J. Aust. Math. Soc. **98** (2015), 1–38
doi:10.1017/S1446788714000445

HIGHER ORDER CONGRUENCES AMONGST HASSE–WEIL L-VALUES

DANIEL DELBOURGO✉ and LLOYD PETERS

(Received 22 January 2014; accepted 13 August 2014; first published online 14 October 2014)

Communicated by F. Calegari

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 L-functions arises from an element in $K_1(\mathbb{Z}_p[\![G]\!])$. If E is a semistable elliptic curve over $\mathbb{Q}$, these abelian L-functions already exist; therefore, one can obtain many new families of higher order p-adic congruences. The first layer congruences are then verified computationally in a variety of cases.

2010 *Mathematics subject classification*: primary 11R23; secondary 11G40, 19B28.

Keywords and phrases: Iwasawa theory, elliptic curves, K-theory, L-functions.

1. Introduction

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 coprime, and write $\underline{\Delta}$ for the product $\prod_{i=1}^d \Delta_i$. The d-fold false Tate curve tower

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

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 semidirect product

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

where $H_\infty^{(d)}$ is a free $\mathbb{Z}_p$-module of rank d, and $\Sigma_\infty = \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ acts on $H_\infty^{(d)}$ through the cyclotomic character. The Iwasawa algebra $\mathbb{Z}_p[\![G_\infty^{(d)}]\!]$ is then given by the projective limit $\varprojlim_{\mathcal{P}} \mathbb{Z}_p[G_\infty^{(d)}/\mathcal{P}]$, where the inverse system of the $\mathcal{P}$ range over normal subgroups of finite index in $G_\infty^{(d)}$.

The authors warmly thank the Australian Research Council for their financial support through an ARC DP1092496 grant, and also the staff of Monash University.

For a ring R, we denote by $K_1(R)$ its first algebraic K-group, in the sense of Milnor. There are three main objectives in this article:

(I) to describe the structure of $K_1(\mathbb{Z}_p[\![G_\infty^{(d)}]\!])$ 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 some explicit examples.

We should point out that (I) is already fully solved when $d = 1$ thanks to the results of Kato [11], 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 [4, 9, 10, 16] devoted to the study of nonabelian Iwasawa Main Conjectures. The extensions we are considering differ from the 'admissible extensions' in [4] in two important ways:

(a) the full Lie extension $\mathbb{Q}_{\infty,\underline{\Delta}}^{(d)}$ is not a union of totally real fields;
(b) there is no subfield $L \subset \mathbb{Q}_{\infty,\underline{\Delta}}^{(d)}$ such that $L/\mathbb{Q}$ is pro-p of dimension $d+1$.

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 [4] is that the congruences derived by Kakde, Hara, Ritter and Weiss are described in terms of ideals inside completed group algebras, whereas the congruences derived here (and by Kato in [11]) are p-adic in flavour. While both approaches ultimately yield necessary and sufficient conditions, 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).

Remarks.

(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. If $U^{(m)} = \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}(\mu_{p^m}))$, then sequences of p-adic L-functions belonging to the algebras $\mathbb{Z}_p[\![U^{(m)}]\!][p^{-1}]$ have already been constructed in [1, 5–7].
(ii) Some weak congruences were established under technical hypotheses in [1, 5–7], inspired by the numerical evidence of the Dokchitser brothers [8].

Following the seminal work of Kakde [4, 10], there is now a precise recipe that, in principle, allows one to describe $K_1(-)$ of a noncommutative Iwasawa algebra. To construct theta-maps, one needs a 'dense enough' family of subgroups for $G_\infty^{(d)}$. In Section 4 we build homomorphisms

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

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^ν with $\nu \leq m$, one next forms the composition

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

As we shall see subsequently in Sections 2 and 4, 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 $\theta_{\mathcal{J}}$.

NOTATION.

(a) Let us denote by $\mathcal{Z}_\infty^{(\nu)}$ 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^ν, and set $\mathcal{Z}_\infty = \bigcup_{\nu \geq 0} \mathcal{Z}_\infty^{(\nu)}$.
(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 then refers to the collection of homomorphisms $\prod_{\mathcal{J} \in \mathcal{Z}_\infty} \theta_{\mathcal{J}}$.

For a fixed $x \in K_1(\mathbb{Z}_p[\![G_\infty^{(d)}]\!])$ and a subgroup $\mathcal{J} \in \mathcal{Z}_\infty^{(\nu)}$, each element $a_{\nu,\mathcal{J}} = \theta_{\mathcal{J}}(x)$ belongs inside $\mathbb{Z}_p[\![U^{(\nu)}]\!]^\times$. One can then turn the situation on its head, by asking the following question.

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

If $d = 1$, Kato provided a complete answer in [11, Section 3] 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 [9, 10, 16].

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 $\nu \leq m$, we shall write

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

to indicate the norm map on algebras, induced from the natural inclusion $U^{(m)} \hookrightarrow U^{(\nu)}$.

Choose an integer $m \geq 1$. We introduce congruences $(1.1)_{m,\underline{\mathfrak{h}}}$ and $(1.2)_m$ as follows:

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

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

- similarly, at the trivial subgroup,

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

  where, for each $\mathcal{J} \in \mathcal{Z}_\infty^{(\nu)}$, one defines

$$\mathfrak{c}_{\mathcal{J}} := a_{\nu,\mathcal{J}}/N_{0,\nu}(a_{0,H_\infty^{(d)}}) \times \varphi \circ N_{0,\nu-1}(a_{0,H_\infty^{(d)}})/\varphi(a_{\nu-1,\widetilde{\mathcal{J}}}).$$

https://doi.org/10.1017/S1446788714000445 Published online by Cambridge University Press

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

THEOREM 1.1. *A collection of elements* $a_{\mathcal{J}} = a_{v,\mathcal{J}} \in \mathbb{Z}_p[\![U^{(v)}]\!]^\times$ *lies in the image of* $K_1(\mathbb{Z}_p[\![G_\infty^{(d)}]\!])$ *under the theta-map if and only if, for all positive integers m:*

(i) *the congruence* (1.1)$_{m,\underline{\mathfrak{h}}}$ *holds at each nontrivial cyclic subgroup* $\langle\underline{\mathfrak{h}}\rangle \subset H_\infty^{(d)}/p^m$*;*
(ii) *the congruence* (1.2)$_m$ *holds.*

Furthermore, the kernel of the theta-map is trivial, that is, $\prod \theta_{\mathcal{J}}$ *is an injection.*

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 [13]. Then a *necessary* set of conditions for a system of $a_{v,\mathcal{J}} \in \mathbb{Z}_p[\![U^{(v)}]\!]^\times_{\mathcal{S}_{\mathcal{J}}}$ to lie in the image of $K_1(\mathbb{Z}_p[\![G_\infty^{(d)}]\!]_{\mathcal{S}})$ under the $\mathcal{S}$-localisation of the theta-map $\prod \theta_{\mathcal{J}}$ is that the associated $\mathfrak{c}_{\mathcal{J}}$ satisfy the congruences (1.1)$_{m,\underline{\mathfrak{h}}}$ and (1.2)$_m$ for $m \geq 1$.

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

As has already occurred with the $d = 1$ situation studied in [11], 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 $O(p^{m(d-1)})$, so the system of congruences to be checked will grow rapidly with m. However, if $d = 1$, the system of congruences grows only 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 1.3. *If* $d = 2$ *and* $m = 1$*, then* (1.1)$_{m,\underline{\mathfrak{h}}}$ *and* (1.2)$_m$ *are equivalent to:*

(i) $(a_{1,\langle\underline{\mathfrak{h}}\rangle})^p \equiv N_{0,1}(a_{0,H_\infty^{(d)}})^p \bmod p^2$*; and*
(ii) $\prod_{\mathcal{J},[H_\infty^{(d)}:\mathcal{J}]=p} (a_{1,\mathcal{J}})^p \equiv N_{0,1}(a_{0,H_\infty^{(d)}})^{p(p+1)} \bmod p^3$*, 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 1.4. 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 $h^1(E) \otimes \tau$ through

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

which is $\mathbb{Q}(\tau)$-rational by a result of Bouganis and Dokchitser [2, Theorem 4.2].

https://doi.org/10.1017/S1446788714000445 Published online by Cambridge University Press

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 [6, Theorem 1.1].

THEOREM 1.5. *Each character $\chi : H_\infty^{(d)} \twoheadrightarrow \mu_{p^v} \hookrightarrow \mathbb{C}^\times$ extends uniquely to the group $G_{\mathbb{Q}(\mu_{p^v})}$, and there exists an element $\mathbf{L}_p(E, \mathcal{J}) \in \mathbb{Z}_p[\![U^{(v)}]\!][p^{-1}]$, with $\mathcal{J} = \mathcal{J}(\chi, v) :=$ Ker(χ), satisfying*

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

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 the $\psi \otimes \mathrm{Ind}(\chi)$, each of which is irreducible (see [17, Section 8.2] for a nice discussion of this).

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

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

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

PROPOSITION 1.6. *If the family of elements $\{\mathbf{L}_p(E, \mathcal{J})\}_{\mathcal{J}}$ belongs to $\prod \theta_{\mathcal{J}}(K_1(\mathbb{Z}_p[\![G_\infty^{(2)}]\!]_S))$, their constant terms satisfy first layer congruences:*

$$\mathcal{L}_{E,\underline{\Delta}}(\rho_{\chi_{\Delta_1}\chi_{\Delta_2}^t})^p \times \prod_{j=0}^{p-2} \mathcal{L}_{E,\underline{\Delta}}(\omega^j)^{-p} \equiv 1 \mod p^2 \quad \textit{for } t \in \{0, \ldots, p-1\}, \tag{1.6.1}$$

$$\mathcal{L}_{E,\underline{\Delta}}(\rho_{\chi_{\Delta_2}})^p \times \prod_{j=0}^{p-2} \mathcal{L}_{E,\underline{\Delta}}(\omega^j)^{-p} \equiv 1 \mod p^2 \quad \textit{and} \tag{1.6.2}$$

$$\left(\mathcal{L}_{E,\underline{\Delta}}(\rho_{\chi_{\Delta_2}}) \times \prod_{t=0}^{p-1} \mathcal{L}_{E,\underline{\Delta}}(\rho_{\chi_{\Delta_1}\chi_{\Delta_2}^t})\right)^p \times \prod_{j=0}^{p-2} \mathcal{L}_{E,\underline{\Delta}}(\omega^j)^{-p(p+1)} \equiv 1 \mod p^3. \tag{1.6.3}$$

The congruences (1.6.1)–(1.6.3) follow directly from Corollary 1.3 and Theorem 1.5, 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

$$(2,5),\quad (2,7),\quad (2,13),\quad (2,17),\quad (2,19),\quad (2,23),\quad (2,31),\quad (2,37),$$
$$(2,41),\quad (5,7),\quad (5,13),\quad (5,17),\quad (5,19),\quad (5,23),\quad (7,13),\quad (7,17);$$

https://doi.org/10.1017/S1446788714000445 Published online by Cambridge University Press

- the elliptic curve $E = 77C1$, the prime $p = 3$ and (Δ_1, Δ_2) in the list

$$(2,5), \quad (2,13), \quad (5.13);$$

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

The L-values themselves are calculated in Section 6 using the MAGMA package. We should point out that the *LSeries* routine can take a very long time to run, especially if the conductor of the motive $h^1(E) \otimes \rho$ is large; in total these four examples represent six months worth of computation. 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 article. In Sections 2 and 3 we define the additive version of the theta-map, and describe its image fully using trace relations. Then in Section 4 we follow the method of Kakde *et al.*, relating the multiplicative and additive worlds via the Taylor–Oliver logarithm. The proof of Theorem 1.1 is completed in Section 5. Lastly, Section 6 focuses on applications to L-functions of modular elliptic curves, in particular the verification of (1.6.1)–(1.6.3) for the examples mentioned above, as well as the proofs of Theorem 1.5 and Proposition 1.6.

2. The combinatorics of $G_\infty^{(d)}$-representations

Throughout, we adopt the convention that $(1 + p^0\mathbb{Z})/(1 + p^n\mathbb{Z})$ indicates the group $(\mathbb{Z}/p^n\mathbb{Z})^\times$. Let us consider the finite semidirect products

$$G_n^{(d)} := (\mathbb{Z}/p^n\mathbb{Z})^\times \ltimes (\mathbb{Z}/p^n\mathbb{Z})^{\oplus d} = \Sigma_n \ltimes H_n^{(d)} \quad \text{say},$$

where $d \geq 1$ is a fixed integer. Consequently, $G_\infty^{(d)} \cong \lim_{\longleftarrow n} G_n^{(d)}$ and $H_\infty^{(d)} \cong \lim_{\longleftarrow n} H_n^{(d)}$.

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

We start by discussing some basic representation theory of the finite group $G_n^{(d)}$. For an element $\underline{\alpha} \in (\mathbb{Z}/p^n\mathbb{Z})^{\oplus d}$, consider the associated character $\chi_{\underline{\alpha}} : H_n^{(d)} \longrightarrow \mathbb{C}^\times$ given by

$$\chi_{\underline{\alpha}}(h_1, \ldots, h_d) := \exp\left(\frac{2\pi\sqrt{-1}}{p^n} \times \sum_{j=1}^{d} \alpha_j h_j\right) \quad \text{for all } \underline{h} = (h_1, \ldots, h_d) \in H_n^{(d)}.$$

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

https://doi.org/10.1017/S1446788714000445 Published online by Cambridge University Press

THEOREM 2.1.

(i) *If* $\chi : H_n^{(d)} \twoheadrightarrow \mu_{p^{\mathfrak{f}_\chi}}$, *then* $\mathrm{Stab}_{\Sigma_n}(\chi) = (1 + p^{\mathfrak{f}_\chi}\mathbb{Z})/(1 + p^n\mathbb{Z})$.

(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*

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

where $\psi : \Sigma_n \to \mathbb{C}^\times$ *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. Part (i) follows easily from the description of the stabiliser subgroup as

$$\mathrm{Stab}_{\Sigma_n}(\chi_{\underline{\alpha}}) = \{\sigma \in \Sigma_n \mid \chi_{\underline{\alpha}}(\sigma \underline{h} \sigma^{-1}) = \chi_{\underline{\alpha}}(\underline{h}) \text{ for all } \underline{h} \in H_n^{(d)}\}$$

and the fact that $\chi_{\underline{\alpha}}(\sigma \underline{h} \sigma^{-1}) = \chi_{\sigma \underline{\alpha}}(\underline{h})$. Parts (ii)–(iv) are a corollary of [17, Proposition 25]. □

Since the irreducible representations are already completely determined, let us now compute the cardinalities of the various objects occurring in the theorem above.

PROPOSITION 2.2.

(a) *In the previous notation,* $\#\mathrm{Stab}_{\Sigma_n}(\chi) = \phi(p^n)/\phi(p^{\mathfrak{f}_\chi})$ *and* $\dim_{\mathbb{C}}(\rho_n^{(d)}(\chi, \psi)) = \phi(p^{\mathfrak{f}_\chi})$.

(b) *For a fixed* $\mathfrak{f}_\chi \geq 1$, *there are exactly*

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

nonisomorphic irreducible representations $\rho_n^{(d)}(\chi, \psi)$ *induced from the subgroup* $(1 + p^{\mathfrak{f}_\chi})/(1 + p^n\mathbb{Z}) \ltimes H_n^{(d)}$.

PROOF. The statement (a) is an immediate consequence of the index formula

$$\dim_{\mathbb{C}}(\mathrm{Ind}_{\mathrm{Stab}_{\Sigma_n}(\chi) \ltimes H_n^{(d)}}^{G_n^{(d)}} (\chi^\dagger \otimes \psi)) = [G_n^{(d)} : \mathrm{Stab}_{\Sigma_n}(\chi) \ltimes H_n^{(d)}] = \frac{\#\Sigma_n}{\#\mathrm{Stab}_{\Sigma_n}(\chi)}.$$

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,

$$\begin{aligned} \#\text{reps of the form } \rho_n^{(d)}(\chi, \psi) &\overset{\text{by 2.1(iv)}}{=} \frac{\#\{\text{chars } \chi : H_n^{(d)} \twoheadrightarrow \mu_{p^{\mathfrak{f}_\chi}}\}}{\#(\mathbb{Z}/p^{\mathfrak{f}_\chi}\mathbb{Z})^\times} \times \#\mathrm{Stab}_{\Sigma_n}(\chi) \\ &\overset{\text{by 2.2(a)}}{=} \frac{(p^{\mathfrak{f}_\chi})^d - (p^{\mathfrak{f}_\chi - 1})^d}{\phi(p^{\mathfrak{f}_\chi})} \times \frac{\phi(p^n)}{\phi(p^{\mathfrak{f}_\chi})}. \end{aligned}$$

Note here that 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 set $\{\chi_{a\underline{\alpha}} \mid a \in (\mathbb{Z}/p^{\mathfrak{f}_\chi}\mathbb{Z})^\times\}$. □

https://doi.org/10.1017/S1446788714000445 Published online by Cambridge University Press

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 $\mathbb{Z}_p[\mathrm{Conj}(G_n^{(d)})]$.

Lemma 2.3. *The* $\mathbb{Z}_p$*-rank of* $\mathbb{Z}_p[\mathrm{Conj}(G_n^{(d)})]$ *equals*

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

Proof. Assuming initially that $d \geq 1$, the size of $\mathrm{Conj}(G_n^{(d)})$ equals

$$\begin{aligned}\#\{\text{irr. reps of } G_n^{(d)}, \text{ up to IM}\} &\overset{\text{by 2.2(b)}}{=} \#\Sigma_n + \sum_{\mathfrak{f}_\chi=1}^{n} \frac{(p^{d\mathfrak{f}_\chi} - p^{d(\mathfrak{f}_\chi-1)}) \times \phi(p^n)}{\phi(p^{\mathfrak{f}_\chi})^2} \\ &= \phi(p^n) \times \left(1 + \frac{p^d-1}{(p-1)^2} \sum_{\mathfrak{f}_\chi=1}^{n} p^{(d-2)(\mathfrak{f}_\chi-1)}\right).\end{aligned}$$

The result then follows by summing up the geometric progression on the right, according to the three cases $d \geq 3$, $d = 2$ and $d = 1$. □

For each integer $m \leq n$, we now define a normal subgroup of $G_n^{(d)} = \Sigma_n \ltimes H_n^{(d)}$ by taking

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

Lemma 2.4.

(i) *The commutator subgroup* $[\mathfrak{S}_m, \mathfrak{S}_m]$ *equals* $(H_n^{(d)})^{p^m}$.

(ii) *Each quotient group* $\mathfrak{S}_m^{\mathrm{ab}} = \mathfrak{S}_m/[\mathfrak{S}_m, \mathfrak{S}_m]$ *is isomorphic to the product* $(1+p^m\mathbb{Z})/(1+p^n\mathbb{Z}) \times H_m^{(d)}$.

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

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

By construction, the trace map $\mathrm{Tr}_{G_n^{(d)}/\mathfrak{S}_m} : \mathbb{Z}_p[\mathrm{Conj}(G_n^{(d)})] \to \mathbb{Z}_p[\mathrm{Conj}(\mathfrak{S}_m)]$ averages a conjugacy class over the coset representatives of $G_n^{(d)}/\mathfrak{S}_m$; more precisely,

$$\mathrm{Tr}_{G_n^{(d)}/\mathfrak{S}_m} : [g]_{G_n^{(d)}} \mapsto \sum_{u \in G_n^{(d)}/\mathfrak{S}_m, ugu^{-1} \in \mathfrak{S}_m} [ugu^{-1}]_{\mathfrak{S}_m}.$$

Secondly, by quotienting an element of $\mathfrak{S}_m$ modulo $[\mathfrak{S}_m, \mathfrak{S}_m]$, one induces a map

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

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

Definition 2.5.

(a) We can now build the mth level of the additive theta-map

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

by taking the composition $\theta_m^+([g]) := \mathrm{Tr}_{G_n^{(d)}/\mathfrak{S}_m}([g]) \bmod [\mathfrak{S}_m, \mathfrak{S}_m]$.

(b) Extending each character $\chi : H_m^{(d)} \twoheadrightarrow \mu_{p^m}$ to the ring $\mathbb{Z}_p[(1+p^m\mathbb{Z})/(1+p^n\mathbb{Z})][H_m^{(d)}]$,

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

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

Notation. We 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

$$\nu_m(\underline{h}) = \min\{t \geq 0 \mid \underline{h}^{p^t} \in (H_n^{(d)})^{p^m}\}.$$

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 that $\nu_m(\underline{h}) = \max\{\nu_{m+j}(\underline{h}) - j, 0\}$ when $j \leq n - m$.

Proposition 2.6. *Let* $\mathcal{A}_{H_m^{(d)}}\langle\underline{\mathfrak{h}}\rangle := \sum_{\underline{z}\in\langle\underline{\mathfrak{h}}\rangle, \langle\underline{z}\rangle=\langle\underline{\mathfrak{h}}\rangle}[\underline{z}] \in \mathbb{Z}_p[H_m^{(d)}]$ *for each* $\underline{\mathfrak{h}} \in H_m^{(d)}$*; then:*

(i)

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

(ii)

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

https://doi.org/10.1017/S1446788714000445 Published online by Cambridge University Press

Proof. Let $g = \sigma \cdot \underline{h}$ be an arbitrary element of $G_n^{(d)}$. Since $G_n^{(d)}/\mathfrak{S}_m \cong (\mathbb{Z}/p^m\mathbb{Z})^\times$, a simple calculation reveals that

$$\mathrm{Tr}_{G_n^{(d)}/\mathfrak{S}_m}([g]_{G_n^{(d)}}) = \begin{cases} \sum_{u \in (\mathbb{Z}/p^m\mathbb{Z})^\times} [\sigma \cdot (u\underline{h})]_{\mathfrak{S}_m} & \text{if } \sigma \equiv 1 \mod p^m, \\ 0 & \text{if } \sigma \not\equiv 1 \mod p^m. \end{cases}$$

Suppose now that $\sigma \equiv 1 \bmod p^m$. Reducing the above equation modulo $[\mathfrak{S}_m, \mathfrak{S}_m]$, one quickly deduces that

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

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

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

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

whose proof is a straightforward exercise in cyclotomy. □

Corollary 2.7. *The image of θ_m^+ is naturally a free $\mathbb{Z}_p[(1 + p^m\mathbb{Z})/(1 + p^n\mathbb{Z})]$-module, and*

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

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

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

The stated formula is a direct consequence of evaluating this geometric progression.

For instance, if $0 \leq m \leq n$ and $\Sigma' = (1 + p^m\mathbb{Z})/(1 + p^n\mathbb{Z})$, then

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

where the set

$$\mathcal{S}_m^{(\mathcal{A})} := \{\phi(p^m) \cdot \mathrm{id}_{H_m^{(d)}}\} \cup \{p^{m-\nu_m(\underline{\mathfrak{h}})} \cdot \mathcal{A}_{H_m^{(d)}}\langle \underline{\mathfrak{h}} \rangle \mid 0 \neq \langle \underline{\mathfrak{h}} \rangle < H_m^{(d)}\}. \quad □$$

https://doi.org/10.1017/S1446788714000445 Published online by Cambridge University Press

REMARKS.

(i) To illustrate what happens in the familiar false-Tate situation $d = 1$, by Corollary 2.7 the rank of $\mathrm{Im}\,(\theta_m^+)$ grows linearly with m, while θ_0^+ is a surjection. Therefore, to recover $\mathbb{Z}_p[\mathrm{Conj}(G_n^{(1)})]$ 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 [11, 12], Kato provided 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 $\lim_{\longleftarrow n} G_n^{(d)}$.

(iii) For general $d \geq 1$, a necessary condition for a sequence $\{y_m\}_m \in \prod_{m=0}^n \mathbb{Z}_p[\mathfrak{S}_m^{\mathrm{ab}}]$ to originate from an element $x \in \mathbb{Z}_p[\mathrm{Conj}(G_n^{(d)})]$ under $\prod_{m=0}^n \theta_m^+$ is given by the following lemma.

LEMMA 2.8. *If $y_m = \theta_m^+(x)$ for each $m \in \{0, \dots, n\}$, then one obtains relations*

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

that is, 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 $\sigma \not\equiv 1 \bmod p^m$, both of the terms are zero. If $\sigma \equiv 1 \bmod p^m$, then, by Proposition 2.6(i),

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

whilst

$$y_m = \phi(p^m)[\sigma]_{(1+p^m\mathbb{Z})/(1+p^n\mathbb{Z})} \times \frac{1}{\phi(p^{\nu_m(\underline{h})})}\mathcal{A}_{H_m^{(d)}}\langle\overline{\underline{h}}\rangle.$$

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

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

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

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

together with the fact that

$$\nu_m(\underline{h}) = 1 + \nu_{m-1}(\underline{h}) > 1 \implies \phi(p^{\nu_m(\underline{h})}) = p \times \phi(p^{\nu_{m-1}(\underline{h})}). \qquad \square$$

https://doi.org/10.1017/S1446788714000445 Published online by Cambridge University Press

3. The additive setting (I): describing the image of Θ^+

This trace compatibility is not only necessary for a sequence to belong to the image of the map $\prod \theta_m^+$ but it also turns out be a sufficient condition, as evidenced below. In fact, the remainder of this section is devoted to establishing the following result.

THEOREM 3.1. *Defining*

$$\Psi_n^{(d)} := \{\{y_m\}_{0\le m\le n} \text{ such that } \mathrm{Tr}(y_{m-1}) \equiv y_m\}$$

to be the $\mathbb{Z}_p$-submodule of

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

consisting of trace-compatible elements, there is an isomorphism

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

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

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

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

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

LEMMA 3.2. *The conjugacy classes in $G_n^{(d)}$ are represented by the sets*

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

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 $p^{\mathrm{ord}_p(\sigma-1)}$.*

PROOF. It is beneficial to realise each element $g = \sigma\cdot\underline{h} \in \Sigma_n \ltimes H_n^{(d)}$ as a matrix $\begin{pmatrix} \sigma & \dots & 0 & h_1 \\ \vdots & & \vdots & \vdots \\ 0 & \dots & \sigma & h_d \\ 0 & \dots & 0 & 1 \end{pmatrix} \in \mathrm{GL}(d+1, \mathbb{Z}/p^n\mathbb{Z})$. Indeed, if $k = \kappa\cdot\underline{t}$,

https://doi.org/10.1017/S1446788714000445 Published online by Cambridge University Press

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

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

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

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

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

which (after some manipulation) can be shown to equal the formula in Lemma 2.3. □

Corollary 3.3.

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

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

https://doi.org/10.1017/S1446788714000445 Published online by Cambridge University Press

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

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

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

Proof. The first statement follows because, by Lemma 3.2, the conjugacy classes of $G_n^{(d)}$ are indexed by pairs $(\sigma, \langle \overline{h} \rangle)$, where each $\sigma \in \Sigma_n = \bigcup_{\nu=0}^{n} (1 + p^\nu\mathbb{Z})/(1 + p^n\mathbb{Z}) - (1 + p^{\nu+1}\mathbb{Z})/(1 + p^n\mathbb{Z})$ and, additionally, $\langle \overline{h} \rangle < H_\nu^{(d)}$ generates a cyclic subgroup of size p^r with $0 \le r \le \nu$. The second statement is easy, as $\mathrm{Im}(\theta_m^+)$ is generated over $\mathbb{Z}_p[(1 + p^m\mathbb{Z})/(1 + p^n\mathbb{Z})]$ by $\mathcal{S}_m^{(\mathcal{A})}$. □

The proof of Theorem 3.1. There are precisely two assertions we need to establish, namely the injectivity of $\prod \theta_m^+ : \mathbb{Z}_p[\mathrm{Conj}(G_n^{(d)})] \longrightarrow \prod_{m=0}^{n} \mathbb{Z}_p[\mathfrak{S}_m^{\mathrm{ab}}]$ 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 that 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 2.1(iii), all irreducible characters are of the form $\widetilde{\rho} = \mathrm{Tr}(\rho_n^{(d)}(\chi, \psi))$, 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,

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

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 $\mathbb{Q}$-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 $y_m \in \mathbb{Z}_p[\mathfrak{S}_m^{\mathrm{ab}}]$.

Lemma 3.4. *Let* $\{y_m\}_{0 \le m \le n} \in \Psi_n^{(d)}$ *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* $m \ge 0$ *and* $k \in \{1, \ldots, n - m\}$,

$$\alpha_{\sigma,m} = \alpha_{\sigma,m+k} + \sum_{r=1}^{k} \sum_{\substack{\langle \underline{\mathfrak{h}}^\dagger \rangle < H_{m+k}^{(d)} \\ \#\langle \underline{\mathfrak{h}}^\dagger \rangle = p^r}} \beta_{\sigma,\langle \underline{\mathfrak{h}}^\dagger \rangle,r,m+k}, \qquad (3.4.1)_{m,k}$$

$$\beta_{\sigma,\langle \underline{\mathfrak{h}} \rangle,r,m} = \sum_{\substack{\langle \underline{\mathfrak{h}}^\dagger \rangle < H_{m+k}^{(d)}, \\ \langle \underline{\mathfrak{h}}^\dagger \rangle + p^m \equiv \langle \underline{\mathfrak{h}} \rangle}} \beta_{\sigma,\langle \underline{\mathfrak{h}}^\dagger \rangle,r+k,m+k} \quad \textit{for all } \langle \underline{\mathfrak{h}} \rangle < H_m^{(d)} \quad \textit{with } \#\langle \underline{\mathfrak{h}} \rangle = p^r. \qquad (3.4.2)_{m,k}$$

https://doi.org/10.1017/S1446788714000445 Published online by Cambridge University Press

Proof. Let us suppose that $m \geq 1$. A short computation involving the trace map shows that

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

On the other hand, the element y_m is equal to

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

as a congruence modulo $(H^{(d)}_m)^{p^{m-1}}$.

Remarks.

(a) By assumption, each $\mathrm{Tr}(y_{m-1}) \equiv y_m \bmod (H^{(d)}_m)^{p^{m-1}}$; furthermore, the linear independence of $[\mathrm{id}]_{H^{(d)}_{m-1}}$ and the $\mathcal{A}_{H^{(d)}_{m-1}}\langle\underline{\mathfrak{h}}\rangle$ over $\mathbb{Z}_p[(1+p^m\mathbb{Z})/(1+p^n\mathbb{Z})]$ implies

https://doi.org/10.1017/S1446788714000445 Published online by Cambridge University Press

that

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

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

which are none other than Equations $(3.4.1)_{m,k}$ and $(3.4.2)_{m,k}$, respectively.

(b) A straightforward inductive argument shows that the general equation $(3.4.1)_{m,k}$ follows by combining $(3.4.\star)_{m,m+1}, (3.4.\star)_{m+1,m+2}, \ldots, (3.4.\star)_{m+k-1,m+k}$ together.

(c) An identical induction works for the second set of equations, so we are done.

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 $x \in \mathrm{Conj}(G_n^{(d)})$ by

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

Then, repeatedly applying Proposition 2.6(i), at each $m \in \{0, \ldots, n\}$,

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

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

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

and

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

Substituting in Equations $(3.4.1)_{m,k}$ and $(3.4.2)_{m,k}$ with $k = \nu - m$ yields

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

Therefore, we can simplify our expression for $\theta^+_m(x)$, which neatly collapses down to

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

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

4. The multiplicative setting

To translate back from the additive to the multiplicative world, one employs the method of Kakde *et al.* [4, 9, 10]. We begin with some short background on the logarithm map over group algebras.

Let G be an arbitrary finite group (not necessarily a p-group) and $\mathcal{O}$ a complete discrete valuation ring unramified at p. We use the notation Frob_p for the Frobenius automorphism on $\mathcal{O}$, and write $\varphi_G : \mathrm{Frac}(\mathcal{O})[\mathrm{Conj}(G)] \to \mathrm{Frac}(\mathcal{O})[\mathrm{Conj}(G)]$ to denote the map sending $\sum_g k_g[g]_G$ to the group ring element $\sum_g \mathrm{Frob}_p(k_g)[g^p]_G$.

The Taylor–Oliver logarithm $\Gamma_G : K_1(\mathcal{O}[G]) \to \mathcal{O}[\mathrm{Conj}(G)]$ is defined by the formula

$$\Gamma_G(x) := \log_{\mathcal{O}[G]}(x) - \frac{1}{p}\varphi_G(\log_{\mathcal{O}[G]}(x)),$$

where $\log_{\mathcal{O}[G]}$ indicates the unique extension of

$$\log_{\mathrm{Jac}(\mathcal{O}[G])} : K_1(\mathcal{O}[G], \mathrm{Jac}(R[G])) \longrightarrow \frac{\mathrm{Jac}(\mathcal{O}[G]) \otimes \mathbb{Q}}{[\mathcal{O}[G] \otimes \mathbb{Q}, \mathcal{O}[G] \otimes \mathbb{Q}]}$$

to the full K-group $K_1(\mathcal{O}[G])$ (we refer the reader to Oliver [14] for further details). Throughout this article, we will take $\mathcal{O} = \mathbb{Z}_p$, and need only consider subquotients G of the finite group $G^{(d)}_n \cong \Sigma_n \ltimes H^{(d)}_n$.

The following construction mimics the additive theta-maps in Definition 2.5.

Definition 4.1.

(a) If $m \le n$, we build the mth-level multiplicative theta-map

$$\theta_m : K_1(\mathbb{Z}_p[G^{(d)}_n]) \longrightarrow K_1(\mathbb{Z}_p[\mathfrak{S}^{\mathrm{ab}}_m]) \cong \mathbb{Z}_p[\mathfrak{S}^{\mathrm{ab}}_m]^\times$$

https://doi.org/10.1017/S1446788714000445 Published online by Cambridge University Press

by forming the composition $\theta_m(z) := \mathrm{Nr}_{G_n^{(d)}/\mathfrak{S}_m}(z) \bmod [\mathfrak{S}_m, \mathfrak{S}_m]$, where we have written $\mathrm{Nr}_{G_n^{(d)}/\mathfrak{S}_m} : K_1(\mathbb{Z}_p[G_n^{(d)}]) \to K_1(\mathbb{Z}_p[\mathfrak{S}_m])$ 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 nonnormal subgroup of $G_n^{(d)}$, and thus induces a map $\iota_* : K_1(\mathbb{Z}_p[\Sigma_n]) \to K_1(\mathbb{Z}_p[G_n^{(d)}])$. Moreover, the projection

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

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) and hence our claim is true.

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

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

where the complementary subgroup

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

REMARKS.

(i) For $m \le n$, we write $N_{0,m}$ as an abbreviation for the homomorphism

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

induced from the norm map on group algebras.

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

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

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

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

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

(iv) Lastly, for all $x \in K_1(\mathbb{Z}_p[G_n^{(d)}])$, one easily checks the identities

$$\underline{\mathrm{tw}}_n\Big(\prod \theta_m(x)\Big) = \underline{\mathrm{tw}}_n\Big(\prod \theta_m(x^{\dagger})\Big) \quad \text{and} \quad \underline{\mathrm{tw}}_n\Big(\prod \theta_m(x^{\mathrm{cy}})\Big) = (1, \dots, 1)$$

(in fact, the second identity implies the first).

https://doi.org/10.1017/S1446788714000445 Published online by Cambridge University Press

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

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

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 $\underline{\log}^{\dagger}_n : \{1\} \times \prod_{m=1}^n K_1(\mathbb{Z}_p[\mathfrak{S}^{\mathrm{ab}}_m]) \longrightarrow \{0\} \times \prod_{m=1}^n \mathbb{Q}_p[\mathfrak{S}^{\mathrm{ab}}_m]$ is then defined to be

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

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

$$\Omega^{(d)}_{n,\mathrm{cy}} := \{(\ldots, \tau_* N_{0,m}(z), \ldots)_{0 \leq m \leq n}, \text{ where } z \in \mathbb{Z}_p[\Sigma_n]^{\times}\},$$
$$\Omega^{(d)}_{n,\dagger} := \left\{\underline{z} \in \{1\} \times \prod_{m=1}^{n} 1 + p\mathbb{Z}_p[\mathfrak{S}^{\mathrm{ab}}_m] \text{ such that } \underline{\log}^{\dagger}_n \circ \underline{\mathrm{tw}}_n(\underline{z}) \in \Psi^{(d)}_n\right\}$$

and write $\Omega^{(d)}_n \subset \prod_{m=0}^n K_1(\mathbb{Z}_p[\mathfrak{S}^{\mathrm{ab}}_m])$ 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 [4, Proposition 4.1].

Theorem 4.3. *For each integer $n \geq 1$, there is a commutative diagram*

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

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

Thus, the question as to whether a vector $\underline{z}$ arises from an element of $K_1(\mathbb{Z}_p[G^{(d)}_n])$ under $\prod \theta_m$ reduces to establishing whether $\underline{\mathrm{tw}}_n(\underline{z})$ belongs to $\Omega^{(d)}_n = \mathrm{Im}(\prod \theta_m)$, which in turn is equivalent to checking if $\underline{\log}^{\dagger}_n \circ \underline{\mathrm{tw}}_n(\underline{z})$ lies in $\Psi^{(d)}_n = \mathrm{Im}\,(\prod \theta^{+}_m)$.

The proof of the above theorem is lengthy and will occupy the rest of this section.

https://doi.org/10.1017/S1446788714000445 Published online by Cambridge University Press

4.1. 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 4.4.

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

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

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

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

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

$$\theta_m^+ \circ \varphi_{G_n^{(d)}}(y) \overset{\text{by 2.6(i)}}{=} \begin{cases} [\sigma^p]_{(1+p^m\mathbb{Z})/(1+p^n\mathbb{Z})} \times \displaystyle\sum_{u \in (\mathbb{Z}/p^m\mathbb{Z})^\times} [u\underline{h}^{p}]_{H_m^{(d)}} & \text{if } \sigma^p \equiv 1 \mod p^m, \\ 0 & \text{otherwise.} \end{cases}$$

On the other hand,

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

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

$$\theta_1^+ \circ \varphi_{G_n^{(d)}}(y) \overset{\text{by 2.6(i)}}{=} \begin{cases} [\sigma^p]_{(1+p\mathbb{Z})/(1+p^n\mathbb{Z})} \times (p-1)[\mathrm{id}]_{H_1^{(d)}} & \text{if } \sigma^p \equiv 1 \mod p, \\ 0 & \text{otherwise.} \end{cases}$$

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

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

which means that both quantities above coincide. □

https://doi.org/10.1017/S1446788714000445 Published online by Cambridge University Press

LEMMA 4.5.

(a) *The mutually inverse maps* $\log\colon 1+p\mathbb{Z}_p[\mathfrak{S}_m^{\mathrm{ab}}] \xrightarrow{\sim} p\mathbb{Z}_p[\mathfrak{S}_m^{\mathrm{ab}}]$ *and* $\exp\colon p\mathbb{Z}_p[\mathfrak{S}_m^{\mathrm{ab}}] \xrightarrow{\sim} 1+p\mathbb{Z}_p[\mathfrak{S}_m^{\mathrm{ab}}]$ *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*

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

induced by the p*-adic logarithm.*

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

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

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 it is simple to show that

$$\mathfrak{a}_{\underline{\mathfrak{h}}_1}\times\mathfrak{a}_{\underline{\mathfrak{h}}_2}=\sum_{t\in(\mathbb{Z}/p^m\mathbb{Z})^\times}\mathfrak{a}_{\underline{\mathfrak{h}}_1\underline{\mathfrak{h}}_2^t}$$

upon expressing each $\mathfrak{a}_{\underline{\mathfrak{h}}_j}$ as the sum $\sum_{s\in(\mathbb{Z}/p^m\mathbb{Z})^\times}[\underline{\mathfrak{h}}_j^s]_{H_m^{(d)}}$.

In particular, the image of θ_m^+ is generated over $\mathbb{Z}_p[\Sigma']$ by the finite set of the $\mathfrak{a}_{\underline{\mathfrak{h}}}$ (which are closed under multiplication) and 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 in [4, bottom of page 106].

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

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

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

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

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

where $\mathcal{T}_N = \langle \underline{\mathfrak{h}}_1 \rangle_{\mathrm{gen}} \langle \underline{\mathfrak{h}}_2 \rangle_{\mathrm{gen}} \cdots \langle \underline{\mathfrak{h}}_{N+1} \rangle_{\mathrm{gen}}$. 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 that

$$(\mathfrak{a}_{\underline{h}})^2 = \mathfrak{a}_{\underline{h}} \times \mathfrak{a}_{\underline{h}} = \sum_{t \in (\mathbb{Z}/p^m\mathbb{Z})^\times} \mathfrak{a}_{\underline{h}^{1+t}} = \sum_{\substack{t \in (\mathbb{Z}/p^m\mathbb{Z})^\times \\ p \nmid t+1}} \mathfrak{a}_{\underline{h}^{1+t}} + \sum_{\substack{t \in (\mathbb{Z}/p^m\mathbb{Z})^\times \\ p \mid t+1}} \mathfrak{a}_{\underline{h}^{1+t}}$$

$$= \sum_{\substack{t \in (\mathbb{Z}/p^m\mathbb{Z})^\times \\ p \nmid t+1}} \mathfrak{a}_{\underline{h}} + \sum_{s=1}^{p^{m-1}} \mathfrak{a}_{\underline{h}^{ps}} = (p^m - 2p^{m-1}) \times \mathfrak{a}_{\underline{h}} + \sum_{s=1}^{p^{m-1}} \mathfrak{a}_{(\underline{h}^p)^s},$$

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 that

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

because Fact 1 implies that $\mathfrak{a}_{\underline{h}} \times \mathfrak{a}_{(\underline{h}^p)^s} \equiv 0 \bmod p\ \mathrm{Im}(\theta_m^+)$ has order $((\underline{h}^p)^s) < m$. □

Proof of Fact 3. Let us write $y = \sum_{\langle \underline{h} \rangle < H_m^{(d)}} \kappa_{\langle \underline{h} \rangle} \times \mathfrak{a}_{\underline{h}}$, where each $\kappa_{\langle \underline{h} \rangle} \in \mathbb{Z}_p[\Sigma']$. Using Fermat's little theorem,

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

which implies that $y^p \in p\ \mathrm{Im}(\theta_m^+)$. Applying simple induction, one deduces that $y^i \in p^{\lfloor i/p \rfloor}\mathrm{Im}\,(\theta_m^+)$, 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 $\underline{\mathfrak{h}}_j$ has order $<p^m$, then the product must automatically lie in $p\ \mathrm{Im}(\theta_m^+)$. Without loss of generality, assume that order$(\underline{\mathfrak{h}}_j) = p^m$ for all j, in which case

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

There are precisely $(p^{md} - p^{(m-1)d})/(p^m - p^{m-1})$ cyclic subgroups of $H_m^{(d)}$ of size p^m; consequently, if $N + 1 > (p^{md} - p^{(m-1)d})/(p^m - p^{m-1})$, then at least one of the above $\langle \underline{\mathfrak{h}}_j \rangle_{\mathrm{gen}}$ 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 the $\mathfrak{a}_{\underline{\mathfrak{h}}_j}$ inside $\mathrm{Im}\,(\theta_m^+)$ not divisible by p must have length $\leq (p^{md} - p^{(m-1)d})/(p^m - p^{m-1})$. 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 4.5(b). Since $(1 + y)^{-1}$ exists, the elements in $1 + \mathrm{Im}(\theta_m^+)$ form a multiplicative group. In fact, the convergence of the formal power series $\sum_{i=1}^{\infty} ((-1)^{i+1} y^i / i)$ yields a homomorphism $\log\colon 1 + \mathrm{Im}(\theta_m^+)^n \to \mathrm{Im}\,(\theta_m^+)^n$, and we shall write

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

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

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

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 '$\overline{\log}(1 + y) \equiv 0$ implies that $y \in \mathrm{Im}(\theta_m^+)^{n+1}$'; 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 $\log(1 + y) = y + \sum_{i=2}^{\infty} ((-1)^{i+1} y^i / i)$; 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 $a_1^p / p \in \mathrm{Im}\,(\theta_m^+)$ 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 that $(-1)^{p+1} y^p / p \in \mathrm{Im}(\theta_m^+)^{n+1}$. 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 $p \nmid c$,

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

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

https://doi.org/10.1017/S1446788714000445 Published online by Cambridge University Press

Lemma 4.6. *If $m \geq 2$ and $x \in K_1(\mathbb{Z}_p[G_n^{(d)}])$, then*

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

Proof. Let us define $\mathcal{G}_{n,m} := (1+p^{m-1}\mathbb{Z})/(1+p^n\mathbb{Z}) \ltimes H_m^{(d)}$, so that $\mathcal{G}_{n,m}^p = (1+p^m\mathbb{Z})/(1+p^n\mathbb{Z}) \times (H_m^{(d)})^p$ 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

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

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

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

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 $\varphi_{\mathcal{G}_{n,m}}$, the result follows. □

4.2. A proof of Theorem 4.3. Let us start by establishing commutativity of the maps in the fundamental square. This amounts to checking for all $x \in K_1(\mathbb{Z}_p[G_n^{(d)}])$ that the required formula

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

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 $\theta_0(x^\dagger) = 1$,

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

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

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

https://doi.org/10.1017/S1446788714000445 Published online by Cambridge University Press

where the second line follows from Lemma 4.4(ii). Again $\theta_0(x^\dagger) = 1$, so the last summand is zero, whilst $\theta_1(x^{\mathrm{cy}}) = \tau_*^{(1)} \circ N_{0,1}(\theta_0(x))$; hence,

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

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

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

upon applying Lemma 4.4(i).

Now $\theta_m(x^{\mathrm{cy}}) = \tau_*^{(m)} N_{0,m}(\theta_0(x))$; thus, one deduces that $\theta_m(x^\dagger) = \theta_m(x)/\tau_* N_{0,m}(\theta_0(x))$; furthermore, $\mathrm{Tr}_{G_n^{(d)}/\mathfrak{S}_{m-1}} \circ \log = \log \circ \mathrm{Nr}_{G_n^{(d)}/\mathfrak{S}_{m-1}}$, whence

$$\begin{aligned}\theta_m^+ \circ \Gamma_{G_n^{(d)}}(x^\dagger) \quad &= \quad \log(\theta_m(x)) - \log(\tau_* N_{0,m}(\theta_0(x))) \\ &\qquad - \varphi_{(1+p^{m-1}\mathbb{Z})/(1+p^n\mathbb{Z}) \ltimes H_m^{(d)}}(\log \circ \mathrm{Nr}_{G_n^{(d)}/\mathfrak{S}_{m-1}}(x^\dagger) \bmod (H_n^{(d)})^{p^m}) \\ &\overset{\text{by } 4.6}{=} \log(\theta_m(x)) - \log(\tau_* N_{0,m}(\theta_0(x))) - \tilde{\varphi}_{\mathfrak{S}_{m-1}^{\mathrm{ab}}} \circ \log_{\mathfrak{S}_{m-1}^{\mathrm{ab}}}(\theta_{m-1}(x^\dagger)).\end{aligned}$$

Exploiting the relation $\theta_{m-1}(x^\dagger) = \theta_{m-1}(x)/\tau_* N_{0,m-1}(\theta_0(x))$ once more,

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

which is equivalent to the required formula.

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

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

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

where ι_* was the section reversing the projection θ_0, and $\mathcal{W}^\dagger$ is the complement. Since the morphism Θ maps $\iota_* K_1(\mathbb{Z}_p[\Sigma_n])$ isomorphically onto the group $\Omega_{n,\mathrm{cy}}^{(d)}$, the kernel of Θ will coincide with

$$\mathrm{Ker}(\Theta|_{\mathcal{W}^\dagger}) \overset{\text{by } 4.5}{=} \mathrm{Ker}(\underline{\log}_n^\dagger \circ \underline{\mathrm{tw}}_n \circ \Theta|_{\mathcal{W}^\dagger}) = \mathrm{Ker}(\Theta^+ \circ \Gamma_{G_n^{(d)}}|_{\mathcal{W}^\dagger}),$$

which is precisely the kernel of $\Gamma_{G_n^{(d)}}|_{\mathcal{W}^\dagger}$ because Θ^+ is injective. However, the latter is well known to equal $SK_1(\mathbb{Z}_p[G_n^{(d)}])$, so the same must be true for $\mathrm{Ker}(\Theta)$.

https://doi.org/10.1017/S1446788714000445 Published online by Cambridge University Press

Finally, as $\Theta(\iota_* K_1(\mathbb{Z}_p[\Sigma_n]) = \Omega^{(d)}_{n,\mathrm{cy}}$, we must therefore show that $\Theta(\mathcal{W}^\dagger) = \Omega^{(d)}_{n,\dagger}$. Clearly, $\Theta(\mathcal{W}^\dagger) \subset \{1\} \times \prod_{m=1}^n 1 + p\mathbb{Z}_p[\mathfrak{S}_m^{\mathrm{ab}}]$ and moreover $\Theta^+ \circ \Gamma_{G_n^{(d)}}(\mathcal{W}^\dagger) \subset \Psi_n^{(d)}$. By Lemma 4.5(a) and the commutativity of our fundamental square,

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

Conversely, every element $\underline{z} \in \Omega^{(d)}_{n,\dagger}$ can be written as $\underline{z} = \Theta(w)$ for some $w \in \mathcal{W}^\dagger$, and the proof of Theorem 4.3 is now complete.

5. The additive setting (II): evaluation at characters χ

As we have seen in the previous section, a vector $\underline{z} \in \prod_{m=0}^n \mathbb{Z}_p[\mathfrak{S}_m^{\mathrm{ab}}]^\times$ arises from an element of $K_1(\mathbb{Z}_p[G_n^{(d)}])$ 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 $(1 + p^m\mathbb{Z})/(1 + p^n\mathbb{Z})$ 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 3.1, the image of Θ^+ consists of the trace-compatible terms

$$\Psi_n^{(d)} = \{\{y_m\}_{0\le m\le n} \text{ such that } \mathrm{Tr}_{\Sigma'_{(m-1)}/\Sigma'_{(m)}}(y_{m-1}) \equiv y_m \bmod (H_m^{(d)})^{p^{m-1}}\}.$$

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 [11, Section 3].

Notation.

(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 (in fact, $\mathcal{J}_{\chi^t} = \mathcal{J}_\chi$ for all t coprime to p).

(b) At every index $v \in \{0, \ldots, m\}$, we introduce a family of subgroups

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

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 $H_m^{(d)}$; in particular, one easily checks that $\mathrm{char}_{\mathcal{J}}(\underline{\mathfrak{h}}^t) = \mathrm{char}_{\mathcal{J}}(\underline{\mathfrak{h}})$ for each t coprime to p; hence, 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 $\chi : H_m^{(d)} \to \mu_{p^\infty} \hookrightarrow \mathbb{C}_p^\times$ (for example, the ring $\mathbb{Z}_p[\mu_{p^n}]$ suffices). For each character χ on $H_v^{(d)}$ with $0 \le v \le m \le n$, if $y_m \in \mathbb{Z}_p[\Sigma'_{(m)} \times H_m^{(d)}]$, then one naturally obtains $\chi(y_m) \in \mathcal{O}[\Sigma'_{(m)}]$ by linearly extending χ to the group ring.

Question. Given a collection of $a_{m,\chi} \in \mathcal{O}[\Sigma'_{(m)}]$ with $m \le n$ and characters $\chi : H_m^{(d)} \to \mathcal{O}^\times$, 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 $\{y_m\}_m \in \Psi_n^{(d)}$?

https://doi.org/10.1017/S1446788714000445 Published online by Cambridge University Press

Let us work backwards—for the sake of argument, suppose that $\{y_m\}_{0\le m\le n} \in \Psi_n^{(d)}$ gives rise to these terms $a_{m,\chi}$ through evaluation at χ.

By Theorem 3.1, there exists $z \in \mathbb{Z}_p[\mathrm{Conj}(G_n^{(d)})]$ such that $y_m = \theta_m^+(z)$, in which case $a_{m,\chi} = \chi(y_m) = \theta_{\chi_m}^+(z)$. Moreover, upon examining Proposition 2.6(ii), we further deduce that:

- each element $\theta_{\chi_m}^+(z)$ belongs to $p^{m-1}\mathbb{Z}_p[\Sigma'_{(m)}]$, 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 $H_{m-1}^{(d)}$, then $a_{m,\chi} = \mathrm{Tr}_{\Sigma'_{(m-1)}/\Sigma'_{(m)}}(a_{m-1,\chi})$.

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

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

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

Theorem 5.1. *A sequence $(\ldots, a_{\mathcal{J}_\chi}^{(v)}, \ldots) \in \prod_{\chi: H_m^{(d)} \twoheadrightarrow \mu_{p^v}} \mathbb{Z}_p[\Sigma'_{(v)}]$ arises from a trace-compatible system lying in $\Psi_n^{(d)}$ if and only if, for all positive integers $m \le n$ and all nontrivial subgroups $\langle \underline{\mathfrak{h}} \rangle \subset H_m^{(d)}$,*

$$\mathrm{Tr}_{\Sigma'_{(0)}/\Sigma'_{(m)}}(a_{H_m^{(d)}}^{(0)}) + \sum_{v=1}^{m} \sum_{\mathcal{J}_\chi \in \mathcal{Z}_m^{(v)}} p^{v-1} \mathrm{Tr}_{\Sigma'_{(v)}/\Sigma'_{(m)}}(a_{\mathcal{J}_\chi}^{(v)}) \times (p\, \mathrm{char}_{\mathcal{J}_\chi}(\underline{\mathfrak{h}}) - \mathrm{char}_{\mathcal{J}_\chi}(\underline{\mathfrak{h}}^p)) \tag{5.1.1$_{m,\underline{\mathfrak{h}}}$}$$

is congruent to zero modulo $p^{m(d+1)-\nu_m(\underline{\mathfrak{h}})}\mathbb{Z}_p[\Sigma'_{(m)}]$, whilst at the trivial subgroup

$$p\mathrm{Tr}_{\Sigma'_{(0)}/\Sigma'_{(m)}}(a_{H_m^{(d)}}^{(0)}) + \sum_{v=1}^{m} \sum_{\mathcal{J}_\chi \in \mathcal{Z}_m^{(v)}} p^{v}(p-1)\, \mathrm{Tr}_{\Sigma'_{(v)}/\Sigma'_{(m)}}(a_{\mathcal{J}_\chi}^{(v)}) \equiv 0 \mod p^{m(d+1)}. \tag{5.1.2$_{m,\mathrm{id}}$}$$

In Section 5.2 we explain why the above result implies Theorem 1.1 in the Introduction. However, we first use properties of characteristic functions to give its demonstration.

5.1. The proof of Theorem 5.1. The initial step is to construct an inverse to the mapping $y_m \mapsto (\ldots, \chi(y_m), \ldots)$. Assume that we are given a collection of elements $a_{m,\chi} \in \mathbb{Z}_p[\Sigma'_{(m)}]$; then one defines

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

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.

https://doi.org/10.1017/S1446788714000445 Published online by Cambridge University Press

Lemma 5.2. *Providing that each $a_{m,\chi}$ depends only on* $\mathrm{Ker}(\chi) \subset H_m^{(d)}$,

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

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

Proof. Let us denote by $\mathfrak{X}_m$ the group of characters $\chi : H_m^{(d)} \longrightarrow \mathbb{C}_p^\times$, so that

$$c_{\underline{\mathfrak{h}}}^{(m)} = p^{-md} \sum_{\chi \in \mathfrak{X}_m} \chi^{-1}(\underline{\mathfrak{h}}) a_{m,\chi} = p^{-md} \sum_{\mathcal{J} \in \mathcal{Z}_m} a_{\mathcal{J}} \sum_{\substack{\chi \in \mathfrak{X}_m,\\ \mathrm{Ker}(\chi) = \mathcal{J}}} \chi^{-1}(\underline{\mathfrak{h}})$$

$$= p^{-md} \Big(a_{m,\mathbf{1}} + \sum_{\mathcal{J} \in \mathcal{Z}_m - \{H_m^{(d)}\}} a_{\mathcal{J}} \Big(\sum_{\mathrm{Ker}(\chi) \supset \mathcal{J}} \chi^{-1}(\underline{\mathfrak{h}}) - \sum_{\substack{\mathrm{Ker}(\chi) \supset \mathcal{J},\\ \mathrm{Ker}(\chi) \neq \mathcal{J}}} \chi^{-1}(\underline{\mathfrak{h}}) \Big) \Big),$$

where $a_{\mathcal{J}} = a_{m,\chi}$. However, $\sum_{\mathrm{Ker}(\chi) \supset \mathcal{J}} \chi^{-1}(\underline{\mathfrak{h}})$ will be equal to $\#H_m^{(d)} / \#\mathcal{J} \times \mathrm{char}_{\mathcal{J}}(\underline{\mathfrak{h}})$ and moreover

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

which is $\#H_m^{(d)} / \#\mathcal{J} \times (1/p)\,\mathrm{char}_{\mathcal{J}}(\underline{\mathfrak{h}}^p)$; 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 coprime 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 the image of θ_m^+ is generated over $\mathbb{Z}_p[\Sigma_m']$ by $\phi(p^m) \cdot \mathrm{id}_{H_m^{(d)}}$ and the $p^{m - \nu_m(\underline{\mathfrak{h}})} \mathcal{A}_{H_m^{(d)}} \langle \underline{\mathfrak{h}} \rangle$, 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 3.1, the full ensemble $\{Y_m\}_{0 \le m \le n}$ belongs to $\mathrm{Im}(\prod \theta_m^+)$ if and only if:

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

https://doi.org/10.1017/S1446788714000445 Published online by Cambridge University Press

To make the above conditions more explicit, we shall rewrite the coefficients $c^{(m)}_{\underline{\mathfrak{h}}}$. Let us henceforth assume that each $a_{m,\chi}$ depends only on $\mathcal{J}_\chi$, and set $a^{(m)}_{\mathcal{J}_\chi} = a_{m,\chi}$.

Decomposing $\mathcal{Z}_m$ into its constituent $\mathcal{Z}^{(\nu)}_m$,

$$\begin{aligned} c^{(m)}_{\underline{\mathfrak{h}}} &= p^{-md} a^{(m)}_{H^{(d)}_m} + \sum_{\nu=1}^{m} \sum_{\mathcal{J}_\chi \in \mathcal{Z}^{(\nu)}_m} \frac{1}{p^{md-\nu}} \times \Big(\mathrm{char}_{\mathcal{J}_\chi}(\underline{\mathfrak{h}}) - \frac{1}{p}\,\mathrm{char}_{\mathcal{J}_\chi}(\underline{\mathfrak{h}}^p)\Big) a^{(m)}_{\mathcal{J}_\chi} \\ &= p^{-md}\Big(a^{(m)}_{H^{(d)}_m} + \sum_{\nu=1}^{m} \sum_{\mathcal{J}_\chi \in \mathcal{Z}^{(\nu)}_m} p^{\nu-1} \times (p\,\mathrm{char}_{\mathcal{J}_\chi}(\underline{\mathfrak{h}}) - \mathrm{char}_{\mathcal{J}_\chi}(\underline{\mathfrak{h}}^p)) a^{(m)}_{\mathcal{J}_\chi}\Big). \end{aligned}$$

In fact, the trace compatibility $a_{m,\chi} = \mathrm{Tr}_{\Sigma'_{(m-1)}/\Sigma'_{(m)}}(a_{m-1,\chi})$ we mentioned earlier implies (via simple induction) that $a^{(m)}_{\mathcal{J}_\chi} = \mathrm{Tr}_{\Sigma'_{(\nu)}/\Sigma'_{(m)}}(a^{(\nu)}_{\mathcal{J}_\chi})$ at every $\mathcal{J}_\chi \in \mathcal{Z}^{(\nu)}_m$.

COROLLARY 5.3. *Under the assumptions of 5.2, each element $p^{md} \times c^{(m)}_{\underline{\mathfrak{h}}}$ equals*

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

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 $(5.1.1)_{m,\underline{\mathfrak{h}}}$. 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 $(5.1.2)_{m,\mathrm{id}}$.

Finally, one needs to verify that $\mathrm{Tr}_{\Sigma'_{(m-1)}/\Sigma'_{(m)}}(Y_{m-1}) \equiv Y_m$ modulo $(H^{(d)}_m)^{p^{m-1}}$. The latter task amounts to establishing the identity

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

whose proof is left as an exercise for the reader (or see [15, Section 6.1] for the full details).

5.2. The proof of Theorem 1.1. Recall from our earlier discussion that the key conditions underpinning the main result collapse down to checking whether or not $\underline{\log}^{\dagger}_n \circ \underline{\mathrm{tw}}_n(\underline{z}) \in \Psi^{(d)}_n$, which can now be tested using the p-power congruences $(5.1.1)_{m,\underline{\mathfrak{h}}}$ and $(5.1.2)_{m,\mathrm{id}}$ of Theorem 5.1.

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

$$\begin{aligned} a_{\nu,\chi} &= \chi\Big(\log_{\mathcal{O}[\mathfrak{S}^{\mathrm{ab}}_\nu]}\Big(\frac{z_\nu}{\tau_* N_{0,\nu}(z_0)} \times \frac{\tilde{\varphi}_{\mathfrak{S}^{\mathrm{ab}}_{\nu-1}}(\tau_* N_{0,\nu-1}(z_0))}{\tilde{\varphi}_{\mathfrak{S}^{\mathrm{ab}}_{\nu-1}}(z_{\nu-1})}\Big)\Big) \\ &= \log_{\mathcal{O}[\Sigma'_{(\nu)}]}\Big(\frac{\chi(z_\nu)}{N_{0,\nu}(z_0)} \times \frac{\varphi_{\Sigma'_{\nu-1}}(N_{0,\nu-1}(z_0))}{\varphi_{\Sigma'_{\nu-1}}(\chi^p(z_{\nu-1}))}\Big) = \log_{\mathcal{O}[\Sigma'_{(\nu)}]}(\mathfrak{c}_{\nu,\chi}) \text{ say.} \end{aligned}$$

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

REMARKS.

(a) Substituting these $a_{\nu,\chi}$ into the left-hand side of (5.1.1)$_{m,\underline{\mathfrak{h}}}$,

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

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

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

(b) Analogously, substituting the elements $a_{\nu,\chi}$ into (5.1.2)$_{m,\mathrm{id}}$ instead,

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

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

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

It only remains therefore to pass from $K_1(\mathbb{Z}_p[G_n^{(d)}])$ to the projective limit over n. The procedure is identical to that described in Sujatha's article in [4, pages 23–50]. Firstly, the identification $\mathbb{Z}_p[\![G_\infty^{(d)}]\!] \cong \lim_{\leftarrow n} \mathbb{Z}_p[G_n^{(d)}]$ extends to yield isomorphisms

$$K_1(\mathbb{Z}_p[\![G_\infty^{(d)}]\!]) \cong \varprojlim_n K_1(\mathbb{Z}_p[G_n^{(d)}]) \quad \text{and} \quad K'_1(\mathbb{Z}_p[\![G_\infty^{(d)}]\!]) \cong \varprojlim_n K'_1(\mathbb{Z}_p[G_n^{(d)}]),$$

where K'_1 denotes the quotient of K_1 by SK_1. Applying Theorem 4.3, the diagram

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

https://doi.org/10.1017/S1446788714000445 Published online by Cambridge University Press

commutes and, taking $\lim_{\longleftarrow n}$, yields a Θ-mapping between $K_1(\mathbb{Z}_p[\![G_\infty^{(d)}]\!])$ and $\Omega_\infty^{(d)}$. Finally, the kernel of this Θ-homomorphism is $SK_1(\mathbb{Z}_p[\![G_\infty^{(d)}]\!])$, which can be easily seen to vanish upon using [14, Proposition 12.7].

The proof of our main theorem is now complete.

6. An application to elliptic curves

Our initial task is to prove the two results mentioned at the end of the Introduction. We first recall the situation of Section 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 $\mathrm{d}x_\nu$.

(If $F = \mathbb{Q}$, one sets $\epsilon(\rho) = \epsilon_{\mathbb{Q}}(\rho, 0)$ and $\epsilon_p(\rho) = \epsilon_{\mathbb{Q}_p}(\rho_p, \varpi_p, \mathrm{d}x_p; 0)$.)

The Artin L-function attached to ρ is then given by an Euler product

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

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

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

The proof of Theorem 1.5. We begin by making the following three assertions:

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

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

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

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

(c) for each rational prime l dividing $\underline{\Delta}$, there exists an element $\Phi_l(E, \tau_\chi) \in \mathbb{Z}_p[U^{(\nu)}]$ satisfying

$$\psi(\Phi_l(E, \tau_\chi)) = \iota_p\Big(\prod_{\nu\mid l} L_\nu(E, \psi \otimes \tau_\chi, 1)\Big)$$

at all such ψ above.

https://doi.org/10.1017/S1446788714000445 Published online by Cambridge University Press

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

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

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

It therefore remains to prove these statements. Beginning with the claim (a), the character χ extends to a character on $\mathrm{Stab}_{\Sigma_n}(\chi) \ltimes H_n^{(d)}$ by Theorem 2.1(ii), where n is any chosen integer $\geq \nu$. The latter group is precisely $(1 + p^\nu\mathbb{Z})/(1 + p^n\mathbb{Z}) \ltimes H_\infty^{(d)}/p^n$; hence, taking the projective limit over n, we naturally obtain a character on the group $(1 + p^\nu\mathbb{Z}_p) \ltimes H_\infty^{(d)} \cong \mathrm{Gal}(\mathbb{Q}_{\infty,\Delta}^{(d)}/\mathbb{Q}(\mu_{p^\nu}))$. Moreover, the induced representation down to $\mathbb{Q}$ has degree $[\mathbb{Q}(\mu_{p^\nu}) : \mathbb{Q}] = \phi(p^\nu)$, and is irreducible by Theorem 2.1(iii).

In order to establish (b), observe that χ yields a Hecke character over $\mathbb{Q}(\mu_{p^\nu})$; by the work of Serre, there is a corresponding parallel weight-one Hilbert modular form $\mathbf{g}$ over $\mathbb{Q}(\mu_{p^\nu})^+$, whose L-series coincides with that attached to $\mathrm{Ind}_{\mathbb{Q}(\mu_{p^\nu})}^{\mathbb{Q}(\mu_{p^\nu})^+}(\chi)$. Associated to E is a classical cusp form $f_E \in \mathcal{S}_2(\Gamma_0(N_E))$, and its base change $\mathbf{f}$ to the totally real subfield $\mathbb{Q}(\mu_{p^\nu})^+$ has parallel weight-two and square-free conductor. The proof of [6, Theorem 1.1] then yields a $\mathbb{C}_p$-valued bounded measure on $U^{(\nu)}$, 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 $v \mid \Delta$, we form the polynomial

$$\mathrm{Pol}_v(x) := \det(1 - x \cdot \mathrm{Frob}_v^{-1} \mid (H^1_{\text{ét}}(E_{\overline{\mathbb{Q}}}, \mathbb{Z}_p(1)) \otimes V_p(\tau_\chi))^{I_v}),$$

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

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

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

The proof of Proposition 1.6. Let us assume that the elements $a_{\nu,\mathcal{J}} = \mathbf{L}_p(E, \mathcal{J})$ satisfy the nonabelian congruences. From Corollary 1.3:

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

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

Any character on $H_\infty^{(2)}$ is of the form $\chi_{\Delta_1}^s \chi_{\Delta_2}^t$ for appropriately chosen integers s and t. If we take as representatives

$$\mathcal{T} := \{\chi_{\Delta_1}\chi_{\Delta_2}^t \text{ with } 0 \leq t \leq p - 1\} \cup \{\chi_{\Delta_2}\},$$

every subgroup $\mathcal{J} \in \mathcal{Z}_\infty^{(1)}$ of index p in $H_\infty^{(2)}$ arises as the kernel of χ for some $\chi \in \mathcal{T}$.

https://doi.org/10.1017/S1446788714000445 Published online by Cambridge University Press

Therefore, it is sufficient to check (i) at characters in $\mathcal{T}$, that is, to check:

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

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

Evaluating the above pair at the trivial character $\psi = \mathbf{1}$ and applying Theorem 1.5, one obtains the congruences (1.6.1) and (1.6.2), respectively.

Focusing now on condition (ii), the product over subgroups $\mathcal{J} \in \mathcal{Z}^{(1)}_\infty$ with $[H^{(2)}_\infty : \mathcal{J}] = p$ 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)′ $\prod_{\chi\in\mathcal{T}} \mathbf{L}_p(E, \mathrm{Ker}(\chi))^p \equiv N_{0,1}(\mathbf{L}_p(E, H^{(2)}_\infty))^{p(p+1)} \bmod p^3$.

Lastly, evaluating at $\psi = \mathbf{1}$ and applying Theorem 1.5 again, the final congruence (1.6.3) falls out immediately.

The proof of the proposition is complete. □

6.1. Numerical results for $d = 2$ and $n = 1$. Recall that each representation $\rho_{\chi^s_{\Delta_1}\chi^t_{\Delta_2}} = \mathrm{Ind}^{\mathbb{Q}}_{\mathbb{Q}(\mu_p)}(\chi^s_{\Delta_1}\chi^t_{\Delta_2})$ was of degree $p-1$. The goal is to numerically verify the congruences (1.6.1)–(1.6.3) in Proposition 1.6, but, due to computational limitations, these are only checked for $p = 3$ and $p = 5$. We have tabulated the following L-value information in Tables 1, 2, 3 and 4:

$$\bullet\; L^* = L^*(E, \rho_{\chi^s_{\Delta_1}\chi^t_{\Delta_2}}) := \left| \frac{L(E, \rho_{\chi_{\Delta_1^s}\chi_{\Delta_2^t}}, 1) \times \sqrt{\mathrm{disc}_{\mathbb{Q}((\Delta_1^s\Delta_2^t)^{1/p})}}}{(2\Omega^+_E\Omega^-_E)^{(p-1)/2}} \right|$$

$$\bullet\; \mathcal{L}_{E,\underline{\Delta}}(\rho_{\chi_{\Delta_1^s}\chi_{\Delta_2^t}}) \qquad \bullet\; \mathcal{L}_{E,\underline{\Delta}}\Big(\bigoplus_{j=0}^{p-2} \omega^j\Big) \qquad \bullet\; \frac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{\chi_{\Delta_1^s}\chi_{\Delta_2^t}})}{\mathcal{L}_{E,\underline{\Delta}}(\bigoplus_{j=0}^{p-2} \omega^j)} \quad \text{and}$$

$$\bullet\; \Big(\prod_{s,t} \frac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{\chi_{\Delta_1^s}\chi_{\Delta_2^t}})}{\mathcal{L}_{E,\underline{\Delta}}(\bigoplus_{j=0}^{p-2} \omega^j)}\Big)^p := \frac{(\mathcal{L}_{E,\underline{\Delta}}(\rho_{\chi_{\Delta_2}}) \times \prod_{t=0}^{p-1} \mathcal{L}_{E,\underline{\Delta}}(\rho_{\chi_{\Delta_1}\chi_{\Delta_2^t}}))^p}{\mathcal{L}_{E,\underline{\Delta}}(\bigoplus_{j=0}^{p-2} \omega^j)^{p(p+1)}}.$$

The first quantity is a rational number (in fact, it turns out to be an integer in every case considered here), while the latter four quantities are p-adic numbers whose coefficients have been expressed below to an accuracy of order $O(p^9)$.

Remark. In particular, congruences (1.6.1)–(1.6.2) hold at each pair (s, t) provided that

$$\frac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{\chi_{\Delta_1^s}\chi_{\Delta_2^t}})}{\mathcal{L}_{E,\underline{\Delta}}(\bigoplus_{j=0}^{p-2} \omega^j)} = [1, \ldots] \in 1 + p\mathbb{Z}_p,$$

whilst congruence (1.6.3) is true if and only if

$$\Big(\prod_{s,t} \frac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{\chi_{\Delta_1^s}\chi_{\Delta_2^t}})}{\mathcal{L}_{E,\underline{\Delta}}(\bigoplus_{j=0}^{p-2} \omega^j)}\Big)^p = [1, 0, 0, \ldots] \in 1 + p^3\mathbb{Z}_p.$$

The data below confirm that these hold for all examples calculated in this article.

https://doi.org/10.1017/S1446788714000445 Published online by Cambridge University Press

TABLE 1. $p = 3$, $E = 11A3$ with equation $y^2 + y = x^3 - x^2$.

$\Delta_1^s\Delta_2^t$	L^*	$\mathcal{L}_{E,\underline{\Delta}}(\rho_{\chi_{\Delta_1^s}\chi_{\Delta_2^t}})$	$\mathcal{L}_{E,\underline{\Delta}}\left(\bigoplus_{j=0}^{p-2}\omega^j\right)$	$\dfrac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{\chi_{\Delta_1^s}\chi_{\Delta_2^t}})}{\mathcal{L}_{E,\underline{\Delta}}\left(\bigoplus_{j=0}^{p-2}\omega^j\right)}$
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]
		$\left(\prod_{s,t}\frac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{s,t})}{\mathcal{L}_{E,\underline{\Delta}}(\oplus\omega^j)}\right)^p = [1,0,0,2,1,2,2,1,1]$		
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]
		$\left(\prod_{s,t}\frac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{s,t})}{\mathcal{L}_{E,\underline{\Delta}}(\oplus\omega^j)}\right)^p = [1,0,0,1,2,0,2,0,1]$		
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]
		$\left(\prod_{s,t}\frac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{s,t})}{\mathcal{L}_{E,\underline{\Delta}}(\oplus\omega^j)}\right)^p = [1,0,0,2,2,2,2,2,2]$		

https://doi.org/10.1017/S1446788714000445 Published online by Cambridge University Press

Table 1. Continued.

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]
		$\left(\prod_{s,t} \frac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{s,t})}{\mathcal{L}_{E,\underline{\Delta}}(\oplus\omega^j)}\right)^p = [1, 0, 0, 0, 2, 0, 2, 0, 2]$		
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]
		$\left(\prod_{s,t} \frac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{s,t})}{\mathcal{L}_{E,\underline{\Delta}}(\oplus\omega^j)}\right)^p = [1, 0, 0, 0, 0, 2, 0, 2, 2]$		
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]
		$\left(\prod_{s,t} \frac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{s,t})}{\mathcal{L}_{E,\underline{\Delta}}(\oplus\omega^j)}\right)^p = [1, 0, 0, 1, 1, 0, 1, 0, 0]$		

https://doi.org/10.1017/S1446788714000445 Published online by Cambridge University Press

Table 1. Continued.

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 2. $p = 3$, $E = 77C1$ with equation $y^2 + xy = x^3 + x^2 + 4x + 11$.

$\Delta_1^s\Delta_2^t$	L^*	$\mathcal{L}_{E,\underline{\Delta}}(\rho_{\chi_{\Delta_1^s}\chi_{\Delta_2^t}})$	$\mathcal{L}_{E,\underline{\Delta}}\left(\bigoplus_{j=0}^{p-2}\omega^j\right)$	$\frac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{\chi_{\Delta_1^s}\chi_{\Delta_2^t}})}{\mathcal{L}_{E,\underline{\Delta}}\left(\bigoplus_{j=0}^{p-2}\omega^j\right)}$
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]
		$\left(\prod_{s,t} \frac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{s,t})}{\mathcal{L}_{E,\underline{\Delta}}(\oplus\omega^j)}\right)^p = [1, 0, 0, 2, 2, 1, 1, 1, 2]$		
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 3. $p = 5$, $E = 19A3$ with equation $y^2 + y = x^3 + x^2 + x$.

$\Delta_1^s\Delta_2^t$	L^*	$\mathcal{L}_{E,\underline{\Delta}}(\rho_{\chi_{\Delta_1^s}\chi_{\Delta_2^t}})$	$\mathcal{L}_{E,\underline{\Delta}}\left(\bigoplus_{j=0}^{p-2}\omega^j\right)$	$\frac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{\chi_{\Delta_1^s}\chi_{\Delta_2^t}})}{\mathcal{L}_{E,\underline{\Delta}}\left(\bigoplus_{j=0}^{p-2}\omega^j\right)}$
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]
		$\left(\prod_{s,t} \frac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{s,t})}{\mathcal{L}_{E,\underline{\Delta}}(\oplus\omega^j)}\right)^p = [1, 0, 0, 2, 3, 3, 1, 2, 0]$		

https://doi.org/10.1017/S1446788714000445 Published online by Cambridge University Press

TABLE 4. $p = 5$, $E = 56A1$ with equation $y^2 = x^3 + x + 2$.

$\Delta_1^s\Delta_2^t$	L^*	$\mathcal{L}_{E,\underline{\Delta}}(\rho_{\chi_{\Delta_1^s}\chi_{\Delta_2^t}})$	$\mathcal{L}_{E,\underline{\Delta}}\left(\bigoplus_{j=0}^{p-2}\omega^j\right)$	$\dfrac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{\chi_{\Delta_1^s}\chi_{\Delta_2^t}})}{\mathcal{L}_{E,\underline{\Delta}}\left(\bigoplus_{j=0}^{p-2}\omega^j\right)}$
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]
$\left(\prod_{s,t}\dfrac{\mathcal{L}_{E,\underline{\Delta}}(\rho_{s,t})}{\mathcal{L}_{E,\underline{\Delta}}(\oplus\omega^j)}\right)^p = [1,0,0,1,4,3,2,1,0]$				

We conclude by discussing what one might expect if the μ-invariants are nonzero. Recall that $\mathcal{S} \subset \mathbb{Z}_p[\![G_\infty^{(d)}]\!]$ denoted a canonical Ore set; let us define $\mathcal{S}^* := \bigcup_{n\geq 0} p^n\mathcal{S}$. Burns and Venjakob [3, Proposition 3.4] established the existence of an isomorphism

$$K_1(\mathbb{Z}_p[\![G_\infty^{(d)}]\!]_{\mathcal{S}^*}) \cong K_1(\mathbb{Z}_p[\![G_\infty^{(d)}]\!]_{\mathcal{S}}) \oplus K_0(\mathbb{F}_p[\![G_\infty^{(d)}]\!])$$

and the right-most module is free of finite rank (encoding all the μ-invariant data).

Therefore, one expects that, in addition to the congruences $(1.1)_{m,\underline{\mathfrak{h}}}$ and $(1.2)_m$ holding, there should be a system of exact relations amongst the μ-invariants of $\mathbf{L}_p(E,\mathcal{J})$. As an illustration, if $(d,m) = (2,1)$ and the μ-invariant of $\mathbf{L}_p(E,\oplus\omega^j)$ is positive, we suspect that the numerical congruences above should hold higher than just the third power of p. This is a computational question worthy of future investigation.

Acknowledgements

Both authors are very grateful to Tom Ward for his help with the computations, and to Antonio Lei for many lively discussions on this topic.

References

[1] A. Bouganis, 'Special values of L-functions and false Tate curve extensions', *J. Lond. Math. Soc. (2)* **82** (2010), 596–620.

[2] A. Bouganis and V. Dokchitser, 'Algebraicity of L-values for elliptic curves in a false Tate curve tower', *Math. Proc. Cambridge Philos. Soc.* **142** (2007), 193–204.

[3] D. Burns and O. Venjakob, 'On descent theory and main conjectures in noncommutative Iwasawa theory', *J. Inst. Math. Jussieu* **142** (2011), 59–118.

[4] J. Coates, P. Schneider, R. Sujatha and O. Venjakob (eds) 'Noncommutative Iwasawa main conjectures over totally real fields', in: *Proc. Münster Workshop on Iwasawa Theory*, Springer Proceedings in Mathematics and Statistics, 29 (Springer, Berlin, Heidelberg, 2013).

[5] D. Delbourgo and A. Lei, 'Noncommutative Iwasawa theory for elliptic curves with multiplicative reduction', Preprint, 2014.

[6] D. Delbourgo and T. Ward, 'Nonabelian congruences between L-values of elliptic curves', *Ann. Inst. Fourier (Grenoble)* **58** (2008), 1023–1055.

[7] D. Delbourgo and T. Ward, 'The growth of CM periods over false Tate extensions', *Exp. Math.* **19** (2010), 195–210.

https://doi.org/10.1017/S1446788714000445 Published online by Cambridge University Press

[8] V. Dokchitser and T. Dokchitser, 'Computations in noncommutative Iwasawa theory', *Proc. Lond. Math. Soc.* (3) **94** (2007), 211–272.

[9] T. Hara, 'Iwasawa theory of totally real fields for certain noncommutative p-extensions', *J. Number Theory* **130** (2010), 1068–1097.

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

[11] K. Kato, 'K_1 of some noncommutative completed group rings', *J. K-Theory* **34** (2005), 99–140.

[12] K. Kato, 'Iwasawa theory of totally real fields for Galois extensions of Heisenberg type', Preprint.

[13] K. Kato, R. Sujatha, O. Venjakob, J. Coates and T. Fukaya, 'The GL_2 main conjecture for elliptic curves without complex multiplication', *Publ. Math. Inst. Hautes Études Sci.* **101** (2005), 163–208.

[14] R. Oliver, *Whitehead Groups of Finite Groups*, LMS Lecture Note Series, 132 (Cambridge University Press, London, 1988).

[15] L. Peters, 'Noncommutative Iwasawa theory for d-fold false Tate extensions', PhD Thesis, Monash University, 2014.

[16] J. Ritter and A. Weiss, 'Toward equivariant Iwasawa theory. III', *Math. Ann.* **336** (2006), 27–49.

[17] J.-P. Serre, *Linear Representations of Finite Groups*, Graduate Texts in Mathematics, 42 (Springer, New York, 1977).

DANIEL DELBOURGO, Department of Mathematics,
University of Waikato, Hamilton 3240, New Zealand
e-mail: delbourg@waikato.ac.nz

LLOYD PETERS, School of Mathematical Sciences,
Monash University, Melbourne 3800, Australia
e-mail: lloydcpeters@yahoo.com

https://doi.org/10.1017/S1446788714000445 Published online by Cambridge University Press