C. Hsu et al. *Res. Number Theory* (2023) 9:16
https://doi.org/10.1007/s40993-022-00401-1

Research in Number Theory

RESEARCH

Explicit non-Gorenstein $R = \mathbb{T}$ via rank bounds II: Computational aspects

Catherine Hsu[1*], Preston Wake[2] and Carl Wang-Erickson[3]

*Correspondence:
chsu2@swarthmore.edu
[1]Department of Mathematics & Statistics, Swarthmore College, Swarthmore, PA 19081, USA
Full list of author information is available at the end of the article

Abstract

This is the second in a pair of papers about residually reducible Galois deformation rings with non-optimal level. In the first paper, we proved a Galois-theoretic criterion for the deformation ring to be as small as possible. This paper focuses on the computations needed to verify this criterion. We adapt a technique developed by Sharifi to compute number fields with twisted-Heisenberg Galois group and prescribed ramification, and compute the splitting behavior of primes in these extensions.

Contents

1 Introduction

1.1 Summary

In this series of two papers, we prove, under some hypotheses, an integral $R = \mathbb{T}$ theorem for the mod-p Galois representation $\bar{\rho} = 1 \oplus \omega$, where $\mathbb{T}$ is the Hecke algebra acting on weight 2 modular forms of level $N = \ell_0\ell_1$, $p \geq 5$ is a prime number, ω is the mod-p cyclotomic character, and R is a universal pseudodeformation ring for $\overline{\rho}$. We are concerned with the case where

- ℓ_0 is a prime with $\ell_0 \equiv 1 \pmod{p}$, and
- ℓ_1 is a prime with $\ell_1 \not\equiv \pm 1 \pmod{p}$ such that ℓ_1 is a pth power modulo ℓ_0.
- There is a unique weight 2 cusp form of level ℓ_0 that is congruent to the Eisenstein series modulo p.

See the introduction of Part I [3] for a discussion of why this particular setup is interesting from the point of view of Galois representations. This second paper is focused on the computations needed to verify the hypotheses of the $R = \mathbb{T}$ theorem proven in Part I.

The method we use to prove $R = \mathbb{T}$ is new. As with the standard approach, we start with a surjection $R \twoheadrightarrow \mathbb{T}$ and show that if R is "small enough," this surjection must be an isomorphism. Standard methods use tangent space computations to show that R is "small enough," but these techniques are not enough in our setting because of the failure of the Gorenstein property. Instead, we show that R is "small enough" by bounding the dimension of R/pR (as a vector space) under certain conditions.

In Part I of this pair of papers, we prove that

$$\dim_{\mathbb{F}_p} R/pR \leq 3 \iff \dim_{\mathbb{F}_p} R/pR = 3 \iff R = \mathbb{T},$$

and then prove that $\dim_{\mathbb{F}_p} R/pR > 3$ if and only if certain Galois cochains exist and satisfy specific local conditions about their restrictions to decomposition groups at ℓ_0, ℓ_1, and p. Broadly, the main steps of this paper are as follows.

- Translate the cochain existence problem into a problem about the existence of extensions of $\mathbb{Q}(\zeta_p)$ with prescribed (nilpotent p-group) Galois group, and translate the local conditions into conditions on splitting behavior of primes in these extensions.
- Describe extensions with the desired Galois groups explicitly as iterated Kummer extensions, following Sharifi's construction of generalized Heisenberg extensions [7, 14,15]. We refer to these as *twisted-Heisenberg extensions*.
- Adjust the extensions constructed in the previous step so that they have the desired local properties. This involves understanding the local behavior of certain global cochains, which we achieve using a tame analog of the Gross–Stark conjecture, developed in [18,19].
- Use Kummer theory to express the splitting behavior of primes in these extensions in terms of conditions on the Kummer generators.
- Perform computations in Sage [11] using the unit/S-unit interface to the unit/S-unit groups computed in Pari/GP [17].
- Establish number-theoretic characterizations of these extension fields.

Using these computations, we find many explicit examples where the conditions for $\dim_{\mathbb{F}_p} R/pR \leq 3$ are satisfied and conclude that $R = \mathbb{T}$ in these cases. Moreover, we find examples where $\dim_{\mathbb{F}_p} R/pR > 3$, and we compute that $\operatorname{rank}_{\mathbb{Z}_p} \mathbb{T} > 3$ in each of these cases, which is consistent with our $R = \mathbb{T}$ conjecture.

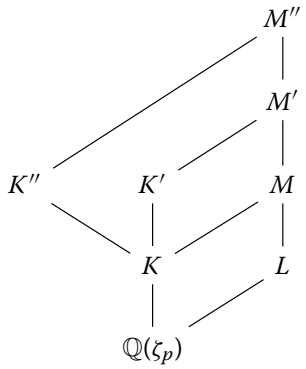
Although the focus of this paper is on computing bounds for $\dim_{\mathbb{F}_p} R/pR$, we expect that some of the techniques developed here will be of independent interest. We expect that the same methods can be used to compute bounds on dimensions of residually-reducible deformation rings in other contexts. We also hope that this paper can serve as a guide for further computation and exploration in generalized Heisenberg extensions of number fields.

1.2 Main results

We begin by formulating our main results in terms of splitting conditions in certain unipotent p-extensions of $\mathbb{Q}(\zeta_p)$ determined by $N = \ell_0\ell_1$. In the description below, we use C_p to denote a cyclic order p group.

Let $K = \mathbb{Q}(\zeta_p, \ell_1^{1/p})$, and let $L/\mathbb{Q}(\zeta_p)$ be the ω^{-1}-isotypic C_p-extension such that $(1-\zeta_p)$ splits and only the primes over ℓ_0 ramify. (For the existence and uniqueness of $L/\mathbb{Q}(\zeta_p)$, see, e.g., [1, Lem. 3.9].) To state the main result of this paper, we require two special C_p-extensions of K defined in Sect. 4.5, which we denote by K'/K and K''/K. These C_p-extensions are characterized by certain Galois-theoretic and splitting conditions, including the "ω^i-isotypic" condition that is defined in Definition 3.5.4. In particular, the Galois-theoretic conditions also involve a tower of C_p-extensions of L in which each extension in the tower is constructed by composing the previous subextension with an extension of K.

Diagrammatically, letting $M = KL$, we have:



In this setup, M'/M is the unique C_p-extension such that

- $M'/\mathbb{Q}$ is Galois and M'/M is ω^0-isotypic
- M'/M is unramified
- the primes of M over ℓ_0 split in M'/M.

Then K'/K is characterized up to isomorphism by being a C_p-extension of K contained in M' but not equal to M. See Proposition 6.1.2 for details.

Likewise, assuming that the primes over ℓ_1 split in K'/K (equivalently, in M'/M), we can construct and identify another C_p-extension M''/M'. It is the unique C_p-extension of M' such that

- $M''/\mathbb{Q}$ is Galois and M''/M' is ω-isotypic
- the conductor of M''/M' divides (resp. is equal to) $\mathfrak{m}^{\text{flat}} := \prod_{v|p} v^2$; that is, the product of the squares of the primes of M' over p
- primes of M' over ℓ_0 split in M''/M'.

Then K''/K is characterized up to isomorphism by being a C_p-extension of K contained in M'', not contained in M', and being a member of an isomorphism class (of subfields of M'') of cardinality p. See Proposition 6.2.2 for details.

The first main result of this paper gives splitting conditions in the C_p-extensions K'/K and K''/K for when $\dim_{\mathbb{F}_p} R/pR > 3$.

Theorem 1.2.1 (Theorem 4.5.1) *We have* $\dim_{\mathbb{F}_p} R/pR > 3$ *if and only if the following conditions hold:*

(i) *all primes of* K *over* ℓ_1 *split in* K'/K*;*
(ii) *there exists some prime of* K *over* ℓ_0 *that splits in both* K'/K *and* K''/K*.*

In particular, when $\dim_{\mathbb{F}_p} R/pR = 3$*, we have* $R = \mathbb{T}$*.*

The second main result of this paper is an algorithm that computes whether conditions (i) and (ii) in Theorem 4.5.1 hold. Indeed, since K'/K and K''/K are both C_p-extensions, each can be constructed by adjoining the pth root of an S-unit in K, where we have taken S to be the set of primes of K dividing Np. In particular, Kummer theory provides a computationally feasible way to check conditions (i) and (ii) even when the degrees of $K'/\mathbb{Q}$ and $K''/\mathbb{Q}$ are large, i.e., of degree $p^2(p-1) \geq 100$. The main components of our algorithm are given in Sect. 4, and the entire program, implemented using Sage [11], can

be found online at https://github.com/cmhsu2012/RR3. Our program is efficient enough that we have run it for some small values of p and many values of N.

Here is a sample result of our calculations. For a detailed discussion of all computed examples, see Sect. 5.

Theorem 1.2.2 *Let $p = 5$ and $\ell_0 = 11$. Then for*

$$\ell_1 = 23, 67, 263, 307, 373, 397, 593, 857, 967, 1013,$$

condition (i) of Theorem 4.5.1 holds, but condition (ii) does not. In particular, for these values of ℓ_1, the $\mathbb{F}_p$-dimension of R/pR equals 3 and $R \cong \mathbb{T}$.

For $\ell_1 = 43, 197, 683, 727$, conditions (i) and (ii) of Theorem 4.5.1 both hold. Consequently, the $\mathbb{F}_p$-dimension of R/pR exceeds 3 for these values of ℓ_1.

Remark 1.2.3 For the values of p and N where we found $\dim_{\mathbb{F}_p} R/pR > 3$, we also computed $\dim_{\mathbb{F}_p} \mathbb{T}/p\mathbb{T} > 3$. This is consistent with our conjecture that $R \cong \mathbb{T}$.

For the remainder of this introduction, we outline how conditions (i) and (ii) in Theorem 4.5.1 arise. Specifically, we explain how the C_p-extensions K'/K and K''/K are the splitting fields of certain Galois cochains and then show how to compute explicit S-units corresponding to these cochains using Kolyvagin derivative operators. To describe this precisely, we summarize the necessary Galois cohomological framework established in Part I.

1.3 Differential equations and the rank of *R*

Let R be the ring representing deformations of the pseudorepresentation $\omega \oplus 1$ that have determinant equal to the cyclotomic character and that are finite-flat at p, unramified-or-Steinberg at the primes ℓ_0, ℓ_1 that divide N, and unramified outside Np. Note that R only plays a motivational role in this paper, so we do not discuss this definition further—see Part I for more information.

As we explain in the introduction of Part I, there is a particular first-order deformation ρ_1 of $\bar{\rho}$ such that $\dim_{\mathbb{F}_p} R/pR \leq 3$ unless a deformation ρ_2 of ρ_1 satisfying certain local conditions exists.

There is a helpful analogy between this problem and boundary value problems in the theory of differential equations. The existence of ρ_2 is analogous to the existence of a general solution to the system of differential equations, and satisfying the local conditions is analogous to the existence of a solution to the boundary value problem. We will now use this analogy to frame our main results from Part I.

1.3.1 The system of equations defining ρ_1

The starting point for our study of $\dim_{\mathbb{F}_p} R/pR$ is the representation ρ_1 of $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. As an input, we start with two cocycles:

- $b^{(1)}$ represents the Kummer class of ℓ_1 in $H^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1))$, and
- $c^{(1)}$ represents a nontrivial class in $H^1(\mathbb{Z}[1/Np], \mathbb{F}_p(-1))$ that is ramified only at ℓ_0 (such a class is unique up to scaling).

If we wanted to represent ρ_1 as a matrix with values in $\mathrm{GL}_2(\mathbb{F}_p[\epsilon]/(\epsilon^2))$, there are two choices:

$$\begin{pmatrix} \omega(1+a^{(1)}\epsilon) & \epsilon b^{(1)} \\ \omega(c^{(1)}+\epsilon c^{(2)}) & 1+d^{(1)}\epsilon \end{pmatrix} \text{ or } \begin{pmatrix} \omega(1+a^{(1)}\epsilon) & b^{(1)}+\epsilon b^{(2)} \\ \omega\epsilon c^{(1)} & 1+d^{(1)}\epsilon \end{pmatrix}.$$

In other words, we have to choose either the upper-right or lower-left entry to be a multiple of ϵ. From the point of view of pseudorepresentations, both choices give the same answer because they have the same trace and determinant. To obviate this choice, we write ρ_1 as

$$\rho_1 = \begin{pmatrix} \omega(1+a^{(1)}\epsilon) & b^{(1)} \\ \omega c^{(1)} & 1+d^{(1)}\epsilon \end{pmatrix}$$

to refer to the pseudorepresentation obtained by either of these choices. (This ad hoc definition can be made more formal using the theory of *Generalized Matrix Algebras (GMA)*—see [Part I, §2.2.2] for the definition of GMAs or [Part I, §4.1] for the 1-reducible GMAs relevant here.)

The determinant of ρ_1 is $\omega(1+(a^{(1)}+d^{(1)}-b^{(1)}c^{(1)})\epsilon)$. Since we require our deformations to have cyclotomic determinant, we must have $d^{(1)} = b^{(1)}c^{(1)} - a^{(1)}$. Since $b^{(1)}$ and $c^{(1)}$ are fixed, the data of ρ_1 is equivalent to the data of a cochain $a^{(1)}$. For ρ_1 to be a homomorphism, it is equivalent that $a^{(1)}$ satisfy the differential equation

$$-da^{(1)} = b^{(1)} \smile c^{(1)}. \tag{1.3.1}$$

In order for this equation to have a solution, it is equivalent that ℓ_1 be a pth power modulo ℓ_0 (see [Part I, Lem. 3.2.1]), which we assume. Hence (1.3.1) has a solution.

Note that the solution $a^{(1)}$ to (1.3.1) is not unique, but any two solutions differ by a cocycle. In order for ρ_1 to satisfy the local conditions defining R, we must impose a condition on the ramification of $a^{(1)}$ at p (it can be shown that ρ_1 satisfies the conditions at ℓ_0 and ℓ_1 for all choices of $a^{(1)}$—see [Part I, Lem. 4.3.2]). Still, the solution with this condition is not unique: any two solutions differ by a cocycle that is unramified at p.

1.3.2 The system of equations defining ρ_2

Next we want to deform ρ_1 to a pseudorepresentation ρ_2 with coefficients in $\mathbb{F}_p[\epsilon]/(\epsilon^3)$. We write our desired deformation as

$$\rho_2 = \begin{pmatrix} \omega(1+a^{(1)}\epsilon+a^{(2)}\epsilon^2) & b^{(1)}+b^{(2)}\epsilon \\ \omega(c^{(1)}+c^{(2)}\epsilon) & 1+d^{(1)}\epsilon+d^{(2)}\epsilon^2 \end{pmatrix} \tag{1.3.2}$$

with the same convention as for ρ_1 that one or the other of the upper-right or lower-left entries should be multiplied by ϵ (or using the 1-reducible GMAs of [Part I, Sect. 4.1]).

Just as with $d^{(1)}$, in order that $\det(\rho_2) = \omega$ we must have $d^{(2)} = b^{(1)}c^{(2)} + b^{(2)}c^{(1)} - a^{(1)}d^{(1)} - a^{(2)}$. The data of the deformation ρ_2 is the remaining cochains $a^{(2)}$, $b^{(2)}$, and $c^{(2)}$. These cochains must satisfy the following system of equations in order for ρ_2 to be a homomorphism:

$$-da^{(2)} = a^{(1)} \smile a^{(1)} + b^{(1)} \smile c^{(2)} + b^{(2)} \smile c^{(1)} \tag{1.3.3}$$

$$-db^{(2)} = a^{(1)} \smile b^{(1)} + b^{(1)} \smile d^{(1)} \tag{1.3.4}$$

$$-dc^{(2)} = c^{(1)} \smile a^{(1)} + d^{(1)} \smile c^{(1)}. \tag{1.3.5}$$

This system is much more complex than (1.3.1), due to the coupling of equations. However, we find that:

- Equation (1.3.5) has a solution for a unique value of $a^{(1)}$ (among those that satisfy (1.3.1) and the condition on ramification at p). This value is characterized by the condition that $a^{(1)}|_{\ell_0}$ be in the image of the cup product

$$H^0(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(1)) \xrightarrow{\smile c^{(1)}|_{\ell_0}} H^1(\mathbb{Q}_{\ell_0}, \mathbb{F}_p).$$

  From now on, we fix $a^{(1)}$ to be that solution, and we define $\alpha \in H^0(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(1))$ such that $\alpha \smile c^{(1)}|_{\ell_0} = a^{(1)}|_{\ell_0}$.
- Equation (1.3.4) has a solution if and only if $a^{(1)}|_{\ell_1} = 0$.
- Supposing that (1.3.4) has a solution, Eq. (1.3.3) has a solution only for certain values of $b^{(2)}$. These values are characterized by the condition that $b^{(2)}|_{\ell_0}$ be in the image of the cup product

$$H^0(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(2)) \xrightarrow{\smile c^{(1)}|_{\ell_0}} H^1(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(1)).$$

  For such a choice of $b^{(2)}$, we define $\beta \in H^0(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(2))$ such that $\beta \smile c^{(1)}|_{\ell_0} = b^{(2)}|_{\ell_0}$.

In summary, we see that ρ_2 exists if and only if $a^{(1)}|_{\ell_1} = 0$. Moreover, when this is the case, there are invariants $\alpha \in H^0(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(1))$ and $\beta \in H^0(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(2))$.

Now assume that ρ_2 exists. In order for ρ_2 to satisfy the local conditions defining R, there are conditions that $a^{(2)}$, $b^{(2)}$, and $c^{(2)}$ be finite-flat at p, and an additional condition at ℓ_0 (No additional condition at ℓ_1 is necessary—we show that the condition on ρ_2 at ℓ_1 is satisfied for all choices of $a^{(2)}$, $b^{(2)}$, and $c^{(2)}$.) We show that the finite-flat conditions can always be satisfied, and from now on we fix $b^{(2)}$ to be a solution satisfying the finite-flat condition and fix β to satisfy $\beta \smile c^{(1)}|_{\ell_0} = b^{(2)}|_{\ell_0}$ for this choice. The extra condition at ℓ_0 can be expressed in terms of α and β:

- $\alpha^2 + \beta = 0$ in $H^0(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(2))$.

Remark 1.3.6 In the theory of differential equations, an *inverse problem* is one where the system of equations and the solution are given, and the unknown is the boundary values. This is analogous to our situation, in that we use the Eq. (1.3.5) to find the correct local conditions for $a^{(1)}$.

We summarize the important information as follows:

- $a^{(1)}$ is the unique solution to (1.3.1) such that
  - $a^{(1)}$ satisfies a finite-flat condition at p, and
  - $a^{(1)}|_{\ell_0} = \alpha \smile c^{(1)}|_{\ell_0}$ for some unique $\alpha \in H^0(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(1))$.
- $b^{(2)}$ is a solution to (1.3.4) (if it exists) such that
  - $b^{(2)}$ satisfies a finite-flat condition at p, and
  - $b^{(2)}|_{\ell_0} = \beta \smile c^{(1)}|_{\ell_0}$ for some unique $\beta \in H^0(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(2))$.

Moreover, we know that $b^{(2)}$ exists if and only if $a^{(1)}|_{\ell_1} = 0$. The following theorem is the main result of Part I.

Theorem 1.3.7 (Part I, Theorem 7.3.3) *We have* $\dim_{\mathbb{F}_p} R/pR > 3$ *if and only if the following conditions hold:*

(i) $a^{(1)}|_{\ell_1} = 0$
(ii) $\alpha^2 + \beta = 0$ *in* $H^0(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(2))$.

By realizing K'/K as the splitting field of $a^{(1)}|_{G_K}$ and K''/K as the splitting field of $b^{(2)}|_{G_K}$, we can translate Theorem 1.3.7 into the language of Theorem 1.2.1. It remains to compute the S-units corresponding to $a^{(1)}|_{G_K}$ and $b^{(2)}|_{G_K}$.

1.4 Computing *S*-units to solve cup product and Massey product equations

In the theory of differential equations, one technique used for solving boundary value problems is to first find a particular solution to the equation, then adjust that solution so it satisfies the boundary conditions. We take a similar two-step approach to computing $a^{(1)}$ and $b^{(2)}$:

Step 1 Find cochains that solve (1.3.1) and (1.3.4). We denote these by $a^{(1)}_{\text{cand}}$ and $b^{(2)}_{\text{cand}}$, for *candidate solutions*.

Step 2 Find *local adjustments* needed to make the candidate solutions satisfy the necessary local conditions. These local adjustments are global cocycles a_{adj} and b_{adj} such that $a^{(1)} = a^{(1)}_{\text{cand}} + a_{\text{adj}}$ and $b^{(2)} = b^{(2)}_{\text{cand}} + b_{\text{adj}}$ satisfy the desired local properties.

As we described above, we do not compute with cochains directly, but rather with their S-units associated by Kummer theory. For the purposes of this introduction, we will abuse notation and conflate these two.

1.4.1 Computing candidate solutions

To compute our candidate solutions, we start with an alternate interpretation of the Eqs. (1.3.1) and (1.3.4). A solution $a^{(1)}_{\text{cand}}$ to (1.3.1) gives a twisted-Heisenberg extension of $\mathbb{Q}$, which is cut out by the following upper-triangular 3-dimensional representation of $G_{\mathbb{Q}}$:

$$\begin{pmatrix} \omega & b^{(1)} & \omega a^{(1)}_{\text{cand}} \\ 0 & 1 & \omega c^{(1)} \\ 0 & 0 & \omega \end{pmatrix}. \tag{1.4.1}$$

In his thesis, Sharifi gave a way to find such extensions using Kummer theory [14]. The idea is to start by interpreting $c^{(1)}$ as a unit in $\mathbb{Q}(\zeta_p)$. Since $b^{(1)} \cup c^{(1)}$ vanishes in cohomology, the Hasse norm theorem implies that $c^{(1)}$ is a norm from K; let $\gamma \in K^\times$ be such that $N_{K/\mathbb{Q}(\zeta_p)}\gamma = c^{(1)}$. Then Sharifi proves that $a^{(1)}_{\text{cand}}$ can be obtained as a kind of Kolyvagin derivative of γ [14, Proposition 2.6].

There is a similar interpretation of (1.3.4). Namely, a solution to (1.3.4) gives a twisted-Heisenberg extension of $\mathbb{Q}$ one dimension greater, cut out by

$$\begin{pmatrix} \omega & b^{(1)} & \omega a^{(1)}_{\text{cand}} & b^{(2)}_{\text{cand}} \\ 0 & 1 & \omega c^{(1)} & d^{(1)}_{\text{cand}} \\ 0 & 0 & \omega & b^{(1)} \\ 0 & 0 & 0 & 1 \end{pmatrix}, \tag{1.4.2}$$

where we define $d^{(1)}_{\text{cand}} = b^{(1)}c^{(1)} - a^{(1)}_{\text{cand}}$. The obstruction to the existence of a cochain $b^{(2)}_{\text{cand}}$ is a generalization of the cup product called the *triple Massey product* $(b^{(1)}, c^{(1)}, b^{(1)})$. With this notation, (1.3.4) can be rewritten as

$$-db^{(2)} = (b^{(1)}, c^{(1)}, b^{(1)}).$$

Sharifi generalized his results from cup products to higher *cyclic* Massey products [7,15], which include triple Massey products of the form $(b^{(1)}, b^{(1)}, c^{(1)})$, but not $(b^{(1)}, c^{(1)}, b^{(1)})$. The result is that a solution to the equation

$$-dZ = (b^{(1)}, b^{(1)}, c^{(1)})$$

can be obtained as a second Kolyvagin derivative of γ [15, Thm. 4.3] (where, as above, $\gamma \in K^\times$ satisfies $N_{K/\mathbb{Q}(\zeta_p)}\gamma = c^{(1)}$). We show, using commutativity relations for Massey products, that a solution $b^{(2)}_{\text{cand}}$ can be derived from such a Z.

1.4.2 Computing local adjustments

There are two types of local adjustments that need to be made:

- local adjustments at p to ensure finite-flatness,
- local adjustments at ℓ_0, used in defining α and β.

For $a^{(1)}$, the finite-flat condition translates to the extension K'/K being unramified at p. This can be achieved by multiplying $a^{(1)}_{\text{cand}}$ by an appropriate pth root of unity. For $b^{(2)}$, the finite-flat condition boils down to a *peu ramifeé* condition as in [13, §2.4]. If $K/\mathbb{Q}$ is tamely ramified at p, this amounts to $b^{(2)}_{\text{cand}}$ being prime-to-p (as an S-unit), which is automatic by our Kolyvagin derivative construction. If $K/\mathbb{Q}$ is wildly ramified, the condition is slightly more involved, but can be achieved by multiplying $b^{(2)}_{\text{cand}}$ by an appropriate power of p.

The local adjustment at ℓ_0 is more interesting because it involves the cocycle $c^{(1)}$. Unlike $b^{(1)}$, the splitting field of $c^{(1)}$ is not easy to write down. Even if we do compute it, checking the condition globally would involve working with the compositum of K and the splitting field of $c^{(1)}$. Instead, we take advantage of the fact that the local condition only involves the local restriction $c^{(1)}|_{\ell_0}$, not the global cocycle. The structure of this local restriction is known by a tame version of the Gross–Stark conjecture [18]. This result computes slope of $c^{(1)}|_{\ell_0}$ (with respect to a canonical basis of $H^1(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(-1))$) in terms of an analytic invariant called the *Mazur–Tate derivative* ζ'_{MT} (of a family of Dirichlet L-functions). The quantity ζ'_{MT} is completely explicit and easily computed, so this allows us to explicitly compute $c^{(1)}|_{\ell_0}$ up to scalar, and find the adjustments purely locally.

1.5 Organization of the paper

In Sect. 2, we summarize the relevant constructions from Part I; this section also contains a subsection (Sect. 2.6) of new material that focuses on formulating the finite-flat condition for $b^{(2)}$ in language that is explicit enough for computations. In Sect. 3, we construct our candidate solutions, including the background material required to apply Sharifi's methods in our setting. In Sect. 4, we prove the main result of this paper (Theorem 4.5.1) and give explicit algorithms for checking whether the splitting conditions in Theorem 4.5.1 hold. In Sect. 5, we present a broad selection of computed examples that illustrate our main result. Lastly, in Sect. 6, we establish the characterizations of K'/K and K''/K that appear in Sect. 1.2 as part of this paper's main result; we also use this content to state a terminal result (Theorem 6.5.2) of the pair of papers.

2 Key Galois cochains and their local properties

The purpose of this section is to recall the constructions of Part I as a point of departure. In Sect. 2.6, there will also be some new content that makes these constructions more

amenable to computation. We begin with notation and conventions to make the Galois cochains featured in Sect. 1.3 precise.

2.1 Assumptions, notation, and conventions

The following statement of assumptions, which are in force throughout this paper, recapitulates the assumptions given at the outset of Sect. 1.1 in a slightly more precise form. We write

$$\mathbb{T} \twoheadrightarrow \mathbb{T}_{\ell_0}$$

for the surjection of Hecke algebras, from level N to ℓ_0, as described in Part I, Sect. 2.1.

Assumption 2.1.1 Assume $p \geq 5$ is prime. Throughout the paper, we specialize to level $N = \ell_0\ell_1$, where ℓ_0 and ℓ_1 are primes such that

(1) $\ell_0 \equiv 1 \pmod{p}$
(2) $\ell_1 \not\equiv 0, \pm 1 \pmod{p}$
(3) ℓ_1 is a pth power modulo ℓ_0
(4) $\mathrm{rk}_{\mathbb{Z}_p}\mathbb{T}_{\ell_0} = 2$, which is easily checked via a criterion Merel [9], c.f., Part I, Remark 1.3.3

The assumption that $\mathrm{rk}_{\mathbb{Z}_p}\mathbb{T}_{\ell_0} = 2$ is equivalent to the assumption that there is a unique Eisenstein-congruent cusp form at level ℓ_0, which is the assumption we used in the introduction (Sect. 1.1).

Actions of and functions on profinite groups are presumed continuous without further comment. This includes cochains on Galois groups, which are thought of as functions on a finite self-product of the group, which we will establish notation for shortly.

For $q = \ell_0, \ell_1, p$, we fix embeddings of algebraic closures $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_q$, inducing inclusions of decomposition groups $G_q := \mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q) \hookrightarrow G_{\mathbb{Q},Np}$, where $G_{\mathbb{Q},Np}$ is the Galois group of the maximal algebraic extension of $\mathbb{Q}$ ramified only at places dividing $Np\infty$. Write $I_q \subset G_q$ for the inertia subgroup, and $\mathrm{Fr}_q \in G_q$ for a lift of the arithmetic Frobenius element of G_q/I_q to G_q.

A primitive pth root of unity $\zeta \in \overline{\mathbb{Q}}$ plays an important role by inducing an isomorphism between the group of pth roots of unity $\mu_p \subset \overline{\mathbb{Q}}^\times$ and $\mathbb{F}_p(1)$, which we write for the representation of $G_{\mathbb{Q},Np}$ on the 1-dimensional $\mathbb{F}_p$-vector space $\mathbb{F}_p$ with action by the modulo p cyclotomic character ω. Likewise, ζ induces isomorphisms $\mu_p^{\otimes i} \xrightarrow{\sim} \mathbb{F}_p(i)$ for all $i \in \mathbb{Z}$, where $\mathbb{F}_p(i)$ denotes $\mathbb{F}_p(1)^{\otimes i}$.

Definition 2.1.2 Let $i \in \mathbb{Z}$ and $j \in \mathbb{Z}_{\geq 0}$. We use $C^j(\mathbb{Z}[1/Np], \mathbb{F}_p(i))$ to denote j-cochains of $G_{\mathbb{Q},Np}$ valued in $\mathbb{F}_p(i)$. Likewise, when Z^j, B^j, or H^j replaces "C^j" in this notation, we are referring to cocycles, coboundaries, and cohomology, respectively. When $Y \in Z^j(-)$ is a cocycle, we write $[Y] \in H^j(-)$ for its associated cohomology class.

Similarly, when q is a prime, we write $C^j(\mathbb{Q}_q, \mathbb{F}_p(i))$ for local cochain groups. We have restriction maps

$$(-)|_q : H^j(\mathbb{Z}[1/Np], \mathbb{F}_p(i)) \to H^j(\mathbb{Q}_q, \mathbb{F}_p(i)), \quad C^j(\mathbb{Z}[1/Np], \mathbb{F}_p(i)) \to C^j(\mathbb{Q}_q, \mathbb{F}_p(i))$$

for $q = \ell_0, \ell_1, p$. We say that a cohomology class (resp. cochain) is

- *unramified at q* when its further restriction to $H^j(\mathbb{Q}_q^{\mathrm{ur}}, \mathbb{F}_p(i))$ (resp. $C^j(\mathbb{Q}_q^{\mathrm{ur}}, \mathbb{F}_p(i))$) vanishes, and

- *splits at q* when it vanishes under these map.

We have cup product maps

$$\begin{aligned} \smile &: C^j(-, \mathbb{F}_p(i)) \times C^{j'}(-, \mathbb{F}_p(i')) \to C^{j+j'}(-, \mathbb{F}_p(i+i')), \\ \cup &: H^j(-, \mathbb{F}_p(i)) \times H^{j'}(-, \mathbb{F}_p(i')) \to H^{j+j'}(-, \mathbb{F}_p(i+i')). \end{aligned} \tag{2.1.3}$$

2.2 Pinning data

Because many of the constructions in Part I depend in subtle ways on additional choices that we refer to as *pinning data*, we recall this information here.

Definition 2.2.1 We refer to the following choices a *pinning data*.

- For each $q \in \{\ell_0, \ell_1, p\}$, an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_q$
- a primitive pth root of unity $\zeta_p \in \overline{\mathbb{Q}}$
- for $i = 0, 1$, a pth root $\ell_i^{1/p} \in \overline{\mathbb{Q}}$ of ℓ_i, such that, if possible, the image of $\ell_1^{1/p}$ in $\overline{\mathbb{Q}}_p$, under the fixed embedding, is in $\mathbb{Q}_p$. (See Lemma 2.4.1 for when this is possible.)

We fix a choice of pinning data for the entire paper. Notice that our choice defines a decomposition subgroup of q in $G_{\mathbb{Q},Np}$ for each prime q dividing Np as well as an isomorphism between this subgroup and G_q. Likewise, for any number field $F \subset \overline{\mathbb{Q}}$, the induced embedding $F \hookrightarrow \overline{\mathbb{Q}}_q$ singles out a prime of F lying over q, which we call the *distinguished prime of F over q*.

We are now ready to write down precise descriptions of the key Galois cochains from Part I, overviewed in Sect. 1.3. Indeed, recall the canonical isomorphism

$$\mathbb{Z}[1/Np]^\times \otimes_{\mathbb{Z}} \mathbb{F}_p \xrightarrow{\sim} H^1(\mathbb{Z}[1/Np], \mu_p) \tag{2.2.2}$$

of Kummer theory, which sends an element $n \in \mathbb{Z}[1/Np]^\times \otimes_{\mathbb{Z}} \mathbb{F}_p$ to the class of the cocycle $G_{\mathbb{Q},Np} \ni \sigma \mapsto \frac{\sigma(n^{1/p})}{n^{1/p}}$ for a choice $n^{1/p} \in \overline{\mathbb{Q}}$ of pth root of n. We call this element of $H^1(\mathbb{Z}[1/Np], \mu_p)$ the *Kummer class of n* and call any cocycle in this class a *Kummer cocycle of n*. Because $\zeta_p \notin \mathbb{Q}$, each Kummer cocycle of n is given by $\sigma \mapsto \frac{\sigma(n^{1/p})}{n^{1/p}}$ for a unique choice $n^{1/p} \in \overline{\mathbb{Q}}$ of pth root of n. We use the isomorphism $\mathbb{F}_p(1) \cong \mu_p$ induced by the choice of ζ_p in the pinning data (Definition 2.2.1) to think of Kummer classes and cocycles as having coefficients in $\mathbb{F}_p(1)$.

We fix the following cohomology classes and cocycles throughout the paper:

Definition 2.2.3

- Let

$$b_0, b_1, b_p \in H^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1))$$

be the Kummer classes of ℓ_0, ℓ_1, and p, respectively.

- For $i = 0, 1$, let

$$\gamma_0 \in I_{\ell_0}, \ \gamma_1 \in I_{\ell_1}$$

be a lift of a generator of the maximal pro-p quotient of the tame quotient of I_{ℓ_i} and fixed such that $b_i(\gamma_i) = 1 \in \mathbb{F}_p(1)$.[1]

[1] Note that $b_i|_{I_{\ell_i}} : I_{\ell_i} \to \mathbb{F}_p(1)$ is a well-defined homomorphism because I_{ℓ_i} acts trivially on $\mathbb{F}_p(1)$).

- Let

$$b_0^{(1)}, b_1^{(1)} \in Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1))$$

be the Kummer cocycles associated to pth roots $\ell_0^{1/p}$ and $\ell_1^{1/p}$, respectively, chosen in our pinning data (Definition 2.2.1). Let $b^{(1)} = b_1^{(1)}$.

- Let

$$c^{(1)} \in Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p(-1))$$

with cohomology class $c_0 = [c^{(1)}]$ be the unique cocycle such that

(i) c_0 is ramified exactly at ℓ_0,
(ii) $c_0|_p = 0$,
(iii) $c^{(1)}(\gamma_0) = 1$, and
(iv) $c^{(1)}|_{\ell_1} = 0$.

Note that properties (i)–(iii) specify c_0 uniquely, and property (iv) specifies $c^{(1)}$ uniquely. See Part I, Definition 3.1.1 for more details.

- Let

$$a_0, a_p \in Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p)$$

be non-zero homomorphisms ramified exactly at ℓ_0 and at p, respectively, and such that $a_0(\gamma_0) = 1$. This determines a_0 uniquely and determines a_p up to $\mathbb{F}_p^\times$-scaling (which is sufficient for our purposes).

We note that the choices of $b^{(1)}, c^{(1)}$, and a_0 depend only on the pinning data of Definition 2.2.1. Additionally, while we define all of the cohomology classes and cocycles appearing in the contructions of Part I for the sake of completeness, the content of this paper primarily requires the cocycles $b^{(1)}, c^{(1)}$, and a_0.

2.3 The solution $a^{(1)}$ to differential equation (1.3.1) and the invariant α

We move on to Galois cochains that are not cocyles, but satisfy differential equations whose origin was discussed in Sect. 1.3. Then, the crucial numerical invariant $\alpha^2 + \beta \in H^0(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(2))$ will be derived from them, which is proven to be canonical—that is, independent of the pinning data and therefore only dependent on a choice of p and N satisfying Assumption 2.1.1—in Part I, Theorem 8.1.2.

By definition of $c^{(1)}$, its associated cohomology class c_0 splits at p. This means that there exists some $x_c \in \mathbb{F}_p(-1)$ such that

$$c^{(1)}|_p = dx_c.$$

Concretely, for any $\tau \in G_p$, we have $c_0^{(1)}(\tau) = (\omega^{-1}(\tau) - 1)x_c$. This x_c is determined by the pinning data.

We will use x_c to normalize the solution to our first differential equation (1.3.1), which is

$$-dX = b^{(1)} \smile c^{(1)},$$

where X is an unknown in $C^1(\mathbb{Z}[1/Np], \mathbb{F}_p)$.

In the statement of Proposition 2.3.1 below, we use the fact that a primitive pth root of unity in $\mathbb{Q}_{\ell_0}$ exists becuase $\ell_0 \equiv 1 \pmod{p}$ and supplies a $\mathbb{F}_p$-basis for $H^0(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(1))$ under the natural isomorphism $\mu_p(\mathbb{Q}_{\ell_0}) \cong H^0(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(1))$.

Proposition 2.3.1 (Part I, Lemma 4.2.1) *There exists a unique solution $a^{(1)} \in C^1(\mathbb{Z}[1/Np], \mathbb{F}_p)$ of the differential equation (1.3.1) that satisfies the local conditions*

(a) $(a^{(1)} + b_1^{(1)} \smile x_c)|_{I_p} = 0$ *in* $Z^1(\mathbb{Q}_p^{\mathrm{nr}}, \mathbb{F}_p)$
(b) $a^{(1)}|_{\ell_0}$ *is on the line in* $Z^1(\mathbb{Q}_{\ell_0}, \mathbb{F}_p) \cong H^1(\mathbb{Q}_{\ell_0}, \mathbb{F}_p)$ *spanned by* $\zeta \cup c_0|_{\ell_0}$ *under the cup product*

$$H^0(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(1)) \times H^1(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(-1)) \to H^1(\mathbb{Q}_{\ell_0}, \mathbb{F}_p),$$

where ζ is a choice of $\mathbb{F}_p$-basis of $H^0(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(1))$.

This cochain $a^{(1)}$ is uniquely determined by the pinning data.

Condition (a) is a finite-flat condition at p, as discussed in Part I, Sect. 2.2.5.

Remark 2.3.2 We point out a phenomenon that will frequently appear in various forms. Even though $a^{(1)}$ is a global cochain that is not a global cocycle, its restriction $a^{(1)}|_{\ell_0}$ to G_{ℓ_0} is a cocycle because the factor $b^{(1)}$ of the differential equation splits at ℓ_0. We will often encounter situations where a global non-cocycle is a local cocycle, allowing us to impose arithmetic conditions on it.

We now define an important numerical invariant.

Definition 2.3.3 Let $\alpha \in \mu_p(\mathbb{Q}_{\ell_0}) \cong H^0(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(1))$ be the unique solution to

$$[a^{(1)}|_{\ell_0}] = \alpha \cup c_0|_{\ell_0}.$$

By Proposition 2.3.1, α depends only on the pinning data of Definition 2.2.1.

2.4 The solution $b^{(2)}$ to differential equation (1.3.4) and the invariant β

In preparation to discuss the differential equation solved by $b^{(2)}$, we recall the following well-known analogue, for general odd primes p, of the ramification behavior of the prime 2 in quadratic (degree 2) number fields. As far as notation, recall that b_1 denotes the Kummer class of ℓ_1, which contains the Kummer cocycle $b^{(1)}$.

Lemma 2.4.1 (Part I, Lemma 3.2.2) *The following conditions are equivalent.*

(1) $\ell_1^{p-1} \equiv 1 \pmod{p^2}$
(2) b_1 *is unramified at* p
(3) p *is tamely ramified in* $\mathbb{Q}(\ell_1^{1/p})/\mathbb{Q}$.

We recall differential equation (1.3.4), which has the form

$$-dY = a^{(1)} \smile b^{(1)} + b^{(1)} \smile d^{(1)},$$

where we have let $d^{(1)} = b^{(1)}c^{(1)} - a^{(1)}$.

Proposition 2.4.2 (Part I, Lemma 7.1.1 and Proposition 7.2.1) *There exists a solution* $b^{(2)} \in C^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1))$ *of the differential equation (1.3.4) if and only if* $a^{(1)}|_{\ell_1} = 0$ *in* $Z^1(\mathbb{Q}_{\ell_1}, \mathbb{F}_p)$. *If any such solution exists, then there also exists a solution* $b^{(2)}$ *satisfying the local conditions that*

(a) $b^{(2)}|_{\ell_0}$ *is a cocycle on the line in* $Z^1(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(1)) \cong H^1(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(1))$ *spanned by* $\zeta' \cup c_0|_{\ell_0}$ *under the cup product*

$$H^0(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(2)) \times H^1(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(-1)) \to H^1(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(1)),$$

where ζ' *is a choice of* $\mathbb{F}_p$*-basis of* $H^0(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(2))$

(b) there exists some ρ_2 *as in (1.3.2) such that* $\rho_2|_p$ *is finite-flat and* $b^{(2)}$ *is a coordinate of* ρ_2 *(as in (1.3.2)).*

There exists a single $\beta \in H^0(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(2)) \cong \mathbb{F}_p(2)$ *such that, for any of the* $b^{(2)}$ *satisfying these local conditions,*

$$b^{(2)}|_{\ell_0} = \beta \smile c^{(1)}|_{\ell_0}.$$

Moreover, the set of solutions of (1.3.4) satisfying these two local conditions is contained in a torsor under the subspace of $Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1))$ *spanned by coboundaries* $B^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1))$ *and the cocycle* $b^{(1)}$.

Proof The first claim of the proposition is exactly Lemma 6.2.9 of Part I.

Applying that first claim, the existence of a solution $b^{(2)}$ of (1.3.4) is sufficient, by Proposition 7.2.1, to deduce that

- there exists a ρ_2 as in (1.3.2) that is finite-flat at p, meaning that its $b^{(2)}$-coordinate satisfies (b); and
- its $b^{(2)}$-coordinate also satisfies (a), according to Lemma 7.1.1(2) of Part I.

Finally, the claim about containment in a torsor is in Part I, Proposition 7.2.1. □

Definition 2.4.3 Whenever a deformation ρ_2 of ρ_1 exists, i.e., when $a^{(1)}|_{\ell_1} = 0$ by Proposition 2.4.2, we define $\beta \in H^0(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(2))$ to be the unique element (depending only on the pinning data) that satisfies

$$b^{(2)}|_{\ell_0} = \beta \smile c^{(1)}|_{\ell_0}.$$

for any choice of $b^{(2)}$ satisfying the local conditions (a) and (b) Proposition 2.4.2.

2.5 Local slope and a zeta-value

The purpose of this section is to relate the class of the cocycle $c^{(1)}$ to a Mazur–Tate ζ-function ξ, following [18, §8.3]. This formula expresses the slope of the line spanned by the global class $c^{(1)}$ in the 2-dimension local Galois cohomology group $H^1(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(-1))$ as a ratio of classical and tame L-values. This can be thought of as a tame analog of the (p-adic) Gross–Stark formula.

We consider the basis $\{a_0|_{\ell_0}, \lambda\}$ of $H^1(\mathbb{Q}_{\ell_0}, \mathbb{F}_p)$, where a_0 is as in Defintion 2.2.3 and λ is the unique unramified character sending Fr_{ℓ_0} to 1. We also let $\zeta'_{\mathrm{MT}} \in \mathbb{F}_p$ denote the

element

$$\zeta'_{\mathrm{MT}} = \frac{1}{2}\sum_{i=1}^{\ell_0-1} B_2(i)\log_{\ell_0}(i), \tag{2.5.1}$$

where $B_2(x)$ is the second Bernoulli polynomial. This element can be seen as the derivative of the Mazur-Tate type L-funciton $\chi \mapsto L(\chi, 1)$ for Dirichlet characters χ of modulus N and p-power order (see [19, §1.5] or [18, §4.1]). Note that we have $\zeta'_{\mathrm{MT}} \neq 0$ due to our assumption that there is a unique cusp form of level ℓ_0 that is congruent to the Eisenstein series modulo p, according to [19, Thm. 1.5.2].

Remark 2.5.2 We remark that this is closely related to Merel's result [9, Thm. 2] characterizing the uniqueness of the cusp form in terms of *Merel's number*, defined in Part I, §1.3.2, equation (ℓ_0 Rank1). Indeed, ζ'_{MT} vanishes if and only if *Merel's number* does; a direct link between the two quantities was proved in [19, Lem. 12.3.1] (see also [5]).

We have the following description of the line spanned by $c^{(1)}|_{\ell_0}$.

Theorem 2.5.3 [18, Prop. 8.3.2] *Let $\zeta \in H^0(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(1)) \cong \mathbb{F}_p(1)$ be a basis. The line in $H^1(\mathbb{Q}_{\ell_0}, \mathbb{F}_p)$ spanned by $\zeta \smile c^{(1)}|_{\ell_0}$ contains the element*

$$\zeta'_{\mathrm{MT}}\lambda + \frac{1}{6}a_0|_{\ell_0}.$$

This is computationally significant because ζ'_{MT}, λ, and $a_0|_{\ell_0}$ are easy to compute even though $c^{(1)}$ is not.

2.6 Explicit formulation of the finite-flat condition on $b^{(2)}|_p$

In this section, we shift from recollections to new content. It is readily apparent that the finite-flat condition of Proposition 2.4.2 is too inexplicit for computation; the goal of this section is to remedy that problem.

For orientation, we recall the "basis change" argument of [Part I, §7.2], which is a first step in making the finite-flat condition testable using Kummer theory. We let ρ'_2 be a conjugate of ρ_2 (as in (1.3.2)) by generalized matrix such that $\rho'_2|_p$ is upper-triangular. This conjugation was achieved with a lower-triangular generalized matrix of the form

$$\begin{pmatrix} 1 & 0 \\ x_c + \epsilon x'_c & 1 \end{pmatrix},$$

where x_c was prescribed in Proposition 2.3.1. We write ρ'_2 using the coordinate system

$$\rho'_2 = \begin{pmatrix} \omega(1 + a^{(1)'}\epsilon + a^{(2)'}\epsilon^2) & b^{(1)'} + b^{(2)'}\epsilon \\ \omega(c^{(1)'} + c^{(2)'}\epsilon) & 1 + d^{(1)'}\epsilon + d^{(2)'}\epsilon^2 \end{pmatrix},$$

and, from Proposition 2.3.1, we have an unramified homomorphism

$$a^{(1)'}|_p = (a^{(1)} + b^{(1)} \smile x_c)|_p : G_p \to \mathbb{F}_p.$$

Also, we have $b^{(2)'} = b^{(2)}$ and $b^{(1)'} = b^{(1)}$ because the conjugation is lower-triangular.

We have the following simplified form of $\rho'_2|_p$, namely,

$$\rho'_2|_p = \begin{pmatrix} \omega(1 + a^{(1)'}\epsilon + a^{(2)'}\epsilon^2) & b^{(1)} + b^{(2)}\epsilon \\ 0 & 1 - a^{(1)'}\epsilon + d^{(2)'}\epsilon^2 \end{pmatrix}\Bigg|_p.$$

The constant determinant property implies that

$$d^{(1)'} = -a^{(1)'}, \qquad d^{(2)'} = (a^{(1)'})^2 - a^{(2)'}.$$

We observe that the differential equation imposed on $b^{(2)'} = b^{(2)}$ by the homomorphism property of ρ_2' is

$$-db^{(2)'} = a^{(1)'} \smile b^{(1)'} + b^{(1)'} \smile d^{(1)'},$$

which simplifies upon restriction to G_p as

$$-db^{(2)}|_p = a^{(1)'}|_p \smile b^{(1)}|_p + b^{(1)}|_p \smile -a^{(1)'}|_p.$$

In Part I, we translate the finite-flat property of the GMA representation $\rho_2'|_p$ to a typical (matrix-valued) representation. For convenience, we write

$$\chi_2 := (1 + \epsilon a^{(1)'} + \epsilon^2 a^{(2)'})|_p : G_p \to \mathbb{F}_p[\epsilon]/(\epsilon^3)^\times, \text{ and } \chi_1 = 1 + \epsilon a^{(1)'}|_p : G_p \to \mathbb{F}_p[\epsilon_1]^\times,$$

so that $\chi_1 = (\chi_2 \mod \epsilon^2)$ and

$$\rho_2'|_p = \begin{pmatrix} \omega\chi_2 & b^{(1)} + \epsilon b^{(2)} \\ 0 & \chi_2^{-1} \end{pmatrix}.$$

We also establish notation for the homomorphism

$$\eta_1 = \begin{pmatrix} \omega(1 + \epsilon a^{(1)'}) & b^{(1)} + \epsilon b^{(2)} \\ \epsilon c^{(1)'} & 1 + d^{(1)'} \end{pmatrix} : G_{\mathbb{Q},Np} \to \mathrm{GL}_2(\mathbb{F}_p[\epsilon]/(\epsilon^2)) \tag{2.6.1}$$

assembled from the coordinates of ρ_2', as in [Part I, Def. 7.2.8]. Note that $\eta_1|_p$ is upper-triangular, extending χ_1^{-1} by $\omega\chi_1$, since we have arranged that $c^{(1)'}|_p = 0$.

Proposition 2.6.2 (Part I, Lemma 7.2.11) *Assume the deformation ρ_2 of ρ_1 exists. Then ρ_2 is finite-flat at p if and only if both the following (a) and (b) hold.*

(a) the homomorphism η_1 is finite-flat at p
(b) $\chi_2 : G_p \to \mathbb{F}_p[\epsilon_2]$ is unramified.

Moreover, if ρ_2 satisfies (a), then there exists some deformation $\rho_{2,\mathrm{new}}$ of ρ_1 that is finite-flat at p and such that η_1 equals the $\eta_{1,\mathrm{new}}$ formed from $\rho_{2,\mathrm{new}}$ via (2.6.1).

Proof The first claim is the equivalence (1) $\Rightarrow$ (3) of Part I, Lemma 7.2.11. The second claim follows from the proof of Part I, Lemma 7.2.14: the proof shows that once we have a ρ_2 whose induced η_1 is finite-flat at p, then it is possible to adjust at most the $a^{(2)}$ and $d^{(2)}$-coordinates to form $\rho_{2,\mathrm{new}}$ from ρ_2 such that $\rho_{2,\mathrm{new}}$ is finite-flat at p and such that $\eta_{1,\mathrm{new}}$ (assembled from the coordinates of $\rho_{2,\mathrm{new}}$) equals η_1. □

Next, we want to understand when $\eta_1|_p : G_p \to \mathrm{GL}_2(\mathbb{F}_p[\epsilon]/(\epsilon^2))$, or equivalently the extension class $B := [b^{(1)} + \epsilon b^{(2)}] \in \mathrm{Ext}^1_{\mathbb{F}_p[\epsilon_1][G_p]}(\chi_1^{-1}, \omega\chi_1)$, is finite flat. Indeed, note that χ_1^{-1} and $\omega\chi_1$ are finite-flat because χ_1 is unramified. This issue is especially straightforward when $a^{(1)'}|_p = 0$, making χ_1 trivial and $b^{(2)}|_p$ a cocycle. Otherwise, $a^{(1)'}|_p$ cuts out the unique unramified cyclic degree p extension $\mathbb{Q}_{p^p}/\mathbb{Q}_p$, and $b^{(2)}|_p$ is not a cocycle on G_p. In order to apply Kummer theory in the latter case, we restrict $b^{(2)}$ to the absolute Galois group of $\mathbb{Q}_{p^p}$. We write

$$b^{(2)}|_{p^p} \in Z^1(\mathbb{Q}_{p^p}, \mathbb{F}_p(1)), \text{ so that } [b^{(2)}|_{p^p}] \in H^1(\mathbb{Q}_{p^p}, \mathbb{F}_p(1)) \cong \mathbb{Q}_{p^p}^\times/(\mathbb{Q}_{p^p}^\times)^p,$$

where the final isomorphism comes from Kummer theory.

Proposition 2.6.3 *The finite-flatness of $\eta_1|_p$ is characterized by Kummer theory.*

(a) When $\chi_1 = 1$, η_1 is finite-flat at p if and only if the class

$$[b^{(2)}|_p] \in H^1(\mathbb{Q}_p, \mathbb{F}_p(1)) \cong \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^p$$

of the cocycle $b^{(2)}|_p$ is in the line spanned by the Kummer class of $1+p$.

(b) When $\chi_1 \neq 1$, η_1 is finite-flat at p if and only if the class

$$[b^{(2)}|_{p^p}] \in H^1(\mathbb{Q}_{p^p}, \mathbb{F}_p(1)) \cong \mathbb{Q}_{p^p}^\times/(\mathbb{Q}_{p^p}^\times)^p$$

is in the subspace spanned by the subgroup of units in $\mathbb{Z}_{p^p}^\times$ that are $1 \pmod p$.

Proof Simple application of Part I, Lemma 2.2.8. □

While the condition of Proposition 2.6.3 is arguably explicit, our application requires the finite-flatness of η_1 to be tested using Kummer theory in the extension field of $\mathbb{Q}_p$ *cut out* by $b^{(1)}$, meaning that it is the minimal extension $A/\mathbb{Q}_p$ such that $b^{(1)}|_{G_A} = 0$. It is important to understand how this condition behaves, which we describe in this lemma with proof omitted.

Lemma 2.6.4 *Let $x \in Z^1(\mathbb{Q}_p, \mathbb{F}_p(i))$ and assume $(p-1) \nmid i$. If $x \in B^1(\mathbb{Q}_p, \mathbb{F}_p(i))$ is non-zero, $\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p$ is the extension cut out by x. Otherwise, letting*

$$\rho_x = \begin{pmatrix} \omega^i & x \\ 0 & 1 \end{pmatrix} : G_p \to \mathrm{GL}_2(\mathbb{F}_p),$$

the finite extension of $\mathbb{Q}_p$ cut out by x is the subfield of $\overline{\mathbb{Q}}_p^{\ker \rho_x}$ that is fixed by the image of $\left(\begin{smallmatrix} \omega^i & \\ & 1 \end{smallmatrix}\right)$ under the isomorphism $\mathrm{Gal}(\overline{\mathbb{Q}}_p^{\ker \rho_x}/\mathbb{Q}_p) \cong \mathrm{image}(\rho_x)$.

Lemma 2.6.5 *The extension of $\mathbb{Q}_p$ cut out by $b^{(1)}|_p$ falls into two isomorphism classes,*

$$\mathbb{Q}_p(\ell_1^{1/p}) \simeq \begin{cases} \mathbb{Q}_p & \text{if } \ell_1^{p-1} \equiv 1 \pmod{p^2} \\ \mathbb{Q}_p((1+p)^{1/p}) & \text{if } \ell_1^{p-1} \not\equiv 1 \pmod{p^2} \end{cases}$$

where the latter is totally ramified over $\mathbb{Q}_p$.

Proof To prove the claim, we apply the condition for the ramification of b_1 determined in Lemma 2.4.1, and note that b_1 is ramified at p if and only if it is non-trivial at p.

First we address the ramified case. We recall from [Part I, Lem. 2.2.8] that $H^1(\mathbb{Q}_p, \mathbb{F}_p(1))^{\mathrm{flat}}$ is 1-dimensional, being spanned by the Kummer class of $1+p$. Therefore, because $b_1|_p \in H^1(\mathbb{Q}_p, \mathbb{F}_p(1))$ is always contained in the finite-flat subspace, the extension of $\mathbb{Q}_p$ cut out by $\left(\begin{smallmatrix} \omega & b^{(1)} \\ 0 & 1 \end{smallmatrix}\right)$ is $\mathbb{Q}_p(\zeta_p, (1+p)^{1/p})$. By Galois theory, all of its subfields of degree p over $\mathbb{Q}_p$ are mutually isomorphic, and therefore isomorphic to $\mathbb{Q}_p((1+p)^{1/p})$.

In the unramified case, our restriction on $b^{(1)}$ in Definition 2.2.3 implies that $b^{(1)}|_p = 0$, making it cut out the trivial extension of $\mathbb{Q}_p$. □

When $\mathbb{Q}_p(\ell_1^{1/p}) = \mathbb{Q}_p$, the finite-flatness of η_1 can be tested just as easily as in Proposition 2.6.3. However, when $\mathbb{Q}_p(\ell_1^{1/p})/\mathbb{Q}_p$ is totally ramified, the test becomes more difficult: Lemma 2.2.8 of Part I does not apply over ramified extensions of $\mathbb{Q}_p$. This difficulty can be circumvented when $a^{(1)'}|_p = 0$, because $b^{(2)}|_p$ is a cocycle. Hence the remaining difficulty is concentrated in the case where

$$a^{(1)'}|_p \neq 0 \text{ and } b^{(1)}|_{I_p} \neq 0. \qquad (\star)$$

The following proposition, which ends up being an exercise in Kummer theory, addresses this most difficult case ($\star$). Let $F := \mathbb{Q}_p((1+p)^{1/p})$ and fix an isomorphism between F and $\mathbb{Q}_p(\ell_1^{1/p})$. Let $\pi \in F$ denote a uniformizer.

Lemma 2.6.6 *In case* ($\star$)*, the following conditions are equivalent.*

(1) $[b^{(2)}|_{\mathbb{Q}_{p^p}}] \in H^1(\mathbb{Q}_{p^p}, \mathbb{F}_p(1))$ *corresponds to a p-unit under the isomorphism* $H^1(\mathbb{Q}_{p^p}, \mathbb{F}_p(1)) \cong \mathbb{Q}_{p^p}^\times/(\mathbb{Q}_{p^p}^\times)^p$ *of Kummer theory*

(2) $[b^{(2)}|_F] \in H^1(F, \mathbb{F}_p(1))$ *corresponds to a* π*-unit that is* $1 \pmod{\pi^2}$ *under the isomorphism*

$$H^1(F, \mathbb{F}_p(1)) \cong F^\times/(F^\times)^p$$

of Kummer theory.

Proof Let M denote the composite field of F and $\mathbb{Q}_{p^p}$, $M := \mathbb{Q}_{p^p}((1+p)^{1/p})$. We choose a uniformizer of F and M,

$$\pi := (1+p)^{1/p} - 1 \in F.$$

We have a commutative diagram with exact rows and columns

$$\begin{array}{ccccc}
 & & 0 & & 0 \\
 & & \downarrow & & \downarrow \\
 & & \langle 1+p \rangle & \xrightarrow{\sim} & \langle 1+p \rangle \\
 & & \downarrow & & \downarrow \\
0 & \longrightarrow & \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^p & \longrightarrow & \mathbb{Q}_{p^p}^\times/(\mathbb{Q}_{p^p}^\times)^p \\
 & & \downarrow & & \downarrow \\
0 & \longrightarrow & F^\times/(F^\times)^p & \longrightarrow & M^\times/(M^\times)^p
\end{array}$$

where both horizontal inclusions arise from taking invariants of an equivariant Galois action of $\mathrm{Gal}(\mathbb{Q}_{p^p}/\mathbb{Q}_p) \cong \mathrm{Gal}(M/F)$.

In case ($\star$), the fact that $b^{(2)}|_p$ is a cocycle upon restriction to both G_F and $G_{\mathbb{Q}_{p^p}}$ means that the classes induced by these cocycles are sent, via Kummer theory, to elements $y \in \mathbb{Q}_{p^p}^\times/(\mathbb{Q}_{p^p}^\times)^p$ and $z \in F^\times/(F^\times)^p$ that map to the same element of $M^\times/(M^\times)^p$. Thus the $\mathrm{Gal}(\mathbb{Q}_{p^p}/\mathbb{Q}_p)$-action on y is trivial.

In order to apply Proposition 2.6.3(b), it will be useful to know what the coordinates of p are in the decomposition

$$F^\times/(F^\times)^p \cong \langle \pi \rangle \oplus (1+\pi\mathcal{O}_F)/(1+\pi\mathcal{O}_F)^p.$$

The key calculation is the equality

$$\frac{\pi^p}{p} = 1 + (1+p)^{1/p} - \frac{1}{p}\sum_{i=2}^{p-1}(-1)^i(1+p)^{i/p} \in \mathcal{O}_F^\times,$$

which means that p has trivial $\langle \pi \rangle$-part in the decomposition of $F^\times/(F^\times)^p$. Moreover, its image in $(1+\pi\mathcal{O}_F)/(1+\pi\mathcal{O}_F)^p$ is non-trivial modulo the image of $(1+\pi^2\mathcal{O}_F)$.

Using the natural isomorphism

$$\mathbb{Q}_{p^p}^\times/(\mathbb{Q}_{p^p}^\times)^p \cong \langle p \rangle \oplus (1+p\mathbb{Z}_{p^p})/(1+p\mathbb{Z}_{p^p})^p$$

and the Galois-equivariant exp-log isomorphism $(1 + p\mathbb{Z}_{p^p}, \cdot) \cong (p\mathbb{Z}_{p^p}, +)$, we find that $y \in \langle 1 + p \rangle$ if and only if its $\langle p \rangle$-coordinate, under the summand, vanishes.

Putting the above two facts together, we observe that the equivalence of (1) and (2) follows from proving that the pullback to $F^\times/(F^\times)^p$ of the image of $(1+p\mathbb{Z}_{p^p})/(1+p\mathbb{Z}_{p^p})^p$ in $M^\times/(M^\times)^p$ lies in the span of $1+\pi^2\mathcal{O}_F$. This is easily verified by viewing $1+p\mathbb{Z}_{p^p}$ and $1+\pi^2\mathcal{O}_F$ within $1+\pi^2\mathcal{O}_M$ and using the fact that we have a logarithm isomorphism $(1+\pi^2\mathcal{O}_M, \cdot) \xrightarrow{\sim} (\pi^2\mathcal{O}_M, +)$. □

3 Sharifi's explicit solutions to Massey product differential equations

We now turn our focus to developing a method for computing whether the cohomological conditions (*i*) and (*ii*) in Theorem 1.3.7 hold. Central to our approach is work of Sharifi giving explicit solutions to cup product and certain Massey product equations [14,15]. More specifically, from Propositions 2.3.1 and 2.4.2, we know that there exist solutions of the differential equations given by

$$\begin{aligned} -da^{(1)}_{\text{cand}} &= b^{(1)} \smile c^{(1)}, \\ -db^{(2)}_{\text{cand}} &= a^{(1)} \smile b^{(1)} + b^{(1)} \smile d^{(1)}, \end{aligned} \tag{3.0.1}$$

but it is unclear how to write down even a single such solution.

The key observations required to produce explict soltuions to these equations are, first, that we can derive our desired solutions from related differential equations involving a special type of Massey product, *cyclic Massey products*, and, second, that cyclic Massey products for absolute Galois groups can be solved via Kolyvagin derivative operators using Sharifi's theory [15].

3.1 Cup products and triple Massey products

Let G be a profinite group and let $\chi_1, \chi_2, \chi_3 \in H^1(G, \mathbb{F}_p)$. For $n > 1$, let $U_n(\mathbb{F}_p) \subset \mathrm{GL}_n(\mathbb{F}_p)$ denote the subgroup of upper-triangular unipotent matrices, and let $Z_n(\mathbb{F}_p) \subset U_n(\mathbb{F}_p)$ denote the center. Since $U_2(\mathbb{F}_p) \cong \mathbb{F}_p$ we can think of χ_i as a representation $\left(\begin{smallmatrix} 1 & \chi_i \\ 0 & 1 \end{smallmatrix}\right)$ of G with values in $U_2(\mathbb{F}_p)$

The cup product $\chi_i \cup \chi_j$ obstructs the extension of the representations (χ_i, χ_j), with values in $U_3(\mathbb{F}_p)/Z_3(\mathbb{F}_p) \cong U_2(\mathbb{F}_p) \times U_2(\mathbb{F}_p)$, to a representation with values in $U_3(\mathbb{F}_p)$. We can represent this in matrix form as

$$\begin{pmatrix} 1 & \chi_i & * \\ 0 & 1 & \chi_j \\ 0 & 0 & 1 \end{pmatrix} : G \to U_3(\mathbb{F}_p)/Z_3(\mathbb{F}_p).$$

Lifting this to $U_3(\mathbb{F}_p)$ is equivalent to finding a cochain $\nu : G \to \mathbb{F}_p$ (to go in the "$*$"-entry) such that

$$-d\nu = \chi_i \smile \chi_j.$$

Example 3.1.1 It is well known that the ring $H^*(G, \mathbb{F}_p)$ is graded-commutative. In particular, for $\chi \in H^1(G, \mathbb{F}_p)$, the cup-square of χ is zero: $\chi \cup \chi = 0$. We can realize the vanishing explicitly, defining a 1-cochain $\binom{\chi}{2} = \frac{1}{2}(\chi^2 - \chi)$ and calculating

$$-d\binom{\chi}{2} = \chi \smile \chi.$$

The corresponding representation $G \to U_3(\mathbb{F}_p)$ is given by the composition of $\chi : G \to \mathbb{F}_p$ with the map $\mathbb{F}_p \to U_3(\mathbb{F}_p)$ sending 1 to the standard Jordan block matrix

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Triple Massey products can be interpreted as an obstruction to extending two "overlapping" representations with values in $U_3(\mathbb{F}_p)$ to a single representation with values in $U_4(\mathbb{F}_p)$. In particular, the "overlapping" representations

$$\begin{pmatrix} 1 & \chi_1 & \kappa_{1,3} \\ 0 & 1 & \chi_2 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & \chi_2 & \kappa_{2,4} \\ 0 & 1 & \chi_3 \\ 0 & 0 & 1 \end{pmatrix} : G \to U_3(\mathbb{F}_p).$$

constitute an *extension problem*, which we may represent as a homomorphism

$$\begin{pmatrix} 1 & \chi_1 & \kappa_{1,3} & * \\ 0 & 1 & \chi_2 & \kappa_{2,4} \\ 0 & 0 & 1 & \chi_3 \\ 0 & 0 & 0 & 1 \end{pmatrix} : G \to U_4(\mathbb{F}_p)/Z_4(\mathbb{F}_p).$$

A *solution to the extension problem* is a $U_4(\mathbb{F}_p)$-valued representation where the missing "$*$" is filled in by a 1-cochain $\nu : G \to \mathbb{F}_p$. One readily calculates the differential equation that ν must solve, namely,

$$-d\nu = \chi_1 \smile \kappa_{2,4} + \kappa_{1,3} \smile \chi_3.$$

The quantity on the right-hand side is *a priori* a 2-cocycle, and its cohomology class is an instance of the triple Massey product of the triple (χ_1, χ_2, χ_3).

We formalize the foregoing discussion in the following definition.

Definition 3.1.2 A *defining system for the triple Massey product* (χ_1, χ_2, χ_3) is a pair of cochains $\kappa_{1,3}, \kappa_{2,4}$ such that

$$-d\kappa_{1,3} = \chi_1 \smile \chi_2$$
$$-d\kappa_{2,4} = \chi_2 \smile \chi_3.$$

The *triple Massey product* $(\chi_1, \chi_2, \chi_3) \in H^2(G, \mathbb{F}_p)$ with respect to the defining system $\kappa_{1,3}, \kappa_{2,4}$ is the class of the 2-cocycle

$$\chi_1 \smile \kappa_{2,4} + \kappa_{1,3} \smile \chi_3.$$

Remark 3.1.3 Note that the triple Massey product (χ_1, χ_2, χ_3) depends on the defining system. The usual notion of a Massey product, which we are departing from in Definition 3.1.2, is a *multi-valued* product where all possible defining systems are used to produce the values. We hope the reader does not mind our non-standard use of terminology, which allows us to avoid grammatical contortions.

Example 3.1.4 Restricting the cocycles $b^{(1)}$ and $c^{(1)}$ to $G_{\mathbb{Q}(\zeta_p)}$, we see that the Eq. (3.0.1) is expressing $-db^{(2)}_{\text{cand}}$ as the triple Massey product $(b^{(1)}, c^{(1)}, b^{(1)})$ with respect to the defining system $a^{(1)}, d^{(1)}$.

3.2 Commutativity relations

Cup products in $H^\bullet(G, \mathbb{F}_p)$ are known to be skew-symmetric. Similarly, Massey products, when considered as multivalued functions as in Remark 3.1.3, are known to satisfy certain commutativity relations, cf., [8, §3] or [4, §2]. For triple Massey products, these relations are

$$(\chi_1, \chi_2, \chi_3) - (\chi_3, \chi_2, \chi_1) = 0$$
$$(\chi_1, \chi_2, \chi_3) + (\chi_2, \chi_3, \chi_1) + (\chi_3, \chi_1, \chi_2) = 0.$$

When $\chi_2 = \chi_1$, we can combine these relations to obtain:

$$(\chi_1, \chi_3, \chi_1) + 2(\chi_1, \chi_1, \chi_3) = 0.$$

In particular, if (χ_1, χ_1, χ_3) vanishes, then (χ_1, χ_3, χ_1) also vanishes.

For our purposes, we require an "enhanced version" of these relations, which keeps track of the 1-cochains realizing vanishing Massey products as their coboundaries, and also relates the various defining systems. Recall from (2.1.3) that $\cup$ denotes a cup product on cohomology while $\smile$ denotes a cup product on cochains. We extract the following result from the proofs of the commutativity relations.

Lemma 3.2.1 *Let $\chi_1, \chi_2 \in H^1(G, \mathbb{F}_p)$ and suppose $\chi_1 \cup \chi_2 = 0$. Let $\kappa : G \to \mathbb{F}_p$ be a cochain such that $-d\kappa = \chi_1 \smile \chi_2$, and let $\binom{\chi_1}{2}$ be as in Example 3.1.1.*

Define

$$\kappa_{1,3} = \binom{\chi_1}{2}, \quad \kappa_{2,4} = \kappa$$

and

$$\kappa'_{1,3} = \kappa, \quad \kappa'_{2,4} = \chi_1\chi_2 - \kappa.$$

Then

- *$(\kappa_{1,3}, \kappa_{2,4})$ is a defining system for the Massey product (χ_1, χ_1, χ_2),*
- *$(\kappa'_{1,3}, \kappa'_{2,4})$ is a defining system for the Massey product (χ_1, χ_2, χ_1).*
- *If $\nu : G \to \mathbb{F}_p$ satisfies*

$$-d\nu = \chi_1 \smile \kappa + \binom{\chi_1}{2} \smile \chi_2$$

then $\nu' = \chi_1\kappa - 2\nu - \kappa$ satisfies

$$-d\nu' = \chi_1 \smile \kappa'_{2,4} + \kappa'_{1,3} \smile \chi_1.$$

Proof Direct computations show that

$$-d(\chi_1\chi_2) = \chi_1 \smile \chi_2 + \chi_2 \smile \chi_1.$$

and that

$$-d(\chi_1\kappa) = \chi_1 \smile \kappa + \kappa \smile \chi_1 + \chi_1^2 \smile \chi_2 + \chi_1 \smile \chi_1\chi_2.$$

The result follows by rearranging. □

3.3 Cyclic triple Massey products

We now narrow our discussion to triple Massey products of the form (χ_1, χ_1, χ_2), which we will call *cyclic* triple Massey products when we use only certain defining systems. In this special case, we will relate them to a connecting homomorphism in Galois cohomology.

As motivation, first we recall the following well-known interpretation of the cup product $\chi_1 \cup \chi_2$, for fixed χ_1, as a connecting homomorphism in Galois cohomology.

Example 3.3.1 Let $\chi_1 \in H^1(G, \mathbb{F}_p)$ be non-trivial, let $H = G/\ker(\chi_1)$ be the coimage of χ_1, and let $I \subset \mathbb{F}_p[H]$ be the augmentation ideal. Let $h \in H$ be the unique generator with $\chi_1(h) = 1$ and let $X = [h] - 1 \in I$. Taking X as a generator of I and writing $k_0 + k_1 X = (k_1, k_0)^T$, G acts on $\mathbb{F}_p[H]/I^2$ via the matrix $\left(\begin{smallmatrix} 1 & \chi_1 \\ 0 & 1 \end{smallmatrix}\right)$. In particular, we can identify I/I^2 with $\mathbb{F}_p$ as G-modules (with trivial G-action) and have an exact sequence

$$0 \to \mathbb{F}_p \to \mathbb{F}_p[H]/I^2 \to \mathbb{F}_p \to 0 \tag{3.3.2}$$

of G-modules. The class of the extension (3.3.2) in $\mathrm{Ext}^1_{\mathbb{F}_p[G]}(\mathbb{F}_p, \mathbb{F}_p) = H^1(G, \mathbb{F}_p)$ is χ_1, so the connecting map

$$H^1(G, \mathbb{F}_p) \to H^2(G, \mathbb{F}_p)$$

sends χ_2 to $\chi_1 \cup \chi_2$.

We now consider an analogous result for cyclic triple Massey products. In this case, we have the homomorphism

$$\begin{pmatrix} 1 & \chi_1 & \binom{\chi_1}{2} \\ 0 & 1 & \chi_1 \\ 0 & 0 & 1 \end{pmatrix} : G \to U_3(\mathbb{F}_p)$$

given by composing $\chi_1 : G \to \mathbb{F}_p$ with the homomorphism $\mathbb{F}_p \to U_3(\mathbb{F}_p)$ sending 1 to the standard Jordan block matrix in $U_3(\mathbb{F}_p)$. This cochain $\binom{\chi_1}{2}$ gives part of the data for a defining system, and we call a defining system *proper* if it includes $\binom{\chi_1}{2}$. In particular, a proper defining system is determined by a single cochain $\kappa : G \to \mathbb{F}_p$ such that

$$-d\kappa = \chi_1 \smile \chi_2. \tag{3.3.3}$$

Just as for (3.3.2), the generator X of I identifies I^2/I^3 with $\mathbb{F}_p$ as G-modules, and we have an exact sequence

$$0 \to \mathbb{F}_p \to \mathbb{F}_p[H]/I^3 \to \mathbb{F}_p[H]/I^2 \to 0 \tag{3.3.4}$$

of G-modules.

Lemma 3.3.5 *The preimage of χ_2 under the map*

$$H^1(G, \mathbb{F}_p[H]/I^2) \to H^1(G, \mathbb{F}_p)$$

is in bijection with the set of proper defining systems of the Massey product (χ_1, χ_1, χ_2). Moreover, the connecting map

$$\partial : H^1(G, \mathbb{F}_p[H]/I^2) \to H^2(G, \mathbb{F}_p)$$

for the sequence (3.3.4) sends a proper defining system to the associated Massey product.

Proof This is a special case of [7, Theorem 3.3.4]. We only review the construction here. A cocycle $H^1(G, \mathbb{F}_p[H]/I^2)$ mapping to χ_2 in $H^1(G, \mathbb{F}_p)$ can be written as $\chi_2 + \kappa X$ for

some cochain κ. The cocycle condition exactly amounts to (3.3.3), so it is equivalent to a proper defining system. The statement about the connecting map is a straightforward computation. □

Definition 3.3.6 We call Massey products (χ_1, χ_1, χ_2) with proper defining systems *cyclic (triple) Massey products* because of the appearence of the cyclic group H in the lemma. (Other groups are considered in [7].)

Changing the defining system for a cyclic triple Massey product changes the value in a simple way.

Lemma 3.3.7 *Let $\kappa, \kappa' : G \to \mathbb{F}_p$ be two proper defining systems for the cyclic triple Massey product (χ_1, χ_1, χ_2), and let $(\chi_1, \chi_1, \chi_2)_\kappa, (\chi_1, \chi_1, \chi_2)_{\kappa'} \in H^2(G, \mathbb{F}_p)$ be the corresponding values. Then*

$$(\chi_1, \chi_1, \chi_2)_{\kappa'} = (\chi_1, \chi_1, \chi_2)_\kappa + \chi_1 \cup (\kappa' - \kappa).$$

Proof Immediate from the definition. □

3.4 Vanishing of cyclic Massey products for absolute Galois groups

In this section, we recapitulate [7, §5.1]. From the previous section, we see the vanishing of the cyclic Massey product (χ_1, χ_1, χ_2) for *some* proper defining system is equivalent to χ_2 being in the image of the augmentation

$$H^1(G, \mathbb{F}_p[H]/I^3) \xrightarrow{\iota} H^1(G, \mathbb{F}_p).$$

Indeed, suppose $\iota(x) = \chi_2$ for some $x \in H^1(G, \mathbb{F}_p[H]/I^3)$ and let $x' \in H^1(G, \mathbb{F}_p[H]/I^2)$ be the image of x. By Lemma 3.3.5, x' defines a proper defining system for the Massey product (χ_1, χ_1, χ_2) and the value is $\partial(x')$. Since x is a lift of x', it follows that $\partial(x') = 0$ and the Massey product vanishes. Conversely, if $x' \in H^1(G, \mathbb{F}_p[H]/I^2)$ corresponds to a proper defining system such that the Massey product vanishes, then $\partial(x') = 0$ so x' lifts to $H^1(G, \mathbb{F}_p[H]/I^3)$.

Of course, a proper defining system for (χ_1, χ_1, χ_2) exists if and only if $\chi_1 \cup \chi_2 = 0$. This discussion can be summarized in the following lemma (see also [7, Proposition 5.1.3]).

Lemma 3.4.1 *Let $\chi_1 : G \to \mathbb{F}_p$ be a homomorphism and let $H = G/\ker(\chi_1)$ be the coimage. If the sequence*

$$H^1(G, \mathbb{F}_p[H]) \to H^1(G, \mathbb{F}_p) \xrightarrow{\cup\chi_1} H^2(G, \mathbb{F}_p) \tag{3.4.2}$$

is exact, then for any $\chi_2 \in H^1(G, \mathbb{F}_p)$ such that $\chi_1 \cup \chi_2 = 0$, there is a proper defining system for which the cyclic Massey product (χ_1, χ_1, χ_2) vanishes.

Now we specialize to a case where (3.4.2) is always exact: when G is the absolute Galois group of a field (this is a standard property of local symbols—see [12, Sect. XIV.1], for example). This allows us not only to show that cyclic triple Massey product vanish, but also to compute explicit solutions, as in the following theorem, due to Sharifi (it is a special case of [15, Theorem 4.3]).

In order to state this theorem, we require Kolyvagin derivative operators.

Definition 3.4.3 [15, p. 14]Let $\sigma \in C_p$ denote a generator of a cyclic p-group C_p. The *ith Kolyvagin derivative operator (with respect to* σ*)* is

$$D_\sigma^i = \sum_{j=0}^{p-1} \binom{j}{i} \sigma^j \in \mathbb{F}_p[C_p].$$

Theorem 3.4.4 (Sharifi) *Let F be a field containing a primitive pth root of unity and let G_F be the absolute Galois group of F. Let $s, t \in F^\times$ and let $\chi_s, \chi_t : G_F \to \mathbb{F}_p$ be the associated Kummer characters. Suppose $\chi_s \cup \chi_t = 0$, and let $\theta \in F(\sqrt[p]{s})^\times$ be such that $\mathrm{Nm}(\theta) = t$.*

Let $\sigma \in G_F$ satisfy $\chi_s(\sigma) = 1$ so that the image of σ in $\mathrm{Gal}(F(\sqrt[p]{s})/F)$ is a generator. Then there are cochains $c_1, c_2 : G_F \to \mathbb{F}_p$ satisfying

$$-dc_1 = \chi_s \smile \chi_t$$
$$-dc_2 = \chi_s \smile c_1 + \binom{\chi_s}{2} \smile \chi_t$$

and such that, under the identification $H^1(F(\sqrt[p]{s}), \mathbb{F}_p) \cong F(\sqrt[p]{s})^\times \otimes \mathbb{F}_p$, we have

$$c_1|_{G_{F(\sqrt[p]{s})}} = D_\sigma^1(\theta)$$
$$c_2|_{G_{F(\sqrt[p]{s})}} = D_\sigma^2(\theta)$$

where $D_\sigma^i \in \mathbb{F}_p[\mathrm{Gal}(F(\sqrt[p]{s})/F)]$ denotes the ith Kolyvagin derivative operator.

Proof Let $H = \mathrm{Gal}(F(\sqrt[p]{s})/F)$ and let $\mathrm{Sh} : H^1(F(\sqrt[p]{s}), \mathbb{F}_p) \xrightarrow{\sim} H^1(F, \mathbb{F}_p[H])$ be the isomorphism of Shapiro's lemma. The composition

$$F(\sqrt[p]{s})^\times \otimes \mathbb{F}_p \cong H^1(F(\sqrt[p]{s}), \mathbb{F}_p) \xrightarrow{\mathrm{Sh}} H^1(F, \mathbb{F}_p[H]) \to H^1(F, \mathbb{F}_p) \cong F^\times \otimes \mathbb{F}_p$$

is the norm map, so

$$\mathrm{Sh}(\chi_\theta) = \chi_t + c_1 X + c_2 X^2 + \ldots c_{p-1} X^{p-1}$$

for some cochains c_i. By Lemma 3.3.5, the cochain c_1 is a proper defining system for the Massey product $\langle \chi_s, \chi_s, \chi_t \rangle$, and dc_2 is the Massey product for that defining system. The desired formulas for dc_1 and dc_2 then follow from the definition of defining system.

To complete the proof, it suffices to explicitly write down the isomorphism Sh. For this, apply Lemma 3.4.5 below with $G = G_F$, $X = H$, and $Y = \{1, \sigma, \sigma^2, \ldots, \sigma^{p-1}\}$, so that the function $y : G_F \to Y$ is $y(g) = \sigma^{[\chi_s(g)]}$ where $[x] \in \mathbb{Z}$ is the smallest non-negative representative of $x \in \mathbb{F}_p$. Then Lemma 3.4.5 states that $\mathrm{Sh}(\chi_\theta)$ is the class of the cocycle $\Phi \in Z^1(G_F, \mathbb{F}_p[H])$ defined by

$$\Phi_g(\sigma^i) = \chi_\theta(\sigma^i g \sigma^{-[\chi_s(\sigma^i g)]})$$

for $g \in G_F$ and $i \in \mathbb{Z}$. It remains to write Φ_g in terms of the basis $1, X, \ldots, X^{p-1}$ of $\mathbb{F}_p[H]$ for $g \in G_{F(\sqrt[p]{s})}$.

If $g \in G_{F(\sqrt[p]{s})}$ and $i \in \{0, \ldots, p-1\}$, then $[\chi_s(\sigma^i g)] = i$, so we have

$$\Phi_g(\sigma^i) = \chi_\theta(\sigma^i g \sigma^{-i}).$$

Now, let $\mathbb{1}_{\sigma^i} \in \mathbb{F}_p[H]$ denote the indicator function of σ^i so that $\mathbb{1}_{\sigma^i} = (X+1)^i$. Then we have

$$\begin{aligned}\Phi_g &= \sum_{i=0}^{p-1} \chi_\theta(\sigma^i g \sigma^{-i}) \mathbb{1}_{\sigma^i} \\ &= \sum_{i=0}^{p-1} \chi_\theta(\sigma^i g \sigma^{-i}) \left(\sum_{j=0}^{p-1} \binom{i}{j} X^j \right) \\ &= \sum_{j=0}^{p-1} \left(\sum_{i=0}^{p-1} \binom{i}{j} \chi_\theta(\sigma^i g \sigma^{-i}) \right) X^j \\ &= \sum_{j=0}^{p-1} (D^j \chi_\theta)(g) X^j.\end{aligned}$$

Since the class of $g \mapsto \Phi_g$ is $\mathrm{Sh}(\chi_\theta)$, we have $c_i(g) = (D^i\chi_\theta)(g) = \chi_{D^i(\theta)}(g)$ for all $g \in G_{F(\sqrt[p]{s})}$. This completes the proof. □

Lemma 3.4.5 *Let G be a group, $G' < G$ be a finite-index subgroup, and $X = G'\backslash G$. Let $\mathbb{F}_p[X]$ denote the G-module of left-G'-invariant functions on G. The isomorphism of Shapiro's Lemma is given by*

$$\mathrm{Sh}^{-1} : H^1(G, \mathbb{F}_p[X]) \xrightarrow{\sim} H^1(G', \mathbb{F}_p),\ (g \mapsto f_g) \mapsto (g' \mapsto f_{g'}(1)).$$

The inverse is given as follows. Let $Y \subset G$ be set of coset representatives such that $1 \in Y$ and let $y : G \to Y$ be the function satisfying $G'g = G'y(g)$ for all $g \in G$, so that y induces an isomorphism $y : X \xrightarrow{\sim} Y$. For $g \in G$ let $\tilde{g} = gy(g)^{-1} \in G'$. For a cocycle $(g' \mapsto \phi_{g'}) \in Z^1(G, \mathbb{F}_p)$ and $g \in G$, define $\Phi_g \in \mathbb{F}_p[X]$ by

$$\Phi_g(x) = \phi_{\widetilde{y(x)g}}.$$

Then $\mathrm{Sh}(\phi) = \Phi$.

Proof Let $\phi \in Z^1(G', \mathbb{F}_p)$. Note that $y(g') = 1$ and $\widetilde{g'} = g'$ for all $g' \in G'$. It follows that

$$(\mathrm{Sh}^{-1}(\mathrm{Sh}(\phi)))_{g'} = \mathrm{Sh}(\phi)_{g'}(1) = \phi_{\widetilde{y(1)g'}} = \phi_{g'}.$$

This shows that Sh and Sh^{-1} are inverse functions on the level of cocycles. It remains only to show that $\mathrm{Sh}(\phi)$ is indeed a cocycle. It suffices to show that, for all $x \in Y$ and all $s, t \in G$,

$$\Phi_{st}(x) = \Phi_s(x) + \Phi_t(xs).$$

First note that, for all $a, b \in G$, there are equalties of cosets,

$$G'y(ab) = G'ab = G'y(a)b = G'y(y(a)b),$$

so $y(ab) = y(y(a)b)$. Then a simple computation shows that

$$\widetilde{ab} = \tilde{a}\widetilde{y(a)b}.$$

Applying this identity to $a = xs$ and $b = t$ gives

$$\begin{aligned}\Phi_{st}(x) &= \phi_{\widetilde{xst}} \\ &= \phi_{\widetilde{xs}y\widetilde{(xs)}t} \\ &= \phi_{\widetilde{xs}} + \phi_{y\widetilde{(xs)}t} \\ &= \Phi_s(x) + \Phi_t(xs).\end{aligned}$$

□

3.5 Computing $a^{(1)}_{\text{cand}}$ and $b^{(2)}_{\text{cand}}$

We now apply Theorem 3.4.4 to compute $a^{(1)}_{\text{cand}}$ and $b^{(2)}_{\text{cand}}$, candidate solutions to the differential equations in (3.0.1).

Let $K = \mathbb{Q}(\ell_1^{1/p}, \zeta_p)$ be the splitting field of $b^{(1)}$ and let $\sigma \in \text{Gal}(K/\mathbb{Q}(\zeta_p))$ be the generator satisfying $\sigma(\ell_1^{1/p}) = \zeta_p \ell_1^{1/p}$. Let L be the splitting field of $c^{(1)}$ and let $c \in \mathbb{Q}(\zeta_p)$ be such that $L = \mathbb{Q}(\zeta_p, \sqrt[p]{c})$.

Theorem 3.5.1 *Let $\gamma \in K^\times \otimes_{\mathbb{Z}} \mathbb{F}_p$ be such that $\text{Nm}_{K/\mathbb{Q}(\zeta_p)}(\gamma) = c$. Then there are cochains $a^{(1)}_{\text{cand}}, b^{(2)}_{\text{cand}} : G_{\mathbb{Q}(\zeta_p)} \to \mathbb{F}_p$ satisfying*

$$\begin{aligned}-da^{(1)}_{\text{cand}} &= b^{(1)} \smile c^{(1)} \\ -db^{(2)}_{\text{cand}} &= a^{(1)}_{\text{cand}} \smile b^{(1)} + b^{(1)} \smile d^{(1)}_{\text{cand}},\end{aligned} \tag{3.5.2}$$

where $d^{(1)}_{\text{cand}} = b^{(1)}c^{(1)} - a^{(1)}_{\text{cand}}$, and such that, under the identification $H^1(K, \mathbb{F}_p) \cong K^\times \otimes \mathbb{F}_p$, we have

$$\begin{aligned}-a^{(1)}_{\text{cand}}|_{G_K} &= D^1_\sigma(\gamma) \\ -b^{(2)}_{\text{cand}}|_{G_K} &= D^2_\sigma(\gamma)^{-2} D^1_\sigma(\gamma)^{-1}.\end{aligned} \tag{3.5.3}$$

Proof Applying Theorem 3.4.4, we find that there are cochains

$$a^{(1)}_{\text{cand}}, Z : G_{\mathbb{Q}(\zeta_p)} \to \mathbb{F}_p$$

satisfying

$$\begin{aligned}-da^{(1)}_{\text{cand}} &= b^{(1)} \smile c^{(1)} \\ -dZ &= b^{(1)} \smile a^{(1)}_{\text{cand}} + \binom{b^{(1)}}{2} \smile c^{(1)}\end{aligned}$$

and

$$\begin{aligned}a^{(1)}_{\text{cand}}|_{G_K} &= D^1_\sigma(\gamma) \\ Z|_{G_K} &= D^2_\sigma(\gamma).\end{aligned}$$

By the commutativity relation (Lemma 3.2.1), if we define

$$b^{(2)}_{\text{cand}} = b^{(1)} a^{(1)}_{\text{cand}} - 2Z - a^{(1)}_{\text{cand}}$$

then

$$-db^{(2)}_{\text{cand}} = a^{(1)}_{\text{cand}} \smile b^{(1)} + b^{(1)} \smile d^{(1)}_{\text{cand}}.$$

Since $(b^{(1)} a^{(1)}_{\text{cand}})|_{G_K} = 0$, we see that $b^{(2)}_{\text{cand}}|_{G_K} = -2Z|_{G_K} - a^{(1)}_{\text{cand}}|_{G_K}$, and the theorem follows. □

Notice that the theorem only defines cochains on $G_{\mathbb{Q}(\zeta_p)}$, whereas we will eventually want to work with cochains on $G_{\mathbb{Q}}$. Accounting for this will amount to keeping track of actions of $\Delta := \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$.

We establish some notation.

Definition 3.5.4 For a character $\psi : \Delta \to \mathbb{F}_p^\times$, let $\epsilon_\psi \in \mathbb{F}_p[\Delta]$ be the corresponding idempotent. For a $\mathbb{F}_p[\Delta]$-module M, let $M^{\Delta=\psi} = \epsilon_\psi M$. We call this the *$\psi$-isotypic* summand of M. If M is a Galois group $M = \mathrm{Gal}(F'/F)$ and M is ψ-isotypic, then we call the extension F'/F ψ-isotypic as well.

Lemma 3.5.5 *Let M be a $\mathbb{F}_p[\mathrm{Gal}(K/\mathbb{Q})]$-module. Suppose that $\theta \in M^{\Delta=\omega^i}$ for some $i \in \mathbb{Z}/(p-1)\mathbb{Z}$. Then $D^1_\sigma(\theta) \in M^{\Delta=\omega^{i-1}}$*

Proof Note the conjugation action of Δ on $\mathrm{Gal}(K/\mathbb{Q}(\zeta_p))$ is through ω, so $\delta\sigma\delta^{-1} = \sigma^{\omega(\delta)}$ for all $\delta \in \Delta$. Then a simple computation shows that $\delta D^1_\sigma \delta^{-1} = \omega^{-1}(\delta) D^1_\sigma$. Hence we see that

$$\delta \cdot D^1_\sigma(\theta) = \omega^{-1}(\delta) D^1_\sigma(\delta \cdot \theta) = \omega^{i-1}(\delta) D^1_\sigma(\theta). \qquad \square$$

In particular, if γ in Theorem 3.5.1 is chosen to be an element in $(K^\times \otimes_{\mathbb{Z}} \mathbb{F}_p)^{\Delta=\omega^2}$, then $a^{(1)}_{\mathrm{cand}}|_{G_K} \in (K^\times \otimes_{\mathbb{Z}} \mathbb{F}_p)^{\Delta=\omega}$.

4 Adjusting solutions to satisfy boundary conditions

By Propositions 2.3.1 and 2.4.2, we know that there exist solutions

$$a^{(1)} \in C^1(\mathbb{Z}[1/Np], \mathbb{F}_p), \quad b^{(2)} \in C^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1))$$

of the differential equations (1.3.1) and (1.3.4) that also satisfy local conditions delineated there. In this section, we explicitly construct these solutions and then prove the main result of this paper, Theorem 4.5.1. We also include explicit algorithms for the main computations in the construction of $a^{(1)}$ and $b^{(2)}$.

4.1 Set up for computations

By Theorem 3.5.1, we already have constructions of 1-cochains

$$a^{(1)}_{\mathrm{cand}} : G_{\mathbb{Q}(\zeta_p)} \to \mathbb{F}_p, \qquad b^{(2)}_{\mathrm{cand}} : G_{\mathbb{Q}(\zeta_p)} \to \mathbb{F}_p(1)$$

satisfying those same differential equations (see (3.0.1)), along with the explicit determination (3.5.3) of the 1-cocycles $a^{(1)}_{\mathrm{cand}}|_{G_K}$ and $b^{(2)}_{\mathrm{cand}}|_{G_K}$. Moreover, Kummer theory, along with our choice of ζ_p that identifies $\mathbb{F}_p$ with $\mathbb{F}_p(1)$ and μ_p, provides that the corresponding elements $a^{(1)}|_{G_K}, b^{(2)}|_{G_K} \in K^\times \otimes_{\mathbb{Z}} \mathbb{F}_p$ are uniquely determined.

To satisfy the local conditions of Propositions 2.3.1 and 2.4.2, we will add 1-cocycles to our explicitly constructed 1-cochains. Namely, we want to compute the following "adjustment" cocycles:

- $a^{(1)}_{\mathrm{adj}} \in Z^1(\mathbb{Q}(\zeta_p), \mathbb{F}_p)$, which expresses the difference
$$a^{(1)}_{\mathrm{adj}} := a^{(1)}|_{G_{\mathbb{Q}(\zeta_p)}} - a^{(1)}_{\mathrm{cand}},$$
- $b^{(2)}_{\mathrm{adj}} \in Z^1(\mathbb{Q}(\zeta_p), \mathbb{F}_p(1))$, which expresses the difference
$$b^{(2)}_{\mathrm{adj}} := b^{(2)}|_{G_{\mathbb{Q}(\zeta_p)}} - \tilde{b}^{(2)}_{\mathrm{cand}},$$

where $\tilde{b}^{(2)}_{\text{cand}}$ is constructed similarly to $b^{(2)}_{\text{cand}}$ via Theorem 3.5.1 but also accounts for the dependence of (3.0.1) on $a^{(1)}$.

For each of these two adjustments, we establish a method for how to determine a corresponding element in $\mathbb{Q}(\zeta_p)^\times \otimes_{\mathbb{Z}} \mathbb{F}_p$ and then give algorithms that can be used for explicit computation. In particular, our algorithms involve extensive calculations within S-unit groups of Kummer extensions, so we recall two classical results from Kummer theory, without proof, that are quite useful in our setting.

First, we implicitly use the following lemma when translating between the language of cocycles and S-units.

Lemma 4.1.1 (Kummer theory) *Let F be a number field that is Galois over $\mathbb{Q}$ and contains $\mathbb{Q}(\zeta_p)$, and let F'/F be a C_p-extension, so that Kummer theory provides for the existence of some $h \in F^\times$ such that $F' = F(h^{1/p})$. Consider $\Delta = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ to be a subset of $\mathrm{Gal}(F/\mathbb{Q})$ under any section of the standard projection $\mathrm{Gal}(F/\mathbb{Q}) \twoheadrightarrow \Delta$. Then $\mathrm{Gal}(F'/F)$ and $F^\times$ admit a natural Δ-action that does not depend on the choice of section. The conjugation action of Δ on $\mathrm{Gal}(F'/F)$ is ω^i-isotypic if and only if $h \otimes 1 \in F^\times \otimes_{\mathbb{Z}} \mathbb{F}_p$ is ω^{1-i}-isotypic.*

Second, the theorem below allows us to compute the splitting behavior of primes in a Kummer extension F'/F in terms of the arithmetic of the base field F; it is one of the main advantages of computing in Kummer extensions and makes it feasible to test local conditions in number fields of degree $p^2(p-1) \geq 100$.

Theorem 4.1.2 [6, Theorem 4.12] *Let p be a prime and let F be a number field containing a primitive pth root of unity. Let $\alpha \in F^\times$ be p-power-free, and let $F' = F(\sqrt[p]{\alpha})$. Let $\mathfrak{p}$ be a prime of F.*

(1) if $\mathfrak{p} \mid \alpha$, then $\mathfrak{p}$ is ramified in F'/F,
(2) if $\mathfrak{p} \nmid \alpha$ and $\mathfrak{p} \nmid p$, the $\mathfrak{p}$ splits if α is a pth power mod $\mathfrak{p}$ and is inert otherwise.
(3) if $\mathfrak{p} \nmid \alpha$ and $\mathfrak{p} \mid p$, let a be the highest power of $\mathfrak{p}$ dividing $1 - \zeta_p$ in F. Then

$$\begin{array}{ll} \mathfrak{p} \textit{ splits} & \textit{if } \alpha \textit{ is a } p\textit{th power modulo } \mathfrak{p}^{ap+1} \\ \mathfrak{p} \textit{ ramifies} & \textit{if } \alpha \textit{ is not a } p\textit{th power modulo } \mathfrak{p}^{ap} \\ \mathfrak{p} \textit{ is inert} & \textit{otherwise} \end{array}$$

It remains to outline the data fixed in our set up for computing $a^{(1)}_{\text{adj}}$ and $b^{(2)}_{\text{adj}}$. From a computational perspective, the pinning data in Definition 2.2.1 plays a much less salient role, with our algorithms depending directly only on our choices of ζ_p, $\ell_p^{1/p} \in \overline{\mathbb{Q}}$. Our algorithms also require that we have fixed S-units, with S taken to be the set of primes over ℓ_0, for the following elements from Theorem 3.5.1:

- $c \in (\mathbb{Q}(\zeta_p)^\times \otimes_{\mathbb{Z}} \mathbb{F}_p)^{\Delta=\omega^2}$ such that $L = \mathbb{Q}(\zeta_p, \sqrt[p]{c})$,
- $\gamma \in (K^\times \otimes_{\mathbb{Z}} \mathbb{F}_p)^{\Delta=\omega^2}$ such that $\mathrm{Nm}_{K/\mathbb{Q}(\zeta_p)}(\gamma) = c$,
- $a^{(1)}_{\text{cand}}|_{G_K} = D^1_\sigma(\gamma) \in (K^\times \otimes_{\mathbb{Z}} \mathbb{F}_p)^{\Delta=\omega}$,
- $b^{(2)}_{\text{cand}}|_{G_K} = D^2_\sigma(\gamma)^{-2} D^1_\sigma(\gamma)^{-1} \in (K^\times \otimes_{\mathbb{Z}} \mathbb{F}_p)$.

In computing these S-units, we must fix a choice of generators

- $\sigma \in \mathrm{Gal}(K/\mathbb{Q}(\zeta_p))$ satisfying $\sigma(\ell^{1/p}) = \zeta_p \ell^{1/p}$,

- $\delta \in \Delta = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$.

Note that throughout the algorithms in this section, we view S-units in any field $F^\times$ as elements in $F^\times \otimes_{\mathbb{Z}} \mathbb{F}_p$ by implicitly reducing modulo p-powers.

A complete computational example is given in Sect. 5.2; the reader might find it useful to work through this example alongside the remainder of this section.

4.2 Adjustment for local conditions on $a^{(1)}$

The cochains $a^{(1)}$ and $a^{(1)}_{\mathrm{cand}}$ both satisfy the differential equation in (1.3.1). The difference is that $a^{(1)}$ also satisfies the two local conditions of Proposition 2.3.1:

(a) $a^{(1)}|_{I_p} = -(b^{(1)} \cup x_c)|_{I_p}$, and
(b) $a^{(1)}|_{\ell_0}$ is on the line spanned by $\zeta_p \cup c_0|_{\ell_0}$.

Recall the element $a_0 \in H^1(\mathbb{Z}[1/Np], \mathbb{F}_p)$, ramified only at ℓ_0, that we selected in Definition 2.2.3. In what follows, we will think of it as an element of $\mathbb{Q}(\zeta_p)^\times \otimes_{\mathbb{Z}} \mathbb{F}_p$ via

$$a_0|_{G_{\mathbb{Q}(\zeta_p)}} \in H^1(\mathbb{Q}(\zeta_p), \mathbb{F}_p) \xrightarrow{\sim} H^1(\mathbb{Q}(\zeta_p), \mathbb{F}_p(1)) \cong \mathbb{Q}(\zeta_p)^\times \otimes_{\mathbb{Z}} \mathbb{F}_p,$$

where the isomorphism $H^1(\mathbb{Q}(\zeta_p), \mathbb{F}_p) \xrightarrow{\sim} H^1(\mathbb{Q}(\zeta_p), \mathbb{F}_p(1))$ is drawn using our chosen primitive pth root of unity ζ_p.

We also want to point out to the reader that we evaluate the special element from Theorem 2.5.3,

$$\zeta'_{\mathrm{MT}}\lambda + \frac{1}{6}a_0|_{\ell_0} \in H^1(\mathbb{Q}_{\ell_0}, \mathbb{F}_p) = \mathrm{Hom}(G_{\ell_0}, \mathbb{F}_p) = \mathrm{Hom}(G^{\mathrm{ab}}_{\ell_0}, \mathbb{F}_p),$$

at elements of $K^\times \otimes_{\mathbb{Z}} \mathbb{F}_p$ by using the local Artin map

$$\mathrm{Art}_{\mathfrak{L}_0} : K^\times \to \mathbb{Q}^\times_{\ell_0} \xrightarrow{\mathrm{Art}} G^{\mathrm{ab}}_{\ell_0} \tag{4.2.1}$$

arising from the distinguished place $\mathfrak{L}_0$ of K over the prime ℓ_0. Specifically, under the local Artin map, we identify the basis $\{\lambda, a_0|_{\ell_0}\}$ of $H^1(\mathbb{Q}_{\ell_0}, \mathbb{F}_p)$ with the basis $\{\mathrm{ord}_{\ell_0}, \log_{\ell_0}\}$ of $\mathrm{Hom}(\mathbb{Q}^\times_{\ell_0}, \mathbb{F}_p)$, where ord_{ℓ_0} is the usual ℓ_0-valuation on $\mathbb{Q}^\times_{\ell_0}$, and $\log_{\ell_0}$ is the projection $\mathbb{Q}^\times_{\ell_0} \to \mathbb{Z}^\times_{\ell_0} \to \mathbb{F}^\times_{\ell_0}$ composed with the discrete logarithm $\mathbb{F}^\times_{\ell_0} \twoheadrightarrow \mathbb{F}_p$ determined by $a_0|_{\ell_0}$. Then, for $y \in K^\times \otimes_{\mathbb{Z}} \mathbb{F}_p \hookrightarrow \mathbb{Q}^\times_{\ell_0} \otimes_{\mathbb{Z}} \mathbb{F}_p$, we obtain

$$\left(\zeta'_{\mathrm{MT}}\lambda + \frac{1}{6}a_0|_{\ell_0}\right)(\mathrm{Art}_{\mathfrak{L}_0}(y)) = \zeta'_{\mathrm{MT}}\mathrm{ord}_{\ell_0}(y) + \log_{\ell_0}\left(\frac{y}{\ell_0^{\mathrm{ord}_{\ell_0}(y)}}\right) \in \mathbb{F}_p. \tag{4.2.2}$$

We now determine $a^{(1)}_{\mathrm{adj}} = a^{(1)} - a^{(1)}_{\mathrm{cand}} \in Z^1(\mathbb{Q}(\zeta_p), \mathbb{F}_p)$.

Theorem 4.2.3 *The element $a^{(1)}_{\mathrm{adj}} \in \mathbb{Q}(\zeta_p)^\times \otimes_{\mathbb{Z}} \mathbb{F}_p$ is given by $\zeta_p^i a_0|^j_{G_{\mathbb{Q}(\zeta_p)}}$, where*

- *$i \in \mathbb{F}_p$ is the unique element such that $K\left(\sqrt[p]{D^1_\sigma(\gamma)\zeta_p^i}\right)/K$ is unramified at p, and*
- *$j \in \mathbb{F}_p$ is the unique element such that the evaluation*

$$\left(\zeta'_{\mathrm{MT}}\lambda + \frac{1}{6}a_0|_{\ell_0}\right)\left(\mathrm{Art}_{\mathfrak{L}_0}\left(D^1_\sigma(\gamma)\zeta_p^i a_0|^j_{G_{\mathbb{Q}(\zeta_p)}}\right)\right) = 0 \in \mathbb{F}_p,$$

where $\mathrm{Art}_{\mathfrak{L}_0}$ is as in (4.2.1).

Proof First note that, since $a^{(1)}|_{G_K}, a^{(1)}_{\mathrm{cand}}|_{G_K} \in (K^\times \otimes_{\mathbb{Z}} \mathbb{F}_p)^{\Delta=\omega}$ by Lemma 4.1.1, and since both $a^{(1)}$ and $a^{(1)}_{\mathrm{cand}}$ are unramified outside Np, $a^{(1)}_{\mathrm{adj}}$ enjoys the same properties. In

particular, $a^{(1)}_{\text{adj}} \in (\mathbb{Z}[\zeta_p, 1/Np]^\times \otimes_{\mathbb{Z}} \mathbb{F}_p)^{\Delta=\omega}$, which is spanned by ζ_p and $a_0|_{G_{\mathbb{Q}(\zeta_p)}}$. Hence we have $a^{(1)}_{\text{adj}} = \zeta_p^i a_0|^j_{G_{\mathbb{Q}(\zeta_p)}}$ for some i and j.

This implies that $a^{(1)}|_{G_K} = D^1_\sigma(\gamma)\zeta_p^i a_0|^j_{G_{\mathbb{Q}(\zeta_p)}}$. The first condition on $a^{(1)}$ implies that $K\left(\sqrt[p]{a^{(1)}|_{G_K}}\right)/K$ is unramified at p. Since a_0 is unramified at p, we see that this is equivalent to $K\left(\sqrt[p]{D^1_\sigma(\gamma)\zeta_p^i}\right)/K$ being unramified at p. This determines i.

By Theorem 2.5.3, the second condition on $a^{(1)}$ is equivalent to

$$\left(\zeta'_{\text{MT}}\lambda + \frac{1}{6}a_0|_{\ell_0}\right)\left(\text{Art}_{\mathfrak{L}_0}(a^{(1)}|_{G_K})\right) = 0.$$

This determines j. □

Algorithms for computing $a^{(1)}_{\text{adj}}$

To explicitly compute the first adjustment of $a^{(1)}_{\text{cand}}$, we apply Theorem 4.1.2(3), which states that if a is the highest power of $\mathfrak{p}$ dividing $(1-\zeta_p)$ in K, then $\mathfrak{p}$ ramifies if the Kummer generator α is not a pth power modulo $\mathfrak{p}^{ap}$. The exponent a depends on whether p tamely or wildly ramifies in $K/\mathbb{Q}$, so we handle these cases separately in Algorithm 1.

Algorithm 1: Adjustment of $a^{(1)}_{\text{cand}}$ for condition at p in Theorem 4.2.3

Input: $a^{(1)}_{\text{cand}}|_{G_K} \in (K^\times \otimes_{\mathbb{Z}} \mathbb{F}_p)^{\Delta=\omega}$

Output: $i \in \mathbb{F}_p$ such that $a^{(1)}_{\text{cand}}|_{G_K}\zeta_p^i$ generates a Kummer extension that is unramified at p

(1) If p *tamely* ramifies in K, let $i \in \mathbb{F}_p$ be such that $a^{(1)}_{\text{cand}}|_{G_K}\zeta_p^i$ is congruent to a $(p-1)$st root of unity in $\mathcal{O}_K/\mathfrak{p}^p$ for each $\mathfrak{p}$ above p in K.

(2) If p *wildly* ramifies in K:

  (a) Let $\mathfrak{p}$ denote the prime above p in K.
  (b) Compute a set of representatives for the pth-powers in $\mathcal{O}_K/\mathfrak{p}^{p^2}$.
  (c) Let $i \in \mathbb{F}_p$ be such that $a^{(1)}_{\text{cand}}|_{G_K}\zeta_p^i$ is a pth power $\mathcal{O}_K/\mathfrak{p}^{p^2}$.

(3) Return i.

For the second adjustment of $a^{(1)}_{\text{cand}}$, it would be straightforward to implement the method outlined in Theorem 4.2.3 provided that we have computationally identified the distinguished prime of K over ℓ_0. However, even after computing $a^{(1)}$, it would be unclear how to compute the value of α in Definition 2.3.3. So, for computational purposes, we take a different approach that involves changing the pinning data to arrange for $\alpha = 0$; this is permitted because $\alpha^2 + \beta$ is independent of the pinning data (Part I, Theorem 8.1.2) and guaranteed to be possible by the following lemma.

Lemma 4.2.4 *There is a choice of pinning data such that $\alpha = 0$. Moreover, when $\alpha = 0$, the primes over ℓ_0 that are split in the Kummer extension generated by $a^{(1)}|_{G_K}$ are exactly the Δ-orbit of the distinguished place of K over ℓ_0.*

Proof Given any choice of pinning data, define $\alpha \in \mathbb{F}_p(1)$ as in Definition 2.3.3. Then, change our choice of decomposition group at p and pth root of ℓ_1 so that the new choice

corresponds to the Kummer cocycle in $Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1))$ given by

$$b^{(1)} + \alpha(\omega - 1).$$

By Part I, Lemma 8.3.2, this gives $\alpha = 0$ for the new choice of cocycle $a^{(1)}$.

Now, let K'/K be the Kummer extension generated by $a^{(1)}|_{G_K}$. By the definition of α, if $\alpha = 0$, then $a^{(1)}|_{\ell_0} = 0$. So the distinguished prime of K over ℓ_0 splits in K'/K. Because K'/K is ω^0-isotypic (in the sense of Definition 3.5.4), all places in the Δ-orbit of the distinguished prime also split in K'/K. Because ℓ_0 ramifies in $L/\mathbb{Q}(\zeta_p)$ and the Galois closure of $K'/\mathbb{Q}$ is $M' = K'L$, this Δ-orbit consists of exactly those places of K over ℓ_0 that split in K'/K. Note that $M'/\mathbb{Q}$ is Galois since it is cut out by the homomorphism (1.4.1). □

In light of this observation, we assume that we have arranged for $\alpha = 0$ for the remainder of the paper. Moreover, when $\alpha = 0$, Lemma 4.2.4 suggests an alternative method for computing the value of the adjustment $j \in \mathbb{F}_p$ in Theorem 4.2.3 that does not involve the distinguished prime of K over ℓ_0:

Lemma 4.2.5 *When $\alpha = 0$, the element $j \in \mathbb{F}_p$ determined in Theorem 4.2.3 is also the unique element such that $a^{(1)}_{\text{cand}}|_{G_K}\zeta_p^i a_0|^j_{G_{\mathbb{Q}(\zeta_p)}}$ generates a Kummer extension that is split at exactly one Δ-orbit of primes above ℓ_0 in K.*

Proof Let $j \in \mathbb{F}_p$ be determined as in Theorem 4.2.3, and suppose that $j' \in \mathbb{F}_p$ is such that $a^{(1)}_{\text{cand}}|_{G_K}\zeta_p^i a_0|^{j'}_{G_{\mathbb{Q}(\zeta_p)}}$ generates a Kummer extension that is split at exactly one Δ-orbit of primes above ℓ_0 in K. Denote this Δ-orbit of primes by L_{split}.

By Part I, Lemma 8.4.1, the construction of $a^{(1)}|_{G_K}$, and hence the value of $j \in \mathbb{F}_p$, is invariant if we change the distinguished prime of K over ℓ_0 within its $\text{Gal}(K/\mathbb{Q}(\zeta_p))$-orbit. So, we can change the distinguished prime, if necessary, to be a prime of L_{split} without changing the value of $j \in \mathbb{F}_p$. In particular, after this change, we conclude that $j = j'$ by the uniqueness of $a^{(1)}$ since both choices of j and j' satsify the conditions in Theorem 2.3.1. □

We implement the method outlined in Lemma 4.2.5 in Algorithm 2, which appears on the next page, using Theorem 4.1.2(2) to check the splitting behavior of primes above ℓ_0 in the various Kummer extensions of K. Note that once we compute $j \in \mathbb{F}_p$ via Lemma 4.2.5, we have computationally identified the Δ-orbit of the distinguished prime of K over ℓ_0. Without loss of generality, we can fix one of the split primes in the Kummer extension generated by $a^{(1)}|_{G_K}$ to be the distinguished prime of K over ℓ_0 for future computations.

4.3 Adjusting $b^{(2)}_{\text{cand}}$ along with $a^{(1)}_{\text{cand}}$

Having computed $a^{(1)}$, we turn to $b^{(2)}$. Recall that in Theorem 3.5.1, the differential equation that $b^{(2)}_{\text{cand}}$ satisfies depends on the choice of $a^{(1)}_{\text{cand}}$. So, before we can make adjustments for the local conditions on $b^{(2)}$, we must do a preliminary adjustment to $b^{(2)}_{\text{cand}}$ to ensure it satisfies the correct differential equation, now depending on $a^{(1)}$. In particular, by Proposition 2.4.2, this preliminary adjustment is possible only when $a^{(1)}|_{\ell_1} = 0$.

Algorithm 2: Adjustment of $a^{(1)}_{\text{cand}}$ for condition at ℓ_0 in Theorem 4.2.3

Input: $a^{(1)}_{\text{cand}}|_{G_K}\zeta_p^i \in (K^\times \otimes_{\mathbb{Z}} \mathbb{F}_p)^{\Delta=\omega}$

Output: $j \in \mathbb{F}_p$ such that $a^{(1)}|_{G_K} = a^{(1)}_{\text{cand}}|_{G_K}\zeta_p^i a_0|^j_{G_{\mathbb{Q}(\zeta_p)}}$

Output: $\mathfrak{L}_0$, the distinguished prime of K over ℓ_0

(1) Compute an S-unit for $a_0|_{G_{\mathbb{Q}(\zeta_p)}} \in \mathbb{Q}(\zeta_p)^\times \otimes_{\mathbb{Z}} \mathbb{F}_p$.

(2) For $t = 0, 1, 2, \ldots, p-1$:

  (a) Initialize L_{split} to the empty set {}.

  (b) For each prime $\mathfrak{L}$ in K above ℓ_0:

    (i) If $a^{(1)}_{\text{cand}}|_{G_K}\zeta_p^i a_0|^t_{G_{\mathbb{Q}(\zeta_p)}}$ is a pth power mod $\mathfrak{L}$, append $\mathfrak{L}$ to L_{split}.

  (c) If L_{split} contains exactly one Δ-orbit of primes above ℓ_0:

    (ii) Let $j = t$ and $\mathfrak{L}_0$ be any prime in L_{split}.

    (iii) Break for loop.

(3) Return j, $\mathfrak{L}_0$.

Lemma 4.3.1 *When $a^{(1)}|_{\ell_1} = 0$, there is an element $\xi \in K^\times \otimes_{\mathbb{Z}} \mathbb{F}_p$ such that $\mathrm{Nm}_{K/\mathbb{Q}(\zeta_p)}(\xi) = a^{(1)}_{\text{adj}}$ in $\mathbb{Q}(\zeta_p)^\times \otimes_{\mathbb{Z}} \mathbb{F}_p$.*

Moreover, there is a cocycle $\tilde{b}^{(2)}_{\text{cand}} : G_{\mathbb{Q}(\zeta_p)} \to \mathbb{F}_p(1)$ satisfing

$$d\tilde{b}^{(2)}_{\text{cand}} = a^{(1)} \smile b^{(1)} + b^{(1)} \smile d^{(1)},$$

where $d^{(1)} = b^{(1)}c^{(1)} - a^{(1)}$ and such that

$$\tilde{b}^{(2)}_{\text{cand}}|_{G_K} = (D^2_\sigma(\gamma)D^1_\sigma(\xi))^{-2}a^{(1)}|^{-1}_{G_K}. \tag{4.3.2}$$

Proof When $a^{(1)}|_{\ell_1} = 0$, we know $a^{(1)}_{\text{adj}} \cup b^{(1)} = 0$ in $H^2(\mathbb{Z}[1/Np], \mathbb{F}_p(1))$. The result then follows immediately from Lemma 3.3.7 and Theorem 3.4.4. □

Since it is straightfoward to compute an S-unit for $\tilde{b}^{(2)}_{\text{cand}}|_{G_K} \in (K^\times \otimes_{\mathbb{Z}} \mathbb{F}_p)^{\Delta=\omega^0}$, we assume that we have done so. While there is no result analogous to Lemma 3.5.5 for ensuring $\tilde{b}^{(2)}_{\text{cand}}$ is in the proper ω-isotypic class, we can to obtain the desired Δ-action on $\tilde{b}^{(2)}_{\text{cand}}$ by multiplying it by an appropriate p-power S-unit in K.

4.4 Adjustment for local conditions on $b^{(2)}$

Now, assuming that we have constructed $\tilde{b}^{(2)}_{\text{cand}}$, it satisfies the same differential equation as $b^{(2)}$, but $b^{(2)}$ also satisfies the two local conditions stipulated in Proposition 2.4.2:

(a) $b^{(2)}|_{\ell_0}$ is on the line spanned by $\zeta' \cup c_0|_{\ell_0}$ for some basis $\zeta' \in H^0(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(2))$, and

(b) $b^{(2)}|_p$ is finite-flat in the sense of Proposition 2.4.2(b); we may and do use the much simpler finite-flatness criterion of Proposition 2.6.3, thanks to the equivalence drawn in Proposition 2.6.2.

Let $b^{(2)}_{\text{adj}} = b^{(2)} - \tilde{b}^{(2)}_{\text{cand}} \in Z^1(\mathbb{Q}(\zeta_p), \mathbb{F}_p(1))$.

Theorem 4.4.1 *The element* $b_{\mathrm{adj}}^{(2)} \in \mathbb{Q}(\zeta_p)^\times \otimes_{\mathbb{Z}} \mathbb{F}_p$ *is given by* $p^k \ell_0^m$ *where*

- $k \in \mathbb{F}_p$ *is the unique element such that* $\tilde{b}_{\mathrm{cand}}^{(2)}|_{G_K} p^k \in K^\times \otimes_{\mathbb{Z}} \mathbb{F}_p$ *is* 1 *modulo* $\mathfrak{p}^{2(p-1)}$, *where* $\mathfrak{p} \subset K$ *is a prime above* p,
- $m \in \mathbb{F}_p$ *is the unique element such that*

$$\left(\zeta'_{\mathrm{MT}}\lambda + \frac{1}{6}a_0|_{\ell_0}\right)\left(\mathrm{Art}_{\mathfrak{L}_0}(\tilde{b}_{\mathrm{cand}}^{(2)}|_{G_K} p^k \ell_0^m)\right) = 0,$$

where $\mathrm{Art}_{\mathfrak{L}_0}$ *is as in (4.2.1).*

Proof We follow the proof of Theorem 4.2.3, with appropriate modifications. Indeed, since $b^{(2)}|_{G_K}, \tilde{b}_{\mathrm{cand}}^{(2)}|_{G_K} \in (K^\times \otimes_{\mathbb{Z}} \mathbb{F}_p)^{\Delta=\omega^0}$, we have $b_{\mathrm{adj}}^{(2)} \in \mathbb{Z}[1/Np]^\times \otimes_{\mathbb{Z}} \mathbb{F}_p$. We can drop the ℓ_1-part of $b_{\mathrm{adj}}^{(2)}$ and aim to compute the k and m in $b_{\mathrm{adj}}^{(2)} = p^k \ell_0^m$, because, by the last claim in Proposition 2.4.2, $b^{(2)}$ is only well defined up to coboundaries and multiples of ℓ_1. Indeed, only the ℓ_0-local behavior of $b^{(2)}$ matters, and, as the existence of β proved in Proposition 2.4.2 corroborates, adjustments by powers of ℓ_1 are ℓ_0-locally trivial.

The stated formula for the $k \in \mathbb{F}_p$, which comprises the first adjustment for $b^{(2)}$, follows directly from the finite-flatness criterion of Proposition 2.6.3 as made explicit in Lemma 2.6.6 and the discussion before it. Note these results are stated for $\mathbb{Q}(\ell_1^{1/p})$ rather than K, so the condition 1 modulo $\mathfrak{p}^{2(p-1)}$ in Theorem 4.4.1 accounts for multiplication by the ramification degree $(p-1)$ of the prime p in $\mathbb{Q}(\zeta_p)/\mathbb{Q}$.

The method for computing the second adjustment for $b^{(2)}$, which determines m, can be done by relying on the expression for the slope of $c^{(1)}|_{\ell_0}$ in Theorem 2.5.3, exactly as in Theorem 4.2.3. □

Algorithms for computing $b_{\mathrm{adj}}^{(2)}$

To explicitly compute the adjustments for the local conditions on $b^{(2)}$, we use straightforward implementations of the methods outlined in Theorem 4.4.1, starting with the adjustment for the finite-flat condition.

As discussed in Sect. 2.6, the level of difficulty in computing the adjustment for the finite-flat condition on $b^{(2)}$ is controlled by whether $b^{(1)}|_{I_p} = 0$ and $a^{(1)}|_p = 0$. Ideally, the algorithm for this adjustment would isolate the most difficult case, $b^{(1)}|_{I_p} \neq 0$ and $a^{(1)}|_p \neq 0$, but in practice, checking whether $a^{(1)}|_p = 0$ can be an infeasible computation. Therefore, Algorithm 3, which appears on the next page, considers two cases based on whether $b^{(1)}|_{I_p} = 0$:

- When $b^{(1)}|_{I_p} = 0$, i.e., p tamely ramifies in $K/\mathbb{Q}$, we can apply Proposition 2.6.3 to see that $\tilde{b}_{\mathrm{cand}}^{(2)}|_{G_K}$ is finite-flat at p as long as it is prime-to-p as an S-unit, which is guaranteed by its construction.
- When $b^{(1)}|_{I_p} \neq 0$, i.e., p wildly ramifies in $K/\mathbb{Q}$, we can apply Lemma 2.6.6 to see that $\tilde{b}_{\mathrm{cand}}^{(2)}|_{G_K}$ is finite-flat at p if it is congruent to 1 modulo $\mathfrak{p}^{2(p-1)}$, where $\mathfrak{p}$ is the prime above p in K.

Remark 4.4.2 Ultimately, we want to determine β, which depends on the restriction of $b^{(2)}$ to ℓ_0. When p is a pth power modulo ℓ_0, the p^k part of $b_{\mathrm{adj}}^{(2)}$ vanishes at ℓ_0. That is, when $\log_{\ell_0}(p) = 0$, then $b_p|_{\ell_0} = 0$. Hence, when p is a pth power modulo ℓ_0, we do not need to run Algorithm 3 since the adjustment by p^k is trivial at ℓ_0.

Algorithm 3: Adjustment of $\tilde{b}^{(2)}_{\text{cand}}$ for finite-flat condition in Theorem 4.4.1

Input: $\tilde{b}^{(2)}_{\text{cand}}|_{G_K} \in (K^\times \otimes_{\mathbb{Z}} \mathbb{F}_p)^{\Delta=\omega^0}$
Output: $k \in \mathbb{F}_p$ such that $\tilde{b}^{(2)}_{\text{cand}}|_{G_K} p^k$ satisfies the finite-flat condition at p

(1) If p *tamely* ramifies in K, let $k = 0$.
(2) If p *wildly* ramifies in K:
   (a) Let $\mathfrak{p}$ be the unique prime in K above p.
   (b) Let $k \in \mathbb{F}_p$ be such that $\tilde{b}^{(2)}_{\text{cand}}|_{G_K} p^k \equiv 1 \pmod{\mathfrak{p}^{2(p-1)}}$.
(3) Return k.

To compute the second adjustment of $b^{(2)}$, we follow the method outlined in Theorem 4.4.1, which requires the distinguished prime $\mathfrak{L}_0$ identified in the output of Algorithm 2. The computation of this last adjustment is given in Algorithm 4.

Algorithm 4: Adjustment of $\tilde{b}^{(2)}_{\text{cand}}$ for condition at ℓ_0 in Theorem 4.4.1

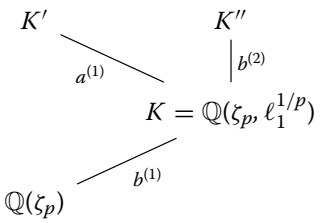
Input: $\tilde{b}^{(2)}_{\text{cand}}|_{G_K} p^k \in (K^\times \otimes_{\mathbb{Z}} \mathbb{F}_p)^{\Delta=\omega^0}$
Input: $\mathfrak{L}_0$, the distinguished prime of K over ℓ_0
Output: $m \in \mathbb{F}_p$ such that $b^{(2)}|_{G_K} = \tilde{b}^{(2)}_{\text{cand}}|_{G_K} p^k \ell_0^m$

(1) Compute ζ'_{MT}, λ, and $a_0|_{\ell_0}$.
(2) Let $a = \left(\zeta'_{\text{MT}}\lambda + \frac{1}{6}a_0|_{\ell_0}\right)\left(\text{Art}_{\mathfrak{L}_0}\left(\tilde{b}^{(2)}_{\text{cand}}|_{G_K} p^k\right)\right)$.
(3) Let $b = \left(\zeta'_{\text{MT}}\lambda + \frac{1}{6}a_0|_{\ell_0}\right)(\text{Art}_{\mathfrak{L}_0}(\ell_0))$.
(4) Return $m = -ab^{-1}$.

4.5 Deducing the main theorem

Now that we have established a method to construct the elements $a^{(1)}|_K, b^{(2)}|_K \in K^\times \otimes_{\mathbb{Z}} \mathbb{F}_p$ when $a^{(1)}$ and $b^{(2)}$ exist, we can prove Theorem 4.5.1. More precisely, we deduce Theorem 4.5.1 from the main theorem of Part I (restated in this paper as Theorem 1.3.7).

Both of these theorems express a criterion for $\dim_{\mathbb{F}_p} R/pR > 3$, and our work is to draw an equivalence between these criteria. The criterion of Theorem 4.5.1 is expressed in terms of certain twisted-Heisenberg extension of $\mathbb{Q}$, which we now set up. Assuming $a^{(1)}$ and $b^{(2)}$ both exist, we construct a lattice of C_p-extensions



in which each C_p-extension is generated by the p-th root of the S-unit labeling it. Note that while this constructive definition of K'/K and K''/K suffices for the purposes of this section, we give a number-theoretic characterization of these extensions in Propositions 6.1.2 and 6.2.2, respectively.

Having defined these fields, we state this paper's main theorem.

Theorem 4.5.1 *We have* $\dim_{\mathbb{F}_p} R/pR > 3$ *if and only if (i) and (ii) hold:*

(i) all primes of K *over* ℓ_1 *split in* K'/K*;*
(ii) there exists some prime of K *over* ℓ_0 *that splits in both* K'/K *and* K''/K*.*

In particular, when $\dim_{\mathbb{F}_p} R/pR = 3$*, we have* $R = \mathbb{T}$*.*

Theorem 4.5.1 follows directly from the following key lemma relating the criterion "$a^{(1)}|_{\ell_1} = 0$ and $\alpha^2 + \beta = 0$" of Theorem 1.3.7 to the criterion of Theorem 4.5.1.

Lemma 4.5.2 *We have the following equivalences.*

(1) $a^{(1)}|_{\ell_1} = 0$ *if and only if all primes of* K *over* ℓ_1 *split in* K'/K
(2) $\alpha^2 + \beta = 0$ *if and only if there exists some prime of* K *over* ℓ_0 *that splits in both* K'/K *and* K''/K*.*

Proof The first equivalence is standard. For the second equivalence, recall that we have arranged for $\alpha = 0$ via our choice in pinning data. So, $\alpha^2 + \beta = 0$ if and only if $\beta = 0$. Thus, if $\alpha^2 + \beta = 0$, the distinguished prime of K over ℓ_0 satisfies the desired property: it splits in both K'/K and K''/K.

On the other hand, if we assume that there exists some place $\mathcal{L}_0'$ of K at ℓ_0 that splits in both K'/K and K''/K, our goal is to prove that $\beta = 0$. By Lemma 4.2.4, we know that this place lies in the Δ-orbit of the distinguised prime $\mathcal{L}_0$ of K over ℓ_0, so let $\sigma \in \Delta$ such that $\sigma(\mathcal{L}_0) = \mathcal{L}_0'$ and consider the homomorphism

$$\nu = \begin{pmatrix} \omega & b^{(1)} & \omega a^{(1)} & b^{(2)} \\ 0 & 1 & \omega c^{(1)} & d^{(1)} \\ 0 & 0 & \omega & b^{(1)} \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

We see that the conjugate of ν by σ—that is, $\tau \mapsto \nu(\sigma^{-1}\tau\sigma)$—has its $b^{(2)}$-coordinate vanishing at ℓ_0. Its $b^{(2)}$-coordinate would be given by $\omega(\sigma^{-1}) \cdot b^{(2)}$. Therefore, $b^{(2)}$ also vanishes at ℓ_0, which means $\beta = 0$. □

Algorithms to verify conditions in Theorem 4.5.1

To check condition (i) in Theorem 4.5.1, i.e, whether $a^{(1)}|_{\ell_1} = 0$, we apply Theorem 4.1.2(2) in the Kummer extension K'/K generated by $a^{(1)}|_{G_K} \in K^\times \otimes_{\mathbb{Z}} \mathbb{F}_p$.

Algorithm 5: Verify condition (i) in Theorem 4.5.1

Input: $a^{(1)}|_{G_K} \in (K^\times \otimes_{\mathbb{Z}} \mathbb{F}_p)^{\Delta=\omega}$
Output: True if $a^{(1)}|_{\ell_1} = 0$; False otherwise

(1) If $a^{(1)}|_{G_K}$ is a pth power mod $\mathfrak{L}$ for each prime $\mathfrak{L}$ in K above ℓ_1, return True.
(2) Else, return False.

Assuming Algorithm 5 returns True, we proceed to check condition (ii) in Theorem 4.5.1, i.e., whether $\beta = 0$, by applying Theorem 4.1.2(2) in the Kummer extension K''/K generated by $b^{(2)}|_{G_K} \in K^\times \otimes_{\mathbb{Z}} \mathbb{F}_p$.

Algorithm 6: Verify condition (*ii*) in Theorem 4.5.1

Input: $b^{(2)}|_{G_K} \in (K^\times \otimes_{\mathbb{Z}} \mathbb{F}_p)^{\Delta=\omega^0}$
Input: $\mathfrak{L}_0$, the distinguished prime of K over ℓ_0 (from Algorithm 2)
Output: True if $\beta = 0$; False otherwise

(1) If $b^{(2)}|_{G_K}$ is a pth power mod $\mathfrak{L}_0$, return True.

(2) Else, return False.

Remark 4.5.3 While our goal in this section has been to verify whether $\alpha^2 + \beta$ vanishes as an element in $\mathbb{F}_p(2)$, we could instead compute $\alpha^2 + \beta$ as a canonical element in $\mu_p^{\otimes 2}$. (See [Part I, Sect. 8] for a precise explanation of what we mean by "canonical" in this setting.) The key observation required to compute $\alpha^2 + \beta$ as an element in $\mu_p^{\otimes 2}$ is that under the isomorphisms

$$\mathbb{F}_p(1) \cong \mu_p, \quad \mathbb{F}_p(-1) \cong \mu_p^{\otimes -1}$$

induced by our choice of $\zeta_p \in \mu_p$, the ratio of $b_0(\gamma_0)$ and $c^{(1)}(\gamma_0)$ is $\zeta_p \otimes \zeta_p \in \mu_p^{\otimes 2}$. Then, assuming that we have arranged for $\alpha = 0$, we can compute $\alpha^2 + \beta$ as $\zeta_p \otimes \zeta_p^e \in \mu_p^{\otimes 2}$, where e is equal to $b^{(2)}|_{\mathfrak{L}_0}(\gamma_0)$.

5 Computed examples

Using Sage [11], we have computed whether the conditions in the main Theorem 4.5.1 hold for a wide selection of examples with $p = 5, 7$. To summarize our results, every example for which our algorithm completed within the allotted time is consistent with our conjecture that $R = \mathbb{T}$. Specifically, we either:

- compute that (*i*) and (*ii*) of Theorem 4.5.1 are satisfied, and hence

  $$\dim_{\mathbb{F}_p} R/pR \geq 4,$$

  and independently compute that $\mathrm{rank}_{\mathbb{Z}_p}(\mathbb{T}) \geq 4$, or
- compute that (*ii*) of Theorem 4.5.1 is not satisfied, and hence $R = \mathbb{T}$.

Remark 5.0.1 A particularly interesting computational observation is that condition (*i*) in Theorem 4.5.1 has been satisfied in every example computed to date. We have been unable to explain why we might always expect $a^{(1)}|_{\ell_1} = 0$ from a theory perspective but hope to either do so in future work or find an example in which $a^{(1)}|_{\ell_1} \neq 0$.

5.1 Scope of computations

Our program for checking the conditions in Theorem 4.5.1, available online at https://github.com/cmhsu2012/RR3, is written for Sage Version 9.2 and implements the algorithms outlined in Sect. 4 using the S-units interface to Pari/GP. All of our computations were carried out using either the Strelka Computer Cluster[2] or the SMP Cluster[3] with an allotted computing time of 3 days per example.

We have attempted to verify whether the conditions in Theorem 4.5.1 hold for the triples (p, ℓ_0, ℓ_1) that satisfy Assumption 2.1.1 and are in the following ranges:

- $(5, \ell_0, \ell_1)$ with $\ell_0 \leq 100$ and $\ell_1 \leq 1000$,
- $(7, \ell_0, \ell_1)$ with $\ell_0 \leq 50$ and $\ell_1 \leq 500$.

For computational convenience when reducing S-units modulo p-powers, our program also requires that p does not divide the class number of $K = \mathbb{Q}(\zeta_p, \ell_1^{1/p})$. In these ranges, this additional assumption excludes only one triple, (7, 29, 347).

The most common Sage error that prevented the program from finishing–other than the program simply timing out–was the Sage interface for the Pari S-unit functionalities that led to high inefficiency or even memory overflow in some cases.[4] When $p \geq 11$, our method for computing the S-unit $a_0|_{G_{\mathbb{Q}(\zeta_p)}} \in \mathbb{Q}(\zeta_p)^\times \otimes_{\mathbb{Z}} \mathbb{F}_p$ used in Algorithm 2 becomes infeasible for the 3-day time constraint.

5.2 A complete example

Let $p = 5$, $\ell_0 = 11$, and $\ell_1 = 23$. To set-up for our computations, we construct the number field $K = \mathbb{Q}(\zeta_5, \sqrt[5]{23})$. Taking S denote the set of primes over ℓ_0, we also construct S-unit groups $U_{\mathbb{Q}(\zeta_5),S}$ and $U_{K,S}$, which have respective ranks 5 and 29 as $\mathbb{Z}$-modules. In particular, in Sage, we represent lines in $U_{\mathbb{Q}(\zeta_5),S} \otimes_{\mathbb{Z}} \mathbb{F}_5$ and $U_{K,S} \otimes_{\mathbb{Z}} \mathbb{F}_5$ as elements of $\mathbb{P}^5(\mathbb{F}_5)$ and $\mathbb{P}^{29}(\mathbb{F}_5)$, respectively. Lastly, we check that 5 wildly ramifies in $K/\mathbb{Q}$, which affects the method for computing the local adjustments in Algorithms 1 and 3.

To construct $a^{(1)}$ and $b^{(2)}$, we start by computing $a_0|_{G_{\mathbb{Q}(\zeta_5)}} = (1, 0, 2, 3, 4, 1)$ and $c = (3, 4, 4, 4, 1, 1)$ in $U_{\mathbb{Q}(\zeta_5),S} \otimes_{\mathbb{Z}} \mathbb{F}_5$ through a brute-force check of the lines in $\mathbb{P}^5(\mathbb{F}_5)$, searching for the Kummer extensions of $\mathbb{Q}(\zeta_5)$ uniquely characterized by the definitions of a_0 and c. Next, we translate the conditions $\gamma \in (K^\times \otimes_{\mathbb{Z}} \mathbb{F}_5)^{\Delta=\omega^2}$ and $\mathrm{Nm}_{K/\mathbb{Q}(\zeta_5)}(\gamma) = c$ into a system of linear equations and solve to obtain

$$\gamma = (2, 0, 1, 4, 0, 4, 1, 4, 2, 0, 0, 0, 0, 0, 4, 0, 4, 0, 0, 0, 0, 0, 0, 1, \ldots, 0) \in U_{K,S} \otimes_{\mathbb{Z}} \mathbb{F}_5.$$

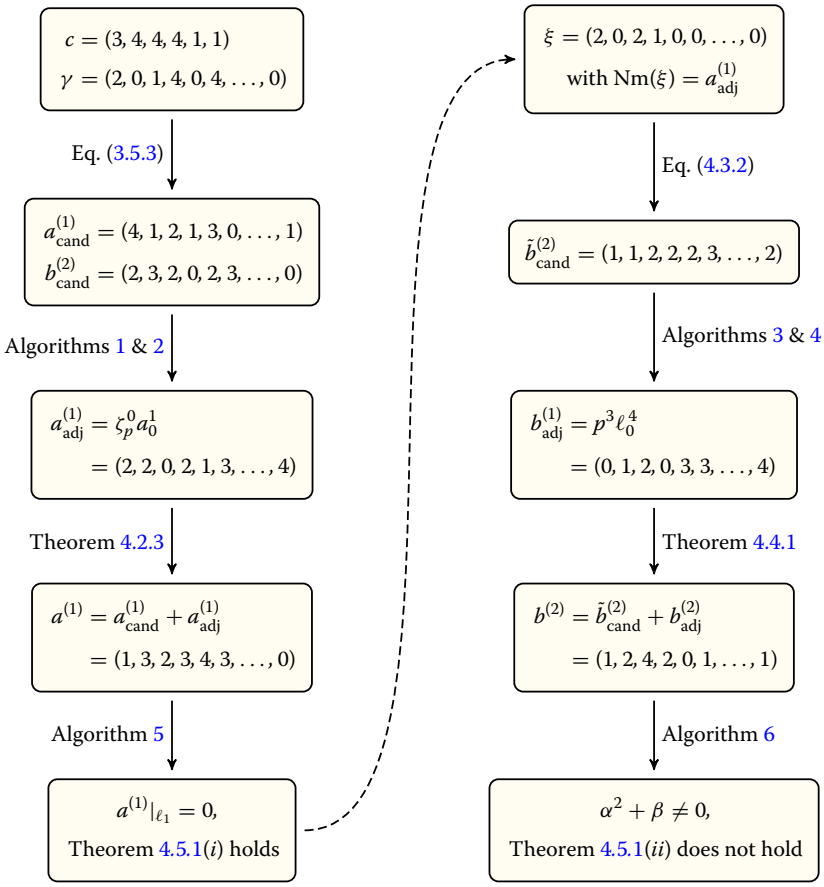
Using the formulas in Theorem 3.5.1, we can now compute $a^{(1)}_{\mathrm{cand}}$ and $b^{(2)}_{\mathrm{cand}}$ and proceed to our computation of the required local adjustments.

[2] The Strelka Computer Cluster is located at Swarthmore College. Its technical specifications can be found at https://kb.swarthmore.edu/display/ACADTECH/Strelka+Computer+Cluster.

[3] The HTC Cluster is located at the Center for Research Computing at the University of Pittsburgh. Its technical specifications can be found at https://crc.pitt.edu/resources.

[4] This problem is in the process of being fixed by Sage and Pari developers and is logged at https://trac.sagemath.org/ticket/31327.

The diagram below follows the organization and notation of Sect. 4, giving the output at each step of our implementation. To ease notation in this diagram, we omit subscripts, such as "$|_{G_K}$", from the names of 1-cocycles. While subtleties of course arise, especially in making sure that the algorithms are compatible with each other, our implementation is largely straightforward, so we refer the reader to our Sage code for further details.



Since Theorem 4.5.1(*ii*) fails, we conclude $\dim_{\mathbb{F}_p}(R/pR) = 3$, and hence, $R = \mathbb{T}$.

5.3 Tables

For each choice of (p, ℓ_0, ℓ_1) in Tables 1-6, we provide the following data related to the construction of K'/K and K''/K:

- The first three columns specify primes (p, ℓ_0, ℓ_1) satisfying Assumption 2.1.1.
- The next two columns of "β difficulty factors" indicate the two influences, outlined in Sect. 2.6, on the difficulty of the computations of the correct adjustments to $b^{(2)}$ to find β; these computations are not strictly necessary to verify the conditions in Theorem 4.5.1 but can simplify the finite-flat adjustment computations significantly. Note that DNC stands for "did not complete" within 3 days.
- The next four columns are the adjustments for the local conditions on $a^{(1)}$ and $b^{(2)}$ discussed in Sect. 4:
  - ζ_p^i and $a_0^j = a_0|^j_{G_{\mathbb{Q}(\zeta_p)}}$ give $a^{(1)}_{\text{adj}}$, influencing α;
  - p^k and ℓ_0^m give $b^{(2)}_{\text{adj}}$, influencing β.

  Note that we record the exponents i, j, k, m of these adjustments in the tables.

Table 1 $p = 5, \ell_0 = 11$

Primes			β difficulty factors		Local adjustments				Conclusion	Hecke rank
					$a^{(1)} \rightsquigarrow \alpha$		$b^{(2)} \rightsquigarrow \beta$			
p	ℓ_0	ℓ_1	p in K	$a^{(1)}\vert_p$	ζ_p^i	d_0^j	p^k	ℓ_0^m	$\alpha^2 + \beta = 0$?	rk($\mathbb{T}$)
5	11	23	Wild	$\neq 0$	0	1	3	4	No	3
5	11	43	Tame	$\neq 0$	3	2	0	4	Yes	≥ 4
5	11	67	Wild	$\neq 0$	0	0	1	3	No	3
5	11	197	Wild	$\neq 0$	0	2	1	4	Yes	≥ 4
5	11	263	Wild	$= 0$	0	2	4	3	No	3
5	11	307	Tame	$= 0$	1	3	0	0	No	3
5	11	373	Wild	$\neq 0$	0	4	0	3	No	3
5	11	397	Wild	$\neq 0$	0	4	2	3	No	3
5	11	593	Tame	$= 0$	0	3	0	2	No	3
5	11	683	Wild	$= 0$	0	4	3	0	Yes	≥ 4
5	11	727	Wild	$\neq 0$	0	1	1	3	Yes	≥ 4
5	11	857	Tame	$\neq 0$	2	0	0	4	No	3
5	11	967	Wild	$\neq 0$	0	0	2	2	No	3
5	11	1013	Wild	$\neq 0$	0	3	3	1	No	3

Table 2 $p = 7, \ell_0 = 29$

Primes			β difficulty factors		Local adjustments				Conclusion	Hecke rank
					$a^{(1)} \rightsquigarrow \alpha$		$b^{(2)} \rightsquigarrow \beta$			
p	ℓ_0	ℓ_1	p in K	$a^{(1)}\vert_p$	ζ_p^i	d_0^j	p^k	ℓ_0^m	$\alpha^2 + \beta = 0$?	rk($\mathbb{T}$)
7	29	17	Wild	DNC	0	3	0	0	No	3
7	29	157	Wild	DNC	0	6	4	4	No	3
7	29	521	Tame	$\neq 0$	3	6	0	2	Yes	≥ 4

- The second rightmost column says whether condition (*ii*) in Theorem 4.5.1 holds. Since condition (*i*) in Theorem 4.5.1 has been satisfied in all computed examples so far, we do not record this in our tables. As such, the second rightmost column gives the conclusion of Theorem 4.5.1.
- As a check on our main computations, the rightmost column gives the rank of $\mathbb{T}$, computed independently using modular symbols. Note that "$\geq 4^*$" means that this computation did not complete within 3 days but allowed for the Hecke rank to be at least 4 after checking the first 20 Hecke operators.

Table 7 provides some additional examples in which large values of ℓ_1 prevent a direct computation of the Hecke rank via modular symbols. So, although our computations have not been independently verified for these examples, we can conclude that the Hecke rank is 3 when condition (*ii*) in Theorem 4.5.1 fails.

Table 3 $p = 5, \ell_0 = 41$

	Primes		β difficulty factors		Local adjustments				Conclusion	Hecke rank
					$a^{(1)} \rightsquigarrow \alpha$		$b^{(2)} \rightsquigarrow \beta$			
p	ℓ_0	ℓ_1	p in K	$a^{(1)}\vert_p$	ζ_p^i	d_0^j	p^k	ℓ_0^m	$\alpha^2 + \beta = 0$?	rk($\mathbb{T}$)
5	41	73	Wild	$\neq 0$	0	4	2	1	Yes	≥ 4
5	41	83	Wild	$\neq 0$	0	4	3	3	No	3
5	41	137	Wild	$\neq 0$	0	3	2	0	No	3
5	41	163	Wild	$\neq 0$	0	2	3	1	No	3
5	41	167	Wild	$\neq 0$	0	2	4	0	No	3
5	41	173	Wild	$= 0$	0	0	3	2	No	3
5	41	383	Wild	$= 0$	0	3	2	2	No	3
5	41	547	Wild	$\neq 0$	0	3	0	0	No	3
5	41	577	Wild	$\neq 0$	0	0	2	0	Yes	$\geq 4^*$
5	41	683	Wild	$\neq 0$	0	2	3	0	No	3
5	41	983	Wild	$\neq 0$	0	1	4	1	Yes	$\geq 4^*$

Table 4 $p = 5, \ell_o = 61$

	Primes		β difficulty factors		Local adjustments				Conclusion	Hecke rank
					$a^{(1)} \rightsquigarrow \alpha$		$b^{(2)} \rightsquigarrow \beta$			
p	ℓ_0	ℓ_1	p in K	$a^{(1)}\vert_p$	ζ_p^i	d_0^j	p^k	ℓ_0^m	$\alpha^2 + \beta = 0$?	rk($\mathbb{T}$)
5	61	13	Wild	$\neq 0$	0	2	2	3	No	3
5	61	47	Wild	$\neq 0$	0	0	1	0	Yes	≥ 4
5	61	197	Wild	$= 0$	0	3	4	3	No	3
5	61	257	Tame	$\neq 0$	2	0	0	4	No	3
5	61	337	Wild	$= 0$	0	0	1	1	No	3
5	61	353	Wild	$\neq 0$	0	3	4	3	No	3
5	61	367	Wild	$\neq 0$	0	1	4	2	No	3
5	61	487	Wild	$\neq 0$	0	4	4	3	Yes	$\geq 4^*$
5	61	563	Wild	$\neq 0$	0	4	3	1	No	3
5	61	733	Wild	$\neq 0$	0	0	3	1	No	3
5	61	853	Wild	$\neq 0$	0	4	1	2	Yes	$\geq 4^*$
5	61	977	Wild	$\neq 0$	0	3	2	2	Yes	$\geq 4^*$

Table 5 $p = 5, \ell_0 = 71$

	Primes		β difficulty factors		Local adjustments				Conclusion	Hecke rank
					$a^{(1)} \rightsquigarrow \alpha$		$b^{(2)} \rightsquigarrow \beta$			
p	ℓ_0	ℓ_1	p in K	$a^{(1)}\vert_p$	ζ_p^i	d_0^j	p^k	ℓ_0^m	$\alpha^2 + \beta = 0$?	rk($\mathbb{T}$)
5	71	23	Wild	$\neq 0$	0	0	0	2	No	3
5	71	37	Wild	$\neq 0$	0	4	2	1	No	3
5	71	97	Wild	$= 0$	0	3	2	3	No	3
5	71	103	Wild	$\neq 0$	0	2	2	3	No	3
5	71	193	Tame	$\neq 0$	2	2	0	3	No	3
5	71	233	Wild	$= 0$	0	3	1	2	Yes	$\geq 4^*$
5	71	283	Wild	$\neq 0$	0	1	3	0	No	3
5	71	307	Tame	$\neq 0$	3	2	0	3	No	3
5	71	463	Wild	$\neq 0$	0	4	0	0	No	3
5	71	853	Wild	$\neq 0$	0	2	0	4	No	3

Table 6 $p = 7, \ell_o = 43$

	Primes		β difficulty factors		Local adjustments				Conclusion	Hecke rank
					$a^{(1)} \rightsquigarrow \alpha$		$b^{(2)} \rightsquigarrow \beta$			
p	ℓ_0	ℓ_1	p in K	$a^{(1)}\vert_p$	ζ_p^i	d_0^j	p^k	ℓ_0^m	$\alpha^2 + \beta = 0$?	rk($\mathbb{T}$)
7	43	37	Wild	DNC	0	5	0	1	Yes	≥ 4
7	43	79	Tame	$\neq 0$	2	4	0	3	No	3

Table 7 Examples without an independent computation of Hecke rank

	Primes		β difficulty factors		Local adjustments				Conclusion
					$a^{(1)} \rightsquigarrow \alpha$		$b^{(2)} \rightsquigarrow \beta$		
p	ℓ_0	ℓ_1	p in K	$a^{(1)}\vert_p$	ζ_p^i	d_0^j	p^k	ℓ_0^m	$\alpha^2 + \beta = 0$?
5	41	653	Wild	$= 0$	0	2	1	0	Yes
5	41	823	Wild	$= 0$	0	0	1	3	No
5	61	743	Tame	$= 0$	2	0	0	4	No
5	61	883	Wild	$\neq 0$	0	0	4	2	No
5	61	997	Wild	$\neq 0$	0	0	3	2	No
5	71	613	Wild	$= 0$	0	4	2	1	No
5	71	673	Wild	$\neq 0$	0	2	2	1	No
5	71	733	Wild	$\neq 0$	0	4	1	3	No

6 Algebraic number theory

While the C_p-extensions K'/K and K''/K in Theorem 4.5.1 are defined in terms of the cochains $a^{(1)}$ and $b^{(2)}$, an intrinsic characterization is desirable. These fields are not Galois over $\mathbb{Q}$; accordingly, they depend on choices, such as the pinning data. In this section, we will characterize the Galois closures (over $\mathbb{Q}$) M' of K' and M'' of K'', and characterize the isomorphism class of subfields of M'' to which K' and K'' belong. This establishes the descriptions of K' and K'' used to state the main theorem in the introduction (Theorem 1.2.1). Additionally, this allows us to rephrase the conditions of the main Theorem 4.5.1 in order to refer to the decomposition subgroups of $\mathrm{Gal}(M''/\mathbb{Q})$ for primes over ℓ_0. This translation appears in Theorem 6.4.2 as well as in another form in Theorem 6.5.2.

6.1 The extensions M'/M and K'/K

To describe M'/M and K'/K, the 3-dimensional $G_{\mathbb{Q},Np}$-representation of (1.4.1) is a convenient tool; it is

$$\upsilon = \begin{pmatrix} \omega & b^{(1)} & \omega a^{(1)}_{\mathrm{cand}} \\ 0 & 1 & \omega c^{(1)} \\ 0 & 0 & \omega \end{pmatrix} : G_{\mathbb{Q},Np} \to \mathrm{GL}_3(\mathbb{F}_p), \tag{6.1.1}$$

where we view $a^{(1)}_{\mathrm{cand}}$ as a general choice of matrix entry making υ a homomorphism. We recall that $K/\mathbb{Q}(\zeta_p)$ is cut out by $b^{(1)}$, $L/\mathbb{Q}(\zeta_p)$ is cut out by $c^{(1)}$, $M = KL/\mathbb{Q}(\zeta_p)$ is cut out by $(b^{(1)}, c^{(1)})$, K'/K is cut out by $a^{(1)}$, and $M'/\mathbb{Q}$ is cut out by the entire representation υ when we let $a^{(1)}_{\mathrm{cand}} = a^{(1)}$.

To state the proposition, some notation and terminology is needed. Let F/M be its maximal extension that is ramfied only at primes dividing Np, abelian, of exponent p, and Galois over $\mathbb{Q}$. We also call a number field extension A'/A ℓ_0-*split* to briefly say that all primes of A over ℓ_0 are split in A'/A.

Proposition 6.1.2 *M'/M is the unique unramified and ℓ_0-split C_p-extension contained in F whose Galois group is coinvariant under the conjugation action of* $\mathrm{Gal}(M/\mathbb{Q})$ *on* $\mathrm{Gal}(F/M)$*. The isomorphism class of K'/K is characterized by being a C_p-extension contained in M' and not equal to M/K.*

Proof Let M'_{cand}/M be a C_p-extension contained in F/M whose Galois group is coinvariant under the conjugation action of $\mathrm{Gal}(M/\mathbb{Q})$ on $\mathrm{Gal}(F/M)$. A central extension sequence arises from M'_{cand},

$$1 \to \mathrm{Gal}(M'_{\mathrm{cand}}/M) \to \mathrm{Gal}(M'_{\mathrm{cand}}/\mathbb{Q}) \to \mathrm{Gal}(M/\mathbb{Q}) \to 1.$$

Using the semi-direct product decomposition

$$\mathrm{Gal}(M/\mathbb{Q}) = \mathrm{Gal}(M/\mathbb{Q}(\zeta_p)) \rtimes \mathrm{Gal}(M/\mathbb{Q}(\ell_1^{1/p}, c^{(1)}) =: \mathrm{Gal}(M/\mathbb{Q}(\zeta_p)) \rtimes \Delta,$$

and the description of group cohomology of a semi-direct product of [16], we find that the element of $H^2(\mathrm{Gal}(M/\mathbb{Q}), \mathrm{Gal}(M'_{\mathrm{cand}}/M))$ determined by $\mathrm{Gal}(M'_{\mathrm{cand}}/\mathbb{Q})$ arises from $H^2(\mathrm{Gal}(M_{\mathrm{cand}}/\mathbb{Q}(\zeta_p), \mathrm{Gal}(M'_{\mathrm{cand}}/M))^{\Delta}$. We use the natural isomorphism $\Delta \cong \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ and represent its actions on $\mathbb{F}_p$-vector spaces according the usual notation $\mathbb{F}_p(i)$ for $i \in \mathbb{Z}$. Since $\mathrm{Gal}(M/\mathbb{Q}(\zeta_p)) \simeq \mathbb{F}_p(-1) \times \mathbb{F}_p(1)$ and $\mathrm{Gal}(M'_{\mathrm{cand}}/M) \simeq \mathbb{F}_p(0)$, standard calculations yield that

$$H^2(\mathrm{Gal}(M_{\mathrm{cand}}/\mathbb{Q}(\zeta_p), \mathrm{Gal}(M'/M))^{\Delta}$$

is 1-dimensional. Since the class of $\mathrm{Gal}(M'_{\mathrm{cand}}/\mathbb{Q})$ as a central extension is non-trivial, as is the extension generated by the group $\mathrm{Gal}(M/\mathbb{Q})$, they are equal up to a scalar and therefore isomorphic. The upshot is that we obtain a faithful matrix representation of $\mathrm{Gal}(M'_{\mathrm{cand}}/\mathbb{Q})$, just like the faithful representation (6.1.1) of $\mathrm{Gal}(M'/\mathbb{Q})$.

The upper right coordinate of this matrix representation yields a new $a^{(1)}_{\mathrm{cand}} : G_{\mathbb{Q},Np} \to \mathbb{F}_p$ such that $-da^{(1)}_{\mathrm{cand}} = b^{(1)} \smile c^{(1)}$. The conclusion of what we have argued so far is that C_p-extensions of M contained in F/M whose Galois groups that are coinvariant for the action of $\mathrm{Gal}(M/\mathbb{Q})$ correspond with solutions $a^{(1)}_{\mathrm{cand}}$ to $-da^{(1)}_{\mathrm{cand}} = b^{(1)} \smile c^{(1)}$. This correspondence is bi-directional, and it is not necessary to refine this statement in order to obtain a bijection.

Let us fix a corresponding pair M'_{cand} and $a^{(1)}_{\mathrm{cand}}$, also letting K'_{cand}/K be the C_p-extension of K cut out by $a^{(1)}_{\mathrm{cand}}|_{G_K}$, and review the local conditions characterizing $a^{(1)}$ that are stated in Proposition 2.3.1. In order to complete the proof using this correspondence, we claim that $a^{(1)}_{\mathrm{cand}}$ satisfies the local conditions of Proposition 2.3.1 if and only if M'_{cand}/M is unramified. Then the uniqueness of M'/M, claimed here, will follow from the uniqueness of $a^{(1)}$ proved in Proposition 2.3.1.

We first prove that M'_{cand}/M is unramified and ℓ_0-split if and only if the local conditions of Proposition 2.3.1 hold true for $a^{(1)}_{\mathrm{cand}}$. We will use the following implication of the fact that both M' and M are Galois over $\mathbb{Q}$ throughout the argument: M'/M being unramified at a single prime of M over a rational prime q is equivalent to M'/M being unramified at all primes of M over q. A similar statement applies to the ℓ_0-split condition. We also implicitly use the fact that $a^{(1)}_{\mathrm{cand}}|_{G_M}$ cuts out M'/M.

Unconditionally, M'/M is unramified at all primes of M over ℓ_1. Becuase $a^{(1)}_{\mathrm{cand}}|_{\ell_1} : G_{\ell_1} \to \mathbb{F}_p$ is a cocycle (since $b^{(1)}|_{\ell_1} = 0$), it is automatically unramified. Thus $a^{(1)}_{\mathrm{cand}}|_{G_M}$ is unramified at ℓ_1.

M'/M **is ℓ_0-split if and only if condition (c) holds.** Condition (c) of Proposition 2.3.1, imposed on $a^{(1)}_{\mathrm{cand}}$, is equivalent to the two non-zero homomorphisms

$$c^{(1)}|_{\ell_0} : G_{\ell_0} \to \mathbb{F}_p(-1), \quad a^{(1)}|_{\ell_0} : G_{\ell_0} \to \mathbb{F}_p$$

having identical kernels. Since M/K is cut out by $c^{(1)}|_{G_K}$, we deduce that $a^{(1)}|_{G_M}$ vanishes at the distinguished prime over ℓ_0 if and only if M'/M is ℓ_0-split.

M'/M **is unramified at all primes of M over p if and only if condition (a) holds.** Condition (a) of 2.3.1 reads that $(a^{(1)}_{\mathrm{cand}} + b^{(1)} \smile x_c)|_{I_p} = 0$. Let $L_c \subset L$ be the subfield fixed by $\mathbb{F}_p^\times$ under the isomorphism

$$\mathrm{Gal}(L/\mathbb{Q}) \xrightarrow{\sim} \mathbb{F}_p^\times \ltimes \mathbb{F}_p \xrightarrow[\left(\begin{smallmatrix} 1 & \omega c^{(1)} \\ 0 & \omega \end{smallmatrix}\right)]{\sim} \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \subset \mathrm{GL}_2(\mathbb{F}_p).$$

This $L_c/\mathbb{Q}$ has degree p and its Galois closure is $L/\mathbb{Q}$. It is a brief exercise to check that $a^{(1)}|_{G'_p}$ is a cocycle and condition (a) is equivalent to $a^{(1)}_{\mathrm{cand}}|_{I'_p} = 0$, where $I'_p \subset G'_p \subset G_{\mathbb{Q},Np}$ is an alternate choice of decomposition group and inertia group at p such that the alternate distinguished prime has trivial ramification degree in $L_c/\mathbb{Q}$. Using the facts about M'/M listed above, we conclude that $a^{(1)}_{\mathrm{cand}}|_{I'_p} = 0$ if and only if M'/M is unramified at all primes of M over p.

Finally, we establish the claimed characterization of K'/K as a C_p-extension contained in M'/K. Under the isomorphism υ, the subgroup $\mathrm{Gal}(M'/K) \subset \mathrm{Gal}(M'/\mathbb{Q})$ is identified with the subgroup of $\mathrm{GL}_3(\mathbb{F}_p)$ isomorphic to $\mathbb{F}_p \oplus \mathbb{F}_p$ that differs from the identity matrix in the $b^{(1)}$ and $a^{(1)}$-coordinates. Consider the action of $\mathrm{Gal}(K/\mathbb{Q})$ by conjugation on the $p+1$ subgroups of $\mathrm{Gal}(M'/K)$ of order p. One of them is fixed (the one concentrated in the $a^{(1)}$-coordinate), and has fixed field M. The remaining p are a single orbit. Therefore, any of their fixed fields are isomorphic, and one of them is K'. □

6.2 The extensions M''/M' and K''/K

Recall that the cochain $b^{(2)}$ satisfying differential equation (1.3.4) exists if and only if $a^{(1)}|_{\ell_1} = 0$. When $b^{(2)}$ does not exist, we consider K'' undefined and let $M'' = M'$.

For the rest of this section, we assume that $b^{(2)}$ does exist. Let K''/K be the extension cut out by $b^{(2)}|_{G_K}$ as usual, and let M'' denote the Galois closure of K'' over $\mathbb{Q}$. Our goal is to describe these extensions using the 4-dimensional $G_{\mathbb{Q},Np}$-representation of (1.4.2),

$$\nu := \begin{pmatrix} \omega & b^{(1)} & \omega a^{(1)} & b^{(2)} \\ 0 & 1 & \omega c^{(1)} & d^{(1)} \\ 0 & 0 & \omega & b^{(1)} \\ 0 & 0 & 0 & 1 \end{pmatrix} : G_{\mathbb{Q},Np} \to \mathrm{GL}_4(\mathbb{F}_p). \tag{6.2.1}$$

Note that $d^{(1)} = a^{(1)} - b^{(1)}c^{(1)}$, so that $M'' = \overline{\mathbb{Q}}^{\ker \nu}$ is a C_p-extension of $M' = \overline{\mathbb{Q}}^{\ker \upsilon}$ cut out by $b^{(2)}|_{G_{M'}}$. In addition to satisfying the differential equation required to make ν a homomorphism, we recall that $b^{(2)} \in C^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1))$ is characterized by the local conditions of Proposition 2.4.2, but only up to addition by the subspace of cocycles spanned by $\{b^{(1)}, dx\}$ for some choice of non-zero $x \in \mathbb{F}_p(1)$. However, since $b^{(1)}|_{G_K} = 0$, such changes to $b^{(2)}$ do not change the kernel of ν. We therefore may and do regard the Galois extension $M''/\mathbb{Q}$ as well-defined.

To state the proposition, let F'/M' be its maximal extension that is ramfied only at primes dividing Np, abelian, of exponent p, and Galois over $\mathbb{Q}$. Let $\mathfrak{m}^{\mathrm{flat}}$ be the modulus

of M' (in the sense of ray class field theory) defined as the product of all squares of primes of M' over p; that is,

$$\mathfrak{m}^{\text{flat}} := \prod_{\mathfrak{p}|(p)} \mathfrak{p}^2.$$

Finally, when V is an irreducible $\mathbb{F}_p$-linear representation of $\mathrm{Gal}(M'/\mathbb{Q})$, we say that an intermediate field F'', $F' \supset F'' \supset M$, is *V-equivariant* when $\mathrm{Gal}(F'/M) \otimes_{\mathbb{F}_p} V \twoheadrightarrow \mathrm{Gal}(F''/M) \otimes_{\mathbb{F}_p} V$ factors through the coinvariants of the $\mathrm{Gal}(M/\mathbb{Q})$-action (by conjugation in $\mathrm{Gal}(F/\mathbb{Q})$).

Proposition 6.2.2 *Assume that $a^{(1)}|_{\ell_1} = 0$. Then M''/M' is the unique C_p-extension contained in F' such that it has conductor $\mathfrak{m}^{\text{flat}}$, it is ℓ_0-split, and its Galois group's $\mathrm{Gal}(M'/\mathbb{Q})$-action is $\mathbb{F}_p(1)$-equivariant. The isomorphism class of K''/K is characterized by being a C_p-extension contained in M'', not contained in M', and having cardinality p.*

We can rephrase the proposition in terms of a ray class group. Let C denote the maximal quotient of the ray class group of M' of conductor $\mathfrak{m}^{\text{flat}}$ such that it has exponent p and such that the images of prime ideals over ℓ_0 vanish. We use C_ω to denote the maximal quotient of C whose $\mathrm{Gal}(M'/\mathbb{Q})$-action is ω-isotypic.

Corollary 6.2.3 *The group C_ω has order p if $a^{(1)}|_{\ell_1} = 0$ and has order 1 if $a^{(1)}|_{\ell_1} \neq 0$. The extension of M' associated to C_ω is M''.*

To prove Proposition 6.2.2, first we prove the following local lemma, which justifies calling $\mathfrak{m}^{\text{flat}}$ the "finite-flat modulus." We write "v_p" for the normalized valuation on $\overline{\mathbb{Q}}_p$, that is, the valuation $v_p : \overline{\mathbb{Q}}_p^\times \to \mathbb{Q}$ such that $v_p(p) = 1$. Also, write π_A for the uniformizer of a finite extension $A/\mathbb{Q}_p$. In this lemma, we allow $p \geq 3$, in contrast with our usual assumption that $p \geq 5$.

Lemma 6.2.4 *Let p be an odd prime. Let $F/\mathbb{Q}_p$ be a Galois extension of degree $p^d(p-1)$ that contains $\mathbb{Q}_p(\zeta_p)$ and is contained in a finite extension of $\mathbb{Q}_p$ cut out by the Galois action on the $\bar{\mathbb{Q}}_p$-points of a finite-flat group scheme over $\mathbb{Z}_p$ of exponent p. Let $F \supset H \supset \mathbb{Q}_p$ such that $[F : H] = p$, $H/\mathbb{Q}_p$ is Galois, and F/H is totally ramified. Then the conductor of F/H is $(\pi_H)^2$.*

Remark 6.2.5 As the proof will explain, the statement of the lemma is equivalent to the following formula for the valuation of the different of $F/\mathbb{Q}_p$. If the ramification degree of $F/\mathbb{Q}_p$ is written $p^e(p-1)$, then

$$v_p(\mathrm{Diff}(F/\mathbb{Q}_p)) = \frac{p^{e+1} - 2}{p^e(p-1)}. \tag{6.2.6}$$

Proof The key input is Fontaine's upper bound on the different of an extension $F/\mathbb{Q}_p$ cut out by the action on a finite-flat group scheme: as a particular case of [2, §0.1, Corollaire, pg. 516], we find that

$$v_p(\mathrm{Diff}(F/\mathbb{Q}_p)) < \frac{p}{p-1}.$$

Because differents are multiplicative in towers, this bound on the different also applies to subextensions of $F/\mathbb{Q}_p$.

We prove (6.2.6) by induction. The base case $e = 0$ follows from the standard calculation that $\mathrm{Disc}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p) = (p^{p-2})$; it follows that $\mathrm{Diff}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p) = ((\zeta_p - 1)^{p-2})$, which has absolute valuation $(p-2)/(p-1)$ as desired.

Now we deduce the truth of (6.2.6) for $e' = e + 1$ in place of e from its truth as written. Let $F/\mathbb{Q}_p$ be as in the lemma, with ramification degree $p^{e'}(p-1)$. Since $\mathrm{Gal}(F/\mathbb{Q}_p)$ is solvable and we can always decompose an extension into an unramified extension followed by a totally ramified extension, we may choose an intermediate field H such that $F \supset H \supset \mathbb{Q}_p(\zeta_p)$, F/H is of degree p and ramified, and $\mathrm{Gal}(F/H) \subset \mathrm{Gal}(F/\mathbb{Q}_p)$ is a normal subgroup. Therefore we can apply (6.2.6) to H and conclude that

$$v_p(\mathrm{Diff}(H/\mathbb{Q}_p)) = \frac{p^{e+1} - 2}{p^e(p-1)}.$$

Because the different is multiplicative in towers, Fontaine's bound on $\mathrm{Diff}(F/\mathbb{Q}_p)$ implies that

$$\begin{aligned} &v_p(\mathrm{Diff}(F/H)) \\ &\quad = v_p(\mathrm{Diff}(F/\mathbb{Q}_p)) - v_p(\mathrm{Diff}(H/\mathbb{Q}_p)) < \frac{p}{p-1} - \frac{p^{e+1}-2}{p^e(p-1)} = \frac{2p}{p^{e'}(p-1)}. \end{aligned}$$

On the other hand, because F/H is abelian and ramified, a standard result bounding the possible differents of wildly ramified extensions (see e.g. [10, Thm. 2.6, Ch. III]) states that

$$v_p(\mathrm{Diff}(F/H)) \geq \frac{p}{p^{e'}(p-1)}.$$

Altogether, letting m be the integer satisfying $\mathrm{Diff}(F/H) = (\pi_F)^m$, the bounds above dictate that

$$p \leq m \leq 2p - 1$$

To determine m, we apply the conductor-discriminant formula for F/H, which states that $\mathrm{Cond}(F/H)^{p-1} = \mathrm{Disc}(F/H)$. Note also that $\mathrm{Disc}(F/H) = (\pi_H)^m$. Therefore $(p-1) \mid m$ as well. Because p is odd, the bounds on m imply that $m = 2(p-1)$.

Applying the calculation of m, (6.2.6) follows by calculating

$$\begin{aligned} v_p(\mathrm{Diff}(F/\mathbb{Q}_p)) &= v_p(\mathrm{Diff}(H/\mathbb{Q}_p)) + v_p(\mathrm{Diff}(F/H)) \\ &= \frac{p^{e+1}-2}{p^e(p-1)} + \frac{2p-2}{p^{e'}(p-1)} = \frac{p^{e'+1}-2}{p^{e'}(p-1)} \end{aligned}$$

and $\mathrm{Cond}(F/H) = (\pi_F)^2$, as desired. □

Proof of Proposition 6.2.2 An argument similar to the one appearing in the beginning of the proof of Proposition 6.1.2 proves that a C_p-extension of M' contained in F' and with the $\mathbb{F}_p(1)$-coinvariance property of Proposition 6.1.2 exists if and only if a matrix representation of $G_{\mathbb{Q},Np}$ the form ν cuts it out. Proposition 2.4.2 proves that ν exists if and only if $a^{(1)}|_{\ell_1} = 0$, and that, in that case, there exists a choice of its $b^{(2)}$-coordinate with the properties (a) and (b) of Proposition 2.4.2.

What we will prove is that properties (a) and (b) of a candidate solution $b^{(2)}_{\mathrm{cand}}$ to differential equation (1.3.4) listed in Proposition 2.4.2 hold true if and only if the extension M''_{cand}/M' cut out by $b^{(2)}_{\mathrm{cand}}|_{G_{M'}}$ satisfies the properties listed in Proposition 6.2.2. We have

already observed that, while there is a torsor of possibilities for $b^{(2)}_{\text{cand}}$, the extension M''/M' cut out by $b^{(2)}|_{G_{M'}}$ is nonetheless well-defined. Therefore, the uniqueness of M''/M' will follow.

Unconditionally, M''_{cand}/M' is unramified at all primes of M' over ℓ_1. Under our assumption that $a^{(1)}|_{\ell_1} = 0$, which implies that $d^{(1)}|_{\ell_1} = 0$, the cochain $b^{(2)}_{\text{cand}}|_{\ell_1} : G_{\ell_1} \to \mathbb{F}_p$ is a cocycle, since $-db^{(2)}$ equals $b^{(1)} \smile d^{(1)} + a^{(1)} \smile b^{(1)}$. Therefore, $b^{(2)}_{\text{cand}}|_{\ell_1}$ is in the span of $b^{(1)}$ up to 1-coboundaries. Since 1-coboundaries on G_{ℓ_1} valued in $\mathbb{F}_p(1)$ vanish on inertia and $b^{(1)}|_{G_{M'}} = 0$, we conclude that M''_{cand}/M' is unramified at the distinguished prime over ℓ_1. Because both M' and M''_{cand} are Galois over $\mathbb{Q}$, it follows that all primes of M' over ℓ_1 are unramified in M''_{cand}.

M''_{cand}/M' is ℓ_0-split if and only if condition (a) of Proposition 2.4.2 holds if and only if there exists a $\rho_{2,\text{cand}} : G_{\mathbb{Q},Np} \to E_2^\times$ as in (1.3.2) with $b^{(2)}_{\text{cand}}$ as its $b^{(2)}$-coordinate. A very similar argument to the case of M'_{cand}/M argued in the proof of Proposition 6.1.2 applies to prove the first equivalence. The second equivalence follows directly from [Part I, Lem. 7.1.1(2)].

M''_{cand}/M' has conductor dividing $\mathfrak{m}^{\text{flat}}$ and is ℓ_0- split if and only if $\rho_{2,\text{cand}}$ as in (1.3.2) exists and also satisfies condition (b) of Proposition 2.4.2. Condition (b) states that there exists some ρ_2 as in (1.3.2) such that $\rho_2|_p$ is finite-flat and has $b^{(2)}_{\text{cand}}$ as its $b^{(2)}$-coordinate. Using the previous ℓ_0-local claim, we assume that the corresponding pair $(b^{(2)}_{\text{cand}}, M''_{\text{cand}})$ occurs as the $b^{(2)}$-coordinate of some $\rho_{2,\text{cand}}$, so that it only remains to address the p-local conditions

Assume condition (b) is true. At the distinguished prime v'' of M''_{cand} over p, $(M''_{\text{cand}})_{v''}/\mathbb{Q}_p$ is contained in $\overline{\mathbb{Q}}_p^{\ker \rho_{2,\text{cand}}|_p}$. Condition (b) implies that $\overline{\mathbb{Q}}_p^{\ker \rho_{2,\text{cand}}|_p}/\mathbb{Q}_p$ is cut out by the G_p-action on the $\overline{\mathbb{Q}}_p$-points of a finite-flat group scheme over $\mathbb{Z}_p$ with exponent p. The same statement applies to the subfield $M' \subset M''$ with distinguished prime v' over p. Therefore, by Lemma 6.2.4, the conductor of $(M''_{\text{cand}})_{v''}/M'_{v'}$ is either v'^2 or 1. Because both $M''_{\text{cand}}/\mathbb{Q}$ and $M'/\mathbb{Q}$ are Galois extensions, this local conductor calculation applies to all primes of M' over p. In other words, $\text{Cond}(M''_{\text{cand}}/M') \mid \mathfrak{m}^{\text{flat}}$, as desired.

We next prove the converse: assume that M''_{cand}/M' has conductor dividing $\mathfrak{m}^{\text{flat}}$, having been cut out by $b^{(2)}_{\text{cand}}|_{G_{M'}}$ where the only assumption on $b^{(2)}_{\text{cand}}$ is that it is an element of $C^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1))$ satisfying the differential equation (3.0.1). The set of solutions $b^{(2)}_{\text{cand}}$ is a torsor under $Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1))$, which has basis $\{dx, b_p, b^{(1)}, b_0^{(1)}\}$. By [19, Lem. C.4.1], the set of solutions $b^{(2)}_{\text{cand}}$ making $\nu|_p$ finite-flat are a torsor under the subspace $Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1))^{\text{flat}} = \langle dx, b^{(1)}, b_0^{(1)} \rangle$ computed in [Part I, Lem. 2.2.9], namely,

$$b^{(2)} + Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1))^{\text{flat}}.$$

Lemma 6.2.4 implies that the C_p-extensions of $M'_{v'}$ cut out by $b|_{G_{M'_{v'}}}$ for any $b \in b^{(2)} + Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1))^{\text{flat}}$ satisfies the conductor bound stated in the Lemma. Conversely, one can calculate that the conductor of $b_p|_{G_{\mathbb{Q}_p(\zeta_p)}}$ does not cut out a C_p-extension satisfying the conductor bound, which implies the same result for the C_p-extension of $M'_{v'}$ cut out by $b|_{G_{M'_{v'}}}$ for any

$$b \in \left[b^{(2)} + Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1))\right] \smallsetminus \left[b^{(2)} + Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1))^{\text{flat}}\right].$$

Therefore, because M''_{cand}/M' has conductor bounded by $\mathfrak{m}^{\text{flat}}$, $b^{(2)}_{\text{cand}} \in b^{(2)} + Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1))^{\text{flat}}$, which is equivalent to $\nu|_p$ being finite-flat. According to the torsor

structures on $\Pi_2^{\det}$ and $\Pi_2^{\det,p}$ described in Part I, Lemma 7.1.4 and Part I, Proposition 7.2.1, one can adjust ρ_2 only in its $a^{(2)}$, $c^{(2)}$, and $d^{(2)}$-coordinates to produce a $\rho'_{2,\mathrm{cand}}$ that is finite-flat at p with $b^{(2)}$-coordinate $b^{(2)}_{\mathrm{cand}}$. This completes the claimed equivalence.

It only remains to prove the claimed characterization of K''/K. Under the embedding $\nu : \mathrm{Gal}(M''/\mathbb{Q}) \hookrightarrow \mathrm{GL}_4(\mathbb{F}_p)$ of (6.2.1), the abelian subgroup $\mathrm{Gal}(M''/K)$ admits an isomorphism

$$\left.\begin{pmatrix} a^{(1)} & b^{(2)} \\ c^{(1)} & -a^{(1)} \end{pmatrix}\right|_{G_K} : \mathrm{Gal}(M''/K) \xrightarrow{\sim} V \subset M_2(\mathbb{F}_p) \tag{6.2.7}$$

to the subspace of trace 0 matrices $V \subset M_2(\mathbb{F}_p)$. Likewise, ν produces an isomorphism

$$\begin{pmatrix} \omega & b^{(1)} \\ 0 & 1 \end{pmatrix} : \mathrm{Gal}(K/\mathbb{Q}) \xrightarrow{\sim} B := \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix} \subset \mathrm{GL}_2(\mathbb{F}_p).$$

It follows from the shape of ν in (6.2.1) that the natural conjugation action of $\mathrm{Gal}(K/\mathbb{Q})$ on $\mathrm{Gal}(M''/K)$ matches the usual adjoint action of B on V via these isomorphisms.

Our characterization of K''/K will follow from the following description of orbits of the action of $\mathrm{Gal}(K/\mathbb{Q})$ by conjugation on the p^2+p+1 subgroups of $\mathrm{Gal}(M''/K)$ isomorphic to $C_p \times C_p$, one of which has fixed field equal to K''. Under the isomorphisms above, the following description of five orbits of this action, labeled (a)–(e), matches the listing labeled (a)–(e) in Lemma 6.3.1.

(a) One orbit is a singleton: the one concentrated in the $a^{(1)}$ and $b^{(2)}$-coordinates. Its fixed field is M.
(b) There is an orbit of cardinality p, one of which is the subgroup $\mathrm{Gal}(M''/K') \subset \mathrm{Gal}(M''/K)$, which is concentrated in the $c^{(1)}$ and $b^{(2)}$-coordinates. The fixed fields of its conjugates are the subfields of M'' isomorphic to K', all of which are contained in their common Galois closure, M'.
(c) Another orbit of cardinality p includes the subgroup $\mathrm{Gal}(M''/K'')$ that is concentrated in the $c^{(1)}$ and $a^{(1)}$-coordinates. The fixed fields of its conjugates are the subfields of M'' isomorphic to K''; none of these are contained in M'.
(d) An orbit of cardinality $p(p-1)/2$.
(e) Another orbit of cardinality $p(p-1)/2$.

Because of the running assumption that $p \geq 5$, we conclude that the isomorphism class of K'' is the only isomorphism class of C_p-extensions of K contained in M'' that has cardinality p and also is not contained in M'. □

6.3 Orbits in Grassmannians of the trace zero adjoint representation of the conjugation action of the Borel subgroup

While there is usually a running assumption that $p \geq 5$, in this section only we also allow $p = 3$. Consider the adjoint action of the matrix subgroup

$$B = \mathbb{F}_p^\times \ltimes \mathbb{F}_p \cong \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix} \subset \mathrm{GL}_2(\mathbb{F}_p)$$

on the 3-dimensional $\mathbb{F}_p$-vector subspace $V \subset M_2(\mathbb{F}_p)$ consisting of matrices of trace 0. This induces an action of B on the set of two-dimensional subspaces of V, which we now

describe. We will use the expression in coordinates $a, b, c \in \mathbb{F}_p$ according to the basis

$$V \ni v = b \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + a \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} + c \cdot \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = (b, a, c).$$

We will also use the self-adjointness of the trace pairing on V.

Lemma 6.3.1 *There are 5 orbits of the adjoint action of B on the set of two-dimensional subspaces of V. A complete list of orbits and their cardinalities, along with at least one representative of the orbit, follows.*

(a) $\langle (1, 0, 0), (0, 1, 0) \rangle$, *the upper-triangular matrices, comprises an orbit of cardinality* 1
(b) $\langle (1, 0, 0), (0, a, 1) \rangle$ *for $a \in \mathbb{F}_p$, the 2-dimensional subspaces that contain $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ but are not contained in the upper-triangular matrices, together comprise an orbit of size p*
(c) $\langle (0, a, 1), (4a, 1, 0) \rangle$ *for $a \in \mathbb{F}_p$, which together comprise an orbit of size p*
(d) $\langle (0, 1, 0), (-1, 0, 1) \rangle$ *is a representative of an orbit of size $p(p-1)/2$*
(e) $\langle (0, 1, 0), (-1, 0, c) \rangle$, *where $c \in \mathbb{F}_p^\times$ is not a square, is a representative of an orbit of size $p(p-1)/2$*

When $p \geq 5$, the orbit (c) is the only orbit of cardinality p that has no representative containing $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$.

Lemma 6.3.1 follows directly from the following lemma characterizing the orbits of the B-action on 1-dimensional subspaces of V, along with the perfect self-duality of V with respect to the trace pairing. We omit the proof deducing Lemma 6.3.1 from the following lemma, but list the orbits there in the same order that their duals were listed in Lemma 6.3.1.

Lemma 6.3.2 *There are 5 orbits of the adjoint action of B on the set of one-dimensional subspaces of V. A complete list of orbits and their cardinalities, along with at least one representative of the orbit, follows.*

(a) $\langle (1, 0, 0) \rangle$, *the strictly upper-triangular matrices, comprise an orbit of cardinality* 1
(b) $\langle (b, 1, 0) \rangle$ *for $b \in \mathbb{F}_p$, the lines that are upper-triangular but not strictly upper-triangular, together comprise an orbit of size p*
(c) $\langle (-a^2, a, 1) \rangle$ *for $a \in \mathbb{F}_p$, which together comprise an orbit of size p*
(d) $\langle (1, 0, 1) \rangle$ *is a representative of an orbit of size $p(p-1)/2$*
(e) $\langle (b, 0, 1) \rangle$, *where $b \in \mathbb{F}_p^\times$ is not a square, is a representative of an orbit of size $p(p-1)/2$*

When $p \geq 5$, the orbit (c) is the only orbit of cardinality p whose members do not consist entirely of upper-triangular matricies.

Proof The orbit listed in (a) is, indeed, an orbit, because conjugation by B preserves the properties "upper-triangular" and "strictly upper-triangular." For this reason, along with the fact that the stabilizer of $\langle (0, 1, 0) \rangle \subset V$ is the diagonal subgroup $\mathbb{F}_p^\times$ of B, we apply the orbit-stabilizer lemma to deduce that there is an orbit as listed in (b).

The diagonal subgroup $\mathbb{F}_p^\times$ of B fixes $\langle (0, 0, 1) \rangle \subset V$, but one easily checks that its normal subgroup $\mathbb{F}_p \subset B$ acts faithfully on the orbit of $\langle (0, 0, 1) \rangle$. By the orbit-stabilizer lemma, we have the orbit (c).

One readily checks that the stabilizer of $\langle (b, 0, 1) \rangle$, for any $b \in \mathbb{F}_p^\times$, is the subgroup $\left(\begin{smallmatrix} \pm 1 & \\ & 1 \end{smallmatrix}\right) \subset B$. In addition, the maximal subgroup of B preserving the set of all lines of the

form $\langle(b, 0, 1)\rangle$, for $b \in \mathbb{F}_p^\times$, is the diagonal subgroup $\mathbb{F}_p^\times \subset B$. Because the representatives listed in (d) and (e) are not in the same orbit under the adjoint action of the diagonal subgroup of B, we deduce from the orbit-stabilizer lemma that they each are representatives of orbits of size $p(p-1)/2$.

Because the total number of lines in V is $p^2 + p + 1$, which equals the sum of the cardinalities of orbits listed in (a)–(e), the list of orbits is complete. □

6.4 The value and vanishing of $\alpha^2 + \beta$ in terms of algebraic number theory

In line with the long tradition of theorems relating congruences between cusp forms and Eisenstein series with an algebraic number-theoretic condition that started with Ribet's converse to Herbrand's theorem, we would like to rephrase the conditions for $\mathbb{T}$ to have minimal rank, proved in the main Theorem 4.5.1, in terms of algebraic number theory. This has precedent, for example, the main theorem of [19] that shows that $\mathbb{T}_{\ell_0}$ has minimal rank if and only if a certain class group has p-torsion of minimal rank.

We have already seen in Proposition 6.2.2 that condition (i) of Theorem 4.5.1 is equivalent to the existence of p-torsion in a ray class group of M'. It remains to interpret condition (ii), the vanishing of $\alpha^2 + \beta$, in terms of algebraic number theory. This is already partially complete in this expression of condition (ii) of Theorem 4.5.1 in terms of prime decomposition in the extensions K'/K and K''/K cut out by $a^{(1)}|_{G_K}$ and $b^{(2)}|_{G_K}$, respectively. Therefore our goal is to "remove $a^{(1)}$ and $b^{(2)}$" from this expression by substituting universal characterizations of K', K'' as completed in Propositions 6.1.2 and 6.2.2. Additionally, we characterize whether or not $\alpha^2 + \beta \in \mu_p^{\otimes 2}$ is a square, where *squares* have the form $\zeta \otimes \zeta$ for some $\zeta \in \mu_p$.

We begin with the following description of the $C_p \times C_p$-extension $K'K''/K$, a corollary of the proof of Proposition 6.2.2.

Corollary 6.4.1 *The composite $K'K'' \subset M''$ is a member of the unique isomorphism class of $C_p \times C_p$-extensions of K contained in M'' that has cardinality p and does not contain M.*

Proof Under the homomorphism ν of (6.2.1), $K'K'' \subset M''$ is the fixed field of the cyclic order p subgroup of $\mathrm{Gal}(M''/\mathbb{Q})$ concentrated in the $c^{(2)}$-coordinate. This subgroup belongs to the conjugacy class listed as item (c) in Lemma 6.3.2. As we see in that lemma, this is the only conjugacy class of cardinality p that has members that are non-trivial in the $c^{(2)}$-coordinate, and therefore does not fix M. □

Theorem 6.4.2 *The following algebraic number theoretic conditions characterize $\alpha^2 + \beta \in \mu_p^{\otimes 2}$.*

(1) $\alpha^2 + \beta$ vanishes if and only if the isomorphism class consisting of decomposition subfields of $M''/\mathbb{Q}$ at primes over ℓ_0 has cardinality p if and only if this isomorphism class equals the isomorphism class of $K'K''$.

(2) $\alpha^2 + \beta \in \mu_p^{\otimes 2}$ is a non-vanishing square if and only if the isomorphism class of decomposition subfields of $M''/\mathbb{Q}$ at the prime ℓ_0 is equal to the fixed fields of the order p subgroups of $\mathrm{Gal}(M''/K)$ given in part (d) of Lemma 6.3.2 under the isomorphism $V \cong \mathrm{Gal}(M''/K)$.

(3) *$\alpha^2+\beta \in \mu_p^{\otimes 2}$ is a non-square if and only if the isomorphism class of decomposition subfields of $M''/\mathbb{Q}$ at the prime ℓ_0 is equal to the fixed fields of the order p subgroups of $\mathrm{Gal}(M''/K)$ given in part (e) of Lemma 6.3.2 under the isomorphism $V \cong \mathrm{Gal}(M''/K)$.*

Proof Characterization (1) of the vanishing of $\alpha^2+\beta$ follows directly from Theorem 4.5.1. Indeed, if there exists a prime of M'' over ℓ_0 such that the prime of K lying below it splits in both K'/K and K''/K, then the decomposition subgroup of this prime fixes $K'K''$. (Recall that ℓ_0 splits completely in $K/\mathbb{Q}$.)

Let $D_{\ell_0} \subset \mathrm{Gal}(M''/\mathbb{Q})$ denote a decomposition subgroup arising from the choice of a prime of M'' over ℓ_0. It has order p. In order to prove characterizations (2) and (3), determining the image of $\alpha^2+\beta \in \mu_p^{\otimes 2} \smallsetminus \{1\otimes 1\}$ in the doubleton set $(\mu_p^{\otimes 2} \smallsetminus \{1\otimes 1\})/\mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q})$, we simply need to review definitions of α, β, and the isomorphism (6.2.7). Putting these together, isomorphism (6.2.7) simplifies when restricted to D_{ℓ_0} according to

$$\begin{pmatrix} a^{(1)} & b^{(2)} \\ c^{(1)} & -a^{(1)} \end{pmatrix}\Big|_{D_{\ell_0}} = \begin{pmatrix} \alpha c^{(1)} & \beta c^{(1)} \\ c^{(1)} & -\alpha c^{(1)} \end{pmatrix}\Big|_{D_{\ell_0}}.$$

The existence of a choice of prime over ℓ_0 such that $a^{(1)}|_{\ell_0} = 0$ and equivalently $\alpha = 0$, discussed in Lemma 4.2.4, implies that we can replace $D_{\ell_0} \subset \mathrm{Gal}(M''/\mathbb{Q})$ by a conjugate subgroup such that

$$\begin{pmatrix} a^{(1)} & b^{(2)} \\ c^{(1)} & -a^{(1)} \end{pmatrix}\Big|_{D_{\ell_0}} = \begin{pmatrix} 0 & (\alpha^2+\beta)c^{(1)} \\ c^{(1)} & 0 \end{pmatrix}\Big|_{D_{\ell_0}}.$$

Therefore, because $c^{(1)}|_{\ell_0} \neq 0$, there is a generator of D_{ℓ_0} whose image in V is $\left(\begin{smallmatrix} 0 & \alpha^2+\beta \\ 1 & 0 \end{smallmatrix}\right)$. Looking at the list of conjugacy classes of order p subgroups of $\mathrm{Gal}(M''/K)$ listed in Lemma 6.3.2, one can read off characterizations (2) and (3). □

6.5 A terminal result of Parts I and II

In this final section, we present the preceding results, especially Corollary 6.2.3 and Theorem 6.4.2(1), in a form that allows us to deduce a "terminal result" of this pair of papers, which is stated below as Theorem 6.5.2.

Let N_{ℓ_0} be the normalizer of a decomposition group $D_{\ell_0} \subset \mathrm{Gal}(M''/\mathbb{Q})$, and let n_{ℓ_0} denote the order of N_{ℓ_0}. This integer n_{ℓ_0} is independent of the choice of D_{ℓ_0}. Here is a complete description of n_{ℓ_0}. Recall that $M''=M'$ if and only if $a^{(1)}|_{\ell_1}=0$.

Proposition 6.5.1 *If $M''=M'$, then $n_{\ell_0}=p^2(p-1)$. If M''/M' has degree p, then n_{ℓ_0} is described by the following two cases.*

- *$n_{\ell_0}=2p^3$ if and only if the conjugacy class of the subgroup $D_{\ell_0} \subset \mathrm{Gal}(M''/\mathbb{Q})$ has order $p(p-1)/2$.*
- *$n_{\ell_0}=p^3(p-1)$ if and only if the conjugacy class of the subgroup $D_{\ell_0} \subset \mathrm{Gal}(M''/\mathbb{Q})$ has order p.*

Proof First we claim that D_{ℓ_0} has order p and is contained in $\mathrm{Gal}(M''/K)$. The claim about the order follows from the facts that

- ℓ_0 splits completely in $K/\mathbb{Q}$ (see [Part I, Lem. 3.2.1])

- the primes over ℓ_0 are ramified in $M/K = KL/K$ because the same is true for $L/\mathbb{Q}(\zeta_p)$ (see the description of $L/\mathbb{Q}(\zeta_p)$ in Sect. 1.2)
- the primes over ℓ_0 are split in M'/M and M''/M' according to Propositions 6.1.2 and 6.2.2.

According to the claim, in the case $[M'' : M'] = p$, $D_{\ell_0} \subset \mathrm{Gal}(M''/K)$ is a line in a 3-dimensional $\mathbb{F}_p$-vector space. Moreover, its conjugacy class in $\mathrm{Gal}(M''/\mathbb{Q})$ is described by Lemma 6.3.2 under the isomorphism (6.2.7) from $\mathrm{Gal}(M''/K)$ to V. Because $[M'' : \mathbb{Q}] = p^4(p-1)$ and the normalizer N_{ℓ_0} is the stablizer of the conjugacy action of $\mathrm{Gal}(M''/\mathbb{Q})$ on D_{ℓ_0}, the proposition's claims in the case $[M'' : M'] = p$ follow from the orbit-stabilizer lemma.

In the case $M'' = M'$, we use the representation $\upsilon : \mathrm{Gal}(M'/\mathbb{Q}) \to \mathrm{GL}_3(\mathbb{F}_p)$ of (6.1.1) to draw an isomorphism

$$(a^{(1)}, c^{(1)})|_{G_K} : \mathrm{Gal}(M'/K) \to \mathbb{F}_p \oplus \mathbb{F}_p.$$

The claim implies that each choice of decomposition group $D_{\ell_0} \subset \mathrm{Gal}(M'/K)$ is a line. Because of the form of υ, a much simpler analysis than Lemma 6.3.2 yields that the conjugacy classes of order p subgroups of $\mathrm{Gal}(M'/\mathbb{Q})$ contained in $\mathrm{Gal}(M'/K)$ are described as follows in terms of υ.

- The subgroup concentrated in the $a^{(1)}$-coordinate comprises a singleton orbit.
- The subgroups containing elements with non-zero $c^{(1)}$-coordinate comprise an orbit of order p.

Because $c^{(1)}|_{\ell_0} \neq 0$, the conjugacy class containing $D_{\ell_0} \subset \mathrm{Gal}(M'/\mathbb{Q})$ has cardinality p. Therefore, the proposition's claim in the case $M'' = M'$ follows from the fact that $[M' : \mathbb{Q}] = p^3(p-1)$ and an applicaiton of the orbit-stabilizer lemma. □

Theorem 6.5.2 *If $n_{\ell_0} = p^2(p-1)$ or $n_{\ell_0} = 2p^3$, then the $\mathbb{Z}_p$-rank of R is 3, there is a unique newform of level N congruent to the Eisenstein series, and $R \cong \mathbb{T}$. If $n_{\ell_0} = p^3(p-1)$, then $\dim_{\mathbb{F}_p} R/pR > 3$.*

Proof The conclusions of this theorem are the same as those of Theorem 4.5.1, so we only need to check that the condition "$n_{\ell_0} = p^3(p-1)$" is equivalent to the condition that "both conditions (i) and (ii) of Theorem 4.5.1 are true." Indeed, Proposition 6.5.1 also tells us that $n_{\ell_0} = p^2(p-1)$ or $n_{\ell_0} = 2p^3$ when $n_{\ell_0} \neq p^3(p-1)$.

Corollary 6.2.3 draws an equivalence between condition (i) and the condition that $[M'' : M'] = p$. Given that (i) is true, Theorem 6.4.2(1) draws an equivalence between condition (ii) and the condition that the conjugacy class of subgroups of $\mathrm{Gal}(M''/\mathbb{Q})$ containing (any choice of) D_{ℓ_0} has cardinality p. By Proposition 6.5.1, we conclude that condition (ii) is equivalent to $n_{\ell_0} = p^3(p-1)$ upon the assumption that (i) is true. And (i) is also necessarily true when $n_{\ell_0} = p^3(p-1)$, according to Proposition 6.5.1. □

Supplementary Information

The online version contains supplementary material available at https://doi.org/10.1007/s40993-022-00401-1.

Acknowledgements

The first-named author thanks the University of Bristol and the Heilbronn Institute for Mathematical Research for its partial support of this project. The second-named author was supported in part by NSF grant DMS-1901867, and would like to thank his coauthors on the paper [7]; that paper inspired many of the ideas used here about how to compute

Massey products. The third-named author was supported in part by Simons Foundation award 846912, and thanks the Department of Mathematics of Imperial College London for its partial support of this project from its Mathematics Platform Grant. We also thank John Cremona for several insightful conversations about computational aspects of this project as well as the referee for their helpful comments and suggestions. This research was supported in part by the University of Pittsburgh Center for Research Computing and Swarthmore College through the computing resources provided.

Data availability All data generated or analysed during this study are included in this published article (and its supplementary information files).

Author details
[1]Department of Mathematics & Statistics, Swarthmore College, Swarthmore, PA 19081, USA, [2]Department of Mathematics, Michigan State University, East Lansing, MI 48824, USA, [3]Department of Mathematics, University of Pittsburgh, Pittsburgh, PA 15260, USA.

Received: 8 September 2022 Accepted: 5 October 2022 Published online: 26 January 2023

References

1. Calegari, F., Emerton, M.: On the ramification of Hecke algebras at Eisenstein primes. Invent. Math. **160**(1), 97–144 (2005)
2. Fontaine, J.-M.: Il n'y a pas de variété abélienne sur Z. Invent. Math. **81**(3), 515–538 (1985)
3. Hsu, C., Wake, P., Wang-Erickson, C.: Explicit non-Gorenstein $R = \mathbb{T}$ via rank bounds I: Deformation theory (2022). Preprint, arXiv: 2209.00536 [math.NT]
4. Kraines, D.: Massey higher products. Trans. Am. Math. Soc. **124**, 431–449 (1966)
5. Lecouturier, E.: On the Galois structure of the class group of certain Kummer extensions. J. Lond. Math. Soc. (2) **98**(1), 35–58 (2018)
6. Lemmermeyer, F.: Reciprocity laws. Springer Monographs in Mathematics. From Euler to Eisenstein. Springer, Berlin (2000)
7. Lam, Y.H.J., Liu, Y., Sharifi, R., Wake, P., Wang, J.: Generalized Bockstein maps and Massey products (2021). arXiv:2004.11510v2 [math.NT]
8. May, J.P.: Matric Massey products. J. Algebra **12**, 533–568 (1969)
9. Merel, L.: L'accouplement de Weil entre le sous-groupe de Shimura et le sous-groupe cuspidal de $J_0(p)$. J. Reine Angew. Math. **477**, 71–115 (1996)
10. Neukirch, J.: Algebraic Number Theory, volume 322 of Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer, Berlin: Translated from the 1992 German original and with a note by Norbert Schappacher. With a foreword by G, Harder (1999)
11. Stein, W.A., et al.: SageMath, the Sage Mathematics Software System (accessed online through CoCalc). The Sage Development Team (2018). http://www.sagemath.org, https://cocalc.com
12. Serre, J.-P.: Local Fields, vol. 67 of Graduate Texts in Mathematics. Springer, New York. Translated from the French by Marvin Jay Greenberg (1979)
13. Serre, J.-P.: Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Duke Math. J. **54**(1), 179–230 (1987)
14. Sharifi, R.T.: Twisted Heisenberg representations and local conductors. ProQuest LLC, Ann Arbor, MI. Thesis (Ph.D.), The University of Chicago (1999)
15. Sharifi, R.T.: Massey products and ideal class groups. J. Reine Angew. Math. **603**, 1–33 (2007)
16. Tahara, K.: On the second cohomology groups of semidirect products. Math. Z. **129**, 365–379 (1972)
17. The PARI Group, Univ. Bordeaux. PARI/GP version `2.13.4` (2022). http://pari.math.u-bordeaux.fr/
18. Wake, P.: The Eisenstein ideal for weight k and a Bloch-Kato conjecture for tame families. J. Eur. Math. Soc. (2022). https://doi.org/10.4171/JEMS/1251
19. Wake, P., Wang-Erickson, C.: The rank of Mazur's Eisenstein ideal. Duke Math. J. **169**(1), 31–115 (2020)

Publisher's Note