Non-Commutative Iwasawa Theory for d-Fold False Tate Extensions

Lloyd Christopher Peters

Submitted in total fulfilment of the requirements of the degree of

Doctor of Philosophy

School of Mathematical Sciences
MONASH UNIVERSITY

January 2014

1 Errata/Addendum

Page	Line	Amendments/Comments
2	-10	Replace "in the sense of Milnor" with "in the sense of Bass"
12	-2	"*Ind*" should not be italic
13	-4	Increase space between | and l in "$V_l(E)\,\vert l$"
25	-5	Replace "cyclotomic fields" with "cyclotomic field"
29	11	Replace "co-efficients" with 'coefficients" here, on $p86$, line -4, and $p102$, line -11. Similarly replace 'co-efficient" with 'coefficient" on $p100$, line 13
30	2	Replace "Let U be a subgroup of G" with "Let U be a subgroup of finite index in G"
30	3	Replace "The trace map is defined on an arbitrary conjugacy class $[g] \in \mathrm{Conj}(G)$ in the following way:" with "The trace map, $\mathrm{Tr}_{G/U} : \mathrm{Conj}(G) \longrightarrow \mathrm{Conj}(U)$, acting on an arbitrary conjugacy class $[g] \in \mathrm{Conj}(G)$, is defined in the following way:"
30	6	Replace $G_n^{(d)}/U$ with G/U, and "The trace map $\mathrm{Tr}_{G/U}$" with "Further, $\mathrm{Tr}_{G/U}$"
38	-1	Replace "τ_i" with "τ_j", and "S_χ" with "$\mathfrak{S}_m$". Note that the definition of the trace map here is an application of the definition on $p30$
45		Note that $\mathcal{S}_m^{(\mathcal{A})}$ is as on $p41$
86	3	Replace "Focussing" with "Focusing"
89	4	Replace "$*$" with "$\times$"
103	9	Replace "$E15a1$" with "$E15A1$" here, and every subsequent occurance in section 8.2.2. Similarly replace "$E21a1$" with "$E21A1$", "$E30a1$" with "$E30A1$", "$E33a1$" with "$E33A1$", "$E35a1$" with "$E35A1$", "$E55a1$" with "$E55A1$", "$E65a1$" with "$E65A1$", and "$E70a1$" with "$E70A1$" in every occurance in section 8.2.2
104	1	Replace "Dokchitsers" with "Dokchitser's "
114	1	Replace "*MathÃl'matiques*" with "*Mathématiques*", and "*ÃL'tudes*" with "*Études*"

E-thesis Copyright Notices

Abstract

For the $(d+1)$-dimensional Lie group $G = \mathbb{Z}_p^\times \ltimes \mathbb{Z}_p^{\oplus d}$, we determine through the use of p-power congruences, a necessary and sufficient set of conditions whereby a collection of abelian p-adic L-functions arises from an element in $K_1\big(\mathbb{Z}_p[\![G]\!]\big)$. We construct an additive theta map which produces additive p-power congruences, and then using the Taylor Oliver logarithm, we arrive at a multiplicative version of these congruences.

If E is a semistable elliptic curve over $\mathbb{Q}$ with good ordinary reduction at p, the abelian p-adic L-functions already exist, therefore one can predict many new families of higher order congruences. The first layer congruences are then verified computationally in a variety of cases.

The final chapter contains computations for elliptic curves with bad multiplicative reduction at p, that the author performed for Delbourgo and Lei in [10]. All of the computations were done using the package MAGMA.

Declaration

This is to certify that

1 Parts of Chapters 1 and 3-7 of the thesis comprise joint work with Delbourgo in [11], and the rest of the thesis is my original work,
2 due acknowledgement has been made in the text to all other material used,
3 the thesis is less than 100,000 words in length, exclusive of tables, maps, bibliographies and appendices.

Lloyd Christopher Peters, January 2014

Acknowledgements

First and foremost, I give all praise to my God who blessed me with the opportunity, ability, resources, and motivation to undertake and complete this PhD!

Secondly, I am indebted to my supervisor, Daniel Delbourgo, who has provided invaluable support and guidance throughout my PhD, and for helping me grasp the abstract world of Iwasawa theory after having only been introduced to it in my PhD. Thank you, Daniel, for remaining committed after your move to Waikato University through our weekly Skype chats. I also thank you and Kathrine for your incredible hospitality during my two visits to you in New Zealand. It is cool to have a supervisor with whom I can have barbecues and chat cricket.

A big thank you to my co-supervisor, Tom Hall, for his words of wisdom and help with proof-reading, which was a support and encouragement during the course of my PhD.

I am so grateful to Tom Ward for providing me with his MAGMA code, for explaining complex concepts of Iwasawa theory, and for his support during my trip to Bristol University. Antonio Lei, I cannot thank you enough for taking so much out of your time to help fill in the gaps of my understanding of Iwasawa theory. I thank you both for your friendship and continued advice.

I would also like to thank the Univeristy of Sydney for providing me with a free developers licence for the package MAGMA, without which the computations in this thesis would have been impossible to obtain.

To my beautiful wife, Adele: thank you for providing support, advice, and strength during the tough times of this PhD, for being the backbone at home that enabled me to complete this PhD, and for helping with proof-reading. Seth, my 11-month darling son, you have been my motivation since you have arrived, and your smiles have added sunshine to my writing-up.

To my parents and brother, Haldane: thank you for your continued love, care, sacrifice, and unwavering support throughout my life, which has helped me to embark on this PhD. You can certainly take much credit in this success.

Finally, I would like to thank the staff and students at Monash University for their help and encouragement in the last four years, which has made it a joy to come in to university.

Contents

1 Introduction **1**

1.1 Notation 8

2 Background **11**

2.1 Artin Representations 11

2.2 The L-function of an Elliptic Curve and its Twists 13

2.2.1 L-function of an Elliptic Curve 13

2.2.2 Artin Twists of L-functions of Elliptic Curves 15

2.3 The Canonical Ore Set 16

2.4 Selmer Groups and their Pontryagin Duals 18

2.5 K-theory and Characteristic Elements 19

2.5.1 K_0 of a Ring 20

2.5.2 K_1 of a Ring 20

2.5.3 Characteristic Elements 22

2.6 The Evaluation at ρ Map 23

2.7 The GL_2-Main Conjecture 25

2.8 Norm and Trace Maps in K-Theory 27

2.8.1 Norm Maps 28

2.8.2 Trace Maps 30

2.9 The Taylor-Oliver p-Adic Integral Logarithm 30

3 The Behaviour of $G_\infty^{(d)}$–Representations **33**

3.1 Combinatorics of $G_n^{(d)}$–Representations 34

4 Describing the Image of Θ^+ **45**

5 The Multiplicative Setting **55**

5.1 Three Technical Lemmas 58

5.2 A Proof of Theorem 5.0.21 64

6 Evaluation at Multiplicative Characters χ **69**

6.1 The Proof of Theorem 6.0.1 71

6.2 The Proof of Theorem 1.0.2 80

7 An Application to Elliptic Curves **83**

7.1 The Proof of Theorem 1.0.6 84

7.2 The Proof of Proposition 1.0.7 85

7.3 A Worked Example 86

7.4 Numerical Results for $d = 2$ and $n = 1$ 89

8 Computations on Elliptic Curves with Bad Reduction **99**

8.1 Non-Commutative Iwasawa Theory of Elliptic Curves with Semistable Reduction 99

8.2 The Numerical Calculations 101

8.2.1 Numerical Examples 103

8.2.2 Tables 105

1 Introduction

The connection between ideal class groups and the special values of L-functions has it origins in the work of Ernst Kummer in the nineteenth century. However, the topic really took off in the mid-twentieth century through the seminal work of Kenkichi Iwasawa. His so called "Main Conjecture" gives a deep relationship between two important objects, attached to a number field K:

- p-adic L-functions (which interpolate special values of Hecke L-functions over K), and
- certain Galois modules attached to towers of ideal class groups over K.

In the case $K = \mathbb{Q}$, the Iwasawa Main Conjecture was proven by Mazur and Wiles [26]. Rubin subsequently found a more elementary proof using Euler systems (which is documented in the Appendix of [25] and Chapter 15 of [39]). Wiles later extended his proof [41] to number fields K which are totally real, whilst Rubin [29] used the Euler system of elliptic units to prove the conjecture over imaginary quadratic fields K.

Let p be a prime number, K_∞/K be a p-adic Lie extension, and write G_∞ for the Galois group of K_∞ over K. If G_∞ is commutative (the abelian case) and K_∞ is a union of totally real fields, then the Iwasawa Main Conjecture is straightforward to formulate. Unfortunately, when G_∞ is not commutative (the non-abelian case) then significant problems arise even to formulate such a conjecture. Worse still, if K_∞ is not totally real then there are no p-adic L-functions to play with, which means one must avoid these extensions completely.

In 2005, a significant breakthrough occurred in the non-abelian case. Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication, and suppose K_∞ is the field of definition of all p-power torsion points on E. Then $K_\infty/\mathbb{Q}$ is a p-adic Lie

extension, and $G_\infty = \mathrm{Gal}(K_\infty/\mathbb{Q})$ is a open normal subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$. Coates, Fukaya, Kato, Sujatha, and Venjakob in [7] managed to formulate the Iwasawa Main Conjecture for E/K_∞, by using new ideas from K-theory and homological algebra.

In this thesis, we will develop a non-commutative Iwasawa theory for Lie extensions K_∞/K where $G_\infty = \mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p^\times \ltimes \mathbb{Z}_p^{\oplus d}$. Fix a prime $p \neq 2$, and a positive integer d. We also choose p-power free integers $\Delta_1, \ldots, \Delta_d > 1$ which are pairwise co-prime, and write $\underline{\Delta}$ for the product $\prod_{i=1}^d \Delta_i$. The d-fold false Tate curve tower

$$\mathbb{Q}^{(d)}_{\infty,\underline{\Delta}} := \bigcup_{n\geq 1} \mathbb{Q}\Big(\mu_{p^n}, \Delta_1^{1/p^n}, \ldots, \Delta_d^{1/p^n}\Big)$$

is normal over $\mathbb{Q}$, and has the structure of a $(d+1)$-dimensional p-adic Lie extension. Its Galois group is isomorphic to the semi-direct product

$$G^{(d)}_\infty := \mathrm{Gal}\big(\mathbb{Q}^{(d)}_{\infty,\underline{\Delta}}/\mathbb{Q}\big) \cong \Sigma_\infty \ltimes H^{(d)}_\infty$$

where $H^{(d)}_\infty$ is a free $\mathbb{Z}_p$-module of rank d, and $\Sigma_\infty = \mathrm{Gal}\big(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}\big)$ acts on $H^{(d)}_\infty$ through the cyclotomic character.

The Iwasawa algebra $\mathbb{Z}_p\big[\big[G^{(d)}_\infty\big]\big]$ is given by the projective limit $\varprojlim_{\mathcal{P}} \mathbb{Z}_p\big[G^{(d)}_\infty/\mathcal{P}\big]$ where the inverse system of $\mathcal{P}$'s range over normal subgroups of finite index in $G^{(d)}_\infty$. For a ring R we denote by $K_1(R)$ its first algebraic K-group, in the sense of Bass. There are three main objectives in this thesis:

(I) To describe $K_1\big(\mathbb{Z}_p[\![G^{(d)}_\infty]\!]\big)$ and its localisations, via p-power congruences;

(II) To work out these congruences for a family of abelian p-adic L-functions;

(III) To numerically verify the predicted congruences in explicit examples.

We should point out that (I) is already fully solved when $d = 1$ thanks to the results of Kato [24], so our theorems here generalise his method to the $d > 1$ situation. There already exists a large body of work due to Kakde, Hara, Ritter and Weiss [8, 20, 22, 28] devoted to the study of non-abelian Iwasawa Main Conjectures. The extensions we are considering differ from the 'admissible extensions'

in [8] in two important ways:

(a) $\mathbb{Q}_{\infty,\underline{\Delta}}^{(d)}$ is not a union of totally real fields, and

(b) its Galois group $G_\infty^{(d)}$ is not pro-p.

Part (a) obstructs the formulation of an Iwasawa Main Conjecture, as nobody has yet constructed abelian p-adic L-functions in this setting. Part (b) is not so serious. Another point of departure from [8] is that the congruences derived by Kakde, Hara, Ritter-Weiss are described in terms of ideals inside completed group algebras, whereas the congruences derived here (and by Kato in [24]) are p-adic in flavour. While neither approach is better than the other, in terms of checking congruences via a computer program, the latter is the only one that can be easily implemented (and even then, numerous computational headaches arise).

Remark 1.0.1. *(i) As no Main Conjecture can be formulated over $\mathbb{Q}_{\infty,\underline{\Delta}}^{(d)}$ for Tate motives, the next obvious place to look for examples is from the theory of elliptic curves. Bouganis and Delbourgo-Ward [3,12,13] have constructed families of p-adic L-functions inside the algebras $\mathbb{Z}_p[\![U^{(m)}]\!] \otimes \mathbb{Q}$, where $U^{(m)} = \mathrm{Gal}\big(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}(\mu_{p^m})\big)$.*
(ii) Some weak congruences were established under technical hypotheses in op. cit., partly inspired by the numerical evidence of the Dokchitser brothers [17].

Following the seminal work of Kakde [8,22] there is now a precise recipe that, in principle, allows one to describe $K_1(-)$ of a non-commutative Iwasawa algebra. To construct theta-maps, one needs a 'dense enough' family of subgroups for $G_\infty^{(d)}$. In Chapter 5 we build homomorphisms

$$\theta_m : K_1\Big(\mathbb{Z}_p\big[\big[G_\infty^{(d)}\big]\big]\Big) \longrightarrow K_1\Big(\mathbb{Z}_p\big[\big[U^{(m)} \times H_\infty^{(d)}/p^m\big]\big]\Big) \quad \text{at each } m \geq 0,$$

by applying the appropriate norm map, and then quotienting out the commutator. Given any multiplicative character $\chi : H_\infty^{(d)} \to \mathbb{C}_p^\times$ of finite order p^v with $v \leq m$, one next forms the composition

$$\chi \circ \theta_m : K_1\big(\mathbb{Z}_p[\![G_\infty^{(d)}]\!]\big) \longrightarrow K_1\big(\mathcal{O}_{\mathbb{C}_p}[\![U^{(m)}]\!]\big) \;\cong\; \mathcal{O}_{\mathbb{C}_p}[\![U^{(m)}]\!]^\times.$$

The coefficient ring for the image of $\chi \circ \theta_m$ is in fact $\mathbb{Z}_p$, and the homomorphism $\chi \circ \theta_m$ depends only on $\mathcal{J} = \mathrm{Ker}(\chi)$. We therefore relabel $\chi \circ \theta_m$ simply with $\theta_{\mathcal{J}}$.

Notations: (a) Let us denote by $\mathcal{Z}_\infty^{(v)}$ the finite set of subgroups $\mathcal{J} < H_\infty^{(d)}$ such that the quotient group $H_\infty^{(d)}/\mathcal{J}$ is cyclic of order p^v, and set $\mathcal{Z}_\infty = \bigcup_{v \geq 0} \mathcal{Z}_\infty^{(v)}$.

(b) If $\mathcal{J} = \mathrm{Ker}(\chi)$ for a character χ on $H_\infty^{(d)}$, we write $\widetilde{\mathcal{J}}$ for the subgroup $\mathrm{Ker}(\chi^p)$.

(c) The full theta-mapping refers to the collection of homomorphisms $\prod_{\mathcal{J} \in \mathcal{Z}_\infty} \theta_{\mathcal{J}}$. For a fixed $x \in K_1\big(\mathbb{Z}_p[\![G_\infty^{(d)}]\!]\big)$ and subgroup $\mathcal{J} \in \mathcal{Z}_\infty^{(v)}$, each element $a_{v,\mathcal{J}} = \theta_{\mathcal{J}}(x)$ belongs inside $\mathbb{Z}_p[\![U^{(v)}]\!]^\times$. One can then turn the situation on its head, by asking:

Question Given a collection of $a_{v,\mathcal{J}}$'s, under what conditions does there exist a global element $x \in K_1\big(\mathbb{Z}_p[\![G_\infty^{(d)}]\!]\big)$ such that $a_{v,\mathcal{J}} = \theta_{\mathcal{J}}(x)$ at each $\mathcal{J}$?

If $d = 1$, Kato provided a complete answer in Section 3 of [24] by using p-power congruences. For the case $d > 1$ we shall adopt a hybrid approach, mixing together his original p-adic method with the powerful logarithmic techniques in [20, 22, 28].

First we need some notation. For each $m > 0$, let $\varphi : \mathbb{Z}_p[\![U^{(m)}]\!] \to \mathbb{Z}_p[\![U^{(m+1)}]\!]$ denote the extension of the p-power map on $U^{(0)}$. Secondly if $v \leq m$, we shall write

$$N_{v,m} : \mathbb{Z}_p[\![U^{(v)}]\!] \longrightarrow \mathbb{Z}_p[\![U^{(m)}]\!]$$

to indicate the norm map on algebras, induced from the inclusion $U^{(m)} \hookrightarrow U^{(v)}$. Choose an integer $m \geq 1$. We introduce congruences (1.1m,$\underline{\mathfrak{h}}$) and (1.2m,id) as follows:

- for a non-trivial cyclic subgroup $\langle \underline{\mathfrak{h}} \rangle \subset H_\infty^{(d)}/p^m$ of exponent $p^{\nu(\underline{\mathfrak{h}})}$,

$$\prod_{v=1}^{m} \prod_{\substack{\mathcal{J} \in \mathcal{Z}_\infty^{(v)}, \\ \underline{\mathfrak{h}} \in \mathcal{J}/p^m H_\infty^{(d)}}} N_{v,m}\big(\mathfrak{c}_J\big)^{p^v} \equiv \prod_{v=1}^{m} \prod_{\substack{\mathcal{J} \in \mathcal{Z}_\infty^{(v)}, \\ \underline{\mathfrak{h}}^p \in \mathcal{J}/p^m H_\infty^{(d)}}} N_{v,m}\big(\mathfrak{c}_J\big)^{p^{v-1}} \mod p^{m(d+1)-\nu(\underline{\mathfrak{h}})}; \quad (1.1\mathrm{m},\underline{\mathfrak{h}})$$

• similarly, at the trivial subgroup we have

$$\prod_{v=1}^{m} \prod_{\mathcal{J} \in \mathcal{Z}_\infty^{(v)}} N_{v,m}\big(\mathfrak{c}_J\big)^{p^v} \;\equiv\; 1 \mod p^{m(d+1)} \tag{1.2m,id}$$

where for each $\mathcal{J} \in \mathcal{Z}_\infty^{(v)}$, one defines $\mathfrak{c}_J := \frac{a_{v,\mathcal{J}}}{N_{0,v}\left(a_{0,H_\infty^{(d)}}\right)} \times \frac{\varphi \circ N_{0,v-1}\left(a_{0,H_\infty^{(d)}}\right)}{\varphi\left(a_{v-1,\tilde{\mathcal{J}}}\right)}$.

The following statement constitutes the main algebraic result derived in this thesis.

Theorem 1.0.2. *A collection of elements $a_{\mathcal{J}} = a_{v,\mathcal{J}} \in \mathbb{Z}_p[\![U^{(v)}]\!]^\times$ lies in the image of $K_1\big(\mathbb{Z}_p[\![G_\infty^{(d)}]\!]\big)$ under the theta-map, if and only if for all positive integers m:*
(i) the congruence (1.1m,$\underline{\mathfrak{h}}$) *holds at each non-trivial cyclic subgroup $\langle \underline{\mathfrak{h}} \rangle \subset H_\infty^{(d)}/p^m$;*
(ii) the congruence (1.2m,id) *holds.*
Furthermore, the kernel of the theta-map is isomorphic to the group $\mu_{p-1} \times \Sigma_\infty$.

There is a localised version of this theorem which works in the following manner. Let $\mathcal{S}$ denote a canonical Ore set in the sense of [7], and put $\mathcal{S}^* = \bigcup_{n \geq 0} p^n \mathcal{S}$. Then a *necessary* set of conditions for a system of $a_{v,\mathcal{J}} \in \mathbb{Z}_p[\![U^{(v)}]\!][p^{-1}]$ to belong to the image of $K_1\big(\mathbb{Z}_p[\![G_\infty^{(d)}]\!]_{\mathcal{S}^*}\big)$ under the $\mathcal{S}^*$-localisation of the theta-map $\prod \theta_{\mathcal{J}}$, is that the associated $\mathfrak{c}_J$'s satisfy the congruences (1.1m,$\underline{\mathfrak{h}}$) and (1.2m,id) for $m \geq 1$.

Conjecture 1.0.3. *The family of congruences* (1.1m,$\underline{\mathfrak{h}}$) *and* (1.2m,id) *is also sufficient to determine whether the elements $a_{v,\mathcal{J}} \in \mathbb{Z}_p[\![U^{(v)}]\!][p^{-1}]$ arise from $K_1\big(\mathbb{Z}_p[\![G_\infty^{(d)}]\!]_{\mathcal{S}^*}\big)$.*

As already occurred with the $d = 1$ situation studied in [24], we have been unable to establish the sufficiency of these p-power congruences, and unfortunately the conjecture remains unresolved at this point (though almost certainly it is true).

For a fixed value of $d > 1$, the number of cyclic subgroups of $H_\infty^{(d)}/p^m$ is of type $O\big(p^{m(d-1)}\big)$ so the system of congruences to be checked will grow rapidly with m. However if $d = 1$, the system of congruences only grows linearly as a function of m. If $d = 2$ then we are dealing with the three-dimensional Lie

group $G_\infty^{(2)} \cong \mathbb{Z}_p^\times \ltimes \mathbb{Z}_p^2$, and the result below has some surprising implications for Hasse-Weil L-functions.

Corollary 1.0.4. *If $d = 2$ and $m = 1$, then* (1.1m,$\underline{\mathfrak{h}}$) *and* (1.2m,id) *are equivalent to*

(i) $\big(a_{1,\langle \underline{\mathfrak{h}} \rangle}\big)^p \equiv N_{0,1}\big(a_{0,H_\infty^{(d)}}\big)^p \mod p^2$, *and*

(ii) $\prod_{\mathcal{J},\,[H_\infty^{(d)}:\mathcal{J}]=p}\big(a_{1,\mathcal{J}}\big)^p \equiv N_{0,1}\big(a_{0,H_\infty^{(d)}}\big)^{p(p+1)} \mod p^3$, *respectively.*

Suppose that E denotes an elliptic curve defined over $\mathbb{Q}$, and let $p \neq 2$ be a prime of good ordinary reduction. The Hecke polynomial of E at p factorises into

$$X^2 - a_p(E)X + p \;=\; (X-u)(X-w) \quad \text{where } u \in \mathbb{Z}_p^\times \text{ and } w = p/u.$$

We shall write $\Omega_E^+ \in \mathbb{R}$ and $\Omega_E^- \in \sqrt{-1}\cdot\mathbb{R}$ for the real and imaginary periods associated to a minimal Weierstrass equation for E over the integers.

Definition 1.0.5. *Given an Artin representation $\tau : G_\infty^{(d)} \to \mathrm{GL}(V)$ of conductor $\mathfrak{f}_\tau$, one defines the algebraic L-value associated to $h^1(E)\otimes\tau$ by*

$$\mathcal{L}_{E,\underline{\Delta}}(\tau) \;:=\; \frac{L_{v\nmid p\underline{\Delta}}(E,\tau,1)}{(\Omega_E^+)^{\dim(\tau^+)}(\Omega_E^-)^{\dim(\tau^-)}}\cdot\epsilon_p(\tau)\cdot\frac{L_p(\tau^*,u^{-1})}{L_p(\tau,w^{-1})}\cdot u^{-\mathrm{ord}_p(\mathfrak{f}_\tau)}$$

which is $\mathbb{Q}(\tau)$-rational by a result of Bouganis and Dokchitser [4] (Theorem 4.2).

Here $\epsilon_p(\tau)$ is the local epsilon factor at p for the representation τ (see [36] for details). Henceforth assume that E is semistable, that its conductor N_E is coprime to $\underline{\Delta}$, and fix an embedding $\iota_p : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$. The next statement modifies Theorem 1.1 in [12].

Theorem 1.0.6. *Each character $\chi : H_\infty^{(d)} \twoheadrightarrow \mu_{p^v} \hookrightarrow \mathbb{C}^\times$ extends uniquely to $G_{\mathbb{Q}(\mu_{p^v})}$, and there exists $\mathbf{L}_p(E,\mathcal{J}) \in \mathbb{Z}_p[\![U^{(v)}]\!][p^{-1}]$ with $\mathcal{J} = \mathcal{J}(\chi,v) := \mathrm{Ker}(\chi)$, satisfying*

$$\psi\big(\mathbf{L}_p(E,\mathcal{J})\big) \;=\; \iota_p\Big(\mathcal{L}_{E,\underline{\Delta}}\big(\psi\otimes\mathrm{Ind}_{\mathbb{Q}(\mu_{p^v})}^{\mathbb{Q}}(\chi)\big)\Big)$$

at all finite order characters $\psi : U^{(v)} \to \mathbb{C}^\times$.

Note that every Artin representation τ which factors through the Galois group $G_\infty^{(d)}$ can be decomposed into a direct sum of $\psi \otimes \mathrm{Ind}(\chi)$'s, each of which is irreducible.

For simplicity we now consider the case $d = 2$; over the first layer $m = 1$,

$$\mathrm{Gal}\Big(\mathbb{Q}\big(\mu_p, \Delta_1^{1/p}, \Delta_2^{1/p}\big)/\mathbb{Q}(\mu_p)\Big) \;\cong\; H_\infty^{(2)}/p \;=\; \mathbb{F}_p \oplus \mathbb{F}_p.$$

If we define $\chi_{\Delta_j} : G_{\mathbb{Q}} \twoheadrightarrow \mathrm{Gal}\big(\mathbb{Q}\big(\mu_p, \Delta_j^{1/p}\big)/\mathbb{Q}(\mu_p)\big) \twoheadrightarrow \mu_p$ by sending $\sigma \mapsto \frac{\sigma\left(\Delta_j^{1/p}\right)}{\Delta_j^{1/p}}$, the characters $\big\{\chi_{\Delta_1}^s \chi_{\Delta_2}^t \;\big|\; s,t \in \mathbb{Z}\big\}$ form a basis of the dual $\mathrm{Hom}\big(H_\infty^{(2)}/p\;, \overline{\mathbb{Q}}\big)$. Moreover each $\chi_{\Delta_1}^s \chi_{\Delta_2}^t$ is anticyclotomic, so that $\rho_{\chi_{\Delta_1}^s \chi_{\Delta_2}^t} := \mathrm{Ind}_{\mathbb{Q}(\mu_p)}^{\mathbb{Q}}\big(\chi_{\Delta_1}^s \chi_{\Delta_2}^t\big)$ will be realisable over the rational numbers, and thus $\mathcal{L}_{E,\underline{\Delta}}\big(\rho_{\chi_{\Delta_1}^s \chi_{\Delta_2}^t}\big) \in \mathbb{Q}$. Note that the dimension of $\rho_{\chi_{\Delta_1}^s \chi_{\Delta_2}^t}$ is $p-1$.

Proposition 1.0.7. *If the elements $\mathbf{L}_p(E, \mathcal{J}) \in \mathbb{Z}_p[\![U^{(v)}]\!][p^{-1}]$ lie in the image of $\prod \theta_{\mathcal{J}}\left(K_1\big(\mathbb{Z}_p[\![G_\infty^{(2)}]\!]_{\mathcal{S}^*}\big)\right)$, their constant terms satisfy the first layer congruences:*

$$\mathcal{L}_{E,\underline{\Delta}}\big(\rho_{\chi_{\Delta_1}\chi_{\Delta_2}^t}\big)^p \times \prod_{j=0}^{p-2} \mathcal{L}_{E,\underline{\Delta}}\big(\omega^j\big)^{-p} \equiv 1 \mod p^2 \quad \textit{for } t \in \{0, \cdots, p-1\}, \tag{1.3}$$

$$\mathcal{L}_{E,\underline{\Delta}}\big(\rho_{\chi_{\Delta_2}}\big)^p \times \prod_{j=0}^{p-2} \mathcal{L}_{E,\underline{\Delta}}\big(\omega^j\big)^{-p} \equiv 1 \mod p^2, \tag{1.4}$$

$$\left(\mathcal{L}_{E,\underline{\Delta}}\big(\rho_{\chi_{\Delta_2}}\big) \times \prod_{t=0}^{p-1} \mathcal{L}_{E,\underline{\Delta}}\big(\rho_{\chi_{\Delta_1}\chi_{\Delta_2}^t}\big)\right)^p \times \prod_{j=0}^{p-2} \mathcal{L}_{E,\underline{\Delta}}\big(\omega^j\big)^{-p(p+1)} \equiv 1 \mod p^3. \tag{1.5}$$

The congruences (1.3), (1.4), (1.5) follow directly from Corollary 1.0.4 and Theorem 1.0.6, upon evaluating the p-adic avatars $a_{1,\mathcal{J}} = \mathbf{L}_p(E, \mathcal{J})$ at the trivial character $\psi = \mathbf{1}$. By undertaking various computer calculations, we have numerically verified them for the following elliptic curves and parameter choices:

- the elliptic curve $E = 11A3$, the prime $p = 3$, and (Δ_1, Δ_2) in the list

$$(2,5),\quad (2,7),\quad (2,13),\quad (2,17),\quad (2,19),\quad (2,23),\quad (2,31),\quad (2,37),$$

$$(2,41),\quad (5,7),\quad (5,13),\quad (5,17),\quad (5,19),\quad (5,23),\quad (7,13),\quad (7,17);$$

- the elliptic curve $E = 77C1$, $p = 3$ and $(\Delta_1, \Delta_2) = (2,5)$, $(2,13)$ or $(5,13)$;
- the elliptic curve $E = 19A3$, $p = 5$ and $(\Delta_1, \Delta_2) = (2,3)$;
- the elliptic curve $E = 56A1$, $p = 5$ and $(\Delta_1, \Delta_2) = (2,3)$.

The L-values themselves are calculated in Chapter 7 using the MAGMA package. The *LSeries* routine can take a very long time to run, especially if the dimension of ρ is large. The dimension of ρ depends on p, and so computations only up to the prime 5 are feasible. Note also that a large conductor for the motive $h^1(E) \otimes \rho$ increases the time of the computation; in total these four examples represent six months work. Moreover we did not find any situations where the congruences failed to hold, within the limitations of our search range.

Here is a brief plan of the thesis. Chapter 2 contains all the necessary background material. In Chapters 3 and 4 we define the additive version of the theta-map, and use trace relations to describe its image. Then in Chapter 5 we follow the method of Kakde et al. relating the multiplicative and additive worlds via the Taylor-Oliver logarithm. The proof of Theorem 1.0.2 is completed in Chapter 6. Chapter 7 focuses on applications to L-functions of modular elliptic curves, in particular the verification of congruences (1.3)–(1.5) for the examples mentioned above, as well as the proofs of Theorem 1.0.6 and Proposition 1.0.7. The material in the final chapter focuses on elliptic curves with multiplicative reduction at p.

1.1 Notation

The following notation will be used throughout:

p	fixed odd prime
$\mathbb{N}$	set of natural numbers
$\mathbb{Q}$	field of rational numbers
$\mathbb{Z}_p$	p-adic integers
$\mathbb{Q}_p$	p-adic numbers
$\overline{\mathbb{Q}}_p$	a fixed algebraic closure of $\mathbb{Q}_p$

μ_{p^n}	the group of p^n-th roots of unity
μ_{p^∞}	union of μ_{p^n} for $n \geq 1$
K	a number field
K_v	completion of the field, K, at a place v
R_v	ring of integers of K_v
k_v	residue field of R_v
E	an elliptic curve over $\mathbb{Q}$.

We fix embeddings of $\overline{\mathbb{Q}}$ into $\overline{\mathbb{Q}_q}$ for every rational prime q, and of $\overline{\mathbb{Q}}$ into $\mathbb{C}$. The inertia subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)$ will be denoted by I_q. For an arbitrary group G, $\mathrm{Conj}(G)$ denotes the set of conjugacy classes of G.

2 Background

In order to formulate the non-commutative GL_2-Main Conjecture, Coates et al. [7] provided a definition of a characteristic element, and conjectured the existence of a non-abelian p-adic L-function. Their Main Conjecture then predicts that this characteristic element coincides with the non-abelian p-adic L-function, up to normalisation.

We therefore provide a brief account of the GL_2-Main Conjecture, and give the necessary background material (such as Selmer groups and their Pontryagin duals, the canonical Ore set used to localise an Iwasawa algebra, characteristic elements, and the evaluation at ρ map). Although we can state their conjecture in full and set up our main problem, these notions themselves are not necessary to understand the proofs. In this thesis we study $\mathbb{Z}_p^\times \ltimes \mathbb{Z}_p^{\oplus d}$-extensions, and reduce the question of existence for the non-abelian p-adic L-function into a sequence of congruence relations.

To achieve this goal we construct both additive and multiplicative theta maps. These homomorphisms utilise trace and norm maps in K-theory, which are defined in this chapter. Lastly the Taylor-Oliver p-adic logarithm is crucial when translating from the additive to the multiplicative setting, so we also give some preliminaries on this map.

2.1 Artin Representations

Let K be a number field, and $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$. Also, let q be a prime number, and write Frob_q for the Frobenius automorphism of q in $\mathrm{Gal}(\overline{\mathbb{Q}_q}/\mathbb{Q}_q)/I_q$, where I_q is the inertia subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}_q}/\mathbb{Q}_q)$.

Definition 2.1.1. *Let ρ be a finite dimensional complex representation of* $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$*, i.e.* $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/K) \longrightarrow \mathrm{GL}(V_\rho)$*, where V_ρ is a finite dimensional complex vector space. If there exists a finite extension M/K, such that ρ factors through the quotient map*

$$\mathrm{Gal}(\overline{\mathbb{Q}}/K) \twoheadrightarrow \mathrm{Gal}(M/K),$$

then ρ is called an Artin representation. Equivalently an Artin representation is a continuous homomorphism $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/K) \longrightarrow \mathrm{GL}(V_\rho)$ under the Krull topology.

Assume now that ρ is an Artin representation.

Definition 2.1.2. *The complex Artin L-function is given by the Euler product*

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

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

$$P_q(\rho, T) := \det(1 - \mathrm{Frob}_q^{-1}.T|V_\rho^{I_q}) \ \in \mathbb{C}[T].$$

Artin's conjecture predicts that $L(\rho, s)$ has meromorphic continuation to the whole complex plane [1]. The completed Artin L-function, $\Lambda(\rho, s)$ (which is a product of gamma factors multiplied by $L(\rho, s)$), satisfies the functional equation

$$\Lambda(\rho, s) = \epsilon(\rho, s)\Lambda(\widehat{\rho}, 1 - s),$$

where $\widehat{\rho}$ is the contragredient representation, and $\epsilon(\rho, s)$ denotes the epsilon factor for the representation (normalised as in [14]).

Artin representations exhibit a property known as *Artin formalism*. Let K be a subfield of M, and ρ be an Artin representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/M)$. The induced representation from $\mathrm{Gal}(\overline{\mathbb{Q}}/M)$ down to $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ satisfies the identity

$$L(\rho/M, s) = L(\mathrm{Ind}_K^M \rho/K, s)$$

which Artin proved in Theorem 3.1 of [1].

2.2 The L-function of an Elliptic Curve and its Twists

We will now review how to attach an L-function to an elliptic curve, and then how to twist it by an Artin representation.

2.2.1 L-function of an Elliptic Curve

Let E be an elliptic curve defined over K, and m be a non-zero integer.

Definition 2.2.1. *The m-torsion subgroup of $E(\overline{\mathbb{Q}})$ is*

$$E[m] := \ker[m] := \left\{ P \in E(\overline{\mathbb{Q}}) \mid [m]P = O \right\}.$$

Since K has characteristic zero, from Corollary 6.4 of [32], there is a decomposition $E[m] \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$.

Definition 2.2.2. *For a fixed prime l, the l-adic Tate module of E is given by*

$$T_l(E) := \varprojlim_n E[l^n],$$

where the inverse limit is taken via the natural maps $[l] : E[l^{n+1}] \to E[l^n]$.

Since $E[l^n]$ is a $\mathbb{Z}/l^n\mathbb{Z}$-module, $T_l(E)$ has a natural structure as a $\mathbb{Z}_l$-module, and

$$T_l(E) \cong \mathbb{Z}_l \times \mathbb{Z}_l.$$

It is often more convenient to work with a $\mathbb{Q}_l$-vector space, so we set

$$V_l(E) := T_l(E) \otimes \mathbb{Q}_l \text{ and } H^1_l(E) := \mathrm{Hom}(V_l(E), \mathbb{Q}_l).$$

Consider the collection $V := \{V_l(E) \mid l \text{ is a rational prime}\}$ of l-adic representations. For any finite place v of K such that $v \nmid l$, we define the local polynomial

$$P_v(E/K, T) := \det\left(1 - \mathrm{Frob}_v^{-1} T | V_l(E)^{I_v}\right)$$

which is independent of the choice of l.

Let $q_v := \#k_v$, i.e. the cardinality of the residue field at v. Then the *Hasse-Weil* L-series for an elliptic curve defined over a number field K is given by the product

$$L(E/K, s) := \prod_v P_v(E/K, q_v^{-s})^{-1}.$$

These local polynomials $P_v(E/K, T)$ can be computed explicitly, as follows. Let K_v denote the completion of K with respect to v, R_v be the ring of integers of K_v, and k_v be the residue field of R_v. For a finite place v in K at which E has good reduction, we write $\overline{E}(k_v)$ to denote the reduced curve over the residue field at v. Lastly, define the integer

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

The local factor of the *Hasse-Weil* L-series of E/K at v is explicitly given by

$$P_v(E/K, T) = \begin{cases} 1 - a_v T + q_v T^2 & \text{if } E \text{ has good reduction at } v, \\ 1 - T & \text{if } E \text{ has split multiplicative reduction at } v, \\ 1 + T & \text{if } E \text{ has non-split multiplicative reduction at } v, \\ 1 & \text{if } E \text{ has bad reduction at } v. \end{cases}$$

It is known that the Euler product for $L(E/K, s)$ converges when $\mathrm{Re}(s) > 3/2$ (Chapter 16 of [32]).

Conjecture 2.2.3. *The Hasse-Weil L-series $L(E/K, s)$ has analytic continuation to the whole complex plane, and satisfies a functional equation relating the values s and $2 - s$ (Conjecture* 16.1 *of [32]).*

This conjecture is known to be true for elliptic curves with complex multiplication, and for modular elliptic curves. For elliptic curves with complex multiplication by the ring of integers of K, it was shown that $L(E/K, s)$ is equal to a Hecke L-series by Deuring [16] and Weil [40].

One the other hand, Wiles [42] and Taylor-Wiles [37] proved that all semistable elliptic curves are modular, which was extended by Breuil et al. [5] to all elliptic curves over $\mathbb{Q}$. Thus for elliptic curves $E/\mathbb{Q}$, we have the result that the com-

pleted L-function

$$\Lambda(E/\mathbb{Q}, s) := N_{E/K}^{s/2}(2\pi)^{-s}\Gamma(s)L(E/\mathbb{Q}, s)$$

has an analytic continuation to the whole complex plane, and satisfies the functional equation

$$\Lambda(E/\mathbb{Q}, s) = \pm\Lambda(E/\mathbb{Q}, 2-s).$$

Here $N_{E/K}$ is the conductor of E/K, and the term $\pm$ is called the sign in the functional equation.

2.2.2 Artin Twists of L-functions of Elliptic Curves

Let ρ be an Artin representation with its associated vector space V_ρ defined over the field M_ρ, and again let l be a fixed prime number. Fix some prime λ of M_ρ above l, and put $V_{\rho,\lambda} := V_\rho \otimes_{M_\rho} M_{\rho,\lambda}$ where $M_{\rho,\lambda}$ denotes the completion of M_ρ at λ. Recall from Section 2.2.1 that we had set

$$V_l(E) := T_l(E) \otimes \mathbb{Q}_l \text{ and } H_l^1(E) := \mathrm{Hom}(V_l(E), \mathbb{Q}_l).$$

Definition 2.2.4. *The complex L-function of an elliptic curve E over $\mathbb{Q}$ twisted by an Artin representation ρ is defined by the Euler product*

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

Here $P_q(E, \rho, T)$ is the polynomial

$$P_q(E, \rho, T) := \det(1 - \mathrm{Frob}_q^{-1}.T|(H_l^1(E) \otimes_{\mathbb{Q}_l} V_{\rho,\lambda})^{I_q})$$

where l is any prime number different from q.

In general, this Euler product converges only for the $\mathrm{Re}(s) > \frac{3}{2}$, and this L-function has meromorphic continuation if ρ factors through a soluble extension of $\mathbb{Q}$ (see Chapter 5 of [7]). Analytic continuation will now be assumed for $L(E, \rho, s)$ to $s = 1$ for all Artin representations ρ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

The point $s = 1$ is crucial because of Deligne's period conjecture [15], which predicts that

$$\frac{L(E,\rho,1)}{(\Omega_E^+)^{d(\rho^+)}(\Omega_E^-)^{d(\rho^-)}} \in \overline{\mathbb{Q}}$$

for all Artin representations ρ. Here Ω_E^+ and Ω_E^- denote real and complex periods associated with E, defined as

$$\Omega_E^+ := \int_{\gamma^+} \omega, \quad \Omega_E^- := \int_{\gamma^-} \omega,$$

with ω being the Néron differential associated to a fixed minimal Weierstrass equation for E over $\mathbb{Z}$. Also, γ^+ and γ^- are chosen generators for the subspaces of $H_1(E(\mathbb{C}),\mathbb{Z})$ on which complex conjugation acts by $+1$ and -1, with $d(\rho^+)$ and $d(\rho^-)$ being the respective dimensions of the $+$ and $-$ subspaces in V_ρ.

2.3 The Canonical Ore Set

In Section 2 and 3 of [7], Coates et al. prove the existence of a canonical Ore set, and use it to localise the Iwasawa algebra of the Lie group they considered. Then they were able to define characteristic elements that live in the first algebraic K-group of this localised Iwasawa algebra, so now we will review the construction of this Ore set.

A p-adic Lie group G is a group which is also a finite dimensional p-adic smooth manifold, and in which the group operations of multiplication and inversion are smooth maps. These two requirements can be combined into the single requirement that the mapping $\mu : G \times G \to G$, defined as $\mu(x,y) := x^{-1}y$, is a smooth mapping of the product manifold $G \times G$ into G. In other words, G is a topological group equipped with the p-adic topology.

Definition 2.3.1. *If G is a p-adic Lie group, then the Iwasawa algebra of G is defined as*

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

where U runs over all open normal subgroups of G.

If G is a compact p-adic Lie group, then it is well known that $\Lambda(G)$ is left and right Noetherian (Section 2 of [7]). We assume throughout that G has a closed normal subgroup H such that $G/H \cong \Gamma$, where Γ is a commutative p-adic Lie group isomorphic to $\mathbb{Z}_p$ (this is a key assumption made by Coates et al. [7]).

Motivated by the results of Venjakob [38], Coates et al. [7] constructed a canonical Ore set S in $\Lambda(G)$ as we now describe. A multiplicative set S is called a left and right Ore set if for each $s \in S$ and $r \in \Lambda(G)$, there exist $t_1, t_2 \in S$ and $\omega_1, \omega_2 \in \Lambda(G)$, such that

$$s\omega_1 = rt_1 \text{ and } \omega_2 s = t_2 r.$$

Definition 2.3.2. *Let G and H be as above. Then one defines*

$$S := \{f \in \Lambda(G) \text{ such that } \Lambda(G)/\Lambda(G)f \text{ is a finitely generated } \Lambda(H)\text{-module}\}$$

The set S is a left and right Ore set in $\Lambda(G)$, and its elements are nonzero divisors of $\Lambda(G)$ (see Theorem 2.4 of [7]). Since S is a left and right Ore set, then from the universality property of Chapter II in [34], it follows that the left and right localisation of $\Lambda(G)$ at S are isomorphic to each other. The localised Iwasawa algebra $\Lambda(G)_S$ is then a semi-local ring (see Proposition 4.2 of [7]).

Let M be a left or right $\Lambda(G)$-module. If for each $x \in M$, there exists $s \in S$, such that $s \cdot x = 0$ or $x \cdot s = 0$, according as the action is on the left or right, then we say that M is S-torsion. Since p is not an element of S we make the following:

Definition 2.3.3. *One defines $S^* := \bigcup_{n \geq 1} p^n S$, and writes $\mathcal{M}_H(G)$ for the category of all finitely generated $\Lambda(G)$-modules which are S^*-torsion.*

As p commutes with every element in $\Lambda(G)$, thus p lies in the centre of $\Lambda(G)$. Moreover, S^* is a multiplicatively closed set that is a left and right Ore set in $\Lambda(G)$, and all of whose elements are non-zero divisors.

Localisation allows a formal method to introduce denominators to $\Lambda(G)$, and we will write $\Lambda(G)_{S^*}$ for the left and right localisation of $\Lambda(G)$ at S^*, so that

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

Write $M(p)$ for the submodule of M consisting of all the elements of finite order. From Proposition 2.3 of [7] a finitely generated $\Lambda(G)$-module M will be S^*-torsion if and only if $M/M(p)$ is finitely generated over $\Lambda(H)$.

Remark 2.3.4. *The category $\mathcal{M}_H(G)$ is introduced because the characteristic element is only defined for every finitely generated $\Lambda(G)$-module M which has the property that $M/M(p)$ is finitely generated over $\Lambda(H)$.*

2.4 Selmer Groups and their Pontryagin Duals

Let L be any algebraic extension of K. For an elliptic curve E defined over K, our aim here is to introduce the Pontryagin dual of its Selmer group. Let v be any prime in L. If L is an infinite algebraic extension, then L_v denotes the union of the completions at v of all finite extensions of $\mathbb{Q}$ contained in L. If L is a finite extension of $\mathbb{Q}$, then L_v is simply the completion of L at v.

Definition 2.4.1. *The p-primary Selmer group is defined as*

$$Sel(E/L)[p^\infty] := \ker\left(H^1(L, E[p^\infty]) \longrightarrow \prod_v H^1(L_v, E(\overline{L}_v))[p^\infty]\right), \tag{2.1}$$

which sits inside the exact sequence

$$0 \longrightarrow Sel(E/L)[p^\infty] \longrightarrow H^1(L, E[p^\infty]) \longrightarrow \prod_v H^1(L_v, E(\overline{L}_v))[p^\infty].$$

Definition 2.4.2. *The Tate-Shafarevich group $Ш(E/L)$ is defined as*

$$Ш(E/L) := \ker\left(H^1(L, E(\overline{L})) \longrightarrow \prod_v H^1(L_v, E(\overline{L}_v))\right), \tag{2.2}$$

which sits inside the short exact sequence

$$0 \longrightarrow Ш(E/L) \longrightarrow H^1(L, E(\overline{L})) \longrightarrow \prod_v H^1(L_v, E(\overline{L}_v)).$$

By Kummer theory, these groups lie in the fundamental exact sequence

$$0 \longrightarrow E(L) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow \mathrm{Sel}(E/L)[p^\infty] \longrightarrow Ш(E/L)[p^\infty] \longrightarrow 0. \tag{2.3}$$

The Pontryagin dual $X(E/L)$ of a Selmer group $\mathrm{Sel}(E/L)[p^\infty]$ is defined as

$$X(E/L) := \mathrm{Hom}(\mathrm{Sel}(E/L)[p^\infty], \mathbb{Q}_p/\mathbb{Z}_p). \tag{2.4}$$

Recall now the definition of a group ring. If G is any group and R is a commutative ring, then the group ring $R[G]$ is the free R-module with basis G defined as

$$R[G] := \left\{ \sum_{g \in G} r_g g \,\middle|\, r_g \in R, r_g = 0 \text{ for all but finitely many } g \in G \right\}.$$

Here multiplication in $R[G]$ is defined by extending the product operation of the group G, and addition in $R[G]$ is defined by formal R-linear combinations of elements in G.

We are only interested in studying the scenario when the algebraic extension L is Galois over the number field K. In this scenario both $\mathrm{Sel}(E/L)[p^\infty]$ and $X(E/L)$ have a natural left $\mathrm{Gal}(L/K)$-action, which makes them into $\mathbb{Z}_p[\mathrm{Gal}(L/K)]$-modules.

2.5 K-theory and Characteristic Elements

We now recall the basics of algebraic K-theory with the aim of introducing characteristic elements, which are the algebraic objects that appear in the GL_2-Main Conjecture. The connecting homomorphism which arises from the localisation sequence in K-theory for the Ore set S^* is used to define a characteristic element ξ_M in $K_1(\Lambda(G)_{S^*})$ for any module M in $\mathcal{M}_H(G)$.

2.5.1 K_0 of a Ring

Let M be a commutative monoid. Its Grothendieck group $\mathcal{G}(M)$ has the universal property that there exists a monoid homomorphism $\gamma : M \to \mathcal{G}(M)$, such that for all abelian groups A and all monoid homomorphisms $f : M \to A$, there exists a unique group homomorphism $f_* : \mathcal{G}(M) \to A$, such that $f = f_* \circ \gamma$. That is to say, $\mathcal{G}(M)$ is universal with respect to homomorphisms of M into abelian groups.

To explicitly construct the Grothendieck group of M, we form the Cartesian product $M \times M$, and impose the equivalence relation

$$(m_1, n_1) \sim (m_2, n_2),$$

if and only if there exists $z \in M$, such that

$$m_2 + n_1 + z = m_1 + n_2 + z.$$

Let $[m_1, n_1]$ denote the equivalence class of (m_1, n_1). Then the Grothendieck group of M is given as $\mathcal{G}(M) := M \times M/\sim$, with the group operation of addition defined component-wise by

$$[m_1, n_1] + [m_2, n_2] = [m_1 + m_2, n_1 + n_2].$$

The group operation is associative, commutative, and any element of the form $[m, m]$ represents the identity. Likewise the inverse element of $[m_1, n_1]$ is $[n_1, m_1]$.

Example 2.5.1. *If $M = \mathbb{N}$, which is a monoid under addition, then $\mathcal{G}(M) \cong \mathbb{Z}$.*

Definition 2.5.2. *Let R be a ring, and consider the monoid, M, of isomorphism classes of finitely generated projective R-modules. If $[P]$ and $[Q]$ denote the isomorphism classes of P and Q, we define the monoid operation by $[P] + [Q] := [P \oplus Q]$. In particular, $K_0(R)$ denotes the Grothendieck group of this monoid, M.*

2.5.2 K_1 of a Ring

Let R be any ring, and let $\mathrm{GL}(n, R)$ be the general linear group consisting of $n \times n$ invertible matrices over R. For any matrix A in $\mathrm{GL}(n, R)$ there is an injection

$$\iota : \mathrm{GL}(n,R) \to \mathrm{GL}(n+1,R)$$
$$A \longmapsto \left(\begin{smallmatrix} A & 0 \\ 0 & 1 \end{smallmatrix}\right),$$

which sends $A \in \mathrm{GL}(n,R)$ to $\left(\begin{smallmatrix} A & 0 \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{GL}(n+1,R)$. This gives rise to an infinite sequence

$$\mathrm{GL}(1,R) \xrightarrow{\iota} \mathrm{GL}(2,R) \xrightarrow{\iota} \mathrm{GL}(3,R) \xrightarrow{\iota} \cdots$$

and enables us to define an infinite general linear group

$$\mathrm{GL}(R) := \varinjlim_{n} \mathrm{GL}(n,R).$$

To be more concrete, an element of $\mathrm{GL}(R)$ is an infinite invertible matrix that differs from the infinite identity matrix in only finitely many places.

Definition 2.5.3. *The first algebraic K-group is defined as*

$$K_1(R) := \frac{\mathrm{GL}(R)}{[\mathrm{GL}(R), \mathrm{GL}(R)]}$$

where $[\mathrm{GL}(R), \mathrm{GL}(R)]$ *denotes the commutator subgroup of* $\mathrm{GL}(R)$.

An element of $\mathrm{GL}(n,R)$ is called an elementary matrix if it coincides with the identity matrix except for a single off-diagonal entry. Let $E(n,R)$ be the subgroup of $\mathrm{GL}(n,R)$ generated by all the elementary matrices of $\mathrm{GL}(n,R)$. The natural injection ι maps $E(n,R)$ into $E(n+1,R)$ giving rise to the infinite sequence

$$E(1,R) \xrightarrow{\iota} E(2,R) \xrightarrow{\iota} E(3,R) \xrightarrow{\iota} \cdots .$$

We therefore define $E(R) := \varinjlim_{n} E(n,R)$. Whitehead's lemma (Theorem 1.13 of [27]) then tells us that $E(R) = [\mathrm{GL}(R), \mathrm{GL}(R)]$, so that $K_1(R)$ can be written as a quotient

$$K_1(R) := \frac{\mathrm{GL}(R)}{E(R)}.$$

If R is any commutative ring and $R^\times$ the multiplicative group of units of R, then the usual matrix determinant defines a surjective group homomorphism

$$\det : \mathrm{GL}(R) \longrightarrow R^\times$$

because of the property of $\det(AB) = \det(A)\det(B)$ for square matrices, and $\mathrm{GL}(1,R) \cong R^\times$. Notice that the determinant of any element in $E(R)$ is 1, and that $E(R)$ is a proper subset of the kernel of the determinant homomorphism, thus in the case of $K_1(R)$, the homomorphism det induces the homomorphism

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

This homomorphism will be composed with the norm homomorphism in a later section.

Consider the special linear group $\mathrm{SL}(n,R)$ of $n \times n$ matrices with entries in R and determinant 1, and the infinite special linear group that is defined as $\mathrm{SL}(R) := \varinjlim_n \mathrm{SL}(n,R)$, which leads us to the following:

Definition 2.5.4. *For any commutative ring R,*

$$\mathrm{SK}_1(R) := \frac{\mathrm{SL}(R)}{E(R)}.$$

This definition occurs in the proof of Theorem 1.0.2.

2.5.3 Characteristic Elements

Recall that p does not belong to S, and that the localisation of $\Lambda(G)$ at S^* satisfies

$$\Lambda(G)_{S^*} := \Lambda(G)_S \left[\frac{1}{p}\right].$$

Since $\mathcal{M}_H(G)$ is the category of finitely generated $\Lambda(G)$-modules which are S^*-torsion, there is a connecting homomorphism

$$\partial_G : K_1(\Lambda(G)_{S^*}) \longrightarrow K_0(\mathcal{M}_H(G)) \quad \text{(see Section 3 of [7] and [35]).}$$

This connecting homomorphism occurs in a long exact sequence, which in turn arises by an application of the Localisation Theorem due to Quillen. The precise long exact sequence is given by

$$\cdots K_1(\Lambda(G)) \to K_1(\Lambda(G)_{S^*}) \stackrel{\partial_G}{\to} K_0(\mathcal{M}_H(G)) \to K_0(\Lambda(G)) \to K_0(\Lambda(G)_{S^*}) \to 0.$$

Assuming G has no element of order p, then Coates et al. (in Proposition 3.4 of [7]) showed ∂_G is surjective. This naturally leads us to define a characteristic element for M, which appears in the GL_2-Main Conjecture. Recall that the class of M in $K_0(\mathcal{M}_H(G))$ is denoted by $[M]$.

Definition 2.5.5. *For each $M \in \mathcal{M}_H(G)$, a characteristic element for M is any ξ_M in $K_1(\Lambda(G)_{S^*})$, such that $\partial_G(\xi_M) = [M]$.*

2.6 The Evaluation at ρ Map

We now explain how to evaluate a characteristic element at an Artin representation ρ. The definition (Section 3 of [7]) will be reviewed under the usual condition that G is a p-adic Lie group, which contains a closed normal subgroup H, such that $G/H = \Gamma$ is isomorphic to $\mathbb{Z}_p$.

Let L be a finite extension of $\mathbb{Q}_p$, and set O to be its ring of integers. Fixing a topological generator T of Γ, then we can identify the Iwasawa algebra of Γ with the formal power series ring $\mathbb{Z}_p[[T]]$, by mapping T to $1 + T$. Write $\Lambda_O(\Gamma)$ for the O-Iwasawa algebra of Γ, which we identify with $O[[T]]$.

Assume we are given a continuous group homomorphism $\rho : G \longrightarrow \mathrm{GL}_n(O)$. By continuity the group homomorphism ρ induces a ring homomorphism $\rho : \Lambda(G) \longrightarrow M_n(O)$, and consequently a group homomorphism

$$K_1(\Lambda(G)) \longrightarrow K_1(M_n(O)) = O^\times.$$

Remark 2.6.1. *Note that O is a free $\mathbb{Z}_p$-module of finite rank, so $M_n(O) \otimes_{\mathbb{Z}_p} \Lambda_O(\Gamma) \cong M_n(\Lambda_O(\Gamma))$.*

Definition 2.6.2. *For $\sigma \in G$, write $\overline{\sigma}$ for the image of σ in $\Gamma = G/H$. Define the continuous group homomorphism $\Phi_\rho : G \longrightarrow \left(M_n(O) \otimes_{\mathbb{Z}_p} \Lambda(\Gamma)\right)^\times \cong M_n\left(\Lambda_O(\Gamma)\right)^\times$ in the following way:*

$$\Phi_\rho(\sigma) := \rho(\sigma) \otimes \overline{\sigma}, \quad \textit{where } \rho(\sigma) \in GL_n(O) \subset M_n(O).$$

By extending Φ_ρ to the whole Iwasawa algebra $\Lambda(G)$, we get the induced ring homomorphism

$$\Phi_\rho : \Lambda(G) \longrightarrow \left(M_n(O) \otimes_{\mathbb{Z}_p} \Lambda(\Gamma)\right) \cong M_n\left(\Lambda_O(\Gamma)\right). \tag{2.5}$$

Lemma 2.6.3. *(Lemma 3.3 in Coates et al. [7]) For the Iwasawa algebra localised at S^*, the homomorphism (2.5) extends to a ring homomorphism,*

$$\Phi_\rho : \Lambda(G)_{S*} \longrightarrow M_n\left(Q_O(\Gamma)\right), \tag{2.6}$$

which we also denote by Φ_ρ, where $Q_O(\Gamma)$ is the quotient field of $\Lambda_O(\Gamma)$.

Furthermore, on the level of K_1-groups (2.6) induces a homomorphism

$$\Phi'_\rho : K_1(\Lambda(G)_{S*}) \longrightarrow K_1(M_n\left(Q_O(\Gamma)\right)) \cong Q_O(\Gamma)^\times.$$

Definition 2.6.4. *Let $x = \sum_{\gamma\in\Gamma} o_\gamma \gamma$ be an element in the group ring $O[\Gamma]$. The augmentation map $\varphi : O[\Gamma] \longrightarrow O$ is defined as follows:*

$$\varphi(x) = \varphi(\sum_{\gamma\in\Gamma} o_\gamma\gamma) := \sum_{\gamma\in\Gamma} o_\gamma.$$

One can see that φ is well defined, additive, onto, and moreover it induces a map on the whole Iwasawa algebra of Γ

$$\varphi : \Lambda_O(\Gamma) \longrightarrow O.$$

Lemma 2.6.5. *The augmentation map φ is a homomorphism.*

Proof. For elements $a, b \in O[[T]]$, we have $a = \sum_{i\geq 0} o_i T^i$ and $b = \sum_{j\geq 0} s_j T^j$, where

$o_i, s_j \in O$. Applying φ on the product ab gives

$$\varphi(ab) = \varphi\left(\sum_{k\geq 0}\left(\sum_{\substack{i,j\\ i+j=k}} o_i s_j\right) T^k\right) = \sum_{k\geq 0}\sum_{\substack{i,j\\ i+j=k}} o_i s_j = \sum_{i\geq 0} o_i \sum_{j\geq 0} s_j = \varphi(a)\phi(b).$$

□

The kernel of any ring homomorphism into an integral domain is a prime ideal, and we will write $\mathfrak{p}$ for the kernel of φ. The localisation of the Iwasawa algebra of Γ at $\mathfrak{p}$ will be denoted by $\Lambda_O(\Gamma)_\mathfrak{p}$. The augmentation map φ extends naturally to a homomorphism

$$\varphi : \Lambda_O(\Gamma)_\mathfrak{p} \longrightarrow L.$$

Definition 2.6.6. *For any element ξ in $K_1(\Lambda(G)_{S^*})$, the evaluation at ρ map is defined in the following way:*

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

2.7 The GL_2-Main Conjecture

Coates et al. [7] formulated the GL_2-Main Conjecture for an elliptic curve $E/\mathbb{Q}$ over the field generated by the co-ordinates of all p-power division points, where p is a fixed prime ≥ 5 of good ordinary reduction. Before we give their construction, we recall the definition of a cyclotomic $\mathbb{Z}_p$-extension.

Let K be a number field and define $K_n := K(\mu_{p^n})$ (the p^n-th cyclotomic field) for all $n \geq 1$. Then we have a tower of Galois extensions $K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset L = \bigcup_n K_n$, such that the Galois group $\mathrm{Gal}(K_n/K)$ is isomorphic to $(\mathbb{Z}/p^n\mathbb{Z})^\times$ and is cyclic of order $p^{n-1}(p-1)$. Since

$$\mathrm{Gal}(L/K) \cong \mathbb{Z}_p^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times \times 1 + p\mathbb{Z}_p,$$

there is a unique subfield K^{cyc} of L such that $\text{Gal}(K^{\text{cyc}}/K) \cong 1 + p\mathbb{Z}_p \cong (\mathbb{Z}_p, +)$. We call K^{cyc} the cyclotomic $\mathbb{Z}_p$-extension of K.

Now instead let $K_n := \mathbb{Q}(E[p^n])$ be the field generated over $\mathbb{Q}$ by the coordinates of the p^n-torsion points of E, and put

$$K_\infty := \bigcup_{n \geq 1} \mathbb{Q}(E[p^n]) = \mathbb{Q}(E[p^\infty]).$$

Because of the Weil pairing, we have the containment $K_\infty \supset \mathbb{Q}(\mu_{p^\infty})$; in particular, K_∞ contains $\mathbb{Q}^{cyc}$. Define

$$G := \text{Gal}(K_\infty/\mathbb{Q}), \quad H := \text{Gal}(K_\infty/\mathbb{Q}^{cyc}), \text{ and } \Gamma := \text{Gal}(\mathbb{Q}^{cyc}/\mathbb{Q}).$$

Thus in this setup, G is a compact p-adic Lie group that contains a closed normal subgroup H, such that $\Gamma = G/H \cong \mathbb{Z}_p$. The Galois group G is a closed subgroup of $\text{GL}_2(\mathbb{Z}_p) \cong \text{Aut}(E[p^\infty])$, and the condition $p \geq 5$ ensures that G has no element of order p.

It is known from Serre [30] that when E admits complex multiplication G has dimension 2 inside $\text{GL}_2(\mathbb{Z}_p)$, and when E does not admit complex multiplication G has dimension 4 inside $\text{GL}_2(\mathbb{Z}_p)$. The GL_2-Main Conjecture is formulated for elliptic curves without complex multiplication over K_∞.

Let j_E denote the j-invariant of E, and set

$$R := \{p\} \bigcup \{\text{primes } q | \text{ord}_q(j_E) < 0\}.$$

Now, define

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

to be the L-function of the elliptic curve over $\mathbb{Q}$ twisted by the Artin representation ρ with the primes in R removed. Denote the conductor of ρ by N_ρ, and set

$$f_\rho := \text{ord}_p(N_\rho).$$

Since E has good ordinary reduction at p, the local polynomial $P_p(E, T)$ can be

easily factorized, which was written explicitly in section 2.2.1:

$$P_p(E,T) = 1 - a_pT + pT^2 = (1-uX)(1-wX),$$

where $u \in \mathbb{Z}_p^\times$ and $w \in p\mathbb{Z}_p$. Write $\epsilon_p(\rho)$ for the local epsilon factor of ρ at p, normalized in the same way as Deligne [14]. Let $\hat{\rho}$ be the contragredient representation of ρ, namely

$$\hat{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL(V_\rho^*),$$

where V_ρ^* is the dual of V_ρ.

Recall that $X(E/K_\infty)$ was the Pontryagin dual of $\mathrm{Sel}(E/K_\infty)[p^\infty]$ (see Section 2.4 for the definition), and $\mathcal{M}_\mathcal{H}(G)$ is the category of all finitely generated S^*-torsion modules (see Section 2.3). As before, let Ω_E^+ and Ω_E^- denote the real and complex periods of E (see Section 2.2.2).

Conjecture 2.7.1. *(Conjecture 5.7 in [7])*
Assume that $p \geq 5$ and E has good ordinary reduction at p. Then there exists $\mathcal{L}_E \in K_1(\Lambda(G)_{S^*})$, such that for all Artin representations ρ of G we have $\mathcal{L}_E(\rho)$ is finite, and

$$\mathcal{L}_E(\rho) \;=\; \frac{L_R(E,\rho,1)}{(\Omega_E^+)^{d(\rho^+)}(\Omega_E^-)^{d(\rho^+)}} \cdot \epsilon_p(\rho) \cdot \frac{P_p(\hat{\rho},u^{-1})}{P_p(\rho,w^{-1})} \cdot u^{-f_p} \tag{2.7}$$

Conjecture 2.7.2. *(GL_2-Main Conjecture: Conjecture 5.8 in [7])*
Assume that $X(E/K_\infty)$ belongs to $\mathcal{M}_H(G)$. Let ξ_E be a characteristic element for $X(E/K_\infty)$. Then given that the previous conjecture holds, the images of the non-abelian p-adic L-function $\mathcal{L}_E$ and the characteristic element ξ_E coincide modulo $K_1(\Lambda(G))$.

2.8 Norm and Trace Maps in K-Theory

Norm and trace maps are used to construct theta maps in the multiplicative and additive setting of our problem, respectively. These theta maps are essential in reducing the question of the existence for the non abelian p-adic L-function into a sequence of congruence relations amongst abelian L-functions.

2.8.1 Norm Maps

Let S be an extension ring of R, such that S is a finitely generated projective left R-module. Choose P to be a projective left R-module so that the direct sum $S \oplus P$ is free, say on k generators over R. Before defining the norm map on K_1, we must define an embedding

$$f : \mathrm{GL}_n(S) \longrightarrow GL(R).$$

Remark 2.8.1. *Because of the isomorphism* $\mathrm{GL}_n(S) \cong \mathrm{Aut}(S^n)$*, any matrix* $X \in \mathrm{GL}_n(S)$ *gives rise to S-linear automorphisms of the free module* S^n*, which we also denote by X.*

The direct sum $S^n \oplus P^n$ is also an R-module, and so we can consider the R-linear automorphism

$$X \oplus (\text{Identity map of } P^n)$$

of $S^n \oplus P^n$. Choosing a basis of R for $S^n \oplus P^n$, one can represent the automorphism $X \oplus (\text{Identity map of } P^n)$ as a matrix, which is by definition the image of X under f. Note that $f(X)$ lives in $\mathrm{GL}_{nk}(R) \subset \mathrm{GL}(R)$.

These homomorphisms, f, are independent of the choice of isomorphism $S \oplus P \cong R^k$(see Section (1d) of [27]). By abelianizing and taking the direct limit as $n \to \infty$, we obtain

$$\mathrm{Nr}_{S/R} := f : K_i(S) \longrightarrow K_i(R) \quad (i = 0, 1).$$

Let G be a group and H a subgroup of finite index. Then we have the inclusion $\mathbb{Z}_p[H] \longrightarrow \mathbb{Z}_p[G]$, and so obtain the norm map

$$\mathrm{Nr}_{\mathbb{Z}_p[G]/\mathbb{Z}_p[H]} : K_i(\mathbb{Z}_p[G]) \longrightarrow K_i(\mathbb{Z}_p[H]) \quad (i = 0, 1).$$

When G is a profinite group and H an open subgroup of G, we also write

$$\mathrm{Nr}_{\Lambda(G)/\Lambda(H)} : K_i(\Lambda(G)) \longrightarrow K_i(\Lambda(H)) \quad (i = 0, 1).$$

We will now calculate $\mathrm{Nr}_{\mathbb{Z}_p[G]/\mathbb{Z}_p[H]}(a)$ for $a \in K_1(\mathbb{Z}_p[G])$, in the setting where G is a group with a commutative subgroup H. Analogous to Proposition 1.4 part (1) in Bass's book [2], there must exist a surjective group homomorphism

$$\mathbb{Z}_p[G]^\times \longrightarrow K_1(\mathbb{Z}_p[G]); \quad b \longmapsto \tau(- \cdot b),$$

where $b \in \mathbb{Z}_p[G]^\times$, $- \cdot b$ is the automorphism of $\mathbb{Z}_p[G]$ defined by multiplication of b on the right, and τ maps $- \cdot b$ to an element in $K_1(\mathbb{Z}_p[G])$. Thus, there exists $x \in \mathbb{Z}_p[G]^\times$, where τ maps the $\mathbb{Z}_p[G]$ automorphism $- \cdot x$ to a, i.e. $\tau(- \cdot x) = a$.

Choosing a system of coset representatives $\{u_1, u_2, .., u_r\}$ for the quotient group G/H, then as H is a subgroup of G, $\mathbb{Z}_p[G]$ is a left $\mathbb{Z}_p[H]$-module with basis $\{u_1, u_2, .., u_r\}$. Each basis element multiplied by x can be written as a linear combination of the basis, where the coefficients in the linear combination live in $\mathbb{Z}_p[H]$. In other words, for $1 \leq j \leq r$,

$$u_j x = \sum_{i=1}^{r} x_{ij} u_i, \quad \text{where } x_{ij} \in \mathbb{Z}_p[H].$$

In this manner, each coset representative corresponds to a column in the matrix $(x_{ij})_{1 \leq i,j \leq r}$.

Now, from the definition of the norm homomorphism above, $\mathrm{Nr}_{\mathbb{Z}_p[G]/\mathbb{Z}_p[H]}(a)$ can be identified with the image of the matrix $(x_{ij})_{1 \leq i,j \leq r}$ in $K_1(\mathbb{Z}_p[H])$. Note that the norm homomorphism is independent of the choice of coset representatives (see Theorem 9.3 of [21]), and in the setting where G is a profinite group with a commutative open subgroup H, the same approach can be used to calculate $\mathrm{Nr}_{\Lambda(G)/\Lambda(H)}$ explicitly.

Furthermore, since H is commutative, the determinant map $K_1(\mathbb{Z}_p[H]) \to \mathbb{Z}_p[H]^\times$ is an isomorphism (Chapter IX, Proposition 1.4 of [2]). Then applying the determinant map to the norm homomorphism, one obtains

$$\det\left(\mathrm{Nr}_{\mathbb{Z}_p[G]/\mathbb{Z}_p[H]}(a)\right) = \det(x_{ij})_{1 \leq i,j \leq r} \qquad \in \mathbb{Z}_p[H]^\times.$$

2.8.2 Trace Maps

Let U be a subgroup of finite index in G. Consider the system of coset representatives $\{u_1, u_2, .., u_r\}$ of the quotient group G/U. The trace map, $\mathrm{Tr}_{G/U}$: $\mathrm{Conj}(G) \longrightarrow \mathrm{Conj}(U)$, acting on an arbitrary conjugacy class $[g] \in \mathrm{Conj}(G)$, is defined in the following way:

$$\mathrm{Tr}_{G/U}([g]) := \sum_{u_j^{-1} g u_j \in U} [u_j^{-1} g u_j],$$

namely averaging a conjugacy class over the coset representatives of G/U. Further, $\mathrm{Tr}_{G/U}$ is clearly independent of the choice of coset representatives, thus it induces the well defined R-module homomorphisms,

$$\mathrm{Tr}_{R[G]/R[U]} : R[\mathrm{Conj}(G)] \longrightarrow R[\mathrm{Conj}(U)], \text{ and}$$
$$\mathrm{Tr}_{R[[G]]/R[[U]]} : R[[\mathrm{Conj}(G)]] \longrightarrow R[[\mathrm{Conj}(U)]].$$

2.9 The Taylor-Oliver p-Adic Integral Logarithm

As with the usual logarithm over $\mathbb{R}$, p-adic logarithms transfer problems in the multiplicative setting involving units to the additive setting, which are simpler to study. The main result of this thesis, Theorem 1.0.2, is first solved in the additive setting, and then the Taylor-Oliver p-adic logarithm is used to arrive at the congruences in Theorem 1.0.2.

Throughout this section let Ω be a p-adic order, i.e. Ω is any $\mathbb{Z}_p$-algebra which is finitely generated as a free $\mathbb{Z}_p$-module. For any pair of ideals $I_1, I_2 \subseteq \Omega$, denote by $[I_1, I_2]$ the subgroup of Ω generated by elements $[a, b] = ab - ba$, for all $a \in I_1$ and $b \in I_2$.

Definition 2.9.1. *For any $x \in \Omega$, define the p-adic logarithm*

$$\mathrm{Log}(1 + x) := x - \frac{x^2}{2} + \frac{x^3}{3} - \cdots$$

whenever this series converges in $\mathbb{Q} \otimes_{\mathbb{Z}} \Omega$.

Lemma 2.9.2. *(Lemma 2.7(i) in [27]) Let $J(\Omega) \subseteq \Omega$ denote the Jacobson radical, and $I \subseteq J(\Omega)$ be any radical ideal. Set $\Omega_{\mathbb{Q}} := \mathbb{Q} \otimes_{\mathbb{Z}} \Omega = \Omega\left[\frac{1}{p}\right]$ and $I_{\mathbb{Q}} = \mathbb{Q} \otimes_{\mathbb{Z}} I = I\left[\frac{1}{p}\right]$. Then for any $x, y \in I$, $\mathrm{Log}(1+x)$ and $\mathrm{Log}(1+y)$ converge inside $I_{\mathbb{Q}}$, and satisfy the relation*

$$\mathrm{Log}((1+x)(1+y)) \equiv \mathrm{Log}(1+x) + \mathrm{Log}(1+y) \qquad \mod\ [\Omega_{\mathbb{Q}}, I_{\mathbb{Q}}].$$

Let I be any 2 sided ideal that is a subset of R. The set

$$\mathrm{GL}(R, I) := \{A \in \mathrm{GL}(R) \,|\, A \equiv \mathrm{Id} \mod I\}$$

is the group of invertible matrices which are congruent to the identity modulo I. Denote by $E(R, I)$ the smallest normal subgroup of $\mathrm{GL}(R)$ containing the elementary matrices of $\mathrm{GL}(R)$ where the off-diagonal entry that differs from the identity matrix is an element of I.

From Whitehead's lemma (Theorem 1.13 in [27]), we have the exact equality $E(R, I) = [GL(R), GL(R, I)]$, which enables us to define the abelian group

$$K_1(R, I) := \mathrm{GL}(R, I)/E(R, I).$$

Lemma 2.9.3. *(Theorem 2.8 in [27]) Let I be a subset of Ω, and $J(\Omega)$ be as above. The p-adic logarithm $Log(1+x)$ for $x \in I \bigcap J(\Omega)$, induces a homomorphism*

$$\log_I : K_1(\Omega, I) \longrightarrow \mathbb{Q} \otimes_{\mathbb{Z}} (I/[\Omega, I]).$$

For the rest of this section, let R be the ring of integers of a field extension F of $\mathbb{Q}_p$, G be a finite group, and $R[G]$ be any p-adic group ring. Assume that p is unramified in F. Note that $\log_{J(R[G])}$ can be extended uniquely to the full K-group $K_1(R[G])$ by setting

$$\log_{R[G]} a := \frac{1}{b} \log_{J(R[G])} a^b,$$

where $a \in K_1(R[G])$, $b = \#K_1(R[G]/J(R[G]))$, so that $a^b \in K_1(R[G], J(R[G]))$.

The ring of integers R is a principal ideal domain, with exactly one maximal ideal. As a result, R/pR is a field and $\mathrm{Gal}(F/\mathbb{Q}_p) \cong \mathrm{Gal}\left((R/pR)/\mathbb{F}_p\right)$. In this case, there is a unique generator $\mathrm{Frob}_p \in \mathrm{Gal}(F/\mathbb{Q}_p)$, such that for any $r \in R$ we have $\mathrm{Frob}_p(r) \equiv r^p \mod pR$ (section (6a) of [27]; [6]).

We can identify $R[G]/[R[G], R[G]]$ with the free R-module with basis $\mathrm{Conj}(G)$, and $F(R)[G]/[F(R)[G], F(R)[G]]$ with the F-vector space whose basis is $\mathrm{Conj}(G)$. In other words, there are isomorphisms $R[G]/[R[G], R[G]] \cong R[\mathrm{Conj}(G)]$, and also $F[G]/[F[G], F[G]] \cong F[\mathrm{Conj}(G)]$.

Definition 2.9.4. *Let $\varphi_G : F\,[Conj(G)] \longrightarrow F[Conj(G)]$ be the homomorphism defined by*

$$\varphi_G\left(\sum_{g\in G} k_g[g]\right) := \sum_g \mathrm{Frob}_p\left(k_g\right)[g^p],$$

where $k_g \in F$ and $[g] \in \mathrm{Conj}(G)$.

Proposition 2.9.5. *(Definition* 6.1 *and Theorem* 6.2 *in Oliver [27])*
Let F be a finite unramified extension of $\mathbb{Q}_p$, and R its integer ring. For $u \in K_1(R[G])$, if we set

$$\Gamma_G(u) := \log_{R[G]}(u) - \frac{1}{p}\varphi(\log_{R[G]}(u)) \in F[\mathrm{Conj}(G)],$$

then this induces an integral homomorphism

$$\Gamma_G : K_1(R[G]) \longrightarrow R[\mathrm{Conj}(G)]$$

henceforth called the Taylor-Oliver logarithm map.

3

The Behaviour of $G_\infty^{(d)}$–Representations

This chapter concerns the construction and basic properties of the additive theta map, which is a key player in the proof of the K_1-congruences (Theorem 1.0.2). As we shall see, the image of this homomorphism consists of sequences that are trace-compatible, a property that will be vital later on.

Throughout we adopt the convention that $\frac{1+p^0\mathbb{Z}}{1+p^n\mathbb{Z}}$ indicates the group $\left(\mathbb{Z}/p^n\mathbb{Z}\right)^\times$. Let us consider the finite semi-direct products

$$G_n^{(d)} \;:=\; \left(\mathbb{Z}/p^n\mathbb{Z}\right)^\times \ltimes \left(\mathbb{Z}/p^n\mathbb{Z}\right)^{\oplus d} \;=\; \Sigma_n \ltimes H_n^{(d)}.$$

In particular, an element $\sigma \in \Sigma_n$ acts on $H_n^{(d)}$ (through conjugation) by sending $(h_1, \ldots, h_d) \mapsto (\sigma \times h_1, \ldots, \sigma \times h_d)$. Furthermore every element $g \in G_n^{(d)}$ can be uniquely expressed as

$$g = \sigma \cdot \underline{h} \quad \text{for some } \sigma \in \Sigma_n \text{ and } \underline{h} \in H_n^{(d)}.$$

Strictly speaking the true binary operation on $H_n^{(d)} = \left(\mathbb{Z}/p^n\mathbb{Z}\right)^{\oplus d}$ should be '$+$', however we often switch notation between $+$ and the standard group multiplication on $G_n^{(d)}$, provided the context is clear.

We can also realise these objects as Galois groups, in the following manner. Let p, n, d and $\Delta_1, \ldots, \Delta_d$ be as in the Introduction, and set

$$K_n := \mathbb{Q}(\mu_{p^n}), \quad L_n := K_n(\sqrt[p^n]{\Delta_1}, \ldots, \sqrt[p^n]{\Delta_d}),$$

$$\text{so that } \Sigma_n \cong \mathrm{Gal}(K_n/\mathbb{Q}), \quad H_n^{(d)} \cong \mathrm{Gal}(L_n/K_n), \text{ and } G_n^{(d)} \cong \mathrm{Gal}(L_n/\mathbb{Q}).$$

Consequently, when we pass to the projective limit

$$\Sigma_\infty = \varprojlim_n \Sigma_n \cong \mathbb{Z}_p^\times, \quad H_\infty^{(d)} = \varprojlim_n H_n^{(d)} \cong \mathbb{Z}_p^{\oplus d}, \text{ and}$$

$$G_\infty^{(d)} = \varprojlim_n G_n^{(d)} \cong \mathbb{Z}_p^\times \ltimes \mathbb{Z}_p^{\oplus d}.$$

Here $H_\infty^{(d)}$ is a closed normal subgroup of $G_\infty^{(d)}$, and $G_\infty^{(d)}/H_\infty^{(d)} = \Sigma_\infty \cong \mathbb{Z}_p^\times$. The Galois group $G_\infty^{(d)}$ is a $(d+1)$-dimensional p-adic Lie group, and it can be identified with a matrix subgroup of $\mathrm{GL}(d+1, \mathbb{Z}_p)$.

3.1 Combinatorics of $G_n^{(d)}$–Representations

We begin by discussing some basic representation theory of the finite group $G_n^{(d)}$.

Definition 3.1.1. *For an element $\underline{\alpha} = (\alpha_1, \ldots, \alpha_d) \in (\mathbb{Z}/p^n\mathbb{Z})^{\oplus d}$, the character $\chi_{\underline{\alpha}} : H_n^{(d)} \to \mathbb{C}^\times$ is defined on all elements $\underline{h} = (h_1, \ldots, h_d) \in H_n^{(d)}$ by*

$$\chi_{\underline{\alpha}}(\underline{h}) := \exp\left(\frac{2\pi\sqrt{-1}}{p^n}\sum_{j=1}^{d}\alpha_j h_j\right).$$

Every character on $H_n^{(d)}$ into $\mathbb{C}^\times$ has this form for an appropriate choice of $\underline{\alpha}$.

Definition 3.1.2. *The stabilizer of $\chi_{\underline{\alpha}}$ in Σ_n is defined by*

$$\mathrm{Stab}_{\Sigma_n}(\chi) := \left\{\sigma \in \Sigma_n \,\middle|\, \chi_{\underline{\alpha}}(\sigma^{-1}h\sigma) = \chi_{\underline{\alpha}}(h), \forall h \in H_n^{(d)}\right\}.$$

Theorem 3.1.3. *(i) Let $\mathfrak{f}_\chi$ be a fixed integer, such that $0 \leq \mathfrak{f}_\chi \leq n$. If $\chi : H_n^{(d)} \twoheadrightarrow \mu_{p^{\mathfrak{f}_\chi}}$ then $\mathrm{Stab}_{\Sigma_n}(\chi) = \frac{1+p^{\mathfrak{f}_\chi}\mathbb{Z}}{1+p^n\mathbb{Z}}$;*

(ii) Each character χ extends to $\mathrm{Stab}_{\Sigma_n}(\chi) \ltimes H_n^{(d)}$ via the rule $\chi^\dagger(\sigma \cdot \underline{h}) = \chi(\underline{h})$;

(iii) All irreducible representations on $G_n^{(d)}$ are of the form

$$\rho_n^{(d)}(\chi, \psi) \;:=\; \mathrm{Ind}_{\mathrm{Stab}_{\Sigma_n}(\chi)\ltimes H_n^{(d)}}^{G_n^{(d)}}\left(\chi^\dagger \otimes \psi\right)$$

where $\psi : \Sigma_n \longrightarrow \mathbb{C}^\times$ is a multiplicative character;

(iv) Two representations $\rho_n^{(d)}(\chi, \psi)$ and $\rho_n^{(d)}(\chi', \psi')$ are isomorphic if and only if the character χ' lies in the Σ_n-orbit of χ, and ψ' agrees with ψ on $\mathrm{Stab}_{\Sigma_n}(\chi)$.

Proof. (i) Notice that

$$\sigma^{-1}h\sigma = \begin{pmatrix} \sigma^{-1} & 0 & 0 & 0 & \cdots & 0 \\ 0 & \sigma^{-1} & 0 & 0 & \cdots & 0 \\ 0 & 0 & \sigma^{-1} & 0 & \cdots & 0 \\ \vdots & & & \ddots & & \vdots \\ 0 & & \cdots & & \sigma^{-1} & 0 \\ 0 & & \cdots & & \cdots & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & \cdots & h_1 \\ 0 & 1 & 0 & 0 & \cdots & h_2 \\ 0 & 0 & 1 & 0 & \cdots & h_3 \\ \vdots & & & \ddots & & \vdots \\ 0 & & \cdots & & 1 & h_d \\ 0 & & \cdots & & \cdots & 1 \end{pmatrix} \begin{pmatrix} \sigma & 0 & 0 & 0 & \cdots & 0 \\ 0 & \sigma & 0 & 0 & \cdots & 0 \\ 0 & 0 & \sigma & 0 & \cdots & 0 \\ \vdots & & & \ddots & & \vdots \\ 0 & & \cdots & & \sigma & 0 \\ 0 & & \cdots & & \cdots & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 & \cdots & \sigma^{-1}h_1 \\ 0 & 1 & 0 & 0 & \cdots & \sigma^{-1}h_2 \\ 0 & 0 & 1 & 0 & \cdots & \sigma^{-1}h_3 \\ \vdots & & & \ddots & & \vdots \\ 0 & & \cdots & & 1 & \sigma^{-1}h_d \\ 0 & & \cdots & & \cdots & 1 \end{pmatrix}, \text{ which allows us to write}$$

$$\begin{aligned} \mathrm{Stab}_{\Sigma_n}(\chi) &= \left\{ \sigma \in (\mathbb{Z}/p^n\mathbb{Z})^\times \,\middle|\, \chi_{\underline{\alpha}}(h)^{\sigma^{-1}} = \chi_{\underline{\alpha}}(h), \forall h \in H_n^{(d)} \right\} \\ &= \left\{ \sigma \in (\mathbb{Z}/p^n\mathbb{Z})^\times \,\middle|\, \sum_{j=1}^{d} \sigma^{-1}\alpha_j h_j \equiv \sum_{j=1}^{d} \alpha_j h_j \mod p^n, \forall h_j \in (\mathbb{Z}/p^n\mathbb{Z}) \right\} \\ &= \left\{ \sigma \in (\mathbb{Z}/p^n\mathbb{Z})^\times \,\middle|\, \sigma^{-1}\alpha_j \equiv \alpha_j \mod p^n, \forall j = 1, \ldots, d \right\}. \end{aligned}$$

Any choice of $\underline{\alpha}$ of order $p^{\mathfrak{f}_\chi}$ produces a character $\chi_{\underline{\alpha}} : H_n^{(d)} \twoheadrightarrow \mu_{p^{\mathfrak{f}_\chi}}$. As a result $\sigma^{-1}\alpha_j \equiv \alpha_j \mod p^n$ holds only when $\sigma \in \frac{1+p^{\mathfrak{f}_\chi}\mathbb{Z}}{1+p^n\mathbb{Z}}$, therefore

$$\mathrm{Stab}_{\Sigma_n}(\chi) = \frac{1 + p^{\mathfrak{f}_\chi}\mathbb{Z}}{1 + p^n\mathbb{Z}}.$$

(ii) This is obvious from the rule $\chi^\dagger(\sigma \cdot \underline{h}) = \chi(\underline{h})$, and because χ is a character, thus $\chi^\dagger$ must be a character of $\mathrm{Stab}_{\Sigma_n}(\chi) \ltimes H_n^{(d)}$.

(iii) and (iv) are corollaries of Serre (Proposition 25, [31]). □

Proposition 3.1.4. *(a)* $\#\mathrm{Stab}_{\Sigma_n}(\chi) = \frac{\phi(p^n)}{\phi(p^{\mathfrak{f}_\chi})}$ *and* $\dim_{\mathbb{C}} \left(\rho_n^{(d)}(\chi, \psi) \right) = \phi\left(p^{\mathfrak{f}_\chi}\right)$*;*
(b) For a fixed $\mathfrak{f}_\chi$ *when* $1 \le \mathfrak{f}_\chi \le n$*, there are exactly*

$$\# \left\{ \rho \in \underline{\mathrm{Rep}} \left(G_n^{(d)} \right) \,\middle|\, \dim_{\mathbb{C}}(\rho) = \phi\left(p^{\mathfrak{f}_\chi}\right) \right\} = \frac{\left(p^{d\mathfrak{f}_\chi} - p^{d(\mathfrak{f}_\chi - 1)} \right) \times \phi(p^n)}{\phi(p^{\mathfrak{f}_\chi})^2}$$

non-isomorphic irreducible representations $\rho_n^{(d)}(\chi, \psi)$ *induced from* $\frac{1+p^{\mathfrak{f}_\chi}}{1+p^n\mathbb{Z}} \ltimes H_n^{(d)}$.

Proof. (a) Since there are $\phi(p^n)$ elements in $(\mathbb{Z}/p^n\mathbb{Z})^\times$, and $\phi(p^{\mathfrak{f}_\chi})$ elements in $\left(\mathbb{Z}/p^{\mathfrak{f}}\mathbb{Z}\right)^\times$, there must be $\frac{\phi(p^n)}{\phi(p^{\mathfrak{f}_\chi})}$ elements in $\mathrm{Stab}_{\Sigma_n}(\chi)$. The dimension of a rep-

resentation $\rho_n^{(d)}(\chi,\psi)$ is calculated via the index formula

$$\begin{aligned}\dim_{\mathbb{C}}\left(\mathrm{Ind}_{\mathrm{Stab}_{\Sigma_n}(\chi)\ltimes H_n^{(d)}}^{G_n^{(d)}}\left(\chi^{\dagger}\otimes\psi\right)\right) &= \left[G_n^{(d)} : \mathrm{Stab}_{\Sigma_n}(\chi)\ltimes H_n^{(d)}\right]\\ &= \frac{\left|G_n^{(d)}\right|}{\left|\mathrm{Stab}_{\Sigma_n}(\chi)\ltimes H_n^{(d)}\right|} = \frac{|\Sigma_n|}{|\mathrm{Stab}_{\Sigma_n}(\chi)|}\\ &= \frac{\phi(p^n)}{\left(\frac{\phi(p^n)}{\phi(p^{\mathfrak{f}_\chi})}\right)} = \phi(p^{\mathfrak{f}_\chi}).\end{aligned}$$

To show (b), let us first fix the exponent $\mathfrak{f}_\chi$. Then the dimension of each induced representation ρ must equal $\phi(p^{\mathfrak{f}_\chi})$; furthermore

$$\begin{aligned}\#\text{rep's of the form } \rho_n^{(d)}(\chi,\psi) &\overset{\text{by 3.1.3(iv)}}{=} \frac{\#\left\{\text{char's } \chi : H_n^{(d)} \twoheadrightarrow \mu_{p^{\mathfrak{f}_\chi}}\right\}}{\#(\mathbb{Z}/p^{\mathfrak{f}_\chi}\mathbb{Z})^\times} \times \#\mathrm{Stab}_{\Sigma_n}(\chi)\\ &\overset{\text{by 3.1.4(a)}}{=} \frac{(p^{\mathfrak{f}_\chi})^d - (p^{\mathfrak{f}_\chi-1})^d}{\phi(p^{\mathfrak{f}_\chi})} \times \frac{\phi(p^n)}{\phi(p^{\mathfrak{f}_\chi})}\,.\end{aligned}$$

Note that here we have utilised the fact that the Σ_n-orbit of a character $\chi_{\underline{\alpha}}$ with $\mathrm{order}_{H_n^{(d)}}(\underline{\alpha}) = p^{\mathfrak{f}_\chi}$ coincides exactly with the finite set $\left\{\chi_{a\underline{\alpha}} \mid a \in (\mathbb{Z}/p^{\mathfrak{f}_\chi}\mathbb{Z})^\times\right\}$. □

In order to calculate ranks for the group rings occurring in the additive theta map, we first need to calculate the rank (as a $\mathbb{Z}_p$-module) of its domain $\mathbb{Z}_p\left[\mathrm{Conj}(G_n^{(d)})\right]$.

Lemma 3.1.5. *The rank of* $\mathbb{Z}_p\left[\mathrm{Conj}(G_n^{(d)})\right]$ *equals*

$$\#\mathrm{Conj}\left(G_n^{(d)}\right) = \begin{cases} p^{n-1}\times\left(\frac{p^{(d-2)n}-1}{p^{d-2}-1}\times\frac{p^d-1}{p-1}+p-1\right) & \text{if } d\geq 3\\ p^{n-1}\times(n(p+1)+p-1) & \text{if } d=2\\ \frac{p^n-1}{p-1}+p^n-p^{n-1} & \text{if } d=1.\end{cases}$$

Proof. First, for general d we calculate the size of $\mathrm{Conj}(G_n^{(d)})$:

$$\begin{aligned}\#\mathrm{Conj}(G_n^{(d)}) &= \#\{\text{irreducible representations of } G_n^{(d)} \text{ up to isomorphism}\}\\ &\overset{\text{by 3.1.4(b)}}{=} \#\Sigma_n + \sum_{\mathfrak{f}_\chi=1}^{n}\frac{(p^{d\mathfrak{f}_\chi}-p^{d(\mathfrak{f}_\chi-1)})\phi(p^n)}{\phi(p^{\mathfrak{f}_\chi})^2} \qquad (3.1)\end{aligned}$$

$$
\begin{aligned}
&= \phi(p^n) + \phi(p^n) \sum_{\mathfrak{f}_\chi=1}^{n} \frac{p^{d\mathfrak{f}_\chi} - p^{d(\mathfrak{f}_\chi-1)}}{\phi(p^{\mathfrak{f}_\chi})^2} \\
&= \phi(p^n) \left(1 + \sum_{\mathfrak{f}_\chi=1}^{n} \frac{p^{d(\mathfrak{f}_\chi-1)}(p^d-1)}{(p-1)^2 p^{2(\mathfrak{f}_\chi-1)}} \right) \\
&= \phi(p^n) \left(1 + \frac{1}{(p-1)^2} \sum_{\mathfrak{f}_\chi}^{n} p^{(d-2)(\mathfrak{f}_\chi-1)}(p^d-1) \right) \\
&= \frac{\phi(p^n)}{(p-1)^2} \left((p-1)^2 + (p^d-1) \sum_{\mathfrak{f}_\chi=1}^{n} p^{(d-2)(\mathfrak{f}_\chi-1)} \right). \qquad (3.2)
\end{aligned}
$$

Then, we proceed by calculating $\#\mathrm{Conj}(G_n^{(d)})$ in three different cases.

Case $d \geq 3$: Since $\sum_{\mathfrak{f}_\chi=1}^{n} p^{(d-2)(\mathfrak{f}_\chi-1)} = \frac{(p^{(d-2)n}-1)}{p^{d-2}-1}$ holds for $d \geq 3$, Equation (3.2) becomes

$$
\begin{aligned}
\#\mathrm{Conj}(G_n^{(d)}) &= \frac{\phi(p^n)}{(p-1)^2} \left((p-1)^2 + (p^d-1) \frac{(p^{(d-2)n}-1)}{p^{d-2}-1} \right) \\
&= \frac{p^{n-1}}{(p-1)} \left((p-1)^2 + (p^d-1) \frac{(p^{(d-2)n}-1)}{p^{d-2}-1} \right) \\
&= p^{n-1} \left((p-1) + \frac{(p^d-1)}{(p-1)} \frac{(p^{(d-2)n}-1)}{(p^{d-2}-1)} \right).
\end{aligned}
$$

Case $d = 1$: Substituting $d = 1$ in Equation (3.2) gives

$$
\begin{aligned}
\#\mathrm{Conj}(G_n^{(1)}) &= \frac{\phi(p^n)}{(p-1)^2} \left((p-1)^2 + (p-1) \sum_{\mathfrak{f}_\chi=1}^{n} \frac{1}{p^{\mathfrak{f}_\chi-1}} \right) \\
&= \phi(p^n) + \frac{\phi(p^n)}{p-1} \sum_{\mathfrak{f}_\chi=1}^{n} \frac{1}{p^{\mathfrak{f}_\chi-1}}.
\end{aligned}
$$

Recall the geometric series formula for n terms when $r \neq 1$ is: $a + ar + ar^2 + ar^3 + \cdots + ar^{n-1} = \sum_{k=0}^{n-1} ar^k = a\,\frac{r^n-1}{r-1}$. Thus,

$$
\begin{aligned}
\#\mathrm{Conj}(G_n^{(1)}) &= \phi(p^n) + \frac{\phi(p^n)}{p-1} \left(\frac{(\frac{1}{p})^n - 1}{(\frac{1}{p}) - 1} \right) \\
&= \phi(p^n) + p^{n-1} \left(\frac{p^n - 1}{p^n - p^{n-1}} \right)
\end{aligned}
$$

$$= \phi(p^n) + \frac{p^n - 1}{p - 1}.$$

Case $d = 2$: Finally, substituting $d = 2$ in Equation (3.2) implies

$$\begin{aligned}\#\mathrm{Conj}(G_n^{(2)}) &= \frac{\phi(p^n)}{(p-1)^2}\left((p-1)^2 + (p^2-1)n\right) \\ &= \phi(p^n) + \frac{n(p+1)\phi(p^n)}{p-1} \\ &= \phi(p^n) + n(p+1)p^{n-1}.\end{aligned}$$

□

With the representation theory for $G_n^{(d)}$ well understood, we now construct the m^{th}-level additive theta map. For each integer $m \leq n$, define a normal subgroup of $G_n^{(d)} = \Sigma_n \ltimes H_n^{(d)}$ by

$$\mathfrak{S}_m \;:=\; \frac{1 + p^m\mathbb{Z}}{1 + p^n\mathbb{Z}} \ltimes H_n^{(d)}.$$

Lemma 3.1.6. *(i) The commutator subgroup $[\mathfrak{S}_m, \mathfrak{S}_m]$ equals $\left(H_n^{(d)}\right)^{p^m}$;*
(ii) Each quotient group $\mathfrak{S}_m^{\mathrm{ab}} = \mathfrak{S}_m/[\mathfrak{S}_m, \mathfrak{S}_m]$ is isomorphic to $\frac{1+p^m\mathbb{Z}}{1+p^n\mathbb{Z}} \times H_m^{(d)}$.

Proof. Note that $1 + p^m \in \Sigma_n$ acts trivially on the quotient $H_m^{(d)} \cong H_n^{(d)} / \left(H_n^{(d)}\right)^{p^m}$, therefore $\mathfrak{S}_m / \left(H_n^{(d)}\right)^{p^m} \cong \frac{1+p^m\mathbb{Z}}{1+p^n\mathbb{Z}} \ltimes H_m^{(d)}$ is actually a direct product, and so must be abelian; it follows that $[\mathfrak{S}_m, \mathfrak{S}_m] \subseteq \left(H_n^{(d)}\right)^{p^m}$.

However if this were to be a strict inclusion, $H_n^{(d)}/[\mathfrak{S}_m, \mathfrak{S}_m]$ would contain an element $\underline{\mathfrak{h}}'$ of order p^{m+1}. The action of $1 + p^m$ on $\underline{\mathfrak{h}}'$ would then be non-trivial implying that $\mathfrak{S}_m/[\mathfrak{S}_m, \mathfrak{S}_m]$ is non-commutative, which is clearly nonsense. □

The trace map is now constructed mimicking Hara's definition (Section 3.2 [20]):

Definition 3.1.7. *Let $\{u_1, .., u_r\} \subseteq G_n^{(d)}$ be a system of coset representatives for $G_n^{(d)}/\mathfrak{S}_m$. Then for an arbitrary conjugacy class $[g]_{G_n^{(d)}} \in \mathrm{Conj}(G_n^{(d)})$, define*

$$\mathrm{Tr}_{G_n^{(d)}/\mathfrak{S}_m}([g]_{G_n^{(d)}}) := \sum_{j=1}^{r} \tau_j([g]_{G_n^{(d)}}) = \begin{cases} \sum_{j=1}^{r}[u_j^{-1}gu_j] & u_j^{-1}gu_j \in \mathfrak{S}_m \\ 0 & u_j^{-1}gu_j \notin \mathfrak{S}_m. \end{cases}$$

The trace map, $\mathrm{Tr}_{G_n^{(d)}/\mathfrak{S}_m}$, averages a conjugacy class over the coset representatives of $G_n^{(d)}/\mathfrak{S}_m$. Secondly, by quotienting an element of $\mathfrak{S}_m$ modulo $[\mathfrak{S}_m, \mathfrak{S}_m]$, one induces a map

$$\mathbb{Z}_p\left[\mathrm{Conj}(\mathfrak{S}_m)\right] \overset{\text{mod } [\mathfrak{S}_m,\mathfrak{S}_m]}{\longrightarrow} \mathbb{Z}_p\left[\mathrm{Conj}\left(\frac{\mathfrak{S}_m}{[\mathfrak{S}_m,\mathfrak{S}_m]}\right)\right] \cong \mathbb{Z}_p\left[\frac{1+p^m\mathbb{Z}}{1+p^n\mathbb{Z}} \times H_m^{(d)}\right].$$

Here the last isomorphism arises because the conjugacy classes of an abelian group are in one-to-one correspondence with its elements.

Definition 3.1.8. *(a) The m^{th}-level of the additive theta map*

$$\theta_m^+ : \mathbb{Z}_p\left[\mathrm{Conj}(G_n^{(d)})\right] \longrightarrow \mathbb{Z}_p\left[\frac{1+p^m\mathbb{Z}}{1+p^n\mathbb{Z}}\right]\left[H_m^{(d)}\right]$$

is defined by the composition $\theta_m^+([g]) := \mathrm{Tr}_{G_n^{(d)}/\mathfrak{S}_m}([g]) \mod [\mathfrak{S}_m, \mathfrak{S}_m]$.
(b) Extending each character $\chi : H_m^{(d)} \twoheadrightarrow \mu_{p^m}$ to the ring $\mathbb{Z}_p\left[\frac{1+p^m\mathbb{Z}}{1+p^n\mathbb{Z}}\right]\left[H_m^{(d)}\right]$, then

$$\theta_{\chi_m}^+ : \mathbb{Z}_p\left[\mathrm{Conj}(G_n^{(d)})\right] \longrightarrow \mathbb{Z}_p[\mu_{p^m}]\left[\frac{1+p^m\mathbb{Z}}{1+p^n\mathbb{Z}}\right] \quad \textit{is defined via } \theta_{\chi_m} := \chi \circ \theta_m.$$

As we will soon discover, both these θ^+-maps play a fundamental rôle in describing the image of $\mathbb{Z}_p\left[\mathrm{Conj}(G_n^{(d)})\right]$ inside the direct product of its abelian factor rings. Let us first see the effect of these homomorphisms on individual conjugacy classes.

Notation: Write $\nu_m(\underline{h})$ to denote the p-exponent for the image of $\underline{h}$ inside $H_m^{(d)} \cong H_n^{(d)}/p^m$, so that

$$\nu_m(\underline{h}) \;=\; \min\left\{ t \geq 0 \;\middle|\; \underline{h}^{p^t} \in \left(H_n^{(d)}\right)^{p^m}, \text{ namely } \underline{h}^{p^t} = \text{ Identity in } H_m^{(d)} \right\}.$$

For example, if $m = n$ then $p^{\nu_n(\underline{h})}$ is just the order of $\underline{h}$ within the full group $H_n^{(d)}$. Alternatively if $m < n$, one finds $\nu_m(\underline{h}) = \max\{\nu_{m+j}(\underline{h}) - j, 0\}$ when $j \leq n - m$.

Proposition 3.1.9. *Let* $\mathcal{A}_{H_m^{(d)}}\langle \underline{\mathfrak{h}} \rangle := \sum_{\underline{z} \in \langle \underline{\mathfrak{h}} \rangle,\ \langle \underline{z} \rangle = \langle \underline{\mathfrak{h}} \rangle} [\underline{z}] \in \mathbb{Z}_p\left[H_m^{(d)}\right]$ *for* $\underline{\mathfrak{h}} \in H_m^{(d)}$.

(i) $\theta_m^+\left([\sigma \cdot \underline{h}]_{G_n^{(d)}}\right) = \begin{cases} \frac{\phi(p^m)}{\phi(p^{\nu_m(\underline{h})})}\ [\sigma]_{\frac{1+p^m\mathbb{Z}}{1+p^n\mathbb{Z}}} \times \mathcal{A}_{H_m^{(d)}}\langle \overline{\underline{h}} \rangle & \text{if } \sigma \equiv 1 \ (\mod p^m) \\ 0 & \text{otherwise;} \end{cases}$

$$(ii)\ \ \theta^+_{\chi_m}\left([\sigma\cdot\underline{h}]_{G_n^{(d)}}\right)=\begin{cases}\phi(p^m)\ [\sigma]_{\frac{1+p^m\mathbb{Z}}{1+p^n\mathbb{Z}}} & \text{if } \sigma\equiv 1\ (\mod p^m) \text{ and } \underline{h}\in \mathrm{Ker}(\chi)\\ -p^{m-1}\,[\sigma]_{\frac{1+p^m\mathbb{Z}}{1+p^n\mathbb{Z}}} & \text{if } \sigma\equiv 1\ (\mod p^m),\ \underline{h}\notin \mathrm{Ker}(\chi)\\ & \qquad\qquad \text{but } \underline{h}^p\in \mathrm{Ker}(\chi)\\ 0 & \text{otherwise.}\end{cases}$$

Proof. Let $g=\sigma\cdot\underline{h}$ be an arbitrary element of $G_n^{(d)}$. Since $\frac{G_n^{(d)}}{\mathfrak{S}_m}\cong(\mathbb{Z}/p^m\mathbb{Z})^\times$, its coset representatives are

$$\left\{g_u=\begin{pmatrix}u&0&0&0&\cdots&0\\0&u&0&0&\cdots&0\\0&0&u&0&\cdots&0\\\vdots&&&\ddots&&\vdots\\0&\cdots&&&u&0\\0&\cdots&&&\cdots&1\end{pmatrix}\ \text{such that } u\in(\mathbb{Z}/p^m\mathbb{Z})^\times\right\}.$$

Furthermore,

$$\begin{aligned}g_u^{-1}gg_u &= \begin{pmatrix}u^{-1}&0&0&0&\cdots&0\\0&u^{-1}&0&0&\cdots&0\\0&0&u^{-1}&0&\cdots&0\\\vdots&&&\ddots&&\vdots\\0&\cdots&&&u^{-1}&0\\0&\cdots&&&\cdots&1\end{pmatrix}\begin{pmatrix}\sigma&0&0&0&\cdots&h_1\\0&\sigma&0&0&\cdots&h_2\\0&0&\sigma&0&\cdots&h_3\\\vdots&&&\ddots&&\vdots\\0&\cdots&&&\sigma&h_d\\0&\cdots&&&\cdots&\sigma\end{pmatrix}\begin{pmatrix}u&0&0&0&\cdots&0\\0&u&0&0&\cdots&0\\0&0&u&0&\cdots&0\\\vdots&&&\ddots&&\vdots\\0&\cdots&&&u&0\\0&\cdots&&&\cdots&u\end{pmatrix}\\ &= \begin{pmatrix}\sigma&0&0&0&\cdots&u^{-1}h_1\\0&\sigma&0&0&\cdots&u^{-1}h_2\\0&0&\sigma&0&\cdots&u^{-1}h_3\\\vdots&&&\ddots&&\vdots\\0&\cdots&&&\sigma&u^{-1}h_d\\0&\cdots&&&\cdots&1\end{pmatrix}.\end{aligned}$$

In particular, $g_u^{-1}gg_u\in\mathfrak{S}_m$ if and only if $\sigma\equiv 1\mod p^m$, therefore

$$\begin{aligned}Tr_{G_n^{(d)}/\mathfrak{S}_m}\left([g]_{G_n^{(d)}}\right) &= \begin{cases}\sum_{u\in(\mathbb{Z}/p^m\mathbb{Z})^\times}\begin{pmatrix}\sigma&0&0&0&\cdots&uh_1\\0&\sigma&0&0&\cdots&uh_2\\0&0&\sigma&0&\cdots&uh_3\\\vdots&&&\ddots&&\vdots\\0&\cdots&&&\sigma&uh_d\\0&\cdots&&&\cdots&1\end{pmatrix}_{\mathfrak{S}_m} & g\in\mathfrak{S}_m\\ 0 & g\notin\mathfrak{S}_m\end{cases}\\ &= \begin{cases}\sum_{u\in(\mathbb{Z}/p^m\mathbb{Z})^\times}[\sigma(u\cdot\underline{h})]_{\mathfrak{S}_m} & \sigma\equiv 1\mod p^m\\ 0 & \sigma\not\equiv 1\mod p^m.\end{cases}\end{aligned}\tag{3.3}$$

Suppose now that $\sigma\equiv 1(\mod p^m)$. Reducing equation (3.3) modulo $[\mathfrak{S}_m,\mathfrak{S}_m]$,

one deduces that

$$\begin{aligned}\theta_m\left([g]_{G_n^{(d)}}\right) &= [\sigma]_{\frac{1+p^m\mathbb{Z}}{1+p^n\mathbb{Z}}} \times \sum_{u\in(\mathbb{Z}/p^m\mathbb{Z})^\times}\left[(u\bar{h}_1,\ldots,u\bar{h}_d)\right]_{H_m^{(d)}}\\ &= [\sigma]_{\frac{1+p^m\mathbb{Z}}{1+p^n\mathbb{Z}}} \times \frac{\phi(p^m)}{\phi(p^{\nu_m(\underline{h})})}\sum_{u\in(\mathbb{Z}/p^{\nu_m(\underline{h})}\mathbb{Z})^\times}\left[(u\bar{h}_1,\ldots,u\bar{h}_d)\right]_{H_m^{(d)}}.\end{aligned}$$

The last sum ranges over precisely the generators of the cyclic subgroup $\langle\bar{\underline{h}}\rangle \subset H_m^{(d)}$, in which case (i) is established.

To show (ii), we simply appeal to the character-sum identities

$$\chi\left(\mathcal{A}_{H_m^{(d)}}\langle\underline{\mathfrak{h}}\rangle\right) = \sum_{u\in(\mathbb{Z}/p^{\nu_m(\underline{\mathfrak{h}})}\mathbb{Z})^\times}\chi(\underline{\mathfrak{h}})^u\begin{cases}\phi\left(p^{\nu_m(\underline{\mathfrak{h}})}\right) & \text{if } \underline{\mathfrak{h}}\in\mathrm{Ker}(\chi)\\ -p^{\nu_m(\underline{\mathfrak{h}})-1} & \text{if } \underline{\mathfrak{h}}\notin\mathrm{Ker}(\chi) \text{ but } \underline{\mathfrak{h}}^p\in\mathrm{Ker}(\chi)\\ 0 & \text{otherwise,}\end{cases}$$

whose proof is a straightforward exercise in cyclotomy. □

Corollary 3.1.10. *The image of θ_m^+ is naturally a free $\mathbb{Z}_p\left[\frac{1+p^m\mathbb{Z}}{1+p^n\mathbb{Z}}\right]$-module, and*

$$\mathrm{rank}_{\mathbb{Z}_p\left[\frac{1+p^m\mathbb{Z}}{1+p^n\mathbb{Z}}\right]}\left(\mathrm{Im}\left(\theta_m^+\right)\right) = \begin{cases}1+\frac{p^{m(d-1)}-1}{p^{d-1}-1}\times\frac{p^d-1}{p-1} & \text{if } d\geq 2\\ 1+m & \text{if } d=1.\end{cases}$$

Proof. Since the elements $\mathcal{A}_{H_m^{(d)}}\langle\underline{\mathfrak{h}}\rangle$ are linearly independent over $\mathbb{Z}_p\left[\frac{1+p^m\mathbb{Z}}{1+p^n\mathbb{Z}}\right]$, the rank of $\mathrm{Im}\left(\theta_m^+\right)$ must equal

$$\begin{aligned}\left(\text{the no. of } \mathcal{A}_{H_m^{(d)}}\langle\underline{\mathfrak{h}}\rangle\text{'s}\right) &= \textstyle\sum_{j=0}^m\left(\text{no. of cyclic subgroups } \langle\underline{\mathfrak{h}}\rangle\subset H_m^{(d)} \text{ of size } p^j\right)\\ &= 1+\textstyle\sum_{j=1}^m\frac{p^{jd}-p^{(j-1)d}}{\phi(p^j)} = 1+\frac{p^d-1}{p-1}\times\sum_{j=1}^m\frac{p^{(j-1)d}}{p^{j-1}}.\end{aligned}$$

When $d\geq 2$, the sum of the first m terms of the geometric series $\sum_{j=1}^m p^{(j-1)(d-1)}$ equals $\frac{p^{m(d-1)}-1}{p^{d-1}-1}$; and when $d=1$, obviously $\sum_{j=1}^m p^{(j-1)(d-1)}$ equals m. Thus the stated formula is established. For instance, if $0\leq m\leq n$ and $\Sigma'=\frac{1+p^m\mathbb{Z}}{1+p^n\mathbb{Z}}$, then

$$\mathrm{Im}\left(\theta_m^+\right) \cong \mathbb{Z}_p[\Sigma']\otimes_{\mathbb{Z}_p}\mathbb{Z}_p\left\langle\mathcal{S}_m^{(\mathcal{A})}\right\rangle$$

where the set $\mathcal{S}_m^{(\mathcal{A})} := \left\{\phi(p^m)\cdot\mathrm{id}_{H_m^{(d)}}\right\}\cup\left\{p^{m-\nu_m(\underline{\mathfrak{h}})}\cdot\mathcal{A}_{H_m^{(d)}}\langle\underline{\mathfrak{h}}\rangle \;\middle|\; 0\neq\langle\underline{\mathfrak{h}}\rangle<H_m^{(d)}\right\}$.

□

Remark 3.1.11. *(i) To illustrate what happens in the familiar false-Tate situation $d = 1$, by Corollary 3.1.10 the rank of $\mathrm{Im}(\theta_m^+)$ grows linearly with m, while θ_0^+ is a surjection. Therefore to recover $\mathbb{Z}_p\left[\mathrm{Conj}(G_n^{(1)})\right]$ inside the finite direct product $\prod_{m=0}^n \mathrm{Im}(\theta_m^+)$, one would need only a single relation linking $\mathrm{Im}(\theta_{m-1}^+)$ with $\mathrm{Im}(\theta_m^+)$ for each m.*
(ii) In his works [24], [23] Kato provides exactly these relations for finite quotients of $\begin{pmatrix} \mathbb{Z}_p^\times & \mathbb{Z}_p \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & \mathbb{Z}_p & \mathbb{Z}_p \\ 0 & 1 & \mathbb{Z}_p \\ 0 & 0 & 1 \end{pmatrix}$ respectively. Our task will be to find analogues of these relations on finite quotients of the $(d+1)$-dimensional Lie group $\varprojlim_n G_n^{(d)}$.
(iii) For general $d \geq 1$, a necessary condition for a sequence $\{y_m\}_m \in \prod_{m=0}^n \mathbb{Z}_p\left[\mathfrak{S}_m^{\mathrm{ab}}\right]$ to originate from an element $x \in \mathbb{Z}_p\left[\mathrm{Conj}(G_n^{(d)})\right]$ under $\prod_{m=0}^n \theta_m^+$, is given by

Lemma 3.1.12. *If $y_m = \theta_m^+(x)$ for each $m \in \{0, \ldots, n\}$, then one obtains relations*

$$\mathrm{Tr}_{\mathbb{Z}_p\left[\frac{1+p^{m-1}\mathbb{Z}}{1+p^n\mathbb{Z}} \times H_{m-1}^{(d)}\right] / \mathbb{Z}_p\left[\frac{1+p^m\mathbb{Z}}{1+p^n\mathbb{Z}} \times H_{m-1}^{(d)}\right]} (y_{m-1}) \equiv y_m \mod \left(H_m^{(d)}\right)^{p^{m-1}} \tag{3.4}$$

i.e. the elements $\{y_m\}_{0 \leq m \leq n}$ are trace compatible.

Proof. Without loss of generality, one may assume that $x = [\sigma \cdot \underline{h}]_{G_n^{(d)}}$ since the maps in question are all $\mathbb{Z}_p$-linear. If $\sigma \not\equiv 1 (\mathrm{mod}\ p^m)$, both of the terms in (3.4) are zero. If $\sigma \equiv 1 (\mathrm{mod}\ p^m)$ then by Proposition 3.1.9(i),

$$\begin{aligned} y_{m-1} &= \frac{\phi(p^{m-1})}{\phi(p^{\nu_{m-1}(\underline{h})})} [\sigma]_{\frac{1+p^{m-1}\mathbb{Z}}{1+p^n\mathbb{Z}}} \times \mathcal{A}_{H_{m-1}^{(d)}} \left\langle \overline{\underline{h}} \right\rangle, \text{and} \\ y_m &= \frac{\phi(p^m)}{\phi(p^{\nu_m(\underline{h})})} [\sigma]_{\frac{1+p^m\mathbb{Z}}{1+p^n\mathbb{Z}}} \times \mathcal{A}_{H_m^{(d)}} \left\langle \overline{\underline{h}} \right\rangle. \end{aligned}$$

Applying the trace map to y_{m-1}, we have

$$\begin{aligned} \mathrm{Tr}\,(y_{m-1}) &= \frac{\phi(p^{m-1})}{\phi(p^{\nu_{m-1}(\underline{h})})} \mathrm{Tr}_{\mathbb{Z}_p\left[\frac{1+p^{m-1}\mathbb{Z}}{1+p^n\mathbb{Z}}\right] / \mathbb{Z}_p\left[\frac{1+p^m\mathbb{Z}}{1+p^n\mathbb{Z}}\right]} \left([\sigma]_{\frac{1+p^{m-1}\mathbb{Z}}{1+p^n\mathbb{Z}}} \right) \times \mathcal{A}_{H_{m-1}^{(d)}} \left\langle \overline{\underline{h}} \right\rangle \\ &= \frac{\phi(p^m)}{\phi(p^{\nu_{m-1}(\underline{h})})} [\sigma]_{\frac{1+p^m\mathbb{Z}}{1+p^n\mathbb{Z}}} \times \mathcal{A}_{H_{m-1}^{(d)}} \left\langle \overline{\underline{h}} \right\rangle. \end{aligned}$$

If $\nu_m(\underline{h}) = 0$, then $\frac{1}{\phi(p^{\nu_m(\underline{h})})} \mathcal{A}_{H_m^{(d)}} \left\langle \overline{\underline{h}} \right\rangle = [\mathrm{id}]_{H_m^{(d)}} \equiv [\mathrm{id}]_{H_{m-1}^{(d)}} = \frac{1}{\phi(p^{\nu_{m-1}(\underline{h})})} \mathcal{A}_{H_{m-1}^{(d)}} \left\langle \overline{\underline{h}} \right\rangle$.
Alternatively, if $\nu_m(\underline{h}) = 1$ so that $\nu_{m-1}(\underline{h}) = 0$, then

$$\frac{1}{\phi(p^{\nu_m(\underline{h})})} \mathcal{A}_{H_m^{(d)}} \left\langle \overline{\underline{h}} \right\rangle = \frac{1}{p-1} \sum_{\underline{z} \in \left\langle \overline{\underline{h}} \right\rangle - \{\underline{0}\}} [\underline{z}]_{H_m^{(d)}} \equiv [\mathrm{id}]_{H_{m-1}^{(d)}} = \frac{1}{\phi(p^{\nu_{m-1}(\underline{h})})} \mathcal{A}_{H_{m-1}^{(d)}} \left\langle \overline{\underline{h}} \right\rangle.$$

Lastly, if $\nu_m(\underline{h}) \geq 2$, the result follows due to the congruence

$$\mathcal{A}_{H_m^{(d)}}\left\langle \underline{h} \mod \left(H_n^{(d)}\right)^{p^m} \right\rangle \mod \left(H_n^{(d)}\right)^{p^{m-1}} \equiv p \times \mathcal{A}_{H_{m-1}^{(d)}}\left\langle \underline{h} \mod \left(H_n^{(d)}\right)^{p^{m-1}} \right\rangle$$

together with the fact $\nu_m(\underline{h}) = 1 + \nu_{m-1}(\underline{h}) > 1 \implies \phi(p^{\nu_m(\underline{h})}) = p \times \phi(p^{\nu_{m-1}(\underline{h})})$.

□

4

Describing the Image of Θ^+

The property of trace-compatibility is not only necessary for a sequence to belong to the image of the map $\prod \theta_m^+$, but it is also a sufficient condition. This is evidenced in the following result, which the rest of this chapter is devoted to establishing.

Theorem 4.0.13. *Defining* $\Psi_n^{(d)} := \left\{ \{y_m\}_{0 \leq m \leq n} \text{ such that } \mathrm{Tr}(y_{m-1}) \equiv y_m \right\}$ *to be the* $\mathbb{Z}_p$*-submodule of*

$$\prod_{m=0}^{n} \mathbb{Z}_p \left[\frac{1+p^m\mathbb{Z}}{1+p^n\mathbb{Z}} \right] \left\langle \mathcal{S}_m^{(\mathcal{A})} \right\rangle$$

consisting of trace compatible elements, there is an isomorphism

$$\prod \theta_m^+ \ : \ \mathbb{Z}_p \left[\mathrm{Conj}(G_n^{(d)}) \right] \ \xrightarrow{\sim} \ \Psi_n^{(d)} \ \subset \ \prod_{m=0}^{n} \mathbb{Z}_p \left[\mathfrak{S}_m^{\mathrm{ab}} \right].$$

Thus on an infinite level, a sequence $\{y_m\}$ arises from $\mathbb{Z}_p \left[\left[\mathrm{Conj}(G_\infty^{(d)}) \right] \right]$ in this way if and only if the relations $\mathrm{Tr}\,(y_{m-1}) \equiv y_m \bmod \left(H_\infty^{(d)} \right)^{p^{m-1}}$ hold at every $m \in \mathbb{N}$.

Notation: Recall that $\langle \underline{h} \rangle$ denoted the cyclic subgroup of $H_n^{(d)}$ generated by $\underline{h}$. Henceforth, we shall write

$$\langle \underline{h} \rangle_{\mathrm{gen}} := \left\{ \underline{h}' \in \langle \underline{h} \rangle < H_n^{(d)} \text{ such that } \langle \underline{h}' \rangle = \langle \underline{h} \rangle \right\}$$

for its set of generators; in particular $\# \langle \underline{h} \rangle_{\mathrm{gen}} = \phi \left(p^{\nu_n(\underline{h})} \right)$.

Before giving the proof of the main theorem, we require some preparatory results.

Lemma 4.0.14. *The conjugacy classes in $G_n^{(d)}$ are represented by the sets*

$$[\sigma\cdot\underline{h}]_{G_n^{(d)}} \;=\; \left\{\sigma\cdot\underline{h}' \;\middle|\; \underline{h}'\in\langle\underline{h}\rangle_{\text{gen}}+\left(H_n^{(d)}\right)^{p^{\text{ord}_p(\sigma-1)}}\right\} \quad \textit{with } \sigma\in\Sigma_n,\ \underline{h}\in H_n^{(d)}$$

and the individual class associated to $g=\sigma\cdot\underline{h}$ depends **uniquely** *on:*

(i) the choice of element σ,

(ii) the cyclic subgroup generated by $\underline{h}$ modulo $p^{\text{ord}_p(\sigma-1)}$.

Proof. Each element $g=\sigma\cdot\underline{h}\in\Sigma_n\ltimes H_n^{(d)}$ can be represented as a matrix $\begin{pmatrix}\sigma & \dots & 0 & h_1\\ \vdots & & \vdots & \vdots\\ 0 & \dots & \sigma & h_d\\ 0 & \dots & 0 & 1\end{pmatrix}$, which is an element of $\text{GL}\,(d+1,\mathbb{Z}/p^n\mathbb{Z})$. Indeed if $k=\kappa\cdot\underline{t}\in\Sigma_n\ltimes H_n^{(d)}$, one calculates

$$\begin{aligned} kgk^{-1} &= \begin{pmatrix}\kappa & 0 & \dots & 0 & t_1\\ 0 & \kappa & \dots & 0 & t_2\\ \vdots & \vdots & & \vdots & \vdots\\ 0 & 0 & \dots & \kappa & t_d\\ 0 & 0 & \dots & 0 & 1\end{pmatrix}\begin{pmatrix}\sigma & 0 & \dots & 0 & h_1\\ 0 & \sigma & \dots & 0 & h_2\\ \vdots & \vdots & & \vdots & \vdots\\ 0 & 0 & \dots & \sigma & h_d\\ 0 & 0 & \dots & 0 & 1\end{pmatrix}\begin{pmatrix}\kappa & 0 & \dots & 0 & t_1\\ 0 & \kappa & \dots & 0 & t_2\\ \vdots & \vdots & & \vdots & \vdots\\ 0 & 0 & \dots & \kappa & t_d\\ 0 & 0 & \dots & 0 & 1\end{pmatrix}^{-1}\\ &= \begin{pmatrix}\sigma & 0 & \dots & 0 & -\sigma\times t_1+\kappa\times h_1+t_1\\ 0 & \sigma & \dots & 0 & -\sigma\times t_2+\kappa\times h_2+t_2\\ \vdots & \vdots & & \vdots & \vdots\\ 0 & 0 & \dots & \sigma & -\sigma\times t_d+\kappa\times h_d+t_d\\ 0 & 0 & \dots & 0 & 1\end{pmatrix} \;=\; \sigma\cdot\left(\kappa\times\underline{h}+(1-\sigma)\times\underline{t}\right). \end{aligned}$$

The span of the elements $\kappa\times\underline{h}$ coincides with the subset of generators inside $\langle\underline{h}\rangle$, while one has $\left\{(1-\sigma)\times\underline{t}\;\middle|\;\underline{t}\in H_n^{(d)}\right\} \;=\; \left(\frac{p^\nu\mathbb{Z}}{p^n\mathbb{Z}}\right)^{\oplus d} \;=\; \left(H_n^{(d)}\right)^{p^\nu}$ with $\nu=\text{ord}_p(\sigma-1)$. Therefore, the orbit of g under $G_n^{(d)}$-conjugation is

$$\begin{aligned} [g]_{G_n^{(d)}} \;&=\; \left\{kgk^{-1}\;\middle|\; k=\kappa\cdot\underline{t}\ \text{ with } \kappa\in\Sigma_n \text{ and } \underline{t}\in H_n^{(d)}\right\}\\ &=\; \left\{\sigma\cdot\left(\underline{h}''+\underline{h}'''\right)\;\middle|\; \underline{h}''\in\langle\underline{h}\rangle_{\text{gen}} \text{ and } \underline{h}'''\in\left(H_n^{(d)}\right)^{p^\nu}\right\}, \quad \text{as asserted.} \end{aligned}$$

We should of course check that we have the requisite number of conjugacy classes. Counting the number of classes using our description above, one obtains

$$\begin{aligned} &\sum_{\nu=0}^{n}\#\left\{\sigma\in\Sigma_n \text{ with } \sigma\equiv 1(p^\nu),\ \sigma\not\equiv 1(p^{\nu+1})\right\}\times\#\left\{\langle\underline{h}\rangle\text{'s of order dividing } p^\nu\right\}\\ &=\; \sum_{\nu=0}^{n-1}\left(\frac{\phi(p^n)}{\phi(p^\nu)}-\frac{\phi(p^n)}{\phi(p^{\nu+1})}\right)\left(1+\sum_{r=1}^{\nu}\frac{p^{rd}-p^{(r-1)d}}{\phi(p^r)}\right) \;+\; 1+\sum_{r=1}^{n}\frac{p^{rd}-p^{(r-1)d}}{\phi(p^r)}. \end{aligned} \tag{4.1}$$

We now observe that

$$\sum_{\nu=0}^{n-1}\left(\frac{\phi(p^n)}{\phi(p^\nu)}-\frac{\phi(p^n)}{\phi(p^{\nu+1})}\right)=\phi(p^n)-1, \tag{4.2}$$

$$\begin{aligned}
\text{and } &\sum_{\nu=1}^{n-1}\sum_{r=1}^{\nu}\left(\frac{p^{rd}-p^{(r-1)d}}{\phi(p^r)}\right)\left(\frac{\phi(p^n)}{\phi(p^\nu)}-\frac{\phi(p^n)}{\phi(p^{\nu+1})}\right)= \\
&=\left(\frac{p^d-1}{\phi(p)}\right)\left(\frac{\phi(p^n)}{\phi(p)}-\frac{\phi(p^n)}{\phi(p^2)}+\frac{\phi(p^n)}{\phi(p^2)}-\frac{\phi(p^3)}{\phi(p^2)}+\cdots+\frac{\phi(p^n)}{\phi(p^{n-1})}-1\right)+ \\
&+\left(\frac{p^{2d}-p^d}{\phi(p^2)}\right)\left(\frac{\phi(p^n)}{\phi(p^2)}-\frac{\phi(p^n)}{\phi(p^3)}+\frac{\phi(p^n)}{\phi(p^3)}-\frac{\phi(p^n)}{\phi(p^4)}\cdots+\frac{\phi(p^n)}{\phi(p^{n-1})}-1\right)+\cdots \\
&+\left(\frac{p^{(n-1)d}-p^{(n-2)d}}{\phi(p^{n-1})}\right)\left(\frac{\phi(p^n)}{\phi(p^{n-1})}-1\right) \\
&=\sum_{r=1}^{n-1}\left(\frac{p^{rd}-p^{(r-1)d}}{\phi(p^r)}\right)\left(\frac{\phi(p^n)}{\phi(p^r)}-1\right).
\end{aligned} \tag{4.3}$$

Consequently, substituting (4.2) and (4.3) into (4.1) gives

$$\begin{aligned}
&\sum_{\nu=0}^{n}\#\left\{\sigma\in\Sigma_n \text{ with } \sigma\equiv 1(p^\nu),\ \sigma\not\equiv 1(p^{\nu+1})\right\}\times\#\left\{\langle\underline{h}\rangle\text{'s of order dividing } p^\nu\right\} \\
&=\phi(p^n)+\sum_{r=1}^{n-1}\left(\frac{p^{rd}-p^{(r-1)d}}{\phi(p^r)}\right)\left(\frac{\phi(p^n)}{\phi(p^r)}-1\right)+\sum_{r=1}^{n}\frac{p^{rd}-p^{(r-1)d}}{\phi(p^r)} \\
&=\phi(p^n)+\sum_{r=1}^{n}\left(\frac{p^{rd}-p^{(r-1)d}}{\phi(p^r)}\right)\left(\frac{\phi(p^n)}{\phi(p^r)}\right)
\end{aligned}$$

which is the R.H.S of equation (3.1), namely the size of $\mathrm{Conj}(G_n^{(d)})$. □

Corollary 4.0.15. *(a) A typical element* $x\in\mathbb{Z}_p\left[\mathrm{Conj}(G_n^{(d)})\right]$ *is of the form*

$$\begin{aligned}
x \;=\; &\sum_{\nu=0}^{n}\sum_{\substack{\sigma\equiv 1(\bmod p^\nu),\\ \sigma\not\equiv 1(\bmod p^{\nu+1})}} A_{\sigma,\nu}\times\left[\sigma\cdot\mathrm{id}_{H_n^{(d)}}\right]_{G_n^{(d)}} \\
&+\sum_{\nu=1}^{n}\sum_{r=1}^{\nu}\sum_{\substack{\langle\underline{\bar{h}}\rangle<H_\nu^{(d)},\\ order(\underline{\bar{h}})=p^r}}\ \sum_{\substack{\sigma\equiv 1(\bmod p^\nu),\\ \sigma\not\equiv 1(\bmod p^{\nu+1})}} B_{\sigma,\langle\underline{\bar{h}}\rangle,r,\nu}\times\left[\sigma\cdot\underline{h}\right]_{G_n^{(d)}}\ .
\end{aligned}$$

(b) Assuming that $0 \leq m \leq n$, a typical element $y_m \in \mathrm{Im}(\theta_m^+)$ is of the form

$$y_m = \phi(p^m) \sum_{\sigma \in \frac{1+p^m\mathbb{Z}}{1+p^n\mathbb{Z}}} \alpha_{\sigma,m} \times [\sigma]_{\frac{1+p^m\mathbb{Z}}{1+p^n\mathbb{Z}}} \ [\mathrm{id}]_{H_m^{(d)}}$$
$$+ \sum_{r=1}^{m} \sum_{\substack{\langle \underline{\mathfrak{h}} \rangle < H_m^{(d)}, \\ \#\langle \underline{\mathfrak{h}} \rangle = p^r}} p^{m-r} \sum_{\sigma \in \frac{1+p^m\mathbb{Z}}{1+p^n\mathbb{Z}}} \beta_{\sigma,\langle \underline{\mathfrak{h}} \rangle,r,m} \times [\sigma]_{\frac{1+p^m\mathbb{Z}}{1+p^n\mathbb{Z}}} \ \mathcal{A}_{H_m^{(d)}} \langle \underline{\mathfrak{h}} \rangle \ .$$

Here the scalars $A_{\sigma,\nu}$, $B_{\sigma,\langle \overline{\underline{h}} \rangle,r,\nu}$, $\alpha_{\sigma,m}$, and $\beta_{\sigma,\langle \underline{\mathfrak{h}} \rangle,r,m}$ can be arbitrary elements of $\mathbb{Z}_p$.

Proof. The first statement follows because by Lemma 4.0.14 , the conjugacy classes of $G_n^{(d)}$ are indexed by pairs $\left(\sigma, \left\langle \overline{\underline{h}} \right\rangle\right)$ where each $\sigma \in \Sigma_n = \bigcup_{\nu=0}^{n} \frac{1+p^\nu\mathbb{Z}}{1+p^n\mathbb{Z}} - \frac{1+p^{\nu+1}\mathbb{Z}}{1+p^n\mathbb{Z}}$ and additionally, $\left\langle \overline{\underline{h}} \right\rangle < H_\nu^{(d)}$ generates a cyclic subgroup of size p^r with $0 \leq r \leq \nu$. The second statement is easy as $\mathrm{Im}(\theta_m^+)$ is generated over $\mathbb{Z}_p\left[\frac{1+p^m\mathbb{Z}}{1+p^n\mathbb{Z}}\right]$ by $\mathcal{S}_m^{(\mathcal{A})}$. □

The proof of Theorem 4.0.13. There are precisely two assertions we need to establish, namely the injectivity of $\prod \theta_m^+ : \mathbb{Z}_p\left[\mathrm{Conj}(G_n^{(d)})\right] \longrightarrow \prod_{m=0}^{n} \mathbb{Z}_p\left[\mathfrak{S}_m^{\mathrm{ab}}\right]$, and secondly its surjectivity onto $\Psi_n^{(d)}$. The former is relatively straightforward.

Let $x = \sum_{[g] \in \mathrm{Conj}(G_n^{(d)})} m_{[g]} \times [g]$ be in the kernel of $\prod_{m=0}^{n} \theta_m^+$. To prove x is zero, it is enough to show that $\widetilde{\tau}(x) = 0$ for an arbitrary class function $\widetilde{\tau} = \mathrm{Tr}(\tau)$ on $G_n^{(d)}$. From Theorem 3.1.3(iii), all irreducible characters are of the form $\widetilde{\rho} = \mathrm{Tr}\left(\rho_n^{(d)}(\chi, \psi)\right)$ where $\chi : H_n^{(d)} \twoheadrightarrow \mu_{p^m}$ say, and the multiplicative character $\psi : G_n^{(d)} \twoheadrightarrow \Sigma_n \to \mathbb{C}^\times$. Consequently,

$$\widetilde{\rho}(x) = \sum_{[g] \in \mathrm{Conj}(G_n^{(d)})} m_{[g]} \sum_{\substack{u \in G_n^{(d)}/\mathfrak{S}_m, \\ ugu^{-1} \in \mathfrak{S}_m}} \chi \otimes \psi\left(ugu^{-1}\right) = \chi \otimes \psi \circ \mathrm{Tr}_{G_n^{(d)}/\mathfrak{S}_m}(x) = \psi \circ \ \theta_{\chi_m}^+(x)$$

and the right-hand term vanishes because $x \in \mathrm{Ker}(\theta_m^+) \subset \mathrm{Ker}(\theta_{\chi_m}^+)$ for each m. Furthermore, any class function $\widetilde{\tau}$ can be decomposed into a $\mathbb{Z}$-linear combination of irreducible characters $\widetilde{\rho}$ as above, hence the vanishing of $\widetilde{\tau}(x)$ is a direct corollary of the fact that $\widetilde{\rho}(x) = 0$.

To demonstrate surjectivity, one must first study how the trace maps link together the α and β coefficients associated to a compatible family of elements $y_m \in \mathbb{Z}_p\left[\mathfrak{S}_m^{\mathrm{ab}}\right]$.

Lemma 4.0.16. *Let $\{y_m\}_{0\leq m\leq n} \in \Psi_n^{(d)}$ be a trace compatible system in $\prod \mathrm{Im}(\theta_m^+)$, with the constants $\alpha_{\sigma,m}$ and $\beta_{\sigma,\langle \underline{\mathfrak{h}}\rangle,r,m}$ associated to each y_m as in Corollary 3.3(b). Then for every $m \geq 0$ and $k \in \{1,\dots,n-m\}$:*

$$\alpha_{\sigma,m} \;=\; \alpha_{\sigma,m+k} \;+\; \sum_{r=1}^{k} \sum_{\substack{\langle \underline{\mathfrak{h}}^\dagger\rangle < H_{m+k'}^{(d)} \\ \#\langle \underline{\mathfrak{h}}^\dagger\rangle = p^r}} \beta_{\sigma,\langle \underline{\mathfrak{h}}^\dagger\rangle,r,m+k} \tag{4.4m,k}$$

$$\beta_{\sigma,\langle \underline{\mathfrak{h}}\rangle,r,m} \;=\; \sum_{\substack{\langle \underline{\mathfrak{h}}^\dagger\rangle < H_{m+k'}^{(d)} \\ \langle \underline{\mathfrak{h}}^\dagger\rangle + p^m \equiv \langle \underline{\mathfrak{h}}\rangle}} \beta_{\sigma,\langle \underline{\mathfrak{h}}^\dagger\rangle,r+k,m+k} \quad \textit{for all } \langle \underline{\mathfrak{h}}\rangle < H_m^{(d)} \textit{ with } \#\langle \underline{\mathfrak{h}}\rangle = p^r. \tag{4.5m,k}$$

Proof. Let us suppose $0 \leq m \leq n$. A short computation involving the trace map shows

$$\begin{aligned}\mathrm{Tr}_{\mathbb{Z}_p\left[\frac{1+p^m\mathbb{Z}}{1+p^n\mathbb{Z}}\times H_m^{(d)}\right]/\mathbb{Z}_p\left[\frac{1+p^{m+1}\mathbb{Z}}{1+p^n\mathbb{Z}}\times H_m^{(d)}\right]}(y_m) \;&=\; \phi(p^{m+1}) \sum_{\sigma\in\frac{1+p^{m+1}\mathbb{Z}}{1+p^n\mathbb{Z}}} \alpha_{\sigma,m}\times[\sigma]_{\frac{1+p^{m+1}\mathbb{Z}}{1+p^n\mathbb{Z}}} \\ &+ \sum_{r=1}^{m} \sum_{\substack{\langle \underline{\mathfrak{h}}\rangle < H_m^{(d)}, \\ \#\langle \underline{\mathfrak{h}}\rangle = p^r}} p^{m+1-r} \sum_{\sigma\in\frac{1+p^{m+1}\mathbb{Z}}{1+p^n\mathbb{Z}}} \beta_{\sigma,\langle \underline{\mathfrak{h}}\rangle,r,m}\times[\sigma]_{\frac{1+p^{m+1}\mathbb{Z}}{1+p^n\mathbb{Z}}}\ \mathcal{A}_{H_m^{(d)}}\langle \underline{\mathfrak{h}}\rangle\,.\end{aligned}$$

On the other hand, the element y_{m+1} is equal to

$$\begin{aligned}&\phi(p^{m+1}) \sum_{\sigma\in\frac{1+p^{m+1}\mathbb{Z}}{1+p^n\mathbb{Z}}} \alpha_{\sigma,m+1}\times[\sigma]_{\frac{1+p^{m+1}\mathbb{Z}}{1+p^n\mathbb{Z}}} \;+ \sum_{\substack{\langle \underline{\mathfrak{h}}'\rangle < H_{m+1}^{(d)}, \\ \#\langle \underline{\mathfrak{h}}'\rangle = p}} p^m \sum_{\sigma\in\frac{1+p^{m+1}\mathbb{Z}}{1+p^n\mathbb{Z}}} \beta_{\sigma,\langle \underline{\mathfrak{h}}'\rangle,1,m+1}\times \\ &\times[\sigma]_{\frac{1+p^{m+1}\mathbb{Z}}{1+p^n\mathbb{Z}}}\ \mathcal{A}_{H_{m+1}^{(d)}}\langle \underline{\mathfrak{h}}'\rangle + \sum_{s=2}^{m+1} \sum_{\substack{\langle \underline{\mathfrak{h}}'\rangle < H_{m+1}^{(d)}, \\ \#\langle \underline{\mathfrak{h}}'\rangle = p^s}} p^{m+1-s} \sum_{\sigma\in\frac{1+p^{m+1}\mathbb{Z}}{1+p^n\mathbb{Z}}} \beta_{\sigma,\langle \underline{\mathfrak{h}}'\rangle,s,m+1}\times \\ &\qquad\qquad \times[\sigma]_{\frac{1+p^{m+1}\mathbb{Z}}{1+p^n\mathbb{Z}}}\ \mathcal{A}_{H_{m+1}^{(d)}}\langle \underline{\mathfrak{h}}'\rangle\end{aligned}$$

$$\equiv \phi(p^{m+1}) \sum_{\sigma \in \frac{1+p^{m+1}\mathbb{Z}}{1+p^n\mathbb{Z}}} \alpha_{\sigma,m+1} \times [\sigma]_{\frac{1+p^{m+1}\mathbb{Z}}{1+p^n\mathbb{Z}}} + \sum_{\substack{\langle \underline{\mathfrak{h}}' \rangle < H^{(d)}_{m+1}, \\ \#\langle \underline{\mathfrak{h}}' \rangle = p}} (p-1)p^m \sum_{\sigma \in \frac{1+p^{m+1}\mathbb{Z}}{1+p^n\mathbb{Z}}} \beta_{\sigma,\langle \underline{\mathfrak{h}}' \rangle,1,m+1} \times [\sigma]_{\frac{1+p^{m+1}\mathbb{Z}}{1+p^n\mathbb{Z}}}$$

$$+ \sum_{r=1}^{m} \sum_{\substack{\langle \underline{\mathfrak{h}} \rangle < H^{(d)}_m, \\ \#\langle \underline{\mathfrak{h}} \rangle = p^r}} \sum_{\substack{\langle \underline{\mathfrak{h}}' \rangle < H^{(d)}_{m+1}, \\ \langle \underline{\mathfrak{h}}' \rangle + p^m \equiv \langle \underline{\mathfrak{h}} \rangle}} p^{m-r} \sum_{\sigma \in \frac{1+p^{m+1}\mathbb{Z}}{1+p^n\mathbb{Z}}} \beta_{\sigma,\langle \underline{\mathfrak{h}}' \rangle,r+1,m+1} \times [\sigma]_{\frac{1+p^{m+1}\mathbb{Z}}{1+p^n\mathbb{Z}}} \; p\mathcal{A}_{H^{(d)}_m} \langle \underline{\mathfrak{h}} \rangle$$

as a congruence modulo $\left(H^{(d)}_{m+1}\right)^{p^m}$.

Now we proceed with the rest of the proof using mathematical induction.

Remark 4.0.17. *(a) By assumption each* $\mathrm{Tr}(y_m) \equiv y_{m+1} \mod \left(H^{(d)}_{m+1}\right)^{p^m}$*; furthermore, the linear independence of* $[\mathrm{id}]_{H^{(d)}_m}$ *and the* $\mathcal{A}_{H^{(d)}_m}\langle \underline{\mathfrak{h}} \rangle$*'s over* $\mathbb{Z}_p\left[\frac{1+p^{m+1}\mathbb{Z}}{1+p^n\mathbb{Z}}\right]$ *implies*

$$\alpha_{\sigma,m} = \alpha_{\sigma,m+1} + \sum_{\substack{\langle \underline{\mathfrak{h}}^\dagger \rangle < H^{(d)}_{m+1}, \\ \#\langle \underline{\mathfrak{h}}^\dagger \rangle = p}} \beta_{\sigma,\langle \underline{\mathfrak{h}}^\dagger \rangle,1,m+1} \quad \text{and} \quad \beta_{\sigma,\langle \underline{\mathfrak{h}} \rangle,r,m} = \sum_{\substack{\langle \underline{\mathfrak{h}}^\dagger \rangle < H^{(d)}_{m+1}, \\ \langle \underline{\mathfrak{h}}^\dagger \rangle + p^m \equiv \langle \underline{\mathfrak{h}} \rangle}} \beta_{\sigma,\langle \underline{\mathfrak{h}}^\dagger \rangle,r+1,m+1}$$

which are none other than equations (4.4m,k) *and* (4.5m,k) *with* $k = 1$*. This proves the base step of the induction.*

(b) Let $k \in \{1, \ldots, n-m\}$*, and make the inductive assumption*

$$\alpha_{\sigma,m} = \alpha_{\sigma,m+k-1} + \sum_{r=1}^{k-1} \sum_{\substack{\langle \underline{\mathfrak{h}}^\dagger \rangle < H^{(d)}_{m+k-1}, \\ \#\langle \underline{\mathfrak{h}}^\dagger \rangle = p^r}} \beta_{\sigma,\langle \underline{\mathfrak{h}}^\dagger \rangle,r,m+k-1}.$$

Because of the trace relation $\mathrm{Tr}(y_{m+k-1}) \equiv y_{m+k} \mod \left(H^{(d)}_{m+k}\right)^{p^{m+k-1}}$*, we obtain*

$$\alpha_{\sigma,m+k-1} = \alpha_{\sigma,m+k} + \sum_{\substack{\langle \underline{\mathfrak{h}}^{\dagger\dagger} \rangle < H^{(d)}_{m+k}, \\ \#\langle \underline{\mathfrak{h}}^{\dagger\dagger} \rangle = p}} \beta_{\sigma,\langle \underline{\mathfrak{h}}^{\dagger\dagger} \rangle,1,m+k} \quad \text{and}$$

$$\beta_{\sigma,\langle \underline{\mathfrak{h}}^\dagger \rangle,r,m+k-1} = \sum_{\substack{\langle \underline{\mathfrak{h}}^{\dagger\dagger} \rangle < H^{(d)}_{m+k}, \\ \langle \underline{\mathfrak{h}}^{\dagger\dagger} \rangle + p^{m+k-1} \equiv \langle \underline{\mathfrak{h}}^\dagger \rangle}} \beta_{\sigma,\langle \underline{\mathfrak{h}}^{\dagger\dagger} \rangle,r+1,m+k}.$$

Combining these two equations with our inductive assumption yields

$$\alpha_{\sigma,m} \;=\; \alpha_{\sigma,m+k} \;+\; \sum_{r=1}^{k} \sum_{\substack{\langle \underline{\mathfrak{h}}^{\dagger\dagger} \rangle < H_{m+k}^{(d)}, \\ \#\langle \underline{\mathfrak{h}}^{\dagger\dagger} \rangle = p^r}} \beta_{\sigma,\langle \underline{\mathfrak{h}}^{\dagger\dagger} \rangle,r,m+k}.$$

Thus for each $m \geq 0$, equation (4.4m,k) *holds for any $k \in \{1, \ldots, n-m\}$.*

(c) Again, let $k \in \{1, \ldots, n-m\}$, and make the inductive assumption

$$\beta_{\sigma,\langle \underline{\mathfrak{h}} \rangle,r,m} \;=\; \sum_{\substack{\langle \underline{\mathfrak{h}}^{\dagger} \rangle < H_{m+k-1}^{(d)}, \\ \langle \underline{\mathfrak{h}}^{\dagger} \rangle + p^m \equiv \langle \underline{\mathfrak{h}} \rangle}} \beta_{\sigma,\langle \underline{\mathfrak{h}}^{\dagger} \rangle,r+k-1,m+k-1} \quad \textit{for all } \langle \underline{\mathfrak{h}} \rangle < H_{m+k}^{(d)} \textit{ with } \#\langle \underline{\mathfrak{h}} \rangle = p^r.$$

Finally, by combining

$$\beta_{\sigma,\langle \underline{\mathfrak{h}}^{\dagger} \rangle,r+k-1,m+k-1} \;=\; \sum_{\substack{\langle \underline{\mathfrak{h}}^{\dagger\dagger} \rangle < H_{m+k}^{(d)}, \\ \langle \underline{\mathfrak{h}}^{\dagger\dagger} \rangle + p^{m+k-1} \equiv \langle \underline{\mathfrak{h}}^{\dagger} \rangle}} \beta_{\sigma,\langle \underline{\mathfrak{h}}^{\dagger\dagger} \rangle,r+k,m+k}$$

(which arises from the trace relation $\mathrm{Tr}(y_{m+k-1}) \equiv y_{m+k} \mod \left(H_{m+k}^{(d)}\right)^{p^{m+k-1}}$*) with our inductive assumption,*

$$\beta_{\sigma,\langle \underline{\mathfrak{h}} \rangle,r,m} \;=\; \sum_{\substack{\langle \underline{\mathfrak{h}}^{\dagger\dagger} \rangle < H_{m+k}^{(d)}, \\ \langle \underline{\mathfrak{h}}^{\dagger\dagger} \rangle + p^m \equiv \langle \underline{\mathfrak{h}} \rangle}} \beta_{\sigma,\langle \underline{\mathfrak{h}}^{\dagger\dagger} \rangle,r+k,m+k} \quad \textit{for all } \langle \underline{\mathfrak{h}} \rangle < H_{m}^{(d)} \textit{ with } \#\langle \underline{\mathfrak{h}} \rangle = p^r.$$

Hence for each $m \geq 0$, equation (4.5m,k) *holds for all $k \in \{1, \ldots, n-m\}$.*

The proof of Lemma 4.0.16 is finished. □

We are ready to establish the surjectivity of $\prod \theta_m^+$. Let $\{y_m\} \in \Psi_n^{(d)}$ denote a trace compatible family, whose associated structure constants are $\alpha_{\sigma,m}$ and $\beta_{\sigma,\langle \underline{\mathfrak{h}} \rangle,r,m}$. One next defines an element $x \in \mathrm{Conj}\left(G_n^{(d)}\right)$ by

$$x = \sum_{\sigma\in\Sigma_n - \frac{1+p\mathbb{Z}}{1+p^n\mathbb{Z}}} \alpha_{\sigma,0}\left[\sigma\cdot \mathrm{id}_{H_n^{(d)}}\right]_{G_n^{(d)}} +$$
$$+\sum_{\nu=1}^{n}\sum_{\substack{\sigma\equiv 1(\bmod p^\nu),\\ \sigma\not\equiv 1(\bmod p^{\nu+1})}}\left(\alpha_{\sigma,\nu}\left[\sigma\cdot \mathrm{id}_{H_n^{(d)}}\right]_{G_n^{(d)}} + \sum_{r=1}^{\nu}\sum_{\substack{\langle\overline{\underline{h}}\rangle<H_\nu^{(d)},\\ \mathrm{order}(\overline{\underline{h}})=p^r}}\beta_{\sigma,\langle\overline{\underline{h}}\rangle,r,\nu}\left[\sigma\cdot \underline{h}\right]_{G_n^{(d)}}\right).$$

Then repeatedly applying Proposition 3.1.9(i), at each $m\in\{0,\dots,n\}$ one calculates

$$\theta_m(x) = \sum_{\substack{\sigma\equiv 1(\bmod p^m),\\ \sigma\not\equiv 1(\bmod p^{m+1})}} C_\sigma^{(m)}\times[\sigma]_{\frac{1+p^m\mathbb{Z}}{1+p^n\mathbb{Z}}} + \sum_{\nu=m+1}^{n}\sum_{\substack{\sigma\equiv 1(\bmod p^\nu),\\ \sigma\not\equiv 1(\bmod p^{\nu+1})}} D_{\sigma,\nu}^{(m)}\times[\sigma]_{\frac{1+p^m\mathbb{Z}}{1+p^n\mathbb{Z}}}$$

where the group ring elements $C_\sigma^{(m)},\ D_{\sigma,\nu}^{(m)}\in\mathbb{Z}_p\left[H_m^{(d)}\right]$ satisfy

$$C_\sigma^{(m)} = \phi(p^m)\ \alpha_{\sigma,m}\ [\mathrm{id}]_{H_m^{(d)}} + \sum_{s=1}^{m}\sum_{\substack{\langle\underline{\mathfrak{h}}\rangle<H_m^{(d)},\\ \mathrm{order}(\underline{\mathfrak{h}})=p^s}} p^{m-s}\beta_{\sigma,\langle\underline{\mathfrak{h}}\rangle,s,m}\mathcal{A}_{H_m^{(d)}}\left\langle\underline{\mathfrak{h}}\right\rangle$$

and
$$D_{\sigma,\nu}^{(m)} = \phi(p^m)\left(\alpha_{\sigma,\nu} + \sum_{r=1}^{\nu-m}\sum_{\substack{\langle\overline{\underline{h}}\rangle<H_\nu^{(d)},\\ \mathrm{order}(\overline{\underline{h}})=p^r}}\beta_{\sigma,\langle\overline{\underline{h}}\rangle,r,\nu}\right)[\mathrm{id}]_{H_m^{(d)}}$$
$$+\sum_{s=1}^{m}\sum_{\substack{\langle\underline{\mathfrak{h}}\rangle<H_m^{(d)},\\ \mathrm{order}(\underline{\mathfrak{h}})=p^s}} p^{m-s}\sum_{\substack{\langle\overline{\underline{h}}\rangle<H_\nu^{(d)},\\ \langle\overline{\underline{h}}\rangle+p^m\equiv\langle\underline{\mathfrak{h}}\rangle}}\beta_{\sigma,\langle\overline{\underline{h}}\rangle,s+\nu-m,\nu}\mathcal{A}_{H_m^{(d)}}\left\langle\underline{\mathfrak{h}}\right\rangle.$$

Substituting in Equations (4.4m,k) and (4.5m,k) with $k=\nu-m$ yields

$$D_{\sigma,\nu}^{(m)} = \phi(p^m)\alpha_{\sigma,m}\,[\mathrm{id}]_{H_m^{(d)}} + \sum_{s=1}^{m}\sum_{\substack{\langle\underline{\mathfrak{h}}\rangle<H_m^{(d)},\\ \mathrm{order}(\underline{\mathfrak{h}})=p^s}} p^{m-s}\beta_{\sigma,\langle\underline{\mathfrak{h}}\rangle,s,m}\mathcal{A}_{H_m^{(d)}}\left\langle\underline{\mathfrak{h}}\right\rangle.$$

Therefore we can simplify our expression for $\theta_m(x)$, which neatly collapses to

$$\sum_{\nu=m}^{n} \sum_{\substack{\sigma\equiv 1(\bmod p^{\nu}),\\ \sigma\not\equiv 1(\bmod p^{\nu+1})}} \left(\phi(p^m)\ \alpha_{\sigma,m} + \sum_{s=1}^{m} \sum_{\substack{\langle \underline{\mathfrak{h}} \rangle < H_m^{(d)},\\ \operatorname{order}(\underline{\mathfrak{h}})=p^s}} p^{m-s} \beta_{\sigma,\langle \underline{\mathfrak{h}} \rangle,s,m} \mathcal{A}_{H_m^{(d)}}\left\langle \underline{\mathfrak{h}} \right\rangle \right) \times [\sigma]_{\frac{1+p^m\mathbb{Z}}{1+p^n\mathbb{Z}}}.$$

The latter formula coincides with that of y_m, i.e. $\theta_m^+(x) = y_m$ for all $m \in \{0, \ldots, n\}$ and the proof of surjectivity is now finished. □

5 The Multiplicative Setting

To translate back from the additive to the multiplicative world, the method of Kakde et al. [8, 20, 22] is employed. The Taylor-Oliver p-adic logarithm (defined in 2.9) is essential in this translation, and the situation is neatly encapsulated in a fundamental commutative diagram (Theorem 5.0.21) whose proof occupies the majority of this chapter.

In regard to the Taylor-Oliver logarithm, throughout this thesis we take $R = \mathbb{Z}_p$, and need only consider sub-quotients G of the finite group $G_n^{(d)} \cong \Sigma_n \ltimes H_n^{(d)}$. The following construction mirrors the additive theta maps in Definition 3.1.8:

Definition 5.0.18. *(a) If $m \leq n$, the m^{th}-level multiplicative theta map*

$$\theta_m : K_1\big(\mathbb{Z}_p[G_n^{(d)}]\big) \longrightarrow K_1\big(\mathbb{Z}_p[\mathfrak{S}_m^{\text{ab}}]\big) \cong \mathbb{Z}_p\big[\mathfrak{S}_m^{\text{ab}}\big]^\times$$

is built by forming the composition $\theta_m(z) := \mathrm{Nr}_{G_n^{(d)}/\mathfrak{S}_m}(z) \mod [\mathfrak{S}_m, \mathfrak{S}_m]$, where we write $\mathrm{Nr}_{G_n^{(d)}/\mathfrak{S}_m} : K_1\big(\mathbb{Z}_p[G_n^{(d)}]\big) \to K_1\big(\mathbb{Z}_p[\mathfrak{S}_m]\big)$ for the norm homomorphism.

(b) Likewise for each character $\chi : H_m \to \mu_{p^m}$, one defines the map $\theta_{\chi_m} := \chi \circ \theta_m$.

We claim that θ_0 is surjective. To justify this assertion, note that the inclusion $\iota : \Sigma_n \cong \Sigma_n \ltimes \{1\} \hookrightarrow \Sigma_n \ltimes H_n^{(d)}$ identifies Σ_n with a non-normal subgroup of $G_n^{(d)}$, and thus induces a map $\iota_* : K_1\big(\mathbb{Z}_p[\Sigma_n]\big) \to K_1\big(\mathbb{Z}_p[G_n^{(d)}]\big)$. Moreover the projection

$$G_n^{(d)} \overset{\mod H_n^{(d)}}{\twoheadrightarrow} \Sigma_n \quad \text{gives rise to} \quad \theta_0 : K_1\big(\mathbb{Z}_p[G_n^{(d)}]\big) \to K_1\big(\mathbb{Z}_p[\Sigma_n]\big);$$

because $\iota \bmod H_n^{(d)}$ is the identity map, the homomorphism it induces $\theta_0 \circ \iota_*$

must also be the identity (and therefore surjective), hence our claim is true.

One should point out that the above construction produces a splitting of K_1 in the following way. If $x \in K_1\big(\mathbb{Z}_p[G_n^{(d)}]\big)$ then define $x^{\mathrm{cy}} := \iota_* \circ \theta_0(x)$ and $x^{\dagger} := x/x^{\mathrm{cy}}$. We thereby obtain a direct product decomposition

$$K_1\big(\mathbb{Z}_p[G_n^{(d)}]\big) \xrightarrow{\sim} K_1\big(\mathbb{Z}_p[\Sigma_n]\big) \times \mathcal{W}^{\dagger} \quad \text{by sending} \quad x \mapsto \big(\theta_0(x), x^{\dagger}\big)$$

where the complementary subgroup $\mathcal{W}^{\dagger} := \big\{ x \cdot \iota_*\big(\theta_0(x)\big)^{-1} \mid x \in K_1\big(\mathbb{Z}_p[G_n^{(d)}]\big) \big\}$.

Remark 5.0.19. *(i) For $m \leq n$ we write $N_{0,m}$ as an abbreviation for the homomorphism*

$$\mathrm{Nr}_{\Sigma_n / \frac{1+p^m\mathbb{Z}}{1+p^n\mathbb{Z}}} : K_1\big(\mathbb{Z}_p[\Sigma_n]\big) \longrightarrow K_1\Big(\mathbb{Z}_p\Big[\frac{1+p^m\mathbb{Z}}{1+p^n\mathbb{Z}}\Big]\Big)$$

induced from the norm map on group algebras.

(ii) The natural inclusion $\tau^{(m)} : \frac{1+p^m\mathbb{Z}}{1+p^n\mathbb{Z}} \cong \frac{1+p^m\mathbb{Z}}{1+p^n\mathbb{Z}} \ltimes \{1\} \hookrightarrow \mathfrak{S}_m^{\mathrm{ab}}$ yields

$$\tau_*^{(m)} : K_1\Big(\mathbb{Z}_p\Big[\frac{1+p^m\mathbb{Z}}{1+p^n\mathbb{Z}}\Big]\Big) \longrightarrow K_1\big(\mathbb{Z}_p[\mathfrak{S}_m^{\mathrm{ab}}]\big)$$

hence the composition $\tau_*^{(m)} \circ N_{0,m}$ allows us to compare elements in $K_1\big(\mathbb{Z}_p[\Sigma_n]\big)$ with those in $K_1\big(\mathbb{Z}_p[\mathfrak{S}_m^{\mathrm{ab}}]\big)$ – if the context is clear, we drop the superscript $^{(m)}$. Also, note that $\tau_*^{(0)} = \iota_*$.

(iii) The twist map $\underline{\mathrm{tw}}_n : \prod_{m=0}^n K_1\big(\mathbb{Z}_p[\mathfrak{S}_m^{\mathrm{ab}}]\big) \longrightarrow \{1\} \times \prod_{m=1}^n K_1\big(\mathbb{Z}_p[\mathfrak{S}_m^{\mathrm{ab}}]\big)$ is given by the formula

$$\underline{\mathrm{tw}}_n\big((z_0, \ldots, z_n)\big) := \Big(1, \ \ldots \ , \frac{z_m}{\tau_* N_{0,m}(z_0)}, \ \ldots\Big).$$

(iv) Lastly for all $x \in K_1\big(\mathbb{Z}_p[G_n^{(d)}]\big)$, notice that

$$\begin{aligned}
\theta_m(x^{\,\mathrm{cy}}) &= \theta_m(\tau_*^{(0)}(\theta_0(x))) \quad \big(\textit{ because } x^{\,\mathrm{cy}} = \tau_*^{(0)}(\theta_0(x))\big) \\
&\overset{\text{by 5.0.18(a)}}{=} \mathrm{Nr}_{G_n^{(d)}/\mathfrak{S}_m}(\tau_*^{(0)}(x \mod H_n^{(d)})) \mod \big(H_n^{(d)}\big)^{p^m} \\
&= \tau_*^{(m)} N_{0,m}(x \mod H_n^{(d)}) = \tau_*^{(m)} N_{0,m}(\theta_0(x)),
\end{aligned}$$

which implies $\theta_0(x^{\,\mathrm{cy}}) = \theta_0(x)$ and the identity

$$\underline{\mathrm{tw}}_n\Big(\prod \theta_m\big(x^{\mathrm{cy}}\big)\Big) = (1,\dots,1).$$

This latter equation also implies

$$\underline{\mathrm{tw}}_n\Big(\prod \theta_m(x)\Big) = \underline{\mathrm{tw}}_n\Big(\prod \theta_m\big(x^{\dagger}\big)\Big).$$

Now if $m \geq 2$, the mapping $\varphi_{\mathfrak{S}^{\mathrm{ab}}_{m-1}}$ can be interpreted as taking values in $\mathbb{Z}_p[\mathfrak{S}^{\mathrm{ab}}_m]$; indeed one can form a sequence

$$\frac{1+p^{m-1}\mathbb{Z}}{1+p^n\mathbb{Z}} \times H^{(d)}_{m-1} \xrightarrow{(-)^p} \frac{1+p^m\mathbb{Z}}{1+p^n\mathbb{Z}} \times \big(H^{(d)}_{m-1}\big)^p \xrightarrow{\sim} \frac{1+p^m\mathbb{Z}}{1+p^n\mathbb{Z}} \times \left(\bigoplus_{j=1}^{d} \frac{p^2\mathbb{Z}}{p^m\mathbb{Z}}\right) \hookrightarrow \mathfrak{S}^{\mathrm{ab}}_m$$

and we abuse notation by writing $\tilde{\varphi}_{\mathfrak{S}^{\mathrm{ab}}_{m-1}} : \mathbb{Z}_p[\mathfrak{S}^{\mathrm{ab}}_{m-1}] \to \mathbb{Z}_p[\mathfrak{S}^{\mathrm{ab}}_m]$ for the composition. The vector logarithm $\underline{\log}^{\dagger}_n : \{1\} \times \prod_{m=1}^n K_1\big(\mathbb{Z}_p[\mathfrak{S}^{\mathrm{ab}}_m]\big) \longrightarrow \{0\} \times \prod_{m=1}^n \mathbb{Q}_p[\mathfrak{S}^{\mathrm{ab}}_m]$ is then defined to be

$$\underline{\log}^{\dagger}_n\big((1,z_1,\dots,z_n)\big) := \left(0,\ \log_{\mathbb{Z}_p[\mathfrak{S}^{\mathrm{ab}}_1]}(z_1),\ \dots\ , \log_{\mathbb{Z}_p[\mathfrak{S}^{\mathrm{ab}}_m]}\Big(\frac{z_m}{\tilde{\varphi}_{\mathfrak{S}^{\mathrm{ab}}_{m-1}}(z_{m-1})}\Big),\ \dots\right).$$

In particular, the vector logarithm can be composed with the twist map to yield a homomorphism $\underline{\log}^{\dagger}_n \circ \underline{\mathrm{tw}}_n$, sending vectors in K_1 to n-tuples of additive elements.

Definition 5.0.20. *Let us define two subgroups of* $\prod_{m=0}^n \mathbb{Z}_p\big[\mathfrak{S}^{\mathrm{ab}}_m\big]^{\times}$ *by taking*

$$\Omega^{(d)}_{n,\mathrm{cy}} := \Big\{\big(\dots, \tau_* N_{0,m}(z),\ \dots\big)_{0\leq m\leq n} \text{ where } z \in \mathbb{Z}_p[\Sigma_n]^{\times}\Big\},$$

$$\Omega^{(d)}_{n,\dagger} := \Big\{\underline{z} \in \{1\} \times \prod_{m=1}^{n} 1 + p\mathbb{Z}_p\big[\mathfrak{S}^{\mathrm{ab}}_m\big] \text{ such that } \underline{\log}^{\dagger}_n \circ \underline{\mathrm{tw}}_n(\underline{z}) \in \Psi^{(d)}_n\Big\}$$

and write $\Omega^{(d)}_n \subset \prod_{m=0}^n K_1\Big(\mathbb{Z}_p\big[\mathfrak{S}^{\mathrm{ab}}_m\big]\Big)$ *for the group generated by* $\Omega^{(d)}_{n,\mathrm{cy}}$ *and* $\Omega^{(d)}_{n,\dagger}$.

The connection between the multiplicative and additive settings is neatly captured by the following result, which gives us a natural analogue of Proposition 4.1 of [8].

Theorem 5.0.21. *For each integer $n \geq 1$, there is a commutative diagram*

$$\begin{array}{ccc} K_1\big(\mathbb{Z}_p[G_n^{(d)}]\big) & \overset{\Gamma_{G_n^{(d)}} \circ (-)^\dagger}{\longrightarrow} & \mathbb{Z}_p\big[\mathrm{Conj}(G_n^{(d)})\big] \\ \big\downarrow \prod \theta_m & & \big\downarrow \prod \theta_m^+ \\ \prod_{m=0}^{n} K_1\big(\mathbb{Z}_p[\mathfrak{S}_m^{\mathrm{ab}}]\big) & \overset{\log_n^\dagger \circ \underline{\mathrm{tw}}_n}{\longrightarrow} & \prod_{m=0}^{n} \mathbb{Q}_p\big[\mathfrak{S}_m^{\mathrm{ab}}\big] \end{array}$$

and the kernel of $\Theta := \prod \theta_m$ is equal to $SK_1\big(\mathbb{Z}_p[G_n^{(d)}]\big)$, while the image of Θ coincides with $\Omega_n^{(d)}$.

Thus the question as to whether a vector $\underline{z}$ arises from an element of $K_1\big(\mathbb{Z}_p[G_n^{(d)}]\big)$ under $\prod \theta_m$ reduces to establishing whether $\underline{\mathrm{tw}}_n(\underline{z})$ belongs to $\Omega_n^{(d)} = \mathrm{Im}\big(\prod \theta_m\big)$, which in turn is equivalent to checking if $\underline{\log}_n^\dagger \circ \underline{\mathrm{tw}}_n(\underline{z})$ lies in $\Psi_n^{(d)} = \mathrm{Im}\big(\prod \theta_m^+\big)$. The proof of the above theorem is lengthy and will occupy the rest of this chapter.

5.1 Three Technical Lemmas

We begin by studying the interactions between the various maps θ_m, φ and log. The results below describe how these homomorphisms commute with each other, although the proofs themselves could probably be skipped on a first reading.

Lemma 5.1.1. *(i) If $m \geq 2$ and $y \in \mathbb{Q}_p\big[\mathrm{Conj}\big(G_n^{(d)}\big)\big]$, then*

$$\theta_m^+ \circ \varphi_{G_n^{(d)}}(y) = p \times \varphi_{\frac{1+p^{m-1}\mathbb{Z}}{1+p^n\mathbb{Z}} \ltimes H_m^{(d)}}\Big(\mathrm{Tr}_{G_n^{(d)}/\mathfrak{S}_{m-1}}(y) \mod \big(H_n^{(d)}\big)^{p^m}\Big).$$

(ii) If $m = 1$ and $y \in \mathbb{Q}_p\big[\mathrm{Conj}\big(G_n^{(d)}\big)\big]$, then

$$\theta_1^+ \circ \varphi_{G_n^{(d)}}(y) = \mathrm{Tr}_{\Sigma_n \big/ \frac{1+p\mathbb{Z}}{1+p^n\mathbb{Z}}}\Big(\varphi_{\Sigma_n}\big(\theta_0^+(y)\big)\Big).$$

Proof. By the $\mathbb{Q}_p$-linearity of the maps involved, it is enough to check the formulae at individual classes $y = \big[\sigma \cdot \underline{h}\big]_{G_n^{(d)}} \in \mathrm{Conj}\big(G_n^{(d)}\big)$. Assuming that $m \geq 2$, one

has

$$\theta_m^+ \circ \varphi_{G_n^{(d)}}(y) \overset{\text{by 3.1.9(i)}}{=} \begin{cases} \left[\sigma^p\right]_{\frac{1+p^m\mathbb{Z}}{1+p^n\mathbb{Z}}} \times \sum_{u\in(\mathbb{Z}/p^m\mathbb{Z})^\times} \left[u\underline{\overline{h}}^p\right]_{H_m^{(d)}} & \text{if } \sigma^p \equiv 1(\bmod p^m) \\ 0 & \text{otherwise.} \end{cases}$$

On the other hand

$$\begin{aligned} &\varphi_{\frac{1+p^{m-1}\mathbb{Z}}{1+p^n\mathbb{Z}}\ltimes H_m^{(d)}} \circ \mathrm{Tr}_{G_n^{(d)}/\mathfrak{S}_{m-1}}(y) \pmod{\left(H_n^{(d)}\right)^{p^m}} \\ &\quad = \begin{cases} \varphi\Big(\sum_{u\in(\mathbb{Z}/p^{m-1}\mathbb{Z})^\times} \left[\sigma\cdot u\underline{\overline{h}}\right]_{\frac{1+p^{m-1}\mathbb{Z}}{1+p^n\mathbb{Z}}\ltimes H_m^{(d)}}\Big) & \text{if } \sigma \equiv 1(\bmod p^{m-1}) \\ 0 & \text{if } \sigma \not\equiv 1(\bmod p^{m-1}) \end{cases} \\ &\quad = \begin{cases} \frac{1}{p}\times\sum_{u\in(\mathbb{Z}/p^m\mathbb{Z})^\times} \left[\sigma^p\cdot u\underline{\overline{h}}^p\right]_{\frac{1+p^m\mathbb{Z}}{1+p^n\mathbb{Z}}\times H_m^{(d)}} & \text{if } \sigma \equiv 1(\bmod p^{m-1}) \\ 0 & \text{if } \sigma \not\equiv 1(\bmod p^{m-1}) \end{cases} \end{aligned}$$

which is exactly $(1/p)$-th of the previous quantity, so the first statement follows. To prove (ii) one calculates that

$$\theta_1^+ \circ \varphi_{G_n^{(d)}}(y) \overset{\text{by 3.1.9(i)}}{=} \begin{cases} \left[\sigma^p\right]_{\frac{1+p\mathbb{Z}}{1+p^n\mathbb{Z}}} \times (p-1)\left[\mathrm{id}\right]_{H_1^{(d)}} & \text{if } \sigma^p \equiv 1(\bmod p) \\ 0 & \text{otherwise.} \end{cases}$$

However $\varphi_{\Sigma_n}\big(\theta_0^+(y)\big) = \left[\sigma^p\right]_{\Sigma_n}$ as $\theta_0^+(y) = [\sigma]_{\Sigma_n}$, hence

$$\mathrm{Tr}_{\Sigma_n/\frac{1+p\mathbb{Z}}{1+p^n\mathbb{Z}}}\Big(\varphi_{\Sigma_n}\big(\theta_0^+(y)\big)\Big) = \begin{cases} \sum_{u\in(\mathbb{Z}/p\mathbb{Z})^\times} \left[\sigma^p\right]_{\frac{1+p\mathbb{Z}}{1+p^n\mathbb{Z}}} & \text{if } \sigma^p \equiv 1(\bmod p) \\ 0 & \text{if } \sigma^p \not\equiv 1(\bmod p), \end{cases}$$

which means both quantities above coincide. □

Lemma 5.1.2. *(a) The mutually inverse maps* $\log : 1 + p\mathbb{Z}_p\left[\mathfrak{S}_m^{\mathrm{ab}}\right] \xrightarrow{\sim} p\mathbb{Z}_p\left[\mathfrak{S}_m^{\mathrm{ab}}\right]$ *and* $\exp : p\mathbb{Z}_p\left[\mathfrak{S}_m^{\mathrm{ab}}\right] \xrightarrow{\sim} 1 + p\mathbb{Z}_p\left[\mathfrak{S}_m^{\mathrm{ab}}\right]$ *restrict to yield isomorphisms*

$$1 + p\mathrm{Im}(\theta_m^+) \xrightarrow{\log} p\mathrm{Im}(\theta_m^+) \xrightarrow{\exp} 1 + p\mathrm{Im}(\theta_m^+).$$

(b) For each pair of integers $m, n \geq 2$, there is an isomorphism

$$\frac{1+\mathrm{Im}(\theta_m^+)^n}{1+\mathrm{Im}(\theta_m^+)^{n+1}} \xrightarrow{\sim} \frac{\mathrm{Im}(\theta_m^+)^n}{\mathrm{Im}(\theta_m^+)^{n+1}}, \quad 1+y \mapsto y$$

induced by the p-adic logarithm.

Proof. Recall first that $\mathrm{Im}(\theta_m^+) \cong \mathbb{Z}_p[\Sigma'] \otimes_{\mathbb{Z}_p} \mathbb{Z}_p \left\langle \mathcal{S}_m^{(\mathcal{A})} \right\rangle$ where $\Sigma' = \frac{1+p^m\mathbb{Z}}{1+p^n\mathbb{Z}}$, and

$$\mathcal{S}_m^{(\mathcal{A})} = \left\{ \phi(p^m) \cdot \mathrm{id}_{H_m^{(d)}} \right\} \cup \left\{ p^{m-\nu_m(\underline{\mathfrak{h}})} \cdot \mathcal{A}_{H_m^{(d)}} \langle \underline{\mathfrak{h}} \rangle \;\middle|\; 0 \neq \langle \underline{\mathfrak{h}} \rangle < H_m^{(d)} \right\}.$$

If we define $\mathfrak{a}_{\underline{\mathfrak{h}}} := \begin{cases} p^{m-\nu_m(\underline{\mathfrak{h}})} \cdot \mathcal{A}_{H_m^{(d)}} \langle \underline{\mathfrak{h}} \rangle & \text{if } \langle \underline{\mathfrak{h}} \rangle \neq 0 \\ \phi(p^m) \cdot \mathrm{id}_{H_m^{(d)}} & \text{if } \langle \underline{\mathfrak{h}} \rangle = 0 \end{cases}$, then

- $$\frac{\phi(p^m)}{\phi(p^{\nu_m(\underline{\mathfrak{h}}_1)})} \mathcal{A}_{H_m^{(d)}} \left\langle \underline{\mathfrak{h}}_1 \right\rangle \frac{\phi(p^m)}{\phi(p^{\nu_m(\underline{\mathfrak{h}}_2)})} \mathcal{A}_{H_m^{(d)}} \left\langle \underline{\mathfrak{h}}_2 \right\rangle = \sum_{t_1 \in (\mathbb{Z}/p^m\mathbb{Z})^\times} [\underline{\mathfrak{h}}_1^{t_1}]_{H_m^{(d)}} \times \sum_{t_2 \in (\mathbb{Z}/p^m\mathbb{Z})^\times} [\underline{\mathfrak{h}}_2^{t_2}]_{H_m^{(d)}}$$
$$= \sum_{t_1,t_2 \in (\mathbb{Z}/p^m\mathbb{Z})^\times} [\underline{\mathfrak{h}}_1^{t_1}\underline{\mathfrak{h}}_2^{t_2}]_{H_m^{(d)}} = \sum_{t_1,t_2 \in (\mathbb{Z}/p^m\mathbb{Z})^\times} [\underline{\mathfrak{h}}_1^{t_1}\underline{\mathfrak{h}}_2^{t_1 t_2}]_{H_m^{(d)}}$$
$$= \sum_{t_1,t_2 \in (\mathbb{Z}/p^m\mathbb{Z})^\times} [(\underline{\mathfrak{h}}_1^{t_1}\underline{\mathfrak{h}}_2^{t_2})^{t_1}]_{H_m^{(d)}} = \sum_{t_2 \in (\mathbb{Z}/p^m\mathbb{Z})^\times} \frac{\phi(p^m)}{\phi(p^{\nu(\underline{\mathfrak{h}}_1\underline{\mathfrak{h}}_2^{t_1})})} \mathcal{A}_{H_m^{(d)}} \left\langle \underline{\mathfrak{h}}_1\underline{\mathfrak{h}}_2^{t_2} \right\rangle;$$
- $$\phi(p^m)[\mathrm{id}]_{H_m^{(d)}} \times \frac{\phi(p^m)}{\phi(p^{\nu_m}(\underline{\mathfrak{h}}_1))} \mathcal{A}_{H_m^{(d)}} \left\langle \underline{\mathfrak{h}}_1 \right\rangle = \phi(p^m) \times \frac{\phi(p^m)}{\phi(p^{\nu_m(\underline{\mathfrak{h}}_1)})} \mathcal{A}_{H_m^{(d)}} \left\langle \underline{\mathfrak{h}}_1 \right\rangle;$$
- and $\phi(p^m)[\mathrm{id}]_{H_m^{(d)}} \times \phi(p^m)[\mathrm{id}]_{H_m^{(d)}} = \phi(p^m)\phi(p^m)[\mathrm{id}]_{H_m^{(d)}}$; thus
$$\mathfrak{a}_{\underline{\mathfrak{h}}_1} \times \mathfrak{a}_{\underline{\mathfrak{h}}_2} = \sum_{t \in (\mathbb{Z}/p^m\mathbb{Z})^\times} \mathfrak{a}_{\underline{\mathfrak{h}}_1\underline{\mathfrak{h}}_2^t}.$$

In particular, the image of θ_m^+ is generated over $\mathbb{Z}_p[\Sigma']$ by the finite set of $\mathfrak{a}_{\underline{\mathfrak{h}}}$'s (which are closed under multiplication), hence $\mathrm{Im}(\theta_m^+)$ forms an ideal of $\mathbb{Z}_p[\mathfrak{S}_m^{\mathrm{ab}}]$. The demonstration of (a) is then identical to that given at the end of p. 106 in [8]. To prove statement (b), we first collect together four key facts describing $\mathrm{Im}(\theta_m^+)$ and assume throughout that $m \geq 2$:

Fact 1. *If one of $\underline{h}_1, \underline{h}_2 \in H_m^{(d)}$ has order $< p^m$, then $\mathfrak{a}_{\underline{h}_1}\mathfrak{a}_{\underline{h}_2} \in p\ \mathrm{Im}(\theta_m^+)$.*

Fact 2. $\left(\mathfrak{a}_{\underline{h}}\right)^3 \in p\ \mathrm{Im}(\theta_m^+)$ *for every $\underline{h} \in H_m^{(d)}$.*

Fact 3. $\frac{y^i}{i} \in p^{\lfloor i/p \rfloor - \log(i)/\log(p)} \mathrm{Im}(\theta_m^+)$ *at each $y \in \mathrm{Im}(\theta_m^+)$.*

Fact 4. $\mathrm{Im}(\theta_m^+)^{1+\frac{p^{md}-p^{(m-1)d}}{p^m-p^{m-1}}} \subset p\ \mathrm{Im}(\theta_m^+)$.

For instance Fact 3 means both the power series $\log(1+y) = \sum_{i=1}^{\infty} \frac{(-1)^{i+1}y^i}{i}$ and $(1+y)^{-1} = \sum_{i=0}^{\infty}(-1)^i y^i$ converge inside $\mathrm{Im}(\theta_m^+)$, whilst Fact 4 implies the topology induced by the neighbourhoods $\left\{\mathrm{Im}(\theta_m^+)^j\right\}_{j\in\mathbb{N}}$ coincides with the p-adic topology.

Proof of Fact 1: Since $\mathfrak{a}_{\underline{\mathfrak{h}}_1} \times \mathfrak{a}_{\underline{\mathfrak{h}}_2} = \sum_{t_1\in(\mathbb{Z}/p^m\mathbb{Z})^\times} \mathfrak{a}_{\underline{\mathfrak{h}}_1\underline{\mathfrak{h}}_2^{t_1}}$, by iterating one obtains

$$\mathfrak{a}_{\underline{\mathfrak{h}}_1} \times \mathfrak{a}_{\underline{\mathfrak{h}}_2} \times \cdots \times \mathfrak{a}_{\underline{\mathfrak{h}}_{N+1}} = \sum_{t_1,t_2,\ldots,t_N\in(\mathbb{Z}/p^m\mathbb{Z})^\times} \mathfrak{a}_{\underline{\mathfrak{h}}_1\underline{\mathfrak{h}}_2^{t_1}\ldots\underline{\mathfrak{h}}_{N+1}^{t_N}} = \prod_{j=1}^{N+1} \frac{\phi(p^m)}{\phi(p^{\nu_m(\underline{h}_j)})} \times \sum_{\underline{\mathfrak{h}}\in\mathcal{T}_N} \mathfrak{a}_{\underline{\mathfrak{h}}}$$

where $\mathcal{T}_N = \left\langle \underline{\mathfrak{h}}_1 \right\rangle_{\mathrm{gen}} \left\langle \underline{\mathfrak{h}}_2 \right\rangle_{\mathrm{gen}} \ldots \left\langle \underline{\mathfrak{h}}_{N+1} \right\rangle_{\mathrm{gen}}$. Note that the coefficient is divisible by

$$\prod_{j=1,\ \nu_m(\underline{\mathfrak{h}}_j)=0}^{N+1} p^{m-1} \ \times \prod_{j=1,\ \nu_m(\underline{\mathfrak{h}}_j)>0}^{N+1} p^{m-\nu_m(\underline{\mathfrak{h}}_j)}.$$

In the special case $N=1$, if either $\nu_m(\underline{\mathfrak{h}}_1) < m$ or $\nu_m(\underline{\mathfrak{h}}_2) < m$ then this quantity must itself be divisible by p, hence $\mathfrak{a}_{\underline{h}_1} \times \mathfrak{a}_{\underline{h}_2} \in p\ \mathrm{Im}(\theta_m^+)$ as asserted. □

Proof of Fact 2: Some elementary calculations reveal

$$\begin{aligned}\left(\mathfrak{a}_{\underline{h}}\right)^2 = \mathfrak{a}_{\underline{h}} \times \mathfrak{a}_{\underline{h}} &= \sum_{t\in(\mathbb{Z}/p^m\mathbb{Z})^\times} \mathfrak{a}_{\underline{h}^{1+t}} = \sum_{\substack{t\in(\mathbb{Z}/p^m\mathbb{Z})^\times \\ p\nmid t+1}} \mathfrak{a}_{\underline{h}^{1+t}} + \sum_{\substack{t\in(\mathbb{Z}/p^m\mathbb{Z})^\times \\ p\mid t+1}} \mathfrak{a}_{\underline{h}^{1+t}} \\ &= \sum_{\substack{t\in(\mathbb{Z}/p^m\mathbb{Z})^\times \\ p\nmid t+1}} \mathfrak{a}_{\underline{h}} + \sum_{s=1}^{p^{m-1}} \mathfrak{a}_{\underline{h}^{ps}} = (p^m - 2p^{m-1}) \times \mathfrak{a}_{\underline{h}} + \sum_{s=1}^{p^{m-1}} \mathfrak{a}_{(\underline{h}^p)^s}\end{aligned}$$

which is congruent to $\sum_{s=1}^{p^{m-1}} \mathfrak{a}_{(\underline{h}^p)^s}$ modulo $p^{m-1}\mathrm{Im}(\theta_m^+)$. It follows directly that

$$\left(\mathfrak{a}_{\underline{h}}\right)^3 = \mathfrak{a}_{\underline{h}} \times \left(\mathfrak{a}_{\underline{h}}\right)^2 \equiv \sum_{s=1}^{p^{m-1}} \mathfrak{a}_{\underline{h}} \times \mathfrak{a}_{(\underline{h}^p)^s} \equiv \sum_{s=1}^{p^{m-1}} 0 \mod p\ \mathrm{Im}(\theta_m^+)$$

because Fact 1 implies $\mathfrak{a}_{\underline{h}} \times \mathfrak{a}_{(\underline{h}^p)^s} \equiv 0 \mod p\ \mathrm{Im}(\theta_m^+)$ as the order$\left((\underline{h}^p)^s\right) < m$. □

Proof of Fact 3: An arbitrary element $y \in \mathrm{Im}(\theta_m^+)$ is of the form $y = \sum_{\langle \underline{h} \rangle < H_m^{(d)}} \kappa_{\langle \underline{h} \rangle} \times \mathfrak{a}_{\underline{h}}$ where each $\kappa_{\langle \underline{h} \rangle} \in \mathbb{Z}_p[\Sigma']$. Using Fermat's little theorem, we have

$$y^p \equiv \sum_{\langle \underline{h} \rangle < H_m^{(d)}} \kappa_{\langle \underline{h} \rangle}^p \times \left(\mathfrak{a}_{\underline{h}}\right)^p \overset{\text{by Fact 2}}{\equiv} \sum_{\langle \underline{h} \rangle < H_m^{(d)}} \kappa_{\langle \underline{h} \rangle}^p \times \left(\mathfrak{a}_{\underline{h}}\right)^{p-3} \times 0 \mod p\ \mathrm{Im}(\theta_m^+)$$

which implies that $y^p \in p\ \mathrm{Im}(\theta_m^+)$. Applying simple induction we obtain $y^i \in p^{\lfloor i/p \rfloor}\mathrm{Im}(\theta_m^+)$ while $1/i \in p^{-\mathrm{ord}_p(i)}\mathbb{Z}_p \subset p^{-\log(i)/\log(p)}\mathbb{Z}_p$, and the estimate follows immediately. □

Proof of Fact 4: We essentially need to bound the length of the longest product $\mathfrak{a}_{\underline{\mathfrak{h}}_1} \times \mathfrak{a}_{\underline{\mathfrak{h}}_2} \times \cdots \times \mathfrak{a}_{\underline{\mathfrak{h}}_{N+1}} \notin p\ \mathrm{Im}(\theta_m^+)$. Exploiting Fact 1 above, we know that if any of the $\underline{\mathfrak{h}}_j$'s has order $< p^m$ then the product must automatically lie in $p\ \mathrm{Im}(\theta_m^+)$. Without loss of generality assume $\mathrm{order}\left(\underline{\mathfrak{h}}_j\right) = p^m$ for all j, in which case

$$\mathfrak{a}_{\underline{\mathfrak{h}}_1} \times \mathfrak{a}_{\underline{\mathfrak{h}}_2} \times \cdots \times \mathfrak{a}_{\underline{\mathfrak{h}}_{N+1}} = \sum_{\underline{\mathfrak{h}} \in \mathcal{T}_N} \mathfrak{a}_{\underline{\mathfrak{h}}} \quad \text{where} \quad \mathcal{T}_N = \left\langle \underline{\mathfrak{h}}_1 \right\rangle_{\mathrm{gen}} \left\langle \underline{\mathfrak{h}}_2 \right\rangle_{\mathrm{gen}} \cdots \left\langle \underline{\mathfrak{h}}_{N+1} \right\rangle_{\mathrm{gen}}.$$

There are precisely $\frac{p^{md} - p^{(m-1)d}}{p^m - p^{m-1}}$ cyclic subgroups of $H_m^{(d)}$ of size p^m; consequently if $N+1 > \frac{p^{md} - p^{(m-1)d}}{p^m - p^{m-1}}$ then at least one of the above $\left\langle \underline{\mathfrak{h}}_j \right\rangle_{\mathrm{gen}}$'s occurs twice or more, in which case $\mathfrak{a}_{\underline{\mathfrak{h}}_1} \times \mathfrak{a}_{\underline{\mathfrak{h}}_2} \times \cdots \times \mathfrak{a}_{\underline{\mathfrak{h}}_{N+1}} \in p\ \mathrm{Im}(\theta_m^+)$.

We conclude that the longest product of $\mathfrak{a}_{\underline{\mathfrak{h}}_j}$'s inside $\mathrm{Im}(\theta_m^+)$ not divisible by p must have length $\leq \frac{p^{md} - p^{(m-1)d}}{p^m - p^{m-1}}$. Because the image of θ_m^+ is generated over $\mathbb{Z}_p[\Sigma']$ by the set $\mathcal{S}_m^{(\mathcal{A})}$, our final Fact 4 has been established. □

We now return to the proof of Lemma 5.1.2(b). If $y \in \mathrm{Im}(\theta_m^+)$, then $(1+y)^{-1} = \sum_{i \geq 0}(-1)^i y^i$ converges with respect to the p-adic topology from Fact 3, since $y^i \in p^{\left\lfloor \frac{i}{p} \right\rfloor}\mathrm{Im}(\theta_m^+)$ and $p^{\left\lfloor \frac{i}{p} \right\rfloor}$ tends to zero as i tends to infinity. Therefore, inverse elements in $1 + \mathrm{Im}(\theta_m^+)$ exist. As a result, the elements in $1 + \mathrm{Im}(\theta_m^+)$ form a multiplicative group. In fact, the convergence of the formal power series $\sum_{i=1}^{\infty} \frac{(-1)^{i+1} y^i}{i}$ yields a homomorphism $\log : 1 + \mathrm{Im}(\theta_m^+)^n \to \mathrm{Im}(\theta_m^+)^n$, and we shall write

$$\overline{\log} : 1 + \mathrm{Im}(\theta_m^+)^n \longrightarrow \frac{\mathrm{Im}(\theta_m^+)^n}{\mathrm{Im}(\theta_m^+)^{n+1}}$$

for its composition with the quotient modulo $\mathrm{Im}(\theta_m^+)^{n+1}$.

Clearly $1 + \mathrm{Im}(\theta_m^+)^{n+1} \subset \mathrm{Ker}(\overline{\log})$, but the reverse inclusion is trickier to obtain. **We claim that if** $m, n \geq 2$ **and** $p \geq 3$**, then**

$$\log(1+y) \equiv y \mod \mathrm{Im}(\theta_m^+)^{n+1} \quad \textbf{for all } y \in \mathrm{Im}(\theta_m^+)^n\textbf{.}$$

Deferring the claim's proof momentarily, we deduce that the map $\overline{\log}$ is surjective; moreover if $y \in \mathrm{Im}(\theta_m^+)^n$ and $\log(1+y) \in \mathrm{Im}(\theta_m^+)^{n+1}$ then one has $y \in \mathrm{Im}(\theta_m^+)^{n+1}$. The latter is equivalent to the statement "$\log(1+y) \equiv 0 \implies y \in \mathrm{Im}(\theta_m^+)^{n+1}$", hence one obtains the inclusion $\mathrm{Ker}(\overline{\log}) \subset 1 + \mathrm{Im}(\theta_m^+)^{n+1}$.

It remains to justify the above claim. Recall that $\log(1+y) = y + \sum_{i=2}^{\infty} \frac{(-1)^{i+1} y^i}{i}$, and we express $y \in \mathrm{Im}(\theta_m^+)^n$ as the product $y = a_1 \times a_2 \times \cdots \times a_n$ with $a_j \in \mathrm{Im}(\theta_m^+)$. If $i \geq 2$ and $p \nmid i$, then

$$\frac{(-1)^{i+1} y^i}{i} = \frac{(-1)^{i+1}}{i} \times a_1^i a_2^i \ldots a_n^i \in \mathrm{Im}(\theta_m^+)^{ni} \subset \mathrm{Im}(\theta_m^+)^{n+1}.$$

Alternatively if $i = p$ then $\frac{a_1^p}{p} \in \mathrm{Im}(\theta_m^+)$ by Fact 3, whence

$$\frac{(-1)^{p+1} y^p}{p} = (-1)^{p+1} \times \left(\frac{a_1^p}{p} \right) \times a_2^p \ldots a_n^p \in \mathrm{Im}(\theta_m^+)^{1+p(n-1)};$$

however $1 + p(n-1) > n+1$ if $n \geq 2$ and $p \geq 3$, which means $\frac{(-1)^{p+1} y^p}{p} \in \mathrm{Im}(\theta_m^+)^{n+1}$. Thirdly if $k \geq 2$ and $i = p^k$, then

$$\frac{(-1)^{p^k+1} y^{p^k}}{p^k} = y^{p^k - pk} \times \left(\frac{y^p}{p} \right)^k \in \mathrm{Im}(\theta_m^+)^{n(p^k-pk)+(n+1)k} \subset \mathrm{Im}(\theta_m^+)^{n+1}.$$

Finally, for a general index of the form $i = p^k \times c$ with $p \nmid c$, we have

$$\frac{(-1)^{i+1} y^i}{i} = \frac{(-1)^{i+1}}{c} \times \frac{(y^c)^{p^k}}{p^k} \in \mathrm{Im}(\theta_m^+)^{n+1}$$

by the previous argument (with y replaced by y^c). We may therefore conclude that $\sum_{i=2}^{\infty} \frac{(-1)^{i+1} y^i}{i} \in \mathrm{Im}(\theta_m^+)^{n+1}$ whenever $y \in \mathrm{Im}(\theta_m^+)^n$, and our claim follows.

As a result, $\mathrm{Ker}(\overline{\log}) = 1 + \mathrm{Im}(\theta_m^+)^{n+1}$, which implies

$$\frac{1+\mathrm{Im}(\theta_m^+)^n}{\mathrm{Ker}(\overline{\log})} \cong \mathrm{Im}(\overline{\log}), \quad \text{i.e.} \quad \frac{1+\mathrm{Im}(\theta_m^+)^n}{1+\mathrm{Im}(\theta_m^+)^{n+1}} \cong \frac{\mathrm{Im}(\theta_m^+)^n}{\mathrm{Im}(\theta_m^+)^{n+1}}$$

by the surjectivity of $\overline{\log}$. □

Lemma 5.1.3. *If $m \geq 2$ and $x \in K_1\big(\mathbb{Z}_p[G_n^{(d)}]\big)$, then*

$$\tilde{\varphi}_{\mathfrak{S}_{m-1}^{\mathrm{ab}}} \circ \log_{\mathfrak{S}_{m-1}^{\mathrm{ab}}}\big(\theta_{m-1}(x)\big) = \varphi_{\frac{1+p^{m-1}\mathbb{Z}}{1+p^n\mathbb{Z}} \ltimes H_m^{(d)}} \circ \log\Big(\mathrm{Nr}_{G_n^{(d)}/\mathfrak{S}_{m-1}}(x) \bmod (H_n^{(d)})^{p^m}\Big).$$

Proof. Let us define $\mathcal{G}_{n,m} := \frac{1+p^{m-1}\mathbb{Z}}{1+p^n\mathbb{Z}} \ltimes H_m^{(d)}$, so that $\mathcal{G}_{n,m}^p = \frac{1+p^m\mathbb{Z}}{1+p^n\mathbb{Z}} \times \big(H_m^{(d)}\big)^p$ is isomorphic to a subgroup $\mathcal{J}$ of index p^d in $\mathfrak{S}_m^{\mathrm{ab}}$; we write $\varpi : \mathcal{G}_{n,m}^p \xrightarrow{\sim} \mathcal{J} \hookrightarrow \mathfrak{S}_m^{\mathrm{ab}}$ for the corresponding injection. In particular, there is a commutative diagram

$$\begin{array}{ccccccc}
\mathbb{Z}_p\big[\mathcal{G}_{n,m}\big]^\times & \twoheadrightarrow & K_1\big(\mathbb{Z}_p[\mathcal{G}_{n,m}]\big) & \xrightarrow{\varphi_{\mathcal{G}_{n,m}}} & K_1\big(\mathbb{Z}_p[\mathcal{G}_{n,m}^p]\big) & \cong & \mathbb{Z}_p\big[\mathcal{G}_{n,m}^p\big]^\times \\
\downarrow & & \downarrow \bmod (H_m^{(d)})^{p^{m-1}} & & & & \downarrow \varpi_* \\
\mathbb{Z}_p\big[\mathfrak{S}_{m-1}^{\mathrm{ab}}\big]^\times & \xrightarrow{\sim} & K_1\big(\mathbb{Z}_p[\mathfrak{S}_{m-1}^{\mathrm{ab}}]\big) & \xrightarrow{\tilde{\varphi}_{\mathfrak{S}_{m-1}^{\mathrm{ab}}}} & K_1\big(\mathbb{Z}_p[\mathfrak{S}_m^{\mathrm{ab}}]\big) & \cong & \mathbb{Z}_p\big[\mathfrak{S}_m^{\mathrm{ab}}\big]^\times.
\end{array}$$

If $z := \mathrm{Nr}_{G_n^{(d)}/\mathfrak{S}_{m-1}}(x) \bmod (H_n^{(d)})^{p^m} \in K_1\big(\mathbb{Z}_p[\mathcal{G}_{n,m}]\big)$ then the element $\theta_{m-1}(x)$ coincides with z modulo $(H_m^{(d)})^{p^{m-1}}$, in which case

$$\tilde{\varphi}_{\mathfrak{S}_{m-1}^{\mathrm{ab}}}\big(\theta_{m-1}(x)\big) \;=\; \tilde{\varphi}_{\mathfrak{S}_{m-1}^{\mathrm{ab}}}\big(z \bmod (H_m^{(d)})^{p^{m-1}}\big) \;=\; \varpi_* \circ \varphi_{\mathcal{G}_{n,m}}(z).$$

Taking the logarithm of both sides, and observing that the power series defining 'log' commutes with the action of both Frobenii $\tilde{\varphi}_{\mathfrak{S}_{m-1}^{\mathrm{ab}}}$ and $\varphi_{\mathcal{G}_{n,m}}$, we have the required result. □

5.2 A Proof of Theorem 5.0.21

Let us start by establishing commutativity of the maps in the fundamental square. This amounts to checking for all $x \in K_1\big(\mathbb{Z}_p[G_n^{(d)}]\big)$, that the required formula

$$\theta_m^+\Big(\Gamma_{G_n^{(d)}}\big(x^\dagger\big)\Big) \;=\; \log_{\mathbb{Z}_p[\mathfrak{S}_m^{\mathrm{ab}}]}\left(\frac{\frac{\theta_m(x)}{\tau_* N_{0,m}(\theta_0(x))}}{\tilde{\varphi}_{\mathfrak{S}_{m-1}^{\mathrm{ab}}}\big(\frac{\theta_{m-1}(x)}{\tau_* N_{0,m-1}(\theta_0(x))}\big)}\right)$$

holds true. We subdivide its verification into the three cases listed below.

Case (I): $m = 0$. Noting that $\theta_0^+ \circ \varphi_{G_n^{(d)}} = \varphi_{\Sigma_n} \circ \theta_0^+$ and $\theta_0(x^\dagger) = 1$, one calculates

$$\begin{aligned}\theta_0^+ \circ \Gamma_{G_n^{(d)}}(x^\dagger) &= \theta_0^+ \circ \log(x^\dagger) - \frac{1}{p} \times \theta_0^+\Big(\varphi_{G_n^{(d)}} \circ \log(x^\dagger)\Big) \\ &= \log \circ\, \theta_0(x^\dagger) - \frac{1}{p} \times \varphi_{\Sigma_n}\Big(\theta_0^+ \circ \log(x^\dagger)\Big) \\ &= \log \circ\, \theta_0(x^\dagger) - \frac{1}{p} \times \varphi_{\Sigma_n}\Big(\log \circ\, \theta_0(x^\dagger)\Big) \;=\; 0 - 0 \;=\; \log(1).\end{aligned}$$

Case (II): $m = 1$. By a similar argument,

$$\begin{aligned}\theta_1^+ \circ \Gamma_{G_n^{(d)}}(x^\dagger) &= \theta_1^+ \circ \log(x^\dagger) - \frac{1}{p} \times \theta_1^+\Big(\varphi_{G_n^{(d)}} \circ \log(x^\dagger)\Big) \\ &= \log \circ\, \theta_1(x^\dagger) - \frac{1}{p} \times \mathrm{Tr}_{\Sigma_n / \frac{1+p\mathbb{Z}}{1+p^n\mathbb{Z}}} \circ \varphi_{\Sigma_n}\Big(\theta_0^+ \circ \log(x^\dagger)\Big) \\ &= \log\left(\frac{\theta_1(x)}{\theta_1(x^{\mathrm{cy}})}\right) - \frac{1}{p} \times \mathrm{Tr}_{\Sigma_n / \frac{1+p\mathbb{Z}}{1+p^n\mathbb{Z}}} \circ \varphi_{\Sigma_n}\Big(\log\big(\theta_0(x^\dagger)\big)\Big)\end{aligned}$$

where the second line follows from Lemma 5.1.1(ii), and the third because $\mathrm{Tr} \circ \log = \log \circ \mathrm{Norm}$, which implies $\theta_0^+ \circ \log = \log \circ \theta_0$. Again $\theta_0(x^\dagger) = 1$ so the last summand is zero, whilst $\theta_1(x^{\mathrm{cy}}) = \tau_*^{(1)} \circ N_{0,1}\big(\theta_0(x)\big)$ by Remark 5.0.19(iv); hence we may conclude

$$\theta_1^+ \circ \Gamma_{G_n^{(d)}}(x^\dagger) = \log\big(\theta_1(x)\big) - \log\Big(\tau_* N_{0,1}\big(\theta_0(x)\big)\Big) - \frac{1}{p} \times 0 = \log\left(\frac{\theta_1(x)}{\tau_* N_{0,1}\big(\theta_0(x)\big)}\right).$$

Case (III): $m \geq 2$. This computation relies heavily on our technical lemmas. Firstly, one has the equalities

$$\begin{aligned}\theta_m^+ \circ \Gamma_{G_n^{(d)}}(x^\dagger) &= \theta_m^+ \circ \log(x^\dagger) - \frac{1}{p} \times \theta_m^+\Big(\varphi_{G_n^{(d)}} \circ \log(x^\dagger)\Big) \\ = \log \circ\, \theta_m(x^\dagger) &- \frac{1}{p} \times p \times \varphi_{\frac{1+p^{m-1}\mathbb{Z}}{1+p^n\mathbb{Z}} \ltimes H_m^{(d)}}\Big(\mathrm{Tr}_{G_n^{(d)} / \mathfrak{S}_{m-1}} \circ \log(x^\dagger) \mod \big(H_n^{(d)}\big)^{p^m}\Big)\end{aligned}$$

upon applying Lemma 5.1.1(i).

From Remark 5.0.19(iv), $\theta_m(x^{\mathrm{cy}}) = \tau_*^{(m)} N_{0,m}\big(\theta_0(x)\big)$, therefore one deduces

$\theta_m\big(x^\dagger\big) = \frac{\theta_m(x)}{\tau_* N_{0,m}\big(\theta_0(x)\big)}$; furthermore $\mathrm{Tr}_{G_n^{(d)}/\mathfrak{S}_{m-1}} \circ \log = \log \circ \mathrm{Nr}_{G_n^{(d)}/\mathfrak{S}_{m-1}}$, thence

$$\begin{aligned}\theta_m^+ \circ \Gamma_{G_n^{(d)}}\big(x^\dagger\big) &= \log\big(\theta_m(x)\big) - \log\big(\tau_* N_{0,m}\big(\theta_0(x)\big)\big) \\ &\quad - \varphi_{\frac{1+p^{m-1}\mathbb{Z}}{1+p^n\mathbb{Z}} \ltimes H_m^{(d)}}\Big(\log \circ \mathrm{Nr}_{G_n^{(d)}/\mathfrak{S}_{m-1}}\big(x^\dagger\big) \mod \big(H_n^{(d)}\big)^{p^m}\Big) \\ &\overset{\text{by } 5.1.3}{=} \log\big(\theta_m(x)\big) - \log\big(\tau_* N_{0,m}\big(\theta_0(x)\big)\big) - \tilde{\varphi}_{\mathfrak{S}_{m-1}^{\mathrm{ab}}} \circ \log_{\mathfrak{S}_{m-1}^{\mathrm{ab}}}\big(\theta_{m-1}(x^\dagger)\big).\end{aligned}$$

Exploiting the relation $\theta_{m-1}\big(x^\dagger\big) = \frac{\theta_{m-1}(x)}{\tau_* N_{0,m-1}\big(\theta_0(x)\big)}$ once more, and the commutativity of the the power series defining 'log' with the Frobenius $\tilde{\varphi}_{\mathfrak{S}_{m-1}^{\mathrm{ab}}}$, we obtain

$$\theta_m^+ \circ \Gamma_{G_n^{(d)}}\big(x^\dagger\big) = \log\left(\frac{\theta_m(x)}{\tau_* N_{0,m}\big(\theta_0(x)\big)}\right) - \log\left(\frac{\tilde{\varphi}_{\mathfrak{S}_{m-1}^{\mathrm{ab}}} \circ \theta_{m-1}(x)}{\tilde{\varphi}_{\mathfrak{S}_{m-1}^{\mathrm{ab}}} \circ \tau_* N_{0,m-1}\big(\theta_0(x)\big)}\right)$$

which is equivalent to the required formula.

Conclusion: Combining (I)-(III) establishes that $\Theta^+ \circ \Gamma_{G_n^{(d)}}\big(x^\dagger\big) = \underline{\log}_n^\dagger \circ \underline{\mathrm{tw}}_n \circ \Theta(x)$.

It remains to compute both the kernel and image of Θ. Recall that

$$K_1\big(\mathbb{Z}_p[G_n^{(d)}]\big) = \iota_* K_1\big(\mathbb{Z}_p[\Sigma_n]\big) \times \mathcal{W}^\dagger$$

where ι_* was the section reversing the projection θ_0, and $\mathcal{W}^\dagger$ is the complement.

Since the morphism Θ maps $\iota_* K_1\big(\mathbb{Z}_p[\Sigma_n]\big)$ isomorphically onto the group $\Omega_{n,\mathrm{cy}}^{(d)}$, the kernel of Θ will coincide with

$$\mathrm{Ker}\Big(\Theta\big|_{\mathcal{W}^\dagger}\Big) \overset{\text{by } 5.1.2}{=} \mathrm{Ker}\Big(\underline{\log}_n^\dagger \circ \underline{\mathrm{tw}}_n \circ \Theta\big|_{\mathcal{W}^\dagger}\Big) = \mathrm{Ker}\Big(\Theta^+ \circ \Gamma_{G_n^{(d)}}\big|_{\mathcal{W}^\dagger}\Big)$$

which is precisely the kernel of $\Gamma_{G_n^{(d)}}$ because Θ^+ is injective. However the kernel of the Taylor-Oliver logarithm is well known to equal $SK_1\big(\mathbb{Z}_p[G_n^{(d)}]\big)$, so the same must be true for $\mathrm{Ker}(\Theta)$.

Finally as $\Theta\big(\iota_* K_1\big(\mathbb{Z}_p[\Sigma_n]\big) = \Omega_{n,\mathrm{cy}}^{(d)}$, we must therefore show $\Theta\big(\mathcal{W}^\dagger\big) = \Omega_{n,\dagger}^{(d)}$. Clearly $\Theta\big(\mathcal{W}^\dagger\big) \subset \{1\} \times \prod_{m=1}^n 1 + p\mathbb{Z}_p\big[\mathfrak{S}_m^{\mathrm{ab}}\big]$, and moreover $\Theta^+ \circ \Gamma_{G_n^{(d)}}\big(\mathcal{W}^\dagger\big) \subset$

$\Psi_n^{(d)}$. By Lemma 5.1.2(a) and the commutativity of our fundamental square,

$$\underline{\log}_n^{\dagger} \circ \underline{\mathrm{tw}}_n \circ \Theta\big(\mathcal{W}^{\dagger}\big) \subset \Psi_n^{(d)} \cap \left(\{0\} \times \prod_{m=1}^{n} p\mathbb{Z}_p\big[\mathfrak{S}_m^{\mathrm{ab}}\big] \right).$$

Conversely every element $\underline{z} \in \Omega_{n,\dagger}^{(d)}$ can be written as $\underline{z} = \Theta(w)$ for some $w \in \mathcal{W}^{\dagger}$, and the proof of Theorem 5.0.21 is now complete.

6

Evaluation at Multiplicative Characters χ

The main algebraic result of this thesis, namely Theorem 1.0.2, will now be proved. As we have seen in the previous chapter, a vector $\underline{z} \in \prod_{m=0}^{n} \mathbb{Z}_p[\mathfrak{S}_m^{\mathrm{ab}}]^{\times}$ arises from an element of $K_1\big(\mathbb{Z}_p[G_n^{(d)}]\big)$ via Θ, if and only if $\underline{\log}_n^{\dagger} \circ \underline{\mathrm{tw}}_n(\underline{z})$ belongs to $\mathrm{Im}(\Theta^+)$. For each $m \in \{0, \ldots, n\}$ let us abbreviate the group $\frac{1+p^m\mathbb{Z}}{1+p^n\mathbb{Z}}$ by using $\Sigma'_{(m)}$, so that $\mathfrak{S}_m \cong \Sigma'_{(m)} \ltimes H_n^{(d)}$ and $\mathfrak{S}_m^{\mathrm{ab}} \cong \Sigma'_{(m)} \times H_m^{(d)}$.

Applying Theorem 4.0.13, we have that the image of Θ^+ consists of the trace-compatible terms

$$\Psi_n^{(d)} \;=\; \left\{ \big\{y_m\big\}_{0\leq m\leq n} \text{ such that } \mathrm{Tr}_{\Sigma'_{(m-1)}/\Sigma'_{(m)}}\big(y_{m-1}\big) \equiv y_m \mod \big(H_m^{(d)}\big)^{p^{m-1}} \right\}.$$

We will now seek an alternative description for $\Psi_n^{(d)}$ entirely through the use of p-power congruences, in the same manner as the $d = 1$ situation studied in [24] (Section 3).

Notations: (a) For each character $\chi : H_m^{(d)} \twoheadrightarrow \mu_{p^v}$ we write $\mathcal{J}_\chi$ for the kernel of χ, thus $H_m^{(d)}/\mathcal{J}_\chi$ is a cyclic group of order p^v.
(b) At every index $v \in \{0, \ldots, m\}$, we introduce a family of subgroups

$$\mathcal{Z}_m^{(v)} \;:=\; \Big\{\text{subgroups } \mathcal{J} \subset H_m^{(d)} \text{ such that } H_m^{(d)}/\mathcal{J} \text{ is cyclic of order } p^v\Big\}$$

and denote their disjoint union by $\mathcal{Z}_m = \bigcup_{v=0}^{m} \mathcal{Z}_m^{(v)}$.
(c) Lastly let us write '$\mathrm{char}_{\mathcal{J}}$' for the characteristic function of $\mathcal{J}$ inside of $H_m^{(d)}$.

Let t be co-prime to p. The raising of every element of the set μ_{p^v} to the power t permutes the set μ_{p^v}. Thus if $\chi(\underline{\mathfrak{h}}) \in \mu_{p^v}$, then $\chi(\underline{\mathfrak{h}})^t \in \mu_{p^v}$. Conversely if $\underline{\mathfrak{h}} \in \mathcal{J}_{\chi^t}$, then $\underline{\mathfrak{h}} \in \mathcal{J}_\chi$; likewise if $\underline{\mathfrak{h}} \in \mathcal{J}_\chi$, then $\underline{\mathfrak{h}} \in \mathcal{J}_{\chi^t}$. We therefore conclude $\mathcal{J}_{\chi^t} = \mathcal{J}_\chi$

for all t co-prime to p.

Notice that $\nu_m(\underline{\mathfrak{h}}) = \nu_m(\underline{\mathfrak{h}}^t)$ for t co-prime to p, thus $\underline{\mathfrak{h}}$ and $\underline{\mathfrak{h}}^t$ belong to the same cyclic subgroup $\langle \underline{\mathfrak{h}} \rangle < H_m^{(d)}$. As a result $\mathrm{char}_{\mathcal{J}}(\underline{\mathfrak{h}}^t) = \mathrm{char}_{\mathcal{J}}(\underline{\mathfrak{h}})$, and the value of $\mathrm{char}_{\mathcal{J}}(\underline{\mathfrak{h}})$ depends only on the cyclic subgroup $\langle \underline{\mathfrak{h}} \rangle < H_m^{(d)}$.

Throughout one fixes a finite integral extension $\mathcal{O}$ of $\mathbb{Z}_p$ which contains the values of all multiplicative characters $\chi : H_m^{(d)} \to \mu_{p^\infty} \hookrightarrow \mathbb{C}_p^\times$ (e.g. the ring $\mathbb{Z}_p[\mu_{p^n}]$ suffices). For each character χ on $H_v^{(d)}$ with $0 \leq v \leq m \leq n$, if $y_m \in \mathbb{Z}_p\big[\Sigma'_{(m)} \times H_m^{(d)}\big]$ then one naturally obtains $\chi(y_m) \in \mathcal{O}\big[\Sigma'_{(m)}\big]$ by linearly extending χ to the group ring.

Question *Given a collection of $a_{m,\chi} \in \mathcal{O}[\Sigma'_{(m)}]$ with $m \leq n$ and $\chi : H_m^{(d)} \to \mathcal{O}^\times$, can one find necessary and sufficient conditions to determine whether $a_{m,\chi} = \chi(y_m)$ at every pair (m, χ) above, for a suitable sequence $\{y_m\}_m \in \Psi_n^{(d)}$?*

Let us work backwards – for the sake of argument, suppose that $\{y_m\}_{0 \leq m \leq n} \in \Psi_n^{(d)}$ gives rise to these terms $a_{m,\chi}$ through evaluation at χ. By Theorem 4.0.13 there exists $z \in \mathbb{Z}_p\big[\mathrm{Conj}(G_n^{(d)})\big]$ such that $y_m = \theta_m^+(z)$, in which case $a_{m,\chi} = \chi(y_m) = \theta_{\chi_m}^+(z)$.

Moreover upon examining Proposition 3.1.9(ii), we further deduce

- each element $\theta_{\chi_m}^+(z)$ belongs to $p^{m-1}\mathbb{Z}_p\big[\Sigma'_{(m)}\big]$, so clearly has $\mathbb{Z}_p$-coefficients;
- the term $\theta_{\chi_m}^+(z)$ depends only on $\mathcal{J}_\chi = \mathrm{Ker}(\chi)$, not the individual character;
- if χ factors through the quotient $H_{m-1}^{(d)}$, then $a_{m,\chi} = \mathrm{Tr}_{\Sigma'_{(m-1)}/\Sigma'_{(m)}}\big(a_{m-1,\chi}\big)$.

In fact, the last statement is a consequence of the trace-compatibility for the y_m's. Consequently, we can refine our problem by restricting solely to elements

$$a_{\mathcal{J}_\chi}^{(v)} \;=\; a_{v,\chi} \in \mathbb{Z}_p\big[\Sigma'_{(v)}\big] \quad \text{where } \mathcal{J}_\chi \in \mathcal{Z}_m^{(v)} \text{ and } 0 \leq v \leq m \leq n.$$

The following result provides a purely p-adic answer to the question posed above.

Theorem 6.0.1. *A sequence* $\left(\ldots, a^{(v)}_{\mathcal{J}_\chi}, \ldots\right) \in \prod_{\chi: H_m^{(d)} \twoheadrightarrow \mu_{p^v}} \mathbb{Z}_p\left[\Sigma'_{(v)}\right]$ *arises from a trace-compatible system lying in* $\Psi_n^{(d)}$*, if and only if for all positive integers* $m \leq n$ *and all non-trivial subgroups* $\langle \underline{\mathfrak{h}} \rangle \subset H_m^{(d)}$

$$\mathrm{Tr}_{\Sigma'_{(0)}/\Sigma'_{(m)}}\left(a^{(0)}_{H_m^{(d)}}\right) + \sum_{v=1}^{m} \sum_{\mathcal{J}_\chi \in \mathcal{Z}_m^{(v)}} p^{v-1} \mathrm{Tr}_{\Sigma'_{(v)}/\Sigma'_{(m)}}\left(a^{(v)}_{\mathcal{J}_\chi}\right) \times \\ \times \left(p \ \mathrm{char}_{\mathcal{J}_\chi}(\underline{\mathfrak{h}}) - \mathrm{char}_{\mathcal{J}_\chi}(\underline{\mathfrak{h}}^p)\right) \equiv 0 \mod p^{m(d+1)-\nu_m(\underline{\mathfrak{h}})}, \qquad (6.1\mathrm{m},\underline{\mathfrak{h}})$$

whilst at the trivial subgroup

$$p\mathrm{Tr}_{\Sigma'_{(0)}/\Sigma'_{(m)}}\left(a^{(0)}_{H_m^{(d)}}\right) + \sum_{v=1}^{m} \sum_{\mathcal{J}_\chi \in \mathcal{Z}_m^{(v)}} p^v(p-1) \times \\ \mathrm{Tr}_{\Sigma'_{(v)}/\Sigma'_{(m)}}\left(a^{(v)}_{\mathcal{J}_\chi}\right) \equiv 0 \mod p^{m(d+1)}. \quad (6.2\mathrm{m},\mathrm{id})$$

In Section 6.2 we explain why the above result implies Theorem 1.0.2 in the Introduction. However we first use properties of characteristic functions to give its demonstration.

6.1 The Proof of Theorem 6.0.1

The initial step is to construct an inverse to the mapping $y_m \mapsto (\ldots, \chi(y_m), \ldots)$. Assume we are given a collection of elements $a_{m,\chi} \in \mathbb{Z}_p\left[\Sigma'_{(m)}\right]$; then one defines

$$Y_m := \sum_{\underline{\mathfrak{h}} \in H_m^{(d)}} c^{(m)}_{\underline{\mathfrak{h}}} \left[\underline{\mathfrak{h}}\right]_{H_m^{(d)}} \quad \text{where} \quad c^{(m)}_{\underline{\mathfrak{h}}} = p^{-md} \sum_{\chi: H_m^{(d)} \to \mathbb{C}_p^\times} \chi^{-1}(\underline{\mathfrak{h}}) a_{m,\chi} \in \overline{\mathbb{Q}}_p\left[\Sigma'_{(m)}\right].$$

As $\mathrm{char}_{\underline{\mathfrak{h}}}(x) = p^{-md} \sum_\chi \chi^{-1}(\underline{\mathfrak{h}}) \cdot x$, it follows that $\chi(Y_m) = a_{m,\chi}$ for all such χ. Furthermore, if at each character χ we know $a_{m,\chi} = \chi(y_m)$ for a fixed $y_m \in \mathbb{Q}_p[\mathfrak{S}_m^{\mathrm{ab}}]$, then clearly Y_m and y_m must coincide.

Lemma 6.1.1. *Providing each* $a_{m,\chi}$ *depends only on* $\mathrm{Ker}(\chi) \subset H_m^{(d)}$*, then*

$$c^{(m)}_{\underline{\mathfrak{h}}} \ = \ p^{-md}\, a_{m,\mathbf{1}} \ + \sum_{\mathcal{J}_\chi \in \mathcal{Z}_m - \{H_m^{(d)}\}} \frac{1}{\#\mathcal{J}_\chi} \times \left(\mathrm{char}_{\mathcal{J}_\chi}(\underline{\mathfrak{h}}) - \frac{1}{p}\, \mathrm{char}_{\mathcal{J}_\chi}(\underline{\mathfrak{h}}^p)\right) a_{m,\chi}$$

and one may express Y_m *as the summation* $\sum_{\langle \underline{\mathfrak{h}} \rangle < H_m^{(d)}} c^{(m)}_{\underline{\mathfrak{h}}} \times \mathcal{A}_{H_m^{(d)}}\langle \underline{\mathfrak{h}} \rangle$.

Proof. Let us denote by $\mathfrak{X}_m$ the group of characters $\chi : H_m^{(d)} \longrightarrow \mathbb{C}_p^\times$. Notice that for $x \in \mathbb{Z}_p[\mathrm{Conj}(G_n^{(d)})]$, by Proposition 3.1.9(ii) the element $\theta_{\chi_m}^+(x)$ depends only on $\mathrm{Ker}(\chi)$, and not the particular choice of χ. As a result,

$$\begin{aligned} c_{\underline{\mathfrak{h}}}^{(m)} &= p^{-md} \sum_{\chi \in \mathfrak{X}_m} \chi^{-1}(\underline{\mathfrak{h}}) a_{m,\chi} = p^{-md} \sum_{\mathcal{J} \in \mathcal{Z}_m} a_{\mathcal{J}} \sum_{\substack{\chi \in \mathfrak{X}_m, \\ \mathrm{Ker}(\chi) = \mathcal{J}}} \chi^{-1}(\underline{\mathfrak{h}}) \\ &= p^{-md} \left(a_{m,\mathbf{1}} + \sum_{\mathcal{J} \in \mathcal{Z}_m - \{H_m^{(d)}\}} a_{\mathcal{J}} \left(\sum_{\mathrm{Ker}(\chi) \supset \mathcal{J}} \chi^{-1}(\underline{\mathfrak{h}}) - \sum_{\substack{\mathrm{Ker}(\chi) \supset \mathcal{J}, \\ \mathrm{Ker}(\chi) \neq \mathcal{J}}} \chi^{-1}(\underline{\mathfrak{h}}) \right) \right) \end{aligned}$$

where $a_{\mathcal{J}} = a_{m,\chi}$. However

$$\sum_{\mathrm{Ker}(\chi) \supset \mathcal{J}} \chi^{-1}(\underline{\mathfrak{h}}) = \sum_{\chi : H_m^{(d)}/\mathcal{J} \to \mathbb{C}_p^\times} \chi^{-1}(\underline{\mathfrak{h}}) = \frac{\#H_m^{(d)}}{\#\mathcal{J}} \times \mathrm{char}(\underline{\mathfrak{h}}),$$

and moreover

$$\begin{aligned} \sum_{\substack{\mathrm{Ker}(\chi) \supset \mathcal{J}, \\ \mathrm{Ker}(\chi) \neq \mathcal{J}}} \chi^{-1}(\underline{\mathfrak{h}}) &= \sum_{\substack{\chi : H_m^{(d)}/\mathcal{J} \to \mathbb{C}_p^\times, \\ \mathrm{order}(\chi) \neq [H_m^{(d)} : \mathcal{J}]}} \chi^{-1}(\underline{\mathfrak{h}}) = \frac{1}{p} \times \sum_{\chi : H_m^{(d)}/\mathcal{J} \to \mathbb{C}_p^\times} \chi^{-1}(\underline{\mathfrak{h}})^p \\ &= \frac{\#H_m^{(d)}}{\#\mathcal{J}} \times \frac{1}{p} \mathrm{char}_{\mathcal{J}}(\underline{\mathfrak{h}}^p); \end{aligned}$$

the required expression for $c_{\underline{\mathfrak{h}}}^{(m)}$ now follows easily.

Focusing on the second statement, if $\underline{\mathfrak{h}}' \in \langle \underline{\mathfrak{h}} \rangle_{\mathrm{gen}}$ then $\langle \underline{\mathfrak{h}}' \rangle = \langle \underline{\mathfrak{h}} \rangle$ and $\langle \underline{\mathfrak{h}}'^p \rangle = \langle \underline{\mathfrak{h}}^p \rangle$, in which case $\mathrm{char}_{\mathcal{J}_\chi}(\underline{\mathfrak{h}}') = \mathrm{char}_{\mathcal{J}_\chi}(\underline{\mathfrak{h}})$ and $\mathrm{char}_{\mathcal{J}_\chi}(\underline{\mathfrak{h}}'^p) = \mathrm{char}_{\mathcal{J}_\chi}(\underline{\mathfrak{h}}^p)$ (since an element $\underline{\mathfrak{h}}$ lies in a subgroup $\mathcal{J}_\chi$ if and only $\underline{\mathfrak{h}}^t$ does for all powers t co-prime to p).

Consequently, $c_{\underline{\mathfrak{h}}'}^{(m)} = c_{\underline{\mathfrak{h}}}^{(m)}$ for all $\underline{\mathfrak{h}}' \in \langle \underline{\mathfrak{h}} \rangle_{\mathrm{gen}}$, and one deduces that Y_m equals

$$\sum_{\underline{\mathfrak{h}}' \in H_m^{(d)}} c_{\underline{\mathfrak{h}}'}^{(m)} [\underline{\mathfrak{h}}']_{H_m^{(d)}} = \sum_{\langle \underline{\mathfrak{h}} \rangle < H_m^{(d)}} \sum_{\underline{\mathfrak{h}}' \in \langle \underline{\mathfrak{h}} \rangle_{\mathrm{gen}}} c_{\underline{\mathfrak{h}}'}^{(m)} [\underline{\mathfrak{h}}']_{H_m^{(d)}} = \sum_{\langle \underline{\mathfrak{h}} \rangle < H_m^{(d)}} c_{\underline{\mathfrak{h}}}^{(m)} \sum_{\underline{\mathfrak{h}}' \in \langle \underline{\mathfrak{h}} \rangle_{\mathrm{gen}}} [\underline{\mathfrak{h}}']_{H_m^{(d)}}.$$

Lastly the term $\sum_{\underline{\mathfrak{h}}' \in \langle \underline{\mathfrak{h}} \rangle_{\mathrm{gen}}} [\underline{\mathfrak{h}}']_{H_m^{(d)}}$ is by definition $\mathcal{A}_{H_m^{(d)}} \langle \underline{\mathfrak{h}} \rangle$, so we are done. □

As $\mathrm{Im}(\theta_m^+)$ is generated over $\mathbb{Z}_p\left[\Sigma'_m\right]$ by $\phi(p^m)\cdot \mathrm{id}_{H_m^{(d)}}$ and the $p^{m-\nu_m(\underline{\mathfrak{h}})}\mathcal{A}_{H_m^{(d)}}\left\langle \underline{\mathfrak{h}}\right\rangle$'s, it follows that Y_m will belong to $\mathrm{Im}(\theta_m^+)$ if and only if:

- if $\underline{\mathfrak{h}} \neq \mathrm{id}_{H_m^{(d)}}$ then $p^{m-\nu_m(\underline{\mathfrak{h}})}$ divides each $c_{\underline{\mathfrak{h}}}^{(m)}$;
- if $\underline{\mathfrak{h}} = \mathrm{id}_{H_m^{(d)}}$ then p^{m-1} divides each $c_{\mathrm{id}_{H_m^{(d)}}}^{(m)}$.

Furthermore by Theorem 4.0.13, the full ensemble $\left\{Y_m\right\}_{0\leq m\leq n}$ belongs to $\mathrm{Im}\left(\prod\theta_m^+\right)$ if and only if

- the elements Y_m are trace-compatible, i.e. $\mathrm{Tr}_{\Sigma'_{(m-1)}/\Sigma'_{(m)}}\left(Y_{m-1}\right)\equiv Y_m$.

To make the above conditions more explicit, we shall rewrite the coefficients $c_{\underline{\mathfrak{h}}}^{(m)}$. Because of Proposition 3.1.9(ii), let us henceforth assume that each $a_{m,\chi}$ depends only on $\mathcal{J}_\chi$, and set $a_{\mathcal{J}_\chi}^{(m)} = a_{m,\chi}$. Note that $a_{\mathcal{J}_1}^{(m)} = a_{H_m^{(d)}}^{(m)}$ since $\mathrm{Ker}(\mathbf{1}) = H_m^{(d)}$.

Decomposing $\mathcal{Z}_m$ into its constituent $\mathcal{Z}_m^{(v)}$'s, one calculates that

$$\begin{aligned} c_{\underline{\mathfrak{h}}}^{(m)} &= p^{-md}\, a_{H_m^{(d)}}^{(m)} + \sum_{v=1}^{m}\sum_{\mathcal{J}_\chi\in\mathcal{Z}_m^{(v)}} \frac{1}{p^{md-v}}\times\left(\mathrm{char}_{\mathcal{J}_\chi}\left(\underline{\mathfrak{h}}\right) - \frac{1}{p}\,\mathrm{char}_{\mathcal{J}_\chi}\left(\underline{\mathfrak{h}}^p\right)\right) a_{\mathcal{J}_\chi}^{(m)} \\ &= p^{-md}\left(a_{H_m^{(d)}}^{(m)} + \sum_{v=1}^{m}\sum_{\mathcal{J}_\chi\in\mathcal{Z}_m^{(v)}} p^{v-1}\times\left(p\,\mathrm{char}_{\mathcal{J}_\chi}\left(\underline{\mathfrak{h}}\right) - \mathrm{char}_{\mathcal{J}_\chi}\left(\underline{\mathfrak{h}}^p\right)\right) a_{\mathcal{J}_\chi}^{(m)}\right). \end{aligned}$$

Fact 5. *Consider a character $\chi : H_m^{(d)} \twoheadrightarrow \mu_{p^{m-1}}$; this same character maps $H_{m-1}^{(d)}$ onto $\mu_{p^{m-1}}$, so $\mathcal{J}_\chi$ can be viewed both as a subgroup of $H_m^{(d)}$ and $H_{m-1}^{(d)}$. Thus if $\left\{Y_m\right\}_{0\leq m\leq n}$ belongs to $\Omega_n^{(d)} = \mathrm{Im}\left(\prod\theta_m^+\right)$, then $a_{\mathcal{J}_\chi}^{(m)} = \mathrm{Tr}_{\Sigma'_{(m-1)}/\Sigma'_{(m)}}\left(a_{\mathcal{J}_\chi}^{(m-1)}\right)$.*

Proof of Fact 5: We have a commutative diagram

$$\begin{array}{ccc} \mathbb{Z}_p\left[\Sigma'_{(m)}\times H_m^{(d)}\right] & \xrightarrow{\ \chi\ } & \mathbb{Z}_p\left[\Sigma'_{(m)}\right]\left[\mu_{p^{m-1}}\right] \\ {\scriptstyle \mathrm{mod}\,(H_m^{(d)})^{p^{m-1}}}\downarrow & \nearrow_{\chi} & \\ \mathbb{Z}_p\left[\Sigma'_{(m)}\times H_{m-1}^{(d)}\right] & & \end{array}$$

which implies

$$\begin{aligned} a_{\mathcal{J}_\chi}^{(m)} &= \chi(Y_m) = \chi(Y_m \mod (H_m^{(d)})^{p^{m-1}}) \\ &= \chi(\mathrm{Tr}_{\Sigma'_{(m-1)}/\Sigma'_{(m)}}(Y_{m-1})) \quad \text{(because of the trace relation)} \end{aligned}$$

$$= \mathrm{Tr}_{\Sigma'_{(m-1)}/\Sigma'_{(m)}}(\chi(Y_{m-1})) = \mathrm{Tr}_{\Sigma'_{(m-1)}/\Sigma'_{(m)}}\big(a^{(m-1)}_{\mathcal{J}_\chi}\big).$$

□

Remark 6.1.2. *Fact* 5 *implies (via simple induction) that* $a^{(m)}_{\mathcal{J}_\chi} = \mathrm{Tr}_{\Sigma'_{(v)}/\Sigma'_{(m)}}\big(a^{(v)}_{\mathcal{J}_\chi}\big)$ *at every* $\mathcal{J}_\chi \in \mathcal{Z}^{(v)}_m$.

Corollary 6.1.3. *Under the assumptions of Lemma* 6.1.1, *each element* $p^{md} \times c^{(m)}_{\underline{\mathfrak{h}}}$ *equals*

$$\mathrm{Tr}_{\Sigma'_{(0)}/\Sigma'_{(m)}}\left(a^{(0)}_{H^{(d)}_m}\right) + \sum_{v=1}^{m} \sum_{\mathcal{J}_\chi \in \mathcal{Z}^{(v)}_m} p^{v-1}\mathrm{Tr}_{\Sigma'_{(v)}/\Sigma'_{(m)}}\left(a^{(v)}_{\mathcal{J}_\chi}\right) \times \Big(p\ \mathrm{char}_{\mathcal{J}_\chi}(\underline{\mathfrak{h}}) - \mathrm{char}_{\mathcal{J}_\chi}(\underline{\mathfrak{h}}^p)\Big).$$

Exploiting this new description for the coefficients of Y_m, we see that if $\underline{\mathfrak{h}} \neq \mathrm{id}_{H^{(d)}_m}$ then the divisibility of $p^{m-\nu_m(\underline{\mathfrak{h}})}$ into $c^{(m)}_{\underline{\mathfrak{h}}}$ is equivalent to the congruence (6.1m,$\underline{\mathfrak{h}}$). Secondly, if $\underline{\mathfrak{h}} = \mathrm{id}_{H^{(d)}_m}$ then the divisibility of p^{m-1} into $c^{(m)}_{\mathrm{id}_{H^{(d)}_m}}$ is equivalent to the congruence (6.2m,id).

To complete the proof of Theorem 6.0.1, one needs to verify the congruence $\mathrm{Tr}_{\Sigma'_{(m-1)}/\Sigma'_{(m)}}\big(Y_{m-1}\big) \equiv Y_m$ modulo $\big(H^{(d)}_m\big)^{p^{m-1}}$. The latter task relies on the identity

$$\sum_{\langle \underline{\mathfrak{h}} \rangle < H^{(d)}_{m-1}} \mathrm{Tr}_{\Sigma'_{(m-1)}/\Sigma'_{(m)}}\Big(c^{(m-1)}_{\underline{\mathfrak{h}}}\Big)\mathcal{A}_{H^{(d)}_{m-1}}\langle \underline{\mathfrak{h}} \rangle \;=\; \sum_{\langle \underline{\mathfrak{h}}' \rangle < H^{(d)}_m} c^{(m)}_{\underline{\mathfrak{h}}'} \frac{\phi(p^{\nu_m(\underline{\mathfrak{h}}')})}{\phi(p^{\nu_{m-1}(\underline{\mathfrak{h}}')})}\,\mathcal{A}_{H^{(d)}_{m-1}}\langle \underline{\mathfrak{h}}' \rangle .$$

We now give the details of this calculation.

Lemma 6.1.4. *The trace relation*

$$\mathrm{Tr}_{\Sigma'_{(m-1)}/\Sigma'_{(m)}}\big(Y_{m-1}\big) \equiv Y_m \mod \big(H^{(d)}_m\big)^{p^{m-1}} \text{ holds,}$$

where $Y_m = \sum_{\langle \underline{\mathfrak{h}}' \rangle < H^{(d)}_m} c^{(m)}_{\underline{\mathfrak{h}}'}\mathcal{A}_{H^{(d)}_m}\langle \underline{\mathfrak{h}}' \rangle$ *and* $Y_{m-1} = \sum_{\langle \underline{\mathfrak{h}} \rangle < H^{(d)}_{m-1}} c^{(m-1)}_{\underline{\mathfrak{h}}}\mathcal{A}_{H^{(d)}_{m-1}}\langle \underline{\mathfrak{h}} \rangle$.

Proof. For ease of notation, let us define

$$c^{(m)}_{\underline{\mathfrak{h}}'} := c^{(m)\dagger}_{\underline{\mathfrak{h}}'} + c^{(m)\ddagger}_{\underline{\mathfrak{h}}'}, \text{ where } c^{(m)\dagger}_{\underline{\mathfrak{h}}'} := p^{-md}\mathrm{Tr}_{\Sigma'_{(0)}/\Sigma'_{(m)}}\left(a^{(0)}_{H^{(d)}_m}\right), \text{ and}$$

$$c^{(m)\ddagger}_{\underline{\mathfrak{h}}'} := p^{-md}\sum_{v=1}^{m} \sum_{\mathcal{J}_\chi \in \mathcal{Z}^{(v)}_m} p^{v-1}\mathrm{Tr}_{\Sigma'_{(v)}/\Sigma'_{(m)}}\left(a^{(v)}_{\mathcal{J}_\chi}\right) \times \Big(p\ \mathrm{char}_{\mathcal{J}_\chi}(\underline{\mathfrak{h}}') - \mathrm{char}_{\mathcal{J}_\chi}((\underline{\mathfrak{h}}')^p)\Big).$$

We make a similar definition at level $m-1$ for $c_{\underline{\mathfrak{h}}}^{(m-1)}$.

The trace map $\mathrm{Tr}_{\Sigma'_{(m-1)}/\Sigma'_{(m)}}$ acts only on $\sigma \in \Sigma'_{(m-1)}$, so

$$\mathrm{Tr}_{\Sigma'_{(m-1)}/\Sigma'_{(m)}}(Y_{m-1}) = \sum_{\langle \underline{\mathfrak{h}} \rangle < H_{m-1}^{(d)}} \mathrm{Tr}_{\Sigma'_{(m-1)}/\Sigma'_{(m)}}(c_{\underline{\mathfrak{h}}}^{(m-1)\dagger}) \mathcal{A}_{H_{m-1}^{(d)}} \langle \underline{\mathfrak{h}} \rangle + \sum_{\langle \underline{\mathfrak{h}} \rangle < H_{m-1}^{(d)}} \mathrm{Tr}_{\Sigma'_{(m-1)}/\Sigma'_{(m)}}(c_{\underline{\mathfrak{h}}}^{(m-1)\ddagger}) \mathcal{A}_{H_{m-1}^{(d)}} \langle \underline{\mathfrak{h}} \rangle .$$

On the other hand,

$$Y_m = \sum_{\langle \underline{\mathfrak{h}}' \rangle < H_m^{(d)}} c_{\underline{\mathfrak{h}}'}^{(m)\dagger} \mathcal{A}_{H_m^{(d)}} \langle \underline{\mathfrak{h}}' \rangle + \sum_{\langle \underline{\mathfrak{h}}' \rangle < H_m^{(d)}} c_{\underline{\mathfrak{h}}'}^{(m)\ddagger} \mathcal{A}_{H_m^{(d)}} \langle \underline{\mathfrak{h}}' \rangle .$$

Remark 6.1.5. *Let* $\underline{\mathfrak{h}} \in H_{m-1}^{(d)}$ *and* $\underline{\mathfrak{h}}' \in H_m^{(d)}$.
(i) If $\nu_m(\underline{\mathfrak{h}}') \geq 2$, *then* $\mathcal{A}_{H_m^{(d)}} \langle \underline{\mathfrak{h}}' \rangle \equiv p \mathcal{A}_{H_{m-1}^{(d)}} \langle \underline{\mathfrak{h}} \rangle \mod \left(H_m^{(d)}\right)^{p^{m-1}}$, *where* $\underline{\mathfrak{h}}' \equiv \underline{\mathfrak{h}} \mod \left(H_m^{(d)}\right)^{p^{m-1}}$.
(ii) If $\nu_m(\underline{\mathfrak{h}}') = 1$, *then* $\mathcal{A}_{H_m^{(d)}} \langle \underline{\mathfrak{h}}' \rangle \equiv (p-1)[id]_{H_{m-1}^{(d)}} \mod \left(H_m^{(d)}\right)^{p^{m-1}}$.
(iii) If $\nu_m(\underline{\mathfrak{h}}') = 0$, *then* $[id]_{H_m^{(d)}} \equiv [id]_{H_{m-1}^{(d)}} \mod \left(H_m^{(d)}\right)^{p^{m-1}}$.

We shall now prove a further two facts.

Fact 6.

$$\sum_{\langle \underline{\mathfrak{h}} \rangle < H_{m-1}^{(d)}} Tr_{\Sigma'_{(m-1)}/\Sigma'_{(m)}}(c_{\underline{\mathfrak{h}}}^{(m-1)\dagger}) \mathcal{A}_{H_{m-1}^{(d)}} \langle \underline{\mathfrak{h}} \rangle \equiv \sum_{\langle \underline{\mathfrak{h}}' \rangle < H_m^{(d)}} c_{\underline{\mathfrak{h}}'}^{(m)\dagger} \mathcal{A}_{H_m^{(d)}} \langle \underline{\mathfrak{h}}' \rangle \mod \left(H_m^{(d)}\right)^{p^{m-1}}$$

Fact 7.

$$\sum_{\langle \underline{\mathfrak{h}} \rangle < H_{m-1}^{(d)}} Tr_{\Sigma'_{(m-1)}/\Sigma'_{(m)}}(c_{\underline{\mathfrak{h}}}^{(m-1)\ddagger}) \mathcal{A}_{H_{m-1}^{(d)}} \langle \underline{\mathfrak{h}} \rangle \equiv \sum_{\langle \underline{\mathfrak{h}}' \rangle < H_m^{(d)}} c_{\underline{\mathfrak{h}}'}^{(m)\ddagger} \mathcal{A}_{H_m^{(d)}} \langle \underline{\mathfrak{h}}' \rangle \mod \left(H_m^{(d)}\right)^{p^{m-1}}$$

Proof of Fact 6: As a result of Remarks 6.1.5(i)-(iii),

$$\sum_{\langle \underline{\mathfrak{h}}' \rangle < H_m^{(d)}} c_{\underline{\mathfrak{h}}'}^{(m)\dagger} \mathcal{A}_{H_m^{(d)}} \langle \underline{\mathfrak{h}}' \rangle \equiv c_{\underline{\mathfrak{h}}'}^{(m)\dagger} [\mathrm{id}]_{H_{m-1}^{(d)}} + \sum_{\substack{\langle \underline{\mathfrak{h}}' \rangle < H_m^{(d)}, \#\langle \underline{\mathfrak{h}}' \rangle = p, \\ \langle \underline{\mathfrak{h}}' \rangle \equiv [\mathrm{id}]_{H_{m-1}^{(d)}}}} c_{\underline{\mathfrak{h}}'}^{(m)\dagger} (p-1) [\mathrm{id}]_{H_{m-1}^{(d)}} +$$

$$+ \sum_{r=1}^{m-1} \sum_{\substack{\langle \underline{\mathfrak{h}} \rangle < H_{m-1}^{(d)}, \\ \langle \underline{\mathfrak{h}} \rangle = p^r}} \sum_{\substack{\langle \underline{\mathfrak{h}}' \rangle < H_m^{(d)}, \#\langle \underline{\mathfrak{h}}' \rangle = p^{r+1}, \\ \langle \underline{\mathfrak{h}}' \rangle \equiv \langle \underline{\mathfrak{h}} \rangle}} c_{\underline{\mathfrak{h}}'}^{(m)\dagger} p \mathcal{A}_{H_{m-1}^{(d)}} \langle \underline{\mathfrak{h}} \rangle \mod \left(H_m^{(d)} \right)^{p^{m-1}}.$$

Remark 6.1.6. *(i) The cardinality of the set*

$$\left\{ \langle \underline{\mathfrak{h}}' \rangle < H_m^{(d)} \,\middle|\, \#\langle \underline{\mathfrak{h}}' \rangle = p, \langle \underline{\mathfrak{h}}' \rangle \equiv [\mathrm{id}]_{H_{m-1}^{(d)}} \mod \left(H_m^{(d)} \right)^{p^{m-1}} \right\} \text{ is } \frac{p^d - 1}{p-1}.$$

(ii) There are $\frac{p^{rd} - p^{(r-1)d}}{\phi(p^r)}$ *cyclic subgroups* $\langle \underline{\mathfrak{h}} \rangle < H_{m-1}^{(d)}$ *of size* p^r*, and there are* $\frac{p^{(r+1)d} - p^{rd}}{\phi(p^{r+1})}$ *cyclic subgroups* $\langle \underline{\mathfrak{h}}' \rangle < H_m^{(d)}$ *of size* p^{r+1}*.*

(iii) It follows that modulo $\left(H_m^{(d)} \right)^{p^{m-1}}$ *there are* $\frac{p^{(r+1)d} - p^{rd}}{\phi(p^{r+1})} \div \frac{p^{rd} - p^{(r-1)d}}{\phi(p^r)} = \frac{p^d}{p}$ *cyclic subgroups* $\langle \underline{\mathfrak{h}}' \rangle < H_m^{(d)}$ *of size* p^{r+1} *that are congruent to each* $\langle \underline{\mathfrak{h}} \rangle < H_{m-1}^{(d)}$ *of size* p^r*.*

Notice that there is no $\underline{\mathfrak{h}}$ appearing in $c_{\underline{\mathfrak{h}}}^{(m)\dagger}$. Now from Remarks 6.1.6 (i)-(iii), we have

$$\sum_{\langle \underline{\mathfrak{h}}' \rangle < H_m^{(d)}} c_{\underline{\mathfrak{h}}'}^{(m)\dagger} \mathcal{A}_{H_m^{(d)}} \langle \underline{\mathfrak{h}}' \rangle \equiv c_{\underline{\mathfrak{h}}'}^{(m)\dagger} [\mathrm{id}]_{H_{m-1}^{(d)}} + c_{\underline{\mathfrak{h}}'}^{(m)\dagger} (p^d - 1) [\mathrm{id}]_{H_{m-1}^{(d)}} +$$

$$+ \sum_{r=1}^{m-1} \sum_{\substack{\langle \underline{\mathfrak{h}} \rangle < H_{m-1}^{(d)} \\ \langle \underline{\mathfrak{h}} \rangle = p^r}} c_{\underline{\mathfrak{h}}'}^{(m)\dagger} p^d \mathcal{A}_{H_{m-1}^{(d)}} \langle \underline{\mathfrak{h}} \rangle \mod \left(H_m^{(d)} \right)^{p^{m-1}}$$

$$= \sum_{\langle \underline{\mathfrak{h}} \rangle < H_{m-1}^{(d)}} c_{\underline{\mathfrak{h}}'}^{(m)\dagger} p^d \mathcal{A}_{H_{m-1}^{(d)}} \langle \underline{\mathfrak{h}} \rangle$$

$$= \sum_{\langle \underline{\mathfrak{h}} \rangle < H_{m-1}^{(d)}} p^{-md} p^d \mathrm{Tr}_{\Sigma'_{(0)}/\Sigma'_{(m)}} \left(a_{H_m^{(d)}}^{(0)} \right) \mathcal{A}_{H_{m-1}^{(d)}} \langle \underline{\mathfrak{h}} \rangle$$

$$= \sum_{\langle \underline{\mathfrak{h}} \rangle < H_{m-1}^{(d)}} p^{-(m-1)d} \mathrm{Tr}_{\Sigma'_{(m-1)}/\Sigma'_{(m)}} \left(\mathrm{Tr}_{\Sigma'_{(0)}/\Sigma'_{(m-1)}} (a_{H_{m-1}^{(d)}}^{(0)}) \right) \mathcal{A}_{H_{m-1}^{(d)}} \langle \underline{\mathfrak{h}} \rangle$$

$$= \sum_{\langle \underline{\mathfrak{h}} \rangle < H_{m-1}^{(d)}} \mathrm{Tr}_{\Sigma'_{(m-1)}/\Sigma'_{(m)}}(c_{\underline{\mathfrak{h}}}^{(m-1)\dagger}) \mathcal{A}_{H_{m-1}^{(d)}} \langle \underline{\mathfrak{h}} \rangle .$$

This completes the proof of Fact 6. □

Proof of Fact 7: Again due to Remarks 6.1.5(i)-(iii),

$$\sum_{\langle \underline{\mathfrak{h}}' \rangle < H_m^{(d)}} c_{\underline{\mathfrak{h}}'}^{(m)\ddagger} \mathcal{A}_{H_m^{(d)}} \langle \underline{\mathfrak{h}}' \rangle \equiv c_{\mathrm{id}}^{(m)\ddagger} [\mathrm{id}]_{H_{m-1}^{(d)}} + \sum_{\substack{\langle \underline{\mathfrak{h}}' \rangle < H_m^{(d)}, \#\langle \underline{\mathfrak{h}}' \rangle = p, \\ \langle \underline{\mathfrak{h}}' \rangle \equiv [\mathrm{id}]_{H_{m-1}^{(d)}}}} c_{\underline{\mathfrak{h}}'}^{(m)\ddagger} (p-1)[\mathrm{id}]_{H_{m-1}^{(d)}} +$$

$$+ \sum_{r=1}^{m-1} \sum_{\substack{\langle \underline{\mathfrak{h}} \rangle < H_{m-1}^{(d)}, \\ \langle \underline{\mathfrak{h}} \rangle = p^r}} \sum_{\substack{\langle \underline{\mathfrak{h}}' \rangle < H_m^{(d)}, \#\langle \underline{\mathfrak{h}}' \rangle = p^{r+1}, \\ \langle \underline{\mathfrak{h}}' \rangle \equiv \langle \underline{\mathfrak{h}} \rangle}} c_{\underline{\mathfrak{h}}'}^{(m)\ddagger} p \mathcal{A}_{H_{m-1}^{(d)}} \langle \underline{\mathfrak{h}} \rangle \mod \left(H_m^{(d)}\right)^{p^{m-1}}.$$

One calculates the following:

• $c_{\mathrm{id}}^{(m)\ddagger} = p^{-md}(p-1) \sum_{v=1}^{m} \sum_{\mathcal{J}_\chi \in \mathcal{Z}_m^{(v)}} p^{v-1} \mathrm{Tr}_{\Sigma'_{(v)}/\Sigma'_{(m)}} \left(a_{\mathcal{J}_\chi}^{(v)}\right)$.

• For any fixed character $\chi : H_m^{(d)} \twoheadrightarrow \mu_{p^v}$ with $1 \leq v \leq m-1$, it is clear that if $\nu_m(\underline{\mathfrak{h}}') = 1$, we have $\underline{\mathfrak{h}}' \in \mathcal{J}_\chi$; furthermore, if $\underline{\mathfrak{h}}' \in \mathcal{J}_\chi$, then $(\underline{\mathfrak{h}}')^p \in \mathcal{J}_\chi$. Now by Remark 6.1.6(i) for $1 \leq v \leq m-1$,

$$\sum_{\substack{\langle \underline{\mathfrak{h}}' \rangle < H_m^{(d)}, \#\langle \underline{\mathfrak{h}}' \rangle = p, \\ \langle \underline{\mathfrak{h}}' \rangle \equiv [\mathrm{id}]_{H_{m-1}^{(d)}}}} \left(p \mathrm{char}_{\mathcal{J}_\chi}(\underline{\mathfrak{h}}') - \mathrm{char}_{\mathcal{J}_\chi}((\underline{\mathfrak{h}}')^p) \right) = \frac{p^d - 1}{p-1}(p-1) = p^d - 1.$$

• For any character $\chi : H_m^{(d)} \twoheadrightarrow \mu_{p^m}$ with $\nu_m(\underline{\mathfrak{h}}') = 1$, we have $(\underline{\mathfrak{h}}')^p \in \mathcal{J}_\chi$; by Remark 6.1.6(i) again,

$$\sum_{\substack{\langle \underline{\mathfrak{h}}' \rangle < H_m^{(d)}, \#\langle \underline{\mathfrak{h}}' \rangle = p, \\ \langle \underline{\mathfrak{h}}' \rangle \equiv [\mathrm{id}]_{H_{m-1}^{(d)}}}} \mathrm{char}_{\mathcal{J}_\chi}((\underline{\mathfrak{h}}')^p) = \frac{p^d - 1}{p-1}.$$

• Fix any character $\chi : H_m^{(d)} \twoheadrightarrow \mu_{p^m}$; the size of $\left\{ \underline{\mathfrak{h}}' \in H_m^{(d)} \,\middle|\, \nu_m(\underline{\mathfrak{h}}') \leq 1, \underline{\mathfrak{h}}' \in \mathcal{J}_\chi \right\}$ is p^{d-1}, and the cardinality of the set $\left\{ \underline{\mathfrak{h}}' \in H_m^{(d)} \,\middle|\, \nu_m(\underline{\mathfrak{h}}') = 0, \underline{\mathfrak{h}}' \in \mathcal{J}_\chi \right\}$ equals 1. Consequently, the size of the set $\left\{ \underline{\mathfrak{h}}' \in H_m^{(d)} \,\middle|\, \nu_m(\underline{\mathfrak{h}}') = 1, \underline{\mathfrak{h}}' \in \mathcal{J}_\chi \right\}$ equals $p^{d-1} - 1$.

Notice that when $\nu_m(\underline{\mathfrak{h}}') = 1$, the size of $\langle \underline{\mathfrak{h}}' \rangle_{\text{gen}}$ is $p-1$. Furthermore, there is an equality $\text{char}_{\mathcal{J}_\chi}(\underline{\mathfrak{h}}') = \text{char}_{\mathcal{J}_\chi}((\underline{\mathfrak{h}}')^t)$ for all t co-prime to p, therefore

$$\sum_{\substack{\langle \underline{\mathfrak{h}}' \rangle < H_m^{(d)}, \#\langle \underline{\mathfrak{h}}' \rangle = p, \\ \langle \underline{\mathfrak{h}}' \rangle \equiv [\text{id}]_{H_{m-1}^{(d)}}}} p \times \text{char}_{\mathcal{J}_\chi}(\underline{\mathfrak{h}}') = p\left(\frac{p^{d-1}-1}{p-1}\right).$$

Using the above bullet points, we first calculate that

$$\sum_{\substack{\langle \underline{\mathfrak{h}}' \rangle < H_m^{(d)}, \#\langle \underline{\mathfrak{h}}' \rangle = p, \\ \langle \underline{\mathfrak{h}}' \rangle \equiv [\text{id}]_{H_{m-1}^{(d)}}}} c_{\underline{\mathfrak{h}}'}^{(m)\ddagger}(p-1)[\text{id}]_{H_{m-1}^{(d)}} = \Bigg[p^{-md}(p-1)(p^d-1) \sum_{v=1}^{m-1} \sum_{\mathcal{J}_\chi \in Z_m^{(v)}} p^{v-1} \times$$

$$\text{Tr}_{\Sigma'_{(v)}/\Sigma'_{(m)}}(a_{J_\chi}^{(v)}) + p^{-md}(p-1) \sum_{\mathcal{J}_\chi \in Z_m^{(m)}} p^{m-1} a_{\mathcal{J}_\chi}^{(m)} \left(p\left(\frac{p^{d-1}-1}{p-1}\right) - \frac{p^d-1}{p-1} \right) \Bigg] [\text{id}]_{H_{m-1}^{(d)}}$$

$$= \Bigg[p^{-md}(p-1)(p^d-1) \sum_{v=1}^{m-1} \sum_{\mathcal{J}_\chi \in Z_m^{(v)}} p^{v-1} \text{Tr}_{\Sigma'_{(v)}/\Sigma'_{(m)}}(a_{J_\chi}^{(v)}) - p^{-md}(p-1) \times$$

$$\times \sum_{\mathcal{J}_\chi \in Z_m^{(m)}} p^{m-1} a_{\mathcal{J}_\chi}^{(m)} \Bigg] [\text{id}]_{H_{m-1}^{(d)}}.$$

Then applying our formula for $c_{\text{id}}^{(m)\ddagger}$, we deduce that

$$c_{\text{id}}^{(m)\ddagger}[\text{id}]_{H_{m-1}^{(d)}} + \sum_{\substack{\langle \underline{\mathfrak{h}}' \rangle < H_m^{(d)}, \#\langle \underline{\mathfrak{h}}' \rangle = p, \\ \langle \underline{\mathfrak{h}}' \rangle \equiv [\text{id}]_{H_{m-1}^{(d)}}}} c_{\underline{\mathfrak{h}}'}^{(m)\ddagger}(p-1)[\text{id}]_{H_{m-1}^{(d)}} =$$

$$= p^{-(m-1)d}(p-1) \sum_{v=1}^{m-1} \sum_{\mathcal{J}_\chi \in Z_m^{(v)}} p^{v-1} \text{Tr}_{\Sigma'_{(v)}/\Sigma'_{(m)}}(a_{\mathcal{J}_\chi}^{(v)})[\text{id}]_{H_{m-1}^{(d)}}$$

$$= \text{Tr}_{\Sigma'_{(m-1)}/\Sigma'_{(m)}}\left(c_{\text{id}}^{(m-1)\ddagger}\right)[\text{id}]_{H_{m-1}^{(d)}}.$$

To complete the proof of Fact 7, we are left to show that

$$\sum_{r=1}^{m-1}\sum_{\substack{\langle \underline{\mathfrak{h}}\rangle < H_{m-1}^{(d)},\\ \langle \underline{\mathfrak{h}}\rangle = p^r}} \mathrm{Tr}_{\Sigma'_{(m-1)}/\Sigma'_{(m)}}(c_{\underline{\mathfrak{h}}}^{(m-1)\ddagger})\mathcal{A}_{H_{m-1}^{(d)}}\langle \underline{\mathfrak{h}}\rangle = \sum_{r=1}^{m-1}\sum_{\substack{\langle \underline{\mathfrak{h}}\rangle < H_{m-1}^{(d)},\\ \langle \underline{\mathfrak{h}}\rangle = p^r}} \times \sum_{\substack{\langle \underline{\mathfrak{h}}'\rangle < H_m^{(d)}, \#\langle \underline{\mathfrak{h}}'\rangle = p^{r+1},\\ \langle \underline{\mathfrak{h}}'\rangle \equiv \langle \underline{\mathfrak{h}}\rangle}} c_{\underline{\mathfrak{h}}'}^{(m)\ddagger} p\mathcal{A}_{H_{m-1}^{(d)}}\langle \underline{\mathfrak{h}}\rangle .$$

This equality requires the following further two observations:

- If a character $\chi : H_m^{(d)} \twoheadrightarrow \mu_{p^v}$ with $v \leq m-1$, there is a natural factorization $\chi : H_m^{(d)} \to H_v^{(d)} \twoheadrightarrow \mu_{p^v}$, which means that $\chi(\underline{\mathfrak{h}}') = \chi(\underline{\mathfrak{h}})$. It follows that $\mathrm{char}_{\mathcal{J}_\chi}(\underline{\mathfrak{h}}') = \mathrm{char}_{\mathcal{J}_\chi}(\underline{\mathfrak{h}})$ and $\mathrm{char}_{\mathcal{J}_\chi}((\underline{\mathfrak{h}}')^p) = \mathrm{char}_{\mathcal{J}_\chi}((\underline{\mathfrak{h}})^p)$.
- Alternatively if the character $\chi : H_m^{(d)} \twoheadrightarrow \mu_{p^m}$, we notice that $\chi((\underline{\mathfrak{h}}')^p) = \chi^p(\underline{\mathfrak{h}}')$. Also, observe that $\mathcal{J}_\chi \subset \mathcal{J}_{\chi^p} \subset H_m^{(d)}$, and the character χ^p has the factorization $\chi^p : H_m^{(d)} \xrightarrow{\mathrm{mod}\ (H_m^{(d)})^{p^{m-1}}} H_{m-1}^{(d)} \twoheadrightarrow \mu_{p^{m-1}}$. As a result, the only case we need to consider is if $\underline{\mathfrak{h}}' \in \mathcal{J}_{\chi^p}$, otherwise $p \times \mathrm{char}_{\mathcal{J}_\chi}(\underline{\mathfrak{h}}') - \mathrm{char}_{\mathcal{J}_{\chi^p}}(\underline{\mathfrak{h}}') = 0$. Let

  $$\mathrm{Y}_{\langle \underline{\mathfrak{h}}'\rangle} = \left\{ \langle \underline{\mathfrak{h}}'\rangle < H_m^{(d)} \,\middle|\, \#\langle \underline{\mathfrak{h}}'\rangle = p^{r+1}, \underline{\mathfrak{h}}' \in \mathcal{J}_{\chi^p}, \langle \underline{\mathfrak{h}}'\rangle \equiv \langle \underline{\mathfrak{h}}\rangle \bmod \left(H_m^{(d)}\right)^{p^{m-1}} \right\}.$$

  Since $\underline{\mathfrak{h}}' \in \mathcal{J}_{\chi^p}$ we have $\chi(\underline{\mathfrak{h}}') \in \mu_p$, where the values are equidistributed across μ_p. This equidistribution property implies

  $$\#\left\{ \langle \underline{\mathfrak{h}}'\rangle \subset \mathcal{J}_\chi \,\middle|\, \#\langle \underline{\mathfrak{h}}'\rangle = p^{r+1}, \langle \underline{\mathfrak{h}}'\rangle \equiv \langle \underline{\mathfrak{h}}\rangle \bmod \left(H_m^{(d)}\right)^{p^{m-1}} \right\} = \frac{1}{\#\mu_p}\#\mathrm{Y}_{\langle \underline{\mathfrak{h}}'\rangle}.$$

  Therefore one obtains the cancellation

  $$p \sum_{\substack{\langle \underline{\mathfrak{h}}'\rangle < H_m^{(d)}, \#\langle \underline{\mathfrak{h}}'\rangle = p^{r+1}\\ \langle \underline{\mathfrak{h}}'\rangle \equiv \langle \underline{\mathfrak{h}}\rangle, \underline{\mathfrak{h}}' \in \mathcal{J}_\chi}} - \sum_{\substack{\langle \underline{\mathfrak{h}}'\rangle < H_m^{(d)}, \#\langle \underline{\mathfrak{h}}'\rangle = p^{r+1}\\ \langle \underline{\mathfrak{h}}'\rangle \equiv \langle \underline{\mathfrak{h}}\rangle, \underline{\mathfrak{h}}' \in \mathcal{J}_{\chi^p}}} = p\frac{1}{\#\mu_p}\#\mathrm{Y}_{\langle \underline{\mathfrak{h}}'\rangle} - \#\mathrm{Y}_{\langle \underline{\mathfrak{h}}'\rangle} = 0.$$

Combining these two results with Remark 6.1.6(ii), we have

$$\sum_{\substack{\langle \underline{\mathfrak{h}}' \rangle < H_m^{(d)}, \#\langle \underline{\mathfrak{h}}' \rangle = p^{r+1}, \\ \langle \underline{\mathfrak{h}}' \rangle \equiv \langle \underline{\mathfrak{h}} \rangle}} c_{\underline{\mathfrak{h}}'}^{(m)\ddagger} p = \left(\frac{p^d}{p} \right) p p^{-md} \sum_{v=1}^{m-1} \sum_{\mathcal{J}_\chi \in \mathcal{Z}_m^{(v)}} p^{v-1} \mathrm{Tr}_{\Sigma'_{(v)}/\Sigma'_{(m)}} \left(a_{\mathcal{J}_\chi}^{(v)} \right) \times$$

$$\times \left(p \, \mathrm{char}_{\mathcal{J}_\chi}(\underline{\mathfrak{h}}) - \mathrm{char}_{\mathcal{J}_\chi}((\underline{\mathfrak{h}})^p) \right) + 0$$

$$= \mathrm{Tr}_{\Sigma'_{(m-1)}/\Sigma'_{(m)}} (c_{\underline{\mathfrak{h}}}^{(m-1)\ddagger}),$$

which completes the proof of Fact 7. □

Applying Facts 6 and 7 in tandem, we have

$$\sum_{\langle \underline{\mathfrak{h}} \rangle < H_{m-1}^{(d)}} \mathrm{Tr}_{\Sigma'_{(m-1)}/\Sigma'_{(m)}} (c_{\underline{\mathfrak{h}}}^{(m-1)\dagger}) \mathcal{A}_{H_{m-1}^{(d)}} \langle \underline{\mathfrak{h}} \rangle + \sum_{\langle \underline{\mathfrak{h}} \rangle < H_{m-1}^{(d)}} \mathrm{Tr}_{\Sigma'_{(m-1)}/\Sigma'_{(m)}} (c_{\underline{\mathfrak{h}}}^{(m-1)\ddagger}) \mathcal{A}_{H_{m-1}^{(d)}} \langle \underline{\mathfrak{h}} \rangle$$

is congruent to

$$\sum_{\langle \underline{\mathfrak{h}}' \rangle < H_m^{(d)}} c_{\underline{\mathfrak{h}}'}^{(m)\dagger} \mathcal{A}_{H_m^{(d)}} \langle \underline{\mathfrak{h}}' \rangle + \sum_{\langle \underline{\mathfrak{h}}' \rangle < H_m^{(d)}} c_{\underline{\mathfrak{h}}'}^{(m)\ddagger} \mathcal{A}_{H_m^{(d)}} \langle \underline{\mathfrak{h}}' \rangle$$

modulo $\left(H_m^{(d)} \right)^{p^{m-1}}$. Hence we obtain the required congruence in Lemma 6.1.4. □

6.2 The Proof of Theorem 1.0.2

Recall from our earlier discussion, the key conditions underpinning the main result collapse down to checking whether or not $\underline{\log}_n^\dagger \circ \underline{\mathrm{tw}}_n(\underline{z}) \in \Psi_n^{(d)}$, which can now be tested using the p-power congruences (6.1m,$\underline{\mathfrak{h}}$) and (6.2m,id) of Theorem 6.0.1.

Fix a vector $\underline{z} \in \prod_{m=0}^n \mathbb{Z}_p[\mathfrak{S}_m^{\mathrm{ab}}]^\times$. At each character $\chi : H_n^{(d)} \twoheadrightarrow \mu_{p^v}$ we set $a_{v,\chi} := \chi\big(\underline{\log}_n^\dagger \circ \underline{\mathrm{tw}}_n(\underline{z})_v\big)$; in particular, if $v \geq 1$ then one calculates

$$a_{v,\chi} = \log_{\mathcal{O}[\Sigma'_{(v)}]} \left(\frac{\chi(z_v)}{N_{0,v}(z_0)} \times \frac{\varphi_{\Sigma'_{v-1}}\big(N_{0,v-1}(z_0)\big)}{\varphi_{\Sigma'_{v-1}}\big(\chi^p(z_{v-1})\big)} \right)$$

$$= \log_{\mathcal{O}[\Sigma'_{(v)}]}\left(\mathfrak{c}_{v,\chi}\right) \text{ say.}$$

Similarly, if $v = 0$ then $a_{0,\mathbf{1}} = \log_{\mathcal{O}[\Sigma_n]}(1) = 0$.

Remark 6.2.1. *(a) Substituting these $a_{v,\chi}$'s into the left-hand side of* (6.1m,$\underline{\mathfrak{h}}$)*, one finds*

$$\begin{aligned}
&\mathrm{Tr}_{\Sigma'_{(0)}/\Sigma'_{(m)}}\left(a_{0,\mathbf{1}}\right) + \sum_{v=1}^{m} \sum_{\mathcal{J}_\chi \in \mathcal{Z}_m^{(v)}} p^{v-1} \mathrm{Tr}_{\Sigma'_{(v)}/\Sigma'_{(m)}}\left(a_{v,\chi}\right) \times \left(p \ \mathrm{char}_{\mathcal{J}_\chi}(\underline{\mathfrak{h}}) - \mathrm{char}_{\mathcal{J}_\chi}(\underline{\mathfrak{h}}^p)\right) \\
&= \ 0 \ + \sum_{v=1}^{m} \sum_{\mathcal{J}_\chi \in \mathcal{Z}_m^{(v)}} p^{v-1} \log_{\mathcal{O}[\Sigma'_{(m)}]} \circ \mathrm{Nr}_{\Sigma'_{(v)}/\Sigma'_{(m)}}\left(\mathfrak{c}_{v,\chi}\right) \times \left(p \ \mathrm{char}_{\mathcal{J}_\chi}(\underline{\mathfrak{h}}) - \mathrm{char}_{\mathcal{J}_\chi}(\underline{\mathfrak{h}}^p)\right) \\
&= \ \log_{\mathcal{O}[\Sigma'_{(m)}]} \left(\prod_{v=1}^{m} \prod_{\mathcal{J}_\chi \in \mathcal{Z}_m^{(v)}} N_{v,m}\left(\mathfrak{c}_{v,\chi}\right)^{p^{v-1}(p \ \mathrm{char}_{\mathcal{J}_\chi}(\underline{\mathfrak{h}}) - \mathrm{char}_{\mathcal{J}_\chi}(\underline{\mathfrak{h}}^p))} \right)
\end{aligned}$$

is congruent to zero modulo $p^{m(d+1)-\nu_m(\underline{\mathfrak{h}})}$, if and only if

$$\prod_{v=1}^{m} \prod_{\mathcal{J}_\chi \in \mathcal{Z}_m^{(v)}} N_{v,m}\left(\mathfrak{c}_{v,\chi}\right)^{p^{v-1}(p \ \mathrm{char}_{\mathcal{J}_\chi}(\underline{\mathfrak{h}}) - \mathrm{char}_{\mathcal{J}_\chi}(\underline{\mathfrak{h}}^p))} \ \equiv \ 1 \mod p^{m(d+1)-\nu_m(\underline{\mathfrak{h}})}.$$

(b) Analogously, substituting the elements $a_{v,\chi}$ into (6.2m,id) *instead, we deduce that*

$$p\mathrm{Tr}_{\Sigma'_{(0)}/\Sigma'_{(m)}}\left(a_{0,\mathbf{1}}\right) + \sum_{v=1}^{m} \sum_{\mathcal{J}_\chi \in \mathcal{Z}_m^{(v)}} p^v(p-1) \ \mathrm{Tr}_{\Sigma'_{(v)}/\Sigma'_{(m)}}\left(a_{\mathcal{J}_\chi}^{(v)}\right) \equiv \ 0 \mod p^{m(d+1)}$$

if and only if $\prod_{v=1}^{m} \prod_{\mathcal{J}_\chi \in \mathcal{Z}_m^{(v)}} N_{v,m}\left(\mathfrak{c}_{v,\chi}\right)^{p^v} \equiv 1 \mod p^{m(d+1)}$.

(c) Lastly it is straightforward to check the p-adic congruences outlined above are equivalent to the congruences (1.1m,$\underline{\mathfrak{h}}$) *and* (1.2m,id) *in the Introduction to this thesis.*

It only remains therefore to pass from $K_1\left(\mathbb{Z}_p[G_n^{(d)}]\right)$ to the projective limit over n. The procedure is identical to that described in Sujatha's article in [8] (p23-50). Firstly, the identification $\mathbb{Z}_p\left[\left[G_\infty^{(d)}\right]\right] \cong \varprojlim_n \mathbb{Z}_p[G_n^{(d)}]$ extends to yield isomorphisms

$$K_1\left(\mathbb{Z}_p\left[\left[G_\infty^{(d)}\right]\right]\right) \cong \varprojlim_n K_1\left(\mathbb{Z}_p[G_n^{(d)}]\right) \ \text{ and } \ K_1'\left(\mathbb{Z}_p\left[\left[G_\infty^{(d)}\right]\right]\right) \cong \varprojlim_n K_1'\left(\mathbb{Z}_p[G_n^{(d)}]\right)$$

where K_1' denotes the quotient of K_1 by SK_1.

Applying Theorem 5.0.21, the diagram

$$\begin{array}{ccccc} K_1\big(\mathbb{Z}_p[G_n^{(d)}]\big) & \overset{\prod\theta_m}{\twoheadrightarrow} & \Omega_n^{(d)} & \overset{\prod\chi}{\hookrightarrow} & \prod_{v=0}^{n}\prod_{\mathcal{J}_\chi\in\mathcal{Z}_n^{(v)}}\mathbb{Z}_p[\Sigma_v]^\times \\ \big\downarrow{\scriptstyle \Gamma_{G_n^{(d)}}\circ(-)^\dagger} & & \big\downarrow{\scriptstyle \underline{\log}_n^\dagger\circ\underline{\mathrm{tw}}_n} & & \big\downarrow{\scriptstyle a_{v,\chi}\mapsto c_{v,\chi}} \\ \mathbb{Z}_p\big[\mathrm{Conj}(G_n^{(d)})\big] & \overset{\prod\theta_m^+}{\cong} & \Psi_n^{(d)} & \overset{\prod\chi}{\hookrightarrow} & \prod_{v=0}^{n}\prod_{\mathcal{J}_\chi\in\mathcal{Z}_n^{(v)}}\mathbb{Z}_p[\Sigma_v] \end{array}$$

commutes, and taking '$\varprojlim_n$' yields a Θ-mapping between $K_1\big(\mathbb{Z}_p[G_\infty^{(d)}]\big)$ and $\Omega_\infty^{(d)}$. Finally the kernel of this Θ-homomorphism is $SK_1\big(\mathbb{Z}_p[G_\infty^{(d)}]\big)$, which coincides with the abelian group $\mathbb{G}_m(\mathbb{Z}_p)_{\mathrm{tors}}\times\big(G_\infty^{(d)}\big)^{\mathrm{ab}} \cong \mu_{p-1}\times\Sigma_\infty$.

The proof of our main theorem is now complete.

7

An Application to Elliptic Curves

It turns out that our main algebraic result (Theorem 1.0.6) has some profound implications for the arithmetic of elliptic curves. In particular, it predicts that the Hasse-Weil L-values of each curve should satisfy strong p-adic congruences, arising from our description of $K_1\left(\mathbb{Z}_p[[G_\infty^{(d)}]]\right)$. From now on, we set $d = 2$. The initial task is to prove Theorem 1.0.6 and Proposition 1.0.7, so we first recall the situation of Chapter 1.

Let E denote a semistable elliptic curve over $\mathbb{Q}$ with good ordinary reduction at a prime $p > 2$. For a fixed number field F and an Artin representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \mathrm{GL}(V, \mathbb{C})$, its global ε-factor over F can be decomposed as an infinite product

$$\varepsilon_F(\rho, s) \;=\; \prod_{\text{all places } \nu} \varepsilon_{F_\nu}(\rho_\nu, \varpi_\nu, \mathrm{d}x_\nu; s).$$

Each local factor depends on a normalisation of additive characters ϖ_ν, and of Haar measures $\mathrm{d}x_\nu$. (In the special case $F = \mathbb{Q}$, one sets $\epsilon(\rho) = \epsilon_{\mathbb{Q}}(\rho, 0)$ and $\epsilon_p(\rho) = \epsilon_{\mathbb{Q}_p}(\rho_p, \varpi_p, \mathrm{d}x_p; 0)$.)

Recall the Artin L-function attached to ρ is given by an Euler product

$$L(\rho, s) \;=\; \prod_{\text{places } \nu} \det\Big(1 - \mathcal{N}_{F/\mathbb{Q}}(\nu)^{-s} \cdot \mathrm{Frob}_\nu^{-1} \Big| V_l(\rho)^{I_\nu}\Big) \quad \text{for } \mathrm{Re}(s) \gg 0$$

where Frob_ν is an arithmetic Frobenius element for ν, and I_ν is the inertia group. Likewise if $\mathrm{Re}(s) \gg 0$, the ρ-twisted Hasse-Weil L-function is given by the product

$$L(E, \rho, s) \;:=\; \prod_{\text{places } \nu} \det\left(1 - \mathcal{N}_{F/\mathbb{Q}}(\nu)^{-s} \cdot \mathrm{Frob}_\nu^{-1} \Big| \Big(H^1_{\text{ét}}(E_{\overline{\mathbb{Q}}}, \mathbb{Z}_l(1)) \otimes V_l(\rho)\Big)^{I_\nu}\right).$$

7.1 The Proof of Theorem 1.0.6

We begin by making the following three assertions:

(a) Each character $\chi : H_\infty^{(d)} \twoheadrightarrow \mu_{p^v}$ extends to a character on $\mathrm{Gal}\big(\mathbb{Q}_{\infty,\underline{\Delta}}^{(d)}/\mathbb{Q}(\mu_{p^v})\big)$, and the representation $\tau_\chi := \mathrm{Ind}_{\mathbb{Q}(\mu_{p^v})}^{\mathbb{Q}}(\chi)$ is irreducible of dimension $\phi(p^v)$;

(b) There exists a unique element $\mathbf{L}_{p,\chi}(E) \in \mathbb{Z}_p[\![U^{(v)}]\!][p^{-1}]$, which interpolates at each ψ-twist the p-adic number

$$\iota_p\left(\frac{L_{v\nmid \mathfrak{f}_{\tau_\chi}}(E,\psi\otimes\tau_\chi,1)}{(\Omega_E^+\Omega_E^-)^{[\mathbb{Q}(\mu_{p^v})^+:\mathbb{Q}]}}\cdot\epsilon_p(\psi\otimes\tau_\chi)\cdot\frac{L_p(\psi^{-1}\otimes\tau_\chi^*,u^{-1})}{L_p(\psi\otimes\tau_\chi,w^{-1})}\cdot u^{-\mathrm{ord}_p(\mathfrak{f}_{\psi\otimes\tau_\chi})}\right)$$

for every character $\psi : U^{(v)} \to \overline{\mathbb{Q}}^\times$ of finite order;

(c) For each rational prime l dividing $\underline{\Delta}$, there exists an $\Phi_l(E,\tau_\chi) \in \mathbb{Z}_p\big[U^{(v)}\big]$ satisfying $\psi\big(\Phi_l(E,\tau_\chi)\big) = \iota_p\big(\prod_{v|l} L_v(E,\psi\otimes\tau_\chi,1)\big)$ at all such ψ above.

Providing all three claims are correct, if $\mathcal{J} = \mathrm{Ker}(\chi)$ then defining

$$\mathbf{L}_p(E,\mathcal{J}) \;:=\; \mathbf{L}_{p,\chi}(E) \;\times \prod_{l|\underline{\Delta}} \Phi_l(E,\tau_\chi) \;\times \prod_{l|\mathfrak{f}_{\tau_\chi},\, l\neq p} \Phi_l(E,\tau_\chi)^{-1}$$

this element belongs to $\mathbb{Z}_p[\![U^{(v)}]\!][p^{-1}]$, and interpolates the required L-value data.

It therefore remains to prove these statements. Beginning with the first claim, the character χ extends to a character on $\mathrm{Stab}_{\Sigma_n}(\chi) \ltimes H_n^{(d)}$ by Theorem 3.1.3(ii), where n is any chosen integer $\geq v$. The latter group is precisely $\frac{1+p^v\mathbb{Z}}{1+p^n\mathbb{Z}} \ltimes H_\infty^{(d)}/p^n$ hence taking the projective limit over n, we naturally obtain a character on the group $(1+p^v\mathbb{Z}_p) \ltimes H_\infty^{(d)} \cong \mathrm{Gal}\big(\mathbb{Q}_{\infty,\underline{\Delta}}^{(d)}/\mathbb{Q}(\mu_{p^v})\big)$. Moreover, the induced representation down to $\mathbb{Q}$ has degree $[\mathbb{Q}(\mu_{p^v}) : \mathbb{Q}] = \phi(p^v)$, and is irreducible by Theorem 3.1.3(iii).

In order to establish (b), observe that χ yields a Hecke character over $\mathbb{Q}(\mu_{p^v})$; by the work of Serre, there is a corresponding parallel weight one Hilbert modular form $\mathbf{g}$ over $\mathbb{Q}(\mu_{p^v})^+$, whose complex L-function coincides with that attached to $\mathrm{Ind}_{\mathbb{Q}(\mu_{p^v})}^{\mathbb{Q}(\mu_{p^v})^+}(\chi)$. Associated to E is a classical cusp form $f_E \in \mathcal{S}_2\big(\Gamma_0(N_E)\big)$, and its base-change $\mathbf{f}$ to the totally real subfield $\mathbb{Q}(\mu_{p^v})^+$ has parallel weight two

and square-free conductor. The proof of Theorem 1.1 in [12] then yields a $\mathbb{C}_p$-valued bounded measure on $U^{(v)}$, interpolating the prescribed data in statement (b). However as the Hecke character χ is purely anticyclotomic, each Artin representation τ_χ is self-dual and $\mathbb{Q}$-rational, in which case the bounded measure takes values in $\mathbb{Q}_p(\psi)$.

Finally proving (c) is straightforward: at each place $\nu \mid \underline{\Delta}$ we form the polynomial

$$\mathrm{Pol}_\nu(x) \;:=\; \det\left(1 - x\cdot \mathrm{Frob}_\nu^{-1}\Big|\Big(H^1_{\text{ét}}\big(E_{\overline{\mathbb{Q}}},\mathbb{Z}_p(1)\big)\otimes V_p(\tau_\chi)\Big)^{I_\nu}\right)$$

which has rational integer coefficients; if $\gamma_\nu \in U^{(v)}$ corresponds to $\nu \in \mathrm{Spec}\,\mathbb{Z}[\mu_{p^v}]$ under the reciprocity map of class field theory, then the group ring element

$$\Phi_l(E,\tau_\chi) \;:=\; \prod_{\nu\mid l}\mathrm{Pol}_\nu(x)\Big|_{x=\gamma_\nu\cdot\mathcal{N}_{\mathbb{Q}(\mu_{p^v})/\mathbb{Q}}(\nu)^{-1}}$$

by construction interpolates the same values as in statement (c), so we are done.

7.2 The Proof of Proposition 1.0.7

Let us assume the elements $a_{v,\mathcal{J}} = \mathbf{L}_p(E,\mathcal{J})$ satisfy the non-abelian congruences. From Corollary 1.0.4 one deduces that:

(i) $\mathbf{L}_p\big(E,\mathrm{Ker}(\chi)\big)^p \equiv N_{0,1}\Big(\mathbf{L}_p\big(E,H^{(2)}_\infty\big)\Big)^p \mod p^2$, for every $\chi : H^{(2)}_\infty \twoheadrightarrow \mu_p$;

(ii) $\prod_{\mathcal{J},\,[H^{(2)}_\infty:\mathcal{J}]=p}\mathbf{L}_p\big(E,\mathcal{J}\big)^p \equiv N_{0,1}\Big(\mathbf{L}_p\big(E,H^{(2)}_\infty\big)\Big)^{p(p+1)} \mod p^3$.

Any character on $H^{(2)}_\infty$ is of the form $\chi^s_{\Delta_1}\chi^t_{\Delta_2}$ for appropriately chosen integers s and t. If we take as representatives $\mathcal{T} := \{\chi_{\Delta_1}\chi^t_{\Delta_2} \text{ with } 0\le t\le p-1\}\cup\{\chi_{\Delta_2}\}$, every subgroup $\mathcal{J}\in\mathcal{Z}^{(1)}_\infty$ of index p in $H^{(2)}_\infty$ arises as the kernel of χ for some $\chi\in\mathcal{T}$. Therefore it is sufficient to check (i) at characters in $\mathcal{T}$, i.e. to check that:

(i)′ $\mathbf{L}_p\big(E,\mathrm{Ker}(\chi_{\Delta_1}\chi^t_{\Delta_2})\big)^p \equiv N_{0,1}\Big(\mathbf{L}_p\big(E,H^{(2)}_\infty\big)\Big)^p \mod p^2$, with $0\le t\le p-1$;

(i)″ $\mathbf{L}_p\big(E,\mathrm{Ker}(\chi_{\Delta_2})\big)^p \equiv N_{0,1}\Big(\mathbf{L}_p\big(E,H^{(2)}_\infty\big)\Big)^p \mod p^2$.

Evaluating the above pair at the trivial character $\psi = \mathbf{1}$ and applying Theorem 1.0.6, one obtains the congruences (1.3) and (1.4) respectively.

Focusing now on condition (ii), the product over $\mathcal{J} \in \mathcal{Z}_\infty^{(1)}$ with $[H_\infty^{(2)} : \mathcal{J}] = p$ is identical to the product over $\mathcal{J} = \mathrm{Ker}(\chi)$ where χ ranges over elements from $\mathcal{T}$. In particular, we obtain the equivalent condition

(ii)' $\prod_{\chi \in \mathcal{T}} \mathbf{L}_p\big(E, \mathrm{Ker}(\chi)\big)^p \equiv N_{0,1}\Big(\mathbf{L}_p\big(E, H_\infty^{(2)}\big)\Big)^{p(p+1)} \bmod p^3$.

Lastly evaluating at $\psi = \mathbf{1}$ and applying Theorem 1.0.6 again, the final congruence (1.5) falls out immediately.

The proof of the proposition is complete.

7.3 A Worked Example

To illustrate the computational results, the numerical calculations for the elliptic curve $E = 19A3$, the prime $p = 5$ and $(\Delta_1, \Delta_2) = (2, 3)$ will be described. For these parameters, define $K := \mathbb{Q}(\mu_5)$ and $L := \mathbb{Q}\big(\mu_5, 2^{1/5}, 3^{1/5}\big)$, then we have the intermediate fields $\mathbb{Q}\big(\mu_5, (2 \times 3^t)^{1/5}\big)$ where $0 \leq t \leq p-1$, and $\mathbb{Q}\big(\mu_5, 3^{1/5}\big)$. We describe how the congruences (1.3)–(1.5) are checked for these parameters, and give the details of the computation involving the intermediate field $\mathbb{Q}\big(\mu_5, 3^{1/5}\big)$, since the computations are identical for the other intermediate fields.

The L-function of the elliptic curve, $L(E, s)$, will be twisted by:

- the self-dual Artin representation of $\mathrm{Gal}\big(\mathbb{Q}_{\infty,\underline{\Delta}}^{(d)}/\mathbb{Q}\big)$ (obtained by inducing a character χ_3 of exact order p of $\mathrm{Gal}\big(\mathbb{Q}\big(\mu_5, 3^{1/5}\big)/K\big)$ to $\mathrm{Gal}\big(\mathbb{Q}\big(\mu_5, 3^{1/5}\big)/\mathbb{Q}\big)$) will be denoted by ρ_{χ_3}, and its twist is $L(E, \rho_{\chi_3}, s)$;
- the regular representation $\oplus_{j=0}^{p-2}\omega^j$ of $\mathrm{Gal}(K/\mathbb{Q})$, with twist $L(E, \oplus_{j=0}^{p-2}\omega^j, s)$.

Note that p-adic numbers will be written in terms of their coefficients to an accuracy of order $O(p^9)$. In this example, we have $p = 5$, so in our calculations we work with a precision of 10 significant figures, since higher precision is not feasible computationally and lower precision may not be reliable.

Define $L^* := \left| \frac{L(E,\rho_{\chi_{\Delta_1^s\Delta_2^t}},1)\sqrt{\text{disc}_{\mathbb{Q}((\Delta_1^s\Delta_2^t)^{1/p})}}}{(2\Omega_E^+\Omega_E^-)^{(p-1)/2}} \right|$, where $\text{disc}_{\mathbb{Q}((\Delta_1^s\Delta_2^t)^{1/p})}$ is the discriminant of $\mathbb{Q}((\Delta_1^s\Delta_2^t)^{1/p})$. The calculation of L^* will now be described within the above setup. Using code written in MAGMA, $L(E,\rho_{\chi_3},1)$ is evaluated, and we calculate that

$$\sqrt{\text{disc}_{\mathbb{Q}(3^{1/5})}} \approx 503.115294937452,$$
$$\Omega_E^+ \approx 6.346046521, \text{ and } \Omega_E^- \approx 1.458816617i.$$

This leads us to compute

$$L^* = \left| \frac{L(E,\rho_{\chi_3},1)\sqrt{\text{disc}_{\mathbb{Q}(3^{1/5})}}}{(2\Omega_E^+\Omega_E^-)^{(5-1)/2}} \right| \approx 4.$$

Note that we do not expect L^* to be divisible by large primes for the varying $\Delta_1^s\Delta_2^t$'s in our computations; however, if large primes divide L^*, then L^* has not been identified correctly. Calculating L^* consumes 99% of the time for the computations, so tabulating L^* is handy if computations need to be repeated.

We now describe the calculation of $\mathcal{L}_{E,\underline{\Delta}}(\rho_{\chi_3})$. The Hecke polynomial of $E = 19A3$ at $p = 5$ has 5-adic roots $u = 140843 + O(5^8)$ = [3,3,3,1,0,0,4,1,0] (which is a 5-adic unit), and $w = 49957 \times 5 + O(5^9)$ = [0,2,1,3,4,4,0,3,4]. Then, because $\text{ord}_5(\mathfrak{f}_{\rho_{\chi_3}}) = 5$, we get $u^{-\text{ord}_5(\mathfrak{f}_{\rho_{\chi_3}})} = 116557 + O(5^8)$ = [2,1,2,2,1,2,2,1,0]. The primes dividing $p\Delta_1\Delta_2$ are 2, 3, and 5, which leads us to calculate the product of the local L-factors of $L(E,\rho_{\chi_3},s)$ at the primes 2, 3 and 5:

$$\prod_{\nu|p\Delta_1\Delta_2} P_\nu(E,\rho_{\chi_3},\nu^{-s}) = P_2(E,\rho_{\chi_3},2^{-1})P_3(E,\rho_{\chi_3},3^{-1})P_5(E,\rho_{\chi_3},5^{-1}) = \frac{9}{16}.$$

Using the Dokchitsers' equations (Section 6.10, [17]) for the local epsilon factors, the epsilon factor of ρ_{χ_3} at $p = 5$ is calculated, namely $\epsilon_5(\rho) \approx -55.90169944 - i2.035974660E-8$. As a result, we get $\epsilon_5(\rho)/\sqrt{\text{disc}_{\mathbb{Q}(3^{1/5})}} \approx \frac{-1}{9}$. It turns out that $L_5(\rho_{\chi_3},T) = 1$, thus $\frac{L_5(\rho_{\chi_3}^*,u^{-1})}{L_5(\rho_{\chi_3},w^{-1})} = 1$.

Compiling the above information, one calculates

$$\begin{aligned}\mathcal{L}_{E,\underline{\Delta}}(\rho_{\chi_3}) &= L^*\frac{(-2i)^{(5-1)/2}}{u^{\mathrm{ord}_5(\mathfrak{f}_{\rho_{\chi_3}})}}\prod_{\nu=2,3,5}P_\nu(E,\rho_{\chi_3},\nu^{-1})\frac{\epsilon_5(\rho_{\chi_3})}{\sqrt{\mathrm{disc}_{\mathbb{Q}(3^{1/5})}}}\frac{L_5(\rho^*_{\chi_3},u^{-1})}{L_5(\rho_{\chi_3},w^{-1})}\\ &\approx 4\times(-4)\frac{9}{16}\Big(\frac{-1}{9}\Big)u^{-\mathrm{ord}_5(\mathfrak{f}_{\rho_{\chi_3}})}\\ &\approx 116557+O(5^8)=[2,1,2,2,1,2,2,1,0].\end{aligned}$$

Let us now compute $\mathcal{L}_{E,\underline{\Delta}}\left(\oplus_{j=0}^{p-2}\omega^j\right)$ in this situation. Using $L(E,\oplus_{j=0}^{5-2}\omega^j,s)=\prod_{j=0}^{5-2}L(E,\omega^j,s)$, we evaluate $L(E,\oplus_{j=0}^{3}\omega^j,1)\approx 2.816811133-i1.195712318E-11$. With in-built functions in MAGMA, the discriminant of K is calculated to be 125. One defines $L^*(E,\oplus_{j=0}^{p-2}\omega^j)$ via the formula

$$L^*(E,\oplus_{j=0}^{p-2}\omega^j):=\left|\frac{L(E,\oplus_{j=0}^{p-2}\omega^j,1)\sqrt{\mathrm{disc}_K}}{(2\Omega_E^+\Omega_E^-)^{\frac{(p-1)}{2}}}\right|,$$

in which case MAGMA works out

$$L^*(E,\oplus_{j=0}^{3}\omega^j)\approx 0.1111111111-i4.716571961E-13\approx\frac{1}{9}.$$

Note that $L^*(E,\oplus_{j=0}^{p-2}\omega^j)$ does not change with respect to $\Delta_1^s\Delta_2^t$'s, but L^* does. Since $L^*(E,\oplus_{j=0}^{p-2}\omega^j)$ is not computationally expensive to compute, $L^*(E,\oplus_{j=0}^{p-2}\omega^j)$ is not recorded in the tables.

The local epsilon factor $\epsilon_p(\oplus_{j=0}^{p-2}\omega^j)$ is computed via the equation $\epsilon_p(\oplus_{j=0}^{p-2}\omega^j)=\prod_{j=0}^{p-2}\epsilon_p(\omega^j)$, and $\epsilon_p(\omega^j)$ for $0\le j\le p-2$ is calculated from the formula the Dokchitsers provide (Section 6.10 [17]). As a result,

$$\epsilon_5(\oplus_{j=0}^{3}\omega^j)\approx -11.18033989-i3.294446094E-9,$$

and $\frac{\epsilon_5(\oplus_{j=0}^{3}\omega^j)}{\sqrt{\mathrm{disc}_K}}\approx -1$. The primes dividing $p\Delta_1\Delta_2$ are $2,3,$ and 5, which leads us to calculate that

$$\prod_{\nu=2,3,5}P_\nu(E,\oplus_{j=0}^{p-2}\omega^j,\nu^{-1})\approx 0.4000000000\approx\frac{2}{5}.$$

In this example, $\mathrm{ord}_p(\mathfrak{f}_{\oplus_{j=0}^{p-2}\omega^j}) = \mathrm{ord}_5(\mathfrak{f}_{\oplus_{j=0}^{3}\omega^j}) = 3$, so $u^{-\mathrm{ord}_5(\mathfrak{f}_{\oplus_{j=0}^{3}\omega^j})} = 82993 + O(5^8) = [3,3,4,3,2,1,0,1,0]$. Using MAGMA, the local L-factor for $\oplus_{j=0}^{p-2}\omega^j$ at p, $L_p(\oplus_{j=0}^{p-2}\omega^j, T)$, is found to be $1 - T$. Thus

$$\frac{L_5(\oplus_{j=0}^{3}(\omega^*)^j, u^{-1})}{L_5(\oplus_{j=0}^{3}\omega^j, w^{-1})} \approx -7688 \times 5 + O(5^9) = [0,2,2,2,3,2,2,4,4].$$

Putting all of this together, we obtain

$$\begin{aligned}\mathcal{L}_{E,\underline{\Delta}}(\oplus_{j=0}^{3}\omega^j) = L^*(E, \oplus_{j=0}^{3}\omega^j) \prod_{\nu=2,3,5} P_\nu(E,\sigma,\nu^{-1}) \frac{2^2}{u^3} \frac{\epsilon_5(\oplus_{j=0}^{3}\omega^j)}{\sqrt{\mathrm{disc}_K}} \\ \times \frac{L_5(\oplus_{j=0}^{3}(\omega^*)^j, u^{-1})}{L_5(\oplus_{j=0}^{3}\omega^j, w^{-1})} \\ \approx \left(\frac{1}{9}\right)\left(\frac{2}{5}\right)\frac{2^2}{u^3}(-1)\frac{L_5(\oplus_{j=0}^{3}(\omega^*)^j, u^{-1})}{L_5(\oplus_{j=0}^{3}\omega^j, w^{-1})} \\ \approx -185233 + O(5^8) = [2,3,0,3,3,0,3,2,4].\end{aligned}$$

Now, taking the quotient $\frac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{\chi_3})}{\mathcal{L}_{E,\underline{\Delta}}(\oplus_{j=0}^{3}\omega^j)}$, yields the approximation $-170004 + O(5^8)$ = [1,4,4,4,2,0,4,2,4], which clearly is an element of $1 + 5\mathbb{Z}_5$, and thus verifies congruence (1.4).

The computations are identical for the other $\Delta_1^s\Delta_2^t$'s and they verify congruence (1.3), which can be seen in Table 7.4.3 of Section 7.4. Here one finds that for $E = 19A3$, $p = 5$, and $(\Delta_1, \Delta_2) = (2,3)$,

$$\left(\prod_{\Delta_1^s\Delta_2^t} \frac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{\Delta_1^s\Delta_2^t})}{\mathcal{L}_{E,\underline{\Delta}}(\oplus_{j=0}^{3}\omega^j)}\right)^5 \approx 183376 + O(5^8) = [1,0,0,2,3,3,1,2,0],$$

which verifies the congruence (1.5).

7.4 Numerical Results for $d = 2$ and $n = 1$

Our aim now is to numerically verify the congruences (1.3)–(1.5) in Proposition 1.0.7. Due to computational limitations, the congruences are only checked at the primes $p = 3$, and 5.

Take Δ_1 and Δ_2 to be p-power free integers, which are both co-prime to p. The elliptic curves are labelled according to Cremona's tables [9]. Let $K := \mathbb{Q}(\mu_p)$ and $L := \mathbb{Q}\big(\mu_p, \Delta_1^{1/p}, \Delta_2^{1/p}\big)$, then we have the intermediate field extensions $\mathbb{Q}\big(\mu_p, (\Delta_1 \times \Delta_2^t)^{1/p}\big)$ where $0 \leq t \leq p-1$, and $\mathbb{Q}\big(\mu_p, \Delta_2^{1/p}\big)$. The L-function of the elliptic curve, $L(E,s)$, will be twisted by the self-dual irreducible Artin representation $\rho_{\chi_{\Delta_1^s\Delta_2^t}}$ on $\mathrm{Gal}(\mathbb{Q}(\mu_p, \Delta_1^s\Delta_2^t))$ of dimension $p-1$, and by the regular representation $\oplus_{j=0}^{p-2}\omega^j$ of $\mathrm{Gal}(K/\mathbb{Q})$.

We have tabulated the following L-value information in Tables 7.4.1–7.4.4:

- $\Delta_1^s\Delta_2^t$: specifies the intermediate field $K((\Delta_1^s\Delta_2^t)^{1/p})$.
- $L^* := L^*\big(E, \rho_{\chi_{\Delta_1}^s\chi_{\Delta_2}^t}\big) := \left|\dfrac{L(E,\rho_{\chi_{\Delta_1^s\Delta_2^t}},1)\sqrt{\mathrm{disc}_{\mathbb{Q}((\Delta_1^s\Delta_2^t)^{1/p})}}}{(2\Omega_E^+\Omega_E^-)^{\frac{(p-1)}{2}}}\right|$, where $\mathrm{disc}_{\mathbb{Q}((\Delta_1^s\Delta_2^t)^{1/p})}$ is the discriminant of $\mathbb{Q}((\Delta_1^s\Delta_2^t)^{1/p})$.
- $\mathcal{L}_{E,\underline{\Delta}}(\rho_{\chi_{\Delta_1^s\Delta_2^t}}) = \dfrac{L_{\nu\nmid p\underline{\Delta}}(E,\rho_{\chi_{\Delta_1^s\Delta_2^t}},1)}{(\Omega_E^+\Omega_E^-)^{\frac{p-1}{2}}}\dfrac{L_p(\rho^*_{\chi_{\Delta_1^s\Delta_2^t}},u^{-1})}{L_p(\rho_{\chi_{\Delta_1^s\Delta_2^t}},w^{-1})}\epsilon_p(\rho_{\chi_{\Delta_1^s\Delta_2^t}})\ u^{-\mathrm{ord}_p\left(\mathfrak{f}_{\rho\chi_{\Delta_1^s\Delta_2^t}}\right)}$.
- $\mathcal{L}_{E,\underline{\Delta}}(\oplus_{j=0}^{p-2}\omega^j) = \dfrac{L_{\nu\nmid p\underline{\Delta}}(E,\oplus_{j=0}^{p-2}\omega^j,1)}{(\Omega_E^+\Omega_E^-)^{\frac{p-1}{2}}}\dfrac{L_p(\oplus_{j=0}^{p-2}(\omega^*)^j,u^{-1})}{L_p(\oplus_{j=0}^{p-2}\omega^j,w^{-1})}\epsilon_p(\oplus_{j=0}^{p-2}\omega^j)\ u^{-\mathrm{ord}_p\left(\mathfrak{f}_{\oplus_{j=0}^{p-2}\omega^j}\right)}$.
- $\dfrac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{\chi_{\Delta_1^s\Delta_2^t}})}{\mathcal{L}_{E,\underline{\Delta}}(\oplus_{j=0}^{p-2}\omega^j)}$.
- $\left(\prod_{s,t}\dfrac{\mathcal{L}_{E,\underline{\Delta}}\left(\rho_{\chi_{\Delta_1^s}\chi_{\Delta_2^t}}\right)}{\mathcal{L}_{E,\underline{\Delta}}\left(\oplus_{j=0}^{p-2}\omega^j\right)}\right)^p := \dfrac{\left(\mathcal{L}_{E,\underline{\Delta}}\left(\rho_{\chi_{\Delta_2}}\right)\times\prod_{t=0}^{p-1}\mathcal{L}_{E,\underline{\Delta}}\left(\rho_{\chi_{\Delta_1}\chi_{\Delta_2^t}}\right)\right)^p}{\mathcal{L}_{E,\underline{\Delta}}\left(\oplus_{j=0}^{p-2}\omega^j\right)^{p(p+1)}}$.

The second quantity L^* is a rational number (in fact, it turns out to be an integer in every case considered here), while the next four quantities are p-adic numbers whose coefficients have been expressed below to an accuracy of order $O(p^9)$.

Remark 7.4.1. *In particular, congruences* (1.3) *and* (1.4) *hold at each pair* (s,t) *provided that*

$$\frac{\mathcal{L}_{E,\underline{\Delta}}\left(\rho_{\chi_{\Delta_1^s}\chi_{\Delta_2^t}}\right)}{\mathcal{L}_{E,\underline{\Delta}}\left(\oplus_{j=0}^{p-2}\omega^j\right)} \;=\; [1,\ \ldots\,] \;\in\; 1+p\mathbb{Z}_p,$$

whilst congruence (1.5) *is true if and only if*

$$\left(\prod_{s,t}\frac{\mathcal{L}_{E,\underline{\Delta}}\left(\rho_{\chi_{\Delta_1^s}\chi_{\Delta_2^t}}\right)}{\mathcal{L}_{E,\underline{\Delta}}\left(\oplus_{j=0}^{p-2}\omega^j\right)}\right)^p \;=\; [1,0,0,\,\ldots] \;\in\; 1+p^3\mathbb{Z}_p.$$

The data below confirm that these hold for all examples calculated in this thesis. When $p = 5$, as was noted earlier, the computations were done with the precision set at 10 significant figures, but when $p = 3$, the computations were done at higher precision because this was not computationally expensive.

It must also be pointed out that due to the Dokchitsers recording the L^* value in [17] (Appendix B Tables) we benefited, because we did not have to recompute this quantity for many of the computations involving the prime 5.

Table 7.4.1: $p = 3$, $E = 11A3$ with equation $y^2 + y = x^3 - x^2$.

$\Delta_1^s\Delta_2^t$	L^*	$\mathcal{L}_{E,\underline{\Delta}}\left(\rho_{\chi_{\Delta_1^s}\chi_{\Delta_2^t}}\right)$	$\mathcal{L}_{E,\underline{\Delta}}\left(\oplus_{j=0}^{p-2}\omega^j\right)$	$\frac{\mathcal{L}_{E,\underline{\Delta}}\left(\rho_{\chi_{\Delta_1^s}\chi_{\Delta_2^t}}\right)}{\mathcal{L}_{E,\underline{\Delta}}\left(\oplus_{j=0}^{p-2}\omega^j\right)}$
2	1	[2,1,1,2,0,1,0,0,0]	[2,1,0,0,2,1,0,0,0]	[1,0,2,1,1,0,2,0,0]
10	1	[2,0,1,2,0,0,2,1,2]	[2,1,0,0,2,1,0,0,0]	[1,1,1,0,2,1,2,2,2]
20	1	[2,0,0,2,2,1,2,0,0]	[2,1,0,0,2,1,0,0,0]	[1,1,2,2,1,2,2,0,0]
5	4	[2,0,2,2,2,0,2,2,2]	[2,1,0,0,2,1,0,0,0]	[1,1,0,1,1,2,1,0,0]
		$\left(\prod_{s,t}\frac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{s,t})}{\mathcal{L}_{E,\underline{\Delta}}(\oplus\omega^j)}\right)^p = [1,0,0,0,2,1,1,2,2]$		
2	1	[1,0,2,2,1,2,2,2,2]	[1,2,2,0,1,1,0,0,0]	[1,1,0,2,1,1,0,2,2]
14	1	[1,1,1,1,1,0,0,1,0]	[1,2,2,0,1,1,0,0,0]	[1,2,0,1,2,1,0,0,0]
28	1	[1,1,0,2,2,1,0,1,0]	[1,2,2,0,1,1,0,0,0]	[1,2,2,0,0,2,2,2,2]
7	1	[1,0,2,0,2,2,1,2,2]	[1,2,2,0,1,1,0,0,0]	[1,1,0,0,0,0,0,2,2]
		$\left(\prod_{s,t}\frac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{s,t})}{\mathcal{L}_{E,\underline{\Delta}}(\oplus\omega^j)}\right)^p = [1,0,0,2,1,2,2,1,1]$		

Table 7.4.1: $p = 3$, $E = 11A3$ with equation $y^2 + y = x^3 - x^2$.

$\Delta_1^s\Delta_2^t$	L^*	$\mathcal{L}_{E,\underline{\Delta}}\left(\rho_{\chi_{\Delta_1^s}\chi_{\Delta_2^t}}\right)$	$\mathcal{L}_{E,\underline{\Delta}}\left(\oplus_{j=0}^{p-2}\omega^j\right)$	$\frac{\mathcal{L}_{E,\underline{\Delta}}\left(\rho_{\chi_{\Delta_1^s}\chi_{\Delta_2^t}}\right)}{\mathcal{L}_{E,\underline{\Delta}}\left(\oplus_{j=0}^{p-2}\omega^j\right)}$
2	1	[1,2,0,0,1,2,1,1,2]	[1,1,1,0,1,2,0,2,2]	[1,1,1,0,1,0,2,2,2]
26	4	[1,0,2,0,1,0,1,2,2]	[1,1,1,0,1,2,0,2,2]	[1,2,1,2,1,0,1,1,0]
52	16	[1,1,0,2,2,2,0,0,0]	[1,1,1,0,1,2,0,2,2]	[1,0,2,2,2,0,0,2,2]
13	1	[1,1,0,0,0,1,0,2,2]	[1,1,1,0,1,2,0,2,2]	[1,0,2,0,2,1,2,2,2]
		$\left(\prod_{s,t}\frac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{s,t})}{\mathcal{L}_{E,\underline{\Delta}}(\oplus\omega^j)}\right)^p = [1,0,0,0,1,0,1,1,2]$		
2	1	[2,1,0,1,1,0,0,0,0]	[2,1,2,1,1,1,0,2,2]	[1,0,2,1,1,0,2,0,0]
34	25	[2,0,0,0,0,0,1,1,0]	[2,1,2,1,1,1,0,2,2]	[1,1,1,0,0,2,0,2,2]
68	16	[2,0,1,0,0,2,2,2,2]	[2,1,2,1,1,1,0,2,2]	[1,1,0,1,2,1,2,2,2]
17	1	[2,0,2,2,1,0,0,1,0]	[2,1,2,1,1,1,0,2,2]	[1,1,2,2,1,1,1,2,2]
		$\left(\prod_{s,t}\frac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{s,t})}{\mathcal{L}_{E,\underline{\Delta}}(\oplus\omega^j)}\right)^p = [1,0,0,0,2,0,1,2,2]$		
2	1	[1,0,2,0,1,0,1,0,0]	[1,1,0,2,1,0,1,2,2]	[1,2,2,1,2,1,0,0,0]
38	49	[1,1,1,1,2,2,0,2,2]	[1,1,0,2,1,0,1,2,2]	[1,0,1,1,2,0,1,1,0]
76	4	[1,1,2,2,0,2,2,0,0]	[1,1,0,2,1,0,1,2,2]	[1,0,2,1,0,0,2,2,2]
19	1	[1,2,2,2,2,1,0,2,2]	[1,1,0,2,1,0,1,2,2]	[1,1,1,2,2,0,1,1,0]
		$\left(\prod_{s,t}\frac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{s,t})}{\mathcal{L}_{E,\underline{\Delta}}(\oplus\omega^j)}\right)^p = [1,0,0,0,0,1,0,1,2]$		
2	1	[2,1,0,0,1,2,1,0,0]	[2,1,2,0,1,2,0,2,2]	[1,0,2,1,1,0,2,0,0]
46	4	[2,2,2,1,2,0,1,0,0]	[2,1,2,0,1,2,0,2,2]	[1,2,0,1,2,1,0,0,0]
92	4	[2,2,1,0,2,0,1,1,0]	[2,1,2,0,1,2,0,2,2]	[1,2,1,1,2,2,0,1,0]
23	16	[2,2,0,0,1,1,0,2,2]	[2,1,2,0,1,2,0,2,2]	[1,2,2,0,1,1,0,1,0]
		$\left(\prod_{s,t}\frac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{s,t})}{\mathcal{L}_{E,\underline{\Delta}}(\oplus\omega^j)}\right)^p = [1,0,0,1,2,0,2,0,1]$		

Table 7.4.1: $p = 3$, $E = 11A3$ with equation $y^2 + y = x^3 - x^2$.

$\Delta_1^s\Delta_2^t$	L^*	$\mathcal{L}_{E,\underline{\Delta}}\left(\rho_{\chi_{\Delta_1^s}\chi_{\Delta_2^t}}\right)$	$\mathcal{L}_{E,\underline{\Delta}}\left(\oplus_{j=0}^{p-2}\omega^j\right)$	$\frac{\mathcal{L}_{E,\underline{\Delta}}\left(\rho_{\chi_{\Delta_1^s}\chi_{\Delta_2^t}}\right)}{\mathcal{L}_{E,\underline{\Delta}}\left(\oplus_{j=0}^{p-2}\omega^j\right)}$
2	1	[1,2,1,2,2,1,1,2,2]	[1,2,2,2,2,2,2,0,0]	[1,0,2,1,1,0,2,0,0]
62	1	[1,2,0,1,0,0,0,2,2]	[1,2,2,2,2,2,2,0,0]	[1,0,1,2,2,2,2,0,0]
124	4	[1,0,1,0,2,1,2,0,0]	[1,2,2,2,2,2,2,0,0]	[1,1,2,2,1,0,0,0,0]
31	1	[1,1,1,2,2,2,1,1,2]	[1,2,2,2,2,2,2,0,0]	[1,2,0,0,0,0,2,2,2]
		$\left(\prod_{s,t}\frac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{s,t})}{\mathcal{L}_{E,\underline{\Delta}}(\oplus\omega^j)}\right)^p = [1,0,0,2,2,2,2,2,2]$		
2	1	[1,2,1,2,2,0,2,2,2]	[1,0,1,0,0,1,2,2,2]	[1,2,0,0,2,2,1,1,2]
74	1	[1,0,0,0,1,0,0,0,0]	[1,0,1,0,0,1,2,2,2]	[1,0,2,2,1,2,1,1,2]
148	4	[1,1,0,0,1,1,0,0,0]	[1,0,1,0,0,1,2,2,2]	[1,1,2,1,1,1,1,0,0]
37	4	[1,0,0,2,0,2,2,0,0]	[1,0,1,0,0,1,2,2,2]	[1,0,2,1,1,2,1,2,2]
		$\left(\prod_{s,t}\frac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{s,t})}{\mathcal{L}_{E,\underline{\Delta}}(\oplus\omega^j)}\right)^p = [1,0,0,0,2,1,0,0,0]$		
2	1	[2,1,1,0,2,1,1,0,0]	[2,1,0,1,0,0,1,1,0]	[1,0,2,1,1,0,2,0,0]
82	1	[2,0,0,0,0,2,2,1,2]	[2,1,0,1,0,0,1,1,0]	[1,1,2,2,0,2,2,0,0]
164	1	[2,0,2,2,0,0,0,0,0]	[2,1,0,1,0,0,1,1,0]	[1,1,0,2,1,0,1,0,0]
41	4	[2,0,1,0,0,0,1,0,0]	[2,1,0,1,0,0,1,1,0]	[1,1,1,0,2,2,2,0,0]
		$\left(\prod_{s,t}\frac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{s,t})}{\mathcal{L}_{E,\underline{\Delta}}(\oplus\omega^j)}\right)^p = [1,0,0,0,0,0,2,0,0]$		
5	4	[1,2,2,1,0,1,0,1,0]	[1,0,0,1,1,2,2,2,2]	[1,2,2,0,0,0,2,2,2]
35	1	[1,2,0,0,1,1,1,0,0]	[1,0,0,1,1,2,2,2,2]	[1,2,0,2,0,2,0,1,0]
175	16	[1,1,1,0,1,1,0,0,0]	[1,0,0,1,1,2,2,2,2]	[1,1,1,2,1,2,0,0,0]
7	1	[1,1,0,1,2,0,2,1,2]	[1,0,0,1,1,2,2,2,2]	[1,1,0,0,0,0,0,2,2]
		$\left(\prod_{s,t}\frac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{s,t})}{\mathcal{L}_{E,\underline{\Delta}}(\oplus\omega^j)}\right)^p = [1,0,0,0,2,0,2,0,2]$		

Table 7.4.1: $p = 3$, $E = 11A3$ with equation $y^2 + y = x^3 - x^2$.

$\Delta_1^s\Delta_2^t$	L^*	$\mathcal{L}_{E,\underline{\Delta}}(\rho_{\chi_{\Delta_1^s}\chi_{\Delta_2^t}})$	$\mathcal{L}_{E,\underline{\Delta}}(\oplus_{j=0}^{p-2}\omega^j)$	$\frac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{\chi_{\Delta_1^s}\chi_{\Delta_2^t}})}{\mathcal{L}_{E,\underline{\Delta}}(\oplus_{j=0}^{p-2}\omega^j)}$
5	4	[1,0,0,0,0,2,1,2,2]	[1,2,0,1,1,1,1,0,0]	[1,1,0,1,1,2,1,0,0]
65	49	[1,1,1,2,1,1,2,0,0]	[1,2,0,1,1,1,1,0,0]	[1,2,2,1,0,0,0,2,2]
325	25	[1,2,0,0,0,1,1,1,0]	[1,2,0,1,1,1,1,0,0]	[1,0,0,2,0,1,1,1,0]
13	1	[1,2,2,2,1,0,1,1,0]	[1,2,0,1,1,1,1,0,0]	[1,0,2,0,2,1,2,2,2]
		$\left(\prod_{s,t}\frac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{s,t})}{\mathcal{L}_{E,\underline{\Delta}}(\oplus\omega^j)}\right)^p = [1,0,0,1,2,1,2,0,0]$		
5	4	[2,2,0,1,0,0,2,0,0]	[2,0,0,2,1,2,2,1,2]	[1,1,0,1,1,2,1,0,0]
85	4	[2,0,2,2,0,2,1,0,0]	[2,0,0,2,1,2,2,1,2]	[1,0,1,0,1,0,0,0,0]
425	16	[2,2,2,1,0,0,1,2,2]	[2,0,0,2,1,2,2,1,2]	[1,1,1,1,1,1,0,0,0]
17	1	[2,2,1,1,1,2,0,2,2]	[2,0,0,2,1,2,2,1,2]	[1,1,2,2,1,1,1,2,2]
		$\left(\prod_{s,t}\frac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{s,t})}{\mathcal{L}_{E,\underline{\Delta}}(\oplus\omega^j)}\right)^p = [1,0,0,2,1,2,2,2,2]$		
5	4	[1,2,2,2,1,0,1,2,2]	[1,2,2,1,2,0,2,0,0]	[1,0,0,1,0,0,0,2,2]
95	16	[1,0,2,2,0,1,1,1,0]	[1,2,2,1,2,0,2,0,0]	[1,1,0,1,0,1,0,2,2]
475	25	[1,0,0,1,2,2,0,2,2]	[1,2,2,1,2,0,2,0,0]	[1,1,1,0,1,1,2,1,2]
19	1	[1,0,0,0,2,0,1,1,0]	[1,2,2,1,2,0,2,0,0]	[1,1,1,2,2,0,1,1,0]
		$\left(\prod_{s,t}\frac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{s,t})}{\mathcal{L}_{E,\underline{\Delta}}(\oplus\omega^j)}\right)^p = [1,0,0,0,2,0,0,1,0]$		
5	4	[2,2,0,0,1,1,0,2,2]	[2,0,0,1,0,2,2,2,2]	[1,1,0,1,1,2,1,0,0]
115	49	[2,1,0,2,2,0,1,2,2]	[2,0,0,1,0,2,2,2,2]	[1,2,1,0,0,0,0,2,2]
575	1	[2,2,0,2,1,1,2,1,2]	[2,0,0,1,0,2,2,2,2]	[1,1,0,2,1,2,0,0,0]
23	16	[2,1,2,2,1,1,2,0,0]	[2,0,0,1,0,2,2,2,2]	[1,2,2,0,1,1,0,1,0]
		$\left(\prod_{s,t}\frac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{s,t})}{\mathcal{L}_{E,\underline{\Delta}}(\oplus\omega^j)}\right)^p = [1,0,0,0,0,2,0,2,2]$		

Table 7.4.1: $p = 3$, $E = 11A3$ with equation $y^2 + y = x^3 - x^2$.

$\Delta_1^s\Delta_2^t$	L^*	$\mathcal{L}_{E,\underline{\Delta}}\left(\rho_{\chi_{\Delta_1^s}\chi_{\Delta_2^t}}\right)$	$\mathcal{L}_{E,\underline{\Delta}}\left(\oplus_{j=0}^{p-2}\omega^j\right)$	$\frac{\mathcal{L}_{E,\underline{\Delta}}\left(\rho_{\chi_{\Delta_1^s}\chi_{\Delta_2^t}}\right)}{\mathcal{L}_{E,\underline{\Delta}}\left(\oplus_{j=0}^{p-2}\omega^j\right)}$
7	1	[2,0,0,0,2,0,2,1,2]	[2,2,0,0,1,2,1,2,2]	[1,2,0,2,2,2,0,0,0]
91	1	[2,0,1,2,1,2,2,2,2]	[2,2,0,0,1,2,1,2,2]	[1,2,2,2,1,1,1,2,2]
637	64	[2,0,2,0,2,0,0,2,2]	[2,2,0,0,1,2,1,2,2]	[1,2,1,1,0,2,1,0,0]
13	1	[2,2,1,2,0,1,0,0,0]	[2,2,0,0,1,2,1,2,2]	[1,0,2,0,2,1,2,2,2]
		$\left(\prod_{s,t}\frac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{s,t})}{\mathcal{L}_{E,\underline{\Delta}}(\oplus\omega^j)}\right)^p = [1,0,0,1,1,0,1,0,0]$		
7	1	[1,1,1,2,0,2,1,2,2]	[1,0,1,1,2,2,1,1,2]	[1,1,0,0,0,0,0,2,2]
119	16	[1,2,0,2,1,0,1,0,0]	[1,0,1,1,2,2,1,1,2]	[1,2,2,1,0,1,2,0,0]
833	4	[1,1,2,2,1,1,2,0,0]	[1,0,1,1,2,2,1,1,2]	[1,1,1,0,0,1,1,2,2]
17	1	[1,2,2,1,1,1,1,0,0]	[1,0,1,1,2,2,1,1,2]	[1,2,1,1,1,0,1,0,0]
		$\left(\prod_{s,t}\frac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{s,t})}{\mathcal{L}_{E,\underline{\Delta}}(\oplus\omega^j)}\right)^p = [1,0,0,1,1,0,2,2,2]$		

Table 7.4.2: $p = 3$, $E = 77C1$ with equation $y^2 + xy = x^3 + x^2 + 4x + 11$.

$\Delta_1^s\Delta_2^t$	L^*	$\mathcal{L}_{E,\underline{\Delta}}\left(\rho_{\chi_{\Delta_1^s}\chi_{\Delta_2^t}}\right)$	$\mathcal{L}_{E,\underline{\Delta}}\left(\oplus_{j=0}^{p-2}\omega^j\right)$	$\frac{\mathcal{L}_{E,\underline{\Delta}}\left(\rho_{\chi_{\Delta_1^s}\chi_{\Delta_2^t}}\right)}{\mathcal{L}_{E,\underline{\Delta}}\left(\oplus_{j=0}^{p-2}\omega^j\right)}$
2	8	[1,2,2,1,0,1,1,0,0]	[1,0,0,2,2,0,2,0,0]	[1,2,2,2,2,2,2,1,2]
10	2	[1,0,0,0,2,2,2,1,2]	[1,0,0,2,2,0,2,0,0]	[1,0,0,1,2,1,1,0,0]
20	2	[1,1,1,1,0,0,0,0,0]	[1,0,0,2,2,0,2,0,0]	[1,1,1,2,1,0,2,0,0]
5	8	[1,0,2,2,1,2,0,0,0]	[1,0,0,2,2,0,2,0,0]	[1,0,2,0,2,0,2,2,2]
		$\left(\prod_{s,t}\frac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{s,t})}{\mathcal{L}_{E,\underline{\Delta}}(\oplus\omega^j)}\right)^p = [1,0,0,2,2,1,1,1,2]$		

Table 7.4.2: $p = 3$, $E = 77C1$ with equation $y^2 + xy = x^3 + x^2 + 4x + 11$.

$\Delta_1^s\Delta_2^t$	L^*	$\mathcal{L}_{E,\underline{\Delta}}(\rho_{\chi_{\Delta_1^s}\chi_{\Delta_2^t}})$	$\mathcal{L}_{E,\underline{\Delta}}(\oplus_{j=0}^{p-2}\omega^j)$	$\frac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{\chi_{\Delta_1^s}\chi_{\Delta_2^t}})}{\mathcal{L}_{E,\underline{\Delta}}(\oplus_{j=0}^{p-2}\omega^j)}$
2	8	[2,0,2,0,0,2,2,1,2]	[2,0,0,0,0,2,0,0,0]	[1,0,1,0,0,0,1,1,0]
26	2	[2,2,1,1,0,2,2,1,2]	[2,0,0,0,0,2,0,0,0]	[1,1,2,0,0,0,0,0,0]
52	2	[2,1,0,2,2,1,1,2,2]	[2,0,0,0,0,2,0,0,0]	[1,2,1,2,2,2,2,0,0]
13	2	[2,0,2,2,1,1,0,1,0]	[2,0,0,0,0,2,0,0,0]	[1,0,1,1,2,2,2,0,0]
		$\left(\prod_{s,t}\frac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{s,t})}{\mathcal{L}_{E,\underline{\Delta}}(\oplus\omega^j)}\right)^p = [1,0,0,2,1,1,1,2,2]$		
5	8	[2,0,2,1,0,0,0,2,2]	[2,0,1,0,0,1,2,2,2]	[1,0,2,0,2,0,2,2,2]
65	98	[2,2,1,2,1,2,0,1,0]	[2,0,1,0,0,1,2,2,2]	[1,1,0,2,0,1,1,0,0]
325	2	[2,1,2,1,2,0,2,0,0]	[2,0,1,0,0,1,2,2,2]	[1,2,0,1,2,0,2,0,0]
13	2	[2,0,0,0,0,2,1,2,2]	[2,0,1,0,0,1,2,2,2]	[1,0,1,1,2,2,2,0,0]
		$\left(\prod_{s,t}\frac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{s,t})}{\mathcal{L}_{E,\underline{\Delta}}(\oplus\omega^j)}\right)^p = [1,0,0,0,0,0,0,2,2]$		

Table 7.4.3: $p = 5$, $E = 19A3$ with equation $y^2 + y = x^3 + x^2 + x$.

$\Delta_1^s\Delta_2^t$	L^*	$\mathcal{L}_{E,\underline{\Delta}}(\rho_{\chi_{\Delta_1^s}\chi_{\Delta_2^t}})$	$\mathcal{L}_{E,\underline{\Delta}}(\oplus_{j=0}^{p-2}\omega^j)$	$\frac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{\chi_{\Delta_1^s}\chi_{\Delta_2^t}})}{\mathcal{L}_{E,\underline{\Delta}}(\oplus_{j=0}^{p-2}\omega^j)}$
2	1	[2,2,0,3,3,2,2,2,4]	[2,3,0,3,3,0,3,2,4]	[1,2,4,0,3,1,4,1,0]
18	1	[2,4,0,1,3,4,4,1,0]	[2,3,0,3,3,0,3,2,4]	[1,3,0,3,0,3,0,1,0]
6	4	[2,3,2,0,0,1,2,3,4]	[2,3,0,3,3,0,3,2,4]	[1,0,1,2,2,2,3,0,0]
12	49	[2,0,4,2,2,2,4,0,0]	[2,3,0,3,3,0,3,2,4]	[1,1,0,2,2,0,4,4,4]
48	4	[2,3,2,0,0,1,2,3,4]	[2,3,0,3,3,0,3,2,4]	[1,0,1,2,2,2,3,0,0]
3	4	[2,1,2,2,1,2,2,1,0]	[2,3,0,3,3,0,3,2,4]	[1,4,4,4,2,0,4,2,4]
		$\left(\prod_{s,t}\frac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{s,t})}{\mathcal{L}_{E,\underline{\Delta}}(\oplus\omega^j)}\right)^p = [1,0,0,2,3,3,1,2,0]$		

Table 7.4.4: $p = 5$, $E = 56A1$ with equation $y^2 = x^3 + x + 2$.

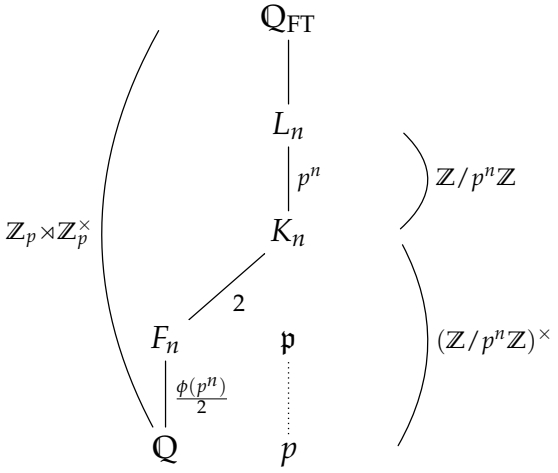
$\Delta_1^s\Delta_2^t$	L^*	$\mathcal{L}_{E,\underline{\Delta}}\left(\rho_{\chi_{\Delta_1^s}\chi_{\Delta_2^t}}\right)$	$\mathcal{L}_{E,\underline{\Delta}}\left(\oplus_{j=0}^{p-2}\omega^j\right)$	$\frac{\mathcal{L}_{E,\underline{\Delta}}\left(\rho_{\chi_{\Delta_1^s}\chi_{\Delta_2^t}}\right)}{\mathcal{L}_{E,\underline{\Delta}}\left(\oplus_{j=0}^{p-2}\omega^j\right)}$
2	16	[2,4,3,2,2,1,4,4,4]	[2,1,0,3,0,2,1,0,0]	[1,4,4,4,4,4,4,2,4]
18	36	[2,2,0,1,1,3,0,3,4]	[2,1,0,3,0,2,1,0,0]	[1,3,3,4,0,2,3,0,0]
6	36	[2,4,4,0,2,0,1,3,4]	[2,1,0,3,0,2,1,0,0]	[1,4,2,2,3,0,4,1,0]
12	16	[2,1,3,2,1,1,3,3,4]	[2,1,0,3,0,2,1,0,0]	[1,0,4,2,1,0,4,0,0]
48	36	[2,4,4,0,2,0,1,3,4]	[2,1,0,3,0,2,1,0,0]	[1,4,2,2,3,0,4,1,0]
3	4	[2,1,3,2,1,1,3,3,4]	[2,1,0,3,0,2,1,0,0]	[1,0,4,2,1,0,4,0,0]
$\left(\prod_{s,t}\frac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{s,t})}{\mathcal{L}_{E,\underline{\Delta}}(\oplus\omega^j)}\right)^p = [1,0,0,1,4,3,2,1,0]$				

8 Computations on Elliptic Curves with Bad Reduction

The author of this thesis wrote the appendix to [10], which contains computations that verify the various congruences predicted in that article. This chapter gives a comprehensive account of those computations, which concern elliptic curves with bad multiplicative reduction at p.

8.1 Non-Commutative Iwasawa Theory of Elliptic Curves with Semistable Reduction

Fix a prime number $p \geq 3$, and let Δ denote a p-power free integer co-prime to p. For each integer $n \geq 0$, define $K_n := \mathbb{Q}(\mu_{p^n})$, $F_n := \mathbb{Q}(\mu_{p^n})^+$, and $L_n := \mathbb{Q}(\mu_{p^n}, \sqrt[p^n]{\Delta})$. Then the false Tate curve extension is defined as $\mathbb{Q}_{\mathrm{FT}} := \bigcup_{n\geq 1} L_n$. In this setting, there is the following field diagram:



Galois theory informs us that

$$\mathrm{Gal}(\mathbb{Q}_{\mathrm{FT}}/\mathbb{Q}) \cong \begin{pmatrix} \mathbb{Z}_p^\times & \mathbb{Z}_p \\ 0 & 1 \end{pmatrix} \triangleleft \mathrm{GL}_2(\mathbb{Z}_p),$$

namely the Galois group $\mathrm{Gal}(\mathbb{Q}_{\mathrm{FT}}/\mathbb{Q})$ is a semidirect product of two Lie groups of dimension one. For each $k \geq 1$, Dokchitser showed in [18] that $\mathrm{Gal}(\mathbb{Q}_{\mathrm{FT}}/\mathbb{Q})$ has a unique self-dual irreducible representation of the form

$$\rho_{k,\mathbb{Q}} = \mathrm{Ind}_{K_k}^{\mathbb{Q}}(\chi_{\rho_k})$$

with dimension $p^k - p^{k-1}$, for any character $\chi_{\rho_k} : \mathrm{Gal}(L_k/K_k) \to \mu_{p^k}$ sending $\sigma \mapsto \frac{\sigma(\sqrt[p^k]{\Delta})}{\sqrt[p^k]{\Delta}}$. Setting $\rho_{0,\mathbb{Q}} = \mathbf{1}$, then every irreducible representation of $\mathrm{Gal}(\mathbb{Q}_{\mathrm{FT}}/\mathbb{Q})$ has the form $\rho_{k,\mathbb{Q}} \otimes \psi$ for some $k \geq 0$, and finite order character $\psi : \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \to \mathbb{C}^\times$. Denote by σ_n the sum of all the one dimensional characters ω_i of $\mathrm{Gal}(K_n/\mathbb{Q})$.

Let E be an elliptic curve over $\mathbb{Q}$ which has multiplicative reduction at p. An elliptic curve has split multiplicative reduction if the p-th Fourier coefficient $a_p(E)$ is $+1$, and the elliptic curve has non-split multiplicative reduction if $a_p(E)$ is -1.

Theorem 8.1.1. *(Theorem 1 in [10]). Let $\mathfrak{p}$ and $\mathfrak{P}$ denote the primes above p of F_n and K_n respectively, and set $U^{(n)} = \ker\left(\mathbb{Z}_p^\times \to (\mathbb{Z}/p^n\mathbb{Z})^\times\right)$. For every $n \geq 1$, there exists a unique element $\mathbf{L}_p(E, \rho_n) \in \mathbb{Z}_p[[U^{(n)}]] \otimes \mathbb{Q}$ satisfying*

$$\psi(\mathbf{L}_p(E,\rho_n)) = \frac{\epsilon_{F_n}(\rho_n \otimes \psi)_{\mathfrak{p}}}{a_p(E)^{f(\rho_n \otimes \psi, \mathfrak{p})}} \left(1 - a_p(E)\chi_{\rho_n}(\mathfrak{P})\psi^{-1}(\mathfrak{p})\right) \frac{L_S(E, \rho_n \otimes \psi^{-1}, 1)}{(\Omega_E^+\Omega_E^-)^{\phi(p^n)/2}}$$

at all finite characters ψ of $U^{(n)}$.

Here $f(\rho_n \otimes \psi, \mathfrak{p})$ is the $\mathfrak{p}$-adic valuation of the conductor of $\rho_n \otimes \psi$, S is the finite set of primes

$$\{v : v \text{ is a prime of } F_n, v|\Delta\},$$

and $\epsilon_{F_n}(\rho_n \otimes \psi)_{\mathfrak{p}}$ is the local epsilon factor at $\mathfrak{p}$ for $\rho_n \otimes \psi$, which depends on the choice of a local Haar measure and additive character at p.

Hypothesis$(\mu = 0)$: At each $n \geq 0$, the analytic μ-invariant of $\mathbf{L}_p(E, \rho_n)$ equals zero.

Now, for $n \geq 1$, put $a_n = \mathbf{L}_p(E, \rho_n)$, and take $a_0 \in \mathbb{Z}_p[[U^{(0)}]] \otimes \mathbb{Q}$ to be the Mazur-Tate-Teitelbaum p-adic L-function, which decomposes into $p-1$ branches in $\mathbb{Z}_p[[T]] \otimes \mathbb{Q}$. Let $N_{i,j} : \mathbb{Z}_p[[U^{(i)}]]^\times \to \mathbb{Z}_p[[U^{(j)}]]^\times$ denote the norm map.

Theorem 8.1.2. *(Theorem 2 in [10]). Under the Hypothesis*$(\mu = 0)$*, for* $n \geq 1$ *the congruence*

$$a_n \equiv N_{0,n}(a_0) \mod p\mathbb{Z}_p[[U^{(n)}]] \quad \textit{holds.}$$

For $n = 1$ and $\psi = \mathbf{1}$, the congruence in Theorem 8.1.2 is equivalent to

$$\mathbf{1}(\mathbf{L}_p(E, \rho_1)) \equiv \mathbf{1}(\mathbf{L}_p(E, \sigma_1)) \mod p. \tag{8.1}$$

Notice that $\mathrm{Ind}_{K_n}^{\mathbb{Q}}(\mathbf{1})$ decomposes into the sum of all the one dimensional characters of $\mathrm{Gal}(K_n/\mathbb{Q})$. An application of the Greenberg-Stevens formula in Theorem 7.1 of [19] for $p \geq 5$ implies that

$$\left.\frac{\mathrm{d}\left(\mathbf{L}_p(E, \mathrm{Ind}_{K_n}^{\mathbb{Q}}(\mathbf{1}), T)\right)}{\mathrm{d}T}\right|_{T=0} = \frac{\log_p(q_{E,p})}{\mathrm{ord}_p(q_{E,p})}\mathcal{L}_E(\mathrm{Ind}_{K_n}^{\mathbb{Q}}(\mathbf{1})),$$

where $q_{E,p}$ denotes the Tate period of the elliptic curve, $\log_p$ is the p-adic logarithm, and the algebraic L-value $\mathcal{L}_E(\mathrm{Ind}_{K_n}^{\mathbb{Q}}(\mathbf{1})) := \sqrt{\mathrm{disc}_{K_n}} \times \frac{L_S(E/K_n, 1)}{(\Omega_E^+ \Omega_E^-)^{[F_n:\mathbb{Q}]}}$.

Conjecture 8.1.3. *(Conjecture 28 in [10])*

If $a_p(E) = +1$*, then*

$$\frac{\log_p(q_{E,p})}{\mathrm{ord}_p(q_{E,p})} \times \mathcal{L}_E(\mathrm{Ind}_{K_1}^{\mathbb{Q}}(\mathbf{1})) \in p\mathbb{Z}_p.$$

8.2 The Numerical Calculations

The aim now is to computationally check congruence (8.1) when E has non-split multiplicative reduction at p, and when E has split multiplicative reduction at p to verify Conjecture 8.1.3. Due to computational limitations the congruences are

only verified for the primes $p = 3$ and 5. The notations employed here are almost identical to the previous section.

Define $K := \mathbb{Q}(\mu_p)$, $F := \mathbb{Q}(\mu_p)^+$, and $L := \mathbb{Q}(\mu_p, \sqrt[p]{\Delta})$. Let σ be the regular representation of $\mathrm{Gal}(K/\mathbb{Q})$, and ρ be the irreducible Artin representation of $\mathrm{Gal}(L/\mathbb{Q})$ with dimension $p-1$. For our computations, ψ is the trivial character. As a result of σ decomposing into $\oplus_{i=1}^{p-1}\omega_i$,

$$L(E, \sigma, s) = \prod_{i=1}^{p-1} L(E, \omega_i, s). \tag{8.2}$$

The right hand side of the equation is easier to compute (at $s = 1$) and is used to calculate $L(E, \sigma, 1)$, because ω_i is a 1-dimensional character, whereas σ is a $(p-1)$-dimensional representation. Moreover, on the level of ϵ-factors, we have

$$\epsilon_F(\sigma)_p = \prod_{i=1}^{p-1} \epsilon(\omega_i)_p. \tag{8.3}$$

Set $\delta = \mathrm{ord}_p(\Delta^{p-1} - 1) - 1 \geq 0$. We will only do computations when the condition $\delta = 0$ is satisfied. The following quantities are recorded in Tables 8.2.1, 8.2.2, 8.2.3, 8.2.4, 8.2.5, 8.2.6, 8.2.7, 8.2.8, 8.2.9, and 8.2.10 using the coefficients of their p-adic expansions up to order $O(p^8)$:

- $L^* = \left| \frac{L(E,\rho,1)\sqrt{\mathrm{disc}_{\mathbb{Q}(\sqrt[p]{\Delta})}}}{(2\Omega_E^+\Omega_E^-)^{\frac{(p-1)}{2}}} \right|$, where $\mathrm{disc}_{\mathbb{Q}(\sqrt[p]{\Delta})}$ is the discriminant of $\mathbb{Q}(\sqrt[p]{\Delta})$.
- $\mathbf{1}\left(\mathbf{L}_p(E,\rho)\right) = \frac{L_S(E,\rho,1)}{\left(\Omega_E^+\Omega_E^-\right)^{\frac{p-1}{2}}} \cdot \frac{\epsilon_F(\rho)_p}{a_p(E)^{f(\rho,p)}} \left(1 - a_p(E)\chi_\rho(\mathfrak{P})\right)$, where $\mathfrak{P}$ is the prime of K above p; however, the condition $\delta = 0$ ensures that there is only one prime above p, so we can identify $\mathfrak{P}$ with p, thus $\left(1 - a_p(E)\chi_\rho\left(\mathfrak{P}\right)\right) = 1$.
- $\mathbf{1}\left(\mathbf{L}_p(E,\sigma)\right) = \frac{L_S(E,\sigma,1)}{\left(\Omega_E^+\Omega_E^-\right)^{\frac{p-1}{2}}} \cdot \frac{\epsilon_F(\sigma)_p}{a_p(E)^{f(\sigma,p)}} \cdot \left(1 - a_p(E)\right)$.

If $a_p(E) = 1$ then $\left(1 - a_p(E)\right) = 0$, which gives an exceptional zero for $\mathbf{L}_p(E, \sigma)$. Thus if E has split multiplicative reduction at p, we instead tabulate the quantity

- $\frac{\log_p(q_{E,p})}{\mathrm{ord}_p(q_{E,p})} \times \mathcal{L}_E(\mathrm{Ind}_K^{\mathbb{Q}}(\mathbf{1})) = \frac{\log_p(q_{E,p})}{\mathrm{ord}_p(q_{E,p})} \sqrt{\mathrm{disc}_K} \frac{L_S(E,\mathrm{Ind}_K^{\mathbb{Q}}(\mathbf{1}),1)}{\left(\Omega_E^+\Omega_E^-\right)^{\frac{p-1}{2}}}$, corresponding to the first derivative of the p-adic L-function attached to the σ-twist of E.

The local L-factors at q of $L(E,\sigma,s)$ and $L(E,\rho,s)$ will be denoted by $P_q(E,\rho,q^{-s})$ and $P_q(E,\sigma,q^{-s})$ respectively. Throughout we will calculate $L(E,\sigma,1)$, $L(E,\rho,1)$, $P_q(E,\rho,q^{-1})$, $P_q(E,\sigma,q^{-1})$, $\epsilon_F(\rho)_p$, $\epsilon_F(\sigma)_p$, Ω_E^+, and Ω_E^- up to 15 digit precision.

8.2.1 Numerical Examples

To illustrate the computational results, two examples are described in detail: one when $a_p(E) = -1$, and one when $a_p(E) = 1$.

The calculation of the L-values when the elliptic curve has non-split multiplicative reduction are first explained. Let $p = 3$, and suppose E is the elliptic curve $E15A1$. Since the conductor of E is 15 and $\mathrm{ord}_3(15) = 1$, E has multiplicative reduction at $p = 3$. Choosing $\Delta = 2$, then the condition $\delta = 0$ is satisfied, while $K = \mathbb{Q}(\mu_3)$ and $L = \mathbb{Q}(\mu_3, \sqrt[3]{2})$.

The calculation of L^* will now be described. Evaluating $L(E,\rho,s)$ at $s = 1$ yields

$$L(E,\rho,1) \approx 1.72104398080992.$$

Using in-built functions in MAGMA, one calculates that

$$\begin{aligned}\sqrt{\mathrm{disc}_{\mathbb{Q}(2^{1/3})}} &\approx 10.3923048454132i,\\ \Omega_E^+ &\approx 1.40060304233260, \text{ and } \Omega_E^- \approx 1.59624222213178i.\end{aligned}$$

Combining this information, one obtains

$$L^* = \left| \frac{L(E,\rho,1)\sqrt{\mathrm{disc}_{\mathbb{Q}(2^{1/3})}}}{(2\Omega_E^+\Omega_E^-)^{(3-1)/2}} \right| \approx 4.00000000000001.$$

Then we make the approximation that $L^* \approx 4$. Note that we do not expect L^* to be divisible by large primes for the Δ's in our computations.

The calculation of $\mathbf{1}(\mathbf{L}_p(E,\rho))$ is now detailed. Since $f(\rho,3) = 3$, we get $a_3(E)^{f(\rho,3)} = -1$. The only prime dividing Δ is 2, thus $S = \{2\}$. Then the local L-factor of $L(E,\rho,s)$ at the prime 2 evaluated at $s = 1$ is given by $P_2(E,\rho,2^{-1}) \approx$

1.00000000000000. Using the Dokchitser's equations (Section 6.10, [17]) for the local epsilon factors, one finds $\epsilon_F(\rho)_3 \approx -1.04520385168448E{-}14 + 5.19615242270663i$, in which case $\epsilon_F(\rho)_3/\sqrt{\text{disc}_{\mathbb{Q}(\sqrt[3]{2})}} \approx \frac{i}{2}$. Compiling this information, one obtains

$$\begin{aligned}\mathbf{1}(\mathbf{L}_p(E,\rho)) &= L^* \frac{2^{(3-1)/2}}{\sqrt{\text{disc}_{\mathbb{Q}(\sqrt[3]{2})}}} P_2(E,\rho,2^{-1}) \frac{\epsilon_F(\rho)_3}{a_3(E)^{f(\rho,3)}} \approx 4 + O(3^8) \\ &= [1,1,0,0,0,0,0,0,0].\end{aligned}$$

An explanation of our calculation of $\mathbf{1}\left(\mathbf{L}_p(E,\sigma)\right)$ is now provided. Using equation (8.2) to evaluate $L(E,\sigma,s)$ at $s=1$, one finds $L(E,\sigma,s) \approx 0.322695746401859$. Again exploiting in-built functions in MAGMA we calculate disc_K, which comes out at -3. Then $L^*(E,\sigma)$ is computed using the formula

$$L^*(E,\sigma) = \left| \frac{L(E,\sigma,1)\sqrt{\text{disc}_K}}{(2\Omega_E^+\Omega_E^-)^{\frac{(3-1)}{2}}} \right| \approx 0.125000000000000 \approx \frac{1}{8}.$$

The local epsilon factor for σ at p is computed via equation (8.3), and $\epsilon(\omega_i)_p$ for $1 \leq i \leq p-1$ is calculated from the formula the Dokchitsers provide (Section 6.10 [17]). As a result, $\epsilon_F(\sigma)_3 \approx -2.66453525910038E - 15 + 1.73205080756888i$, and $\frac{\epsilon_F(\sigma)_3}{\sqrt{\text{disc}_K}} \approx -1$. Furthermore, we calculate that $P_2(E,\sigma,2^{-1}) \approx 2.00000000000000$. Since $f(\sigma,3)=1$, one gets $a_3(E)^{f(\sigma,3)} = -1$. Putting all of this together,

$$\begin{aligned}\mathbf{1}(\mathbf{L}_3(E,\sigma)) &= L^*(E,\sigma) P_2(E,\sigma,2^{-1}) \frac{2^{(3-1)/2}}{\sqrt{\text{disc}_K}} \frac{2\epsilon_F(\sigma)_3}{a_3(E)^{f(\sigma,3)}} \approx 1 + O(3^8) \\ &= [1,0,0,0,0,0,0,0,0].\end{aligned}$$

Finally it is now clear that $\mathbf{1}\left(\mathbf{L}_3(E,\rho)\right) \equiv \mathbf{1}\left(\mathbf{L}_3(E,\sigma)\right) \mod p$, as predicted.

We now consider a situation where $a_p(E) = +1$. Let E be the elliptic curve $E21A1$. Fix $p=3$ and $\Delta = 2$, which satisfies the $\delta = 0$ condition. This curve E has conductor 21 and $\text{ord}_3(21) = 1$, thus E has multiplicative reduction at $p=3$. For these choices, the calculation of $\frac{\log_p(q_{E,p})}{\text{ord}_p(q_{E,p})}\mathcal{L}_E(\text{Ind}_K^{\mathbb{Q}}(\mathbf{1}))$ will now be explained. Note that L^* and $\mathbf{1}\left(\mathbf{L}_p(E,\rho)\right)$ are computed in exactly the same manner as we did for $a_p(E) = -1$.

The 3-adic L-invariant, $\frac{\log_3(q_{E,3})}{\mathrm{ord}_3(q_{E,3})}$, for E is $[0,1,2,2,2,1,2,0,0]$; here MAGMA code found on William Stein's website [33] was used to calculate the Tate period of E, and then the L-invariant was cross-checked with SAGE. As described earlier,

$$L(E,\sigma,1) \approx 0.322695746401859, \quad P_2(E,\sigma,2^{-1}) \approx 2.00000000000000,$$
$$\Omega_E^+ \approx 1.40060304233260, \text{ and } \Omega_E^- \approx 1.59624222213178i,$$

which enables us to compute

$$\frac{\log_3(q_{E,3})}{\mathrm{ord}_3(q_{E,3})} \times \mathcal{L}_E(\mathrm{Ind}_K^{\mathbb{Q}}(\mathbf{1})) = [0,2,2,2,2,0,1,0,0]$$

and verify that $\frac{\log_3(q_{E,3})}{\mathrm{ord}_3(q_{E,3})} \times \mathcal{L}_E(\mathrm{Ind}_K^{\mathbb{Q}}(\mathbf{1})) \in 3\mathbb{Z}_3$, as predicted in Conjecture 8.1.3.

8.2.2 Tables

Table 8.2.1: $E15A1$ with equation $y^2+xy+y = x^3+x^2-10x-10$, which has non-split multiplicative reduction at $p=3$.

Δ	L^*	$\mathbf{1}\left(\mathbf{L}_p(E,\rho)\right)$	$\mathbf{1}\left(\mathbf{L}_p(E,\sigma)\right)$
2	4	[1,1,0,0,0,0,0,0,0]	[1,0,0,0,0,0,0,0,0]
5	0	[0,0,0,0,0,0,0,0,0]	[0,1,2,2,1,2,2,0,0]
7	16	[2,0,2,2,0,1,0,2,2]	[2,2,2,2,0,2,1,1,2]
11	16	[1,2,2,0,0,1,1,2,2]	[1,2,0,1,1,0,2,0,0]
13	4	[2,0,1,1,0,1,1,0,0]	[2,2,2,1,2,1,2,2,2]
14	4	[1,2,1,2,0,1,0,2,2]	[1,2,2,2,1,1,0,0,0]
20	0	[0,0,0,0,0,0,0,0,0]	[0,2,1,2,0,2,2,1,2]
22	64	[2,1,2,1,0,2,2,1,2]	[2,1,1,2,2,0,1,1,0]
23	0	[0,0,0,0,0,0,0,0,0]	[0,0,2,0,0,1,0,0,0]
29	4	[1,1,0,1,2,2,0,0,0]	[1,1,0,0,0,0,2,2,2]
31	4	[2,0,0,1,1,1,0,1,0]	[2,1,0,0,1,1,2,1,2]
34	64	[2,2,2,2,1,2,0,2,2]	[2,1,1,0,2,2,2,2,2]

Table 8.2.1: $E15A1$ with equation $y^2 + xy + y = x^3 + x^2 - 10x - 10$, which has non-split multiplicative reduction at $p = 3$.

Δ	L^*	$\mathbf{1}\left(\mathbf{L}_p(E,\rho)\right)$	$\mathbf{1}\left(\mathbf{L}_p(E,\sigma)\right)$
38	4	[1,1,1,0,0,2,2,1,2]	[1,1,0,1,0,0,0,1,0]
41	4	[1,2,1,0,2,0,1,2,2]	[1,2,0,0,0,0,0,1,0]
43	64	[2,2,0,1,1,1,0,2,2]	[2,0,2,1,2,0,2,1,2]
47	16	[1,2,0,2,2,1,0,1,0]	[1,0,2,2,0,1,1,1,0]
50	0	[0,0,0,0,0,0,0,0,0]	[0,2,1,2,0,2,2,1,2]
52	100	[1,2,1,2,2,0,2,2,2]	[1,2,2,0,2,0,2,2,2]
58	400	[2,0,1,0,2,1,1,0,0]	[2,2,0,0,0,0,1,2,2]
59	64	[1,1,0,1,0,1,1,0,0]	[1,1,2,2,2,0,0,0,0]
61	64	[2,2,2,0,0,0,1,0,0]	[2,2,1,1,2,1,0,2,2]
67	16	[2,2,1,1,0,0,2,2,2]	[2,2,0,0,2,1,0,2,2]
68	196	[2,0,0,0,1,2,1,1,2]	[2,1,1,0,2,2,2,2,2]
70	0	[0,0,0,0,0,0,0,0,0]	[0,2,2,0,1,2,2,2,2]
74	36	[0,0,1,1,2,0,2,2,2]	[0,0,1,1,2,1,0,1,0]
76	64	[1,0,2,1,2,2,0,0,0]	[1,1,0,1,0,0,0,1,0]
77	64	[1,1,2,1,0,0,2,2,2]	[1,1,1,0,2,1,2,1,2]
79	64	[2,2,1,0,0,1,2,1,2]	[2,2,1,2,2,2,2,2,2]
83	0	[0,0,0,0,0,0,0,0,0]	[0,0,0,2,1,0,1,1,0]
85	0	[0,0,0,0,0,0,0,0,0]	[0,2,2,2,2,2,1,1,2]
86	4	[1,2,0,1,0,0,1,0,0]	[1,1,1,0,2,1,1,0,0]
92	36	[0,0,2,2,2,1,0,2,2]	[0,0,1,1,0,2,0,0,0]
94	484	[2,2,0,2,0,1,1,1,0]	[2,0,1,2,1,2,2,2,2]
95	0	[0,0,0,0,0,0,0,0,0]	[0,1,0,2,2,0,2,2,2]
97	144	[0,0,2,0,0,0,1,0,0]	[0,0,2,0,0,0,2,0,0]

Table 8.2.2: $E21A1$ with equation $y^2 + xy = x^3 - 4x - 1$, which has split multiplicative reduction at $p = 3$.

Δ	L^*	$\mathbf{1}\left(\mathbf{L}_p(E,\rho)\right)$	$\frac{\log_p(q_{E,p})}{\mathrm{ord}_p(q_{E,p})}\mathcal{L}_E(\mathrm{Ind}_K^{\mathbb{Q}}(\mathbf{1}))$
2	0	[0,0,0,0,0,0,0,0,0]	[0,2,2,2,2,0,1,0,0]
5	0	[0,0,0,0,0,0,0,0,0]	[0,2,2,0,1,2,1,1,2]
7	0	[0,0,0,0,0,0,0,0,0]	[0,1,0,0,0,1,2,0,0]
11	0	[0,0,0,0,0,0,0,0,0]	[0,2,0,2,1,2,2,0,0]
13	0	[0,0,0,0,0,0,0,0,0]	[0,1,0,0,1,2,2,2,2]
14	0	[0,0,0,0,0,0,0,0,0]	[0,2,0,0,0,2,1,1,2]
20	0	[0,0,0,0,0,0,0,0,0]	[0,1,2,1,2,1,0,0,0]
22	0	[0,0,0,0,0,0,0,0,0]	[0,1,1,1,0,2,2,1,2]
23	0	[0,0,0,0,0,0,0,0,0]	[0,0,0,1,2,2,1,1,2]
29	0	[0,0,0,0,0,0,0,0,0]	[0,2,1,2,2,0,2,2,2]
31	0	[0,0,0,0,0,0,0,0,0]	[0,1,1,2,2,0,2,2,2]
34	0	[0,0,0,0,0,0,0,0,0]	[0,0,0,1,1,0,1,2,2]
38	0	[0,0,0,0,0,0,0,0,0]	[0,2,1,2,1,0,2,1,2]
41	0	[0,0,0,0,0,0,0,0,0]	[0,2,2,1,1,1,2,1,2]
43	0	[0,0,0,0,0,0,0,0,0]	[0,0,0,1,1,1,2,1,2]
47	0	[0,0,0,0,0,0,0,0,0]	[0,0,0,1,1,0,1,1,0]
50	0	[0,0,0,0,0,0,0,0,0]	[0,1,2,1,2,1,0,0,0]
52	0	[0,0,0,0,0,0,0,0,0]	[0,2,0,0,2,1,2,2,2]
58	0	[0,0,0,0,0,0,0,0,0]	[0,1,0,2,2,1,1,2,2]
59	0	[0,0,0,0,0,0,0,0,0]	[0,0,0,0,2,1,0,1,0]
61	0	[0,0,0,0,0,0,0,0,0]	[0,1,0,1,1,2,2,0,0]
67	0	[0,0,0,0,0,0,0,0,0]	[0,1,2,1,0,2,1,1,2]
68	0	[0,0,0,0,0,0,0,0,0]	[0,0,0,1,1,0,1,2,2]
70	0	[0,0,0,0,0,0,0,0,0]	[0,1,1,2,0,1,1,2,2]

Table 8.2.2: $E21A1$ with equation $y^2 + xy = x^3 - 4x - 1$, which has split multiplicative reduction at $p = 3$.

Δ	L^*	$\mathbf{1}\left(\mathbf{L}_p(E,\rho)\right)$	$\frac{\log_p(q_{E,p})}{\mathrm{ord}_p(q_{E,p})}\mathcal{L}_E(\mathrm{Ind}_K^{\mathbb{Q}}(\mathbf{1}))$
74	0	[0,0,0,0,0,0,0,0,0]	[0,2,0,2,1,1,1,0,0]
76	0	[0,0,0,0,0,0,0,0,0]	[0,2,1,2,1,0,2,1,2]
77	0	[0,0,0,0,0,0,0,0,0]	[0,2,1,1,2,1,0,0,0]
79	0	[0,0,0,0,0,0,0,0,0]	[0,0,0,1,2,0,1,1,0]
83	0	[0,0,0,0,0,0,0,0,0]	[0,0,0,0,1,1,2,1,2]
85	0	[0,0,0,0,0,0,0,0,0]	[0,0,0,1,1,2,1,2,2]
86	0	[0,0,0,0,0,0,0,0,0]	[0,0,0,2,2,2,1,0,0]
92	0	[0,0,0,0,0,0,0,0,0]	[0,0,0,2,1,2,0,0,0]
94	0	[0,0,0,0,0,0,0,0,0]	[0,0,0,2,2,0,2,2,2]
95	0	[0,0,0,0,0,0,0,0,0]	[0,2,1,0,1,0,2,1,2]
97	0	[0,0,0,0,0,0,0,0,0]	[0,1,0,0,1,1,0,2,2]

Table 8.2.3: $E30A1$ with equation $y^2 + xy + y = x^3 + x + 2$, which has split multiplicative reduction at $p = 3$.

Δ	L^*	$\mathbf{1}\left(\mathbf{L}_p(E,\rho)\right)$	$\frac{\log_p(q_{E,p})}{\mathrm{ord}_p(q_{E,p})}\mathcal{L}_E(\mathrm{Ind}_K^{\mathbb{Q}}(\mathbf{1}))$
2	3	[0,2,2,2,2,2,2,2,2]	[0,0,2,1,2,1,2,2,2]
5	12	[0,2,0,2,1,0,1,2,2]	[0,0,1,0,1,2,1,2,2]
7	0	[0,0,0,0,0,0,0,0,0]	[0,0,0,2,2,0,2,1,2]
11	0	[0,0,0,0,0,0,0,0,0]	[0,0,0,2,2,2,2,0,0]
13	0	[0,0,0,0,0,0,0,0,0]	[0,0,0,2,0,0,1,2,2]
14	27	[0,0,0,2,1,2,0,1,0]	[0,0,0,0,2,0,0,2,2]
20	0	[0,0,0,0,0,0,0,0,0]	[0,0,0,1,2,1,0,1,0]
22	0	[0,0,0,0,0,0,0,0,0]	[0,0,0,0,2,0,2,0,0]
23	0	[0,0,0,0,0,0,0,0,0]	[0,0,0,2,2,1,0,1,0]

Table 8.2.3: $E30A1$ with equation $y^2 + xy + y = x^3 + x + 2$, which has split multiplicative reduction at $p = 3$.

Δ	L^*	$\mathbf{1}\left(\mathbf{L}_p(E,\rho)\right)$	$\frac{\log_p(q_{E,p})}{\mathrm{ord}_p(q_{E,p})}\mathcal{L}_E(\mathrm{Ind}_K^{\mathbb{Q}}(\mathbf{1}))$
29	0	[0,0,0,0,0,0,0,0,0]	[0,0,0,0,1,2,0,1,0]
31	0	[0,0,0,0,0,0,0,0,0]	[0,0,0,2,2,1,1,1,2]
34	0	[0,0,0,0,0,0,0,0,0]	[0,0,0,0,1,2,1,2,2]
38	27	[0,0,0,2,2,1,0,2,2]	[0,0,0,0,2,1,2,0,0]
41	0	[0,0,0,0,0,0,0,0,0]	[0,0,0,0,2,2,0,0,0]
43	0	[0,0,0,0,0,0,0,0,0]	[0,0,0,2,0,1,0,2,2]
47	0	[0,0,0,0,0,0,0,0,0]	[0,0,0,2,0,2,2,2,2]
50	0	[0,0,0,0,0,0,0,0,0]	[0,0,0,1,2,1,0,1,0]
52	27	[0,0,0,2,0,0,2,0,0]	[0,0,0,0,2,1,1,2,2]
58	108	[0,0,0,1,2,2,0,0,0]	[0,0,0,0,0,1,1,2,2]
59	0	[0,0,0,0,0,0,0,0,0]	[0,0,0,2,1,1,0,1,0]
61	0	[0,0,0,0,0,0,0,0,0]	[0,0,0,0,0,2,1,0,0]
67	0	[0,0,0,0,0,0,0,0,0]	[0,0,0,0,0,2,2,0,0]

Table 8.2.4: $E33A1$ with equation $y^2 + xy = x^3 + x^2 - 11x$, which has non-split multiplicative reduction at $p = 3$.

Δ	L^*	$\mathbf{1}\left(\mathbf{L}_p(E,\rho)\right)$	$\mathbf{1}\left(\mathbf{L}_p(E,\sigma)\right)$
2	2	[2,0,0,0,0,0,0,0,0]	[2,0,0,0,0,0,0,0,0]
5	2	[2,2,1,0,1,2,1,0,0]	[2,0,1,0,0,2,1,1,2]
7	2	[1,2,1,2,0,1,0,2,2]	[1,1,1,1,0,1,2,0,0]
11	0	[0,0,0,0,0,0,0,0,0]	[0,1,0,0,0,2,0,0,0]
13	50	[1,2,1,2,2,0,2,2,2]	[1,2,2,0,2,0,2,2,2]
14	32	[2,0,2,2,0,1,0,2,2]	[2,2,2,2,0,2,1,1,2]

Table 8.2.4: $E33A1$ with equation $y^2 + xy = x^3 + x^2 - 11x$, which has non-split multiplicative reduction at $p = 3$.

Δ	L^*	$\mathbf{1}\left(\mathbf{L}_p(E,\rho)\right)$	$\mathbf{1}\left(\mathbf{L}_p(E,\sigma)\right)$
20	98	[1,2,2,1,2,1,0,1,0]	[1,1,2,0,0,1,0,0,0]
22	0	[0,0,0,0,0,0,0,0,0]	[0,2,0,0,0,1,1,0,0]
23	2	[2,2,2,1,0,2,2,0,0]	[2,1,0,2,2,1,0,2,2]
29	162	[0,0,0,0,2,0,0,2,2]	[0,0,0,2,2,0,1,0,0]
31	32	[1,2,1,2,1,2,0,0,0]	[1,0,2,1,2,0,1,0,0]
34	338	[1,1,0,2,2,2,1,2,2]	[1,0,0,1,1,2,2,2,2]
38	8	[2,2,2,0,0,1,2,0,0]	[2,2,2,0,2,0,1,2,2]
41	200	[2,2,1,2,1,0,2,0,0]	[2,0,2,2,1,0,2,0,0]

Table 8.2.5: $E15A1$ with equation $y^2 + xy + y = x^3 + x^2 - 10x - 10$, which has split multiplicative reduction at $p = 5$.

Δ	L^*	$\mathbf{1}\left(\mathbf{L}_p(E,\rho)\right)$	$\frac{\log_p(q_{E,p})}{\mathrm{ord}_p(q_{E,p})}\mathcal{L}_E(\mathrm{Ind}_K^{\mathbb{Q}}(\mathbf{1}))$
2	0	[0,0,0,0,0,0,0,0,0]	[0,2,0,1,1,3,4,2,4]
3	80	[0,1,4,0,1,2,4,3,4]	[0,0,2,4,1,4,1,4,4]
6	320	[0,1,4,1,4,4,2,3,4]	[0,0,2,4,1,4,1,4,4]
9	80	[0,1,4,0,1,2,4,3,4]	[0,0,2,4,1,4,1,4,4]

Table 8.2.6: $E30A1$ with equation $y^2 + xy + y = x^3 + x + 2$, which has non-split multiplicative reduction at $p = 5$.

Δ	L^*	$\mathbf{1}\left(\mathbf{L}_p(E,\rho)\right)$	$\mathbf{1}\left(\mathbf{L}_p(E,\sigma)\right)$
2	0	[0,0,0,0,0,0,0,0,0]	[0,1,1,1,1,1,1,1,0]
3	0	[0,0,0,0,0,0,0,0,0]	[0,2,0,1,4,0,3,2,4]
6	180	[0,1,4,4,4,4,4,4,4]	[0,0,1,3,3,1,2,2,0]
9	0	[0,0,0,0,0,0,0,0,0]	[0,2,0,1,4,0,3,2,4]

Table 8.2.7: $E35A1$ with equation $y^2 + y = x^3 + x^2 + 9x + 1$, which has non-split multiplicative reduction at $p = 5$.

Δ	L^*	$\mathbf{1}\left(\mathbf{L}_p(E,\rho)\right)$	$\mathbf{1}\left(\mathbf{L}_p(E,\sigma)\right)$
2	0	[0,0,0,0,0,0,0,0,0]	[0,0,0,0,0,0,0,0,0]
3	0	[0,0,0,0,0,0,0,0,0]	[0,0,0,0,0,0,0,0,0]

Table 8.2.8: $E55A1$ with equation $y^2 + xy = x^3 - x^2 - 4x + 3$, which has split multiplicative reduction at $p = 5$.

Δ	L^*	$\mathbf{1}\left(\mathbf{L}_p(E,\rho)\right)$	$\frac{\log_p(q_{E,p})}{\mathrm{ord}_p(q_{E,p})}\mathcal{L}_E(\mathrm{Ind}_K^{\mathbb{Q}}(\mathbf{1}))$
2	20	[0,4,0,0,0,0,0,0,0]	[0,0,0,0,0,0,0,0,0]

Table 8.2.9: $E65A1$ with equation $y^2 + xy = x^3 - x$, which has non-split multiplicative reduction at $p = 5$.

Δ	L^*	$\mathbf{1}\left(\mathbf{L}_p(E,\rho)\right)$	$\mathbf{1}\left(\mathbf{L}_p(E,\sigma)\right)$
2	0	[0,0,0,0,0,0,0,0,0]	[0,0,0,0,0,0,0,0,0]

Table 8.2.10: $E70A1$ with equation $y^2 + xy + y = x^3 - x^2 + 2x - 3$, which has non-split multiplicative reduction at $p = 5$.

Δ	L^*	$\mathbf{1}\left(\mathbf{L}_p(E,\rho)\right)$	$\mathbf{1}\left(\mathbf{L}_p(E,\sigma)\right)$
2	0	[0,0,0,0,0,0,0,0,0]	[0,3,3,3,3,3,3,3,4]

Bibliography

[1] Emil Artin. Über eine neue art von L-Reihen. *Abh. Math. Sem. Univ. Hamburg*, 3(1):89–108, 1924. English translation in Artin L-Functions: A Historical Approach by N. Snyder.

[2] Hyman Bass. *Algebraic K-theory*. Mathematics Lecture Note Series. W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[3] Thanasis Bouganis. Special values of L-functions and false Tate curve extensions. *J. Lond. Math. Soc. (2)*, 82(3):596–620, 2010. With an appendix by Vladimir Dokchitser.

[4] Thanasis Bouganis and Vladimir Dokchitser. Algebraicity of L-values for elliptic curves in a false Tate curve tower. *Math. Proc. Cambridge Philos. Soc.*, 142(2):193–204, 2007.

[5] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843–939 (electronic), 2001.

[6] John Cassels. *Local fields*, volume 3 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1986.

[7] John Coates, Takako Fukaya, Kazuya Kato, Ramdorai Sujatha, and Otmar Venjakob. The GL_2 main conjecture for elliptic curves without complex mul-

tiplication. *Publications Mathématiques de l'Institut des Hautes Études Scientifiques*, 101:163–208, 2005.

[8] John Coates, Peter Schneider, and Ramdorai Sujatha. *Noncommutative Iwasawa Main Conjectures over Totally Real Fields: Münster, April 2011*. Springer Proceedings in Mathematics & Statistics. Springer, 2012.

[9] John Cremona. Elliptic curves data. `http://homepages.warwick.ac.uk/staff/J.E.Cremona//ftp/data/`.

[10] Daniel Delbourgo and Antonio Lei. On the non-commutative Iwasawa theory of elliptic curves with semistable reduction. Preprint, 2013.

[11] Daniel Delbourgo and Lloyd Peters. Higher order congruences amongst Hasse-Weil L-values. Preprint, 2014.

[12] Daniel Delbourgo and Thomas Ward. Non-abelian congruences between L-values of elliptic curves. *Ann. Inst. Fourier (Grenoble)*, 58(3):1023–1055, 2008.

[13] Daniel Delbourgo and Thomas Ward. The growth of CM periods over false Tate extensions. *Experiment. Math.*, 19(2):195–210, 2010.

[14] Pierre Deligne. Les constantes des équations fonctionnelles des fonctions L. *Springer*, pages 501–597. Lecture Notes in Math., Vol. 349, 1973.

[15] Pierre Deligne. Valeurs de fonctions L et périodes d'intégrales. *American Mathematical Society*, pages 313–346, 1979. With an appendix by N. Koblitz and A. Ogus.

[16] Max Deuring. Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins. *Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. Math.-Phys.-Chem. Abt.*, I, II, III, IV:85–94, 13–42, 37–76, 55–80, 1953, 1955, 1956, 1957.

[17] Tim Dokchitser, Vladimir Dokchitser, John Coates, and Ramdorai Sujatha. Computations in non-commutative Iwasawa theory. *Proceedings of the London Mathematical Society*, 94(1):211–272, 2007.

[18] Vladimir Dokchitser. Root numbers of non-abelian twists of elliptic curves. *Proc. London Math. Soc. (3)*, 91(2):300–324, 2005. With an appendix by Tom Fisher.

[19] Ralph Greenberg and Glenn Stevens. p-adic L-functions and p-adic periods of modular forms. *Invent. Math.*, 111(2):407–447, 1993.

[20] Takashi Hara. Iwasawa theory of totally real fields for certain non-commutative p-extensions. *J. Number Theory*, 130(4):1068–1097, 2010.

[21] I. Martin Isaacs. *Algebra: a graduate course*, volume 100 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2009. Reprint of the 1994 original.

[22] Mahesh Kakde. The main conjecture of Iwasawa theory for totally real fields. *Invent. Math.*, 193(3):539–626, 2013.

[23] Kazuya Kato. Iwasawa theory of totally real fields for Galois extensions of Heisenberg type. Preprint.

[24] Kazuya Kato. K_1 of some non-commutative completed group rings. *K-Theory*, 34(2):99–140, 2005.

[25] Serge Lang. *Cyclotomic fields I and II*, volume 121 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990. With an appendix by Karl Rubin.

[26] Barry Mazur and Andrew Wiles. Class fields of abelian extensions of $\mathbf{Q}$. *Invent. Math.*, 76(2):179–330, 1984.

[27] Robert Oliver. *Whitehead groups of finite groups*, volume 132 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1988.

[28] Jürgen Ritter and Alfred Weiss. Toward equivariant Iwasawa theory. III. *Math. Ann.*, 336(1):27–49, 2006.

[29] Karl Rubin. The "main conjectures" of Iwasawa theory for imaginary quadratic fields. *Invent. Math.*, 103(1):25–68, 1991.

[30] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[31] Jean-Pierre Serre. *Linear representations of finite groups*. Springer-Verlag, New York, 1977. Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42.

[32] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original.

[33] William Stein. `http://modular.math.washington.edu/home/wstein/www/home/rpollack/shp/shp_package/shp/tate.magma`.

[34] Bo Stenström. *Rings of quotients*. Springer-Verlag, New York, 1975. Die Grundlehren der Mathematischen Wissenschaften, Band 217, An introduction to methods of ring theory.

[35] Richard G. Swan. *Algebraic K-Theory*. Springer-Verlag, 1968.

[36] John Tate. Number theoretic background. In *Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2*, Proc. Sympos. Pure Math., XXXIII, pages 3–26. Amer. Math. Soc., Providence, R.I., 1979.

[37] Richard Taylor and Andrew Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3):553–572, 1995.

[38] Otmar Venjakob. Characteristic elements in noncommutative Iwasawa theory. *J. Reine Angew. Math.*, 583:193–236, 2005.

[39] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

[40] André Weil. Jacobi sums as "Grössencharaktere". *Trans. Amer. Math. Soc.*, 73:487–495, 1952.

[41] Andrew Wiles. The Iwasawa conjecture for totally real fields. *Ann. of Math. (2)*, 131(3):493–540, 1990.

[42] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.