}_{\mathrm{Stab}_\Gamma(\chi)/\Gamma^{p^m}}(\mathbf{a}_\chi)$ *holds if* $m \in \{\mathbf{m}_\chi, \ldots, n-s\}$*,*

(C2) *the equality* $\mathbf{a}_{\chi'} = \mathbf{a}_\chi$ *holds at each character* $\chi' \in \Gamma * \chi$*,*

(C3) $\displaystyle\sum_{\chi \in \mathfrak{R}_{m,n}} \mathrm{Tr}_{\mathrm{Stab}_\Gamma(\chi)/\Gamma^{p^m}}(\mathbf{a}_\chi) \cdot \mathrm{Tr}\big(\mathrm{Ind}\chi^*\big)(\varpi) \ \in \ \mathbb{Z}_p\big[\![\Gamma^{p^m}]\!\big],$ *and*

(C4) $\displaystyle\sum_{\chi \in \mathfrak{R}_{m,n}} \mathrm{Tr}_{\mathrm{Stab}_\Gamma(\chi)/\Gamma^{p^m}}(\mathbf{a}_\chi) \cdot \mathrm{Tr}\big(\mathrm{Ind}\chi^*\big)(\varpi) \equiv 0 \mod p^{\mathrm{ord}_p(\#\overline{\mathcal{H}}_\infty^{(m,n)})+m-\mathrm{ord}_p(\#\varpi)}$

where $\mathfrak{R}_{m,n}$ *denotes a set of representatives for the* Γ*-orbits inside* $\mathrm{Hom}\big(\overline{\mathcal{H}}_\infty^{(m,n)}, \mathbb{C}^\times\big)$*.*

To calculate $\#\overline{\mathcal{H}}_\infty^{(m,n)}$ in property (C4) above, one just applies Proposition 4.4. On the other hand, to calculate $\#\varpi$ we use the orbit-stabilizer theorem, so that for any $\overline{h} \in \varpi$ one obtains

$$\#\varpi \ = \ \big[\Gamma/\Gamma^{p^m} : \mathrm{Stab}_{\Gamma/\Gamma^{p^m}}(\overline{h})\big] \ = \ \big[\Gamma : \mathrm{Stab}_\Gamma(\overline{h})\big].$$

Also by property (C2), an element $\mathbf{a}_\chi$ depends only on the representative for χ in $\mathfrak{R}_{m,n}$, hence the last two summations in the above theorem are independent of any choices.

Proof. We begin with the 'only if' part of the argument. Suppose we are given an arbitrary element $\mathbf{a}_m \in \mathbb{Z}_p\big[\big[\mathcal{U}_{m,n}^{\mathrm{ab}}\big]\big]$, and let us put $\mathbf{a}_\chi^{(m)} := \chi\left(\mathbf{a}_m\right)$ for any character $\chi : \mathcal{H}_\infty \to \mu_{p^n}$ (note that if $\mathrm{Stab}_\Gamma(\chi) = \Gamma^{p^m}$, then we will drop the superscript ${}^{(m)}$ above completely). Assuming that $(\mathbf{a}_m) \in \Psi \cap \prod_m \mathbb{Z}_p\big[\big[\mathcal{U}_{m,n}^{\mathrm{ab}}\big]\big]$, we claim the following statements hold:

(a) there are equalities $\mathbf{a}_\chi^{(m)} = \mathbf{a}_{\chi'}^{(m)}$ for any $\chi' \in \Gamma * \chi$, where $\Gamma * \chi := \big\{g * \chi \mid g \in \Gamma\big\}$;

(b) we can express $\mathbf{a}_m = \sum_{\varpi \in \mathrm{orb}_\Gamma(\overline{\mathcal{H}}_\infty^{(m,n)})} C_\varpi^{(m)} \cdot \mathcal{A}_\varpi^{(m,n)}$, where for any $\overline{h} \in \varpi$ one has

$$C_\varpi^{(m)} = \frac{\#\varpi}{p^m \cdot \#\overline{\mathcal{H}}_\infty^{(m,n)}} \times \sum_{\chi \in \mathfrak{R}_{m,n}} \mathbf{a}_\chi^{(m)} \cdot \left(\frac{\#(\Gamma * \chi)}{p^m} \cdot \sum_{i=0}^{p^m-1} \chi^{-1}\left(\gamma^{-i}\overline{h}\gamma^i\right) \right) \in \Lambda\big(\Gamma^{p^m}\big);$$

(c) $-\mathrm{ord}_p\left(\frac{\#\varpi}{p^m \cdot \#\overline{\mathcal{H}}_\infty^{(m,n)}}\right) = \mathrm{ord}_p\big(\#\overline{\mathcal{H}}_\infty^{(m,n)}\big) + m - \mathrm{ord}_p(\#\varpi) \ \geq \ 0;$

(d) $\mathrm{Tr}\big(\mathrm{Ind}\chi^*\big)(\varpi) = \frac{\#(\Gamma*\chi)}{p^m} \cdot \sum_{i=0}^{p^m-1} \chi^{-1}\left(\gamma^{-i}\overline{h}\gamma^i\right);$

(e) one has $\mathbf{a}_\chi^{(m)} = \mathrm{Tr}_{\mathrm{Stab}_\Gamma(\chi)/\Gamma^{p^m}}\left(\mathbf{a}_\chi\right)$ for each $m \geq \mathbf{m}_\chi$, i.e. (C1) is true.

Deferring their proof temporarily, let us first understand why they yield the three assertions in our theorem. Clearly statement (C2) is implied by (a) with $m = \mathrm{ord}_p[\Gamma : \mathrm{Stab}_\Gamma(\chi)]$. Moreover both (C3) and (C4) will now follow upon combining (b), (c), (d) and (e) together, and then observing that the p-integrality of the $C_\varpi^{(m)}$'s is equivalent to each sum

$$\sum_{\chi \in \mathfrak{R}_{m,n}} \mathbf{a}_\chi^{(m)} \cdot \left(\frac{\#(\Gamma * \chi)}{p^m} \cdot \sum_{i=0}^{p^m-1} \chi^{-1}\left(\gamma^{-i}\overline{h}\gamma^i\right) \right) = \sum_{\chi \in \mathfrak{R}_{m,n}} \mathrm{Tr}_{\mathrm{Stab}_\Gamma(\chi)/\Gamma^{p^m}}\left(\mathbf{a}_\chi\right) \cdot \mathrm{Tr}\big(\mathrm{Ind}\chi^*\big)(\varpi)$$

belonging to the lattice $\frac{p^m \cdot \#\overline{\mathcal{H}}_\infty^{(m,n)}}{\#\varpi} \cdot \mathbb{Z}_p\big[\big[\Gamma^{p^m}\big]\big] = p^{\mathrm{ord}_p(\#\overline{\mathcal{H}}_\infty^{(m,n)}) + m - \mathrm{ord}_p(\#\varpi)} \cdot \mathbb{Z}_p\big[\big[\Gamma^{p^m}\big]\big]$.

We are left to prove these five assertions. Part (a) is a consequence of property (A2). To prove statement (b), let us write $\mathbf{a}_m = \sum_{\overline{h} \in \overline{\mathcal{H}}_\infty^{(m,n)}} c_{\overline{h}}^{(m)} \cdot \overline{h}$ where each $c_{\overline{h}}^{(m)} \in \Lambda\big(\Gamma^{p^m}\big)$. Since the characteristic function of $\overline{h}$ can be decomposed into a sum over the characters of the abelian group $\overline{\mathcal{H}}_\infty^{(m,n)}$, one can express each coefficient above as

$$c_{\overline{h}}^{(m)} = \frac{1}{\#\overline{\mathcal{H}}_\infty^{(m,n)}} \times \sum_{\chi : \overline{\mathcal{H}}_\infty^{(m,n)} \to \mu_{p^n}} \chi^{-1}(\overline{h}) \cdot \mathbf{a}_\chi^{(m)}.$$

Using property (A3) and Proposition 4.5, we know that $\mathbf{a}_m$ is a $\Lambda(\Gamma^{p^m})$-linear combination of $\mathcal{A}_{\varpi}^{(m,n)}$'s, which indicates $c_{\overline{h}}^{(m)}$ is constant-valued for all $\overline{h}$ inside a prescribed orbit ϖ. If we denote this common value as '$c_{\varpi}^{(m)}$', then

$$\mathbf{a}_m \;=\; \sum_{\varpi\in\mathrm{orb}_\Gamma(\overline{\mathcal{H}}_\infty^{(m,n)})}\;\sum_{\overline{h}\in\varpi} c_{\varpi}^{(m)}\cdot\overline{h} \;=\; \sum_{\varpi} c_{\varpi}^{(m)}\cdot\sum_{\overline{h}\in\varpi}\overline{h} \;=\; \sum_{\varpi} c_{\varpi}^{(m)}\cdot\frac{\#\varpi}{p^m}\cdot\mathcal{A}_{\varpi}^{(m,n)}.$$

N.B. In this situation, the term $c_{\varpi}^{(m)}\cdot\frac{\#\varpi}{p^m}$ corresponds to the coefficient $C_{\varpi}^{(m)}$ of $\mathcal{A}_{\varpi}^{(m,n)}$.

Now we can break $\sum_{\chi:\overline{\mathcal{H}}_\infty^{(m,n)}\to\mu_{p^n}}$ into a double summation $\sum_{\chi\in\mathfrak{R}_{m,n}}\sum_{\chi'\in\Gamma*\chi}$. Furthermore, $\mathbf{a}_{\chi'}^{(m)}=\mathbf{a}_{\chi}^{(m)}$ whenever $\chi'\in\Gamma*\chi$ from (a), hence for any $\overline{h}\in\varpi$:

$$c_{\varpi}^{(m)} \;=\; \frac{1}{\#\overline{\mathcal{H}}_\infty^{(m,n)}}\cdot\sum_{\chi:\overline{\mathcal{H}}_\infty^{(m,n)}\to\mu_{p^n}}\chi^{-1}(\overline{h})\cdot\mathbf{a}_{\chi}^{(m)} \;=\; \frac{1}{\#\overline{\mathcal{H}}_\infty^{(m,n)}}\cdot\sum_{\chi\in\mathfrak{R}_{m,n}}\mathbf{a}_{\chi}^{(m)}\sum_{\chi'\in\Gamma*\chi}\left(\chi'\right)^{-1}(\overline{h}).$$

Splicing together these last two equations, we therefore conclude

$$\mathbf{a}_m \;=\; \sum_{\varpi\in\mathrm{orb}_\Gamma(\overline{\mathcal{H}}_\infty^{(m,n)})}\left(\frac{\#\varpi}{p^m\cdot\#\overline{\mathcal{H}}_\infty^{(m,n)}}\times\sum_{\chi\in\mathfrak{R}_{m,n}}\mathbf{a}_{\chi}^{(m)}\cdot\sum_{\chi'\in\Gamma*\chi}\left(\chi'\right)^{-1}(\overline{h})\right)\cdot\mathcal{A}_{\varpi}^{(m,n)}.$$

Lastly $\sum_{\chi'\in\Gamma*\chi}\left(\chi'\right)^{-1}(\overline{h})$ coincides with the scaled value $\frac{\#(\Gamma*\chi)}{p^m}\cdot\sum_{i=0}^{p^m-1}\chi^{-1}\left(\gamma^{-i}\overline{h}\gamma^{i}\right)$, which means (b) is also established.

To show part (c) is easy since the size of each orbit $\varpi\in\mathrm{orb}_\Gamma\big(\overline{\mathcal{H}}_\infty^{(m,n)}\big)$ divides into p^m. In order to establish (d) we define $\rho_m:=\mathrm{Ind}_{\Gamma^{p^m}\ltimes\mathcal{H}_\infty/p^n}^{G_{\infty,n}}(\chi)$, so that $\rho_m\cong\bigoplus_\psi\mathrm{Ind}(\chi)\otimes\psi$ where the sum is over all characters $\psi:\mathrm{Stab}_\Gamma(\chi)/\Gamma^{p^m}\to\mathbb{C}^\times$. Thus for $\overline{h}\in\varpi\subset\overline{\mathcal{H}}_\infty^{(m,n)}$,

$$\big[\mathrm{Stab}_\Gamma(\chi):\Gamma^{p^m}\big]\cdot\mathrm{Tr}\big(\mathrm{Ind}\chi^*\big)(\overline{h}) \;=\; \mathrm{Tr}\big(\rho_m^*\big)(\overline{h}) \;=\; \sum_{i=0}^{p^m-1}\chi^{-1}\left(\gamma^{-i}\overline{h}\gamma^{i}\right)$$

and the orbit-stabilizer theorem for Γ/Γ^{p^m} acting on $\mathrm{Hom}\big(\overline{\mathcal{H}}_\infty^{(m,n)},\mu_{p^n}\big)$ then implies

$$\big[\mathrm{Stab}_\Gamma(\chi):\Gamma^{p^m}\big] \;=\; \frac{\big[\Gamma:\Gamma^{p^m}\big]}{\big[\Gamma:\mathrm{Stab}_\Gamma(\chi)\big]} \;=\; \frac{\big[\Gamma:\Gamma^{p^m}\big]}{\big[\Gamma/\Gamma^{p^m}:\mathrm{Stab}_{\Gamma/\Gamma^{p^m}}(\chi)\big]} \;=\; \frac{p^m}{\#\big(\Gamma*\chi\big)}.$$

The assertion (e) follows from property (A1): if we set $m'=\mathbf{m}_\chi$ then

$$\mathrm{Tr}_{\mathrm{Stab}_\Gamma(\chi)/\Gamma^{p^m}}(\mathbf{a}_\chi) \;=\; \chi\left(\mathrm{Tr}_{m',m}(\mathbf{a}_{m'})\right) \;\overset{\text{by (A1)}}{=}\; \chi\left(\pi_{m,m'}(\mathbf{a}_m)\right) \;=\; \mathbf{a}_{\chi}^{(m)}.$$

This completes the 'if' portion of the 'if and only if' statement.

Now, let us focus on the 'only if' part, which means we must show that

"(C1) and (C2) and (C3) and (C4) $\Longrightarrow$ (A1) and (A2) and (A3) ".

We start with establishing (A2); in fact it is enough to show that $\gamma^{-1}\mathbf{a}_m\gamma = \mathbf{a}_m$, for all $\gamma \in \Gamma$.

By a direct computation,

$$\begin{aligned}\gamma^{-1}c^{(m)}_{\overline{h}}\gamma &= \frac{1}{\#\overline{\mathcal{H}}^{(m,n)}_\infty} \times \sum_{\chi:\overline{\mathcal{H}}^{(m,n)}_\infty \to \mu_{p^n}} \gamma^{-1}\chi^{-1}(\overline{h})\cdot \mathbf{a}^{(m)}_\chi\gamma \\ &= \frac{1}{\#\overline{\mathcal{H}}^{(m,n)}_\infty} \times \sum_{\chi:\overline{\mathcal{H}}^{(m,n)}_\infty \to \mu_{p^n}} \chi^{-1}(\overline{h})\cdot \gamma^{-1}\mathbf{a}^{(m)}_\chi\gamma \\ &= \frac{1}{\#\overline{\mathcal{H}}^{(m,n)}_\infty} \times \sum_{\chi:\overline{\mathcal{H}}^{(m,n)}_\infty \to \mu_{p^n}} \chi^{-1}(\overline{h})\cdot \mathbf{a}^{(m)}_\chi \quad \text{since } \gamma \text{ acts trivially on } \Gamma^{p^m},\end{aligned}$$

which coincides with $c^{(m)}_{\overline{h}}$. Consequently,

$$\begin{aligned}\gamma^{-1}\mathbf{a}_m\gamma = \sum_{\overline{h}\in\overline{\mathcal{H}}^{(m,n)}_\infty} \gamma^{-1}c^{(m)}_{\overline{h}}\overline{h}\gamma &= \sum_{\overline{h}\in\overline{\mathcal{H}}^{(m,n)}_\infty} \gamma^{-1}c^{(m)}_{\overline{h}}\gamma\gamma^{-1}\overline{h}\gamma \\ &= \sum_{\overline{h}\in\overline{\mathcal{H}}^{(m,n)}_\infty} c^{(m)}_{\overline{h}}\gamma^{-1}\overline{h}\gamma = \sum_{\overline{h}\in\overline{\mathcal{H}}^{(m,n)}_\infty} c^{(m)}_{\overline{h}}\overline{h}^\gamma.\end{aligned}$$

On the other hand,

$$\begin{aligned}c^{(m)}_{\overline{h}^\gamma} &= \frac{1}{\#\overline{\mathcal{H}}^{(m,n)}_\infty} \times \sum_{\chi:\overline{\mathcal{H}}^{(m,n)}_\infty \to \mu_{p^n}} \chi^{-1}(\overline{h}^\gamma)\cdot \mathbf{a}^{(m)}_\chi = \frac{1}{\#\overline{\mathcal{H}}^{(m,n)}_\infty} \times \sum_{\chi:\overline{\mathcal{H}}^{(m,n)}_\infty \to \mu_{p^n}} (\gamma\star\chi)^{-1}(\overline{h})\cdot \mathbf{a}^{(m)}_\chi \\ &= \frac{1}{\#\overline{\mathcal{H}}^{(m,n)}_\infty} \times \sum_{\chi:\overline{\mathcal{H}}^{(m,n)}_\infty \to \mu_{p^n}} (\gamma\star\chi)^{-1}(\overline{h})\cdot \mathbf{a}^{(m)}_{\gamma\star\chi} \qquad \text{by (C2).}\end{aligned}$$

which implies that $c^{(m)}_{\overline{h}^\gamma} = c^{(m)}_{\overline{h}}$. It follows directly that

$$\gamma^{-1}\mathbf{a}_m\gamma = \sum_{\overline{h}\in\overline{\mathcal{H}}^{(m,n)}_\infty} c^{(m)}_{\overline{h}}\overline{h}^\gamma = \sum_{\overline{h}\in\overline{\mathcal{H}}^{(m,n)}_\infty} c^{(m)}_{\overline{h}^\gamma}\overline{h}^\gamma = \mathbf{a}_m,$$

which means that (A2) now follows.

Secondly, we try to deduce (A3). Since $c^{(m)}_{\overline{h}}$ only depends on $\omega_{\overline{h}}$, as $c^{(m)}_{\overline{h}^\gamma} = c^{(m)}_{\overline{h}}$, thus one can write

$$\mathbf{a}_m \;=\; \sum_{\varpi\in\mathrm{orb}_\Gamma(\overline{\mathcal{H}}^{(m,n)}_\infty)} \sum_{\overline{h}\in\varpi} c^{(m)}_\varpi\cdot\overline{h} \;=\; \sum_\varpi c^{(m)}_\varpi\cdot\sum_{\overline{h}'\in\varpi}\overline{h}' \;=\; \sum_\varpi c^{(m)}_\varpi\cdot\frac{\#\varpi}{p^m}\cdot\mathcal{A}^{(m,n)}_\varpi.$$

As shown before,

$$\begin{aligned} c_{\varpi}^{(m)} &= \frac{1}{\#\overline{\mathcal{H}}_{\infty}^{(m,n)}} \cdot \sum_{\chi:\overline{\mathcal{H}}_{\infty}^{(m,n)} \to \mu_{p^n}} \chi^{-1}(\overline{h}) \cdot \mathbf{a}_{\chi}^{(m)} = \frac{1}{\#\overline{\mathcal{H}}_{\infty}^{(m,n)}} \cdot \sum_{\chi \in \mathfrak{R}_{m,n}} \mathbf{a}_{\chi}^{(m)} \sum_{\chi' \in \Gamma * \chi} \big(\chi'\big)^{-1}(\overline{h}) \\ &= \frac{1}{\#\overline{\mathcal{H}}_{\infty}^{(m,n)}} \cdot \sum_{\chi \in \mathfrak{R}_{m,n}} \mathbf{a}_{\chi}^{(m)} \mathrm{Tr}\big(\mathrm{Ind}\chi^{*}\big)(\varpi) \qquad \text{(by C2)} \end{aligned}$$

Lastly, combining (C3) and (C4) together implies

$$c_{\varpi}^{(m)} \cdot \frac{\#\varpi}{p^m} \cdot \mathcal{A}_{\varpi}^{(m,n)} = \frac{\#\varpi}{p^m \#\overline{\mathcal{H}}_{\infty}^{(m,n)}} \cdot \sum_{\chi \in \mathfrak{R}_{m,n}} \mathbf{a}_{\chi}^{(m)} \mathrm{Tr}\big(\mathrm{Ind}\chi^{*}\big)(\varpi) \in \Lambda(\Gamma^{p^m}),$$

so that $\mathbf{a}_m \in \mathrm{Im}(\sigma_m)$.

Lemma 4.8 and Lemma 4.9 tell us that to prove (A1), it is enough to show that for each $\varpi' \in \mathrm{orb}_{\Gamma}(\overline{\mathcal{H}}_{\infty}^{(m,n)})$,

$$\sum_{\substack{\varpi \in \mathrm{orb}_{\Gamma}(\overline{\mathcal{H}}_{\infty}^{(m,n)}), \\ (\pi_{m,m'})_{*}(\varpi) = \varpi'}} C_{\varpi}^{(m)} \times \left(\frac{\#\varpi}{\#\varpi'}\right) = p^{m-m'} \times \mathrm{char}_{\Gamma^{p^m}}(C_{\varpi'}^{(m')}).$$

Without loss of generality, we assume that $m' = m-1$ for now. Then

$$\begin{aligned} \mathrm{Tr}_{\Gamma^{p^{m-1}}/\Gamma^{p^m}}(C_{\varpi'}^{(m-1)}) &= \mathrm{Tr}_{\Gamma^{p^{m-1}}/\Gamma^{p^m}}\Big(\frac{1}{\#\overline{\mathcal{H}}_{\infty}^{(m-1,n)}} \times \sum_{\tilde{\chi}:\overline{\mathcal{H}}_{\infty}^{(m-1,n)} \mapsto \mathbb{C}^{\times}} \mathbf{a}_{\tilde{\chi}}^{(m-1)} \cdot \tilde{\chi}^{-1}\big(\pi(\overline{h})\big)\Big) \\ &= \frac{1}{\#\overline{\mathcal{H}}_{\infty}^{(m-1,n)}} \sum_{\tilde{\chi}:\overline{\mathcal{H}}_{\infty}^{(m-1,n)} \mapsto \mathbb{C}^{\times}} \mathrm{Tr}_{\Gamma^{p^{m-1}}/\Gamma^{p^m}}\big(\mathbf{a}_{\tilde{\chi}}^{(m-1)}\big) \cdot \tilde{\chi}^{-1}\big(\pi(\overline{h})\big) \\ &= \frac{1}{\#\overline{\mathcal{H}}_{\infty}^{(m-1,n)}} \sum_{\tilde{\chi}:\overline{\mathcal{H}}_{\infty}^{(m-1,n)} \mapsto \mathbb{C}^{\times}} \mathrm{Tr}_{\Gamma^{p^{m-1}}/\Gamma^{p^m}}\big(\mathrm{Tr}_{\mathrm{Stab}_{\Gamma}(\tilde{\chi})/\Gamma^{p^{m-1}}}(\mathbf{a}_{\tilde{\chi}})\big)\tilde{\chi}^{-1}\big(\pi(\overline{h})\big) \end{aligned}$$

where $\mathrm{Tr}_{\Gamma^{p^{m-1}}/\Gamma^{p^m}}\big(\mathrm{Tr}_{\mathrm{Stab}_{\Gamma}(\tilde{\chi})/\Gamma^{p^{m-1}}}(\mathbf{a}_{\tilde{\chi}})\big) = \mathrm{Tr}_{\mathrm{Stab}_{\Gamma}(\tilde{\chi})/\Gamma^{p^m}}(\mathbf{a}_{\tilde{\chi}})$. Therefore, one has

$$\begin{aligned} \mathrm{Tr}_{\Gamma^{p^{m-1}}/\Gamma^{p^m}}(C_{\varpi'}^{(m-1)}) &= \frac{1}{\#\overline{\mathcal{H}}_{\infty}^{(m-1,n)}} \sum_{\tilde{\chi}:\overline{\mathcal{H}}_{\infty}^{(m-1,n)} \mapsto \mathbb{C}^{\times}} \mathbf{a}_{\tilde{\chi}}^{(m)} \cdot \tilde{\chi}^{-1}\big(\pi(\overline{h})\big) \\ &= \frac{1}{\#\overline{\mathcal{H}}_{\infty}^{(m-1,n)}} \sum_{\tilde{\chi}:\overline{\mathcal{H}}_{\infty}^{(m-1,n)} \mapsto \mathbb{C}^{\times}} \tilde{\chi}\big(\mathbf{a}_m \mod [\overline{\mathcal{U}}_{(m-1,n)}, \overline{\mathcal{U}}_{(m-1,n)}]\big) \cdot \tilde{\chi}^{-1}\big(\pi(\overline{h})\big) \end{aligned}$$

On the other hand, the characteristic function of $\overline{h}$ $\mathrm{char}_{\overline{h}}(-) : \Gamma \times \mathcal{H} \mapsto \Gamma$ extends to a map

$$\mathrm{char}_{\overline{h}}(-) : \mathbb{Z}_p[[\Gamma \times \mathcal{H}]] \mapsto \mathbb{Z}_p[[\Gamma]].$$

Hence one my deduce that,

$$\begin{aligned}
\mathrm{Tr}_{\Gamma^{p^{m-1}}/\Gamma^{p^m}}\big(C_{\varpi'}^{(m-1)}\big) &= \mathrm{char}_{\pi(\overline{h})}\big(\,\mathbf{a}_m \mod [\overline{\mathcal{U}}_{(m-1,n)},\overline{\mathcal{U}}_{(m-1,n)}]\big) \\
&= \mathrm{char}_{\pi(\overline{h})}(\pi(\mathbf{a}_m)) \\
&= \sum_{\substack{\varpi_{\overline{h}}\in\mathrm{orb}_\Gamma(\overline{\mathcal{H}}_\infty^{(m,n)}),\\ \pi(\varpi_{\overline{h}})=\varpi'_{\pi(\overline{h})}}} \frac{\#\varpi'_{\pi(\overline{h})}}{\#\varpi_{\overline{h}}} \times \mathrm{char}_{\overline{h}}(\mathbf{a}_m) \\
&= \sum_{\pi(\varpi)=\varpi'} \frac{\#\varpi'}{\#\varpi} \times \frac{1}{\#\overline{\mathcal{H}}_\infty^{(m,n)}} \times \sum_{\chi:\overline{\mathcal{H}}_\infty^{(m,n)}\mapsto\mathbb{C}^\times} \mathbf{a}_\chi^{(m)}\cdot\chi^{-1}(\overline{h}) \\
&= \sum_{\pi(\varpi)=\varpi'} \frac{\#\varpi'}{\#\varpi} \times C_{\varpi}^{(m)} \quad = \quad p\times\mathrm{char}_{\Gamma^{p^m}}\big(C_{\varpi'}^{m-1}\big).
\end{aligned}$$

We have therefore shown that (A1) holds for $m' = m-1$, and the general situation follows by a simple induction on m. □

5.2 A transfer-compatible basis for the set $\mathfrak{R}_{m,n}$

Assume again that $\star\in\{\text{II,III,IV,V,VI}\}$. We can express $\overline{\mathcal{H}}_\infty^{(m,n)}$ as the double quotient

$$\overline{\mathcal{H}}_\infty^{(m,n)} \;\cong\; \frac{\mathcal{H}_\infty/\mathcal{H}_\infty^{p^n}}{\big\langle[\overline{h}_1,\gamma^{p^m}]\;,\;[\overline{h}_2,\gamma^{p^m}]\big\rangle}$$

where $\overline{h}_1$ and $\overline{h}_2$ denote the image inside $\mathcal{H}_\infty/\mathcal{H}_\infty^{p^n}$ of the subgroup generators $h_1,h_2\in\mathcal{H}_\infty$, as outlined in the Classification Theorem.

Clearly any character χ defined on $\overline{\mathcal{H}}_\infty^{(m,n)}$ must satisfy

$$\chi\big([\overline{h}_1,\gamma^{p^m}]\big) = \chi\big([\overline{h}_2,\gamma^{p^m}]\big) = 1.$$

Also $\overline{\mathcal{H}}_\infty^{(m,n)} \cong \frac{\mathbb{Z}}{p^{N_{\star,1}^{(m)}}\mathbb{Z}} \times \frac{\mathbb{Z}}{p^{N_{\star,2}^{(m)}}\mathbb{Z}}$ where $N_{\star,1}^{(m)}, N_{\star,2}^{(m)}\in\mathbb{N}$ can be read off from Proposition 4.4; one may then write

$$\big[h_1,\gamma^{p^m}\big] \;=\; \big(h_1^{\tilde{x}_1}h_2^{\tilde{y}_1}\big)^{p^{N_{\star,1}^{(m)}}} \quad\text{and}\quad \big[h_2,\gamma^{p^m}\big] \;=\; \big(h_1^{\tilde{x}_2}h_2^{\tilde{y}_2}\big)^{p^{N_{\star,2}^{(m)}}}$$

for integer pairs $(\tilde{x}_1,\tilde{y}_1)$ and $(\tilde{x}_2,\tilde{y}_2)$, neither of which is p-divisible in $\frac{\mathbb{Z}}{p^{N_{\star,1}^{(m)}}\mathbb{Z}} \times \frac{\mathbb{Z}}{p^{N_{\star,2}^{(m)}}\mathbb{Z}}$. To precisely determine them, we note that the commutator $\big[h_1^x h_2^y,\gamma^{p^m}\big]$

corresponds to the vector $\big((I_2+M)^{p^m}-I_2\big)\begin{pmatrix} x \\ y \end{pmatrix}$ inside $\mathbb{Z}_p \oplus \mathbb{Z}_p$, whence

$$\begin{pmatrix} \tilde{x}_1 & \tilde{x}_2 \\ \tilde{y}_1 & \tilde{y}_2 \end{pmatrix} = \Big(\big(I_2+M\big)^{p^m}-I_2\Big)\begin{pmatrix} p^{-N^{(m)}_{\star,1}} & 0 \\ 0 & p^{-N^{(m)}_{\star,2}} \end{pmatrix}. \tag{5.1}$$

To construct a basis for $\mathrm{Hom}\big(\overline{\mathcal{H}}^{(m,n)}_\infty, \mathbb{C}^\times\big)$, we therefore need a pair of characters $\tilde{\chi}_1$ and $\tilde{\chi}_2$, sending $h_1^{\tilde{x}_j}h_2^{\tilde{y}_j}$ to a primitive $p^{N^{(m)}_{\star,j}}$-th root of unity for each $j \in \{1,2\}$.

Recall the definition of the generating characters $\chi_{1,n}, \chi_{2,n} : \mathcal{H}_\infty \to \mu_{p^n}$ from Chapter 3, namely

$$\chi_{1,n}\big(h_1^x h_2^y\big) \;=\; \exp\big(2\pi\sqrt{-1}\;x/p^n\big) \quad \text{and} \quad \chi_{2,n}\big(h_1^x h_2^y\big) \;=\; \exp\big(2\pi\sqrt{-1}\;y/p^n\big).$$

As an illustration, in Case (II) we know $\overline{\mathcal{H}}^{(m,n)}_\infty \cong \frac{\mathcal{H}_{1,\infty}}{\mathcal{H}^{p^{s+m}}_{1,\infty}} \times \frac{\mathcal{H}_{2,\infty}}{\mathcal{H}^{p^n}_{2,\infty}}$ from Proposition 4.4, thus one may set

$$\tilde{\chi}_{1,N^{(m)}_{II,1}}\big(h_1^x h_2^y\big) := \chi_{2,n}\big(h_1^x h_2^y\big) = \zeta^y_{p^n} \quad \text{and} \quad \tilde{\chi}_{2,N^{(m)}_{II,2}}\big(h_1^x h_2^y\big) := \chi_{1,s+m}\big(h_1^x h_2^y\big) = \zeta^x_{p^{s+m}}. \tag{5.2}$$

We will now abuse our notation, and employ $\chi\begin{pmatrix} x \\ y \end{pmatrix}$ as an abbreviation for $\chi(h_1^x h_2^y)$.

Definition 5.1 *For $j \in \{1,2\}$, we define characters $\tilde{\chi}_{j,N^{(m)}_{\star,j}} : \overline{\mathcal{H}}^{(m,n)}_\infty \twoheadrightarrow \mu_{p^{N^{(m)}_{\star,j}}}$ through:*

- *if $\star \in \{III, IV, V, VI\}$, then*

$$\tilde{\chi}_{1,N^{(m)}_{\star,1}}\begin{pmatrix} x \\ y \end{pmatrix} \;:=\; \chi_{1,N^{(m)}_{\star,1}}\left(\begin{pmatrix} p^{N^{(m)}_{\star,1}} & 0 \\ 0 & 0 \end{pmatrix}\Big(\big(I_2+M\big)^{p^m}-I_2\Big)^{-1}\begin{pmatrix} x \\ y \end{pmatrix}\right)$$

and

$$\tilde{\chi}_{2,N^{(m)}_{\star,2}}\begin{pmatrix} x \\ y \end{pmatrix} \;:=\; \chi_{2,N^{(m)}_{\star,2}}\left(\begin{pmatrix} 0 & 0 \\ 0 & p^{N^{(m)}_{\star,2}} \end{pmatrix}\Big(\big(I_2+M\big)^{p^m}-I_2\Big)^{-1}\begin{pmatrix} x \\ y \end{pmatrix}\right);$$

- *if $\star = II$, one uses Equation (5.2) instead to define $\tilde{\chi}_{1,N^{(m)}_{II,1}}$ and $\tilde{\chi}_{2,N^{(m)}_{II,2}}$.*

In particular, from Equation (5.1) we see that $\tilde{\chi}_{1,N^{(m)}_{\star,1}}\big(h_1^{\tilde{x}_1}h_2^{\tilde{y}_1}\big) = \chi_{1,N^{(m)}_{\star,1}}\big(h_1^1 h_2^0\big) = \zeta_{p^{N^{(m)}_{\star,1}}}$ and $\tilde{\chi}_{2,N^{(m)}_{\star,2}}\big(h_1^{\tilde{x}_2}h_2^{\tilde{y}_2}\big) = \chi_{2,N^{(m)}_{\star,2}}\big(h_1^0 h_2^1\big) = \zeta_{p^{N^{(m)}_{\star,2}}}$, which satisfies our stated requirement. The main reason why we prefer using the character set $\big\{\tilde{\chi}_{1,N^{(m)}_{\star,1}}, \tilde{\chi}_{2,N^{(m)}_{\star,2}}\big\}$ over the more naive choice $\big\{\chi_{1,N^{(m)}_{\star,1}}, \chi_{2,N^{(m)}_{\star,2}}\big\}$ is motivated by the following compatibility result.

Proposition 5.2 *(a) The elements of* $\mathrm{Hom}\big(\overline{\mathcal{H}}^{(m,n)}_{\infty}, \mathbb{C}^{\times}\big)$ *are explicitly given by the set*

$$\left\{ \tilde{\chi}^{e_1}_{1,N^{(m)}_{\star,1}} \cdot \tilde{\chi}^{e_2}_{2,N^{(m)}_{\star,2}} \ \textit{ where } e_1 \in \mathbb{Z}/p^{N^{(m)}_{\star,1}}\mathbb{Z} \textit{ and } e_2 \in \mathbb{Z}/p^{N^{(m)}_{\star,2}}\mathbb{Z} \right\}.$$

(b) If $\star = II$ *and* $m > m'$*, then*

$$\tilde{\chi}_{1,N^{(m)}_{\star,1}} \circ \mathrm{Ver}_{m',m} = \Big(\tilde{\chi}_{1,N^{(m')}_{\star,1}}\Big)^{p^{m-m'}} \quad \textit{and} \quad \tilde{\chi}_{2,N^{(m)}_{\star,2}} \circ \mathrm{Ver}_{m',m} = \tilde{\chi}_{2,N^{(m')}_{\star,2}}.$$

(c) If $\star \in \{III, IV, V, VI\}$ *and* $m > m'$*, then* $\tilde{\chi}_{j,N^{(m)}_{\star,j}} \circ \mathrm{Ver}_{m',m} = \tilde{\chi}_{j,N^{(m')}_{\star,j}}$ *at each* $j \in \{1,2\}$.

Proof. Let us first suppose $\star =$ II. Here one has $[\overline{h}_1, \gamma^{p^m}] = 1$ and $[\overline{h}_2, \gamma^{p^m}] = \overline{h}_1^{p^{s+m}}$ with $N^{(m)}_{II,1} = n$ and $N^{(m)}_{II,2} = s+m$, whilst $\tilde{\chi}_{1,N^{(m)}_{II,1}}\big(\overline{h}_1^x \overline{h}_2^y\big) = \zeta^y_{p^n}$ and $\tilde{\chi}_{2,N^{(m)}_{II,1}}\big(\overline{h}_1^x \overline{h}_2^y\big) = \zeta^x_{p^{s+m}}$. Part (a) then follows as $\tilde{\chi}_{1,N^{(m)}_{II,1}}$ and $\tilde{\chi}_{2,N^{(m)}_{II,1}}$ are independent, while $\#\overline{\mathcal{H}}^{(m,n)}_{\infty} = p^n \cdot p^{s+m}$. To show (b) one notes for $j = 1,2$ that $\tilde{\chi}_{j,N^{(m)}_{II,j}} \circ \mathrm{Ver}_{m',m}\Big|_{\mathcal{H}^{(m',n)}_{\infty}} = \tilde{\chi}^{p^{m-m'}}_{j,N^{(m)}_{II,j}}$ by Lemma 4.7, in which case

$$\tilde{\chi}_{1,N^{(m)}_{II,1}}\big((\overline{h}_1^x \overline{h}_2^y)^{p^{m-m'}}\big) = \big(\zeta^y_{p^n}\big)^{p^{m-m'}} \text{ and } \tilde{\chi}_{2,N^{(m)}_{II,2}}\big((\overline{h}_1^x \overline{h}_2^y)^{p^{m-m'}}\big) = \big(\zeta^x_{p^{s+m}}\big)^{p^{m-m'}} = \zeta^x_{p^{s+m'}}.$$

Let us instead suppose $\star \in \{$III,IV,V,VI$\}$. Since $\big(I_2+M\big)^{p^m} = P_\star \begin{pmatrix} \lambda^{p^m}_{\star,+} & 0 \\ 0 & \lambda^{p^m}_{\star,-} \end{pmatrix} P_\star^{-1}$, we deduce that

$$\begin{pmatrix} p^{N^{(m)}_{\star,1}} & 0 \\ 0 & 0 \end{pmatrix} \Big(\big(I_2+M\big)^{p^m} - I_2\Big)^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} P_\star \begin{pmatrix} \frac{p^{N^{(m)}_{\star,1}}}{\lambda^{p^m}_{\star,+}-1} & 0 \\ 0 & \frac{p^{N^{(m)}_{\star,1}}}{\lambda^{p^m}_{\star,-}-1} \end{pmatrix} P_\star^{-1}.$$

On the other hand, again from Lemma 4.7 the matrix corresponding to $\mathrm{Ver}_{m',m}\Big|_{\mathcal{H}^{(m',n)}_{\infty}}$ is given by $P_\star \begin{pmatrix} \frac{\lambda^{p^m}_{\star,+}-1}{\lambda^{p^{m'}}_{\star,+}-1} & 0 \\ 0 & \frac{\lambda^{p^m}_{\star,-}-1}{\lambda^{p^{m'}}_{\star,-}-1} \end{pmatrix} P_\star^{-1}$. An elementary calculation reveals the identities

$$\begin{aligned}
&\begin{pmatrix} p^{N^{(m)}_{\star,1}} & 0 \\ 0 & 0 \end{pmatrix} \Big((I_2+M)^{p^m} - I_2 \Big)^{-1} \cdot P_\star \begin{pmatrix} \frac{\lambda_{\star,+}^{p^m}-1}{\lambda_{\star,+}^{p^{m'}}-1} & 0 \\ 0 & \frac{\lambda_{\star,-}^{p^m}-1}{\lambda_{\star,-}^{p^{m'}}-1} \end{pmatrix} P_\star^{-1} \begin{pmatrix} x \\ y \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} P_\star \begin{pmatrix} \frac{p^{N^{(m)}_{\star,1}}}{\lambda_{\star,+}^{p^m}-1} & 0 \\ 0 & \frac{p^{N^{(m)}_{\star,1}}}{\lambda_{\star,-}^{p^m}-1} \end{pmatrix} \begin{pmatrix} \frac{\lambda_{\star,+}^{p^m}-1}{\lambda_{\star,+}^{p^{m'}}-1} & 0 \\ 0 & \frac{\lambda_{\star,-}^{p^m}-1}{\lambda_{\star,-}^{p^{m'}}-1} \end{pmatrix} P_\star^{-1} \begin{pmatrix} x \\ y \end{pmatrix} \\
&= p^{N^{(m)}_{\star,1} - N^{(m')}_{\star,1}} \begin{pmatrix} p^{N^{(m')}_{\star,1}} & 0 \\ 0 & 0 \end{pmatrix} \Big((I_2+M)^{p^{m'}} - I_2 \Big)^{-1} \begin{pmatrix} x \\ y \end{pmatrix}.
\end{aligned}$$

These matrix identities directly imply that $\tilde{\chi}_{1,N^{(m)}_{\star,1}} \circ \mathrm{Ver}_{m',m} \begin{pmatrix} x \\ y \end{pmatrix}$ equals

$$\Big(\chi_{1,N^{(m)}_{\star,1}} \Big)^{p^{N^{(m)}_{\star,1} - N^{(m')}_{\star,1}}} \left(\begin{pmatrix} p^{N^{(m')}_{\star,1}} & 0 \\ 0 & 0 \end{pmatrix} \Big((I_2+M)^{p^{m'}} - I_2 \Big)^{-1} \begin{pmatrix} x \\ y \end{pmatrix} \right).$$

Since $\Big(\chi_{1,N^{(m)}_{\star,1}} \Big)^{p^{N^{(m)}_{\star,1} - N^{(m')}_{\star,1}}} = \chi_{1,N^{(m')}_{\star,1}}$ the above quantity is none other than $\tilde{\chi}_{1,N^{(m')}_{\star,1}} \begin{pmatrix} x \\ y \end{pmatrix}$, which establishes that $\tilde{\chi}_{1,N^{(m)}_{\star,1}} \circ \mathrm{Ver}_{m',m} = \tilde{\chi}_{1,N^{(m')}_{\star,1}}$.

The argument for the second composition $\tilde{\chi}_{2,N^{(m)}_{\star,2}} \circ \mathrm{Ver}_{m',m}$ follows identical lines. □

Lemma 5.3 *(i) If $\overline{h}_1^x \overline{h}_2^y \in \overline{\mathcal{H}}_\infty^{(m',n)}$ and $f(X) \in \mathbb{Z}_p[\![X]\!]$, then*

$$\mathrm{Ver}_{m',m}\Big(f\big(\gamma^{p^{m'}} - 1\big) \cdot \mathcal{A}^{(m',n)}_{\overline{h}_1^x \overline{h}_2^y} \Big) \;=\; p^{-(m-m')} \times f\big(\gamma^{p^m} - 1\big) \cdot \mathcal{A}^{(m,n)}_{\overline{h}_1^{x'} \overline{h}_2^{y'}}$$

where x', y' are as in Lemma 4.7.

(ii) Using exactly the same notation,

$$\tilde{\chi}^{e_1}_{1,N^{(m')}_{\star,1}} \cdot \tilde{\chi}^{e_2}_{2,N^{(m')}_{\star,2}} \Big(\mathcal{A}^{(m',n)}_{\overline{h}_1^x \overline{h}_2^y} \Big) \;=\; p^{-(m-m')} \;\times\; \tilde{\chi}^{e_1}_{1,N^{(m)}_{\star,1}} \cdot \tilde{\chi}^{e_2}_{2,N^{(m)}_{\star,2}} \Big(\mathcal{A}^{(m,n)}_{\overline{h}_1^{x'} \overline{h}_2^{y'}} \Big)$$

unless $\star = II$, in which case one replaces $\tilde{\chi}^{e_1}_{1,N^{(m')}_{\star,1}} \cdot \tilde{\chi}^{e_2}_{2,N^{(m')}_{\star,2}}$ instead with $\tilde{\chi}^{e_1 p^{m-m'}}_{1,N^{(m')}_{\star,1}} \cdot \tilde{\chi}^{e_2}_{2,N^{(m')}_{\star,2}}$ on the left-hand side of this formula.

Proof. Let us start by establishing (i). If $\begin{pmatrix} x_i \\ y_i \end{pmatrix} = \left(I_2 + M\right)^i \begin{pmatrix} x \\ y \end{pmatrix}$ for all $i \geq 0$, then

$$\mathrm{Ver}_{m',m}\left(\gamma^{p^{m'}j} \cdot \mathcal{A}^{(m',n)}_{\overline{h}_1^x \overline{h}_2^y}\right) \;=\; \sum_{i=0}^{p^{m'}-1} \mathrm{Ver}_{m',m}\left(\gamma^{p^{m'}j} \cdot \overline{h}_1^{x_i} \overline{h}_2^{y_i}\right) \;=\; \gamma^{p^m j} \cdot \sum_{i=0}^{p^{m'}-1} \overline{h}_1^{x'_i} \overline{h}_2^{y'_i}$$

upon applying Lemma 4.7. Here in Case ($\star$) with $\star \in$ {III,IV,V,VI}, the vector

$$\begin{aligned} \begin{pmatrix} x'_i \\ y'_i \end{pmatrix} &= P_\star \begin{pmatrix} \frac{\lambda_{\star,+}^{p^m}-1}{\lambda_{\star,+}^{p^{m'}}-1} & 0 \\ 0 & \frac{\lambda_{\star,-}^{p^m}-1}{\lambda_{\star,-}^{p^{m'}}-1} \end{pmatrix} P_\star^{-1} \begin{pmatrix} x_i \\ y_i \end{pmatrix} \\ &= P_\star \begin{pmatrix} \lambda_{\star,+}^i \cdot \frac{\lambda_{\star,+}^{p^m}-1}{\lambda_{\star,+}^{p^{m'}}-1} & 0 \\ 0 & \lambda_{\star,-}^i \cdot \frac{\lambda_{\star,-}^{p^m}-1}{\lambda_{\star,-}^{p^{m'}}-1} \end{pmatrix} P_\star^{-1} \begin{pmatrix} x \\ y \end{pmatrix} \;=\; \left(I_2 + M\right)^i \begin{pmatrix} x' \\ y' \end{pmatrix} \end{aligned}$$

so that $\mathrm{Ver}_{m',m}\left(\gamma^{p^{m'}j} \cdot \mathcal{A}^{(m',n)}_{\overline{h}_1^x \overline{h}_2^y}\right)$ equals $\gamma^{p^m j} \cdot \sum_{i=0}^{p^{m'}-1} \gamma^{-i} \overline{h}_1^{x'} \overline{h}_2^{y'} \gamma^i = \gamma^{p^m j} \cdot p^{m'-m} \mathcal{A}^{(m,n)}_{\overline{h}_1^{x'} \overline{h}_2^{y'}}$ (the same identity for the Verlagerung holds in Case (II) also). The result extends to the completed group algebra by linearity and continuity.

Secondly to show part (ii) is true, we first set $f(X) = 1$ and then evaluate the identity from (i) at the character $\tilde{\chi}^{e_1}_{1,N^{(m)}_{\star,1}} \cdot \tilde{\chi}^{e_2}_{2,N^{(m)}_{\star,2}}$. We next use Proposition 5.2(b)-(c) to rewrite the transformed left-hand side in terms of the powers of $\tilde{\chi}_{1,N^{(m')}_{\star,1}}$ and $\tilde{\chi}_{2,N^{(m')}_{\star,2}}$. □

Chapter 6

The Multiplicative Calculations

To complete the proof of the main theorem, our strategy is to establish the existence, commutativity and row-exactness of the diagram

$$\begin{tikzcd}
1 \arrow[r] & \mathbb{F}_p^\times \times \mathcal{G}_{\infty,n}^{\mathrm{ab}} \arrow[r] \arrow[d, equal] & K_1'\big(\mathbb{Z}_p\llbracket\mathcal{G}_{\infty,n}\rrbracket\big) \arrow[r, "\mathrm{LOG}"] \arrow[d, "\Theta_{\infty,n}"] & \mathbb{Z}_p\big[\big[\mathrm{Conj}(\mathcal{G}_{\infty,n})\big]\big] \arrow[r] \arrow[d, "\Theta_{\infty,n}^{+}"] & \mathcal{G}_{\infty,n}^{\mathrm{ab}} \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & \mathbb{F}_p^\times \times \mathcal{G}_{\infty,n}^{\mathrm{ab}} \arrow[r] \arrow[d, equal] & \Phi \arrow[r, "\mathcal{L}"] \arrow[d, "\underline{\chi}"] & \Psi \arrow[r] \arrow[d, "\underline{\chi}"] & \mathcal{G}_{\infty,n}^{\mathrm{ab}} \arrow[r] & 1 \\
1 \arrow[r] & \mathbb{F}_p^\times \times \mathcal{G}_{\infty,n}^{\mathrm{ab}} \arrow[r] & \underline{\chi}(\Phi) \arrow[r, "\mathcal{L}_{\underline{\chi}}"] \arrow[d, hook] & \underline{\chi}(\Psi) \arrow[d, hook] & & \\
& & \prod\limits_{m,\chi} \mathcal{O}_{\mathbb{C}_p}\big[\big[\mathrm{Stab}_\Gamma(\chi)\big]\big]^\times & \Big(\prod\limits_{m,\chi} \mathcal{O}_{\mathbb{C}_p}\big[\big[\mathrm{Stab}_\Gamma(\chi)\big]\big]\Big) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p. & &
\end{tikzcd} \tag{6.1}$$

The top two lines of this diagram are precisely those occurring in [CSRV12, p80]. The vertical arrows labelled as "$\underline{\chi}$" denote evaluation at a system of representatives $\mathfrak{R}_{m,n}$, and as $\mathcal{G}_{\infty,n}^{\mathrm{ab}} \cong \Gamma$, the whole ensemble $\underline{\chi}$ therefore restricts to being the identity map on $\mathbb{F}_p^\times \times \mathcal{G}_{\infty,n}^{\mathrm{ab}}$. At this preliminary stage, we make no attempt to explain the maps LOG, $\mathcal{L}$ and $\mathcal{L}_{\underline{\chi}}$.

From Chapter 5, the module $\Psi \subset \prod_m \mathbb{Z}_p\big[\big[\mathcal{U}_{m,n}^{\mathrm{ab}}\big]\big]$ will consist of elements satisfying Kakde's additive conditions (A1)-(A3). Analogously, $\Phi \subset \prod_m \mathbb{Z}_p\big[\big[\mathcal{U}_{m,n}^{\mathrm{ab}}\big]\big]^\times$ consists of those elements $\big(\mathbf{y}_m\big)$ satisfying the multiplicative conditions (M1)-(M4) below, which we have specialised from [CSRV12, p107] to our particular situation:

(M1) $\mathcal{N}_{m-1,m}\big(\mathbf{y}_{m-1}\big) = \pi_{m,m-1}\big(\mathbf{y}_m\big)$ for all $m \geq 1$;

(M2) $\mathbf{y}_m = g\mathbf{y}_m g^{-1}$ at every $g \in \mathcal{G}_{\infty,n}$;

(M3) $\mathbf{y}_m \equiv \mathrm{Ver}_{m-1,m}(\mathbf{y}_{m-1}) \mod \mathrm{Im}\big(\widetilde{\sigma_m}\big)$ for each $m \geq 1$;

(M4) $\dfrac{\big(\mathbf{y}_m^{(\nu)}\big)^p}{\mathcal{N}_{m,m+1}\big(\mathbf{y}_m^{(\nu)}\big)} - \varphi\left(\dfrac{\big(\mathbf{y}_{m-1}^{(\nu)}\big)^p}{\mathcal{N}_{m-1,m}\big(\mathbf{y}_{m-1}^{(\nu)}\big)}\right) \in p \cdot \mathrm{Im}\big(\sigma_m^{(\nu)}\big)$ for every $m \geq 0$.

Here in condition (M3), the homomorphism $\widetilde{\sigma_m} : \mathbb{Z}_p\big[\big[\mathcal{U}_{m,n}^{\mathrm{ab}}\big]\big] \to \mathbb{Z}_p\big[\big[\mathcal{U}_{m,n}^{\mathrm{ab}}\big]\big]$ denotes the additive map sending $f \mapsto \sum_{i=0}^{p-1} \gamma^{-p^{m-1}i} f \gamma^{p^{m-1}i}$.

Warning: If a sequence $\big(\mathbf{y}_m\big)$ satisfies conditions (M1)-(M4), then its image under $\mathcal{L}$ automatically satisfies (A1)-(A3) by [CSRV12, p107, Lemma 4.5]. Unfortunately, because the family of abelianizations $\big\{\mathcal{U}_{m,n}^{\mathrm{ab}}\big\}_{0\leq m\leq n-s}$ we use is *coarser* than that considered in [CSRV12, Kak13], we cannot directly apply the results in *op. cit.* to obtain a converse statement such as

$$\mathcal{L}\big((\mathbf{y}_m)\big) \in \Big(\prod_m \mathbb{Z}_p\big[\big[\mathcal{U}_{m,n}^{\mathrm{ab}}\big]\big]\Big)_{\text{(A1)-(A3)}} \overset{?}{\Longrightarrow} \big(\mathbf{y}_m\big) \in \Big(\prod_m \mathbb{Z}_p\big[\big[\mathcal{U}_{m,n}^{\mathrm{ab}}\big]\big]^{\times}\Big)_{\text{(M1)-(M4)}}.$$

The salvage is to show that $K_1\big(\mathbb{Z}_p[\![\mathcal{G}_{\infty,n}]\!]\big)$ splits into a direct product of $K_1\big(\mathbb{Z}_p[\![\Gamma]\!]\big)$ with with a complementary factor $\mathcal{W}_\dagger$; we shall then construct a section $\mathcal{S} : p \cdot \Psi \to \Theta_{\infty,n}\big(\mathcal{W}_\dagger\big)$ for which $\mathcal{L} \circ \mathcal{S}$ and $\mathcal{S} \circ \mathcal{L}\big|_{\Theta_{\infty,n}(\mathcal{W}_\dagger)}$ are both identity maps. One concludes that $\big(\mathbf{y}_m\big)$ arises from $K_1'\big(\mathbb{Z}_p[\![\mathcal{G}_{\infty,n}]\!]\big)$ if and only if $\mathcal{L}\big((\mathbf{y}_m)\big) \in p \cdot \Psi$, which is itself equivalent to the sequence $\underline{\chi} \circ \mathcal{L}\big((\mathbf{y}_m)\big)$ satisfying constraints (C1)–(C4) from Theorem 5.1.

6.1 Convergence of the logarithm on $\mathrm{Im}(\sigma_m)$

We will shortly introduce the Taylor-Oliver logarithm, which is usually defined in terms of group algebras arising from finite groups. Since the profinite groups $\mathcal{G}_{\infty,n}$ and $\mathcal{U}_{m,n}$ are both infinite, one should instead consider their finite counterparts

$$\mathcal{G}_{\infty,n}^{(\nu)} := \Gamma/\Gamma^{p^\nu} \ltimes \mathcal{H}_\infty/\mathcal{H}_\infty^{p^n} \quad \text{and more generally} \quad \mathcal{U}_{m,n}^{(\nu)} := \Gamma^{p^m}/\Gamma^{p^\nu} \ltimes \mathcal{H}_\infty/\mathcal{H}_\infty^{p^n},$$

at each integer triple $m, n, \nu \in \mathbb{Z}$ with $0 \leq m \leq n - s \leq \nu$. For example, $\mathcal{U}_{0,n}^{(\nu)}$ equals $\mathcal{G}_{\infty,n}^{(\nu)}$.

Remark: Using Proposition 4.4, one has $\mathcal{U}_{n-s,n}^{\mathrm{ab}} \cong \mathcal{U}_{n-s,n}$; in other words $\mathcal{U}_{n-s,n}$ is abelian. It follows that Γ^{p^ν} acts trivially on $\mathcal{H}_\infty/\mathcal{H}_\infty^{p^n}$ for all $\nu \geq n-s$, so the semi-direct products above make good sense. Whenever we write the superscript ${}^{(\nu)}$ above an object or a map, we mean the analogue of that object/map for the corresponding finite group (providing the object/map descends to its finite version, of course).

Now recall from Proposition 4.5(ii) that $\mathrm{Im}(\sigma_m)$ is freely generated over $\mathbb{Z}_p[\![\Gamma^{p^m}]\!]$ by the elements $\mathcal{A}_\varpi^{(m,n)}$ with $\varpi \in \mathrm{orb}_\Gamma\big(\overline{\mathcal{H}}_\infty^{(m,n)}\big)$. It is therefore trivially true that $\mathrm{Im}\big(\sigma_m^{(\nu)}\big)$ must be generated over $\mathbb{Z}_p\big[\Gamma^{p^m}/\Gamma^{p^\nu}\big]$ by the same $\mathcal{A}_\varpi^{(m,n)}$'s. If $\varpi_1, \varpi_2 \in \mathrm{orb}_\Gamma\big(\overline{\mathcal{H}}_\infty^{(m,n)}\big)$ contain $\overline{h}_1$ and $\overline{h}_2$ respectively, then

$$\mathcal{A}_{\varpi_1}^{(m,n)} \cdot \mathcal{A}_{\varpi_2}^{(m,n)} = \sum_{i=0}^{p^m-1} \gamma^{-i}\overline{h}_1\gamma^i \cdot \sum_{j=0}^{p^m-1} \gamma^{-j}\overline{h}_2\gamma^j = \sum_{i=0}^{p^m-1}\sum_{j=0}^{p^m-1} \gamma^{-i}\big(\overline{h}_1\overline{h}_2^{\gamma^{j-i}}\big)\gamma^i = \sum_{t=0}^{p^m-1} \mathcal{A}_{\overline{h}_1\overline{h}_2^{\gamma^t}}^{(m,n)}$$

which belongs to the image of $\sigma_m^{(\nu)}$. It follows that $\mathrm{Im}\big(\sigma_m^{(\nu)}\big)$ is an ideal of $\mathbb{Z}_p\big[\mathcal{U}_{m,n}^{(\nu),\mathrm{ab}}\big]$. Iterating the above calculation N-times, one deduces that

$$\mathcal{A}_{\varpi_1}^{(m,n)} \cdot \mathcal{A}_{\varpi_2}^{(m,n)} \cdots \mathcal{A}_{\varpi_{N+1}}^{(m,n)} = \sum_{t_1=0}^{p^m-1}\sum_{t_2=0}^{p^m-1} \cdots \sum_{t_N=0}^{p^m-1} \mathcal{A}_{\overline{h}_1\overline{h}_2^{\gamma^{t_1}}\cdots\overline{h}_{N+1}^{\gamma^{t_N}}}^{(m,n)}$$

which means for each $\varpi \in \mathrm{orb}_\Gamma\big(\overline{\mathcal{H}}_\infty^{(m,n)}\big)$ and element $\overline{h} \in \varpi$,

$$\big(\mathcal{A}_\varpi^{(m,n)}\big)^{N+1} = \sum_{t_1=0}^{p^m-1} \cdots \sum_{t_N=0}^{p^m-1} \mathcal{A}_{\overline{h}\,\overline{h}^{\gamma^{t_1}}\cdots\overline{h}^{\gamma^{t_N}}}^{(m,n)} = \prod_{j=2}^{N+1} \frac{p^m}{\#\varpi} \cdot \sum_{w_2\in\varpi} \cdots \sum_{w_{N+1}\in\varpi} \mathcal{A}_{\overline{h}w_2\cdots w_{N+1}}^{(m,n)}.$$

- Clearly if $\#\varpi < p^m$, then $\left(\mathcal{A}_\varpi^{(m,n)}\right)^{N+1} \in p^N \cdot \mathrm{Im}\big(\sigma_m^{(\nu)}\big) \subset p \cdot \mathrm{Im}\big(\sigma_m^{(\nu)}\big)$.
- Alternatively, if $\#\varpi = p^m$ so that $\mathrm{Stab}_{\Gamma/\Gamma^{p^m}}\big(\overline{h}\big) = \big\{\gamma^{p^m}\big\}$, then

$$\big(\mathcal{A}_\varpi^{(m,n)}\big)^{N+1} = \sum_{w_2\in\varpi} \cdots \sum_{w_{N+1}\in\varpi} \mathcal{A}_{\overline{h}w_2\cdots w_{N+1}}^{(m,n)} = \sum_{(t_1,\ldots,t_N)\in(\mathbb{Z}/p^m\mathbb{Z})^{\oplus N}} \mathcal{A}_{\overline{h}\,\overline{h}^{\gamma^{t_1}}\cdots\overline{h}^{\gamma^{t_N}}}^{(m,n)}.$$

There are at most p^{mN} distinct elements of the form $\overline{h}\;\overline{h}^{\gamma^{t_1}} \cdots \overline{h}^{\gamma^{t_N}}$, whilst the total number of elements in $\overline{\mathcal{H}}_\infty^{(m,n)}$ is $p^{2s+2m+\epsilon_{\star,p}}$ if $(\star)$ $\neq$(II), where by

Proposition 4.4 the term

$$\epsilon_{\star,p} \;:=\; N^{(m)}_{\star,1} + N^{(m)}_{\star,2} - 2s - 2m \;=\; \begin{cases} 0 & \text{in Cases (III),(IV)} \\ \mathrm{ord}_p(d) & \text{in Case (V)} \\ r + \mathrm{ord}_p(t) & \text{in Case (VI)} \end{cases}$$

is independent of m and n.

Consequently for $mN \geq 2s + 2m + \epsilon_{\star,p}$ these elements $\overline{h}\,\overline{h}^{\gamma^{t_1}} \cdots \overline{h}^{\gamma^{t_N}}$ will start repeating, in which case $\left(\mathcal{A}^{(m,n)}_{\varpi}\right)^{N+1} \in p \cdot \mathrm{Im}\big(\sigma^{(\nu)}_m\big)$. Note that the latter inequality is equivalent to $N + 1 \geq 3 + \frac{2s+\epsilon_{\star,p}}{m}$, so we arrive at the following estimate:

$$\frac{\left(\mathcal{A}^{(m,n)}_{\varpi}\right)^j}{j} \;\in\; p^{\left\lfloor \frac{j}{3+\frac{2s+\epsilon_{\star,p}}{m}} \right\rfloor - \frac{\log(j)}{\log(p)}} \cdot \mathrm{Im}\big(\sigma^{(\nu)}_m\big). \tag{6.2}$$

If one sets $\epsilon_{\star,p} = -s$ and $n = m$, a similar argument implies (6.2) also holds for $(\star)$ =(II).

Proposition 6.1 *(a) The two formal power series* $\log(1+y) = \sum_{j=1}^{\infty}(-1)^{j+1}\frac{y^j}{j}$ *and* $(1 + y)^{-1} = \sum_{j=0}^{\infty}(-1)^j y^j$ *converge for all* $y \in \mathrm{Im}\big(\sigma^{(\nu)}_m\big)$.

(b) If $\delta_m := \left\lceil \frac{3+\frac{2s+\epsilon_{\star,p}}{m}}{p} \right\rceil$ *then for every* $N \geq 1$, *the logarithm induces a natural isomorphism*

$$\overline{\log} : \frac{1 + \mathrm{Im}\big(\sigma^{(\nu)}_m\big)^{\delta_m \cdot N}}{1 + \mathrm{Im}\big(\sigma^{(\nu)}_m\big)^{\delta_m \cdot N+1}} \;\xrightarrow{\sim}\; \frac{\mathrm{Im}\big(\sigma^{(\nu)}_m\big)^{\delta_m \cdot N}}{\mathrm{Im}\big(\sigma^{(\nu)}_m\big)^{\delta_m \cdot N+1}}\,;$$

in particular, if $p \geq 5$ *and one chooses* $m \geq 2s + \epsilon_{\star,p}$, *then* $\delta_m = 1$ *above.*

(c) There are isomorphisms $1 + p \cdot \mathrm{Im}\big(\sigma^{(\nu)}_m\big) \overset{\log}{\to} p \cdot \mathrm{Im}\big(\sigma^{(\nu)}_m\big)$ *and* $p \cdot \mathrm{Im}\big(\sigma^{(\nu)}_m\big) \overset{\exp}{\to} 1 + p \cdot \mathrm{Im}\big(\sigma^{(\nu)}_m\big)$ *which are mutually inverse maps to one another.*

Proof. To show (a) one uses the estimate (6.2) together with the fact that the exponent $\left\lfloor \frac{j}{3+\frac{2s+\epsilon_{\star,p}}{m}} \right\rfloor - \frac{\log(j)}{\log(p)} \to \infty$ as $j \to \infty$, which implies both $\lim_{j\to\infty}(-1)^{j+1}\frac{y^j}{j} = 0$ and $\lim_{j\to\infty}(-1)^j y^j = 0$. In fact, since $\mathrm{Im}\big(\sigma^{(\nu)}_m\big)^j \subset p \cdot \mathrm{Im}\big(\sigma^{(\nu)}_m\big)$ for $j \gg 0$, the topology induced by the neighborhoods $\left\{\mathrm{Im}\big(\sigma^{(\nu)}_m\big)^j\right\}_{j\in\mathbb{N}}$ coincides with the p-adic topology.

The assertion in (c) can be proved by following an identical argument to [CSRV12, p106], which leaves us to tackle (b).

For simplicity we suppose that $p \geq 5$ and $m \geq 2s + \epsilon_{\star,p}$, so that $\frac{(\mathcal{A}_{\varpi}^{(m,n)})^p}{p} \in \mathrm{Im}\big(\sigma_m^{(\nu)}\big)$ by the estimate (6.2), whence $\frac{y^p}{p} \in \mathrm{Im}\big(\sigma_m^{(\nu)}\big)$ for all $y \in \mathrm{Im}\big(\sigma_m^{(\nu)}\big)$. Consider the homomorphism

$$\log^{\dagger} : 1 + \mathrm{Im}\big(\sigma_m^{(\nu)}\big)^N \;\to\; \frac{\mathrm{Im}\big(\sigma_m^{(\nu)}\big)^N}{\mathrm{Im}\big(\sigma_m^{(\nu)}\big)^{N+1}} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$$

given by $\log^{\dagger}(1+y) := \log(1+y) \mod \mathrm{Im}\big(\sigma_m^{(\nu)}\big)^{N+1}$. Assuming that $j > 1$, let us examine the p-integrality of $(-1)^{j+1}\frac{y^j}{j}$ for each $y = a_1 \cdots a_N \in \mathrm{Im}\big(\sigma_m^{(\nu)}\big)^N$:

- If $p \nmid j$ then $(-1)^{j+1}\frac{y^j}{j} = \pm\frac{a_1^j \cdots a_N^j}{j} \in \mathrm{Im}\big(\sigma_m^{(\nu)}\big)^{Nj} \subset \mathrm{Im}\big(\sigma_m^{(\nu)}\big)^{N+1}$;
- If $j = p$ then $(-1)^{p+1}\frac{y^p}{p} = \frac{a_1^p}{p} \cdot a_2^p \cdots a_N^p \in \mathrm{Im}\big(\sigma_m^{(\nu)}\big)^{1+p(N-1)} \subset \mathrm{Im}\big(\sigma_m^{(\nu)}\big)^{N+1}$;
- If $j = p^k$ with $k > 1$, then

$$(-1)^{p^k+1}\frac{y^{p^k}}{p^k} = \left(\frac{a_1^p}{p}\right)^k \cdot a_1^{p^k - pk} \cdot a_2^{p^k} \cdots a_N^{p^k} \in \mathrm{Im}\big(\sigma_m^{(\nu)}\big)^{k + p^k N - pk} \subset \mathrm{Im}\big(\sigma_m^{(\nu)}\big)^{N+1}.$$

Lastly, the general case where $j = p^k c$ with $p \nmid c$ and $j > 1$ reduces to the previous cases, upon replacing y with y^c throughout.

We therefore conclude $(-1)^{j+1}\frac{y^j}{j} \in \mathrm{Im}\big(\sigma_m^{(\nu)}\big)^{N+1}$ for every $y \in \mathrm{Im}\big(\sigma_m^{(\nu)}\big)^N$ and $j > 1$. Because $\log^{\dagger}(1+y) \equiv y \mod \mathrm{Im}(\sigma_m^{(\nu)})^{N+1}$, clearly $\log^{\dagger} : 1 + \mathrm{Im}\big(\sigma_m^{(\nu)}\big)^N \to \frac{\mathrm{Im}(\sigma_m^{(\nu)})^N}{\mathrm{Im}(\sigma_m^{(\nu)})^{N+1}}$ must be a surjective map; further, one easily checks that $1 + \mathrm{Im}\big(\sigma_m^{(\nu)}\big)^{N+1} \subset \mathrm{Ker}\big(\log^{\dagger}\big)$. Assertion (b) now follows immediately for $p \geq 5$ and $m \geq 2s + \epsilon_{\star,p}$.

Finally, to treat assertion (b) when $p = 3$ or $m < 2s + \epsilon_{\star,p}$, one simply observes that if $\delta_m \geq \frac{3 + \frac{2s+\epsilon_{\star,p}}{m}}{p}$ then $\frac{(y^{\delta_m})^p}{p} \in \mathrm{Im}\big(\sigma_m^{(\nu)}\big)$ for all $y \in \mathrm{Im}\big(\sigma_m^{(\nu)}\big)$, using the estimate (6.2) again. One then repeats the previous arguments, with y replaced by y^{δ_m} everywhere. □

6.2 Interaction of the theta-maps with both φ and log

We now derive some technical results describing how the Frobenius mapping φ and the logarithm commute with the theta-homomorphisms. Let us recall that in our situation, the trace and norm maps from $\mathcal{G}_{\infty,n}^{(\nu)}$ down to $\mathcal{U}_{m,n}^{(\nu)}$ have the simple description

$$\mathrm{Tr}_{\mathcal{G}^{(\nu)}_{\infty,n}/\mathcal{U}^{(\nu)}_{m,n}}(\alpha) \;=\; \sum_{k=0}^{p^m-1}\gamma^{-k}\alpha\gamma^k \quad\text{ and }\quad \mathrm{Norm}_{\mathcal{G}^{(\nu)}_{\infty,n}/\mathcal{U}^{(\nu)}_{m,n}}(x) \;=\; \prod_{k=0}^{p^m-1}\gamma^{-k}x\gamma^k.$$

Definition 6.1 *(a) The additive theta-map* $\theta^{(\nu),+}_{m,n} : \mathbb{Z}_p\big[\mathrm{Conj}\big(\mathcal{G}^{(\nu)}_{\infty,n}\big)\big] \to \mathbb{Z}_p\big[\mathcal{U}^{(\nu),\mathrm{ab}}_{m,n}\big]$ *is given by the composition*

$$\theta^{(\nu),+}_{m,n}(-) \;:=\; \mathrm{Tr}_{\mathcal{G}^{(\nu)}_{\infty,n}/\mathcal{U}^{(\nu)}_{m,n}}(-) \mod \big[\mathcal{U}^{(\nu)}_{m,n},\mathcal{U}^{(\nu)}_{m,n}\big].$$

(b) The multiplicative theta-map $\theta^{(\nu)}_{m,n} : K_1\big(\mathbb{Z}_p\big[\mathcal{G}^{(\nu)}_{\infty,n}\big]\big) \to \mathbb{Z}_p\big[\mathcal{U}^{(\nu),\mathrm{ab}}_{m,n}\big]^\times$ *is defined by*

$$\theta^{(\nu)}_{m,n}(-) \;:=\; \mathrm{Norm}_{\mathcal{G}^{(\nu)}_{\infty,n}/\mathcal{U}^{(\nu)}_{m,n}}(-) \mod \big[\mathcal{U}^{(\nu)}_{m,n},\mathcal{U}^{(\nu)}_{m,n}\big].$$

Let $\iota : \mathbb{Z}_p\big[\Gamma/\Gamma^{p^\nu}\big] \hookrightarrow \mathbb{Z}_p\big[\mathcal{G}^{(\nu)}_{\infty,n}\big]$ be the map on group algebras induced from the sequence $\Gamma/\Gamma^{p^\nu} \overset{\sim}{\to} \Gamma/\Gamma^{p^\nu} \ltimes \{1\} \hookrightarrow \mathcal{G}^{(\nu)}_{\infty,n}$ that identifies Γ/Γ^{p^ν} with a non-normal subgroup of $\mathcal{G}^{(\nu)}_{\infty,n}$.

Lemma 6.2 *There exists a splitting of abelian groups*

$$K_1\big(\mathbb{Z}_p\big[\mathcal{G}^{(\nu)}_{\infty,n}\big]\big) \;\overset{\sim}{\longrightarrow}\; \mathbb{Z}_p\big[\Gamma/\Gamma^{p^\nu}\big]^\times \times \mathcal{W}^{(\nu)}_\dagger \quad \textit{sending } x \mapsto \big(x^{\mathrm{cy}}, x^\dagger\big),$$

where $x^{\mathrm{cy}} = \iota_* \circ \theta^{(\nu)}_{0,n}(x)$, $x^\dagger = \frac{x}{x^{\mathrm{cy}}}$, *and the complement* $\mathcal{W}^{(\nu)}_\dagger := \big\{x^\dagger \;\big|\; x \in K_1\big(\mathbb{Z}_p\big[\mathcal{G}^{(\nu)}_{\infty,n}\big]\big)\big\}$.

Proof. Firstly $\theta^{(\nu)}_{0,n}$ coincides with the quotient mapping modulo $\big[\mathcal{U}^{(\nu)}_{0,n},\mathcal{U}^{(\nu)}_{0,n}\big] = \mathcal{H}_\infty/\mathcal{H}^{p^n}_\infty$. The composition $\Gamma/\Gamma^{p^\nu} \overset{\iota}{\hookrightarrow} \mathcal{G}^{(\nu)}_{\infty,n} \overset{\mathrm{mod}\ \mathcal{H}_\infty/p^n}{\twoheadrightarrow} \Gamma/\Gamma^{p^\nu}$ equals the identity, and this induces

$$K_1\big(\mathbb{Z}_p\big[\Gamma/\Gamma^{p^\nu}\big]\big) \xrightarrow{\iota_*} K_1\big(\mathbb{Z}_p\big[\mathcal{G}^{(\nu)}_{\infty,n}\big]\big) \xrightarrow{\theta^{(\nu)}_{0,n}} K_1\big(\mathbb{Z}_p\big[\Gamma/\Gamma^{p^\nu}\big]\big)$$

which must then be the identity map on $K_1\big(\mathbb{Z}_p\big[\Gamma/\Gamma^{p^\nu}\big]\big) \cong \mathbb{Z}_p\big[\Gamma/\Gamma^{p^\nu}\big]^\times$. The latter group is therefore isomorphic to a direct factor of $K_1\big(\mathbb{Z}_p\big[\mathcal{G}^{(\nu)}_{\infty,n}\big]\big)$, and the rest follows easily. □

For a group G, the ring homomorphism $\varphi_G : \mathbb{Z}_p[\mathrm{Conj}(G)] \to \mathbb{Z}_p[\mathrm{Conj}(G)]$ denotes the linear extension of the map $[g] \mapsto [g^p]$ on $\mathrm{Conj}(G)$ (note if G is abelian, then $\mathrm{Conj}(G) = G$).

Lemma 6.3 *For all* $\alpha \in \mathbb{Q}_p\big[\mathrm{Conj}\big(\mathcal{G}^{(\nu)}_{\infty,n}\big)\big]$,

$$\theta^{(\nu),+}_{m,n}\circ\varphi_{\mathcal{G}^{(\nu)}_{\infty,n}}(\alpha) \;=\; \begin{cases} p\cdot\varphi_{\mathcal{U}^{(\nu)}_{m-1,n}}\circ \mathrm{Tr}_{\mathcal{G}^{(\nu)}_{\infty,n}/\mathcal{U}^{(\nu)}_{m-1,n}}(\alpha) \mod \big[\mathcal{U}^{(\nu)}_{m,n},\mathcal{U}^{(\nu)}_{m,n}\big] & \textit{if } m\geq 1\\ \varphi_{\mathcal{G}^{(\nu)}_{\infty,n}}(\alpha) \mod \big[\mathcal{U}^{(\nu)}_{0,n},\mathcal{U}^{(\nu)}_{0,n}\big] & \textit{if } m=0.\end{cases}$$

Proof. If $m=0$, the formula is straightforward to establish.

We therefore suppose that $m\geq 1$. It is enough to consider conjugacy classes of the form $\alpha=[\gamma^j\cdot\overline{h}]$ with $j\in\mathbb{Z}/p^\nu\mathbb{Z}$ and $\overline{h}\in\frac{\mathcal{H}_\infty}{\mathcal{H}_\infty^{p^n}}$, since these will generate $\mathbb{Q}_p\big[\mathrm{Conj}\big(\mathcal{G}^{(\nu)}_{\infty,n}\big)\big]$.

Key Claims: (I) For all $j\in\mathbb{Z}/p^\nu\mathbb{Z}$, one has $\big(\gamma^j\cdot\overline{h}\big)^p=\gamma^{pj}\cdot\prod_{i=0}^{p-1}\overline{h}^{\gamma^{ji}}$ inside $\Gamma/\Gamma^{p^\nu}\ltimes\frac{\mathcal{H}_\infty}{\mathcal{H}_\infty^{p^n}}$.

(II) If $k,k'\in\mathbb{Z}$ satisfy $k\equiv k' \pmod{p^{m-1}}$, then

$$\varphi_{\mathcal{U}^{(\nu)}_{m-1,n}}\Big(\big[\gamma^j\cdot\overline{h}^{\gamma^k}\big]\Big)\;\equiv\;\varphi_{\mathcal{U}^{(\nu)}_{m-1,n}}\Big(\big[\gamma^j\cdot\overline{h}^{\gamma^{k'}}\big]\Big)\mod \big[\mathcal{U}^{(\nu)}_{m,n}\;,\;\mathcal{U}^{(\nu)}_{m,n}\big]. \qquad (6.3)$$

Postponing their proof for the moment, one calculates that

$$\begin{aligned}
\theta^{(\nu),+}_{m,n}\circ\varphi_{\mathcal{G}^{(\nu)}_{\infty,n}}\big([\gamma^j\cdot\overline{h}]\big) &\overset{\text{by (I)}}{=} \theta^{(\nu),+}_{m,n}\left(\Big[\gamma^{pj}\cdot\prod_{i=0}^{p-1}\overline{h}^{\gamma^{ji}}\Big]\right)\\
&= \begin{cases}\gamma^{pj}\cdot\sum_{k=0}^{p^m-1}\gamma^{-k}\Big(\prod_{i=0}^{p-1}\overline{h}^{\gamma^{ji}}\Big)\gamma^k \mod \big[\mathcal{U}^{(\nu)}_{m,n},\mathcal{U}^{(\nu)}_{m,n}\big] & \text{if } \gamma^{pj}\in\Gamma^{p^m}\\ 0 & \text{otherwise}\end{cases}\\
&= \begin{cases}\gamma^{pj}\cdot\sum_{k=0}^{p^m-1}\prod_{i=0}^{p-1}\gamma^{-k}\overline{h}^{\gamma^{ji}}\gamma^k \mod \big[\mathcal{U}^{(\nu)}_{m,n},\mathcal{U}^{(\nu)}_{m,n}\big] & \text{if } \gamma^{j}\in\Gamma^{p^{m-1}}\\ 0 & \text{otherwise}\end{cases}\\
&\overset{\text{by (I)}}{=} \begin{cases}\varphi_{\mathcal{U}^{(\nu)}_{m-1,n}}\Big(\gamma^j\cdot\sum_{k=0}^{p^m-1}\overline{h}^{\gamma^k}\Big) \mod \big[\mathcal{U}^{(\nu)}_{m,n},\mathcal{U}^{(\nu)}_{m,n}\big] & \text{if } \gamma^{j}\in\Gamma^{p^{m-1}}\\ 0 & \text{otherwise}\end{cases}\\
&\overset{\text{by (II)}}{=} \begin{cases}\varphi_{\mathcal{U}^{(\nu)}_{m-1,n}}\Big(\gamma^j\cdot p\cdot\sum_{k'=0}^{p^{m-1}-1}\overline{h}^{\gamma^{k'}}\Big) \mod \big[\mathcal{U}^{(\nu)}_{m,n},\mathcal{U}^{(\nu)}_{m,n}\big] & \text{if } \gamma^{j}\in\Gamma^{p^{m-1}}\\ 0 & \text{otherwise}\end{cases}\\
&= p\cdot\varphi_{\mathcal{U}^{(\nu)}_{m-1,n}}\circ\mathrm{Tr}_{\mathcal{G}^{(\nu)}_{\infty,n}/\mathcal{U}^{(\nu)}_{m-1,n}}\Big([\gamma^j\cdot\overline{h}]\Big) \mod \big[\mathcal{U}^{(\nu)}_{m,n},\mathcal{U}^{(\nu)}_{m,n}\big].
\end{aligned}$$

The full lemma now follows for each $m\geq 1$, as $\mathbb{Q}_p\big[\mathrm{Conj}\big(\mathcal{G}^{(\nu)}_{\infty,n}\big)\big]$ is generated by $[\gamma^j\cdot\overline{h}]$'s.

It remains to establish Claims (I) and (II). To prove (I) we know that $\overline{h}\cdot\gamma^j=\gamma^j\cdot\overline{h}^{\gamma^j}$, in which case

$$\begin{aligned}\left(\gamma^j\cdot\overline{h}\right)^p &= \gamma^j\cdot\left(\overline{h}\cdot\gamma^j\right)\cdot\overline{h}\cdot\gamma^j\cdot\overline{h}\ \cdots\ \gamma^j\cdot\overline{h} \ = \ \gamma^{2j}\cdot\overline{h}^{\gamma^j}\cdot\left(\overline{h}\cdot\gamma^j\right)\cdot\overline{h}\ \cdots\ \gamma^j\cdot\overline{h}\\ &= \gamma^{2j}\cdot\left(\overline{h}^{\gamma^j}\cdot\gamma^j\right)\cdot\overline{h}^{\gamma^j}\cdot\overline{h}\ \cdots\ \gamma^j\cdot\overline{h} \ = \ \gamma^{3j}\cdot\overline{h}^{\gamma^{2j}}\cdot\overline{h}^{\gamma^j}\cdot\overline{h}\ \cdots\ \gamma^j\cdot\overline{h}\\ &= \ \ldots \ = \ \gamma^{(p-1)j}\cdot\overline{h}^{\gamma^{(p-2)j}}\cdot\overline{h}^{\gamma^{(p-3)j}}\cdots\left(\overline{h}\cdot\gamma^j\right)\cdot\overline{h} \ = \ \ldots \ = \ \gamma^{pj}\cdot\prod_{i=0}^{p-1}\overline{h}^{\gamma^{ji}}.\end{aligned}$$

To show (II) note that the L.H.S. of (6.3) $\overset{\text{by (I)}}{=}\gamma^{pj}\cdot\prod_{i=0}^{p-1}(\overline{h}^{\gamma^k})^{\gamma^{ji}} = \gamma^{pj}\cdot\prod_{i=0}^{p-1}\overline{h}^{\gamma^{ji+k}}$, while the R.H.S. of (6.3) $=\gamma^{pj}\cdot\prod_{i=0}^{p-1}\overline{h}^{\gamma^{ji+k'}}$ by an identical argument; one deduces that

$$\begin{aligned}\frac{\text{L.H.S. of (6.3)}}{\text{R.H.S. of (6.3)}} &= \gamma^{pj}\cdot\left(\prod_{i=0}^{p-1}\overline{h}^{\gamma^{ji+k}}(\overline{h}^{-1})^{\gamma^{ji+k'}}\right)\cdot\gamma^{-pj}\\ &= \gamma^{pj}\cdot\left(\prod_{i=0}^{p-1}\gamma^{-(ji+k')}\cdot\left(\gamma^{k'-k}\cdot\overline{h}\cdot\gamma^{-(k'-k)}\cdot\overline{h}^{-1}\right)\cdot\gamma^{ji+k'}\right)\cdot\gamma^{-pj}.\end{aligned}$$

However $\overline{h}_{k,k'}:=\gamma^{k'-k}\cdot\overline{h}\cdot\gamma^{-(k'-k)}\cdot\overline{h}^{-1}\in\left[\mathcal{U}^{(\nu)}_{m-1,n},\mathcal{U}^{(\nu)}_{m-1,n}\right]$ because $\gamma^{k-k'}\in\Gamma^{p^{m-1}}$ whenever $k\equiv k'\ (\operatorname{mod} p^{m-1})$, which in turn implies $\frac{\text{L.H.S. of (6.3)}}{\text{R.H.S. of (6.3)}}=\left(\prod_{i=0}^{p-1}\overline{h}_{k,k'}^{\gamma^{ji+k'}}\right)^{\gamma^{-pj}}$. This latter product is divisible by p, in fact

$$\frac{\text{L.H.S. of (6.3)}}{\text{R.H.S. of (6.3)}}\ \in\ \left[\mathcal{U}^{(\nu)}_{m-1,n}\ ,\ \mathcal{U}^{(\nu)}_{m-1,n}\right]^p\ \subset\ \left[\mathcal{U}^{(\nu)}_{m,n}\ ,\ \mathcal{U}^{(\nu)}_{m,n}\right].$$

Therefore L.H.S. $\equiv$ R.H.S. mod $\left[\mathcal{U}^{(\nu)}_{m,n}\ ,\ \mathcal{U}^{(\nu)}_{m,n}\right]$, which establishes Claim (II) as well. □

We now examine how the Frobenius map φ commutes with $\theta^{(\nu)}_{m-1,n}$. Consider the sequence

$$\frac{\Gamma^{p^{m-1}}}{\Gamma^{p^\nu}}\times\frac{\mathcal{H}_\infty}{\left[\mathcal{U}^{(\nu)}_{m-1,n},\mathcal{U}^{(\nu)}_{m-1,n}\right]}\ \xrightarrow{(-)^p}\ \frac{\Gamma^{p^m}}{\Gamma^{p^\nu}}\times\frac{(\mathcal{H}_\infty)^p}{\left[\mathcal{U}^{(\nu)}_{m-1,n},\mathcal{U}^{(\nu)}_{m-1,n}\right]^p}\ \twoheadrightarrow\ \frac{\Gamma^{p^m}}{\Gamma^{p^\nu}}\times\frac{(\mathcal{H}_\infty)^p}{\left[\mathcal{U}^{(\nu)}_{m,n},\mathcal{U}^{(\nu)}_{m,n}\right]}$$

induced from the p-power map, and the containment $\left[\mathcal{U}^{(\nu)}_{m-1,n},\mathcal{U}^{(\nu)}_{m-1,n}\right]^p\hookrightarrow\left[\mathcal{U}^{(\nu)}_{m,n},\mathcal{U}^{(\nu)}_{m,n}\right]$. If we label the composition as $\widetilde{\varphi}:\mathcal{U}^{(\nu),\text{ab}}_{m-1,n}\to\mathcal{U}^{(\nu),\text{ab}}_{m,n}$, by linearly extending $\widetilde{\varphi}$ one obtains

$$\widetilde{\varphi}_{\mathcal{U}^{(\nu),\text{ab}}_{m-1,n}}:\mathbb{Q}_p\left[\mathcal{U}^{(\nu),\text{ab}}_{m-1,n}\right]\to\mathbb{Q}_p\left[\mathcal{U}^{(\nu),\text{ab}}_{m,n}\right],\qquad\sum_{g\in\mathcal{U}^{(\nu),\text{ab}}_{m-1,n}}c_g\cdot[g]\ \mapsto\ \sum_{g\in\mathcal{U}^{(\nu),\text{ab}}_{m-1,n}}c_g\cdot\widetilde{\varphi}[g]$$

as a homomorphism of commutative algebras.

Lemma 6.4 *(i) For each integer $m \geq 1$ and every $x \in K_1\big(\mathbb{Z}_p\big[\mathcal{G}^{(\nu)}_{\infty,n}\big]\big)$,*

$$\begin{aligned}\widetilde{\varphi}_{\mathcal{U}^{(\nu),\mathrm{ab}}_{m-1,n}} \circ \log_{\mathbb{Z}_p[\mathcal{U}^{(\nu),\mathrm{ab}}_{m-1,n}]} \circ \theta^{(\nu)}_{m-1,n}(x) & \\ = \varphi_{\mathcal{U}^{(\nu),\mathrm{ab}}_{m-1,n}} \Big(\log_{\mathbb{Z}_p[\mathcal{U}^{(\nu),\mathrm{ab}}_{m-1,n}]} \circ \mathrm{Norm}_{\mathcal{G}^{(\nu)}_{\infty,n}/\mathcal{U}^{(\nu)}_{m-1,n}}(x)\Big) & \mod \big[\mathcal{U}^{(\nu)}_{m,n}\ ,\ \mathcal{U}^{(\nu)}_{m,n}\big].\end{aligned}$$

(ii) For each integer $m \geq 0$ and every $x \in K_1\big(\mathbb{Z}_p\big[\mathcal{G}^{(\nu)}_{\infty,n}\big]\big)$,

$$\theta^{(\nu)}_{m,n}\big(x^{\dagger}\big) = \frac{\theta^{(\nu)}_{m,n}(x)}{\tau_*^{(m,\nu)} \circ \mathcal{N}_{0,m}\big(\theta^{(\nu)}_{0,n}(x)\big)} \qquad \text{and} \qquad \theta^{(\nu)}_{m,n}\big(x^{\mathrm{cy}}\big) = \tau_*^{(m,\nu)} \circ \mathcal{N}_{0,m}(\theta^{(\nu)}_{0,n}(x))$$

where $\tau^{(m,\nu)}$ denotes the natural inclusion $\mathbb{Q}_p\big[\Gamma^{p^m}/\Gamma^{p^\nu}\big] \hookrightarrow \mathbb{Q}_p\big[\mathcal{U}^{(\nu),\mathrm{ab}}_{m,n}\big]$.

At first glance these statements are rather technical in nature, and their demonstrations could easily be skipped on an initial reading. However they will become important tools for us in the next section, when we calculate the Taylor-Oliver logarithm composed with the family of theta-maps $\big\{\theta^{(\nu),+}_{m,n}\big\}_{0 \leq m \leq n-s}$.

Proof. Starting with assertion (i), since $\big[\mathcal{U}^{(\nu)}_{m-1,n}\ ,\ \mathcal{U}^{(\nu)}_{m-1,n}\big]^p \subset \big[\mathcal{U}^{(\nu)}_{m,n}\ ,\ \mathcal{U}^{(\nu)}_{m,n}\big]$ one deduces

$$\begin{aligned}&\varphi_{\mathcal{U}^{(\nu),\mathrm{ab}}_{m-1,n}} \circ \mathrm{Tr}_{\mathcal{G}^{(\nu)}_{\infty,n}/\mathcal{U}^{(\nu)}_{m-1,n}}(\alpha) \mod \big[\mathcal{U}^{(\nu)}_{m,n}\ ,\ \mathcal{U}^{(\nu)}_{m,n}\big] \\ &= \ \widetilde{\varphi}_{\mathcal{U}^{(\nu),\mathrm{ab}}_{m-1,n}} \Big(\mathrm{Tr}_{\mathcal{G}^{(\nu)}_{\infty,n}/\mathcal{U}^{(\nu)}_{m-1,n}}(\alpha) \mod \big[\mathcal{U}^{(\nu)}_{m-1,n}\ ,\ \mathcal{U}^{(\nu)}_{m-1,n}\big]\Big) \ = \ \widetilde{\varphi}_{\mathcal{U}^{(\nu),\mathrm{ab}}_{m-1,n}} \circ \theta^{(\nu),+}_{m-1,n}(\alpha)\end{aligned} \tag{6.4}$$

for every $\alpha \in \mathbb{Q}_p\big[\mathrm{Conj}\big(\mathcal{G}^{(\nu)}_{\infty,n}\big)\big]$. Evaluating both sides at $\alpha = \log(x)$, it is easily verified

$$\begin{aligned}\varphi_{\mathcal{U}^{(\nu),\mathrm{ab}}_{m-1,n}} \circ \log \circ \mathrm{Norm}_{\mathcal{G}^{(\nu)}_{\infty,n}/\mathcal{U}^{(\nu)}_{m-1,n}}(x) \ &\equiv\ \varphi_{\mathcal{U}^{(\nu),\mathrm{ab}}_{m-1,n}} \circ\ \mathrm{Tr}_{\mathcal{G}^{(\nu)}_{\infty,n}/\mathcal{U}^{(\nu)}_{m-1,n}}\big(\log(x)\big) \\ &\overset{\text{by (6.4)}}{=}\ \ \widetilde{\varphi}_{\mathcal{U}^{(\nu),\mathrm{ab}}_{m-1,n}} \circ \theta^{(\nu),+}_{m-1,n}\big(\log(x)\big) \ = \ \widetilde{\varphi}_{\mathcal{U}^{(\nu),\mathrm{ab}}_{m-1,n}} \circ \log \circ\, \theta^{(\nu)}_{m-1,n}(x).\end{aligned}$$

To prove (ii), one simply observes that

$$\begin{aligned}\tau_*^{(m,\nu)} \circ \mathcal{N}_{0,m}\big(\theta^{(\nu)}_{0,n}(x)\big) \ &= \ \tau_*^{(m,\nu)} \circ \mathrm{Norm}_{\Gamma/\Gamma^{p^m}}\big(x \mod \mathcal{H}_\infty/\mathcal{H}_\infty^{p^n}\big) \\ &= \ \mathrm{Norm}_{\mathcal{G}^{(\nu)}_{\infty,n}/\mathcal{U}^{(\nu)}_{m,n}}\Big(\tau_*^{(0,\nu)}\big(x \mod \mathcal{H}_\infty/\mathcal{H}_\infty^{p^n}\big)\Big) \mod \big[\mathcal{U}^{(\nu)}_{m,n}, \mathcal{U}^{(\nu)}_{m,n}\big] \\ &= \ \theta^{(\nu)}_{m,n} \circ \iota_*\big(x \mod \mathcal{H}_\infty/\mathcal{H}_\infty^{p^n}\big) \ = \ \theta^{(\nu)}_{m,n}\big(x^{\mathrm{cy}}\big).\end{aligned}$$

Consequently $\theta^{(\nu)}_{m,n}\big(x^{\dagger}\big) = \frac{\theta^{(\nu)}_{m,n}(x)}{\theta^{(\nu)}_{m,n}(x^{\mathrm{cy}})} = \frac{\theta^{(\nu)}_{m,n}(x)}{\tau_*^{(m,\nu)} \circ \mathcal{N}_{0,m}(\theta^{(\nu)}_{0,n}(x))}$, and the two identities follow. □

6.3 The image of the Taylor-Oliver logarithm

For a finite group G, the Taylor-Oliver logarithm $\mathrm{LOG}_G : K_1\big(\mathbb{Z}_p[G]\big) \to \mathbb{Z}_p\big[\mathrm{Conj}(G)\big]$ is defined by

$$\mathrm{LOG}_G(x) \;:=\; \log_{\mathbb{Z}_p[G]}(x) - \frac{1}{p}\varphi_G\big(\log_{\mathbb{Z}_p[G]}(x)\big)$$

where $\log_{\mathbb{Z}_p[G]}$ is the unique extension of $\log_{\mathrm{Jac}(\mathbb{Z}_p[G])}$ (see [Oli88] for more details). Note that G need not necessarily be a p-group, even though it happens to be so in this paper.

If $G = \mathcal{G}^{(\nu)}_{\infty,n}$ then $\mathrm{LOG}_{\mathcal{G}^{(\nu)}_{\infty,n}}$ denotes the ν-th layer of the map 'LOG' occurring in (6.1). Our task is to calculate the mappings $\mathcal{L}$ and $\mathcal{L}_{\underline{\chi}}$ which make the diagram (6.1) commutative. The former of these maps may be determined from the following formulae.

Proposition 6.5 *(a) If $m \in \{1, \dots, n-s\}$ and $x \in K_1\big(\mathbb{Z}_p[\![\mathcal{G}^{(\nu)}_{\infty,n}]\!]\big)$, then*

$$\theta^{(\nu),+}_{m,n} \circ \mathrm{LOG}_{\mathcal{G}^{(\nu)}_{\infty,n}}(x) \;=\; \log_{\mathbb{Z}_p[\mathcal{U}^{(\nu),\mathrm{ab}}_{m,n}]}\left(\frac{\theta^{(\nu)}_{m,n}(x)}{\widetilde{\varphi}_{\mathcal{U}^{(\nu),\mathrm{ab}}_{m-1,n}} \circ \theta^{(\nu)}_{m-1,n}(x)}\right).$$

(b) Furthermore, if $x^\dagger = \frac{x}{x^{\mathrm{cy}}} \in \mathcal{W}^{(\nu)}_\dagger$ then

$$\begin{aligned}&\theta^{(\nu),+}_{m,n} \circ \mathrm{LOG}_{\mathcal{G}^{(\nu)}_{\infty,n}}\big(x^\dagger\big)\\ &= \log_{\mathbb{Z}_p[\mathcal{U}^{(\nu),\mathrm{ab}}_{m,n}]}\left(\frac{\theta^{(\nu)}_{m,n}(x)}{\mathcal{T}^{(m,\nu)}_* \circ \mathcal{N}_{0,m}\big(\theta^{(\nu)}_{0,n}(x)\big)} \cdot \widetilde{\varphi}_{\mathcal{U}^{(\nu),\mathrm{ab}}_{m-1,n}}\left(\frac{\mathcal{T}^{(m-1,\nu)}_* \circ \mathcal{N}_{0,m-1}\big(\theta^{(\nu)}_{0,n}(x)\big)}{\theta^{(\nu)}_{m-1,n}(x)}\right)\right).\end{aligned}$$

Proof. Using the definition of the Taylor-Oliver logarithm and our previous results,

$$\begin{aligned}\theta^{(\nu),+}_{m,n} \circ \mathrm{LOG}_{\mathcal{G}^{(\nu)}_{\infty,n}}(x) \;&=\; \theta^{(\nu),+}_{m,n} \circ \log_{\mathbb{Z}_p[\mathcal{G}^{(\nu)}_{\infty,n}]}(x) - \frac{1}{p} \cdot \theta^{(\nu),+}_{m,n} \circ \varphi_{\mathcal{G}^{(\nu)}_{\infty,n}}\big(\log_{\mathbb{Z}_p[\mathcal{G}^{(\nu)}_{\infty,n}]}(x)\big)\\
&\overset{\text{by } 6.3}{=}\; \theta^{(\nu),+}_{m,n}\big(\log(x)\big) \;-\; \frac{1}{p} \cdot p \cdot \varphi_{\mathcal{U}^{(\nu)}_{m-1,n}} \circ \mathrm{Tr}_{\mathcal{G}^{(\nu)}_{\infty,n}/\mathcal{U}^{(\nu)}_{m-1,n}}\big(\log(x)\big) \mod \big[\mathcal{U}^{(\nu)}_{m,n}, \mathcal{U}^{(\nu)}_{m,n}\big]\\
&=\; \theta^{(\nu),+}_{m,n}\big(\log(x)\big) \;-\; \varphi_{\mathcal{U}^{(\nu)}_{m-1,n}} \circ \log\Big(\mathrm{Norm}_{\mathcal{G}^{(\nu)}_{\infty,n}/\mathcal{U}^{(\nu)}_{m-1,n}}(x)\Big) \mod \big[\mathcal{U}^{(\nu)}_{m,n}, \mathcal{U}^{(\nu)}_{m,n}\big]\\
&\overset{\text{by } 6.4(\mathrm{i})}{=}\; \theta^{(\nu),+}_{m,n}\big(\log_{\mathbb{Z}_p[\mathcal{G}^{(\nu)}_{\infty,n}]}(x)\big) \;-\; \widetilde{\varphi}_{\mathcal{U}^{(\nu),\mathrm{ab}}_{m-1,n}} \circ \log_{\mathbb{Z}_p[\mathcal{U}^{(\nu),\mathrm{ab}}_{m-1,n}]} \circ \theta^{(\nu)}_{m-1,n}(x)\\
&=\; \log_{\mathbb{Z}_p[\mathcal{U}^{(\nu),\mathrm{ab}}_{m,n}]}\big(\theta^{(\nu)}_{m,n}(x)\big) \;-\; \log_{\mathbb{Z}_p[\mathcal{U}^{(\nu),\mathrm{ab}}_{m,n}]}\Big(\widetilde{\varphi}_{\mathcal{U}^{(\nu),\mathrm{ab}}_{m-1,n}} \circ \theta^{(\nu)}_{m-1,n}(x)\Big)\end{aligned}$$

which establishes assertion (a).

To prove (b), one simply combines part (a) with the formula from Lemma 6.4(ii). □

Remark: As a direct consequence, in order to make the left-hand square in the diagram

$$\begin{tikzcd}
K_1\big(\mathbb{Z}_p[\mathcal{G}^{(\nu)}_{\infty,n}]\big) \arrow[r, "\prod\theta^{(\nu)}_{m,n}"] \arrow[d, "\mathrm{LOG}_{\mathcal{G}^{(\nu)}_{\infty,n}}"] & \Phi^{(\nu)} \arrow[r, "\prod\chi"] \arrow[d, "\mathcal{L}^{(\nu)}"] & \underline{\chi}\big(\Phi^{(\nu)}\big) \arrow[d, "\mathcal{L}^{(\nu)}_{\underline{\chi}}"] \\
\mathbb{Z}_p\big[\mathrm{Conj}(\mathcal{G}^{(\nu)}_{\infty,n})\big] \arrow[r, "\prod\theta^{(\nu),+}_{m,n}"] & \Psi^{(\nu)} \arrow[r, "\prod\chi"] & \underline{\chi}\big(\Psi^{(\nu)}\big)
\end{tikzcd}$$

commutative, it follows from Proposition 6.5(a) that one should define

$$\mathcal{L}^{(\nu)}\Big(\big(\mathbf{y}^{(\nu)}_m\big)\Big)_m := \log_{\mathbb{Z}_p[\mathcal{U}^{(\nu),\mathrm{ab}}_{m,n}]}\left(\frac{\mathbf{y}^{(\nu)}_m}{\widetilde{\varphi}_{\mathcal{U}^{(\nu),\mathrm{ab}}_{m-1,n}}\big(\mathbf{y}^{(\nu)}_{m-1}\big)}\right) \quad \text{for all } \big(\mathbf{y}^{(\nu)}_m\big) \in \prod_{0\le m\le n-s} \mathbb{Z}_p\big[\mathcal{U}^{(\nu),\mathrm{ab}}_{m,n}\big]^\times . \tag{6.5}$$

To make the right-hand square commutative, we need to work out the map $\mathcal{L}^{(\nu)}_{\underline{\chi}}$ explicitly. Fix a finite order character $\chi : \mathcal{H}_\infty \to \mu_{p^\infty}$ factoring through the quotient group $\overline{\mathcal{H}}^{(m,n)}_\infty$, which one may interpret as a homomorphism

$$\chi : \mathcal{U}^{(\nu),\mathrm{ab}}_{m,n} \cong \Gamma^{p^m}/\Gamma^{p^\nu} \times \overline{\mathcal{H}}^{(m,n)}_\infty \longrightarrow \Gamma^{p^m}/\Gamma^{p^\nu} \times \mathrm{Im}(\chi)$$

sending an element $\gamma^j \cdot \overline{h}$ to $\gamma^j \cdot \chi(\overline{h})$. It follows that its extension to $\mathbb{Z}_p\big[\mathcal{U}^{(\nu),\mathrm{ab}}_{m,n}\big]$ satisfies

$$\chi\left(\theta^{(\nu),+}_{m,n} \circ \mathrm{LOG}_{\mathcal{G}^{(\nu)}_{\infty,n}}(x)\right) \;=\; \log_{\mathcal{O}_\chi\left[\frac{\Gamma^{p^m}}{\Gamma^{p^\nu}}\right]}\left(\frac{\chi \circ \theta^{(\nu)}_{m,n}(x)}{\varphi_{\frac{\Gamma^{p^{m-1}}}{\Gamma^{p^\nu}}}\big(\chi^p \circ \theta^{(\nu)}_{m-1,n}(x)\big)}\right).$$

Moreover by Proposition 6.5(b), for any $x^\dagger = x/x^{\mathrm{cy}} \in \mathcal{W}^{(\nu)}_\dagger$ one has

$$\chi\left(\theta^{(\nu),+}_{m,n} \circ \mathrm{LOG}_{\mathcal{G}^{(\nu)}_{\infty,n}}(x^\dagger)\right) = \log_{\mathcal{O}_\chi\left[\frac{\Gamma^{p^m}}{\Gamma^{p^\nu}}\right]}\left(\frac{\chi \circ \theta^{(\nu)}_{m,n}(x)}{\mathcal{N}_{0,m}\big(\theta^{(\nu)}_{0,n}(x)\big)} \cdot \varphi_{\frac{\Gamma^{p^{m-1}}}{\Gamma^{p^\nu}}}\left(\frac{\mathcal{N}_{0,m-1}\big(\theta^{(\nu)}_{0,n}(x)\big)}{\chi^p \circ \theta^{(\nu)}_{m-1,n}(x)}\right)\right)$$

as χ acts trivially on $\mathbb{Z}_p[\Gamma^{p^m}/\Gamma^{p^\nu}]$, and thus also on $\mathcal{N}_{0,m-1}\big(\theta^{(\nu)}_{0,n}(x)\big)$ and $\mathcal{N}_{0,m}\big(\theta^{(\nu)}_{0,n}(x)\big)$.

Since $\mathbf{y}^{(\nu)}_{m,\chi}$ corresponds to $\chi \circ \theta^{(\nu)}_{m,n}(x)$, the preceding formulae imply one should define

$$\mathcal{L}^{(\nu)}_{\underline{\chi}}\big((\mathbf{y}^{(\nu)}_{m,\chi})\big)_{m,\chi} := \log_{\mathcal{O}_\chi\left[\frac{\Gamma^{p^m}}{\Gamma^{p^\nu}}\right]}\left(\frac{\mathbf{y}^{(\nu)}_{m,\chi}}{\varphi_{\frac{\Gamma^{p^{m-1}}}{\Gamma^{p^\nu}}}\big(\mathbf{y}^{(\nu)}_{m-1,\chi^p}\big)}\right) \quad \text{where } \big(\mathbf{y}^{(\nu)}_{m,\chi}\big) \in \prod_{m,\chi} \mathcal{O}_\chi\left[\frac{\Gamma^{p^m}}{\Gamma^{p^\nu}}\right]^\times .$$

Indeed if $\big(\mathbf{y}_{m,\chi}^{(\nu)}\big) \in \prod_{m,\chi} \chi \circ \theta_{m,n}^{(\nu)}\big(\mathcal{W}_{\dagger}^{(\nu)}\big)$, then one can further say

$$\mathcal{L}_{\underline{\chi}}^{(\nu)}\big((\mathbf{y}_{m,\chi}^{(\nu)})\big)_{m,\chi} = \log_{\mathcal{O}_\chi\left[\frac{\Gamma^{p^m}}{\Gamma^{p^\nu}}\right]}\left(\frac{\mathbf{y}_{m,\chi}^{(\nu)}}{\mathcal{N}_{0,m}\big(\mathbf{y}_{0,\mathbf{1}}^{(\nu)}\big)} \cdot \varphi_{\frac{\Gamma^{p^{m-1}}}{\Gamma^{p^\nu}}}\left(\frac{\mathcal{N}_{0,m-1}\big(\mathbf{y}_{0,\mathbf{1}}^{(\nu)}\big)}{\mathbf{y}_{m-1,\chi^p}^{(\nu)}}\right)\right). \tag{6.6}$$

In fact $\frac{\mathbf{y}_{m,\chi}^{(\nu)}}{\mathcal{N}_{0,m}\left(\mathbf{y}_{0,\mathbf{1}}^{(\nu)}\right)} \in 1 + p \cdot \mathcal{O}_\chi\big[\frac{\Gamma^{p^m}}{\Gamma^{p^\nu}}\big]$ for all m, so the full expression occurring inside the logarithm in Equation (6.6) must automatically be congruent to 1 modulo $p \cdot \mathcal{O}_{\mathbb{C}_p}\big[\frac{\Gamma^{p^m}}{\Gamma^{p^\nu}}\big]$.

Corollary 6.6 *If* $\big(\mathbf{y}_m^{(\nu)}\big) \in \Theta_{\infty,n}^{(\nu)}\big(\mathcal{W}_{\dagger}^{(\nu)}\big)$ *and one sets* $\big(\mathbf{y}_{m,\chi}^{(\nu)}\big) = \underline{\chi}\big((\mathbf{y}_m^{(\nu)})\big)$*, then both*

$$\mathcal{L}^{(\nu)}\big((\mathbf{y}_m^{(\nu)})\big) \in \Psi^{(\nu)} \cap p\cdot\prod_m \mathrm{Im}\big(\sigma_m^{(\nu)}\big) \text{ and } \mathcal{L}_{\underline{\chi}}^{(\nu)}\big((\mathbf{y}_{m,\chi}^{(\nu)})\big) \in \underline{\chi}\big(\Psi^{(\nu)}\big) \cap p\cdot\prod_{m,\chi} \mathcal{O}_{\mathbb{C}_p}\big[\Gamma^{p^m}/\Gamma^{p^\nu}\big].$$

Proof. To address the first assertion, Proposition 6.5(b) implies that

$$\mathcal{L}^{(\nu)}\big((\mathbf{y}_m^{(\nu)})\big)_m = \log_{\mathbb{Z}_p[\mathcal{U}_{m,n}^{(\nu),\mathrm{ab}}]}\left(\frac{\mathbf{y}_m^{(\nu)}}{\mathcal{N}_{0,m}\big(\mathbf{y}_0^{(\nu)}\big)} \cdot \widetilde{\varphi}_{\mathcal{U}_{m-1,n}^{(\nu),\mathrm{ab}}}\left(\frac{\mathcal{N}_{0,m-1}\big(\mathbf{y}_0^{(\nu)}\big)}{\mathbf{y}_{m-1}^{(\nu)}}\right)\right)$$

and as each of the two fractions inside the logarithm belongs to the group $1 + p \cdot \mathrm{Im}(\sigma_m^{(\nu)})$, the containment follows directly from Proposition 6.1(c).

To establish the second assertion, one combines the discussion after Equation (6.6) together with the isomorphism $\log : 1 + p \cdot \mathcal{O}_{\mathbb{C}_p}\big[\Gamma^{p^m}/\Gamma^{p^\nu}\big] \xrightarrow{\sim} p \cdot \mathcal{O}_{\mathbb{C}_p}\big[\Gamma^{p^m}/\Gamma^{p^\nu}\big]$. □

6.4 A proof of Theorems 3.1 and 3.2

Recall from earlier that if a sequence $\big(\mathbf{y}_m^{(\nu)}\big)$ satisfies conditions (M1)-(M4), then its image under $\mathcal{L}^{(\nu)}$ always satisfies (A1)-(A3). We shall now establish a converse statement

$$\mathcal{L}^{(\nu)}\big((\mathbf{y}_m^{(\nu)})\big) \in p \cdot \Psi^{(\nu)} \implies \big(\mathbf{y}_m^{(\nu)}\big) \in \Phi^{(\nu)}.$$

If we are successful, the question as to whether or not $\big(\mathbf{y}_m^{(\nu)}\big)$ arises from $K_1\big(\mathbb{Z}_p[\mathcal{G}_{\infty,n}^{(\nu)}]\big)$ under the mapping $\Theta_{\infty,n}^{(\nu)}$ reduces to determining whether or not $\mathcal{L}_{\underline{\chi}}^{(\nu)}\big((\mathbf{y}_{m,\chi}^{(\nu)})\big) \in \underline{\chi}\big(\Psi^{(\nu)}\big)$. To achieve this goal, we will explicitly construct a section

$$\mathcal{S}^{(\nu)} : \left(\prod_{0\leq m\leq n-s} p\cdot\mathbb{Z}_p\big[\mathcal{U}^{(\nu),\mathrm{ab}}_{m,n}\big]\right)_{\text{(A1)-(A3)}} \longrightarrow \left(\prod_{0\leq m\leq n-s} 1+p\cdot\mathbb{Z}_p\big[\mathcal{U}^{(\nu),\mathrm{ab}}_{m,n}\big]\right)_{\text{(M1)-(M4)}}$$

for which $\mathcal{L}^{(\nu)}\circ\mathcal{S}^{(\nu)}\Big|_{p\cdot\Psi^{(\nu)}}$ and $\mathcal{S}^{(\nu)}\circ\mathcal{L}^{(\nu)}\Big|_{\Theta^{(\nu)}_{\infty,n}(\mathcal{W}^{(\nu)}_{\dagger})}$ are the respective identity mappings.

To produce this map $\mathcal{S}^{(\nu)}$, first fix a sequence $\big(\mathbf{a}^{(\nu)}_m\big)\in\prod_{0\leq m\leq n-s}p\cdot\mathbb{Z}_p\big[\mathcal{U}^{(\nu),\mathrm{ab}}_{m,n}\big]$. Recall that $\exp : p\cdot\mathbb{Z}_p\big[\mathcal{U}^{(\nu),\mathrm{ab}}_{m,n}\big]\xrightarrow{\sim}1+p\cdot\mathbb{Z}_p\big[\mathcal{U}^{(\nu),\mathrm{ab}}_{m,n}\big]$ is an isomorphism of abelian groups.

Definition 6.2 *Given the sequence $\big(\mathbf{a}^{(\nu)}_m\big)$ above, one recursively defines $\mathbf{y}^{(\nu)}_0 :=$ 1 and*

$$\mathbf{y}^{(\nu)}_m \;:=\; \widetilde{\varphi}_{\mathcal{U}^{(\nu),\mathrm{ab}}_{m-1,n}}\big(\mathbf{y}^{(\nu)}_{m-1}\big)\times\exp_{\mathbb{Z}_p[\mathcal{U}^{(\nu),\mathrm{ab}}_{m,n}]}\big(\mathbf{a}^{(\nu)}_m\big)\;\; \textit{for each } m\geq 1,$$

so that $\big(\mathbf{y}_m\big)\in\prod_m 1+p\cdot\mathbb{Z}_p\big[\mathcal{U}^{(\nu),\mathrm{ab}}_{m,n}\big]$. We label this association $\big(\mathbf{a}^{(\nu)}_m\big)\mapsto\big(\mathbf{y}^{(\nu)}_m\big)$ by $\mathcal{S}^{(\nu)}$.

Lemma 6.7 *(i) The composition $\mathcal{L}^{(\nu)}\circ\mathcal{S}^{(\nu)}$ is the identity map on $\prod_m p\cdot\mathbb{Z}_p\big[\mathcal{U}^{(\nu),\mathrm{ab}}_{m,n}\big]$.*
(ii) The composition $\mathcal{S}^{(\nu)}\circ\mathcal{L}^{(\nu)}$ yields the identity map on $\prod_m 1+p\cdot\mathbb{Z}_p\big[\mathcal{U}^{(\nu),\mathrm{ab}}_{m,n}\big]$.

Proof. To establish the first assertion, one simply calculates that

$$\mathcal{L}^{(\nu)}\circ\mathcal{S}^{(\nu)}\big((\mathbf{a}^{(\nu)}_m)\big)_m \;=\; \mathcal{L}^{(\nu)}\big((\mathbf{y}^{(\nu)}_m)\big) \overset{\text{by (6.5)}}{=} \log_{\mathbb{Z}_p[\mathcal{U}^{(\nu),\mathrm{ab}}_{m,n}]}\left(\frac{\mathbf{y}^{(\nu)}_m}{\widetilde{\varphi}_{\mathcal{U}^{(\nu),\mathrm{ab}}_{m-1,n}}\big(\mathbf{y}^{(\nu)}_{m-1}\big)}\right)$$
$$\overset{\text{by 6.2}}{=} \log_{\mathbb{Z}_p[\mathcal{U}^{(\nu),\mathrm{ab}}_{m,n}]}\Big(\exp_{\mathbb{Z}_p[\mathcal{U}^{(\nu),\mathrm{ab}}_{m,n}]}\big(\mathbf{a}^{(\nu)}_m\big)\Big) \;=\; \mathbf{a}^{(\nu)}_m.$$

The proof of the second assertion follows along identical lines. □

For the rest of this section, we assume that $\big(\mathbf{a}^{(\nu)}_m\big)\in\prod_m p\cdot\mathbb{Z}_p\big[\mathcal{U}^{(\nu),\mathrm{ab}}_{m,n}\big]$ satisfies (A1)–(A3). The goal now is to prove that properties (M1)–(M4) all hold for $\big(\mathbf{y}^{(\nu)}_m\big)=\mathcal{S}^{(\nu)}\big((\mathbf{a}^{(\nu)}_m)\big)$. Three of them are straightforward to deduce, but property (M3) requires more effort.

Establishing that $\mathcal{S}^{(\nu)}\big((\mathbf{a}_m^{(\nu)})\big)$ satisfies (M1),(M2),(M4). Let us begin by obtaining (M1). Since (A1) holds for the sequence $\big(\mathbf{a}_m^{(\nu)}\big)$, clearly

$$\begin{aligned}\mathcal{N}_{m-1,m}\circ\exp_{\mathbb{Z}_p[\mathcal{U}_{m-1,n}^{(\nu),\mathrm{ab}}]}\big(\mathbf{a}_{m-1}^{(\nu)}\big) \;&=\; \exp_{\mathbb{Z}_p[\mathcal{U}_{m,n}^{(\nu),\mathrm{ab}}]}\circ\,\mathrm{Tr}_{m-1,m}\big(\mathbf{a}_{m-1}^{(\nu)}\big)\\ &\overset{\text{by (A1)}}{=}\; \exp_{\mathbb{Z}_p[\mathcal{U}_{m,n}^{(\nu),\mathrm{ab}}]}\circ\,\pi_{m,m-1}\big(\mathbf{a}_m^{(\nu)}\big) \;=\; \pi_{m,m-1}\circ\exp_{\mathbb{Z}_p[\mathcal{U}_{m,n}^{(\nu),\mathrm{ab}}]}\big(\mathbf{a}_m^{(\nu)}\big)\end{aligned}$$

i.e. $\dfrac{\mathcal{N}_{m-1,m}\big(\mathbf{y}_{m-1}^{(\nu)}\big)}{\mathcal{N}_{m-1,m}\big(\widetilde{\varphi}(\mathbf{y}_{m-2}^{(\nu)})\big)}=\dfrac{\pi_{m,m-1}\big(\mathbf{y}_m^{(\nu)}\big)}{\pi_{m,m-1}\big(\widetilde{\varphi}(\mathbf{y}_{m-1}^{(\nu)})\big)}$ for each $m\geq 1$. The latter is equivalent to

$$\mathcal{N}_{m-1,m}\big(\mathbf{y}_{m-1}^{(\nu)}\big) \;=\; \pi_{m,m-1}\big(\mathbf{y}_m^{(\nu)}\big)\;\times\;\widetilde{\varphi}_{\mathcal{U}_{m-1,n}^{(\nu),\mathrm{ab}}}\left(\frac{\mathcal{N}_{m-2,m-1}\big(\mathbf{y}_{m-2}^{(\nu)}\big)}{\pi_{m-1,m-2}\big(\mathbf{y}_{m-1}^{(\nu)}\big)}\right).$$

The equality between $\mathcal{N}_{m-1,m}\big(\mathbf{y}_{m-1}^{(\nu)}\big)$ and $\pi_{m,m-1}\big(\mathbf{y}_m^{(\nu)}\big)$ now follows by induction on m, thereby yielding (M1) as a consequence.

Focussing instead on (M2), the semi-direct product structure on $\mathcal{G}_{\infty,n}^{(\nu)}=\Gamma/\Gamma^{p^\nu}\ltimes\frac{\mathcal{H}_\infty}{\mathcal{H}_\infty^{p^n}}$ implies the subset of $\mathcal{G}_{\infty,n}^{(\nu)}$-invariant elements in $\mathbb{Z}_p[\mathcal{U}_{m,n}^{(\nu),\mathrm{ab}}]$ consists of

$$H^0\big(\mathcal{G}_{\infty,n}^{(\nu)},\mathbb{Z}_p[\mathcal{U}_{m,n}^{(\nu),\mathrm{ab}}]\big)\;=\;H^0\big(\Gamma,\mathbb{Z}_p[\mathcal{U}_{m,n}^{(\nu),\mathrm{ab}}]\big)\;=\;\Big(\mathrm{Im}\big(\sigma_m^{(\nu)}\big)\big[1/p\big]\Big)\cap\mathbb{Z}_p\big[\mathcal{U}_{m,n}^{(\nu),\mathrm{ab}}\big].$$

Now (A2) states that $\mathbf{a}_m^{(\nu)}$ belongs to this subset, hence $\mathbf{y}_m^{(\nu)}\in\mathrm{Im}\big(\sigma_m^{(\nu)}\big)\big[1/p\big]\cap\mathbb{Z}_p[\mathcal{U}_{m,n}^{(\nu),\mathrm{ab}}]^\times$ upon combining the recurrence in Definition 6.2 with induction on m, and (M2) follows.

To show that (M4) holds true, consider the trace mapping $\mathrm{Tr}_{m,m+1}$ acting on $\mathbb{Z}_p\big[\mathcal{U}_{m,n}^{(\nu),\mathrm{ab}}\big]$. For each integer $m\geq 0$, one may decompose

$$\mathbb{Z}_p\big[\mathcal{U}_{m,n}^{(\nu),\mathrm{ab}}\big]\;\cong\;\mathbb{Z}_p\Big[\Gamma^{p^{m+1}}/\Gamma^{p^\nu}\times\overline{\mathcal{H}}_\infty^{(m,n)}\Big]\oplus\mathrm{Ker}\big(\mathrm{Tr}_{m,m+1}\big)$$

where by Lemma 4.9, the trace acts through multiplication by p on the first factor and kills off the second factor.

Note that $\mathbf{a}_m^{(\nu)}\in p\cdot\mathbb{Z}_p\big[\mathcal{U}_{m,n}^{(\nu),\mathrm{ab}}\big]$ so $\frac{1}{p}\mathrm{Tr}_{m,m+1}\big(\mathbf{a}_m^{(\nu)}\big)\equiv\mathbf{a}_m^{(\nu)}$ mod $p\cdot\mathrm{Ker}\big(\mathrm{Tr}_{m,m+1}\big)$. Moreover the sequence $\big(\mathbf{a}_m^{(\nu)}\big)$ satisfies (A3), thus $p\cdot\mathbf{a}_m^{(\nu)}-\mathrm{Tr}_{m,m+1}\big(\mathbf{a}_m^{(\nu)}\big)\in p\cdot\mathrm{Im}\big(\sigma_m^{(\nu)}\big)$ and applying Proposition 6.1:

$$\exp_{\mathbb{Z}_p[\mathcal{U}_{m,n}^{(\nu),\mathrm{ab}}]}\Big(p\cdot\mathbf{a}_m^{(\nu)}-\mathrm{Tr}_{m,m+1}\big(\mathbf{a}_m^{(\nu)}\big)\Big)\in\;1+p\cdot\mathrm{Im}\big(\sigma_m^{(\nu)}\big).$$

It is easy to see $\exp\left(p\cdot\mathbf{a}_m^{(\nu)}-\mathrm{Tr}_{m,m+1}(\mathbf{a}_m^{(\nu)})\right)=\frac{\exp(\mathbf{a}_m^{(\nu)})^p}{\mathcal{N}_{m,m+1}\circ\exp(\mathbf{a}_m^{(\nu)})}$. Also, recalling from earlier that $\exp\left(\mathbf{a}_m^{(\nu)}\right)=\frac{\mathbf{y}_m^{(\nu)}}{\widetilde{\varphi}(\mathbf{y}_{m-1}^{(\nu)})}$, we therefore conclude

$$\frac{\left(\mathbf{y}_m^{(\nu)}\right)^p}{\widetilde{\varphi}_{\mathcal{U}_{m-1,n}^{(\nu),\mathrm{ab}}}\left(\mathbf{y}_{m-1}^{(\nu)}\right)^p}\times\left(\frac{\mathcal{N}_{m,m+1}\left(\mathbf{y}_m^{(\nu)}\right)}{\mathcal{N}_{m,m+1}\circ\widetilde{\varphi}_{\mathcal{U}_{m,n}^{(\nu),\mathrm{ab}}}\left(\mathbf{y}_{m-1}^{(\nu)}\right)}\right)^{-1}\in\ 1+p\cdot\mathrm{Im}\left(\sigma_m^{(\nu)}\right).$$

Equivalently $\frac{\left(\mathbf{y}_m^{(\nu)}\right)^p}{\mathcal{N}_{m,m+1}\left(\mathbf{y}_m^{(\nu)}\right)}\times\widetilde{\varphi}_{\mathcal{U}_{m-1,n}^{(\nu),\mathrm{ab}}}\left(\frac{\left(\mathbf{y}_{m-1}^{(\nu)}\right)^p}{\mathcal{N}_{m-1,m}\left(\mathbf{y}_{m-1}^{(\nu)}\right)}\right)^{-1}\in\ 1+p\cdot\mathrm{Im}\left(\sigma_m^{(\nu)}\right)$, so (M4) holds.

Establishing that $\mathcal{S}^{(\nu)}\left((\mathbf{a}_m^{(\nu)})\right)$ satisfies (M3). We begin with a technical result describing the image of the map $\widetilde{\sigma_m}^{(\nu)}\colon\mathbb{Z}_p\left[\mathcal{U}_{m,n}^{(\nu),\mathrm{ab}}\right]\to\mathbb{Z}_p\left[\mathcal{U}_{m,n}^{(\nu),\mathrm{ab}}\right]$ sending $f\mapsto\sum_{i=0}^{p-1}\gamma^{-p^{m-1}i}f\gamma^{p^{m-1}i}$.

Lemma 6.8 *For each $m\in\{0,\dots,n-s\}$, the Γ-invariant submodule $H^0\left(\Gamma,\mathrm{Im}\left(\widetilde{\sigma_m}^{(\nu)}\right)\right)$ is finitely generated over $\mathbb{Z}_p\left[\Gamma/\Gamma^{p^\nu}\right]$ by the combined set*

$$\left\{\mathcal{A}_{\varpi}^{(m,n)}\ \middle|\ \varpi\in\mathrm{orb}_\Gamma\left(\overline{\mathcal{H}}_\infty^{(m,n)}\right),\#\varpi=p^m\right\}\cup\left\{\frac{\#\varpi}{p^{m-1}}\cdot\mathcal{A}_{\varpi}^{(m,n)}\ \middle|\ \varpi\in\mathrm{orb}_\Gamma\left(\overline{\mathcal{H}}_\infty^{(m,n)}\right),\#\varpi<p^m\right\}$$

and in particular, $\mathrm{Im}\left(\sigma_m^{(\nu)}\right)\subset H^0\left(\Gamma,\mathrm{Im}\left(\widetilde{\sigma_m}^{(\nu)}\right)\right)\subset\mathrm{Im}\left(\widetilde{\sigma_m}^{(\nu)}\right)$.

Proof. Because a generator $\gamma\in\Gamma$ acts trivially on $\Gamma^{p^m}/\Gamma^{p^\nu}$ and through I_2+M on $\overline{\mathcal{H}}_\infty^{(m,n)}$,

$$\begin{aligned}H^0\left(\Gamma,\mathbb{Z}_p\left[\mathcal{U}_{m,n}^{(\nu),\mathrm{ab}}\right]\right)\ &=\ \mathbb{Z}_p\left[\Gamma^{p^m}/\Gamma^{p^\nu}\right]\otimes_{\mathbb{Z}_p}H^0\left(\left\langle I_2+M\right\rangle,\mathbb{Z}_p\left[\overline{\mathcal{H}}_\infty^{(m,n)}\right]\right)\\ &=\ \mathbb{Z}_p\left[\Gamma^{p^m}/\Gamma^{p^\nu}\right]\cdot\left\langle\sum_{\overline{h}'\in\varpi}\overline{h}'\ \middle|\ \varpi\in\mathrm{orb}_\Gamma\left(\overline{\mathcal{H}}_\infty^{(m,n)}\right)\right\rangle\\ &=\ \mathbb{Z}_p\left[\Gamma^{p^m}/\Gamma^{p^\nu}\right]\cdot\left\langle\frac{\#\varpi}{p^m}\cdot\mathcal{A}_{\varpi}^{(m,n)}\ \middle|\ \varpi\in\mathrm{orb}_\Gamma\left(\overline{\mathcal{H}}_\infty^{(m,n)}\right)\right\rangle\end{aligned}$$

where we have employed the basic identity $\mathcal{A}_{\varpi_{\overline{h}}}^{(m,n)}=\sum_{i=0}^{p^m-1}\gamma^{-i}\overline{h}\gamma^i=\frac{p^m}{\#\varpi_{\overline{h}}}\cdot\sum_{\overline{h}'\in\varpi_{\overline{h}}}\overline{h}'$.

Now pick an element $\frac{\#\varpi_{\overline{h}}}{p^m}\cdot\mathcal{A}_{\varpi_{\overline{h}}}^{(m,n)}=\sum_{\overline{h}'\in\varpi_{\overline{h}}}\overline{h}'$ belonging to $H^0\left(\left\langle I_2+M\right\rangle,\mathbb{Z}_p\left[\overline{\mathcal{H}}_\infty^{(m,n)}\right]\right)$. Then one easily sees that

$$\frac{\#\varpi_{\overline{h}}}{p^m}\cdot\mathcal{A}_{\varpi_{\overline{h}}}^{(m,n)}\ =\ \frac{\#\varpi_{\overline{h}}}{p^m}\cdot\sum_{j=0}^{p^m-1}\gamma^{-j}\overline{h}\gamma^j\ =\ \sum_{i=0}^{p-1}\sum_{j=0}^{p^{m-1}-1}\frac{\#\varpi_{\overline{h}}}{p^m}\cdot\gamma^{-p^{m-1}i}\left(\gamma^{-j}\overline{h}\gamma^j\right)\gamma^{p^{m-1}i}$$

which coincides exactly with $\widetilde{\sigma_m}^{(\nu)}\big(f_{\overline{h}}\big)$, where $f_{\overline{h}} := \frac{\#\varpi_{\overline{h}}}{p^m} \cdot \sum_{j=0}^{p^{m-1}-1} \gamma^{-j}\overline{h}\gamma^j \in \mathbb{Q}_p\big[\overline{\mathcal{H}}_\infty^{(m,n)}\big]$. It follows that $p^z \cdot \Big(\frac{\#\varpi_{\overline{h}}}{p^m} \cdot \mathcal{A}_{\varpi_{\overline{h}}}^{(m,n)}\Big) \in \mathrm{Im}\big(\widetilde{\sigma_m}^{(\nu)}\big)$ if and only if $p^z \cdot f_{\overline{h}} \in \mathbb{Z}_p\big[\overline{\mathcal{H}}_\infty^{(m,n)}\big]$, and as

$$p^z \cdot f_{\overline{h}} \;=\; \begin{cases} p^z \cdot \sum_{j=0}^{p^{m-1}-1} \gamma^{-j}\overline{h}\gamma^j & \text{if } \#\varpi_{\overline{h}} = p^m \\ p^{z-1} \cdot \sum_{\overline{h}' \in \varpi_{\overline{h}}} \overline{h}' & \text{if } \#\varpi_{\overline{h}} < p^m, \end{cases}$$

the latter condition occurs when $z \geq 0$ if $\#\varpi = p^m$, or alternatively $z \geq 1$ if $\#\varpi < p^m$. Therefore the union of the sets $\big\{f_{\overline{h}} \;\big|\; \#\varpi_{\overline{h}} = p^m\big\}$ and $\big\{p \cdot f_{\overline{h}} \;\big|\; \#\varpi_{\overline{h}} < p^m\big\}$ will generate the Γ-invariant part of $\mathrm{Im}\big(\widetilde{\sigma_m}^{(\nu)}\big)$ over $\mathbb{Z}_p\big[\Gamma/\Gamma^{p^\nu}\big]$, as asserted.

Finally, the inclusion $\mathrm{Im}\big(\sigma_m^{(\nu)}\big) \hookrightarrow H^0\big(\Gamma, \mathrm{Im}\big(\widetilde{\sigma_m}^{(\nu)}\big)\big)$ occurs as the generators $\mathcal{A}_\varpi^{(m,n)}$ of the left-hand module are p-integral multiples of generators for the right-hand module. □

Proposition 6.9 *For each $m \geq 1$, the transfer sends $p \cdot \mathrm{Im}(\sigma_{m-1}) \overset{\mathrm{Ver}_{m-1,m}}{\longrightarrow} \mathrm{Im}\big(\widetilde{\sigma_m}^{(\nu)}\big)$.*

Proof. If we choose any $\overline{h} = \overline{h}_1^x\overline{h}_2^y \in \overline{\mathcal{H}}_\infty^{(m-1,n)}$ and $f(X) \in \mathbb{Z}_p[\![X]\!]$, then from Lemma 5.3:

$$\mathrm{Ver}_{m-1,m}\Big(f\big(\gamma^{p^{m-1}} - 1\big) \cdot \mathcal{A}_{\overline{h}_1^x\overline{h}_2^y}^{(m-1,n)}\Big) \;=\; p^{-1} \times f\big(\gamma^{p^m} - 1\big) \cdot \mathcal{A}_{\overline{h}_1^{x'}\overline{h}_2^{y'}}^{(m,n)}$$

where $\begin{pmatrix} x' \\ y' \end{pmatrix} \in \mathbb{Z}_p^2$ is given in Lemma 4.7. Setting $f(X) = p$, it follows immediately that

$$\mathrm{Ver}_{m-1,m}\Big(p \cdot \mathcal{A}_{\overline{h}_1^x\overline{h}_2^y}^{(m-1,n)}\Big) \;=\; \mathcal{A}_{\overline{h}_1^{x'}\overline{h}_2^{y'}}^{(m,n)} \;\in\; \mathrm{Im}\big(\sigma_m^{(\nu)}\big) \overset{\text{by } 6.8}{\hookrightarrow} \mathrm{Im}\big(\widetilde{\sigma_m}^{(\nu)}\big).$$

Lastly applying Proposition 4.5(ii), we know $p \cdot \mathrm{Im}\big(\sigma_{m-1}^{(\nu)}\big)$ is freely generated over the algebra $\mathbb{Z}_p\big[\Gamma^{p^{m-1}}/\Gamma^{p^\nu}\big]$ by the set of $p \cdot \mathcal{A}_{\overline{h}_1^x\overline{h}_2^y}^{(m-1,n)}$'s, hence the result is proven. □

Let us now establish that (M3) holds for $\big(\mathbf{y}_m^{(\nu)}\big) = \mathcal{S}^{(\nu)}\big((\mathbf{a}_m^{(\nu)})\big)$. For each integer $m \geq 2$,

$$\frac{\mathbf{y}_m^{(\nu)}}{\mathrm{Ver}_{m-1,m}\big(\mathbf{y}_{m-1}^{(\nu)}\big)} \overset{\text{by } 6.2}{=} \frac{\widetilde{\varphi}_{\mathcal{U}^{(\nu),\mathrm{ab}}_{m-1,n}}\big(\mathbf{y}_{m-1}^{(\nu)}\big) \times \exp_{\mathbb{Z}_p[\mathcal{U}^{(\nu),\mathrm{ab}}_{m,n}]}\big(\mathbf{a}_m^{(\nu)}\big)}{\mathrm{Ver}_{m-1,m}\Big(\widetilde{\varphi}_{\mathcal{U}^{(\nu),\mathrm{ab}}_{m-2,n}}\big(\mathbf{y}_{m-2}^{(\nu)}\big) \times \exp_{\mathbb{Z}_p[\mathcal{U}^{(\nu),\mathrm{ab}}_{m-1,n}]}\big(\mathbf{a}_{m-1}^{(\nu)}\big)\Big)}$$

$$= \widetilde{\varphi}_{\mathcal{U}^{(\nu),\mathrm{ab}}_{m-1,n}}\left(\frac{\mathbf{y}_{m-1}^{(\nu)}}{\mathrm{Ver}_{m-2,m-1}\big(\mathbf{y}_{m-2}^{(\nu)}\big)}\right) \times \exp_{\mathbb{Z}_p[\mathcal{U}^{(\nu),\mathrm{ab}}_{m,n}]}\Big(\mathbf{a}_m^{(\nu)} - \mathrm{Ver}_{m-1,m}\big(\mathbf{a}_{m-1}^{(\nu)}\big)\Big)$$

and the term $\mathbf{a}_m^{(\nu)} - \mathrm{Ver}_{m-1,m}\big(\mathbf{a}_{m-1}^{(\nu)}\big) \in \mathrm{Im}\big(\widetilde{\sigma_m^{(\nu)}}\big)$, using Lemma 6.8 and Proposition 6.9.

An identical argument to Proposition 6.1(b) shows that

$$\exp_{\mathbb{Z}_p[\mathcal{U}^{(\nu),\mathrm{ab}}_{m,n}]} : \frac{\mathrm{Im}\big(\widetilde{\sigma_m^{(\nu)}}\big)^N}{\mathrm{Im}\big(\widetilde{\sigma_m^{(\nu)}}\big)^{N+1}} \xrightarrow{\sim} \frac{1 + \mathrm{Im}\big(\widetilde{\sigma_m^{(\nu)}}\big)^N}{1 + \mathrm{Im}\big(\widetilde{\sigma_m^{(\nu)}}\big)^{N+1}}$$

is an isomorphism for every $N \geq 1$, in which case

$$\frac{\mathbf{y}_m^{(\nu)}}{\mathrm{Ver}_{m-1,m}\big(\mathbf{y}_{m-1}^{(\nu)}\big)} = \widetilde{\varphi}_{\mathcal{U}^{(\nu),\mathrm{ab}}_{m-1,n}}\left(\frac{\mathbf{y}_{m-1}^{(\nu)}}{\mathrm{Ver}_{m-2,m-1}\big(\mathbf{y}_{m-2}^{(\nu)}\big)}\right) \times \big(1 + \mathbf{d}_m\big)$$

for some $\mathbf{d}_m \in \mathrm{Im}\big(\widetilde{\sigma_m^{(\nu)}}\big)$.

Furthermore, one easily checks the containment $\widetilde{\varphi}_{\mathcal{U}^{(\nu),\mathrm{ab}}_{m-1,n}}\Big(\mathrm{Im}\big(\widetilde{\sigma_{m-1}^{(\nu)}}\big)\Big) \subset \mathrm{Im}\big(\widetilde{\sigma_m^{(\nu)}}\big)$. Therefore, if we inductively assume $\frac{\mathbf{y}_{m-1}^{(\nu)}}{\mathrm{Ver}_{m-2,m-1}\big(\mathbf{y}_{m-2}^{(\nu)}\big)} \in 1 + \mathrm{Im}\big(\widetilde{\sigma_{m-1}^{(\nu)}}\big)$, one may conclude $\frac{\mathbf{y}_m^{(\nu)}}{\mathrm{Ver}_{m-1,m}\big(\mathbf{y}_{m-1}^{(\nu)}\big)} \in 1 + \mathrm{Im}\big(\widetilde{\sigma_m^{(\nu)}}\big)$. Property (M3) then follows for all $m \geq 2$ by induction. (If $m = 1$ the same argument works fine, except one omits the denominator terms above.)

Proof of Theorem 3.2. As mentioned earlier, now that we have constructed the section $\mathcal{S}^{(\nu)}$ mapping $p \cdot \Psi^{(\nu)}$ into $\Phi^{(\nu)}$, to check whether $\big(\mathbf{y}_m^{(\nu)}\big)$ arises from an element of $K_1\big(\mathbb{Z}_p[\mathcal{G}^{(\nu)}_{\infty,n}]\big)$ it is the same as verifying if $\mathcal{L}^{(\nu)}_{\underline{\chi}}\big((\mathbf{y}^{(\nu)}_{m,\chi})\big) \in \underline{\chi}\big(\Psi^{(\nu)}\big)$. However, the latter is equivalent to checking whether $\mathcal{L}^{(\nu)}_{\underline{\chi}}\big((\mathbf{y}^{(\nu)}_{m,\chi})\big)$ satisfies the conditions (C1)–(C4) listed in Theorem 5.1.

Theorem 6.10 *If $\star \in \{III, IV, V, VI\}$, then $\mathcal{L}^{(\nu)}_{\underline{\chi}}\big((\mathbf{y}^{(\nu)}_{m,\chi})\big)$ satisfies conditions (C1)–(C4) in Theorem 5.1 if and only if:*

(i) $\mathcal{N}_{\mathrm{Stab}_\Gamma(\chi)/\Gamma^{p^m}}\big(\mathbf{y}^{(\nu)}_{\mathbf{m}_\chi,\chi}\big) = \mathbf{y}^{(\nu)}_{m,\chi}$ *at each* $m \in \{\mathbf{m}_\chi, \ldots, n-s\}$,

(ii) $\mathbf{y}^{(\nu)}_{m,\chi'} = \mathbf{y}^{(\nu)}_{m,\chi}$ *whenever* $\chi' \in \Gamma * \chi$, *and*

(iii)
$$\prod_{\chi\in\mathfrak{R}_{m,\infty}} \mathcal{N}_{\mathrm{Stab}_\Gamma(\chi)/\Gamma^{p^m}} \left(\frac{\mathbf{y}^{(\nu)}_\chi}{\varphi\big(\mathbf{y}^{(\nu)}_{\chi^p}\big)} \cdot \frac{\varphi\big(\mathcal{N}_{0,\mathbf{m}_\chi-1}\big(\mathbf{y}^{(\nu)}_{\mathbf{1}}\big)\big)}{\mathcal{N}_{0,\mathbf{m}_\chi}\big(\mathbf{y}^{(\nu)}_{\mathbf{1}}\big)}\right)^{\mathrm{Tr}(\mathrm{Ind}\chi^*)(\varpi)}$$
$$\equiv 1 \mod p^{N^{(m)}_{\star,1}+N^{(m)}_{\star,2}+m-\mathrm{ord}_p(\#\varpi)} \cdot \mathbb{Z}_p\big[\Gamma^{p^m}/\Gamma^{p^\nu}\big]$$

for every integer $m \in \{0,\dots,\nu\}$, *and every orbit* $\varpi \in \mathrm{orb}_\Gamma\big(\overline{\mathcal{H}}^{(m,\infty)}_\infty\big)$.

Proof. If one chooses the sequence $\big(\mathbf{a}^{(m,\nu)}_\chi\big) := \mathcal{L}^{(\nu)}_{\underline{\chi}}\big((\mathbf{y}^{(\nu)}_{m,\chi})\big)$, then (C1) is readily seen to be equivalent to (i), while condition (C2) is equivalent to (ii). Focussing therefore on conditions (C3) and (C4), if one puts $\mathbf{e}^*_{\chi,\varpi} = \mathrm{Tr}\big(\mathrm{Ind}\chi^*\big)(\varpi)$ then

$$\sum_{\chi\in\mathfrak{R}_{m,n}} \mathrm{Tr}_{\mathrm{Stab}_\Gamma(\chi)/\Gamma^{p^m}}\big(\mathbf{a}^{(\nu)}_\chi\big)\cdot \mathrm{Tr}\big(\mathrm{Ind}\chi^*\big)(\varpi) = \sum_{\chi\in\mathfrak{R}_{m,n}} \mathbf{e}^*_{\chi,\varpi} \times \mathrm{Tr}_{\mathrm{Stab}_\Gamma(\chi)/\Gamma^{p^m}}\big(\mathbf{a}^{(\nu)}_\chi\big)$$
$$\overset{\text{by (6.6)}}{=} \sum_{\chi\in\mathfrak{R}_{m,n}} \mathbf{e}^*_{\chi,\varpi} \times \mathrm{Tr}_{\mathrm{Stab}_\Gamma(\chi)/\Gamma^{p^m}} \circ \log\left(\frac{\mathbf{y}^{(\nu)}_\chi}{\mathcal{N}_{0,\mathbf{m}_\chi}\big(\mathbf{y}^{(\nu)}_{\mathbf{1}}\big)} \cdot \varphi_{\frac{\Gamma^{p^{\mathbf{m}_\chi-1}}}{\Gamma^{p^\nu}}}\left(\frac{\mathcal{N}_{0,\mathbf{m}_\chi-1}\big(\mathbf{y}^{(\nu)}_{\mathbf{1}}\big)}{\mathbf{y}^{(\nu)}_{\chi^p}}\right)\right)$$
$$= \log_{\mathbb{Z}_p\left[\frac{\Gamma^{p^m}}{\Gamma^{p^\nu}}\right]}\left(\prod_{\chi\in\mathfrak{R}_{m,n}} \mathcal{N}_{\mathrm{Stab}_\Gamma(\chi)/\Gamma^{p^m}}\left(\frac{\mathbf{y}^{(\nu)}_\chi}{\mathcal{N}_{0,\mathbf{m}_\chi}\big(\mathbf{y}^{(\nu)}_{\mathbf{1}}\big)} \cdot \varphi_{\frac{\Gamma^{p^{\mathbf{m}_\chi-1}}}{\Gamma^{p^\nu}}}\left(\frac{\mathcal{N}_{0,\mathbf{m}_\chi-1}\big(\mathbf{y}^{(\nu)}_{\mathbf{1}}\big)}{\mathbf{y}^{(\nu)}_{\chi^p}}\right)\right)^{\mathbf{e}^*_{\chi,\varpi}}\right).$$

Recall that (C3) and (C4) together imply $\sum_{\chi\in\mathfrak{R}_{m,n}}\mathrm{Tr}_{\mathrm{Stab}_\Gamma(\chi)/\Gamma^{p^m}}\big(\mathbf{a}^{(\nu)}_\chi\big)\cdot\mathrm{Tr}\big(\mathrm{Ind}\chi^*\big)(\varpi)$ is congruent to zero modulo $p^{\mathrm{ord}_p(\#\overline{\mathcal{H}}^{(m,n)}_\infty)+m-\mathrm{ord}_p(\#\varpi)} \cdot \mathbb{Z}_p[\Gamma^{p^m}/\Gamma^{p^\nu}]$, for $m \in \{0,\dots,n-s\}$ and at each orbit $\varpi \in \mathrm{orb}_\Gamma\big(\overline{\mathcal{H}}^{(m,n)}_\infty\big)$. Now for all integers $i \geq 1$, the mappings $\log : 1 + p^i\cdot\mathbb{Z}_p[\Gamma^{p^m}/\Gamma^{p^\nu}] \overset{\sim}{\longrightarrow} p^i\cdot\mathbb{Z}_p[\Gamma^{p^m}/\Gamma^{p^\nu}]$ and $\exp : p^i\cdot\mathbb{Z}_p[\Gamma^{p^m}/\Gamma^{p^\nu}] \overset{\sim}{\longrightarrow} 1 + p^i\cdot\mathbb{Z}_p[\Gamma^{p^m}/\Gamma^{p^\nu}]$ are inverse isomorphisms to each other. As an immediate consequence,

$$\sum_{\chi\in\mathfrak{R}_{m,n}} \mathrm{Tr}_{\mathrm{Stab}_\Gamma(\chi)/\Gamma^{p^m}}\big(\mathbf{a}^{(\nu)}_\chi\big)\cdot\mathrm{Tr}\big(\mathrm{Ind}\chi^*\big)(\varpi) \equiv 0 \mod p^{\mathrm{ord}_p(\#\overline{\mathcal{H}}^{(m,n)}_\infty)+m-\mathrm{ord}_p(\#\varpi)}\cdot\mathbb{Z}_p\left[\frac{\Gamma^{p^m}}{\Gamma^{p^\nu}}\right]$$

if and only if $\prod_{\chi\in\mathfrak{R}_{m,n}} \mathcal{N}_{\mathrm{Stab}_\Gamma(\chi)/\Gamma^{p^m}}\left(\frac{\mathbf{y}^{(\nu)}_\chi}{\varphi\big(\mathbf{y}^{(\nu)}_{\chi^p}\big)}\cdot\frac{\varphi\big(\mathcal{N}_{0,\mathbf{m}_\chi-1}\big(\mathbf{y}^{(\nu)}_{\mathbf{1}}\big)\big)}{\mathcal{N}_{0,\mathbf{m}_\chi}\big(\mathbf{y}^{(\nu)}_{\mathbf{1}}\big)}\right)^{\mathrm{Tr}(\mathrm{Ind}\chi^*)(\varpi)}$ belongs to $1 + p^{\mathrm{ord}_p(\#\overline{\mathcal{H}}^{(m,n)}_\infty)+m-\mathrm{ord}_p(\#\varpi)}\cdot\mathbb{Z}_p[\Gamma^{p^m}/\Gamma^{p^\nu}]$.

Finally, both $\overline{\mathcal{H}}^{(m,n)}_\infty \cong \overline{\mathcal{H}}^{(m,\infty)}_\infty$ and $\mathfrak{R}_{m,n} = \mathfrak{R}_{m,\infty}$ provided that $\star \in$ {III,IV,V,VI}; moreover $\mathrm{ord}_p\big(\#\overline{\mathcal{H}}^{(m,n)}_\infty\big) = N^{(m)}_{\star,1} + N^{(m)}_{\star,2}$, therefore the equivalence is fully established. □

The reader will notice that these congruences are independent of the choice of $n \geq m+s$. They also behave well if we take the projective limit as $\nu \to \infty$, hence one can obtain analogous congruences for the completed group algebras $\mathbb{Z}_p\big[\big[\Gamma^{p^m}\big]\big] = \varprojlim_\nu \mathbb{Z}_p[\Gamma^{p^m}/\Gamma^{p^\nu}]$, i.e. those congruences labelled Equation (3.2) in Chapter 3.

The proof of the 'non-$\mathcal{S}$-localised version' of Theorem 3.2 has therefore been completed, i.e. a sequence $\big(\mathbf{y}_{m,\chi}\big) \in \prod_{m,\chi} \Lambda_{\mathcal{O}_{\mathbb{C}_p}}\big(\Gamma^{p^m}\big)^\times$ belongs to $\Theta_{\infty,\underline{\chi}}\big(K_1'(\Lambda(\mathcal{G}_\infty))\big)$ if and only if $\mathcal{N}_{\mathrm{Stab}_\Gamma(\chi)/\Gamma^{p^m}}\big(\mathbf{y}^{(\nu)}_{\mathbf{m}_\chi,\chi}\big) = \mathbf{y}^{(\nu)}_{m,\chi}$ if $m \geq \mathbf{m}_\chi$, secondly $\mathbf{y}^{(\nu)}_{m,\chi'} = \mathbf{y}^{(\nu)}_{m,\chi}$ for $\chi' \in \Gamma * \chi$, and lastly

$$\prod_{\chi \in \mathfrak{R}_{m,\infty}} \mathcal{N}_{\mathrm{Stab}_\Gamma(\chi)/\Gamma^{p^m}} \left(\frac{\mathbf{y}_\chi}{\varphi\big(\mathbf{y}_{\chi^p}\big)} \cdot \frac{\varphi\big(\mathcal{N}_{0,\mathbf{m}_\chi-1}\big(\mathbf{y}_{\mathbf{1}}\big)\big)}{\mathcal{N}_{0,\mathbf{m}_\chi}\big(\mathbf{y}_{\mathbf{1}}\big)} \right)^{\mathrm{Tr}(\mathrm{Ind}\chi^*)(\varpi)}$$
$$\equiv\ 1 \mod p^{N^{(m)}_{\star,1}+N^{(m)}_{\star,2}+m-\mathrm{ord}_p(\#\varpi)} \cdot \mathbb{Z}_p\big[\big[\Gamma^{p^m}\big]\big]$$

for every positive integer m, and at every orbit $\varpi \in \mathrm{orb}_\Gamma\big(\overline{\mathcal{H}}^{(m,\infty)}_\infty\big)$.

Remarks: (a) If $\star =$II, the proof of Theorem 3.1 runs along identical lines – the only point of departure is that $N^{(m)}_{II,1} = n$ and $N^{(m)}_{II,2} = s+m$, so $\mathfrak{R}_{m,n}$ is no longer independent of n. Nevertheless in Case (II), the multiplicative conditions equivalent to (C3) and (C4) are

$$\prod_{\chi \in \mathfrak{R}_{m,n}} \mathcal{N}_{\mathrm{Stab}_\Gamma(\chi)/\Gamma^{p^m}} \left(\frac{\mathbf{y}_\chi}{\varphi\big(\mathbf{y}_{\chi^p}\big)} \cdot \frac{\varphi\big(\mathcal{N}_{0,\mathbf{m}_\chi-1}\big(\mathbf{y}_{\mathbf{1}}\big)\big)}{\mathcal{N}_{0,\mathbf{m}_\chi}\big(\mathbf{y}_{\mathbf{1}}\big)} \right)^{\mathrm{Tr}(\mathrm{Ind}\chi^*)(\varpi)}$$
$$\equiv\ 1 \mod p^{s+2m+n-\mathrm{ord}_p(\#\varpi)} \cdot \mathbb{Z}_p\big[\big[\Gamma^{p^m}\big]\big] \quad (6.7)$$

for every positive integer $m \leq n-s$, and at every orbit $\varpi \in \mathrm{orb}_\Gamma\big(\overline{\mathcal{H}}^{(m,n)}_\infty\big)$.

(b) To transform these into the congruences labelled Equation (3.1), one must calculate each of $\mathfrak{R}_{m,n}$, $\#\varpi$ and $\mathrm{Tr}(\mathrm{Ind}\chi^*)(\varpi)$ precisely – we refer the reader to the worked example given later in §7.1, for the full details.

(c) Of course, this still only gives us a non-$\mathcal{S}$-localised version of Theorem 3.1, describing $\Theta_{\infty,\underline{\chi}}\big(K_1'(\Lambda(\mathcal{G}_\infty))\big)$ rather than $\Theta_{\infty,\mathcal{S},\underline{\chi}}\big(K_1'\big(\Lambda(\mathcal{G}_\infty)_\mathcal{S}\big)\big)$, which is an issue we address below.

Extending these congruences to the localisations. Finally, we explain how to extend these results from $K_1'\big(\Lambda(\mathcal{G}_\infty)\big)$, to both of the Ore localisations $K_1'\big(\Lambda(\mathcal{G}_\infty)_{\mathcal{S}}\big)$ and $K_1'\big(\Lambda(\mathcal{G}_\infty)_{\mathcal{S}^*}\big)$. Let us focus first on $K_1\big(\Lambda(\mathcal{G}_\infty)_{\mathcal{S}}\big)$, and write

$$\Theta_{\infty,\mathcal{S}} : K_1\big(\Lambda(\mathcal{G}_\infty)_{\mathcal{S}}\big) \to \prod_{m\geq 0} K_1\big(\Lambda(\mathcal{U}_m^{\mathrm{ab}})_{\overline{\mathcal{S}}}\big)$$

for the corresponding collection of morphisms $\prod \theta_{m,\mathcal{S}}$, with $\theta_{m,\mathcal{S}} := \mathcal{N}_{\mathcal{U}_m}(-)$ mod $[\mathcal{U}_m, \mathcal{U}_m]$.

In order to extend the arguments in §6.1-§6.3 so as to produce non-abelian congruence conditions '$\Phi_{\mathcal{S}}$' describing $\mathrm{Im}\big(\Theta_{\infty,\mathcal{S}}\big)$, one must first extend the Taylor-Oliver logarithm to a homomorphism

$$\mathrm{LOG}_{\mathcal{G}_{\infty,n},\mathcal{S}} : K_1\Big(\widehat{\Lambda(\mathcal{G}_{\infty,n})_{\mathcal{S}}}\Big) \longrightarrow \frac{\widehat{\Lambda(\mathcal{G}_{\infty,n})_{\mathcal{S}}}}{\big[\widehat{\Lambda(\mathcal{G}_{\infty,n})_{\mathcal{S}}}, \widehat{\Lambda(\mathcal{G}_{\infty,n})_{\mathcal{S}}}\big]} \quad \text{for every } n \geq 1,$$

where $\widehat{\Lambda(\mathcal{G}_{\infty,n})_{\mathcal{S}}}$ denotes the $\mathrm{Jac}\big(\mathbb{Z}_p[\mathcal{H}_{\infty,n}]\big)$-adic completion of the localisation $\Lambda(\mathcal{G}_{\infty,n})_{\mathcal{S}}$. This task has already been partially accomplished (see for example [CSRV12, Section 5] or [Kak13]), but not enough is known about the kernel and cokernel of these maps on the completion. Indeed by [CSRV12, Lemma 5.2], the extension of the logarithm sits inside a commutative square

$$\begin{tikzcd}
K_1\big(\Lambda(\mathcal{G}_{\infty,n})\big) \arrow[r] \arrow[d, "\mathrm{LOG}_{\mathcal{G}_{\infty,n}}"] & K_1\big(\widehat{\Lambda(\mathcal{G}_{\infty,n})_{\mathcal{S}}}\big) \arrow[d, "\mathrm{LOG}_{\mathcal{G}_{\infty,n},\mathcal{S}}"] \\
\mathbb{Z}_p\big[\big[\mathrm{Conj}(\mathcal{G}_{\infty,n})\big]\big] \arrow[r] & \dfrac{\widehat{\Lambda(\mathcal{G}_{\infty,n})_{\mathcal{S}}}}{\big[\widehat{\Lambda(\mathcal{G}_{\infty,n})_{\mathcal{S}}}, \widehat{\Lambda(\mathcal{G}_{\infty,n})_{\mathcal{S}}}\big]}
\end{tikzcd}$$

where the horizontal arrows are induced from the natural inclusion $\Lambda(\mathcal{G}_{\infty,n}) \hookrightarrow \widehat{\Lambda(\mathcal{G}_{\infty,n})_{\mathcal{S}}}$.

We simply observe that the properties of the Taylor-Oliver logarithm we derived in §6.3 extend to the $\mathrm{Jac}\big(\mathbb{Z}_p[\mathcal{H}_{\infty,n}]\big)$-adic completion if one ignores their kernels/cokernels, and omit the details (which are anyway identical to Section 5 of *op. cit.*). The remainder of the proof of Theorems 3.1 and 3.2 in the $\mathcal{S}$-localised situation then follows readily, albeit the congruences in Equations (3.1) and (3.2) are now taken modulo $p^\bullet \cdot \mathbb{Z}_p\big[\big[\Gamma^{p^m}\big]\big]_{(p)}$ rather than just modulo $p^\bullet \cdot \mathbb{Z}_p\big[\big[\Gamma^{p^m}\big]\big]$, and we unfortunately lose their sufficiency in the process.

We now turn our attention to the $\mathcal{S}^*$-localisation, $\Lambda(\mathcal{G}_\infty)_{\mathcal{S}^*}$, which is less problematic. Recall that $\mathcal{G}_\infty$ has no element of order p, in which case Burns and Venjakob [BV11, Prop 3.4] have constructed a splitting

$$K_1\big(\Lambda(\mathcal{G}_\infty)_{\mathcal{S}^*}\big) \;\cong\; K_1\big(\Lambda(\mathcal{G}_\infty)_{\mathcal{S}}\big) \oplus K_0\big(\mathbb{F}_p[\![\mathcal{G}_\infty]\!]\big).$$

Furthermore, there exists another commutative diagram

$$\begin{tikzcd}
K_1\big(\Lambda(\mathcal{G}_\infty)_{\mathcal{S}^*}\big) \arrow[r, "\sim"] \arrow[d, "\Theta_{\infty,\mathcal{S}^*}"] & K_1\big(\Lambda(\mathcal{G}_\infty)_{\mathcal{S}}\big) \oplus K_0\big(\mathbb{F}_p[\![\mathcal{G}_\infty]\!]\big) \arrow[d, "{(\Theta_{\infty,\mathcal{S}},\Theta_0)}"] \\
\prod_{m\geq 0} K_1\big(\Lambda(\mathcal{U}_m^{\mathrm{ab}})_{\overline{\mathcal{S}}^*}\big) & \prod_{m\geq 0} K_1\big(\Lambda(\mathcal{U}_m^{\mathrm{ab}})_{\overline{\mathcal{S}}}\big) \oplus K_0\big(\mathbb{F}_p[\![\mathcal{U}_m^{\mathrm{ab}}]\!]\big) \arrow[l, hook']
\end{tikzcd}$$

where the map $\Theta_0 : K_0\big(\mathbb{F}_p[\![\mathcal{G}_\infty]\!]\big) \to \prod_{m\geq 0} K_0\big(\mathbb{F}_p[\![\mathcal{U}_m^{\mathrm{ab}}]\!]\big)$ encodes how the non-commutative μ-invariant information in $K_0\big(\mathbb{F}_p[\![\mathcal{G}_\infty]\!]\big)$ gets distributed amongst its abelian fragments.

Thus a sequence $(\mathbf{y}_{\overline{\mathcal{S}}^*,m})$ lies in the image of $\Theta_{\infty,\mathcal{S}^*}$, if and only if each term factorises into $\mathbf{y}_{\overline{\mathcal{S}}^*,m} = \big(\mathbf{y}_{\overline{\mathcal{S}},m}, \mu_m\big)$ where the components $(\mathbf{y}_{\overline{\mathcal{S}},m}) \in \mathrm{Im}\big(\Theta_{\infty,\mathcal{S}}\big)$ and $(\mu_m) \in \mathrm{Im}(\Theta_0)$. Note that $\mathcal{G}_\infty$ is a pro-p-group so that $K_0\big(\mathbb{F}_p[\![\mathcal{G}_\infty]\!]\big) \cong \mathbb{Z}$, and similarly $K_0\big(\mathbb{F}_p[\![\mathcal{U}_m^{\mathrm{ab}}]\!]\big) \cong \mathbb{Z}$. Consequently a tuple $(\mu_m) \in \prod_m K_0\big(\mathbb{F}_p[\![\mathcal{U}_m^{\mathrm{ab}}]\!]\big)$ arises from the image of Θ_0 if and only if for every integer $m \geq 0$, one has $\mu_m = [\mathcal{G}_\infty : \mathcal{U}_m] \times \mu$ for some fixed $\mu \in \mathbb{Z}$.

Because the bottom arrow in the above diagram may possibly not be surjective, the most one can say is that any $(\mathbf{y}_{\overline{\mathcal{S}}^*,m}) \in \mathrm{Im}\big(\Theta_{\infty,\mathcal{S}^*}\big)$ must of necessity satisfy (M1)–(M4). If we denote this subset of $\prod_{m\geq 0} K_1\big(\Lambda(\mathcal{U}_m^{\mathrm{ab}})_{\overline{\mathcal{S}}^*}\big)$ satisfying (M1)–(M4) by '$\Phi_{\mathcal{S}^*}$', then this potential lack of surjectivity yields another obstruction to $\Theta_{\infty,\mathcal{S}^*} : K_1'\big(\Lambda(\mathcal{G}_\infty)_{\mathcal{S}^*}\big) \to \Phi_{\mathcal{S}^*}$ being an isomorphism. In terms of $\Theta_{\infty,\underline{\chi},\mathcal{S}^*} = \underline{\chi} \circ \Theta_{\infty,\mathcal{S}^*}$ from the Introduction, this translates into the necessity of the congruences written down in Theorems 3.1 and 3.2 holding for $\underline{\chi}(\mathbf{y}_{\overline{\mathcal{S}}^*,m}) \in \prod_{m,\chi} \mathrm{Quot}\big(\Lambda_{\mathcal{O}_\chi}(\Gamma^{p^m})\big)^\times$, but *not* their sufficiency regrettably.

Chapter 7

Some Explicit Computations

The various quantities $\mathfrak{R}_{m,n}$, ϖ and $\mathbf{e}^*_{\chi,\varpi}$ occurring in the congruences (3.1) and (3.2) are easy to define in theory, but it is not quite so evident how to work them out in practice. We shall now give a step-by-step guide to calculating these terms algorithmically.

Step 1: We first explain how to express $\tilde{\chi}_{1,N^{(m)}_{\star,1}}$ and $\tilde{\chi}_{2,N^{(m)}_{\star,2}}$ in terms of $\chi_{1,n}$ and $\chi_{2,n}$.

Step 2: We next explicitly list representatives for $\mathfrak{R}_{m,n}$ in the form $\tilde{\chi}^a_{1,N^{(m)}_{\star,1}} \cdot \tilde{\chi}^b_{2,N^{(m)}_{\star,2}}$.

Step 3: We end by giving formulae to compute both $\#\varpi$ and $\mathbf{e}^*_{\chi,\varpi} = \mathrm{Tr}\big(\mathrm{Ind}\chi^*\big)(\varpi)$.

The technical results corresponding to Steps 1, 2, 3 in the text below are respectively Proposition 7.1, Lemma 7.2 and Lemma 7.3. We shall then give an even more concrete description in two special situations, namely Case (II) and Case (III) - see Corollary 7.4 and Corollary 7.8.

Definition 7.1 *(a) We set the non-negative integer pair* $\left(\mathbf{e}^{[1,m]}_{\star,1},\mathbf{e}^{[1,m]}_{\star,2}\right)$ *equal to*

- $(0,1)$
- $\left(\dfrac{p^{s+m}}{\lambda^{p^m}_{III,\pm}-1}\ ,\ 0\right)$
- $\left(\dfrac{p^{s+m}}{2}\left(\dfrac{1}{\lambda^{p^m}_{IV,+}-1}+\dfrac{1}{\lambda^{p^m}_{IV,-}-1}\right),\ \dfrac{p^{s+m}}{2\sqrt{d}}\left(\dfrac{1}{\lambda^{p^m}_{IV,+}-1}-\dfrac{1}{\lambda^{p^m}_{IV,-}-1}\right)\right)$
- $\left(\dfrac{p^{s+m+\mathrm{ord}_p(d)}}{2}\left(\dfrac{1-\frac{p^r}{2\sqrt{\Delta_V}}}{\lambda^{p^m}_{V,+}-1}+\dfrac{1+\frac{p^r}{2\sqrt{\Delta_V}}}{\lambda^{p^m}_{V,-}-1}\right),\dfrac{p^{s+m+\mathrm{ord}_p(d)}}{2\sqrt{\Delta_V}}\left(\dfrac{1}{\lambda^{p^m}_{V,+}-1}-\dfrac{1}{\lambda^{p^m}_{V,-}-1}\right)\right)$
- $\left(\dfrac{p^{s+m}}{2}\left(\dfrac{p^{r+\mathrm{ord}_p(t)}}{\lambda^{p^m}_{VI,+}-1}+\dfrac{p^{r+\mathrm{ord}_p(t)}}{\lambda^{p^m}_{VI,-}-1}\right),\ \dfrac{p^{s+m}}{2\sqrt{p^rt}}\left(\dfrac{p^{r+\mathrm{ord}_p(t)}}{\lambda^{p^m}_{VI,+}-1}-\dfrac{p^{r+\mathrm{ord}_p(t)}}{\lambda^{p^m}_{VI,-}-1}\right)\right)$

in Cases (II), (III), (IV), (V) and (VI) respectively.

(b) Likewise, we shall define a second pair $\left(\mathbf{e}^{[2,m]}_{\star,1},\mathbf{e}^{[2,m]}_{\star,2}\right)$ *by setting it equal to*

- $(1,0)$
- $\left(0\ ,\ \dfrac{p^{s+m}}{\lambda^{p^m}_{III,\pm}-1}\right)$
- $\left(\dfrac{p^{s+m}\sqrt{d}}{2}\left(\dfrac{1}{\lambda^{p^m}_{IV,+}-1}-\dfrac{1}{\lambda^{p^m}_{IV,-}-1}\right),\ \dfrac{p^{s+m}}{2}\left(\dfrac{1}{\lambda^{p^m}_{IV,+}-1}+\dfrac{1}{\lambda^{p^m}_{IV,-}-1}\right)\right)$
- $\left(\dfrac{p^{s+m}d}{2\sqrt{\Delta_V}}\left(\dfrac{1}{\lambda^{p^m}_{V,+}-1}-\dfrac{1}{\lambda^{p^m}_{V,-}-1}\right),\ \dfrac{p^{s+m}}{2}\left(\dfrac{1+\frac{p^r}{2\sqrt{\Delta_V}}}{\lambda^{p^m}_{V,+}-1}+\dfrac{1-\frac{p^r}{2\sqrt{\Delta_V}}}{\lambda^{p^m}_{V,-}-1}\right)\right)$
- $\left(\dfrac{p^{s+m}\sqrt{p^rt}}{2}\left(\dfrac{1}{\lambda^{p^m}_{VI,+}-1}-\dfrac{1}{\lambda^{p^m}_{VI,-}-1}\right),\ \dfrac{p^{s+m}}{2}\left(\dfrac{1}{\lambda^{p^m}_{VI,+}-1}+\dfrac{1}{\lambda^{p^m}_{VI,-}-1}\right)\right)$

again in Cases (II), (III), (IV), (V) and (VI) respectively.

Proposition 7.1 *For integers* $n \gg 0$*, one has the character relations*

$$\tilde{\chi}_{1,N^{(m)}_{\star,1}} \quad = \quad \begin{cases} \chi^{0}_{1,n}\cdot\chi^{1}_{2,n} & \textit{if } \star{=}II \\ \chi^{\mathbf{e}^{[1,m]}_{III,1}}_{1,s+m}\cdot\chi^{0}_{2,s+m} & \textit{if } \star{=}III \\ \chi^{\mathbf{e}^{[1,m]}_{IV,1}}_{1,s+m}\cdot\chi^{\mathbf{e}^{[1,m]}_{IV,2}}_{2,s+m} & \textit{if } \star{=}IV \\ \chi^{\mathbf{e}^{[1,m]}_{V,1}}_{1,s+m+\mathrm{ord}_p(d)}\cdot\chi^{\mathbf{e}^{[1,m]}_{V,2}}_{2,s+m+\mathrm{ord}_p(d)} & \textit{if } \star{=}V \\ \chi^{\mathbf{e}^{[1,m]}_{VI,1}}_{1,s+m+r+\mathrm{ord}_p(t)}\cdot\chi^{\mathbf{e}^{[1,m]}_{VI,2}}_{2,s+m+r+\mathrm{ord}_p(t)} & \textit{if } \star{=}VI \end{cases}$$

and

$$\tilde{\chi}_{2,N^{(m)}_{\star,2}} \;=\; \begin{cases} \chi^{1}_{1,s+m}\cdot\chi^{0}_{2,s+m} & \textit{if } \star\textit{=II} \\ \chi^{0}_{1,s+m}\cdot\chi^{\mathbf{e}^{[2,m]}_{III,2}}_{2,s+m} & \textit{if } \star\textit{=III} \\ \chi^{\mathbf{e}^{[2,m]}_{IV,1}}_{1,s+m}\cdot\chi^{\mathbf{e}^{[2,m]}_{IV,2}}_{2,s+m} & \textit{if } \star\textit{=IV} \\ \chi^{\mathbf{e}^{[2,m]}_{V,1}}_{1,s+m}\cdot\chi^{\mathbf{e}^{[2,m]}_{V,2}}_{2,s+m} & \textit{if } \star\textit{=V} \\ \chi^{\mathbf{e}^{[2,m]}_{VI,1}}_{1,s+m}\cdot\chi^{\mathbf{e}^{[2,m]}_{VI,2}}_{2,s+m} & \textit{if } \star\textit{=VI.} \end{cases}$$

Proof. The situation where $\star$ =II has already been dealt with in §5.2, cf. Equation (5.2). Let us instead suppose $\star\in\{\text{III,IV,V,VI}\}$. We first recall from Definition 5.1 that

- $\tilde{\chi}_{1,N^{(m)}_{\star,1}}\begin{pmatrix} x \\ y \end{pmatrix} = \chi_{1,N^{(m)}_{\star,1}}\left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\mathcal{T}_{\star,m,1}\begin{pmatrix} x \\ y \end{pmatrix}\right)$, and
- $\tilde{\chi}_{2,N^{(m)}_{\star,2}}\begin{pmatrix} x \\ y \end{pmatrix} = \chi_{2,N^{(m)}_{\star,2}}\left(\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\mathcal{T}_{\star,m,2}\begin{pmatrix} x \\ y \end{pmatrix}\right)$

where $\mathcal{T}_{\star,m,j} := p^{N^{(m)}_{\star,j}}\Big(\big(I_2+M\big)^{p^m}-I_2\Big)^{-1}$. Further, one can diagonalise the γ-action via

$$\big(I_2+M\big)^{p^m} = \; P_\star\, D_\star^{p^m} P_\star^{-1} \quad \text{with } \; D_\star = \begin{pmatrix} \lambda_{\star,+} & 0 \\ 0 & \lambda_{\star,-} \end{pmatrix} \text{ and } \; P_\star\in\mathrm{GL}_2(\overline{\mathbb{Q}}_p).$$

The next objective is to calculate the matrices $\mathcal{T}_{\star,m,j}$ on an individual, case-by-case basis.

Case (III). Here $P_{III}=I_2$ and $N^{(m)}_{III,1}=N^{(m)}_{III,2}=s+m$, so that

$$p^{N^{(m)}_{III,j}}\Big((I_2+M)^{p^m}-I_2\Big)^{-1} = \begin{pmatrix} \frac{p^{s+m}}{(1+p^s)^{p^m}-1} & 0 \\ 0 & \frac{p^{s+m}}{(1+p^s)^{p^m}-1} \end{pmatrix}.$$

Case (IV). Here $P_{IV}=\begin{pmatrix} 1 & 1 \\ \sqrt{d} & -\sqrt{d} \end{pmatrix}$ and $N^{(m)}_{IV,1}=N^{(m)}_{IV,2}=s+m$, so that for each $j\in\{1,2\}$, the matrix $p^{N^{(m)}_{IV,j}}\Big((I_2+M)^{p^m}-I_2\Big)^{-1}$ equals

$$\frac{p^{s+m}}{2}\begin{pmatrix} \frac{1}{\lambda^{p^m}_{IV,+}-1}+\frac{1}{\lambda^{p^m}_{IV,-}-1} & \frac{1}{\sqrt{d}}\left(\frac{1}{\lambda^{p^m}_{IV,+}-1}-\frac{1}{\lambda^{p^m}_{IV,-}-1}\right) \\ \sqrt{d}\left(\frac{1}{\lambda^{p^m}_{IV,+}-1}-\frac{1}{\lambda^{p^m}_{IV,-}-1}\right) & \frac{1}{\lambda^{p^m}_{IV,+}-1}+\frac{1}{\lambda^{p^m}_{IV,-}-1} \end{pmatrix}.$$

Case (V). Assume that $n \geq s+m+\mathrm{ord}_p(d)$. Then $P_V = \begin{pmatrix} 1 & 1 \\ \frac{p^r}{2}+\sqrt{\Delta_V} & \frac{p^r}{2}-\sqrt{\Delta_V} \end{pmatrix}$ with $\Delta_V = d + p^{2r}/4 \in \mathbb{Z}_p$, while $N_{V,1}^{(m)} = s+m+\mathrm{ord}_p(d)$ and $N_{V,2}^{(m)} = s+m$; consequently for each choice $j \in \{1,2\}$, the matrix $p^{N_{V,j}^{(m)}}\Big((I_2+M)^{p^m}-I_2\Big)^{-1}$ equals

$$\frac{p^{N_{V,j}^{(m)}}}{2}\begin{pmatrix} \frac{1}{\lambda_{V,+}^{p^m}-1}+\frac{1}{\lambda_{V,-}^{p^m}-1}-\frac{p^r}{2\sqrt{\Delta_V}}\left(\frac{1}{\lambda_{V,+}^{p^m}-1}-\frac{1}{\lambda_{V,-}^{p^m}-1}\right) & \frac{1}{\sqrt{\Delta_V}}\left(\frac{1}{\lambda_{V,+}^{p^m}-1}-\frac{1}{\lambda_{V,-}^{p^m}-1}\right) \\ \frac{d}{\sqrt{\Delta_V}}\left(\frac{1}{\lambda_{V,+}^{p^m}-1}-\frac{1}{\lambda_{V,-}^{p^m}-1}\right) & \frac{1}{\lambda_{V,+}^{p^m}-1}+\frac{1}{\lambda_{V,-}^{p^m}-1}+\frac{p^r}{2\sqrt{\Delta_V}}\left(\frac{1}{\lambda_{V,+}^{p^m}-1}-\frac{1}{\lambda_{V,-}^{p^m}-1}\right) \end{pmatrix}.$$

Case (VI). Assume that $n \geq s+m+r+\mathrm{ord}_p(t)$. Then one has $P_{VI} = \begin{pmatrix} 1 & 1 \\ \sqrt{p^r t} & -\sqrt{p^r t} \end{pmatrix}$, while $N_{VI,1}^{(m)} = s+m+r+\mathrm{ord}_p(t)$ and $N_{VI,2}^{(m)} = s+m$; consequently, for each $j \in \{1,2\}$ the matrix $p^{N_{VI,j}^{(m)}}\Big((I_2+M)^{p^m}-I_2\Big)^{-1}$ equals

$$\frac{p^{N_{VI,j}^{(m)}}}{2}\begin{pmatrix} \frac{1}{\lambda_{VI,+}^{p^m}-1}+\frac{1}{\lambda_{VI,-}^{p^m}-1} & \frac{1}{\sqrt{p^r t}}\left(\frac{1}{\lambda_{VI,+}^{p^m}-1}-\frac{1}{\lambda_{VI,-}^{p^m}-1}\right) \\ \sqrt{p^r t}\left(\frac{1}{\lambda_{VI,+}^{p^m}-1}-\frac{1}{\lambda_{VI,-}^{p^m}-1}\right) & \frac{1}{\lambda_{VI,+}^{p^m}-1}+\frac{1}{\lambda_{VI,-}^{p^m}-1} \end{pmatrix}.$$

Since we know the form of each $\mathcal{T}_{\star,m,j}$, one now computes $\tilde{\chi}_{1,N_{\star,1}^{(m)}}\begin{pmatrix} x \\ y \end{pmatrix}$ and $\tilde{\chi}_{2,N_{\star,2}^{(m)}}\begin{pmatrix} x \\ y \end{pmatrix}$. To illustrate the calculation, suppose we are in the last case $\star =$VI; then one obtains

$$\begin{aligned} \tilde{\chi}_{1,N_{VI,1}^{(m)}}\begin{pmatrix} x \\ y \end{pmatrix} &= \chi_{1,N_{VI,1}^{(m)}}\left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\mathcal{T}_{VI,m,1}\begin{pmatrix} x \\ y \end{pmatrix}\right) \\ &= \chi_{1,s+m+r+\mathrm{ord}_p(t)}\left(\begin{pmatrix} \frac{p^{s+m+r+\mathrm{ord}_p(t)}}{2}\left(\frac{x+\frac{y}{\sqrt{p^r t}}}{\lambda_{VI,+}^{p^m}-1}+\frac{x-\frac{y}{\sqrt{p^r t}}}{\lambda_{VI,-}^{p^m}-1}\right) \\ 0 \end{pmatrix}\right) \\ &= \chi_{1,s+m+r+\mathrm{ord}_p(t)}\left(\begin{pmatrix} \frac{p^{s+m}}{2}\left(\frac{p^{r+\mathrm{ord}_p(t)}}{\lambda_{VI,+}^{p^m}-1}+\frac{p^{r+\mathrm{ord}_p(t)}}{\lambda_{VI,-}^{p^m}-1}\right)x \\ 0 \end{pmatrix}\right) \\ &\quad \cdot \chi_{2,s+m+r+\mathrm{ord}_p(t)}\left(\begin{pmatrix} 0 \\ \frac{p^{s+m}}{2\sqrt{p^r t}}\left(\frac{p^{r+\mathrm{ord}_p(t)}}{\lambda_{VI,+}^{p^m}-1}-\frac{p^{r+\mathrm{ord}_p(t)}}{\lambda_{VI,-}^{p^m}-1}\right)y \end{pmatrix}\right) \end{aligned}$$

which equals $\chi_{1,s+m+r+\mathrm{ord}_p(t)}^{\mathbf{e}_{VI,1}^{[1,m]}}\begin{pmatrix}x\\y\end{pmatrix}\cdot\chi_{2,s+m+r+\mathrm{ord}_p(t)}^{\mathbf{e}_{VI,2}^{[1,m]}}\begin{pmatrix}x\\y\end{pmatrix}$. Likewise, one can show that

$$\begin{aligned}\tilde{\chi}_{2,N_{VI,2}^{(m)}}\begin{pmatrix}x\\y\end{pmatrix} &= \chi_{2,s+m}\left(\begin{pmatrix}0&0\\0&1\end{pmatrix}\mathcal{T}_{VI,m,2}\begin{pmatrix}x\\y\end{pmatrix}\right)\\ &= \chi_{1,s+m}\left(\begin{pmatrix}\frac{p^{s+m}\sqrt{p^r t}}{2}\left(\frac{1}{\lambda_{VI,+}^{p^m}-1}-\frac{1}{\lambda_{VI,-}^{p^m}-1}\right)x\\0\end{pmatrix}\right)\\ &\quad\cdot\chi_{2,s+m}\left(\begin{pmatrix}0\\\frac{p^{s+m}}{2}\left(\frac{1}{\lambda_{VI,+}^{p^m}-1}+\frac{1}{\lambda_{VI,-}^{p^m}-1}\right)y\end{pmatrix}\right) \;=\; \chi_{1,s+m}^{\mathbf{e}_{VI,1}^{[2,m]}}\begin{pmatrix}x\\y\end{pmatrix}\cdot\chi_{2,s+m}^{\mathbf{e}_{VI,2}^{[2,m]}}\begin{pmatrix}x\\y\end{pmatrix}.\end{aligned}$$

The other remaining cases $\star=$III, $\star=$IV and $\star=$V follow in an analogous fashion. □

For Step 2, we introduce an equivalence relation ‘ $\sim$ ’ on ordered pairs of integers (a,b).

Definition 7.2 *(i) If $\star\in\{III,IV,V,VI\}$, then one sets*

$$\mathfrak{X}_{m,n} := \left\{(a,b)\in\left(\frac{\mathbb{Z}}{p^{N_{\star,1}^{(m)}}\mathbb{Z}}\times\frac{\mathbb{Z}}{p^{N_{\star,2}^{(m)}}\mathbb{Z}}\right)-p\cdot\left(\frac{\mathbb{Z}}{p^{N_{\star,1}^{(m)}}\mathbb{Z}}\times\frac{\mathbb{Z}}{p^{N_{\star,2}^{(m)}}\mathbb{Z}}\right)\right\}\Big/\sim$$

where $(a,b)\sim(a',b')$, if and only if

$$\begin{pmatrix}a&0\\0&b\end{pmatrix}\equiv\begin{pmatrix}a'&0\\0&b'\end{pmatrix}\left(I_2+M\right)^j \mod \left(\left(I_2+M\right)^{p^m}-I_2\right) \quad \textit{for some } j\in\mathbb{Z}/p^m\mathbb{Z}.$$

(ii) If $\star=II$, then one sets

$$\mathfrak{X}_{m,n} := \left\{(a,b)\in\frac{\mathbb{Z}}{p^n\mathbb{Z}}\times\left(\frac{\mathbb{Z}}{p^{s+m}\mathbb{Z}}\right)^{\times}\right\}\Big/\sim$$

where $(a,b)\sim(a',b')$ if and only if $a\equiv a'\ (\bmod p^{n-m})$.

The following result describes how to produce an explicit set of representatives for $\mathfrak{R}_{m,n}$. Again we assume that the integer $n\gg 0$ is chosen sufficiently large with respect to m.

Lemma 7.2 *(a) Up to isomorphism, the exact number of irreducible $\mathcal{G}_{\infty,n}$-representations $\rho_\chi = \mathrm{Ind}^{\mathcal{G}_{\infty,n}}_{\mathrm{Stab}_\Gamma(\chi)\ltimes\overline{\mathcal{H}}^{(m,n)}_\infty}(\chi)$ induced from primitive characters $\chi : \overline{\mathcal{H}}^{(m,n)}_\infty \to \mathbb{C}^\times$ equals*

$$\#\mathfrak{R}_{m,n} - \#\mathfrak{R}_{m-1,n} = \begin{cases} p^{n+s-1}\times(p-1) & \textit{in Case (II)} \\ p^{2s+m-2}\times(p^2-1) & \textit{in Cases (III) and (IV)} \\ p^{2s+m+\mathrm{ord}_p(d)-2}\times(p^2-1) & \textit{in Case (V)} \\ p^{2s+m+r+\mathrm{ord}_p(t)-2}\times(p^2-1) & \textit{in Case (VI).} \end{cases}$$

(b) If we define $\mathfrak{R}^{\mathrm{prim}}_{m,n} := \mathfrak{R}_{m,n} - \mathfrak{R}_{m-1,n}$ for every $m \in \{1,\dots,n-s\}$, then we can take as representatives for $\mathfrak{R}^{\mathrm{prim}}_{m,n}$ the set $\left\{\tilde{\chi}^a_{1,N^{(m)}_{\star,1}} \cdot \tilde{\chi}^b_{2,N^{(m)}_{\star,2}} \;\middle|\; (a,b) \in \mathfrak{X}_{m,n}\right\}$.

Proof. Part (a) follows (with $n \gg m$) on combining Proposition 4.5(iii) and Corollary 4.6. To show (b), first suppose that $\star \neq$ II. Then $\tilde{\chi}^a_{1,N^{(m)}_{\star,1}} \cdot \tilde{\chi}^b_{2,N^{(m)}_{\star,2}} = \gamma^j * \left(\tilde{\chi}^{a'}_{1,N^{(m)}_{\star,1}} \cdot \tilde{\chi}^{b'}_{2,N^{(m)}_{\star,2}}\right)$ if and only if $\tilde{\chi}_{1,N^{(m)}_{\star,1}}\begin{pmatrix} ax \\ ay \end{pmatrix} \cdot \tilde{\chi}_{2,N^{(m)}_{\star,2}}\begin{pmatrix} bx \\ by \end{pmatrix}$ equals

$$\tilde{\chi}_{1,N^{(m)}_{\star,1}}\left((I_2+M)^j\begin{pmatrix} a'x \\ a'y \end{pmatrix}\right)\cdot\tilde{\chi}_{2,N^{(m)}_{\star,2}}\left((I_2+M)^j\begin{pmatrix} b'x \\ b'y \end{pmatrix}\right) \quad \text{for all } x,y \in \mathbb{Z}_p.$$

This latter equality is equivalent to the pair of congruences

$$\begin{pmatrix} p^{N^{(m)}_{\star,1}} & 0 \\ 0 & 0 \end{pmatrix}\left((I_2+M)^{p^m}-I_2\right)^{-1}\begin{pmatrix} ax \\ ay \end{pmatrix}$$
$$\equiv \begin{pmatrix} p^{N^{(m)}_{\star,1}} & 0 \\ 0 & 0 \end{pmatrix}\left((I_2+M)^{p^m}-I_2\right)^{-1}(I_2+M)^j\begin{pmatrix} a'x \\ a'y \end{pmatrix} \mod p^{N^{(m)}_{\star,1}}$$

and

$$\begin{pmatrix} 0 & 0 \\ 0 & p^{N^{(m)}_{\star,2}} \end{pmatrix}\left((I_2+M)^{p^m}-I_2\right)^{-1}\begin{pmatrix} bx \\ by \end{pmatrix}$$
$$\equiv \begin{pmatrix} 0 & 0 \\ 0 & p^{N^{(m)}_{\star,2}} \end{pmatrix}\left((I_2+M)^{p^m}-I_2\right)^{-1}(I_2+M)^j\begin{pmatrix} b'x \\ b'y \end{pmatrix} \mod p^{N^{(m)}_{\star,2}}$$

holding for all $x,y \in \mathbb{Z}_p$; here we have exploited the construction of $\tilde{\chi}_{1,N^{(m)}_{\star,1}}$ and $\tilde{\chi}_{2,N^{(m)}_{\star,2}}$ given in Definition 5.1. Because $\left(I_2+M\right)^{p^m}-I_2$ and $(I_2+M)^j$

commute with each other, the above may be rewritten as a single congruence

$$\begin{aligned}&\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\Big((I_2+M)^{p^m}-I_2\Big)^{-1}\\ &\equiv \begin{pmatrix} a' & 0 \\ 0 & b' \end{pmatrix}(I_2+M)^j\Big((I_2+M)^{p^m}-I_2\Big)^{-1} \quad \bmod \ \mathrm{Mat}_{2\times 2}\big(\mathbb{Z}_p\big).\end{aligned}$$

Note this congruence is satisfied for some $j \in \mathbb{Z}/p^m\mathbb{Z}$ precisely when $(a,b) \sim (a',b')$.

Let us instead suppose that $\star = \text{II}$. Then $\tilde{\chi}^{a}_{1,N^{(m)}_{\star,1}} \cdot \tilde{\chi}^{b}_{2,N^{(m)}_{\star,2}} = \gamma^j * \Big(\tilde{\chi}^{a'}_{1,N^{(m)}_{\star,1}} \cdot \tilde{\chi}^{b'}_{2,N^{(m)}_{\star,2}}\Big)$ if and only if

$$\tilde{\chi}_{1,N^{(m)}_{\star,1}}\begin{pmatrix} ax \\ ay \end{pmatrix}\cdot\tilde{\chi}_{2,N^{(m)}_{\star,2}}\begin{pmatrix} bx \\ by \end{pmatrix} = \tilde{\chi}_{1,N^{(m)}_{\star,1}}\begin{pmatrix} a'(x+p^sjy) \\ a'y \end{pmatrix}\cdot\tilde{\chi}_{2,N^{(m)}_{\star,2}}\begin{pmatrix} b'(x+p^sjy) \\ b'y \end{pmatrix}$$

at every $x, y \in \mathbb{Z}_p$. Again using Definition 5.1, we can rewrite this as

$$\zeta_{p^n}^{ay}\cdot\zeta_{p^{s+m}}^{bx} \ = \ \zeta_{p^n}^{a'y}\cdot\zeta_{p^{s+m}}^{b'(x+p^sjy)} \quad \text{for each } x,y\in\mathbb{Z}_p,$$

which is itself equivalent to the congruences

$$b\equiv b' \pmod{p^{s+m}} \qquad \text{and} \qquad a\equiv a'+jp^{n-m}b' \pmod{p^n} \ \text{ for some } j\in\mathbb{Z}/p^m\mathbb{Z}.$$

These last two congruences then reduce to $b \equiv b' \pmod{p^{s+m}}$ and $a \equiv a' \pmod{p^{n-m}}$.

Therefore in all possible cases $\star \in \{\text{II,III,IV,V,VI}\}$, one concludes that $\tilde{\chi}^{a}_{1,N^{(m)}_{\star,1}} \cdot \tilde{\chi}^{b}_{2,N^{(m)}_{\star,2}}$ and $\tilde{\chi}^{a'}_{1,N^{(m)}_{\star,1}} \cdot \tilde{\chi}^{b'}_{2,N^{(m)}_{\star,2}}$ lie in the same Γ-orbit if and only if $(a,b)\sim(a',b')$. □

Consequently Steps 1 and 2 have now been resolved, and it therefore only remains to complete Step 3. The latter task is covered by the next result, which enables us to compute both the size of ϖ and also the exponent $\mathbf{e}^*_{\chi,\varpi}$ occurring in Theorems 3.1 and 3.2, for each orbit ϖ and representative character $\chi \in \mathfrak{R}_{m,n}$.

Lemma 7.3 *(i) If $\varpi \in \mathrm{orb}_\Gamma\big(\overline{\mathcal{H}}_\infty^{(m,n)}\big)$ contains an element $\overline{h} = \overline{h}_1^x \overline{h}_2^y$, then*

$$\varpi \;=\; \left\{ \overline{h}_1^a \overline{h}_2^b \quad \textit{such that} \begin{pmatrix} a \\ b \end{pmatrix} \in \mathcal{Y}_{(x,y)} \mod \Big(\big(I_2+M\big)^{p^m} - I_2\Big)\begin{pmatrix} \mathbb{Z}_p \\ \mathbb{Z}_p \end{pmatrix} + \begin{pmatrix} p^n\mathbb{Z}_p \\ p^n\mathbb{Z}_p \end{pmatrix} \right\}$$

where the set $\mathcal{Y}_{(x,y)}$ consists of the vectors $\left\{ \big(I_2+M\big)^j \begin{pmatrix} x \\ y \end{pmatrix} \textit{ with } j = 0,1,\dots,p^m-1 \right\}$.

(ii) For each character $\chi = \tilde{\chi}^a_{1,N^{(m)}_{\star,1}} \cdot \tilde{\chi}^b_{2,N^{(m)}_{\star,2}}$ on $\overline{\mathcal{H}}_\infty^{(m,n)}$, the number $\mathbf{e}^*_{\chi,\varpi} = \mathrm{Tr}\big(\mathrm{Ind}\chi^*\big)(\varpi)$ can be computed via the exponential sum formula

$$p^{\mathbf{m}_\chi - m} \cdot \sum_{j=0}^{p^m-1} \exp\left(-2\pi\sqrt{-1}\left(\left(\frac{a\mathbf{e}^{[1,m]}_{\star,1}}{p^{N^{(m)}_{\star,1}}} + \frac{b\mathbf{e}^{[2,m]}_{\star,1}}{p^{N^{(m)}_{\star,2}}}\right)x_j + \left(\frac{a\mathbf{e}^{[1,m]}_{\star,2}}{p^{N^{(m)}_{\star,1}}} + \frac{b\mathbf{e}^{[2,m]}_{\star,2}}{p^{N^{(m)}_{\star,2}}}\right)y_j\right)\right)$$

where the integer $\mathbf{m}_\chi$ is given in Proposition 4.2, and $\begin{pmatrix} x_j \\ y_j \end{pmatrix} := \big(I_2+M\big)^j \begin{pmatrix} x \\ y \end{pmatrix}$ *for all j.*

(iii) In particular, if ϖ consists of just the identity element, then $\mathbf{e}^*_{\chi,\varpi} = p^{\mathbf{m}_\chi} \in \mathbb{N}$.

Proof. To establish assertion (i), we remark that γ acts on the quotient group

$$\overline{\mathcal{H}}_\infty^{(m,n)} \;=\; \frac{\mathcal{H}_\infty/\mathcal{H}_\infty^{p^n}}{\Big\langle \big[h_1^x h_2^y \mod \mathcal{H}_\infty^{p^n},\ \gamma^{p^m}\big] \;\Big|\; x,y \in \mathbb{Z}_p \Big\rangle} \;\cong\; \frac{\mathbb{Z}}{p^{N^{(m)}_{\star,1}}\mathbb{Z}} \times \frac{\mathbb{Z}}{p^{N^{(m)}_{\star,2}}\mathbb{Z}}$$

through the matrix $I_2 + M$, hence our description for the Γ-orbit follows immediately.

To show part (ii), by the definition of $\mathrm{Tr}\big(\mathrm{Ind}\chi^*\big)(\varpi)$ one calculates that

$$\begin{aligned}
\mathbf{e}^*_{\chi,\varpi} \;&=\; \frac{\#(\Gamma * \chi)}{p^m}\cdot\sum_{j=0}^{p^m-1}\chi^{-1}\left(\gamma^{-j}\overline{h}\gamma^j\right) \;=\; \frac{[\Gamma:\mathrm{Stab}_\Gamma(\chi)]}{[\Gamma:\Gamma^{p^m}]}\cdot\sum_{j=0}^{p^m-1}\chi^{-1}\left(\overline{h}_1^{x_j}\overline{h}_2^{y_j}\right)\\
&\overset{\text{by } 4.2}{=}\; p^{\mathbf{m}_\chi-m}\cdot\sum_{j=0}^{p^m-1}\tilde{\chi}_{1,N^{(m)}_{\star,1}}\left(\overline{h}_1^{x_j}\overline{h}_2^{y_j}\right)^{-a}\times\tilde{\chi}_{2,N^{(m)}_{\star,2}}\left(\overline{h}_1^{x_j}\overline{h}_2^{y_j}\right)^{-b}\\
&\overset{\text{by } 7.1}{=}\; p^{\mathbf{m}_\chi-m}\cdot\sum_{j=0}^{p^m-1}\chi_{1,N^{(m)}_{\star,1}}^{\mathbf{e}^{[1,m]}_{\star,1}}\cdot\chi_{2,N^{(m)}_{\star,1}}^{\mathbf{e}^{[1,m]}_{\star,2}}\left(\overline{h}_1^{x_j}\overline{h}_2^{y_j}\right)^{-a}\times\chi_{1,N^{(m)}_{\star,2}}^{\mathbf{e}^{[2,m]}_{\star,1}}\cdot\chi_{2,N^{(m)}_{\star,2}}^{\mathbf{e}^{[2,m]}_{\star,2}}\left(\overline{h}_1^{x_j}\overline{h}_2^{y_j}\right)^{-b}\\
&=\; p^{\mathbf{m}_\chi-m}\cdot\sum_{j=0}^{p^m-1}\chi_{1,N^{(m)}_{\star,1}}^{-a\mathbf{e}^{[1,m]}_{\star,1}}\cdot\chi_{1,N^{(m)}_{\star,2}}^{-b\mathbf{e}^{[2,m]}_{\star,1}}\left(\overline{h}_1^{x_j}\overline{h}_2^{y_j}\right)\times\chi_{2,N^{(m)}_{\star,1}}^{-a\mathbf{e}^{[1,m]}_{\star,2}}\cdot\chi_{2,N^{(m)}_{\star,2}}^{-b\mathbf{e}^{[2,m]}_{\star,2}}\left(\overline{h}_1^{x_j}\overline{h}_2^{y_j}\right)
\end{aligned}$$

and the last line is then equivalent to the stated formula.

Finally (iii) is a special case of (ii), corresponding to $x = y = 0$ and $x_j = y_j = 0$. □

7.1 A worked example for Case (II)

We end by using Steps 1–3 to yield an explicit expression for the congruences in Case (II). Firstly by Lemma 7.2(b) and Definition 7.2(ii), if one takes $m \geq 1$ then

$$\mathfrak{R}^{\mathrm{prim}}_{m,n} \;=\; \left\{\chi_{2,n}^a\cdot\chi_{1,s+m}^b\;\middle|\; a\in\mathbb{Z}/p^{n-m}\mathbb{Z}\ \text{ and }\ b\in\left(\mathbb{Z}/p^{s+m}\mathbb{Z}\right)^\times\right\}$$

while $\mathfrak{R}_{0,n}$ coincides with $\left\{\chi_{2,n}^a\cdot\chi_{1,s}^b\;\middle|\; a\in\mathbb{Z}/p^n\mathbb{Z}\ \text{ and }\ b\in\mathbb{Z}/p^s\mathbb{Z}\right\}$. It follows that

$$\prod_{\chi\in\mathfrak{R}_{m,n}}\mathcal{N}_{\mathrm{Stab}_\Gamma(\chi)/\Gamma^{p^m}}\left(\cdots\right)^{\mathbf{e}^*_{\chi,\varpi}} \;=\; \prod_{m'=0}^{m}\;\prod_{a=1}^{p^{n-m'}}\;\prod_{\substack{b\,=\,1,\\ p\,\nmid\, b \text{ if } m'\,>\,0}}^{p^{s+m'}}\mathcal{N}_{\mathbf{m}_\chi,m}\left(\cdots\right)^{\mathbf{e}^*_{\chi,\varpi}}\Bigg|_{\chi=\chi_{2,n}^a\cdot\chi_{1,s+m'}^b}.$$

Now suppose an orbit $\varpi_{\overline{h}}\in\mathrm{orb}_\Gamma\big(\overline{\mathcal{H}}_\infty^{(m,n)}\big)$ contains an element $\overline{h}=\overline{h}_1^x\overline{h}_2^y$. Then

$$\varpi_{\overline{h}} \;=\; \left\{\gamma^{-j}\overline{h}\gamma^j\;\middle|\; j\in\mathbb{Z}\right\} \;=\; \left\{\overline{h}_1^{x+jp^sy}\overline{h}_2^{y}\;\middle|\; j\in\mathbb{Z}\right\} \;=\; \overline{h}\cdot\left\{\overline{h}_1^{jp^sy}\;\middle|\; j=1,\cdots,p^{m-\mathrm{ord}_p(y)}\right\}$$

in which case $\#\varpi_{\overline{h}}=p^{m-\mathrm{ord}_p(\tilde{y})}$, with $\tilde{y}\in\{1,\ldots,p^m\}$ chosen so that $\tilde{y}\equiv y$ (mod p^m).

Finally, if we consider a typical character $\chi = \chi_{2,n}^{a} \cdot \chi_{1,s+m'}^{b} = \chi_{2,n}^{a} \cdot \chi_{1,s+m}^{p^{m-m'}b}$ and the orbit $\varpi = \varpi_{\overline{h}}$ as above, then Lemma 7.3(ii) implies

$$\begin{aligned}
\mathbf{e}^{*}_{\chi,\varpi_{\overline{h}}} &= p^{\mathbf{m}_\chi - m} \cdot \sum_{j=0}^{p^m-1} \exp\left(-2\pi\sqrt{-1}\left(\left(\frac{p^{m-m'}b}{p^{s+m}}\right)(x + jp^s y) + \left(\frac{a}{p^n}\right) y\right)\right) \\
&= p^{\mathbf{m}_\chi - m} \cdot \exp\left(-2\pi\sqrt{-1}\left(\frac{bx}{p^{s+m'}} + \frac{ay}{p^n}\right)\right) \times \sum_{j=0}^{p^m-1} \exp\left(-2\pi\sqrt{-1}\left(\frac{bjy}{p^{m'}}\right)\right) \\
&= p^{\mathbf{m}_\chi - m} \cdot \exp\left(-2\pi\sqrt{-1}\left(\frac{bx}{p^{s+m'}} + \frac{ay}{p^n}\right)\right) \times \begin{cases} p^m & \text{if } p^{m'} \mid by \\ 0 & \text{if } p^{m'} \nmid by. \end{cases}
\end{aligned}$$

However the exponential term $\exp\left(-2\pi\sqrt{-1}\left(\frac{bx}{p^{s+m'}} + \frac{ay}{p^n}\right)\right)$ is then just equal to $\chi^{-1}(\overline{h})$. Because $\chi = \chi_{2,n}^{a} \cdot \chi_{1,s+m'}^{b}$ can be written as $\chi_{1,n}^{\mathbf{e}_1} \cdot \chi_{2,n}^{\mathbf{e}_2}$ with $\mathbf{e}_1 = p^{n-s-m'}b$ and $\mathbf{e}_2 = a$, one calculates via Proposition 4.2 that $\mathbf{m}_\chi = \max\{0, \tilde{\mathbf{m}}_\chi\}$ where

$$\tilde{\mathbf{m}}_\chi \overset{\text{by } 4.2}{=} n - s - \mathrm{ord}_p\big(p^{n-s-m'}b\big) \;=\; m' - \mathrm{ord}_p(b).$$

Consequently, if $\chi = \chi_{2,n}^{a} \cdot \chi_{1,s+m'}^{b}$ then $\mathbf{e}^{*}_{\chi,\varpi_{\overline{h}}} = \begin{cases} \chi^{-1}(\overline{h}) \cdot p^{\max\{0, m' - \mathrm{ord}_p(b)\}} & \text{if } p^{m'} \mid by \\ 0 & \text{if } p^{m'} \nmid by. \end{cases}$

Corollary 7.4 *The congruences described in Equation (6.7) are equivalent to*

$$\prod_{m'=0}^{m} \prod_{a=1}^{p^{n-m'}} \prod_{\substack{b=1, \\ p \nmid b \text{ if } m'>0}}^{p^{s+m'}} \mathcal{N}_{\mathbf{m}_\chi, m}\left(\frac{\mathbf{y}_\chi}{\varphi(\mathbf{y}_{\chi^p})} \cdot \frac{\varphi\big(\mathcal{N}_{0,\mathbf{m}_\chi - 1}(\mathbf{y_1})\big)}{\mathcal{N}_{0,\mathbf{m}_\chi}(\mathbf{y_1})}\right)^{\mathbf{e}^{*}_{\chi,\varpi_{\overline{h}}}} \Bigg|_{\chi = \chi_{2,n}^{a} \cdot \chi_{1,s+m'}^{b}}$$

$$\equiv\; 1 \mod p^{s+m+n+\mathrm{ord}_p(\tilde{y})} \cdot \mathbb{Z}_p\big[\big[\Gamma^{p^m}\big]\big]_{(p)}$$

for all integer pairs $m, n \geq 0$ with $m \leq n - s$, and at every choice of $\overline{h} = \overline{h}_1^{\tilde{x}} \overline{h}_2^{\tilde{y}} \in \overline{\mathcal{H}}_\infty^{(m,n)}$ with $\tilde{x} \in \{1, \ldots, p^n\}$ and $\tilde{y} \in \{1, \ldots, p^m\}$.

This completes the proof of Theorem 3.1, in the precise form stated in the Chapter 3.

7.2 A worked example for Case (III)

We now turn our attention to the situation where the Γ-action is scalar, and relate our congruences to those derived by Delbourgo and Peters in [DP15].

Proposition 7.5 *If we are in Case (III), then*

1. *A set of representative primitive characters is given by*

$$\mathfrak{R}^{\mathrm{prim}}_{m,n} \;=\; \left\{ \chi^{a}_{1,s+m}\chi^{b}_{2,s+m} \;\middle|\; (a,b) \in \mathfrak{X}_{m.n} \right\}$$

   where $\mathfrak{X}_{m,n} \;:=\; \mathfrak{X}^{+}_{m,n} \cup \mathfrak{X}^{-}_{m,n}$ *with*

$$\mathfrak{X}^{+}_{m,n} = \left(\frac{\mathbb{Z}}{p^s\mathbb{Z}}\right)^{\times} \times \frac{\mathbb{Z}}{p^{s+m}\mathbb{Z}}$$

   and

$$\mathfrak{X}^{-}_{m,n} = \frac{p\mathbb{Z}}{p^{s+m}\mathbb{Z}} \times \left(\frac{\mathbb{Z}}{p^s\mathbb{Z}}\right)^{\times}.$$

2. *For an orbit* $\varpi_{\overline{h}} \in \mathrm{orb}_{\Gamma}\big(\overline{\mathcal{H}}^{(m,n)}_{\infty}\big)$ *containing an element* $\overline{h} = \overline{h}_1^{x}\overline{h}_2^{y}$*, we have* $\#\varpi_{\overline{h}} = p^{m - min\{ord_p(\tilde{x}), ord_p(\tilde{y})\}}$*, with* $\tilde{x}, \tilde{y} \in \{1, \ldots, p^m\}$ *chosen so that* $\tilde{x} \equiv x \pmod{p^m}$ *and* $\tilde{y} \equiv y \pmod{p^m}$*.*

3. *For a typical character* $\chi = \chi^{a}_{1,s+m}\chi^{b}_{2,s+m}$*,*

$$\mathbf{e}^{*}_{\chi,\varpi_{\overline{h}}} = \begin{cases} \chi^{-1}(\overline{h}) \cdot p^{\max\{0,n-s\}} & \text{if } m \leq ord_p(ax+by) \\ 0 & \text{otherwise.} \end{cases}$$

Proof. First of all, the set of representatives $\mathfrak{R}^{\mathrm{prim}}_{m,n}$ is abstractly described in Proposition 7.1, but it is not trivial to determine $\mathfrak{X}_{m,n}$. From Definition 7.2, we know that the equivalence relation $(a,b) \sim (a',b')$ holds if and only if $a \equiv a' \times (1+p^s)^j \pmod{p^{s+m}}$ and $b \equiv b' \times (1+p^s)^j \pmod{p^{s+m}}$ for some $j \in \frac{\mathbb{Z}}{p^m\mathbb{Z}}$.

In order to describe the set $\mathfrak{X}_{m,n}$ completely, we shall separate it into two cases. In the first case, where $p \nmid a$, it follows that $\frac{a}{a'} \equiv (1+p^s)^j \pmod{p^{s+m}}$. At the same time, because of the fact that $p^s \mid (1+p^s)^j - 1$, we deduce that $\frac{a}{a'} \in 1 + \frac{p^s\mathbb{Z}}{p^{s+m}\mathbb{Z}}$. This means one may take $a \in \{1, 2, \cdots, p^s\} \cap \mathbb{Z}_p^{\times}$ and $b \in \frac{\mathbb{Z}}{p^{s+m}\mathbb{Z}}$.

Similarly, in the second case for $p \nmid b$, we may choose $b \in \{1, 2, \cdots, p^s\} \cap \mathbb{Z}_p^\times$. (Note as a part of the previous case, the sub-case that $p \nmid a$ and $p \nmid b$ has already been treated, which leaves us only with the sub-case where $a \in \mathbb{Z}/p^{s+m}\mathbb{Z}$ is a multiple of p and $p \nmid b$.)

In general, we conclude that if $p \nmid a$, then one may take $a \in \left(\frac{\mathbb{Z}}{p^s\mathbb{Z}}\right)^\times$ and $b \in \frac{\mathbb{Z}}{p^{s+m}\mathbb{Z}}$. On the other hand, if $p \mid a$ and $p \nmid b$, then we may choose $a \in \frac{p\mathbb{Z}}{p^{s+m}\mathbb{Z}}$ and $b \in \left(\frac{\mathbb{Z}}{p^s\mathbb{Z}}\right)^\times$. This gives us the stated decomposition $\mathfrak{X}_{m,n} = \mathfrak{X}_{m,n}^+ \cup \mathfrak{X}_{m,n}^-$ as above and completes part (i).

Looking instead at part (ii), suppose that an orbit $\varpi_{\overline{h}} \in \mathrm{orb}_\Gamma\big(\overline{\mathcal{H}}_\infty^{(m,n)}\big)$ contains an element $\overline{h} = \overline{h}_1^x \overline{h}_2^y$. Then

$$\begin{aligned} \varpi_{\overline{h}} \;&=\; \{\gamma^{-j}\overline{h}\gamma^j \mid j \in \mathbb{Z}\} \;=\; \left\{\overline{h}^{(1+p^s)^j} \;\middle|\; j \in \mathbb{Z}\right\} \;=\; \overline{h} \cdot \left\{\overline{h}^{(1+p^s)^j - 1} \;\middle|\; j \in \mathbb{Z}\right\} \\ &=\; \overline{h} \cdot \left\{\overline{h}_1^{x((1+p^s)^j-1)} \overline{h}_2^{y((1+p^s)^j-1)} \;\middle|\; j \in \{1, 2, \cdots, \min\{\mathrm{ord}_p(\tilde{x}), \mathrm{ord}_p(\tilde{y})\}\}\right\}, \end{aligned}$$

in which case $\#\varpi_{\overline{h}} = p^{m - \min\{\mathrm{ord}_p(\tilde{x}), \mathrm{ord}_p(\tilde{y})\}}$ with $\tilde{x}, \tilde{y} \in \{1, \ldots, p^m\}$ chosen so that $\tilde{x} \equiv x \pmod{p^m}$ and $\tilde{y} \equiv y \pmod{p^m}$. (Note for example, if $\overline{h}$ is the identity then $\#\varpi_{\overline{h}} = 1$.)

Finally, let us put $u_{m'} = \frac{p^{s+m'}}{\lambda_{III,\pm}^{p^{m'}} - 1} \in \mathbb{Z}_p^\times$. If we consider a typical character $\chi = \tilde{\chi}_{1,s+m'}^a \tilde{\chi}_{2,s+m'}^b = \chi_{1,s+m}^{u_{m'}p^{m-m'}a} \chi_{2,s+m}^{u_{m'}p^{m-m'}b}$ and an orbit $\varpi = \varpi_{\overline{h}}$ as above, then Lemma 7.3(ii) implies

$$\begin{aligned} \mathbf{e}^*_{\chi, \varpi_{\overline{h}}} \;&=\; p^{\mathbf{m}_\chi - m} \cdot \sum_{j=0}^{p^m - 1} \exp\left(-2\pi\sqrt{-1}\left(\left(\frac{u_{m'}p^{m-m'}a}{p^{s+m}}\right) x_j + \left(\frac{u_{m'}p^{m-m'}b}{p^{s+m}}\right) y_j\right)\right) \\ &=\; p^{\mathbf{m}_\chi - m} \cdot \sum_{j=0}^{p^m - 1} \exp\left(-2\pi\sqrt{-1}\left(\left(\frac{u_{m'}p^{m-m'}a}{p^{s+m}}\right) \lambda_{III,\pm}^j x + \left(\frac{u_{m'}p^{m-m'}b}{p^{s+m}}\right) \lambda_{III,\pm}^j y\right)\right) \\ &=\; p^{\mathbf{m}_\chi - m} \cdot \sum_{j=0}^{p^m - 1} \exp\left(-\, 2\pi\sqrt{-1}\left(\frac{\lambda_{III,\pm}^j}{\lambda_{III,\pm}^{p^{m'}} - 1}(ax + by)\right)\right) \\ &=\; p^{\mathbf{m}_\chi - m} \cdot \chi^{-1}(\overline{h}) \times \sum_{j=0}^{p^m - 1} \exp\left(-\, 2\pi\sqrt{-1}\left(\frac{\lambda_{III,\pm}^j - 1}{\lambda_{III,\pm}^{p^{m'}} - 1}(ax + by)\right)\right). \end{aligned}$$

Since $\lambda_{III,\pm}^j - 1$ runs over the elements of $\frac{p^s\mathbb{Z}}{p^{s+m}\mathbb{Z}}$ and $p^{s+m'} \parallel \lambda_{III,\pm}^{p^{m'}} - 1$, we deduce that

$$\mathbf{e}^*_{\chi,\varpi_{\overline{h}}} \;=\; p^{\mathbf{m}_\chi - m} \cdot \chi^{-1}(\overline{h}) \times \begin{cases} p^m & \text{if } m' \leq \mathrm{ord}_p(ax+by) \\ 0 & \text{otherwise.} \end{cases}$$

Consequently, if $\chi = \chi_{1,s+m}^{au_m}\chi_{2,s+m}^{bu_m}$ then $\mathbf{m}_\chi = \max\{0, n-s\}$by Proposition 4.2, in which case

$$\mathbf{e}^*_{\chi,\varpi_{\overline{h}}} = \begin{cases} \chi^{-1}(\overline{h}) \cdot p^{\max\{0,n-s\}} & \text{if } m' \leq \mathrm{ord}_p(ax+by) \\ 0 & \text{otherwise.} \end{cases}$$

The same argument works fine if we replace χ by $\chi_{1,s+m'}^{a}\chi_{2,s+m'}^{b}$, since the map $\zeta \mapsto \zeta^{u_m}$ extends linearly to yield an element of $\mathrm{Gal}(\mathbb{Q}(\mu_{p^m})/\mathbb{Q})$.

□

Corollary 7.6 *The congruences described in Equation (3.2) are equivalent to*

$$\prod_{m'=0}^{m}\Bigg(\prod_{\substack{a\,=\,1,\\ p\,\nmid\, a}}^{p^s} \prod_{b=1}^{p^{s+m'}} \mathcal{N}_{\mathbf{m}_\chi,m}\left(\frac{\mathbf{y}_\chi}{\varphi\big(\mathbf{y}_{\chi^p}\big)} \cdot \frac{\varphi\big(\mathcal{N}_{0,\mathbf{m}_\chi-1}\big(\mathbf{y_1}\big)\big)}{\mathcal{N}_{0,\mathbf{m}_\chi}\big(\mathbf{y_1}\big)}\right)^{\mathbf{e}^*_{\chi,\varpi_{\overline{h}}}}\Bigg|_{\chi=\chi_{1,s+m'}^{a}\cdot\chi_{2,s+m'}^{b}}$$

$$\times \quad \prod_{\substack{a\,=\,1,\\ p\,\mid\, a}}^{p^{s+m'}} \prod_{\substack{b\,=\,1,\\ p\,\nmid\, b}}^{p^s} \mathcal{N}_{\mathbf{m}_\chi,m}\left(\frac{\mathbf{y}_\chi}{\varphi\big(\mathbf{y}_{\chi^p}\big)} \cdot \frac{\varphi\big(\mathcal{N}_{0,\mathbf{m}_\chi-1}\big(\mathbf{y_1}\big)\big)}{\mathcal{N}_{0,\mathbf{m}_\chi}\big(\mathbf{y_1}\big)}\right)^{\mathbf{e}^*_{\chi,\varpi_{\overline{h}}}}\Bigg|_{\chi=\chi_{1,s+m'}^{a}\cdot\chi_{2,s+m'}^{b}}\Bigg)$$

$$\equiv\; 1 \quad \mathrm{mod}\; p^{2s+2m+\min\{\mathrm{ord}_p(\tilde{x}),\mathrm{ord}_p(\tilde{y})\}} \cdot \mathbb{Z}_p\big[\big[\Gamma^{p^m}\big]\big]_{(p)}$$

for all integer pairs $m, n \geq 0$ with $m \leq n-s$, and at every choice of $\overline{h} = \overline{h}_1^{\tilde{x}}\overline{h}_2^{\tilde{y}} \in \overline{\mathcal{H}}_\infty^{(m,n)}$ with $\tilde{x}, \tilde{y} \in \{1, \ldots, p^m\}$.

7.2.1 Comparison with the Delbourgo-Peters congruences

Recall that for all integers $i \geq 1$, the twin mappings $\log : 1+p^i\cdot\mathbb{Z}_p[\Gamma^{p^m}/\Gamma^{p^\nu}] \overset{\sim}{\longrightarrow} p^i\cdot\mathbb{Z}_p[\Gamma^{p^m}/\Gamma^{p^\nu}]$ and $\exp : p^i\cdot\mathbb{Z}_p[\Gamma^{p^m}/\Gamma^{p^\nu}] \overset{\sim}{\longrightarrow} 1+p^i\cdot\mathbb{Z}_p[\Gamma^{p^m}/\Gamma^{p^\nu}]$ are inverse isomorphisms to each other. Note also that, for a character $\chi : \mathcal{H}_\infty \to \mu_{p^\nu}$, we have $a_{m,\chi}^{(\nu)} = \mathrm{Tr}_{\mathrm{Stab}_\Gamma(\chi)/\Gamma^{p^m}}\big(\mathrm{a}_\chi^{(\nu)}\big)$.

Now, as an example, let us further assume that $\mathbf{a}^{(\nu)}_{m,\chi} = \mathbf{a}^{(\nu)}_{m,\chi^u}$ for any $u \in \mathbb{Z}_p^\times$, which corresponds to the scenario considered in [DP15].

Then $\#\omega = 1$ if $\bar{h}$ is the identity, and $p^{\nu - s}$ otherwise for some $\nu \geq s+1$. Let $\tilde{\mathfrak{R}}_{m,\infty}$ denote a set of representatives for the orbits in $\mathrm{Hom}\big(\overline{\mathcal{H}}^{(m)}_\infty, \mathbb{C}^\times\big)$ under the natural action of $\mathbb{Z}_p^\times$. Taking the product over all characters in $\mathfrak{R}_{m,\infty}$,

$$\prod_{\chi \in \mathfrak{R}_{m,\infty}} \mathcal{N}_{\mathrm{Stab}_\Gamma(\chi)/\Gamma^{p^m}} \left(\frac{\mathbf{y}^{(\nu)}_\chi}{\varphi\big(\mathbf{y}^{(\nu)}_{\chi^p}\big)} \cdot \frac{\varphi\big(\mathcal{N}_{0,\mathbf{m}_\chi - 1}\big(\mathbf{y}^{(\nu)}_{\mathbf{1}}\big)\big)}{\mathcal{N}_{0,\mathbf{m}_\chi}\big(\mathbf{y}^{(\nu)}_{\mathbf{1}}\big)} \right)^{\mathrm{Tr}(\mathrm{Ind}\chi^*)(\varpi)}$$

$$= \exp \circ \log \left(\prod_{\chi \in \mathfrak{R}_{m,\infty}} \mathcal{N}_{\mathrm{Stab}_\Gamma(\chi)/\Gamma^{p^m}} \left(\frac{\mathbf{y}^{(\nu)}_\chi}{\varphi\big(\mathbf{y}^{(\nu)}_{\chi^p}\big)} \cdot \frac{\varphi\big(\mathcal{N}_{0,\mathbf{m}_\chi - 1}\big(\mathbf{y}^{(\nu)}_{\mathbf{1}}\big)\big)}{\mathcal{N}_{0,\mathbf{m}_\chi}\big(\mathbf{y}^{(\nu)}_{\mathbf{1}}\big)} \right)^{\mathrm{Tr}(\mathrm{Ind}\chi^*)(\varpi)} \right)$$

$$= \exp \left(\sum_{\chi \in \mathfrak{R}_{m,\infty}} \mathrm{Tr}(\mathrm{Ind}\chi^*)(\varpi) \times \mathrm{Tr}_{\mathrm{Stab}_\Gamma(\chi)/\Gamma^{p^m}} \circ \log \left(\frac{\mathbf{y}^{(\nu)}_\chi}{\varphi\big(\mathbf{y}^{(\nu)}_{\chi^p}\big)} \cdot \frac{\varphi\big(\mathcal{N}_{0,\mathbf{m}_\chi - 1}\big(\mathbf{y}^{(\nu)}_{\mathbf{1}}\big)\big)}{\mathcal{N}_{0,\mathbf{m}_\chi}\big(\mathbf{y}^{(\nu)}_{\mathbf{1}}\big)} \right) \right).$$

Recalling that

$$\mathrm{Tr}_{\mathrm{Stab}_\Gamma(\chi)/\Gamma^{p^m}}\big(\mathrm{a}^{(\nu)}_\chi\big) = \mathrm{Tr}_{\mathrm{Stab}_\Gamma(\chi)/\Gamma^{p^m}} \circ \log \left(\frac{\mathbf{y}^{(\nu)}_\chi}{\varphi\big(\mathbf{y}^{(\nu)}_{\chi^p}\big)} \cdot \frac{\varphi\big(\mathcal{N}_{0,\mathbf{m}_\chi - 1}\big(\mathbf{y}^{(\nu)}_{\mathbf{1}}\big)\big)}{\mathcal{N}_{0,\mathbf{m}_\chi}\big(\mathbf{y}^{(\nu)}_{\mathbf{1}}\big)} \right)$$

from Equation 6.6, it follows directly that,

$$\prod_{\chi \in \mathfrak{R}_{m,\infty}} \mathcal{N}_{\mathrm{Stab}_\Gamma(\chi)/\Gamma^{p^m}} \left(\frac{\mathbf{y}^{(\nu)}_\chi}{\varphi\big(\mathbf{y}^{(\nu)}_{\chi^p}\big)} \cdot \frac{\varphi\big(\mathcal{N}_{0,\mathbf{m}_\chi - 1}\big(\mathbf{y}^{(\nu)}_{\mathbf{1}}\big)\big)}{\mathcal{N}_{0,\mathbf{m}_\chi}\big(\mathbf{y}^{(\nu)}_{\mathbf{1}}\big)} \right)^{\mathrm{Tr}(\mathrm{Ind}\chi^*)(\varpi)}$$

$$= \exp \left(\sum_{\chi \in \mathfrak{R}_{m,\infty}} \mathrm{Tr}_{\mathrm{Stab}_\Gamma(\chi)/\Gamma^{p^m}}\big(\mathrm{a}^{(\nu)}_\chi\big) \cdot \mathrm{Tr}(\mathrm{Ind}\chi^*)(\varpi) \right) = \exp \left(\sum_{\chi \in \mathfrak{R}_{m,\infty}} \mathbf{a}^{(\nu)}_{m,\chi} \cdot \mathrm{Tr}(\mathrm{Ind}\chi^*)(\varpi) \right)$$

$$= \exp \left(\sum_{\chi \in \mathfrak{R}_{m,\infty}} \mathbf{a}^{(\nu)}_{m,\chi} \cdot \sum_{i=0}^{p^m - 1} \chi^{-1}(\bar{h})^{(1+p^s)^i} \right)$$

$$= \exp \left(\sum_{\chi \in \tilde{\mathfrak{R}}_{m,\infty}} \sum_{\substack{\chi' = \chi^u, \\ \text{with } u \in \frac{\mathbb{Z}_p^\times}{1+p^s\mathbb{Z}_p}}} \mathbf{a}^{(\nu)}_{m,\chi'} \cdot \sum_{i=0}^{p^m - 1} (\chi')^{-1}(\bar{h})^{(1+p^s)^i} \right)$$

$$= \exp \left(\sum_{\chi \in \tilde{\mathfrak{R}}_{m,\infty}} \mathbf{a}^{(\nu)}_{m,\chi} \times \sum_{u \in \frac{\mathbb{Z}_p^\times}{1+p^{s+\nu}\mathbb{Z}_p}} \chi^{-1}(\bar{h})^u \right)$$

upon exploiting the fact that $\mathbf{a}^{(\nu)}_{m,\chi} = \mathbf{a}^{(\nu)}_{m,\chi^u}$ if $u \in \mathbb{Z}_p^\times$. We may therefore conclude

$$\prod_{\chi\in\mathfrak{R}_{m,\infty}} \mathcal{N}_{\mathrm{Stab}_\Gamma(\chi)/\Gamma^{p^m}}\left(\frac{\mathbf{y}_\chi^{(\nu)}}{\varphi\big(\mathbf{y}_{\chi^p}^{(\nu)}\big)}\cdot\frac{\varphi\big(\mathcal{N}_{0,\mathbf{m}_\chi-1}\big(\mathbf{y}_{\mathbf{1}}^{(\nu)}\big)\big)}{\mathcal{N}_{0,\mathbf{m}_\chi}\big(\mathbf{y}_{\mathbf{1}}^{(\nu)}\big)}\right)^{\mathrm{Tr}(\mathrm{Ind}\chi^*)(\varpi)}$$
$$= \exp\left(\sum_{\chi\in\tilde{\mathfrak{R}}_{m,\infty}} \mathrm{Tr}_{\mathrm{Stab}_\Gamma(\chi)/\Gamma^{p^m}}\circ\log\left(\frac{\mathbf{y}_\chi^{(\nu)}}{\varphi\big(\mathbf{y}_{\chi^p}^{(\nu)}\big)}\cdot\frac{\varphi\big(\mathcal{N}_{0,\mathbf{m}_\chi-1}\big(\mathbf{y}_{\mathbf{1}}^{(\nu)}\big)\big)}{\mathcal{N}_{0,\mathbf{m}_\chi}\big(\mathbf{y}_{\mathbf{1}}^{(\nu)}\big)}\right)\times\sum_{u\in\frac{\mathbb{Z}_p^\times}{1+p^{s+\nu}\mathbb{Z}_p}}\chi^{-1}(\bar{h})^u\right)$$
$$= \prod_{\chi\in\tilde{\mathfrak{R}}_{m,\infty}} \mathcal{N}_{\mathrm{Stab}_\Gamma(\chi)/\Gamma^{p^m}}\left(\frac{\mathbf{y}_\chi^{(\nu)}}{\varphi\big(\mathbf{y}_{\chi^p}^{(\nu)}\big)}\cdot\frac{\varphi\big(\mathcal{N}_{0,\mathbf{m}_\chi-1}\big(\mathbf{y}_{\mathbf{1}}^{(\nu)}\big)\big)}{\mathcal{N}_{0,\mathbf{m}_\chi}\big(\mathbf{y}_{\mathbf{1}}^{(\nu)}\big)}\right)^{\sum_{u\in\frac{\mathbb{Z}_p^\times}{1+p^{s+\nu}\mathbb{Z}_p}}\chi^{-1}(\bar{h})^u}.$$

Lemma 7.7 *The summation term above is equal to*

$$\sum_{u\in\frac{\mathbb{Z}_p^\times}{1+p^{s+\nu}\mathbb{Z}_p}}\chi^{-1}(\bar{h})^u = \begin{cases}\phi(p^{\nu+s}) & \textit{if } \bar{h}\in\mathrm{Ker}(\chi),\\ -p^{s+\nu-1} & \textit{if } \bar{h}\notin\mathrm{Ker}(\chi) \textit{ but } \bar{h}^p\in\mathrm{Ker}(\chi),\\ 0 & \textit{otherwise.}\end{cases}$$

Proof. We begin by supposing that $\bar{h}\in\mathrm{Ker}(\chi)$, so that $\chi^{-1}(\bar{h})^u = 1$ for all $u\in\frac{\mathbb{Z}_p^\times}{1+p^{s+\nu}\mathbb{Z}_p}$. Here the sum equals the number of elements in $\frac{\mathbb{Z}_p^\times}{1+p^{s+\nu}\mathbb{Z}_p}$, which is exactly $\phi(p^{\nu+s}) = (p-1)p^{\nu+s-1}$.

We next consider the case where $\bar{h}\notin\mathrm{Ker}(\chi)$ but $\bar{h}^p\in\mathrm{Ker}(\chi)$, which means that $\chi^{-1}(\bar{h})\in\mu_p$ with $\chi^{-1}(\bar{h})\neq 1$. Since the group $\frac{\mathbb{Z}_p^\times}{1+p^{s+\nu}\mathbb{Z}_p}$ is isomorphic to $\mathbb{F}_p^\times\times\frac{1+p\mathbb{Z}_p^\times}{1+p^{s+\nu}\mathbb{Z}_p}$, consequently

$$\sum_{u\in\frac{\mathbb{Z}_p^\times}{1+p^{s+\nu}\mathbb{Z}_p}}\chi^{-1}(\bar{h})^u = \sum_{u\in\frac{\mathbb{Z}_p^\times}{1+p^{s+\nu}\mathbb{Z}_p}}(e^{\frac{2\pi i}{p}})^u = p^{s+\nu-1}\times\sum_{\xi\in\mu_p,\,\xi\neq 1}\xi$$
$$= p^{s+\nu-1}\times\Big(\sum_{\xi\in\mu_p}\xi - 1\Big) = p^{s+\nu-1}\cdot(0-1) = -p^{s+\nu-1}.$$

Lastly, if $\bar{h}^p\notin\mathrm{Ker}(\chi)$ then an easy exercise in cyclotomy shows that the sum is zero. □

Corollary 7.8 *Under the assumption that* $\mathbf{a}_{m,\chi}^{(\nu)} = \mathbf{a}_{m,\chi^u}^{(\nu)}$ *for all* $u \in \mathbb{Z}_p^\times$*, the congruences in Theorem 3.2 are equivalent to:*

- *if* $\bar{h} \neq id$*, one has*

$$\prod_{\substack{\chi \in \tilde{\mathfrak{R}}_{m,\infty}, \\ \bar{h} \in Ker(\chi)}} \mathcal{N}_{\mathrm{Stab}_\Gamma(\chi)/\Gamma^{p^m}} \left(\frac{\mathbf{y}_\chi^{(\nu)}}{\varphi\big(\mathbf{y}_{\chi^p}^{(\nu)}\big)} \cdot \frac{\varphi\big(\mathcal{N}_{0,\mathbf{m}_\chi - 1}\big(\mathbf{y}_{\mathbf{1}}^{(\nu)}\big)\big)}{\mathcal{N}_{0,\mathbf{m}_\chi}\big(\mathbf{y}_{\mathbf{1}}^{(\nu)}\big)} \right)^{p^{s+\nu}}$$

$$\equiv \prod_{\substack{\chi \in \tilde{\mathfrak{R}}_{m,\infty}, \\ \bar{h}^p \in Ker(\chi)^u}} \mathcal{N}_{\mathrm{Stab}_\Gamma(\chi)/\Gamma^{p^m}} \left(\frac{\mathbf{y}_\chi^{(\nu)}}{\varphi\big(\mathbf{y}_{\chi^p}^{(\nu)}\big)} \cdot \frac{\varphi\big(\mathcal{N}_{0,\mathbf{m}_\chi - 1}\big(\mathbf{y}_{\mathbf{1}}^{(\nu)}\big)\big)}{\mathcal{N}_{0,\mathbf{m}_\chi}\big(\mathbf{y}_{\mathbf{1}}^{(\nu)}\big)} \right)^{p^{s+\nu-1}} \mod p^{3s+3m-\nu}$$

- *and in the trivial case, if* $\bar{h} = id$ *we have*

$$\prod_{\chi \in \tilde{\mathfrak{R}}_{m,\infty}} \mathcal{N}_{\mathrm{Stab}_\Gamma(\chi)/\Gamma^{p^m}} \left(\frac{\mathbf{y}_\chi^{(\nu)}}{\varphi\big(\mathbf{y}_{\chi^p}^{(\nu)}\big)} \cdot \frac{\varphi\big(\mathcal{N}_{0,\mathbf{m}_\chi - 1}\big(\mathbf{y}_{\mathbf{1}}^{(\nu)}\big)\big)}{\mathcal{N}_{0,\mathbf{m}_\chi}\big(\mathbf{y}_{\mathbf{1}}^{(\nu)}\big)} \right)^{(p-1)p^{s+\nu-1}} \equiv 1 \mod p^{2s+3m},$$

which agree (after re-normalisation) with the congruences lebelled $(1.1)_{m,\underline{h}}$ *and* $(1.2)_m$ *in [DP15].*

Chapter 8

Some numerical calculations for $GL_2(\mathbb{F}_p)$-extensions

Let $p \geq 3$ be a prime. Consider now an elliptic curve E defined over $\mathbb{Q}$ without complex multiplication. By a famous result of Serre [Ser72], the Galois group of $\mathbb{Q}(E[p^\infty])$ over $\mathbb{Q}$ is an open subgroup of $GL_2(\mathbb{Z}_p)$, i.e.

$$G_\infty \;=\; Gal(\mathbb{Q}(E[p^\infty])/\mathbb{Q}) \;\lhd\; GL_2(\mathbb{Z}_p).$$

Since $GL_2(\mathbb{Z}_p) \cong \lim_{\leftarrow n} GL_2(\mathbb{Z}/p^n\mathbb{Z})$, we may then identify $Gal(\mathbb{Q}(E[p])/\mathbb{Q})$ with a subgroup of the finite group $GL_2(\mathbb{F}_p) \cong Aut(E[p])$.

There is an exact sequence of groups

$$1 \to \begin{pmatrix} 1+p\mathbb{Z}_p & p\mathbb{Z}_p \\ p\mathbb{Z}_p & 1+p\mathbb{Z}_p \end{pmatrix} \to GL_2(\mathbb{Z}_p) \xrightarrow{\text{mod } p} GL_2(\mathbb{F}_p) \to 1,$$

which induces on the level of K-groups a sequence

$$K_1\left(\Lambda\begin{pmatrix} 1+p\mathbb{Z}_p & p\mathbb{Z}_p \\ p\mathbb{Z}_p & 1+p\mathbb{Z}_p \end{pmatrix}\right) \to K_1(\Lambda(GL_2(\mathbb{Z}_p))) \xrightarrow{pr_1} K_1(\mathbb{Z}_p[GL_2(\mathbb{F}_p)]).$$

In particular, we have the commutative square

$$\begin{tikzcd}
K_1(\Lambda(Gal(\mathbb{Q}(E[p^\infty])/\mathbb{Q}))) \arrow[r] \arrow[d] & K_1(\mathbb{Z}_p[Gal(\mathbb{Q}(E[p])/\mathbb{Q})]) \arrow[d] \\
K_1(\Lambda(GL_2(\mathbb{Z}_p))) \arrow[r, "pr_1"'] & K_1(\mathbb{Z}_p[GL_2(\mathbb{F}_p)])
\end{tikzcd}$$

where the downward arrows are induced by the inclusion $Gal(\mathbb{Q}(E[p])/\mathbb{Q}) \hookrightarrow GL_2(\mathbb{F}_p)$.

As in Chapter 2, suppose there exists an element $\mathcal{L}_E \in K_1(\Lambda(G_\infty)_{S^*})$ satisfying the interpolation properties

$$\Phi_\rho(\mathcal{L}_E) = \frac{L_R(E,\rho,1)}{\Omega_+(E)^{d^+(\rho)}\Omega_-(E)^{d^-(\rho)}} \cdot e_p(\rho) \cdot \frac{P_p(\hat{\rho},u^{-1})}{P_p(\rho,\omega^{-1})} \cdot {\alpha_p}^{-f_\rho}$$

for all Artin representations

$$\rho : \ Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \to G_\infty \to GL(V_\rho)$$

in the specific notation of Conjecture 2.14 in Chapter 2. If we restrict to considering only those ρ's factoring through $Gal(\mathbb{Q}(E[p])/\mathbb{Q})$, then there is a factorisation

$$\begin{tikzcd}
K_1(\Lambda(G_\infty)_S) \arrow[rr, "pr_1"'] \arrow[drr, "\Phi_\rho"] & & K_1(\mathbb{Z}_p[Gal(\mathbb{Q}(E[p])/\mathbb{Q})]_{\bar{S}}) \arrow[d, "\rho"'] \\
& & \bar{\mathbb{Q}}_p \cup \{\infty\},
\end{tikzcd}$$

so that the value $\Phi_\rho(\mathcal{L}_E)$ depends only on $pr_1(\mathcal{L}_E)$.

Question: How can we describe $pr_1(\mathcal{L}_E)$ inside $K_1(\mathbb{Z}_p[GL_2(\mathbb{F}_p)])$ using congruences?

In fact, if one restricts to the p-primary part of $K_1(\mathbb{Z}_p[GL_2(\mathbb{F}_p)]$ then the answer is given by recent work of Kakde, which we now recall.

8.1 Review of Kakde's $GL_2(\mathbb{F}_p)$-paper

Let G denote the finite group $GL_2(\mathbb{F}_p)$. In the paper [Kak17], Kakde calculated $Conj(G)$ explicitly and derived a relationship between the multiplicative theta-map θ and the additive theta-map ψ, via an integral logarithm.

Let us firstly write $S(G) = \{Z, C, T, K\}$, where Z, C, T, K are the abelian subgroups of G given by

$$Z := \left\{ i_a = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \middle| \; a \in \mathbb{F}_p^\times \right\}$$

$$C := \left\{ c_{a,b} = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \middle| \; a \in \mathbb{F}_p^\times, \;\; b \in \mathbb{F}_p \right\}$$

$$T := \left\{ t_{a,d} = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \middle| \; a, d \in \mathbb{F}_p \right\}$$

$$K := \left\{ k_{a,b} = \begin{pmatrix} a & \epsilon b \\ b & a \end{pmatrix} \middle| \; a, b \in \mathbb{F}_p^\times \right\}$$

with $\epsilon \in \mathbb{F}_p - \mathbb{F}_{p^2}$, a non-square element. In this context, the multiplicative theta-map is defined by

$$\theta : K_1(\mathbb{Z}_p[G]) \longrightarrow \prod_{U \in S(G)} \mathbb{Z}_p[U]^\times,$$

where each component x_U, indexed by the subgroup U, is given by sending $x \mapsto \mathrm{Norm}_{\mathbb{Z}_p[G]/\mathbb{Z}_p[U]}(x) \mod [U, U]$ inside $\mathbb{Z}_p[U^{ab}]$.

Condition (F) Let χ_U be representations of U, and n_U be integers, such that

$$\sum_{U \in S(G)} n_U \mathrm{Ind}_U^G \chi_U = 0.$$

Note that this sum takes place in the group of virtual characters of G. Then we say that a tuple $(x_U) \in \prod_{U \in S(G)} \mathbb{Z}_p[U]^\times$ satisfies (F) if and only if for any χ_U and n_U as above,

$$\prod_U \chi_U(x_U)^{n_U} = 1.$$

Let φ denote the ring homomorphism induced by the p-power map $g \mapsto g^p$.

Definition 8.1 *Let Θ be the set of all tuples $x_U \in \prod_{U \in S(G)} \mathbb{Z}_p[U]_{(p)}^\times$ which are not torsion, and such that:*

- *(x_U) satisfies (F);*

- *$x_Z \equiv \varphi(x_C)(\mod p\mathbb{Z}_p[Z])$.*

We should point out that $C^p = Z$, whence $\phi : \mathbb{Z}_p[C] \to \mathbb{Z}_p[C^p] = \mathbb{Z}_p[Z]$, so the above congruence makes good mathematical sense.

Theorem 8.1 *(Thm 18,[Kak17]) The map θ induces an isomorphism between $K_1(\mathbb{Z}_p[G])_{(p)}$ and Θ.*

For the remainder of this chapter, our task is to verify this congruence numerically for $\mathcal{L}_E$, once these elements have been correctly evaluated at the trivial character.

8.2 The basic structure of $GL_2(\mathbb{F}_p)$

We now derive some useful facts about $GL_2(\mathbb{F}_p)$, which will be needed later.

Lemma 8.2 $\#GL_2(\mathbb{F}_p) = (p-1)^2 \cdot p \cdot (p+1)$.

Proof. Since $G = \mathrm{GL}_2(\mathbb{F}_p)$, one may rewrite G as

$$\begin{aligned} G &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a, b, c, d \in \mathbb{F}_p \text{ and } ad \neq bc \right\} \\ &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a \in \mathbb{F}_p^\times, b, c \in \mathbb{F}_p, d \neq bca^{-1} \in \mathbb{F}_p \right\} \bigcup \left\{ \begin{pmatrix} 0 & b \\ c & d \end{pmatrix} \;\middle|\; b, c \in \mathbb{F}_p^\times, d \in \mathbb{F}_p \right\}. \end{aligned}$$

To calculate the size of the full group of G, it is enough to determine the size of the disjoint subsets above. For the first subset, we have $p-1$ different choices for a, p choices for b and c, and $p-1$ choices for d. For the second subset, a is fixed to be 0, we have $p-1$ choices for b and c, and p choices for d. Therefore,

$$\begin{aligned} \#G &= (p-1) \cdot p \cdot p \cdot (p-1) + (p-1) \cdot (p-1) \cdot p \\ &= (p-1)^2 \cdot p \cdot (p+1) \end{aligned}$$

which establishes the result.

□

Lemma 8.3 *The only element of $S(G)$ that is a normal subgroup of G is Z.*

Proof. Let $A = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$ be an arbitrary element in $\mathrm{GL}_2(\mathbb{F}_p)$. Then we may undertake the following conjugations:

- For an arbitrary $i_a \in Z$, one has
$$Ai_aA^{-1} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in Z.$$
- Let $c = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in C$, then
$$AcA^{-1} = \frac{1}{wx - yz} \begin{pmatrix} awx - bxz - ayz & bx^2 \\ -bz^2 & awx + bxz - ayz \end{pmatrix}.$$
It is clear that $AcA^{-1} \notin C$ if $bz^2 \not\equiv 0 \mod p$.
- Let $t = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \in T$, then
$$AcA^{-1} = \frac{1}{wx - yz} \begin{pmatrix} awx - dyz & dxy - axy \\ awz - dwz & dwx - ayz \end{pmatrix}.$$
It is clear that $AcA^{-1} \notin T$ if $dxy - axy \not\equiv 0 \mod p$ or $awz - dwz \not\equiv 0 \mod p$.
- Let $k = \begin{pmatrix} a & \epsilon b \\ b & a \end{pmatrix} \in K$. Then
$$AkA^{-1} = \frac{1}{wx - yz} \begin{pmatrix} awx + bwy - ayz - \epsilon bxz & \epsilon bx^2 - by^2 \\ bw^2 - \epsilon bz^2 & awx - bwy - ayz + \epsilon bxz \end{pmatrix}.$$
So $AkA^{-1} \notin K$ if $w^2 \equiv \epsilon z^2 \mod p$.

Clearly only Z above is a normal subgroup of G. □

Lemma 8.4 *The sizes of the subgroups Z, C, T and K are respectively:*

(i) $\#Z = p - 1$ *;*

(ii) $\#C = (p-1)p$*;*

(iii) $\#T = (p-1)^2$*;*

(iv) $\#K = (p-1)(p+1)$.

Proof. (i) First let us consider the center Z. Since $Z = \{i_a \mid a \in \mathbb{F}_p^\times\}$, clearly $\#Z = \#\mathbb{F}_p^\times = p - 1$.

(ii) Next we focus on C, which contains all upper triangular matrices. Since there are $p-1$ different a's and p choices for b, then the size of C is simply $(p-1)p$.

(iii) Similarly, for the split Cartan subgroup T, there are $(\#\mathbb{F}_p^\times) \cdot (\#\mathbb{F}_p^\times) = (p-1)^2$ elements.

(iv) Finally, we focus on the non-split Cartan subgroup K. As all its matrices have the form $\begin{pmatrix} a & \epsilon b \\ b & a \end{pmatrix}$, we have to guarantee that $a^2 - \epsilon b^2 \neq 0$, otherwise it fails to be an element in $GL_2(\mathbb{F}_p)$. It turns out the only situation we need to worry about is the case when $a = b = 0$, thus there are $(\#\mathbb{F}_p)^2 - 1 = p^2 - 1$ matrices in K.

□

8.3 Evaluating at the trivial character

We want to translate Kakde's $GL_2(\mathbb{F}_p)$-congruences into a concrete statement, at least at the trivial character. Recall that his second congruence states that

$$x_Z \equiv \varphi(x_C) \mod p\mathbb{Z}_p[Z].$$

Question: What does this imply when we assume that x_Z and x_C are the respective images of $pr_1(\mathcal{L}_E)$ inside $\mathbb{Z}_p[Z]$ and $\mathbb{Z}_p[C]$?

Recall the predicted p-adic interpolation properties of $\mathcal{L}_E \in K_1(\Lambda(GL_2(\mathbb{Z}_p)))$ in Chapter 2. Specifically, if $\rho : G_{\mathbb{Q}} \to Gal(\mathbb{Q}(E[p])/\mathbb{Q}) \to GL(V)$ is an Artin representation factoring through $G = GL_2(\mathbb{F}_p)$, then

$$\mathcal{L}_E(\rho) = \frac{L_{\{pN_E\}}(E, \rho, 1)}{\Omega_+(E)^{d^+(\rho)}\Omega_-(E)^{d^-(\rho)}} \cdot \epsilon_p(\rho) \cdot \frac{P_p(\hat{\rho}, u^{-1})}{P_p(\rho, \omega^{-1})} \cdot u^{-f_\rho}.$$

Now for any Galois extension $K/\mathbb{Q}$ with $K \subset \mathbb{Q}(E[p])$, we can plug in the regular representation $\rho = reg_{K/\mathbb{Q}}$ of $\mathrm{Gal}(K/\mathbb{Q})$. Moreover, if the field K does not have any real embeddings then $d^+(\rho) = d^-(\rho) = [K : \mathbb{Q}]/2$, in which case

$$\mathcal{L}_E(reg_{K/\mathbb{Q}}) = \frac{L_{\{pN_E\}}(E/K, 1)}{(\Omega_+(E)\Omega_-(E))^{[K:\mathbb{Q}]/2}} \cdot \sqrt{\mid \triangle_K \mid} \cdot \frac{\zeta_{K,p}(u^{-1})}{\zeta_{K,p}(w^{-1})}$$

because p does not ramify in K so that $u^{-f_\rho} = u^{-0} = 1$.

As an example, if $F = \mathbb{Q}(E[p])$ and $K = F^Z$ then $K/\mathbb{Q}$ is Galois as $Z \lhd GL_2(\mathbb{F}_p)$ by Lemma 8.3; hence the value of x_Z at the trivial character should be

$$\begin{aligned}\mathbb{L}(x_Z) :&= \mathcal{L}_E(reg_{F^Z/\mathbb{Q}}) \\ &= \frac{L_{\{pN_E\}}(E/F^Z, 1)}{(\Omega_+(E)\Omega_-(E))^{(p-1)p(p+1)/2}} \cdot \sqrt{\mid \triangle_{F^Z} \mid} \cdot \frac{\zeta_{F^Z,p}(u^{-1})}{\zeta_{F^Z,p}(w^{-1})}.\end{aligned}$$

We should also warn the reader that F^C is not a Galois extension over $\mathbb{Q}$ (by Lemma 8.3 again), so we cannot set $\rho := reg_{F^C/\mathbb{Q}}$ as this does not make sense. Let us therefore abuse notation, and put

$$\mathbb{L}(x_C) := \frac{L_{\{pN_E\}}(E/F^C, 1)}{(\Omega_+(E)\Omega_-(E))^{(p-1)(p+1)/2}} \cdot \sqrt{\mid \triangle_{F^C} \mid} \cdot \frac{\zeta_{F^C,p}(u^{-1})}{\zeta_{F^C,p}(w^{-1})}.$$

The following statement should then follow from Kakde's 'mod p' congruence:

$$\mathbb{L}(x_Z) \equiv \mathbb{L}(x_C) \mod p,$$

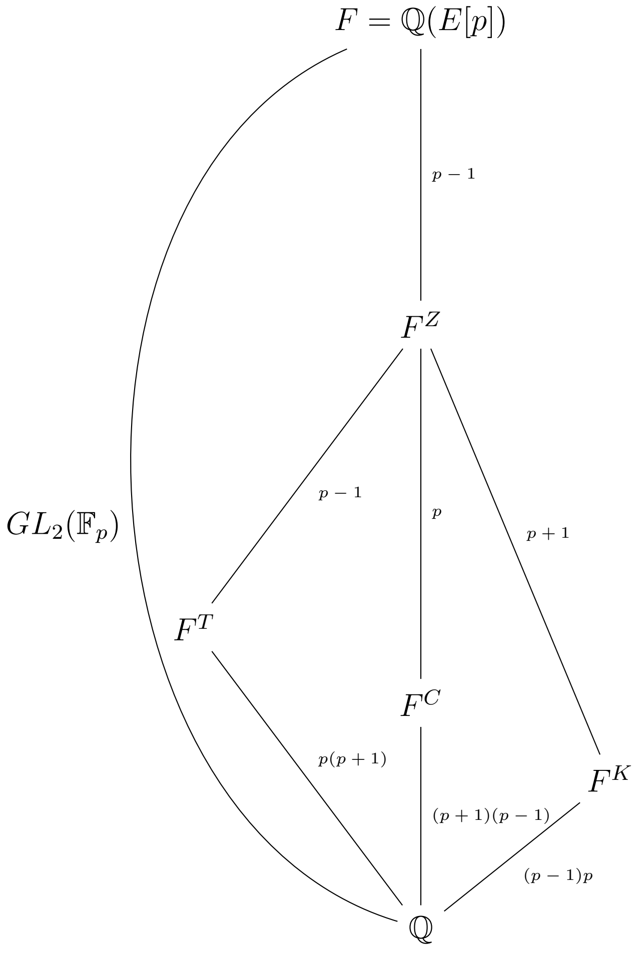
assuming the existence of the analytic element $pr_1(\mathcal{L}_E) \in K_1(\mathbb{Z}_p[GL_2(\mathbb{F}_p)])$ of course. In other words, one should have the congruence

$$\begin{aligned}&\frac{L_{\{pN_E\}}(E/F^Z, 1)}{(\Omega_+(E)\Omega_-(E))^{(p-1)p(p+1)/2}} \cdot \sqrt{\mid \triangle_{F^Z} \mid} \cdot \frac{\zeta_{F^Z,p}(u^{-1})}{\zeta_{F^Z,p}(w^{-1})} \\ \equiv\ &\frac{L_{\{pN_E\}}(E/F^C, 1)}{(\Omega_+(E)\Omega_-(E))^{(p-1)(p+1)/2}} \cdot \sqrt{\mid \triangle_{F^C} \mid} \cdot \frac{\zeta_{F^C,p}(u^{-1})}{\zeta_{F^C,p}(w^{-1})} \mod p. \qquad (\star)\end{aligned}$$

8.4 A numerical strategy for $p = 3$

Recall that $p \geq 3$ is a prime, and let $E[p]$ be the group of p-torsion points on the non-CM elliptic curve E. Note that the p-torsion field $\mathbb{Q}(E[p])$ is an extension of the splitting field of the p-division polynomial, $\psi_p(x)$, whose roots are the x-coordinates of the non-trivial p-torsion points. Using the algorithm in [Sut16], we constructed the splitting field of $\psi_p(x)$, and then took the appropriate quadratic extension to obtain $\mathbb{Q}(E[p])$.

Now, let $F = \mathbb{Q}(E[p])$ be the extension of $\mathbb{Q}$ which contains all x-coordinates and y-coordinates of the p-torsion points on the elliptic curve E. Assume that $Gal(\mathbb{Q}(E[p])/\mathbb{Q}) \cong GL_2(\mathbb{F}_p)$, and write F^Z, F^C, F^T, F^K for the fixed fields of Z, C, T, K respectively. In this setting, there is the field diagram



.

We devote the rest of this chapter to numerically verifying $(\star)$ at the prime $p = 3$.

Lemma 8.5 *Assume that E has good ordinary reduction at $p = 3$, and that $F = \mathbb{Q}(E[3])$ is a $GL_2(\mathbb{F}_3)$-extension of $\mathbb{Q}$.*

(i) Z is the only normal subgroup of $GL_2(\mathbb{F}_3)$ with 2 elements.

(ii) If $p = 3$, then $F^Z = \mathbb{Q}(\psi_3)$.

(iii) F^Z is a degree 3 extension of F^C, and $F^Z \cong F^C(\sqrt[3]{\Delta_E})$.

Proof. (i) Suppose there exists a subgroup H inside $GL_2(\mathbb{F}_3)$ with 2 elements, e.g. $H = \{\mathrm{id}, \tau\}$. Then we must have

$$g\mathrm{id}g^{-1} = \mathrm{id} \text{ and } g\tau g^{-1} = \tau \quad \text{for all } g \in G.$$

It follows that H is a subset of the center Z, and as $\#Z = 2$ clearly $H = Z$

(ii) For simplicity, suppose that the elliptic curve is given by the equation $y^2 = x^3 + Ax + B$. Since $F = \mathbb{Q}(\psi_3)(\sqrt{x^3 + Ax + B})$, one must have $[F : \mathbb{Q}(\psi_3)] = 2$, where $H = Gal(F/\mathbb{Q}(\psi_3)) \cong \mathbb{Z}/2\mathbb{Z}$. However $\mathbb{Q}(\psi_3)/\mathbb{Q}$ is Galois, thus $H \lhd G$ and $H = Z$ by the previous argument.

(iii) Recall that for an elliptic curve E, the 3-division polynomial ψ_3 has the form

$$\psi_3(x) = 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8 = 0,$$

where b_2, b_4, b_6, b_8 are the coefficients defined in Chapter 2, Section 2.1. Assume that x_1, x_2, x_3, x_4 are the roots of ψ_3, and make a choice of labelling $\{i, j, k, l\} = \{1, 2, 3, 4\}$. Serre showed in [Ser72, 48] that these roots satisfy the relation

$$\sqrt[3]{\Delta_E} = b_4 - 3(x_ix_j + x_kx_l).$$

It is clear that $\mathbb{Q}(\sqrt[3]{\Delta_E})$ must be contained in $\mathbb{Q}(\psi_3)$, where $\mathbb{Q}(\psi_3) = F^Z$ as shown in part (ii). Therefore $F^C(\sqrt[3]{\Delta_E})$ is a subfield of F^Z, and it must coincide with it since both fields have degree 24 over $\mathbb{Q}$.

All three parts of the result have now been shown.

□

In summary, one obtains the following field diagram:

$$\begin{tikzcd}
& F \arrow[d, dash, "2"] & \\
& F^Z \arrow[dl, dash, "3"] \arrow[ddr, dash, "4"] & \\
F^C \arrow[ddr, dash, "8"] & & \\
& & \mathbb{Q}(\mu_3, \sqrt[3]{\Delta_E}) \arrow[dl, dash, "6"] \\
& \mathbb{Q} &
\end{tikzcd}$$

We should now point out that if $L(E/F^C, 1) = 0$ then (assuming the BSD conjecture) it will also be the case that $L(E/F^Z, 1) = 0$ as F^C is a subfield of F^Z. Consequently, the congruence labeled $(\star)$ is automatically true in this situation.

We therefore searched for numerical examples with both $L(E/F^C, 1) \neq 0$ and $L(E/F^Z, 1) \neq 0$ using MAGMA. In fact, to cut down the number of curves to consider, we first looked for examples with $L\big(E/\mathbb{Q}(\mu_3, \Delta_E^{1/3}), 1\big) \neq 0$ using the Dokchitser's existing code. Up to conductor $N_E \leq 400$, below are the examples that we calculated. They each confirm that Kakde's congruence holds numerically.

8.4.1 An example at level 128

Let $p = 3$, and suppose that E is the elliptic curve defined by

$$y^2 = x^3 - x^2 - x - 1$$

which is labelled as $E128C1$ in Cremona's tables. We first calculated the 3-division polynomial

$$\psi_3 = 3x^4 - 4x^3 + 6x^2 - 12x + 3,$$

where the roots of the polynomial are just the x-coordinates of the 3-torsion points on the curve. Then one computes its splitting field $\mathbb{Q}(\psi_3)$.

Now, let us pick up a 3-torsion point P on the curve with x-coordinate x_1, a root of ψ_3. We can evaluate the respective y-coordinates, $\pm y_1$, corresponding to x_1 on the curve. Lastly, we obtain the 3-torsion group $\mathbb{Q}(E[3])$ by adjoining $\sqrt{x_1^3 - x_1^2 - x_1 - 1}$ to $\mathbb{Q}(\psi_3)$ (if y_1 is non-square), i.e. $\mathbb{Q}(E[3]) = \mathbb{Q}(\psi_3, y_1)$.

Once one has determined the 3-torsion group of E, we are able to compute the appropriate fixed fields. Recall that if H is a subgroup of G, then the fixed field of H is

$$F^H = \{x \in F : h(x) = x \text{ for all } h \in H\}.$$

Since $Gal(F/\mathbb{Q}) \cong GL_2(\mathbb{F}_3)$, and each of Z, C, T, K are subgroups of $GL_2(\mathbb{F}_3)$, we can therefore realize Z, C, T, K as subgroups of the automorphism group $\mathrm{Aut}(F) \cong GL_2(\mathbb{F}_3)$.

Recall that

$$\mathbb{L}(x_Z) := \frac{L_{\{pN_E\}}(E/F^Z, 1)}{(\Omega_+(E)\Omega_-(E))^{(p-1)p(p+1)/2}} \cdot \sqrt{\mid \triangle_{F^Z} \mid} \cdot \frac{\zeta_{F^Z,p}(u^{-1})}{\zeta_{F^Z,p}(w^{-1})},$$

and

$$\mathbb{L}(x_C) := \frac{L_{\{pN_E\}}(E/F^C, 1)}{(\Omega_+(E)\Omega_-(E))^{(p-1)(p+1)/2}} \cdot \sqrt{\mid \triangle_{F^C} \mid} \cdot \frac{\zeta_{F^C,p}(u^{-1})}{\zeta_{F^C,p}(w^{-1})},$$

Using MAGMA and the commands *Lseries*, *Discriminant* and *TensorProduct*, we numerically calculated the L-values

$$L^*(F^Z, 1) = \left| \frac{L_{(pN_E)}(E/F^Z, 1)\sqrt{\Delta_{F^Z}}}{(\Omega_+(E)\Omega_-(E))^{12}} \right| \approx \frac{12934114635}{2048}$$

and

$$L^*(F^C, 1) = \left| \frac{L_{(pN_E)}(E/F^C, 1)\sqrt{\Delta_{F^C}}}{(\Omega_+(E)\Omega_-(E))^{4}} \right| \approx \frac{390051}{1070}.$$

The Euler factors are easily determined to be

$$\frac{\zeta_{F^Z,p}(u^{-1})}{\zeta_{F^Z,p}(w^{-1})} = 3122 * 3^3 + O(3^{11}) \text{ and } \frac{\zeta_{F^C,p}(u^{-1})}{\zeta_{F^C,p}(w^{-1})} = 2786 * 3 + O(3^9).$$

Combining all this separate information together, one eventually concludes that

$$\begin{aligned}\mathbb{L}(x_Z) &= L^*(F^Z,1)\cdot\prod_{q=2}P_q(E,q^{-1})\cdot\frac{\zeta_{F^Z,p}(u^{-1})}{\zeta_{F^Z,p}(w^{-1})}\\ &= \frac{12934114635}{2048}\cdot\frac{4}{9}\cdot\frac{\zeta_{F^Z,p}(u^{-1})}{\zeta_{F^Z,p}(w^{-1})}\\ &= -1487*3^2+O(3^{10})\\ &= [0,0,1,2,2,1,2,2,2],\end{aligned}$$

and

$$\begin{aligned}\mathbb{L}(x_C) &= L^*(F^C,1)\cdot\prod_{q=2}P_q(E,q^{-1})\cdot\frac{\zeta_{F^C,p}(u^{-1})}{\zeta_{F^C,p}(w^{-1})}\\ &= \frac{390051}{1070}\cdot 1\cdot\frac{\zeta_{F^C,p}(u^{-1})}{\zeta_{F^C,p}(w^{-1})}\\ &= -1784*3^3+O(3^{11})\\ &= [0,0,0,1,2,2,2,1,2],\end{aligned}$$

which verifies the congruence ($\star$) for $p=3$, as predicted!

8.4.2 An example at level 248

Let us instead look at the situation in which $p=3$ and E an elliptic curve defined by

$$y^2=x^3+x^2+8x$$

with Cremona reference $E248B1$.

Using the same method as the previous example, we numerically calculated the L-values

$$L^*(F^Z,1)=\left|\frac{L_{(pN_E)}(E/F^Z,1)\sqrt{\Delta_{F^Z}}}{(\Omega_+(E)\Omega_-(E))^{12}}\right|\approx\frac{6083742632477}{2301}$$

and

$$L^*(F^C,1)=\left|\frac{L_{(pN_E)}(E/F^C,1)\sqrt{\Delta_{F^C}}}{(\Omega_+(E)\Omega_-(E))^{4}}\right|\approx\frac{115361}{9791}.$$

The Euler factors are easily found to be

$$\frac{\zeta_{F^Z,p}(u^{-1})}{\zeta_{F^Z,p}(w^{-1})}=-1676785*3^{22}+O(3^{36})\text{ and }\frac{\zeta_{F^C,p}(u^{-1})}{\zeta_{F^C,p}(w^{-1})}=-12960058636*3^6+O(3^{28}).$$

Combining all this separate information together, one eventually concludes that

$$\begin{aligned}\mathbb{L}(x_Z) &= L^*(F^Z,1)\cdot\prod_{q=2} P_q(E,q^{-1})\cdot\frac{\zeta_{F^Z,p}(u^{-1})}{\zeta_{F^Z,p}(w^{-1})}\\ &= \frac{6083742632477}{2301}\cdot\frac{167168}{11}\cdot\frac{\zeta_{F^Z,p}(u^{-1})}{\zeta_{F^Z,p}(w^{-1})}\\ &= 1278287*3^{21}+O(3^{35}) \;=\; [0,0,0,0,0,0,0,0,0],\end{aligned}$$

and

$$\begin{aligned}\mathbb{L}(x_C) &= L^*(F^C,1)\cdot\prod_{q=2} P_q(E,q^{-1})\cdot\frac{\zeta_{F^C,p}(u^{-1})}{\zeta_{F^C,p}(w^{-1})}\\ &= \frac{115361}{9791}\cdot\frac{416844}{9017}\cdot\frac{\zeta_{F^C,p}(u^{-1})}{\zeta_{F^C,p}(w^{-1})}\\ &= 12169322354*3^8+O(3^{30})\\ &= [0,0,0,0,0,0,0,0,2],\end{aligned}$$

which verifies the congruence ($\star$) for $p=3$, again as predicted.

Appendix A

Computer code

In this Appendix, we have included the Magma code that we used to verify the p-adic congruences of Kakde [Kak17] for those examples in Chapter 8.

```
// Returns poly who's roots are precisely the x-coords of the points of order m on E (this means removing factors that are n-division polys for n dividing m)
PrimitiveDivisionPolynomial := function(E,m)
  local f;
  f:=DivisionPolynomial(E,m);
  for d in Divisors(m) do if d gt 1 and d lt m then f := ExactQuotient(f,$$(E,d)); end if; end for;
  return f;
end function;

// Magma really wants number fields to be defined by integral monic polynomials, so we make sure this happens
IsIntegrallyDefined := function(K)
  local f;
  if K eq Rationals() then return true; end if;
  if not IsAbsoluteField(K) then return false; end if;
  f := DefiningPolynomial(K);
  return IsMonic(f) and &and[c in Integers():c in Coefficients(f)];
end function;

```

```
// Redefines a number field so that it is defined in terms of the absolute minimal polynomial of a generator that is an algebraic integer
MakeIntegrallyDefined := function(K)
  local g;
  while not IsIntegrallyDefined(K) do
    g := SimpleExtension(K).1;
    f := MinimalPolynomial(g);
    g *:= &*PrimeDivisors(LCM([Denominator(c/LeadingCoefficient(f)):c in Coefficients(f)]));
    K:=NumberField(MinimalPolynomial(g));
  end while;
  return K;
end function;


// Returns a pair [P,Q] of independent generators for E[m] (the points P and Q will necessarily have order m), where E is an elliptic curve y^2=x^3+Ax+B with A,B in Q
// Be warned that this is painfully slow: unless the m-division field Q(E[m]) has very small degree you will need to be patient
TorsionField := function(E,m)
  local C, K, L, EL, x1, y1, y1s, x2, y2, y2s, Q, P, S, phi, f, b, g;

  C := Coefficients(E);
  assert C[1] eq 0 and C[2] eq 0 and C[3] eq 0 and C[4] in Rationals() and C[5] in Rationals();
    // To simplify matters, we require E to be in the form y^2=x^3+Ax+B with A,B in Q
  phi:=PrimitiveDivisionPolynomial(E,m);
        roots := Roots(phi);
  if #roots ne Degree(phi) then
        K:=SplittingField(phi);
    return $$(ChangeRing(E,MakeIntegrallyDefined(K)),m);
  end if;
  K:=BaseRing(E);
  L:=K;
  R<x>:=PolynomialRing(K);
  // Our first basis point P (of order m) will have x-coord equal to the first root of phi
  x1:=roots[1][1];
  f:=x^3+C[4]*x+C[5];
  y1s:=Evaluate(f,x1);
    b,y1:=IsSquare(y1s);  // this step is time-consuming
  // if y1 is not in L, extend L so that it is
  if not b then L := NumberField(x^2-y1s); end if;
  if L ne Rationals() and not IsAbsoluteField(L) then L:= AbsoluteField(L); end if;
    return MakeIntegrallyDefined(L);
end function;





//function to find all non-square elements in GF(m)
NonSquare := function(m)
   S:=[];
   for e in GF(m) do
         if not IsSquare(e) then
          Include(~S,e);
          end if;
    end for;

          return S;
end function;




```

```

//Returns the fixed fields of Z,C,T,K.
Fixedfields := function(E,m)
     local F,Gal,G,A,Z,Za,C,Ca,T,Ta,K,Ka;
     F:=TorsionField(E,m);
     Gal:=GaloisGroup(F);
     G:=GL(2,GF(m));
     A:=AutomorphismGroup(F);
     Z:=Center(G);
     Za:=Center(A);
     C:=sub<G|[[a,b, 0,a]:a in [1..m-1],b in [0..m-1]]>;
      for i in [1..#Subgroups(A)] do
         if IsIsomorphic(C,Subgroups(A)[i]`subgroup) then
            Ca:=Subgroups(A)[i]`subgroup;
         end if;
       end for;

      T:=sub<G|[[a,0, 0,d]:a in [1..m-1],d in [1..m-1]]>;
     for i in [1..#Subgroups(A)] do
         if IsIsomorphic(T,Subgroups(A)[i]`subgroup) then
            Ta:=Subgroups(A)[i]`subgroup;
         end if;
     end for;

     K:=sub<G|[[a,e*b, b,a]:a in [1..m-1],b in [1..m-1],e in NonSquare(m)]>;
     for i in [1..#Subgroups(A)] do
         if IsIsomorphic(K,Subgroups(A)[i]`subgroup) then
            Ka:=Subgroups(A)[i]`subgroup;
         end if;
     end for;


return [FixedField(F,Za),FixedField(F,Ca),FixedField(F,Ta),FixedField(F,Ka)];
end function;
```

```

/////////////////////////////////////////////////////////////////
// MAGMA code to compute L-values of elliptic curves, twisted by regular representations factoring through the first level of F^z and F^C.

// We use MAGMA's L-series functions, and methods from Tim and Vladimir Dokchitser's paper "Computations in Non-Commutative Iwasawa Theory".
/////////////////////////////////////////////////////////////////

SetVerbose("LSeries",0);
// Set the verbosity at 1, 2 or 3 if you want to follow progress of the L-series functions


// ELLIPTIC CURVES:

// Worked example from Dokchitsers' paper
E21 := EllipticCurve("21a4");

// Other curves used by Dokchitsers
E11 := EllipticCurve("11a3");
E20 := EllipticCurve("20a3");
E26 := EllipticCurve("26a1");
E77 := EllipticCurve("77C1");
E19 := EllipticCurve("19a3");
E56 := EllipticCurve("56b1");
E128 := EllipticCurve("128c1");

// Set the prime p
p :=3;

// Set the elliptic curves to use
for E in [E128] do

```

```
E;

//Find the fixed fields
time Fix:=Fixedfields(WeierstrassModel(E),p);

Fz:= Fix[1];

Fc:= Fix[2];

Ft:= Fix[3];

Fk:= Fix[4];








// Set the precisions

prec  := 25; // 'prec' is the number of digits precision for computing the L-values.
              // The higher the precision, the slower the computations will be.

prec2 := 4; // 'prec2' is precision for recognising the L-values as rational numbers

bound := 8; // 'bound' is the degree of precision for our p-adic fields

/////////////////////////////////////////////////////////////////

NE:=Conductor(E);
LE:=LSeries(E);
```

```
LSetPrecision(LE,prec);

// Check the curve is ordinary at p

apE := LGetCoefficients(LE,p)[p];
assert (apE mod p) ne 0;

/////////////////////////////////////////////////////////////////


// Create rings and fields

QQ := RationalField();
C<i>:=ComplexField(prec);
ZZ := Integers();
PCC<x> := PolynomialRing(C);
PZZ<y> := PolynomialRing(ZZ);

QQp := pAdicField(p,bound);

// 'period' is Omega(E,+)*Omega(E,-)

period:= Periods(E : Precision:=prec )[1]*Im(Periods(E : Precision:=prec )[2]);


//Discriminant of the fields
DFz:=Abs(Discriminant(MaximalOrder(Fz)));

DFc:=Abs(Discriminant(MaximalOrder(Fc)));



// L-fucntion for the fields
LFz:=LSeries(Fz);

```

```
LFc:=LSeries(Fc);

LEFz:=TensorProduct(LE,LFz,[]);
LSetPrecision(LEFz,prec);
"Coeff reqd for LEFz= ", LCfRequired(LEFz);


LEFc:=TensorProduct(LE,LFc,[]);
LSetPrecision(LEFc,prec);
"Coeff reqd for LEFc= ", LCfRequired(LEFc);


lEFz:=Evaluate(LEFz,1);

lEFc:=Evaluate(LEFc,1);

lEFz2 := Abs((lEFz*Sqrt(DFz)) / ((2*period)^(Degree(Fz) div 2)));
lEFc2 := Abs((lEFz*Sqrt(DFc)) / ((2*period)^(Degree(Fc) div 2)));

lEFz3 := BestApproximation( Re(lEFz2), 10^prec2);
lEFc3 := BestApproximation( Re(lEFc2), 10^prec2);          //this gives the value of L* in Dokchitsers' paper



// Function to factorise a rational number:

function factors(a)
  if a eq 0 then
     return 0;
  end if;
  return Factorization(Numerator(a)) cat [ <vv[1],-vv[2]> : vv in Factorization(Denominator(a)) ];
end function;

////////////////////////////////////////////////
```

```

// Dirichlet L-series of correct precision:
function Lchi(char)
    L := LSeries(char);
    LSetPrecision(L,prec);
    return L;
end function;

// Dirichlet twist of E to correct precision:
function LEtwist(char)
    if IsDivisibleBy(Conductor(char),2) eq true then
      L := TensorProduct(LE,Lchi(char),[<2,5,1>]);
      LSetPrecision(L,prec);
      return L;
    end if;
    L := TensorProduct(LE,Lchi(char),[]);
    LSetPrecision(L,prec);
    return L;
end function;

////////////////////////////////////////////////////////


////////// L-FACTORS /////////////

// Compute local factor: P_q(E,Reg_F,s)

function Lfactor(EE,FF,s,q)
  aqE := FrobeniusTraceDirect(EE,q);
  if Degree(FF) eq 1 then
     return (1 - aqE*(q^(-s)) + (q^(1-2*s)));
  end if;
  alpha, beta := Explode( [ v[1] : v in Roots(x^2-aqE*x+q)] );
  degs := [ Degree(w[1]) : w in Decomposition(FF,q)];
  return &*[ 1 - (alpha^dd + beta^dd)*(q^(-dd*s)) + q^(dd*(1-2*s))
     : dd in degs ];
```

```
end function;

// Local poly of Dedekind zeta of FF over the prime q

function Lpoly(FF,q)
  if Degree(FF) eq 1 then
     return (1-y);
  end if;
  degs := [ Degree(w[1]) : w in Decomposition(FF,q)];
  return &*[ 1-y^dd : dd in degs ];
end function;




//////////////////////////////////////////////////////


//This gives the product of P_q at bad primes q
eulFz1    := &*[ Lfactor(E,Fz,1,q) : q in PrimeDivisors(p*(ZZ!Abs(Discriminant(E)))) ];
eulFz   := &*[ BestApproximation(Lfactor(E,Fz,1,q), 10^prec2) : q in PrimeDivisors(p*(ZZ!Abs(Discriminant(E)))) ];




eulFc1    := &*[ Lfactor(E,Fc,1,q) : q in PrimeDivisors(p*(ZZ!Abs(Discriminant(E)))) ];
eulFc   := &*[ BestApproximation(Lfactor(E,Fc,1,q), 10^prec2) : q in PrimeDivisors(p*(ZZ!Abs(Discriminant(E)))) ];





```

```

/////////////////////////////////////////////

// FUNCTIONS FOR COMPUTING P-ADIC EXPANSIONS
///////////////////////////////////////////////

// Computes q-adic expansion of a, up to q^N
function padicexpansion(a,q,N)
  v := [];
  a := a mod q^(N+2);
  for i := 0 to N do
    v := Append(v,(a mod q));
    a := (a-(a mod q)) div q;
  end for;
  return v;
end function;

// Compute a q-adic expansion of a root of f via Hensel's lemma
function hensel(f,a,q,N)
  a := a mod q;
  v := [a];
  g := Derivative(f);
    for k := 1 to N do
      t := -(Evaluate(f,a) div q^k) * InverseMod( Evaluate(g,a) , q);
      t := t mod q;
      a := a + t*(q^k);
      v := Append(v,t);
    end for;
  return v;
end function;

// Turns q-adic expansion v back into an integer
function expansiontonumber(v,q)
  ans := 0;
  for k := 1 to #v do
```

```
    ans := ans + v[k]*(q^(k-1));
  end for;
  return ans mod p^bound;
end function;

// q-adic expansion of a p-integral rational number

function fractoexp(a,q,bound)
  inverse1 := InverseMod(Denominator(a),p^bound);
  return padicexpansion(Numerator(a)*inverse1 , p, bound);
end function;

////////////////////////////////////////////

// Write a p-adic expansion out in LaTeX
//////////////////////////////////////////

procedure texexpansion(v)
printf "$";
  for k in [1..#v] do
    if v[k] ne 0 then
    printf "  %o.%o^{%o} + ",v[k],p,k-1;
end if;
end for;
printf " + O(%o^{%o})$  \n",p,#v;
end procedure;

// Write the factorisation of a rational number in LaTeX

procedure texfactors(a)
if a eq 0 then
printf "$0$ \n";
 else
 vv := factors(a);
printf "$";
  for k in [1..#vv-1] do
```

```
        printf "%o^{%o} . ",vv[k][1],vv[k][2];
end for;
printf "%o^{%o}$ \n",vv[#vv][1],vv[#vv][2];
end if;
end procedure;

//////////////////////////////////////////////////


"  "; "  "; "  ";
"E = ",CremonaReference(E), "    p = ",p, "    Precision = ",prec; //Delta = ",delta,"
"  ";

// SANITY CHECK: we display the prime factors of the algebraic parts of the twisted L-values. In small test cases we do not expect them to be divisible by enormous primes. If they are, it is likely that the 'BestApproximation' function has not identified them as the correct rational numbers.


"L(EFz,1)   =  ", lEFz;
" ";
"L*(E,Fz)  = ", lEFz2;
"             = ", lEFz3;
"             = ", factors(lEFz3);
"  ";
"L(EFc,1)   =  ", lEFc;
" ";
"L*(E,Fc)    = ", lEFc2;
"             = ", lEFc3;
"             = ", factors(lEFc3);
"  ";

"Check:",[Denominator(lEFz3)*lEFz2,Denominator(lEFc3)*lEFc2];
" ";
```

```



"Euler factor of L(E,Fz,1) at p*Discriminant(E) = ",eulFz;
"Euler factor of L(E,Fc,1)   at p*Discriminant(E) = ",eulFc;
" ";

// Calculate our local roots u and w
// uu = unit root (in the ordinary case)
// ww = non-unit root

expu := hensel( y^2-apE*y+p, apE, p, bound);
expw := hensel( y^2-apE*y+p, 0, p, bound);

uu := QQp!expansiontonumber(expu,p);
ww := QQp!expansiontonumber(expw,p);

//////////////////////////////////////////////////

// N.B. We have P_p(Fz,T) = 1-T, so the Euler factor in the interpolation formula for the Coates et al p-adic L-value is (1-inverse(u))/(1-inverse(w)). Multipling top and bottom by p = u*w, we get = (p-w)/(p-u), which we calculate below.



Fzpoly  := PZZ!(Lpoly(Fz,p) div (1-y));
EEFz := Evaluate(Fzpoly,1/uu) / Evaluate(Fzpoly,1/ww);
Fcpoly  := PZZ!(Lpoly(Fc,p) div (1-y));
EEFc := Evaluate(Fcpoly,1/uu) / Evaluate(Fcpoly,1/ww);



/// XFz and XFc are the values of the conjectural Coates-Fukaya-Kato-Sujatha-Venjakob p-adic L-function at Fz and Fc respectively
```

```

XFz := EEFz*eulFz*lEFz3;

XFc := EEFc*eulFc*lEFc3;



/////////////// RESULTS //////////////////

" "; "/////////////////////////////////////";" ";
"euler factor for Fz = ", EEFz;

"euler factor for Fc   = ", EEFc;

"Lcal(Fz)  = ", XFz;
padicexpansion(ZZ!XFz,p,bound);
" ";
texexpansion(padicexpansion(ZZ!XFz,p,bound));
" ";
"Lcal(Fc)     = ", XFc;
padicexpansion(ZZ!XFc,p,bound);
" ";
texexpansion(padicexpansion(ZZ!XFc,p,bound));
" ";

"Difference   = ", XFc-XFz;


" ";

if lEFc3 eq 0 and Valuation(XFz) gt 0 then
  "L(E,Fc,1) is zero and Lcal(Fz) is zero mod pi, that's OK.";
elif lEFz3 eq 0 and Valuation(XFc) gt 0 then
   "L(E,Fz,1) is zero and Lcal(Fc) is zero mod pi, that's OK.";
else
```

```
  check := Valuation(XFc-XFz) gt Valuation(XFc) and   Valuation(
    XFc-XFz) gt Valuation(XFz);
  "Difference is more p-integral? ",check;
end if;

"  ";

"/////////////////////////////////////";"   ";



end for;
```

References

[Bou10] Thanasis Bouganis. Special values of l-functions and false tate curve extensions. *Journal of the London Mathematical Society*, 82(3):596–620, 2010.

[Bur15] David Burns. On main conjectures in non-commutative iwasawa theory and related conjectures. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 2015(698):105–159, 2015.

[BV11] David Burns and Otmar Venjakob. On descent theory and main conjectures in non-commutative Iwasawa theory. *Journal of the Institute of Mathematics of Jussieu*, 10(01):59–118, 2011.

[CFK$^+$05] John Coates, Takako Fukaya, Kazuya Kato, Ramdorai Sujatha, and Otmar Venjakob. The GL_2 main conjecture for elliptic curves without complex multiplication. *Publications Mathématiques de l'Institut des Hautes Études Scientifiques*, 101(1):163–208, 2005.

[CN79] Pierrette Cassou-Nogues. Valeurs aux entiers négatifs des fonctions zêta et fonctions zêtap-adiques. *Inventiones mathematicae*, 51(1):29–59, 1979.

[CSRV12] John Coates, Peter Schneider, Sujatha Ramdorai, and Otmar Venjakob. *Noncommutative Iwasawa main conjectures over totally real fields: Münster, April 2011*, volume 29. Springer Science & Business Media, 2012.

[CW77] John Coates and Andrew Wiles. On the conjecture of birch and swinnerton-dyer. *Inventiones mathematicae*, 39(3):223–251, 1977.

[DDSMS03] John D Dixon, Marcus PF Du Sautoy, Avinoam Mann, and Dan Segal. *Analytic pro-p groups*, volume 61. Cambridge University Press, 2003.

[Del18] Daniel Delbourgo. Variation of the analytic λ-invariant over a solvable extension. *preprint*, 2018.

[DL17] Daniel Delbourgo and Antonio Lei. Estimating the growth in mordell–weil ranks and shafarevich–tate groups over lie extensions. *The Ramanujan Journal*, 43(1):29–68, 2017.

[DP15] Daniel Delbourgo and Lloyd Peters. Higher order congruences amongst hasse–weil l-values. *Journal of the Australian Mathematical Society*, 98(1):1–38, 2015.

[DR80] Pierre Deligne and Kenneth A Ribet. Values of abelianl-functions at negative integers over totally real fields. *Inventiones mathematicae*, 59(3):227–286, 1980.

[DT10] Henri Darmon and Ye Tian. Heegner points over towers of kummer extensions. *Canad. J. Math*, 62(5):1060–1081, 2010.

[DW08] Daniel Delbourgo and Tom Ward. Non-abelian congruences between l-values of elliptic curves (congruences non-abeliennes entres les valeurs l des courbes elliptiques). In *Annales de l'institut Fourier*, volume 58, pages 1023–1055, 2008.

[DW10] Daniel Delbourgo and Thomas Ward. The growth of cm periods over false tate extensions. *Experimental Mathematics*, 19(2):195–210, 2010.

[Gre94] Ralph Greenberg. Iwasawa theory and p-adic deformations of motives. In *Proceedings of Symposia in Pure Math*, volume 55, page 193, 1994.

[GSK09] Jon González-Sánchez and Benjamin Klopsch. Analytic pro-p groups of small dimensions. *Journal of Group Theory*, 12(5):711–734, 2009.

[GZ86] Benedict H Gross and Don B Zagier. Heegner points and derivatives ofl-series. *Inventiones mathematicae*, 84(2):225–320, 1986.

[Har10] Takashi Hara. Iwasawa theory of totally real fields for certain non-commutative p-extensions. *Journal of Number Theory*, 130(4):1068–1097, 2010.

[K$^+$05] Kazuya Kato et al. p-adic Hodge theory and values of zeta functions of modular forms. *Astérisque Journal*, 294(1), 2005.

[Kak13] Mahesh Kakde. The main conjecture of Iwasawa theory for totally real fields. *Inventiones mathematicae*, 193(3):539–626, 2013.

[Kak17] Mahesh Kakde. Some congruences for non-cm elliptic curves. *Elliptic Curves, Modular Forms and Iwasawa Theory: In Honour of John H. Coates' 70th Birthday, Cambridge, UK, March 2015*, 188:295, 2017.

[Kat05] Kazuya Kato. $K1$ of some non-commutative completed group rings. *K-theory*, 34(2):99–140, 2005.

[Kat06] Kazuya Kato. Iwasawa theory of totally real fields for galois extensions of heisenberg type. *preprint*, 180, 2006.

[Kim15] Dohyeong Kim. On the transfer congruence between p-adic hecke l-functions. *Cambridge Journal of Mathematics*, 3(3):355–438, 2015.

[KL89] Victor A Kolyvagin and Dmitry Yu Logachëv. Finiteness of the shafarevich-tate group and the group of rational points for some modular abelian varieties. *Algebra i Analiz*, 1(5):171–196, 1989.

[Kol07] VA Kolyvagin. Euler systems. In *The Grothendieck Festschrift*, pages 435–483. Springer, 2007.

[MTT86] Barry Mazur, John Tate, and Jeremy Teitelbaum. On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer. *Inventiones Mathematicae*, 84(1):1–48, 1986.

[MW84] Barry Mazur and Andrew Wiles. Class fields of abelian extensions of $\mathbb{Q}$. *Inventiones Mathematicae*, 76(2):179–330, 1984.

[Oli88] Robert Oliver. *Whitehead groups of finite groups*, volume 132. Cambridge University Press, 1988.

[Ros95] Jonathan Rosenberg. *Algebraic K-theory and its applications*, volume 147. Springer Science & Business Media, 1995.

[Rub91] Karl Rubin. The main conjectures of Iwasawa theory for imaginary quadratic fields. *Inventiones Mathematicae*, 103(1):25–68, 1991.

[RW06] Jürgen Ritter and Alfred Weiss. Toward equivariant Iwasawa theory, iii. *Mathematische Annalen*, 336(1):27–49, 2006.

[Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Inventiones mathematicae*, 15(4):259–331, 1972.

[Ser12] Jean-Pierre Serre. *Linear representations of finite groups*, volume 42. Springer Science & Business Media, 2012.

[Sil09] Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106. Springer Science & Business Media, 2009.

[SU14] Christopher Skinner and Eric Urban. The Iwasawa main conjectures for GL_2. *Inventiones Mathematicae*, 195(1):1–277, 2014.

[Sut16] Andrew V Sutherland. Computing images of galois representations attached to elliptic curves. In *Forum of Mathematics, Sigma*, volume 4. Cambridge University Press, 2016.

[SV10] Peter Schneider and Otmar Venjakob. Localizations and completions of skew power series rings. *American journal of mathematics*, 132(1):1–36, 2010.

[Was97] Lawrence C Washington. *Introduction to cyclotomic fields*, volume 83. Springer Science & Business Media, 1997.

[Wil90] Andrew Wiles. The Iwasawa main conjecture for totally real fields. *Annals of Mathematics*, 131(3):493–540, 1990.