EXPLICIT NON-GORENSTEIN $R = \mathbb{T}$ VIA RANK BOUNDS I: DEFORMATION THEORY

CATHERINE HSU, PRESTON WAKE, AND CARL WANG-ERICKSON

Abstract. Ribet has proven remarkable results about non-optimal levels of residually reducible Galois representations. We focus on a non-optimal level N that is the product of two distinct primes and where the Galois deformation ring is not expected to be Gorenstein. We prove a Galois-theoretic criterion for the deformation ring to be as small as possible – that is, for there to be a *unique* newform of level N with reducible residual representation. When this criterion is satisfied, we deduce an $R = \mathbb{T}$ theorem.

Contents

1. Introduction

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

- ℓ_0 is a prime number with $\ell_0 \equiv 1 \pmod{p}$, and
- ℓ_1 is a prime number with $\ell_1 \not\equiv 0, \pm 1 \pmod{p}$, such that ℓ_1 is a pth power modulo ℓ_0.

Under these conditions, a theorem of Ribet [Rib10, Rib15, Yoo19] implies that there are newforms of level N with reducible residual Galois representation $\bar{\rho}$. Moreover, these levels exhibit two behaviors that are of particular interest:

- at such levels N, the algebra $\mathbb{T}$ is expected not to be Gorenstein (and this is borne out computationally),

Date: September 1, 2022.

- the condition on ℓ_1 is very different from the level-raising conditions for residually irreducible representations.

We study $\bar{\rho}$ at such levels N as a prototype for understanding these behaviors in more general residually reducible contexts.

The method we use to prove $R = \mathbb{T}$ is novel. In the paper [WWE21], similar $R = \mathbb{T}$ results for the representation $\bar{\rho}$ and certain squarefree levels are proven. However, in [WWE21], the theorems include conditions that force the rings R and $\mathbb{T}$ to be local complete intersections. Correspondingly, the proofs of $R = \mathbb{T}$ use Wiles's numerical criterion [Wil95, Appendix]. In this paper, the ring $\mathbb{T}$ is not local complete intersection, so a new technique is required. Our method consists of first showing that there is a surjection $R \twoheadrightarrow \mathbb{T}$ and then showing that the rank of R is no greater than the rank of $\mathbb{T}$.

In this, the first paper, we bound the rank of R in terms of cup products and Massey products in Galois cohomology, using similar techniques as in [WWE20]. In particular, we show that the rank of R is at most 3 if and only if a certain numerical invariant is non-zero. In the second paper [HWWE22], we describe this numerical invariant in terms of algebraic number theory and use this to develop an algorithm for computing when it vanishes. We explain how to code this algorithm into SAGE [S$^+$18], and compile data from computer experiments showing that the rank of R is exactly 3 whenever the rank of $\mathbb{T}$ is.

1.2. **Terminal result of the series of two papers.** The terminal result of this series of papers is the following. The main theorem of this paper (Theorem 1.4.3) and of Part II are no less important, but we highlight this result as terminal because it relies on both main theorems. It is distinguished by providing a criteria implying that $\mathbb{T}$ has minimal rank that is expressed in terms of algebraic number theory, much like the main theorem of [WWE20].

We need a few definitions to express some class fields.

- Let $K = \mathbb{Q}(\zeta_p, \ell_1^{1/p})$.
- Let $L/\mathbb{Q}(\zeta_p)$ be the ω^{-1}-isotypic degree p Galois 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., [CE05, Lem. 3.9].)
- Let $M = KL$, the composite field.
- Let M'/M be the unique unramified degree p Galois extension such that
  - $M'/\mathbb{Q}$ is Galois and the natural $\mathrm{Gal}(M/\mathbb{Q})$-action on $\mathrm{Gal}(M'/M)$ is trivial
  - all primes over ℓ_0 split completely in M'/M.
- $\mathfrak{m}^{\mathrm{flat}}$ be the modulus (in the sense of ray class field theory) of M' that is the product of the squares of all primes over p.
- Let M''/M' be the maximal abelian extension of exponent p such that
  - the conductor of M''/M' divides $\mathfrak{m}^{\mathrm{flat}}$,
  - $M''/\mathbb{Q}$ is Galois and the natural action of $\mathrm{Gal}(M'/\mathbb{Q})$ on $\mathrm{Gal}(M''/M')$ is isotypic for the modulo p cyclotomic character $\omega : \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \xrightarrow{\sim} \mathbb{F}_p^\times$ under the composition
$$\mathrm{Gal}(M'/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \xrightarrow{\omega} \mathbb{F}_p^\times.$$
  - all primes over ℓ_0 split in M''/M'.

  This extension M''/M' has degree either 1 or p. The decomposition subgroup of $\mathrm{Gal}(M''/\mathbb{Q})$ for any prime over ℓ_0 has order p.

- We let n_{ℓ_0} be the order of the normalizer of a decomposition subgroup of $\mathrm{Gal}(M''/\mathbb{Q})$ associated to a (or any) prime over ℓ_0. If the degree of M''/M' is p, then $n_{\ell_0} = p^3(p-1)$ or $n_{\ell_0} = 2p^3$. If $M'' = M'$, then $n_{\ell_0} = p^2(p-1)$.

The claimed existence and properties of M' and M'' are guaranteed in [Part II, §6].

Theorem 1.2.1. *Adopt Assumption 1.3.2. 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 $\dim_{\mathbb{F}_p} R/pR > 3$.*

If $n_{\ell_0} = p^3(p-1)$, we do not know how to prove $R = \mathbb{T}$ and we cannot conclude that $\mathrm{rk}_{\mathbb{Z}_p}\mathbb{T} > 3$. However, we have computed examples where $n_{\ell_0} = p^3(p-1)$, and in all such examples we have $\mathrm{rk}_{\mathbb{Z}_p}\mathbb{T} > 3$, which is consistent with the expectation that $R = \mathbb{T}$.

Theorem 1.2.1 follows from combining the main result of this paper (Theorem 1.4.3) with the translation of the main theorem's conditions into algebraic number theory that is accomplished in [Part II, §6]; in particular, the proof of Theorem 1.2.1 appears in [Part II, §6.5].

1.3. **Residually reducible modularity and level raising.** Let $\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_q)$ be a representation with values in a finite field. There are three questions we can ask about the modularity of this representation:

(1) Is $\bar{\rho}$ *modular*? That is, is there an eigenform f such that $\bar{\rho}$ is isomorphic to the residual representation of f?
(2) If $\bar{\rho}$ is modular, what are its possible *levels*? That is, for which integer N is there a *newform* f of level N such that $\bar{\rho}$ is isomorphic to the residual representation of f?
(3) If $\bar{\rho}$ is modular of a given level N, does it satisfy modularity lifting? That is, if $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O})$ is a lift of $\bar{\rho}$ satisfying some conditions, is ρ isomorphic to the Galois representation of a *newform* of level N?

When $\bar{\rho}$ is absolutely irreducible, the answers to these questions are well understood. Question (1) is the subject of Serre's conjecture [Ser87], proven by Khare–Wintenberger [KW09], question (2) is subject of level-raising and level-lowering results of Ribet [Rib84, Rib90] and others, and question (3) is the subject of Wiles's modularity theorem and the Taylor–Wiles method. Regarding (2), let us just recall that there is an *optimal level* $N_{\bar{\rho}}$ that is an absolute minimum, and, for a prime ℓ, $\bar{\rho}$ is modular of level $N_{\bar{\rho}}\ell$ if and only if ℓ satisfies a level-raising condition depending only of ℓ and $\bar{\rho}$.

When $\bar{\rho}$ is reducible, though, the situation is far less clear. Even the questions must be interpreted carefully. If $\bar{\rho}$ is reducible, then for any eigenform f with residual representation $\bar{\rho}$ there will be multiple Galois-stable integral lattices in the Galois representation of f; there is no canonical choice of lattice. Moreover, different lattices may have non-isomorphic residual representations. We avoid making these non-canonical choices by working with pseudorepresentations – which essentially keep track of the characteristic polynomial and do not depend on the choice of lattice – rather than representations.

1.3.1. *Results of Mazur and Ribet.* In this paper, we focus on the most basic case, where $\bar{\rho}$ is the 2-dimensional pseudorepresentation induced by $\omega \oplus 1$, where $\omega : G_{\mathbb{Q}} \to \mathbb{F}_p^{\times}$ is the mod-p cyclotomic character. We also only study modular forms of weight 2 and level $\Gamma_0(M)$ for squarefree M. This case is the subject Mazur's landmark paper on the Eisenstein ideal [Maz77] when M is prime. In this case, Mazur shows that for any prime ℓ, $\bar{\rho}$ is modular of level ℓ if and only if $\ell \equiv 1 \pmod{p}$. In particular, since $\bar{\rho}$ is not modular of level 1, there is no "optimal level" for $\bar{\rho}$ that is an absolute minimum.

Ribet [Rib10] (see also [Yoo19]) initiated the study of level raising in this situation. He observed that, here too, the results are qualitatively very different from the residually irreducible case, as witnessed by the following result (which is a special case of what Ribet proved).

Theorem 1.3.1 (Ribet)**.** *If ℓ_0 is a prime such that $\ell_0 \equiv 1 \pmod{p}$ and $\ell_1 \not\equiv \pm 1$ is another prime, then $\bar{\rho}$ is modular of level $\ell_0\ell_1$ if and only of ℓ_1 is a pth power modulo ℓ_0.*

The key thing to note about this result is that, unlike in the residually irreducible case [Rib84], the level-raising condition on the prime ℓ_1 depends not just on ℓ_1 and $\bar{\rho}$, but also on ℓ_0.

1.3.2. *Interpretation in terms of congruences with Eisenstein series and Hecke algebras.* The trace of $\bar{\rho}(\mathrm{Fr}_\ell)$, where Fr_ℓ is an arithmetic Frobenius element $\mathrm{Fr}_\ell \in G_{\mathbb{Q}}$ at a prime $\ell \neq p$, equals $\ell + 1 \in \mathbb{F}_p$, which is the reduction modulo p of the eigenvalue $\ell + 1$ of the ℓth Hecke operator T_ℓ on the Eisenstein series of weight 2 and level 1. (Although this form is non-holomorphic, it has a holomorphic stabilization to any level N with $N > 1$.) We can say informally that $\bar{\rho}$ *is modular of level* N if there is a cusp form of level N that is congruent to that Eisenstein series. However, if N is not prime, then all Eisenstein series are oldforms. Therefore, in order to set up a bijection between eigenforms and pseudorepresentations, we need to specify the eigenvalues of Hecke operators at primes dividing N, thereby selecting a single Eisenstein series.

Assumption 1.3.2. Now, and for the rest of the paper, we specialize to level $N = \ell_0\ell_1$, where, as in Ribet's Theorem 1.3.1, 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. there is a unique cusp form f of level ℓ_0 that is congruent to the Eisenstein series modulo p (existence is implied by condition (1), by Mazur's theorem [Maz77])

In this case, there is a 3-dimensional space of Eisenstein series, all having T_ℓ-eigenvalue $\ell + 1$ for $\ell \nmid N$. As in the paper [WWE21], we choose a basis of eigenforms for the Atkin–Lehner involutions w_{ℓ_0} and w_{ℓ_1}. The possible pairs of eigenvalues of the Eisenstein series under the Atkin–Lehner operators (w_{ℓ_0}, w_{ℓ_1}) are $(-1,-1), (-1,1), (1,-1)$. However, it is known that a level $\Gamma_0(N)$ newform f that is congruent to any Eisenstein series must have (w_{ℓ_0}, w_{ℓ_1})-eigenvalues $(-1,-1)$; therefore we select that particular Eisenstein series, calling it $E_{2,N}$.

Let $\mathbb{T}'$ be the $\mathbb{Z}_p$-algebra spanned by the operators T_ℓ for $\ell \nmid N$ acting on modular forms of weight 2 and level N with coefficients in $\mathbb{Z}_p$ and Atkin–Lehner eigenvalues $(-1,-1)$. Let $\mathbb{T}$ be the completion of $\mathbb{T}'$ at the maximal ideal generated by $T_\ell - (\ell + 1)$ and p, and let $\mathbb{T}^0$ be the largest quotient that acts faithfully on cusp forms. By Ribet's Theorem 1.3.1, the $\mathbb{Z}_p$-rank of $\mathbb{T}$ is at least 3, accounting for the contributions of the eigensystems of

- the Eisenstein series $E_{2,N}$, valued in $\mathbb{Z}_p$
- the unique stabilization to level N of the $\mathbb{Z}_p$-valued form f of level ℓ_0 specified in (4), above, with the specified (w_{ℓ_0}, w_{ℓ_1})-eigenvalues
- the newform of level N arising from Ribet's theorem, which has $\mathbb{Z}_p$-rank ≥ 1.

Remark 1.3.3. Since condition (4) above might seem somewhat abstract, we want to emphasize that the number of cusp forms of level ℓ_0 with an Eisenstein congruence is well understood [Mer96, CE05, Lec21, WWE20]. In particular, by Merel's Theorem [Mer96, Théorème 2], the assumption (4) is equivalent to the following numerical condition:

$$(\ell_0 \text{ Rank } 1) \qquad \prod_{i=1}^{\frac{\ell_0-1}{2}} i^i \text{ is not a } p\text{th power modulo } \ell_0.$$

This will simplify our study of the number of new cusp forms: it is $\mathrm{rk}_{\mathbb{Z}_p}\mathbb{T} - 2$.

1.3.3. *Residually reducible modularity lifting and imposing conditions at N.* By Ribet's Theorem 1.3.1, we know that $\bar{\rho}$ is modular of level N, so we can ask about modularity lifting. Let R^{univ} denote the universal pseudodeformation ring of $\bar{\rho}$ ramified only at Np. Considering the Galois representations associated to modular forms, it is not too difficult to show that there is a surjective homomorphism $R^{\mathrm{univ}} \twoheadrightarrow \mathbb{T}$ (see [WWE21, §4.1]).

To formulate a modularity lifting theorem, we must then define a *level N quotient* R_N of R^{univ} that parameterizes pseudodeformations that "look modular of level N." We also write R for R_N because the level N is fixed throughout the paper. The putative theorem is that the induced map

$$R \twoheadrightarrow \mathbb{T}$$

is an isomorphism.

For a deformation ρ to "look modular of level N," we want it to satisfy the following conditions. Such ρ are exactly those parameterized by R.

(1) $\det(\rho) = \kappa_{\mathrm{cyc}}$, the p-adic cyclotomic character (weight 2)
(2) ρ is finite-flat at p (geometricity)
(3) ρ is unramified or Steinberg at ℓ_0 and ℓ_1 (level $\Gamma_0(N)$)

Condition (1) is easy to formulate for pseudorepresentations, but (2) and (3) are more involved. For condition (2), which is cohomological in nature, a robust theory was developed in [WWE19]. Condition (3) is even more complex. Roughly, this is for two reasons: because the Steinberg representation is reducible but indecomposible, and because it involves p-integrally interpolating between two conditions, unramified and Steinberg, that do not overlap in characteristic 0.

A candidate definition of (3) was made in [WWE21] and called *unramified-or-Steinberg*[1]. As an initial reasonableness check, it is shown there that $R_M \twoheadrightarrow \mathbb{T}_M$; that is, Galois representations arising from modular forms of level M are unramified or Steinberg at the primes dividing M. Also, it was established that, in many cases at many squarefree levels M, this is the right definition, in that $R_M \cong \mathbb{T}_M$. However, in all the cases of $R_M \cong \mathbb{T}_M$ established by the theorems of [WWE21], the

[1] In [WWE21], the condition is called unramified-or-(-1)-Steinberg, where the sign indicates a choice of unramified-twist of Steinberg at each prime dividing the level. In this paper, we always consider the trivial twist, which corresponds to sign -1 at the primes ℓ_0 and ℓ_1, so we drop the ϵ from the notation.

rings R_M and $\mathbb{T}_M$ are local complete intersection. One of the motivations for this paper is to provide evidence that the definition of unramified-or-Steinberg given in [WWE21] is the right one, even in more pathological cases.

1.4. **Main results: bounding the rank of R.** Our main result shows that $R_N \cong \mathbb{T}$ under certain, numerically verifiable conditions, thereby supplying evidence that $R \cong \mathbb{T}$ in general.

Since $\mathbb{T}$ is not a local complete intersection ring in general (in fact, we expect it never is, outside the cases discussed in [WWE21]), we cannot use Wiles's numerical criterion [Wil95] to prove that $R \twoheadrightarrow \mathbb{T}$ is an isomorphism. Instead, we use a new strategy: we prove that

$$\dim_{\mathbb{F}_p} R/pR \leq \operatorname{rank}_{\mathbb{Z}_p} \mathbb{T}.$$

Because R is p-adically separated, a separated version of Nakayama's lemma then implies that $R \twoheadrightarrow \mathbb{T}$ is an isomorphism. As discussed above, we have made assumptions that ensure that $\operatorname{rk}_{\mathbb{Z}_p} \mathbb{T} \geq 3$. Hence our goal is to find conditions under which $\dim_{\mathbb{F}_p} R/pR \leq 3$, for this will imply that $R_N \cong \mathbb{T}$.

1.4.1. *Conditions for* $\dim_{\mathbb{F}_p} R/pR \leq 3$. The papers [CE05, WWE20] also bound the dimension of a (pseudo)deformation ring in terms of number-theoretic data. However, the situation there is greatly simplified by the fact that the tangent space of the deformation ring is one-dimensional, so computing the dimension amounts to determining the degree to which the tangent vector deforms.

To bound the dimension of R/pR, we follow the same basic strategy of [CE05, WWE20], but we have to deal with the fact that the tangent space of R/pR is two-dimensional. Roughly speaking, we find a basis of the tangent space consisting of an "old reducible vector" (coming from level ℓ_0) and a "new irreducible vector." We show, using the assumption (ℓ_0 Rank 1), that the dimension of R/pR is greater than 3 if and only if the new vector deforms to second order.

To determine when the new vector deforms to second order, we start by explicitly describing it: as a pseudorepresentation with values in $\mathbb{F}_p[\epsilon]/(\epsilon^2)$, it is given by

$$D_1 = \omega + 1 + \epsilon(b^{(1)}c^{(1)} + (\omega - 1)a^{(1)}),$$

where

- $b^{(1)} \in Z^1(G_{\mathbb{Q},Np}, \mathbb{F}_p(1))$ is the Kummer cocycle associated to ℓ_1
- the cocycle $c^{(1)} \in Z^1(G_{\mathbb{Q},Np}, \mathbb{F}_p(-1))$ is ramified only at ℓ_0
- the cochain $a^{(1)} : G_{\mathbb{Q},Np} \to \mathbb{F}_p$ satisfies $-da^{(1)} = b^{(1)} \smile c^{(1)}$.

To make sense of this (and to explain the notation), we think of D_1 as the trace of a *generalized matrix algebra* representation

$$\rho_1 = \begin{pmatrix} \omega(1 + a^{(1)}\epsilon) & b^{(1)} \\ \omega c^{(1)} & 1 + d^{(1)}\epsilon \end{pmatrix} \tag{1.4.1}$$

where $d^{(1)} = b^{(1)}c^{(1)} - a^{(1)}$, and where the generalized matrix multiplication is given by usual matrix multiplication but where the product of the off-diagonal co-ordinates is multiplied by ϵ (see §4.1 below for a formal discussion of these generalized matrix algebras). To determine if ρ_1 deforms to second order, we write down a putative deformation

$$\rho_2 = \begin{pmatrix} \omega(1 + a^{(1)}\epsilon + a^{(2)}\epsilon^2) & b^{(1)} + b^{(2)}\epsilon \\ \omega(c^{(1)} + c^{(2)}\epsilon) & 1 + d^{(1)}\epsilon + d^{(2)}\epsilon^2 \end{pmatrix} \tag{1.4.2}$$

with $\epsilon^3 = 0$ and write down the conditions the new cochains $a^{(2)}, b^{(2)}, c^{(2)}, d^{(2)}$ must satisfy for ρ_2 to define a map $R \to \mathbb{F}_p[\epsilon]/(\epsilon^3)$. We find that, in order for ρ_2 to exist as a generalized matrix algebra representation, we must have

- $a^{(1)}|_{\ell_1} = 0$

and that if any deformation ρ_2 exists, it can be arranged to satisfy

- $a^{(1)}|_{\ell_0} = \alpha c^{(1)}|_{\ell_0}$ for some $\alpha \in \mathbb{F}_p$,
- $b^{(2)}|_{\ell_0} = \beta c^{(1)}|_{\ell_0}$ for some $\beta \in \mathbb{F}_p$,

where "$(-)|_\ell$" indicates restriction to the decomposition group at ℓ. In addition, for ρ_2 to be unramified-or-Steinberg at ℓ_0, we must also have

- $\alpha^2 + \beta = 0$.

Although this construction depends on many choices, we show that the conditions $a^{(1)}|_{\ell_1} = 0$ and $\alpha^2 + \beta$ are independent of the choices. Actually, in §8, we show more: that $\alpha^2 + \beta$ arises from a canonical element of the 1-dimensional $\mathbb{F}_p$-vector space $\mu_p \otimes \mu_p$, where $\mu_p \subset \overline{\mathbb{Q}}^\times$ are the pth roots of unity.

1.4.2. *Main results.* This paper's main theorem relies on showing that there exists ρ_2 as in (1.4.2) if and only if the square of the maximal ideal of R/pR is non-zero. Since the maximal ideal can be generated by two elements, if it is square-zero, then we have $R/pR \simeq \mathbb{F}_p[x,y]/(x^2, xy, y^2)$, with $\mathbb{F}_p$-dimension 3.

Theorem 1.4.3 (Theorem 7.3.3)**.** *Let $p \geq 5$. The $\mathbb{F}_p$-dimension of R/pR is greater than 3 if and only if*

(i) $a^{(1)}|_{\ell_1} = 0$ *and*
(ii) $\alpha^2 + \beta = 0$,

where $a^{(1)}$ and $\alpha^2+\beta$ are as defined in Section 1.4.1. Moreover, if $\dim_{\mathbb{F}_p} R/pR = 3$, then R is a free $\mathbb{Z}_p$-module of rank 3 and the natural map

$$R \twoheadrightarrow \mathbb{T}$$

is an isomorphism.

The conditions (i) and (ii) may at first appear to be unusual enough that this theorem is of no use whatsoever. However, in the sequel to this paper [HWWE22], we translate the conditions (i) and (ii) into explicit statements about splitting behaviors of primes in certain nilpotent extensions of $\mathbb{Q}$. Moreover, we develop algorithms to effectively compute (i) and (ii) using algebraic number theory. We have executed these algorithms for small values of p, establishing the following

Theorem 1.4.4. *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 1.4.3 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 1.4.3 both hold. Consequently, the $\mathbb{F}_p$-dimension of R/pR exceeds 3 for these values of ℓ_1.

Remark 1.4.5. 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 the expectation that $R \cong \mathbb{T}$.

To summarize Theorem 1.4.4, in all of the examples we computed, we find that one of the following cases occurs, witnessing the main Theorem 1.4.3.

- We compute in number field extensions and determine that both (i) and (ii) of Theorem 1.4.3 are true. In addition, we *independently* compute with modular symbols and determine that $\mathrm{rank}_{\mathbb{Z}_p}(\mathbb{T}) \geq 4$.
- We compute in number field extensions and determine that, of the conditions of Theorem 1.4.3, (i) is true but (ii) is false. In addition, we *independently* compute that $\mathrm{rk}_{\mathbb{Z}_p} \mathbb{T} = 3$. Theorem 1.4.3 tells us that $R \cong \mathbb{T}$ in this case.

Both of these cases are consistent with the hypothesis that $R \cong \mathbb{T}$ always – even when $\dim_{\mathbb{F}_p} R/pR > 3$. This leads us to a broader

Conjecture 1.4.6. *For any prime p and squarefree level M as in Section 1.3.3, we have $R_M \cong \mathbb{T}_M$.*

In other words, we conjecture that the unramified-or-Steinberg condition developed in [WWE21, §3] fully captures the "modular of level M" condition on Galois pseudorepresentations. More precisely, the conjecture decomposes into "$R^\varepsilon_M = \mathbb{T}^\varepsilon_M$" as ε varies over sets of Atkin–Lehner eigenvalues, as in [WWE21, §1.9.1].

1.5. **Organization of the paper.** In order to organize non-canonical choices in one place, the notion of *pinning data* is set up in Definition 1.7.1. Section 2 consists of recollections from the antecedent paper [WWE21] regarding the fundamental concepts described in the introduction above. All notation and definitions are present in this section in order to make it reasonably self-contained, while details and proofs are left to *loc. cit.*. Section 3 continues with lemmas and definitions in arithmetic and Galois representations that extends the content of Section 2, going beyond what appears in *loc. cit.*. Section 4 sets up the first-order deformation ρ_1 of (1.4.1) above. Section 5 produces an explicit understanding of R up to second order, and Section 6 applies this in order to prove the "only if" direction of the main Theorem 1.4.3. Section 7 proves the other logical direction by constructing by hand a level N deformation ρ_2 of ρ_1 as in (1.4.2). Section 8 proves that the invariant $\alpha^2 + \beta$ is canonical by showing that the pinning data does not affect it.

1.6. **Acknowledgements.** The first-named author would like to thank 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. The third-named author was supported in part by Simons Foundation award 846912, and would like to thank 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 helpful conversations about the computational aspects of this project. This research was supported in part by the University of Pittsburgh Center for Research Computing and Swarthmore College through the computing resources provided.

1.7. **Notation and conventions.** For a group G, write $C^\bullet(G,-)$ for the complex of continuous, inhomogeneous G-cochains, and $H^i(G,-)$, $Z^i(G,-)$ and $B^i(G,-)$ for its cohomology, cocycles and coboundaries. Let $\mathrm{R}\Gamma(G,-)$ denote the class of $C^\bullet(G,-)$ in the derived category. Let $x \mapsto [x]$ denote the quotient map $Z^i(G,-) \to H^i(G,-)$. Let $\smile$ denote the cup product on $C^\bullet(G,-)$ and $\cup$ for the induced map on $H^*(G,-)$.

When $R = \mathbb{Z}[1/Np]$ or $R = \mathbb{Q}_q$ for a prime q, we use $C^\bullet(R,-)$ as an abbreviation for $C^\bullet(G,-)$ where G is the étale fundamental group of $\mathrm{Spec}(R)$, and similarly for $H^i(R,-)$, $Z^i(R,-)$, $B^i(R,-)$, and $\mathrm{R}\Gamma(G,-)$.

We fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. We work with the maximal subextension $\overline{\mathbb{Q}} \supset \mathbb{Q}_S \supset \mathbb{Q}$ that is ramified only at the places dividing $S = Np\infty$, and let $G_{\mathbb{Q},Np} := \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$.

For each prime number q, let $\overline{\mathbb{Q}}_q/\mathbb{Q}_q$ be an algebraic closure and let $G_q := \mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)$. Let $I_q \subset G_q$ be the inertia group and let I_q^{tame} be the tame quotient.

Let $\mu_p \subset \overline{\mathbb{Q}}^\times$ denote the subgroup of pth roots of unity, and let $\omega : G_{\mathbb{Q},Np} \to \mathbb{F}_p^\times$ denote the mod-p cyclotomic character. For $n \in \mathbb{Z}$, let $\mathbb{F}_p(n)$ denote the $\mathbb{F}_p[G_{\mathbb{Q},Np}]$-module $\mathbb{F}_p$ with $G_{\mathbb{Q},Np}$ acting by ω^n.

Several of our constructions will depend in subtle ways on additional choices we call *pinning data*. In the end (§8), we will show that the invariant $\alpha^2 + \beta$ of Theorem 1.4.3 is independent of the pinning data.

Definition 1.7.1. The following choices constitute *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 3.2.2 for a discussion of when this is possible.)

Notice that the choice of pinning data naturally induce the following further choices of

- for each prime q dividing Np, a decomposition subgroup of q in $G_{\mathbb{Q},Np}$ and an isomorphism between this subgroup and G_q, and
- for each $n \in \mathbb{Z}$, isomorphisms $\mathbb{F}_p(n) \xrightarrow{\sim} \mu_p^{\otimes n}$.

We use these data to identify $\mathbb{F}_p(n)$ with $\mu_p^{\otimes n}$ and, for each prime q dividing Np, G_q as a subgroup of $G_{\mathbb{Q},Np}$ and we let

$$C^i(\mathbb{Z}[1/Np], -) \xrightarrow{|_q} C^i(\mathbb{Q}_q, -), \quad f \mapsto f|_q$$

denote the restriction map. We use the same notation $|_q$ for the induced map on cohomology, cocycles, and coboundaries.

2. Recollection of pseudodeformation theory

Throughout this manuscript, we retain the conventions and terminology of the preceding work [WWE21] of the second-named and third-named authors. In this section, we summarize these items for the convenience of the reader, specializing them to the particular level $N = \ell_0\ell_1$ and Atkin–Lehner eigenvalues $\varepsilon = (-1, -1)$ specified in §1.3.2. Nothing new is proven in this section. Those readers who have some familiarity with the ideas of [WWE21] can safely skip this section on first reading, and refer back when necessary.

2.1. Modular forms.

As in [WWE21, §2.1], we recall the following Hecke algebras and modular forms of weight 2.

Let $\mathfrak{H}_N$ denote the Hecke algebra generated (over $\mathbb{Z}$) by the action of the Hecke operators

$$\begin{aligned} &T_q, \text{ for } q \nmid N \text{ prime, and} \\ &w_\ell, \text{ for } \ell \mid N \text{ prime,} \end{aligned} \tag{2.1.1}$$

on modular forms of weight 2 and level $\Gamma_0(N)$. Here T_q is the standard unramified Hecke operator, while w_ℓ is the Atkin–Lehner involution at ℓ. It is well known that $\mathfrak{H}_N$ is commutative, reduced, and free of finite rank as a $\mathbb{Z}$-module.

As remarked in §1.3.2, the space $\mathrm{Eis}_2(\Gamma_0(N))$ of Eisenstein series of weight 2 and level $\Gamma_0(N)$ is 3-dimensional, and our choice of (w_{ℓ_0}, w_{ℓ_1})-eigenvalues $\varepsilon = (-1,-1)$ specifies a unique normalized Hecke eigenform $E_{2,N} = E^\varepsilon_{2,N}$. It has T_q-eigenvalue $q+1$ for all primes $q \nmid N$. The value at the cusp at infinity of $E^\varepsilon_{2,N}$ is

$$a_0(E^\varepsilon_{2,N}) = \frac{1}{2}\zeta(-1)\prod_{\ell \mid N}(\ell-1) = -\frac{1}{24}\prod_{\ell\mid N}(\ell-1).$$

Now we define the Hecke algebras and Eisenstein ideals that are our primary object of study, measuring congruences of Hecke eigenvalues between $E^\varepsilon_{2,N}$ and cusp forms.

- Let $\mathbb{T}$ denote the completion of $\mathfrak{H}_N$ at its maximal ideal $(p, \mathrm{Ann}_{\mathfrak{H}_N}(E^\varepsilon_{2,N}))$. Its residue field is $\mathbb{F}_p$, because $\mathfrak{H}_N/\mathrm{Ann}_{\mathfrak{H}_N}(E^\varepsilon_{2,N}) \cong \mathbb{Z}$.
- Let $\mathbb{T}^0$ be the cuspidal quotient of $\mathbb{T}$.
- Let $I := \mathrm{Ann}_{\mathfrak{H}_N}(E^\varepsilon_{2,N}) \cdot \mathbb{T}$, which we call the *Eisenstein ideal*. We have $\mathbb{T}/I \cong \mathbb{Z}_p$.
- Let I^0 denote the image of I in $\mathbb{T}^0$.
- Ohta [Oht03] has proved that

$$\mathbb{T}^0/I^0 \cong \mathbb{Z}_p/a_0(E^\varepsilon_{2,N})\mathbb{Z}_p.$$

We call (the p-part of) $a_0(E^\varepsilon_{2,N})$ *the congruence number* for congruences (modulo p) of Hecke eigenvalues between $E^\varepsilon_{2,N}$ and cusp forms. Our assumption that $\ell_0 \equiv 1 \pmod p$ implies that $\mathbb{T}^0/I^0 \neq 0$, which is equivalent to $\mathbb{T}^0 \neq 0$.

Let $M_2(N;\mathbb{Z}_p)^\varepsilon_{\mathrm{Eis}}$ denote the module of modular forms of weight 2 and level $\Gamma_0(N)$ with coefficients in $\mathbb{Z}_p$, subject to the condition that their Hecke eigensystem under the Hecke operators of (2.1.1) are congruent modulo p to that of the Eisenstein series $E^\varepsilon_{2,N}$. Let $S_2(N;\mathbb{Z}_p)^\varepsilon_{\mathrm{Eis}}$ denote the submodule of $M_2(N;\mathbb{Z}_p)^\varepsilon_{\mathrm{Eis}}$ consisting of cusp forms. We have perfect pairings

$$M_2(N;\mathbb{Z}_p)^\varepsilon_{\mathrm{Eis}} \times \mathbb{T} \to \mathbb{Z}_p, \qquad S_2(N;\mathbb{Z}_p)^\varepsilon_{\mathrm{Eis}} \times \mathbb{T}^0_N \to \mathbb{Z}_p. \tag{2.1.2}$$

Under the usual Fourier expansion of a modular form $f(z) = \sum_{n\geq 0} a_n(f)q^n \in M_2(N;\mathbb{Z}_p)^\varepsilon_{\mathrm{Eis}}$, the pairing is given by $(f,T) \mapsto a_1(Tf)$.

In particular, these pairings specialize to a bijection between normalized Hecke eigenforms in $M_2(N;\mathbb{Z}_p)^\varepsilon_{\mathrm{Eis}}$ (resp. $S_2(N;\mathbb{Z}_p)^\varepsilon_{\mathrm{Eis}}$) and homomorphisms $\mathbb{T} \to \overline{\mathbb{Q}}_p$ (resp. $\mathbb{T}^0 \to \overline{\mathbb{Q}}_p$) that encode their eigensystems.

We will also require the Eisenstein-congruent Hecke algebras of weight 2 and level ℓ_0 with Atkin–Lehner sign -1, denoted $\mathbb{T}_{\ell_0}$, along with its cuspidal quotient $\mathbb{T}^0_{\ell_0}$. This $\mathbb{T}^0_{\ell_0}$ is the Hecke algebra studied by Mazur in [Maz77]. There are natural surjections $\mathbb{T} \twoheadrightarrow \mathbb{T}_{\ell_0}$ and $\mathbb{T}^0 \twoheadrightarrow \mathbb{T}^0_{\ell_0}$, because a choice of Atkin–Lehner signature at level N designates a stabilization of level ℓ_0 forms to level N.

In light of (2.1.2) and the fact that each of the spaces of modular forms has a basis of Hecke eigenvectors, we have the well known

Lemma 2.1.3. *The Hecke algebras $\mathbb{T}$, $\mathbb{T}^0$, $\mathbb{T}_{\ell_0}$, and $\mathbb{T}^0_{\ell_0}$ are reduced and, as $\mathbb{Z}_p$-modules, finitely generated and flat.*

2.2. **Galois deformation theory.** The main technical feature of [WWE21] was the development of theory of Galois representations adequate to characterize the Galois representations associated to $M_2(N;\mathbb{Z}_p)^{\varepsilon}_{\mathrm{Eis}}$. In particular, while $\mathbb{T}$ interpolates the Hecke eigensystems, interpolating the associated Galois representations presents technical issues addressed in [WWE21, §3].

The key new notion presented there is the *unramified-or-Steinberg* condition on 2-dimensional pseudorepresentations of G_ℓ, which combined over all $\ell \mid N$ to a global unramified-or-Steinberg condition. Because we view this paper as a test of these notions in a more difficult setting (where $\mathbb{T}$ is not Gorenstein), we carefully recall this notion. Also, since the global unramified-or-Steinberg condition involves the *finite-flat* geometricity condition on representations of G_p, we recall that theory as well.

2.2.1. *Background on pseudodeformations.* We will presume that the reader is familiar with the theory of pseudorepresentations, as developed by Chenevier [Che14]. This is summarized in [WWE21, §3.1], and we recall fundamental notions here. All of our pseudorepresentations are 2-dimensional.

Let A be a commutative ring. We write $D : E \to A$ for a pseudorepresentation, which includes the implication that E is an A-algebra (not necessarily commutative). The data represented by this notation consists of functions

$$D_B : E \otimes_A B \to B$$

associated functorially to commutative A-algebras B.

When H is a group, we write $D : H \to A$ as shorthand for a pseudorepresentation $D : A[H] \to A$. A pseudorepresentation $D : E \to A$ is characterized by its induced characteristic polynomial functions, which in the present 2-dimensional case are the two functions

$$\mathrm{Tr}_D : E \to A \quad \text{and} \quad \det_D : E \to A.$$

When the source and target of a pseudorepresentation D have a topology, D is considered continuous when Tr_D and $\det_D$ are continuous. When H is a profinite group and A is a profinite ring, we will presume that a pseudorepresentation $D : H \to A$ is continuous from $A[H]$ to A without further comment.

2.2.2. *Cayley–Hamilton representations and GMA representations.* While a pseudorepresentation $D : G \to A$ may not arise from a 2-dimensional representation of G over A, it is well-understood how to broaden the category of representations to remedy this. This broader category consists of *Cayley–Hamilton representations* of G. It is fibered over the category of pseudorepresentations and has universal objects. In this section, we overview the theory of Cayley–Hamilton representations, referring to [WWE21, §3] for details. We also point out that the Cayley–Hamilton representations we work with in this paper admit the structure of generalized matrix algebras ("GMAs").

Let A denote a commutative ring.

- We say that a pseudorepresentation $D : E \to A$ is *Cayley–Hamilton* if, for every commutative A-algebra B and every element $\gamma \in E \otimes_A B$, γ satisfies its B-valued characteristic polynomial $X^2 - \mathrm{Tr}_D(\gamma)X + \det_D(\gamma) \in B[X]$.
- A *Cayley–Hamilton algebra over* A is a pair $(E, D : E \to A)$, where D is a Cayley–Hamilton pseudorepresentation.

- An *A-valued Cayley–Hamilton representation of* G is a tuple $(\rho : G \to E^\times, E, D : E \to A)$, where (E, D) is a Cayley–Hamilton algebra over A and ρ is a group homomorphism.
- The *induced pseudorepresentation* of a Cayley–Hamilton representation $(\rho, E, D : E \to A)$ of G, written $\psi(\rho)$, is the A-valued pseudorepresentation of G determined by the composition $D \circ \rho$.

A *generalized matrix algebra over* A, or "A-GMA" for short, is a Cayley–Hamilton algebra over A with extra data. We confine our discussion to 2-by-2 GMAs.

- The data for a $(2 \times 2$-)GMA over A consists of two A-modules B and C together with an A-module map $m : B \otimes_A C \to R$ such that the two maps
$$B \otimes_A C \otimes_A B \to B \otimes_A A \to B \quad \text{and} \quad B \otimes_A C \otimes_A B \to A \otimes_A B \to B$$
coincide, and similarly the two maps $C \otimes_A B \otimes_A C \to C$ coincide. We make an A-algebra $\begin{pmatrix} A & B \\ C & A \end{pmatrix}$ using the rule for 2×2-matrix multiplication.
- We think of a *GMA structure* on a Cayley–Hamilton algebra as the idempotents $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ in the above decomposition.
- When A is a Henselian local ring and a Cayley–Hamilton algebra E over A is finitely generated as an A-module (which will always be true in our applications, and is actually equivalent to being finitely generated as an A-algebra), its A-GMA structures are inner-isomorphic [WWE18, Lem. 5.6.8].
- When a Cayley–Hamilton representation $(\rho, E, D : E \to A)$ of G has its Cayley–Hamilton algebra E equipped with the structure of an A-GMA, it is known as a *GMA representation.*

2.2.3. *Deformation theory of pseudorepresentations.* The functorial basis for deformation theory of pseudorepresentations is rather straightforward in [Che14]. What is less straightforward is the approach to applying representation-theoretic conditions on pseudorepresentations that are most naturally formatted for representations. The main idea for this, developed systematically in [WWE19], is to say that a pseudorepresentation satisfies a condition when some Cayley–Hamilton representation inducing it. In this section, we overview these deformation-theoretic concepts, first specializing to the particular pseudorepresentation that we will deform.

- Let $\omega : G_{\mathbb{Q}} \to \mathbb{F}_p^\times$ denote the modulo p cyclotomic character, which factors through $G_{\mathbb{Q},Np}$. It is the reduction modulo p of the p-adic cyclotomic character that we denote by $\kappa : G_{\mathbb{Q}} \to \mathbb{Z}_p^\times$.
- Let $\bar{D} : G_{\mathbb{Q},Np} \to \mathbb{F}_p$ denote the pseudorepresentation $\psi(\omega \oplus 1)$ of $G_{\mathbb{Q},Np}$.
- When A is a commutative local ring with residue field $\mathbb{F}_p$, we say that $D : G_{\mathbb{Q},Np} \to A$ *deforms* $\bar{D}$ if the composite pseudorepresentation $G_{\mathbb{Q},Np} \to A \twoheadrightarrow \mathbb{F}_p$ equals $\bar{D}$.
- Let $R_{\bar{D}}$ denote the universal pseudodeformation ring of $\bar{D}$, which is known to be Noetherian. This means that there is a universal pseudodeformation $D^u_{\bar{D}} : G_{\mathbb{Q},Np} \to R_{\bar{D}}$.

Now we bring Cayley–Hamilton representations into the deformation theory of pseudorepresentations.

- When A is local with residue field $\mathbb{F}$ and $\bar{D} : G \to \mathbb{F}$ is a pseudorepresentation, we say that an A-valued Cayley–Hamilton representation (ρ, E, D) of G is *over* $\bar{D}$ when the pseudorepresentation $D \circ \rho : G \to A$ deforms $\bar{D}$.

- There exists a universal Cayley–Hamilton representation of $G_{\mathbb{Q},Np}$ over $\bar{D}$, valued in the universal pseudodeformation ring $R_{\bar{D}}$. It is written

$$(\rho^u : G_{\mathbb{Q},Np} \to E^u_{\bar{D}}, E^u_{\bar{D}}, D^u_{E_{\bar{D}}} : E^u_{\bar{D}} \to R^u_{\bar{D}}).$$

- Because $\bar{D}$ is multiplicity-free—that is, its associated semi-simple representation $\omega \oplus 1$ over $\mathbb{F}_p$ has non-isomorphic simple summands—it is known that any Cayley–Hamilton representation of $G_{\mathbb{Q},Np}$ over $\bar{D}$ admits the structure of a GMA representation.

2.2.4. *The unramified-or-Steinberg condition.* We now review the *unramified-or-Steinberg* condition that was introduced in [WWE21, §3]. In [WWE21, §3], it was called the "unramified-or-ε-Steinberg condition" or "$\mathrm{US}^\varepsilon_N$ condition", to allow for arbitrary choice of Atkin–Lehner signs ε. For this paper, we only consider negative Atkin–Lehner signs and we suppress the ε from the notation.

The definition is motivated by the forms of Galois representations of modular forms at decomposition groups, as we now recall. When $\ell \neq p$, it is known that Galois representations $\rho_f : G_{\mathbb{Q},Np} \to \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$ arising from a Hecke eigenform (for the Hecke operators of (2.1.1)) in $M_2(\Gamma_0(N))$ have the following form after restriction to a decomposition group.

- $\rho_f|_{I_\ell}$ is non-trivial if and only if f is new at ℓ. In other words, $\rho_f|_{G_\ell}$ is unramified if and only if f is old at ℓ.
- If f is new at ℓ and its w_ℓ-eigenvalue is -1, then $\rho_f|_\ell : G_\ell \to \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$ has the form

$$\rho_f|_\ell \simeq \begin{pmatrix} \kappa & \tilde{b}_\ell \\ 0 & 1 \end{pmatrix}, \tag{2.2.1}$$

  where $\tilde{b}_\ell : G_\ell \to \overline{\mathbb{Q}}_p(1)$ is an element of $Z^1(\mathbb{Q}_\ell, \overline{\mathbb{Q}}_p(1))$ inducing a non-trivial cohomology class in $H^1(\mathbb{Q}_\ell, \overline{\mathbb{Q}}_p(1))$. By Kummer theory, this cohomology class is unique up to scalar, and consequently the $\rho_f|_\ell$ is uniquely prescribed up to isomorphism.

Definition 2.2.2 ([WWE21, Defn. 3.4.1])**.** A Cayley–Hamilton representation ($\rho : G_\ell \to E, E, D_E : E \to A$) over $\bar{D}|_\ell$ is *unramified-or-Steinberg at* ℓ (or US_ℓ) if

$$(\rho(\sigma) - \kappa(\sigma)) \cdot (\rho(\tau) - 1) = 0 \tag{2.2.3}$$

for all $(\sigma, \tau) \in G_\ell \times I_\ell \cup I_\ell \times G_\ell$.

The initial justification for this definition is that $\rho_f|_{G_\ell}$ of (2.2.1) satisfies the US_ℓ condition. Indeed, in this case the matrix product of (2.2.3) has the form

$$\begin{pmatrix} 0 & * \\ 0 & * \end{pmatrix} \cdot \begin{pmatrix} * & * \\ 0 & 0 \end{pmatrix},$$

and any such product is zero. Next, note that the restriction on (σ, τ)—one of σ, τ must be in I_ℓ—implies that an unramified homomorphism satisfies US_ℓ.

The point of this definition is to interpolate the form (2.2.1) into Cayley–Hamilton algebras, thereby giving rise to a notion of US_ℓ on Cayley–Hamilton representations of G_ℓ over $\bar{D}|_\ell$. In particular, the formulation of US_ℓ is coordinate-free.

2.2.5. *The finite-flat condition.* Since the modular forms we work with have weight 2 and no level at p, the corresponding p-adic representations of G_p should satisfy the finite-flat condition.

Definition 2.2.4. We say that an action on G_p on a finite cardinality $\mathbb{Z}_p$-module M is *finite-flat* provided that there exists a finite flat group scheme $\mathcal{G}/\mathbb{Z}_p$ such that there exists an isomorphism of $\mathbb{Z}_p[G_p]$-modules $M \simeq \mathcal{G}(\overline{\mathbb{Q}}_p)$.

Ramakrishna [Ram93] determined how to apply the finite-flat condition to deformations of Galois representations. The crucial formal property that the finite-flat condition satisfies is that it is *stable*, meaning that when M is a finite-flat $\mathbb{Z}_p[G_p]$-module, then all of its subquotients are also finite-flat; and that if a finite number of $\mathbb{Z}_p[G_p]$-modules M_i are finite-flat, then so is the direct sum $\bigoplus_i M_i$.

Because not all pseudorepresentations arise from Galois representations as characteristic polynomials, it is non-trivial to impose the finite-flat condition on pseudorepresentations. This problem has been addressed in [WWE19], using a formalism that works for any stable condition. It relies on the fact that every pseudorepresentation arises from a Cayley–Hamilton representation.

Definition 2.2.5. We call a Cayley–Hamilton representation $\rho : G_p \to E$ *finite-flat* if the $\mathbb{Z}_p[G]$-module E, where the action of G_p on E is given by ρ composed with the left regular action of E on E, is an inverse limit of finite-flat $\mathbb{Z}_p[G]$-modules. We call a pseudorepresentation $D : G_p \to A$ *finite-flat* if it arises as the induced pseudorepresentation $\psi(\rho)$ of a Cayley–Hamilton representation ρ that is finite-flat.

In [WWE19], it is proved that any stable condition cuts out a universal Cayley–Hamilton representation over any residual pseudorepresentation $\bar{D} : G_p \to \mathbb{F}$, and that the coefficient ring of this Cayley–Hamilton representation is the universal finite-flat pseudodeformation ring of $\bar{D}$. In particular, this result includes the implication that the finite-flat condition on pseudorepresentation cuts out a quotient $R_{\bar{D}} \twoheadrightarrow R_{\bar{D}}^{\mathrm{flat}}$ of the universal pseudodeformation ring; in other words, the finite-flat condition is a Zariski-closed condition on pseudorepresentations.

We have the following result about finite-flat representations over the residual pseudorepresentation $\bar{D}|_p$.

Proposition 2.2.6. *For any finite-flat Cayley–Hamilton representation ρ of G_p over $\bar{D}|_p : G_p \to \mathbb{F}_p$, with coefficient ring A, there exist unique characters $\theta_i : G_p \to A^\times$, $i = 1, 2$, and a GMA structure with respect to which it has the form*

$$\rho \simeq \begin{pmatrix} \kappa\theta_1 & * \\ 0 & \theta_2 \end{pmatrix}. \tag{2.2.7}$$

The characters θ_i are residually trivial and unramified.

Proof. See [WWE21, §3.5]. □

However, the finite-flat condition is more strict than merely having this form: in addition to the unramified condition on θ_i, there is a restriction on the extension denoted "$*$", cutting out an A-submodule

$$\mathrm{Ext}^1_{A[G_p]}(\theta_2, \theta_1(1))^{\mathrm{flat}} \subset \mathrm{Ext}^1_{A[G_p]}(\theta_2, \theta_1(1))$$

consisting of finite-flat extensions of θ_2 by $\kappa\theta_1$. We will especially be interested in the case where $A = \mathbb{F}_p$ and the θ_i are trivial. In that case, since $\omega = (\kappa \mod p)$

lifts to $G_{\mathbb{Q},Np}$, we construct

$$\mathrm{Ext}^1_{\mathbb{F}_p[G_{\mathbb{Q},Np}]}(\mathbb{F}_p, \mathbb{F}_p(1))^{\mathrm{flat}} \subset \mathrm{Ext}^1_{\mathbb{F}_p[G_{\mathbb{Q},Np}]}(\mathbb{F}_p, \mathbb{F}_p(1))$$

consisting of those $G_{\mathbb{Q},Np}$-extensions of $\mathbb{F}_p$ by $\mathbb{F}_p(1)$ that are finite-flat when restricted to G_p.

Later we will have use for the determination of this finite-flat subspace more generally, over $\mathbb{Q}_{p^i}$, which denotes the unique degree i unramified extension of $\mathbb{Q}_p$. Let $H_i := \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_{p^i})$, so $H_1 = G_p$. Let $\mathbb{Z}_{p^i}$ denote the ring of integers of $\mathbb{Q}_{p^i}$.

Lemma 2.2.8 (Local Kummer theory)**.** *Under the canonical isomorphism*

$$\mathrm{Ext}^1_{\mathbb{F}_p[H_i]}(\mathbb{F}_p, \mu_p) \cong H^1(\mathbb{Q}_{p^i}, \mu_p) \cong \mathbb{Q}_{p^i}^\times/(\mathbb{Q}_{p^i}^\times)^p$$

and the canonical decomposition

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

the flat subspace $\mathrm{Ext}^1_{\mathbb{F}_p[H_i]}(\mathbb{F}_p, \mu_p)^{\mathrm{flat}}$ *maps to* $\mathbb{Z}_{p^i}^\times/(\mathbb{Z}_{p^i}^\times)^p$*. In particular, when* $i = 1$*, we have the* $\mathbb{F}_p$*-basis* $\{p, 1+p\}$ *of* $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^p$*, and the subspace* $\mathrm{Ext}^1_{\mathbb{F}_p[G_p]}(\mathbb{F}_p, \mu_p)^{\mathrm{flat}}$ *corresponds with the subspace* $\langle 1+p\rangle$*.*

Proof. This is well known; see, for example, [Sch12, Prop. 2.2]. □

Lemma 2.2.9 (Global Kummer theory)**.**

(1) The subspace

$$\mathrm{Ext}^1_{\mathbb{F}_p[\![G_{\mathbb{Q},Np}]\!]}(\mathbb{F}_p, \mu_p)^{\mathrm{flat}} \subset \mathrm{Ext}^1_{\mathbb{F}_p[\![G_{\mathbb{Q},Np}]\!]}(\mathbb{F}_p, \mu_p)$$

has basis $\{\ell_0, \ell_1\}$ *under the canonical isomorphisms*

$$\mathrm{Ext}^1_{\mathbb{F}_p[\![G_{\mathbb{Q},Np}]\!]}(\mathbb{F}_p, \mu_p) \cong H^1(\mathbb{Z}[1/Np], \mu_p) \cong \mathbb{Z}[1/Np]^\times/(\mathbb{Z}[1/Np]^\times)^p.$$

(2) The natural map

$$\mathrm{Ext}^1_{\mathbb{F}_p[\![G_{\mathbb{Q},Np}]\!]}(\mathbb{F}_p, \mathbb{F}_p(1)) \longrightarrow \mathrm{Ext}^1_{\mathbb{F}_p[\![G_p]\!]}(\mathbb{F}_p, \mathbb{F}_p(1))$$

has image containing a complement of $\mathrm{Ext}^1_{\mathbb{F}_p[\![G_p]\!]}(\mathbb{F}_p, \mathbb{F}_p(1))^{\mathrm{flat}}$*. The image of the element* $p \in \mathbb{Z}[1/Np]^\times/(\mathbb{Z}[1/Np]^\times)^p$ *spans this complement.*

Proof. Parts (1) and (2) follow directly from Lemma 2.2.8 and the fact that $\{p, \ell_0, \ell_1\}$ is a basis for $\mathbb{Z}[1/Np]^\times/(\mathbb{Z}[1/Np]^\times)^p$. □

Here is a method to verify finite-flatness of GMA-representations in practice.

Lemma 2.2.10. *Let* $\rho : G_p \to E$ *be a Cayley–Hamilton representation with coefficient ring* A*. Suppose that* $S \subset E$ *be a subalgebra containing* $\rho(G_p)$*, and let* V *be a faithful* S*-module. If the* G_p*-action on* V *induced by* ρ *is finite-flat, then* ρ *is finite-flat.*

Proof. This is a slight generalization of the argument of the second paragraph of the proof of [WWE21, Lem. 7.1.9]. □

We will also require the delicate use of a few standard and fundamental facts about lifts of group representations and the unobstructedness of finite-flat lifts, which we collect in the following two statements. We state these in less than their maximal generality, fitting our purposes.

Lemma 2.2.11. *Let G be a profinite group, let $\eta : G \to \mathrm{GL}_2(\mathbb{F}_p)$ be a representation, and let $s : (A', \mathfrak{m}_{A'}) \twoheadrightarrow (A, \mathfrak{m}_A)$ be a surjection of local Artinian $\mathbb{F}_p$-algebras such that $\mathfrak{m}_{A'} \cdot \ker s = 0$. Let η_A be a lift of η over $A \twoheadrightarrow A/\mathfrak{m}_A = \mathbb{F}_p$.*

1. *If the set of lifts of η_A over $A' \twoheadrightarrow A$ is non-empty, then it is a torsor over the group*
$$Z^1(G, \mathrm{Ad}(\eta)) \otimes_{\mathbb{F}_p} \ker s$$
under addition of coordinates.
2. *If $A = \mathbb{F}_p$, then this torsor is canonically isomorphic to $Z^1(G, \mathrm{Ad}(\eta)) \otimes_{\mathbb{F}_p} \ker s$ due to the base point given by the trivial lift $\rho \otimes_{\mathbb{F}_p} A$ of ρ to A.*
3. *Conjugation of $\rho_{A'}$ by $x \in \ker(\mathrm{GL}_2(A') \twoheadrightarrow \mathrm{GL}_2(A))$, which is canonically isomorphic to $C^0(G, \mathrm{Ad}(\rho)) \otimes_{\mathbb{F}_p} \ker s$, amounts to acting by coboundary $dx \in B^1(G, \mathrm{Ad}(\rho)) \otimes_{\mathbb{F}_p} \ker s$ on $\rho_{A'}$ (via the torsor structure of (1)).*
4. *If η_A has constant determinant (that is, $\det \eta_A = \det \eta$ under $\mathbb{F}_p^\times \hookrightarrow A^\times$)), then the set of constant determinant lifts of η_A over s is non-empty if and only if the set of (unrestricted) lifts is non-empty; and if it is non-empty, it is a torsor over the group*
$$Z^1(G, \mathrm{Ad}^0(\eta)) \otimes_{\mathbb{F}_p} \ker s$$
under addition of coordinates.

Here "addition of coordinates" on $\rho_{A'}$ means that we add to the function $\rho_{A'} : G \to \mathrm{GL}_2(A')$ the function $G \to M_d(\ker s) \subset \mathrm{GL}_2(A')$ given by an element of $Z^1(G, \mathrm{Ad}(\eta)) \otimes_{\mathbb{F}_p} \ker s$.

Proposition 2.2.12. *Let $\eta : G \to \mathrm{GL}_2(\mathbb{F}_p)$ be a finite-flat representation. Let $s : (A', \mathfrak{m}_{A'}) \twoheadrightarrow (A, \mathfrak{m}_A)$ be a surjection of local Artinian $\mathbb{F}_p$-algebras such that $\mathfrak{m}_{A'} \cdot \ker s = 0$. Let η_A be a finite-flat lift of η over $A \twoheadrightarrow A/\mathfrak{m}_A = \mathbb{F}_p$.*

1. *The set of finite-flat lifts of η_A over s is non-empty, and admits the structure of a torsor over the group*
$$Z^1(G, \mathrm{Ad}(\eta))^{\mathrm{flat}} \otimes_{\mathbb{F}_p} \ker s,$$
where $Z^1(G, \mathrm{Ad}(\eta))^{\mathrm{flat}} \subset Z^1(G, \mathrm{Ad}(\eta))$ is a sub-vector space that contains $B^1(G, \mathrm{Ad}(\eta))$.
2. *In particular, if $A = \mathbb{F}_p$, then this torsor is non-empty and canonically isomorphic to $Z^1(\mathbb{Q}_p, \mathrm{Ad}(\eta)) \otimes_{\mathbb{F}_p} \ker s$.*
3. *The analogue of Lemma 2.2.11(3) holds for finite-flat representations.*
4. *The analogue of Lemma 2.2.11(4) holds for finite-flat representations, with the addition that the set of constant determinant finite-flat lifts is non-empty.*

Proof. The non-emptiness of the set of finite-flat lifts can be found in [CHT08, Lem. 2.4.1], for example. The remaining claims can be deduced from Lemma 2.2.11 using [WWE20, Prop. C.4.1]. □

2.2.6. *The global unramified-or-Steinberg condition.* By combining the local conditions, we arrive at the global condition US_N.

Definition 2.2.13. Let ρ be a Cayley–Hamilton representation over $\bar{D} : G_{\mathbb{Q},Np} \to \mathbb{F}_p$. We say that ρ is *unramified-or-Steinberg of level N*, or US_N, when

1. for all $\ell \mid N$, $\rho|_\ell$ is US_ℓ, and
2. $\rho|_p$ is *finite-flat* in the sense of Definition 2.2.5.

When $D : G_{\mathbb{Q},Np} \to A$ is a deformation of $\bar{D} : G_{\mathbb{Q},Np} \to \mathbb{F}_p$, we say that D is US_N when there exists some A-valued Cayley–Hamilton representation ρ over $\bar{D}$ such that $D = \psi(\rho)$.

We fix notation for the universal objects satisfying US_N, which were produced in [WWE21, §3].

Definition 2.2.14.

- Let R denote the universal pseudodeformation ring of $\bar{D}$ satisfying the US_N condition. It admits a natural surjection $R_{\bar{D}} \twoheadrightarrow R$.
- Likewise, there exists a universal US_N Cayley–Hamilton representation of $G_{\mathbb{Q},Np}$ over $\bar{D}$, denoted
$$(\rho_N : G_{\mathbb{Q},Np} \to E, E, D_E : E \to R)$$
and inducing $D_N : G_{\mathbb{Q},Np} \to R$, the universal US_N deformation of $\bar{D}$.
- We fix a $R^u_{\bar{D}}$-GMA structure on the universal Cayley–Hamilton algebra $E^u_{\bar{D}}$ over $\bar{D}$, which induces a GMA structure on all of the Cayley–Hamilton algebras receiving a map from $E^u_{\bar{D}}$ due to its universal property. In particular, we get a R-GMA structure on the universal US_N Cayley–Hamilton representation (ρ_N, E, D_E) of $G_{\mathbb{Q},Np}$ over $\bar{D}$, and write its matrix coordinates as
$$E \cong \begin{pmatrix} R & B \\ C & R \end{pmatrix}.$$
For $\gamma \in G_{\mathbb{Q},Np}$, we write
$$\begin{pmatrix} a_\gamma & b_\gamma \\ c_\gamma & d_\gamma \end{pmatrix}$$
for its image in E under ρ_N. Letting $\mathfrak{m} \subset R$ denote the maximal ideal, we may and do assume that the GMA structure on $E_{\bar{D}}$ has been chosen such that
$$(a \mod \mathfrak{m}) = \omega \quad \text{and} \quad (d \mod \mathfrak{m}) = 1$$
as homomorphisms $G_{\mathbb{Q},Np} \to \mathbb{F}_p^\times$.
- We will also occasionally refer to R_{ℓ_0} as the universal pseudodeformation of $\bar{D}$ satisfying the (global) US_{ℓ_0} condition (with Atkin–Lehner sign -1 at ℓ_0). There is a natural surjection $R \twoheadrightarrow R_{\ell_0}$.

Having completed these constructions, the crucial application is that we can interpolate over $\mathbb{T}$ the Galois pseudorepresentations induced by the representations $\rho_f : G_{\mathbb{Q},Np} \to \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$ associated to normalized Hecke eigenforms $f \in M_2(N;\mathbb{Z}_p)^\varepsilon_{\mathrm{Eis}}$.

Proposition 2.2.15 ([WWE21, Prop. 4.1.1]). *We have a surjection $R \twoheadrightarrow \mathbb{T}$ characterized by sending traces of Frobenius elements $\mathrm{Tr}_{D_N}(\mathrm{Fr}_q) \in R$ for primes $q \nmid Np$ to the Hecke operator T_q. Similarly, we have $R_{\ell_0} \twoheadrightarrow \mathbb{T}_{\ell_0}$.*

The characterizing property of the map makes its surjectivity visible, since $\mathbb{T}$ is generated by the T_q. The level ℓ_0 map is known to be an isomorphism $R_{\ell_0} \cong \mathbb{T}_{\ell_0}$ [WWE20].

Remark 2.2.16. Our hypothesis is that the local US_ℓ conditions furnish a robust interpolation of the Steinberg shape of Galois representations of (2.2.1) into Cayley–Hamilton algebras. Since the global US_N condition simply puts together these local conditions, we view the putative isomorphism $R \xrightarrow{\sim} \mathbb{T}$ as bearing out this hypothesis.

2.3. **Reducibility of pseudorepresentations.** A 2-dimensional pseudorepresentation $D : G \to A$ is called *reducible* when it has the form $\psi(\chi_1 \oplus \chi_2)$ for some characters $\chi_1, \chi_2 : G \to A^\times$. It is well understood that reducibility is a Zariski-closed condition, meaning that there is a *reducibility ideal* $J^{\mathrm{red}}_{\bar{D}} \subset R_{\bar{D}}$ such that a pseudodeformation $D_A : G \to A$ of $\bar{D}$ is reducible if and only if $J^{\mathrm{red}}_{\bar{D}}$ vanishes under the corresponding homomorphism $R_{\bar{D}} \to A$. And any D_A becomes reducible modulo the image of $J^{\mathrm{red}}_{\bar{D}}$ in A.

When D_A arises from a GMA-representation of G, there is an important expression for the reducibility ideal in terms of the GMA structure. We record the universal US_N case.

Proposition 2.3.1. *The reducibility ideal $J^{\mathrm{red}} \subset R$ is equal to the image of the multiplication map $m : B \otimes_R C \to R$.*

Another canonical ideal of R is the kernel $J^{\min}$ of the composition

$$J^{\min} := \ker(R \twoheadrightarrow \mathbb{T} \twoheadrightarrow \mathbb{Z}_p),$$

that arises from the Eisenstein series $E_{2,N}$. This is characterized by sending $\mathrm{Tr}_{D_N}(\mathrm{Fr}_q) \in R$ for primes $q \nmid Np$ to $q+1$, which is the eigenvalue of T_q on $E_{2,N}$. There is an inclusion of ideals $J^{\mathrm{red}} \subset J^{\min}$ because the $\mathbb{Z}_p$-valued pseudorepresentation $\psi(\kappa \oplus 1)$ associated to $E_{2,N}$ is reducible.

In the following lemma, we compute the quotient of R by the reducibility ideal, which we write as $R^{\mathrm{red}} := R/J^{\mathrm{red}}$.

Lemma 2.3.2. *There is an isomorphism*

$$R^{\mathrm{red}} \cong \frac{\mathbb{Z}_p[Y]}{(Y^2, (\ell_0 - 1)Y)},$$

where Y may be taken to be $a_{\gamma_0} - 1$, and Y generates $J^{\min}/J^{\mathrm{red}}$. The corresponding pseudorepresentation induced by reduction modulo p, $R^{\mathrm{red}} \twoheadrightarrow \mathbb{F}_p[Y]/(Y^2)$, equals

$$D^{\mathrm{red}} := \psi(\omega(1 + Ya_0) \oplus (1 - Ya_0)) : G_{\mathbb{Q},Np} \to \mathbb{F}_p[Y]/(Y^2).$$

Later we will use the local homomorphism $\varphi_{D^{\mathrm{red}}} : R \to \mathbb{F}_p[\epsilon_1]$ induced by D^{red}.

Proof. The first statement is a direct application of the presentation for R^{red} provided in [WWE21, Lem. 4.2.3], and the calculations needed for the second claim are included in its proof. □

2.4. **Designated generators of the universal GMA.** We recall the definitions of some useful cohomology classes and their duals from [WWE21, §3.10]. First we need generators of the pro-p tame part of inertia groups.

Definition 2.4.1. For a prime ℓ_i not equal to p, let $\gamma_i \in I_{\ell_i}$ denote a lift of a topological generator of the maximal pro-p quotient of I_{ℓ_i}, which cuts out a tamely ramified extension of $\mathbb{Q}_p$ and is isomorphic to $\mathbb{Z}_p$.

Proposition 2.4.2. *The elements b_{γ_0} and b_{γ_1} of B generate it as a R-module, and B is not cyclic as a R-module. Similarly, $c_{\gamma_0} \in C$ is a generator as a R-module.*

Proof. See [WWE21, Lem. 3.9.4 and 3.9.8] for the claims about generators, and see [WWE21, Lem. 6.2.1] for the claim that B is not cyclic. □

Lemma 2.4.3. *We have an inclusion of ideals ${J^{\min}}^2 \subset J^{\mathrm{red}} \subset J^{\min}$. The element $b_{\gamma_0} \cdot c_{\gamma_0}$ of J^{red} lies within its submodule ${J^{\min}}^2$.*

Proof. The inclusion of ideals follows from Lemma 2.3.2 because the kernel of $R/J^{\mathrm{red}} = R^{\mathrm{red}} \twoheadrightarrow \mathbb{Z}_p = R/J^{\mathrm{min}}$ is square-nilpotent (similar to the proof of [WWE21, Thm. 6.4.1]). The final claim is [WWE21, Lem. 5.2.5]. □

3. Additional arithmetic preliminaries

In this section, we continue assembling background much as in the previous section, with the distinction that the content of this section is not found in [WWE21]. Our primary focus is a discussion of various implications from our choice of pinning data in Definition 1.7.1 as well as the conditions in Assumption 1.3.2.

3.1. **Cocycles determined by the pinning data.** We fix some notation for Galois cocycles determined by the pinning data of Definition 1.7.1.

Recall the canonical isomorphism

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

of Kummer theory. It sends an element $n \in \mathbb{Z}[1/Np]^\times \otimes_\mathbb{Z} \mathbb{F}_p$ to the class of the cocycle $\sigma \mapsto \frac{\sigma n^{1/p}}{n^{1/p}}$ 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 $\mu_p \not\subset \mathbb{Q}^\times$, each Kummer cocycle of n is given by $\sigma \mapsto \frac{\sigma n^{1/p}}{n^{1/p}}$ for a unique choice of $n^{1/p} \in \overline{\mathbb{Q}}$ of pth root of n. We use the isomorphism $\mathbb{F}_p(1) \cong \mu_p$ chosen in §1.7 to value Kummer classes and cocycles in $\mathbb{F}_p(1)$.

Definition 3.1.1.

- Denote the Kummer classes of ℓ_0, ℓ_1, and p, respectively, by
$$b_0, b_1, b_p \in H^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1)).$$
- Let
$$\gamma_0 \in I_{\ell_0},\ \gamma_1 \in I_{\ell_1}$$
be as in Definition 2.4.1 and fixed such that $b_i(\gamma_i) = 1$.[2]
- 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 $\ell_1^{1/p}$ of ℓ_0 and ℓ_1, respectively, chosen in §1.7. 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) $c^{(1)}|_{\ell_1} = 0$.

  A class c_0 satisfying (i) and (ii) exists and is unique up to $\mathbb{F}_p^\times$-scaling by [WWE21, Lem. 3.10.2], so property (iii) specifies c_0 uniquely. This determines $c^{(1)}$ up to a coboundary and, since elements of elements of $B^1(\mathbb{Q}_{\ell_1}, \mathbb{F}_p(-1))$ are determined by their value on a Frobenius element in G_{ℓ_1}, property (iv) specifies $c^{(1)}$ uniquely.

[2] 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
$$x_{c^{(1)}} \in C^0(G_p, \mathbb{F}_p(-1)) = \mathbb{F}_p(-1)$$
be such that $c^{(1)}|_p = dx_{c^{(1)}}$. Concretely, for any $\tau \in G_p$ such that $\omega(\tau) \neq 1$, we can define $x_{c^{(1)}}$ as $x_{c^{(1)}} = (\omega(\tau)-1)^{-1}c^{(1)}(\tau)$.
- 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).

Remark 3.1.2. The following choices made in Definition 3.1.1 depend only on the pinning data of Definition 1.7.1:

- The cocycles $b^{(1)}$, $c^{(1)}$, and a_0.
- The images of γ_i in $I_{\ell_i}^{\mathrm{tame}} \otimes_{\mathbb{Z}} \mathbb{F}_p$.

3.2. **Cup products and congruence conditions.** The conditions in this paper's running assumption, Assumption 1.3.2, are presented in what we think is the most readable language. However, our methods require various implications of these conditions that are related to the the vanishing of certain cup products among the cohomology classes that we have just defined and/or the local vanishing of the cohomology classes themselves. The point of this section is to record those implications.

We emphasize that we assume $p \geq 5$ throughout.

Lemma 3.2.1 (Conditions equivalent to (3) in Assumption 1.3.2)**.** *Let ℓ_0, ℓ_1 be distinct primes such that $\ell_0 \equiv 1 \pmod p$ and $\ell_1 \not\equiv 0, \pm 1 \pmod p$. The following conditions (1)-(4) are equivalent.*

(1) ℓ_1 is a pth power modulo ℓ_0.
(2) $a_0|_{\ell_1} = 0$ in $H^1(\mathbb{Q}_{\ell_1}, \mathbb{F}_p)$.
(3) $b_1|_{\ell_0} \in H^1(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(1))$ vanishes.
(4) $b_1 \cup c_0 = 0$ in $H^2(\mathbb{Z}[1/Np], \mathbb{F}_p)$.

Proof. (1) $\iff$ (2). Let $\zeta_{\ell_0}^{(p)} \in \overline{\mathbb{Q}}$ represent a primitive element for the unique degree p subextension of $\mathbb{Q}(\zeta_{\ell_0})/\mathbb{Q}$. We see that (2) is true if and only if ℓ_1 splits completely in $\mathbb{Q}(\zeta_{\ell_0}^{(p)})/\mathbb{Q}$, which, in turn, is equivalent to a Frobenius element Fr_{ℓ_1} for ℓ_1 vanishing in $\mathrm{Gal}(\mathbb{Q}(\zeta_{\ell_0}^{(p)})/\mathbb{Q})$. Then the equivalence of (1) and (2) follows from the standard fact that $\mathrm{Fr}_{\ell_1} \mapsto \ell_1$ under the canonical isomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta_{\ell_0})/\mathbb{Q}) \xrightarrow{\sim} \mathbb{F}_{\ell_0}^\times$.

(1) $\iff$ (3). The Kummer theory isomorphism $H^1(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(1)) \cong \mathbb{Q}_{\ell_0}^\times/(\mathbb{Q}_{\ell_0}^\times)^p$ sends b_1 to ℓ_1.

(3) $\iff$ (4). We will apply the injection $H^2(\mathbb{Z}[1/Np], \mathbb{F}_p) \hookrightarrow H^2(\mathbb{Q}_{\ell_0}, \mathbb{F}_p)$ of [WWE20, Lem. 12.1.1] (recorded also in Lemma 3.2.8, below), reducing the condition (4) to $b_1|_{\ell_0} \cup c_0|_{\ell_0} = 0$ in $H^2(\mathbb{Q}_{\ell_0}, \mathbb{F}_p)$. Then (3) $\Rightarrow$ (4) is clear. The converse follows from the characterization of the ℓ_0-local cup product of Lemma 3.2.6: because $c_0|_{\ell_0}$ is ramified, while $b_1|_{\ell_0}$ is non-trivial and unramified, their cup product is non-zero. □

Next, the following lemma generalizes, to odd primes p, the pattern of ramification of the prime 2 in quadratic number fields. In particular, it establishes when

$\ell_i^{1/p} \in \overline{\mathbb{Q}}$ in the pinning data of Definition 1.7.1 can be chosen to have image in $\mathbb{Q}_p$ under the fixed embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$.

Lemma 3.2.2. *Let ℓ be a prime, $\ell \neq p$, and let $b_\ell \in H^1(\mathbb{Q}, \mathbb{F}_p(1))$ be the Kummer class of ℓ. The following conditions are equivalent.*

(1) $\ell^{p-1} - 1$ *is divisible by* p^2
(2) $a_p|_\ell \in H^1(\mathbb{Q}_\ell, \mathbb{F}_p)$ *is trivial*
(3) $b_\ell|_p \in H^1(\mathbb{Q}_p, \mathbb{F}_p(1))$ *is trivial*
(4) $b_\ell|_p \in H^1(\mathbb{Q}_p^{\mathrm{ur}}, \mathbb{F}_p(1))$ *is trivial*
(5) $\mathbb{Q}(\ell^{1/p})/\mathbb{Q}$ *is not totally ramified at p; or, what is the same, tamely ramified at p*
(6) *p splits into two primes in $\mathbb{Q}(\ell^{1/p})/\mathbb{Q}$, one with ramification degree $p-1$ and one with ramification degree 1.*

Proof. (1) $\iff$ (2). Because this proof is very similar to the proof of (1) $\iff$ (2) in Lemma 3.2.1, we omit it.

(1) $\iff$ (3). Likewise, see the proof of (1) $\iff$ (3) in Lemma 3.2.1.

(3) $\iff$ (4). This is [WWE21, Lem. B.1.1].

(4) $\iff$ (5). Consider $b_\ell|_{\mathbb{Q}(\zeta_p)}$, which is a surjective homomorphism $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_p)) \twoheadrightarrow \mathbb{F}_p(1)$. We observe that both (4) and (5) are equivalent to $b_\ell|_{\mathbb{Q}(\zeta_p)}$ being unramified at the unique prime $(1-\zeta_p)$ of $\mathbb{Q}(\zeta_p)$ over p.

(5) $\iff$ (6). The implication (6) $\implies$ (5) is clear. For the converse, note that the Galois closure of $\mathbb{Q}(\ell^{1/p})/\mathbb{Q}$ is $\mathbb{Q}(\ell^{1/p}, \zeta_p)/\mathbb{Q}$, and carry out a prime decomposition exercise. □

We now shift to a discussion of local cup products related to item (1) in Assumption 1.3.2. Indeed, since we have assumed $\ell_0 \equiv 1 \pmod p$, our chosen primitive pth root of unity $\zeta_p \in \overline{\mathbb{Q}}$, along with the chosen embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_{\ell_0}$, induces an isomorphism

$$\mathbb{F}_p(i)|_{\ell_0} \xrightarrow{\sim} \mathbb{F}_p(j)|_{\ell_0}, \qquad x \mapsto x \otimes \zeta_p^{j-i} \tag{3.2.3}$$

of representations of G_{ℓ_0} for any $i, j \in \mathbb{Z}$. We can also view this as a cup product in cohomology, because $\mathbb{F}_p(i) = H^0(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(i))$. One may readily check that cup products with these cohomology classes result in isomorphisms

$$H^0(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(i)) \otimes_{\mathbb{F}_p} H^j(\mathbb{Q}_{\ell_0}, M) \xrightarrow{\sim} H^j(\mathbb{Q}_{\ell_0}, M(i))$$

for any $\mathbb{F}_p[G_{\ell_0}]$-module M and any $i, j \in \mathbb{Z}$. We will also use, in what follows, that the cup product is "bilinear under multiplication (via the cup product) by elements of $H^0(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(s))$, $s \in \mathbb{Z}$." A concise way to precisely state this fact is that the sum of the cup products on $H^1(\mathbb{Q}_{\ell_0}, -)$ applied to all of the $\mathbb{F}_p(i)$, namely,

$$\bigoplus_{i \in \mathbb{Z}} H^1(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(i)) \times \bigoplus_{j \in \mathbb{Z}} H^1(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(j)) \to \bigoplus_{k \in \mathbb{Z}} H^2(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(k)), \tag{3.2.4}$$

is graded bilinear over the graded ring $\bigoplus_{s \in \mathbb{Z}} H^0(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(s))$.

We will be particularly interested in the cup product action of $\mathbb{F}_p(i)|_{\ell_0}$ on the local Tate duality pairing: for $i \in \mathbb{Z}$,

$$H^1(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(i)) \times H^1(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(1-i)) \longrightarrow H^2(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(1)) \cong \mathbb{F}_p. \tag{3.2.5}$$

We express all of the possible twists of this pairing in the following lemma.

Lemma 3.2.6. *For any $i, j \in \mathbb{Z}$, we have a perfect pairing*

$$H^1(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(i)) \times H^1(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(j)) \to H^2(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(i+j)) \cong \mathbb{F}_p(1-i-j) \tag{3.2.7}$$

under which

1. *the cup product of a ramified class with a non-trivial unramified class is non-zero and*
2. *the cup product of any two unramified classes is zero.*

When $i = j$, the self-pairing (3.2.7) *is alternating.*

Proof. The claims (1) and (2) are straightforward for $i = 0, j = 1$ using class field theory. This holds true for all i, j using graded bilinearity of (3.2.4). The alternating property follows from (1), (2), and an extra application of duality. □

We turn from local cup products to implications for global cup products, which we will frequently use.

Lemma 3.2.8 (Hasse principle)**.** *For $i = -1, 0, 1$, the map*

$$H^2(\mathbb{Z}[1/Np], \mathbb{F}_p(i)) \to H^2(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(i)) \oplus H^2(\mathbb{Q}_{\ell_1}, \mathbb{F}_p(i)), \quad x \mapsto (x|_{\ell_0}, x|_{\ell_1})$$

is injective.

Our proof for $i = -1$ also uses (2) in Assumption 1.3.2, i.e., $\ell_1 \not\equiv 0, \pm 1 \pmod{p}$.

Proof. For $i = 0, -1$, the map is an isomorphism. The case $i = 0$ follows directly from [WWE21, Lem. B.1.2]. The case $i = -1$ more-or-less follows from the argument for [WWE20, Lem. 12.1.1], but that argument is written in the setting where "N" is a prime that is $1 \pmod{p}$. The same argument applies in our setting, where $N = \ell_0\ell_1$ with $\ell_0 \equiv 1 \pmod{p}$ and $\ell_1 \not\equiv \pm 1, 0 \pmod{p}$, because $H^j(\mathbb{Q}_{\ell_1}, \mathbb{F}_p(-1)) = 0$ for all $j \in \mathbb{Z}_{\geq i}$, making the exact triangle

$$R\Gamma(\mathbb{Z}[1/\ell_0 p], \mathbb{F}_p(-1)) \to R\Gamma(\mathbb{Z}[1/Np], \mathbb{F}_p(-1)) \to R\Gamma(\mathbb{Q}_{\ell_1}, \mathbb{F}_p(-1))$$

degenerate.

The case $i = 1$ remains. Here the localization map

$$H^2(\mathbb{Z}[1/Np], \mathbb{F}_p(i)) \to H^2(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(i)) \oplus H^2(\mathbb{Q}_{\ell_1}, \mathbb{F}_p(i)) \oplus H^2(\mathbb{Q}_p, \mathbb{F}_p(i))$$

has cokernel of dimension 1, since $H^3_{(c)}(\mathbb{Z}[1/Np], \mathbb{F}_p(1)) \cong \mathbb{F}_p$ (the target of global duality pairings). By the theory of the Brauer group (see e.g. [Poo17, Thm. 1.5.36]), we know that the map is injective with image consisting of the subspace summing to zero under the isomorphisms $H^2(\mathbb{Q}_q, \mathbb{F}_p(1)) \cong \mathbb{F}_p$ for $q = \ell_0, \ell_1, p$. Therefore its projection to any two summands, such as those in the lemma, is injective. □

We conclude this section with several conditions that are equivalent to (4) in Assumption 1.3.2. This assumption states that the Hecke algebra $\mathbb{T}_{\ell_0}$, which captures the Hecke eigensystems all of the weight 2 level $\Gamma_0(\ell_0)$ modular forms congruent to an Eisenstein series (see §2.1), is as small as possible given Mazur's result that there exists some cusp form congruent to an Eisenstein series. Note that this proposition is proven in [WWE20, Thm. 1.2.1].

Proposition 3.2.9 (Conditions equivalent to item (4) in Assumption 1.3.2)**.** *Assume that $\ell_0 \equiv 1 \pmod{p}$ and $\ell_1 \not\equiv \pm 1 \pmod{p}$. The following are equivalent.*

1. $\mathrm{rk}_{\mathbb{Z}_p} \mathbb{T}_{\ell_0} = 2$
2. $b_0 \cup c_0 \neq 0$ *in* $H^2(\mathbb{Z}[1/\ell_0 p], \mathbb{F}_p)$

(3) $b_0 \cup c_0 \neq 0$ *in* $H^2(\mathbb{Z}[1/Np], \mathbb{F}_p)$
(4) $b_0|_{\ell_0} \cup c_0|_{\ell_0} \neq 0$ *in* $H^2(\mathbb{Q}_{\ell_0}, \mathbb{F}_p)$
(5) $a_0 \cup c_0 \neq 0$ *in* $H^2(\mathbb{Z}[1/\ell_0 p], \mathbb{F}_p(-1))$
(6) $a_0 \cup c_0 \neq 0$ *in* $H^2(\mathbb{Z}[1/Np], \mathbb{F}_p(-1))$
(7) $a_0|_{\ell_0} \cup c_0|_{\ell_0} \neq 0$ *in* $H^2(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(-1))$
(8) $\{a_0|_{\ell_0}, \zeta \cup c_0|_{\ell_0}\}$ *is a basis for* $H^1(\mathbb{Q}_{\ell_0}, \mathbb{F}_p)$*, for any non-zero* $\zeta \in H^0(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(1))$*.*
(9) $\{b_0|_{\ell_0}, \zeta' \cup c_0|_{\ell_0}\}$ *is a basis for* $H^1(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(1))$*, for any non-zero* $\zeta' \in H^0(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(2))$*.*

Proof. The equivalence of (1), (2), and (5) is the content of [WWE20, Thm. 1.2.1]. Because $\ell_1 \not\equiv \pm 1 \pmod p$, for $i = -1, 0$, we have $H^2(\mathbb{Q}_{\ell_1}, \mathbb{F}_p(i)) = 0$. Then Lemma 3.2.8 supplies the equivalences of (2) with (3) and (4), and (5) with (6) and (7). The equivalence of (7), (8), and (9) follows from Lemma 3.2.6 and the fact, visible in [WWE20, Lem. 12.1.3], that $a_0 \cup \zeta = b_0$ for some non-zero $\zeta \in H^0(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(1))$. □

4. An explicit first-order deformation

We construct an irreducible first-order pseudodeformation $D_1 : G_{\mathbb{Q},Np} \to \mathbb{F}_p[\epsilon]/(\epsilon^2)$ of $\bar{D} : G_{\mathbb{Q},Np} \to \mathbb{F}_p$ that satisfies the unramified-or-Steinberg (US_N) property. This is a precursor to the constructions at second order that will be needed to prove the main technical result (Proposition 6.4.1).

4.1. 1-reducible GMAs and n-th order pseudodeformations.

When F is a field, write $F[\epsilon_n]$ for the F-algebra $F[\epsilon]/(\epsilon^{n+1})$. For $m < n$, we think of $F[\epsilon_m]$ as an $F[\epsilon_n]$-algebra via the natural quotient map $F[\epsilon_n] \twoheadrightarrow F[\epsilon_m]$. Given some algebraic object X over F, we call a deformation of X to $F[\epsilon_n]$ an *n-th order deformation of X*.

4.1.1. *1-reducible GMAs.* We introduce 1-reducible GMAs as a way to model truncations of a DVR-valued representations in a way that is "lattice-independent". To justify this, consider the following example.

Example 4.1.1. Let F be a field, G be a group, and $\rho : G \to \mathrm{GL}_2(F[\![x]\!])$ be a function that can be written as

$$\rho(g) = \begin{pmatrix} a(g) & xb(g) \\ c(g) & d(g) \end{pmatrix}$$

for some functions $a, b, c, d : G \to F[\![x]\!]$. Suppose we want to check that ρ is a homomorphism. Equivalently, we can check this in stages labeled by natural numbers n: at each stage n, check that $\rho \pmod{x^n}$ is a homomorphism. This amounts to checking some equations involving the functions a, b, c, and d, for instance

$$a(gg') \equiv a(g)a(g') + xb(g)c(g') \pmod{x^n}.$$

Note that this equation and the related equations for $b(gg')$ and $d(gg')$ only involve b and c modulo x^{n-1}. At stage n, only the equation for $c(gg')$ involves c modulo x^n.

On the other hand, another way to check that ρ is a homomorphism is to consider the conjugate $\rho' = \left(\begin{smallmatrix} x^{-1} & 0 \\ 0 & 1 \end{smallmatrix}\right)\rho\left(\begin{smallmatrix} x & 0 \\ 0 & 1 \end{smallmatrix}\right)$—that is

$$\rho'(g) = \begin{pmatrix} a(g) & b(g) \\ xc(g) & d(g) \end{pmatrix}$$

—and check that ρ' is a homomorphism. Again we can check this in stages, and this will involve the very same set of equations as for ρ, but in a different order. For instance, at stage n for ρ', the equation for $b(gg')$ will involve b modulo x^n.

In the example, if ρ is a homomorphism, then ρ and ρ' can be thought of as two different $F[\![x]\!]$-lattices in the same $F(\!(x)\!)$-representation. One can think of 1-reducible GMAs as a tool for studying this kind of problem in a way that does not favor one lattice over the other, and where one considers the minimal set of equations at each stage. This tool is especially well-suited to studying pseudorepresentations (note that ρ and ρ' have the same trace and determinant, and that the trace and determinant of ρ modulo x^n only involve b and c modulo x^{n-1}).

Definition 4.1.2. The 1-reducible GMA over $\mathbb{F}_p[\epsilon_n]$ is the GMA E_n given by

$$E_n = \begin{pmatrix} \mathbb{F}_p[\epsilon_n] & \mathbb{F}_p[\epsilon_{n-1}] \\ \mathbb{F}_p[\epsilon_{n-1}] & \mathbb{F}_p[\epsilon_n] \end{pmatrix}$$

with the multiplication map

$$m : \mathbb{F}_p[\epsilon_{n-1}] \otimes_{\mathbb{F}_p[\epsilon_n]} \mathbb{F}_p[\epsilon_{n-1}] \to \mathbb{F}_p[\epsilon_n]$$

given by the composition

$$\mathbb{F}_p[\epsilon_{n-1}] \otimes_{\mathbb{F}_p[\epsilon_n]} \mathbb{F}_p[\epsilon_{n-1}] \xrightarrow{b\otimes c \mapsto bc} \mathbb{F}_p[\epsilon_{n-1}] \xrightarrow{x \mapsto \epsilon x} \mathbb{F}_p[\epsilon_n].$$

The image of the multiplication map m is $\epsilon\mathbb{F}_p[\epsilon_n]$. In particular, if $\rho : G \to E_n^\times$ is a Cayley–Hamilton representation such that the induced map $\mathbb{F}_p[\![G]\!] \to E_n$ is surjective, then the reducibility ideal of ρ is $\epsilon\mathbb{F}_p[\epsilon_n]$.

Remark 4.1.3. The following relationship between 1-reducible GMAs and their induced pseudorepresentations plays an especially important role in this paper: a representation of a group G valued in E_n induces a $\mathbb{F}_p[\epsilon_n]$-valued pseudorepresentation of G, and we need not concern ourselves over whether this pseudorepresentation comes from a representation of G valued in $\mathrm{GL}_2(\mathbb{F}_p[\epsilon_n])$. Indeed, in some cases, it may not.

Remark 4.1.4. There is also a natural notion of *k-reducible GMA* $E_{k,n}$ for $k = 2, \dots, n$, where $\mathbb{F}_p[\epsilon_{n-1}]$ is replaced by $\mathbb{F}_p[\epsilon_{n-k}]$ and that map $x \mapsto \epsilon x$ is replaced by $x \mapsto \epsilon^k x$. In this case, the reducibility ideal of a surjective Cayley–Hamilton representation $\mathbb{F}_p[\![G]\!] \to E_{k,n}$ is $\epsilon^k\mathbb{F}_p[\epsilon_n]$. This explains the naming convention—the 'k' in k-reducible refers to the exponent of the uniformizer in the reducibility ideal. We will not need this notion in this paper.

Example 4.1.5. For example, when $n = 1$, an element of the 1-reducible GMA E_1 over $\mathbb{F}_p[\epsilon_1]$ can be written uniquely as $\left(\begin{smallmatrix} \alpha_0+\epsilon\alpha_1 & \beta \\ \gamma & \delta_0+\epsilon\delta_1 \end{smallmatrix}\right)$ for $\alpha_i, \beta, \gamma, \delta_i \in \mathbb{F}_p$, and the multiplication is

$$\begin{pmatrix} \alpha_0 + \epsilon\alpha_1 & \beta \\ \gamma & \delta_0 + \epsilon\delta_1 \end{pmatrix} \begin{pmatrix} \alpha_0' + \epsilon\alpha_1' & \beta' \\ \gamma' & \delta_0' + \epsilon\delta_1' \end{pmatrix} =$$
$$\begin{pmatrix} \alpha_0\alpha_0' + \epsilon(\alpha_1\alpha_0' + \alpha_0\alpha_1' + \beta\gamma') & \alpha_0\beta' + \beta\delta_0' \\ \gamma\alpha_0' + \delta_0\gamma' & \delta_0\delta_0' + \epsilon(\delta_1\delta_0' + \delta_0\delta_1' + \beta'\gamma) \end{pmatrix}$$

Example 4.1.6. Let ρ and a, b, c, d, be as in Example 4.1.1 with $F = \mathbb{F}_p$ and with the variable x replaced by ϵ. Suppose that ρ is a homomorphism. Then, for every $n > 0$, the map

$$g \mapsto \begin{pmatrix} a(g) \pmod{\epsilon^n} & b(g) \pmod{\epsilon^{n-1}} \\ c(g) \pmod{\epsilon^{n-1}} & d(g) \pmod{\epsilon^n} \end{pmatrix}$$

gives a homomorphism $G \to E_n^\times$.

4.1.2. *Reduction of 1-reducible GMAs.* When $n \geq m$, the standard surjection $\mathbb{F}_p[\epsilon_n] \twoheadrightarrow \mathbb{F}_p[\epsilon_m]$, $\epsilon \mapsto \epsilon$, extends naturally to 1-reducible GMAs. We have a *reduction map*

$$r_{n,m} : E_n \twoheadrightarrow E_m,$$

simply reducing each of the coordinates under the usual surjections $\mathbb{F}_p[\epsilon_n] \to \mathbb{F}_p[\epsilon_m]$ and $\mathbb{F}_p[\epsilon_{n-1}] \twoheadrightarrow \mathbb{F}_p[\epsilon_{m-1}]$, which is a $\mathbb{F}_p[\epsilon_n]$-algebra homomorphism. We will especially apply the case

$$r_{2,1} : E_2 \twoheadrightarrow E_1. \tag{4.1.7}$$

The reduction map $r_{n,m}$ is distinct from the tensor reduction map

$$E_n \twoheadrightarrow E_n \otimes_{\mathbb{F}_p[\epsilon_n]} \mathbb{F}_p[\epsilon_m], \quad x \mapsto x \otimes 1,$$

which is also a ring homomorphism. As long as $n > m$, the latter has the form

$$\begin{pmatrix} \mathbb{F}_p[\epsilon_n] & \mathbb{F}_p[\epsilon_{n-1}] \\ \mathbb{F}_p[\epsilon_{n-1}] & \mathbb{F}_p[\epsilon_n] \end{pmatrix} \twoheadrightarrow \begin{pmatrix} \mathbb{F}_p[\epsilon_m] & \mathbb{F}_p[\epsilon_m] \\ \mathbb{F}_p[\epsilon_m] & \mathbb{F}_p[\epsilon_m] \end{pmatrix},$$

where the target is a GMA with cross-diagonal multiplication $b \otimes c \mapsto \epsilon bc$. Later, we will apply the factorization of the reduction map $r_{2,1} : E_2 \twoheadrightarrow E_1$ into

$$E_2 \twoheadrightarrow \begin{pmatrix} \mathbb{F}_p[\epsilon_m] & \mathbb{F}_p[\epsilon_m] \\ \mathbb{F}_p[\epsilon_m] & \mathbb{F}_p[\epsilon_m] \end{pmatrix} \twoheadrightarrow E_1, \tag{4.1.8}$$

where the leftmost map is the tensor reduction map for $(n, m) = (2, 1)$, and the rightmost map is reduction modulo ϵ of the off-diagonal coordinates.

4.1.3. *Convenient mappings from 1-reducible GMAs.* We will have to work explicitly with the finite-flat property of Cayley–Hamilton representations of G_p over $\bar{D}$. We know from Proposition 2.2.6 that they must be upper-triangular, which makes it possible to apply the test of finite-flatness in Lemma 2.2.10 in a straightforward way. Now we contextualize it to the 1-reducible GMA, E_n over $\mathbb{F}_p[\epsilon_n]$, for $n \in \mathbb{Z}_{\geq 1}$.

Lemma 4.1.9. *There is an $\mathbb{F}_p[\epsilon_n]$-algebra embedding of the upper-triangular sub-$\mathbb{F}_p[\epsilon_n]$-GMA*

$$U_n := \left(\begin{smallmatrix} \mathbb{F}_p[\epsilon_n] & \mathbb{F}_p[\epsilon_{n-1}] \\ 0 & \mathbb{F}_p[\epsilon_n] \end{smallmatrix}\right) \subset E_n$$

into $M_2(\mathbb{F}_p[\epsilon_n])$ given by

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mapsto \begin{pmatrix} a & \epsilon b \\ 0 & d \end{pmatrix},$$

where the map on the upper right coordinate denotes the natural multiplication-by-ϵ map, written $\cdot\epsilon : \mathbb{F}_p[\epsilon_{n-1}] \to \mathbb{F}_p[\epsilon_n]$.

Proof. The map is clearly a morphism of $\mathbb{F}_p[\epsilon_n]$-modules, so it suffices to show that it respects the multiplication. This is checked easily. $\square$

On the other hand, we can realize some (but not all) of E_n within a matrix algebra by reducing modulo ϵ^n to $\mathbb{F}_p[\epsilon_{n-1}]$.

Lemma 4.1.10. *There is an $\mathbb{F}_p[\epsilon_n]$-algebra homomorphism from E_n to $M_2(\mathbb{F}_p[\epsilon_{n-1}])$ given by*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} \bar{a} & b \\ \epsilon c & \bar{d} \end{pmatrix},$$

where $\bar{a}, \bar{d} \in \mathbb{F}_p[\epsilon_{n-1}]$ indicates reduction modulo ϵ^n.

4.2. **The cochain $a^{(1)}$.** Our goal is to produce a first-order 1-reducible GMA representation $\rho_1 : G_{\mathbb{Q},Np} \to E_1^\times$ deforming $\omega \oplus 1$. We start by defining a cochain $a^{(1)} : G_{\mathbb{Q},Np} \to \mathbb{F}_p$ that will be used in the definition of ρ_1.

Recall the cocycles $b^{(1)}$, $c^{(1)}$, a_0 and a_p, and the cochain $x_{c^{(1)}}$ specified in Definition 3.1.1. The cohomology classes of $b^{(1)}$ and $c^{(1)}$ are b_1 and c_0, respectively.

Lemma 4.2.1. *There is a unique cochain $a^{(1)} \in C^1(\mathbb{Z}[1/Np], \mathbb{F}_p)$ satisfying the following three properties:*

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

(2) $(a^{(1)} - b^{(1)} \smile x_{c^{(1)}})|_{I_p} = 0$ in $H^1(\mathbb{Q}_p^{\mathrm{nr}}, \mathbb{F}_p)$, and

(3) the class of $a^{(1)}|_{\ell_0}$ in $H^1(\mathbb{Q}_{\ell_0}, \mathbb{F}_p)$ is on the line spanned by $\zeta \cup c_0|_{\ell_0}$ for any (equivalently, all) non-trivial $\zeta \in \mu_p(\mathbb{Q}_{\ell_0}) \cong H^0(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(1))$.

Moreover, $a^{(1)}|_{\ell_0}$ is a cocycle, $a^{(1)}|_{\ell_1}$ is an unramified cocycle, and the definition of $a^{(1)}$ depends only on the pinning data of Definition 1.7.1.

Proof. Since $b_1 \cup c_0 = 0$ by Lemma 3.2.1, we know there is a cochain $g \in C^1(\mathbb{Z}[1/Np], \mathbb{F}_p)$ such that $-dg = b^{(1)} \smile c^{(1)}$. The set of such g is a torsor for $Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p)$, which is generated by a_0 and a_p.

For any $-g$ whose coboundary is $b^{(1)} \smile c^{(1)}$, we have

$$-dg|_p = b^{(1)}|_p \smile c^{(1)}|_p = b^{(1)}|_p \smile dx_{c^{(1)}} = -d(b^{(1)}|_p \smile x_{c^{(1)}})$$

Hence $(g - b^{(1)}|_p \smile x_{c^{(1)}})|_p$ is a cocycle. Since $H^1(\mathbb{Q}_p, \mathbb{F}_p)$ is generated by its unramified subgroup $H^1_{\mathrm{un}}(\mathbb{Q}_p, \mathbb{F}_p)$ together with $a_p|_p$, we have

$$(g - b^{(1)}|_p \smile x_{c^{(1)}})|_p \equiv y a_p|_p \pmod{H^1_{\mathrm{un}}(\mathbb{Q}_p, \mathbb{F}_p)}$$

for a unique $y \in \mathbb{F}_p$. Replacing g by $g - ya_p$, we see that the set of g satisfying (1) and (2) is a non-empty torsor for $H^1(\mathbb{Z}[1/N], \mathbb{F}_p)$ (which is spanned by a_0).

By Lemma 3.2.1, the homomorphism $b^{(1)}|_{\ell_0} : G_{\ell_0} \to \mathbb{F}_p(1)$ vanishes. Hence for any g satisfying (1) and (2), we have

$$-dg|_{\ell_0} = b^{(1)}|_{\ell_0} \smile c^{(1)}|_{\ell_0} = 0,$$

so $g|_{\ell_0}$ is a cocycle. Since we assume that the equivalent conditions of Proposition 3.2.9 are true, the set $\{a_0|_{\ell_0}, c_0|_{\ell_0}\}$ is a basis for $H^1(\mathbb{Q}_{\ell_0}, \mathbb{F}_p)$. Hence there is a unique $\gamma \in \mathbb{F}_p$ such that $(g - \gamma a_0)|_{\ell_0}$ is in the line spanned by $c_0|_{\ell_0}$, and we define $a^{(1)} = g - \gamma a_0$ for this γ.

Finally, since $c^{(1)}|_{\ell_1} = 0$, condition (1) implies that $a^{(1)}|_{\ell_1}$ is a cocycle. In particular, $a^{(1)}|_{\ell_1}$ is unramified: because $p \nmid \ell_1(\ell_1 - 1)$, by local class field theory, any homomorphism from G_{ℓ_1} to $\mathbb{F}_p$ is unramified. □

Condition (3) in Lemma 4.2.1 provides the invariant α, which we now define.

Definition 4.2.2. Let $\alpha \in \mathbb{F}_p(1)$ be the unique element such that

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

Observe that α depends only on the pinning data of Definition 1.7.1.

4.3. **An irreducible first-order deformation.** We now produce a first-order 1-reducible GMA representation $\rho_1 : G_{\mathbb{Q},Np} \to E_1^\times$ deforming $\omega \oplus 1$ and satisfying the unramified-or-Steinberg condition US_N of Definition 2.2.13. The construction uses the cocycles $b^{(1)}$ and $c^{(1)}$ fixed in Definition 3.1.1 and the cochain $a^{(1)}$ defined in Lemma 4.2.1, together with the cochain $d^{(1)}$ defined by

$$d^{(1)} = b^{(1)}c^{(1)} - a^{(1)}.$$

Note that, since $-d(b^{(1)}c^{(1)}) = b^{(1)} \smile c^{(1)} + c^{(1)} \smile b^{(1)}$, we have

$$-dd^{(1)} = c^{(1)} \smile b^{(1)}. \tag{4.3.1}$$

Lemma 4.3.2. *Let E_1 be the 1-reducible GMA over $\mathbb{F}_p[\epsilon_1]$. Let $\rho_1 : G_{\mathbb{Q},S} \to E_1^\times$ be the function given in coordinates by*

$$\rho_1 = \begin{pmatrix} \omega(1 + a^{(1)}\epsilon) & b^{(1)} \\ \omega c^{(1)} & 1 + d^{(1)}\epsilon \end{pmatrix}. \tag{4.3.3}$$

Then ρ_1 is a homomorphism that is US_N. In particular, the associated pseudorepresentation

$$D_1 := \psi(\rho_1),\ \mathrm{Tr}_{D_1} = \omega + 1 + \epsilon(b^{(1)}c^{(1)} + (\omega - 1)a^{(1)}) : G_{\mathbb{Q},S} \to \mathbb{F}_p[\epsilon_1]$$

is US_N, and it induces a surjective homomorphism $\varphi_{D_1} : R \to \mathbb{F}_p[\epsilon_1]$.

Proof. We check the conditions one by one, recalling that the US_N condition entails a condition upon restriction to the decomposition group at every prime dividing Np.

Homomorphism: The homomorphism condition on ρ_1 can readily be checked to be equivalent to the following equalities of 2-coboundaries: $db^{(1)} = 0$, $dc^{(1)} = 0$, $-da^{(1)} = b^{(1)} \smile c^{(1)}$ and $-dd^{(1)} = c^{(1)} \smile b^{(1)}$. The first three equations hold by definition, and the last by (4.3.1).

Finite-flat at p: Recall the element $x_{c^{(1)}} \in \mathbb{F}_p(-1)$ of Definition 3.1.1 that satisfies $dx_{c^{(1)}} = c^{(1)}|_p$. Conjugating ρ_1 by $\left(\begin{smallmatrix} 1 & 0 \\ -x_{c^{(1)}} & 1 \end{smallmatrix}\right)$ we find that

$$\mathrm{ad}(\left(\begin{smallmatrix} 1 & 0 \\ -x_{c^{(1)}} & 1 \end{smallmatrix}\right))\rho_1|_p = \begin{pmatrix} \omega(1 + (a^{(1)}|_p - b^{(1)}|_p \smile x_{c^{(1)}})\epsilon) & b^{(1)}|_p \\ 0 & 1 - (a^{(1)}|_p - b_1|_p \smile x_{c^{(1)}})\epsilon \end{pmatrix}$$

Since $a^{(1)}|_p - b^{(1)}|_p \smile x_{c^{(1)}}|_p$ is an unramified element of $Z^1(\mathbb{Q}_p, \mathbb{F}_p)$ and $b^{(1)}$ induces a finite-flat extension of $\mathbb{F}_p$ by $\mathbb{F}_p(1)$ by Lemma 2.2.8, $\rho_1|_p$ is finite-flat by Lemmas 2.2.10 and 4.1.9.

Unramified-or-Steinberg at ℓ_0: Let $\sigma, \tau \in G_{\ell_0}$. Using the facts that $\omega|_{\ell_0} = 1$ and $b^{(1)}|_{\ell_0} = 0$, it follows that

$$(\rho_1(\sigma) - \omega(\sigma))(\rho_1(\tau) - 1) = \begin{pmatrix} \epsilon a^{(1)}(\sigma) & 0 \\ c^{(1)}(\sigma) & \epsilon d^{(1)}(\sigma) \end{pmatrix} \cdot \begin{pmatrix} \epsilon a^{(1)}(\tau) & 0 \\ c^{(1)}(\tau) & \epsilon d^{(1)}(\tau) \end{pmatrix} = 0$$

Unramified-or-Steinberg at ℓ_1: Let $\sigma, \tau \in G_{\ell_1}$. Using the fact that $c^{(1)}|_{\ell_1} = 0$, we find that $(\rho_1(\sigma) - \omega(\sigma))(\rho_1(\tau) - 1)$ is equal to

$$\begin{pmatrix} \epsilon\omega(\sigma)a^{(1)}(\sigma) & b^{(1)}(\sigma) \\ 0 & 1 - \omega(\sigma) + \epsilon d^{(1)}(\sigma) \end{pmatrix} \cdot \begin{pmatrix} \omega(\tau) - 1 + \epsilon\omega(\tau)a^{(1)}(\tau) & b^{(1)}(\tau) \\ 0 & \epsilon d^{(1)}(\tau) \end{pmatrix}$$
$$= \begin{pmatrix} \epsilon a^{(1)}(\sigma)(\omega(\tau) - 1) & 0 \\ 0 & \epsilon(1 - \omega(\sigma))d^{(1)}(\tau) \end{pmatrix}.$$

If $\sigma \in I_{\ell_1}$, then $a^{(1)}(\sigma) = 0$ and $\omega(\sigma) = 1$, so this is zero. If, on the other hand, $\tau \in I_{\ell_1}$, then $d^{(1)}(\tau) = 0$ and $\omega(\tau) = 1$, so this is zero.

φ_{D_1} **is surjective:** We have homomorphisms $b^{(1)}, c^{(1)} : G_{\mathbb{Q}(\zeta_p)} \to \mathbb{F}_p$ that are not scalar multiples of each other. Therefore there exists $\sigma \in G_{\mathbb{Q}(\zeta_p)}$ such that $b^{(1)}(\sigma) \neq 0$ and $c^{(1)}(\sigma) \neq 0$. Then we observe that $\mathrm{Tr}_{D_1}(\sigma) - 2 = \epsilon b^{(1)}(\sigma)c^{(1)}(\sigma)$, so ϵ is in the image of φ_{D_1}. □

Note that ρ_1, D_1 and the homomorphism $R \to \mathbb{F}_p[\epsilon_1]$ depend only on the pinning data of Definition 1.7.1. This is clear since $a^{(1)}$, $b^{(1)}$, $c^{(1)}$, and $d^{(1)}$ only depend on this data.

4.4. **Relation to the universal case.** Recall the universal US_N Cayley–Hamilton representation (ρ_N, E, D_E) from Definition 2.2.14. By the universal property, the representation ρ_1 of Lemma 4.3.2 induces a homomorphism

$$E \otimes_R \mathbb{F}_p[\epsilon_1] \to E_1,$$

of Cayley–Hamilton $\mathbb{F}_p[\epsilon_1]$-algebras. We can assume the GMA structure on E to be compatible with this homomorphism, in the following sense.

Proposition 4.4.1. *There exists a choice of R-GMA structure on E such that*

(1) $E \to E_1$ is a map of GMAs

(2) The elements

$$\begin{pmatrix} 0 & b_{\gamma_0} \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & b_{\gamma_1} \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ c_{\gamma_0} & 0 \end{pmatrix}$$

of E with respect to this GMA structure (as in Definition 2.2.14) map to the elements

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

of E_1, respectively.

Proof. Apply the idempotent lifting lemma of [WWE18, Lem. 5.6.8]. □

We choose the GMA structure on E such that the conditions (1) and (2) are satisfied. Although there may be many such choices, any of them will suffice for our purposes. Note that the conditions (1) and (2) are determined by the pinning data (Definition 1.7.1).

5. Computation of the pseudodeformation ring R/pR

Recall from Definition 2.2.14 that R denotes the pseudodeformation ring of $\omega \oplus 1$ with the US_N condition. In this section, we determine a presentation for the local $\mathbb{F}_p$-algebra R/pR. This will give us a way to distinguish between the cases $\mathrm{rk}_{\mathbb{Z}_p} \mathbb{T}_N = 3$ and $\mathrm{rk}_{\mathbb{Z}_p} \mathbb{T} > 3$, keeping in mind that we have a surjection $R \twoheadrightarrow \mathbb{T}$ from Proposition 2.2.15. As always, Assumption 1.3.2 is in force.

In addition to the notation, such as J^{red}, $J^{\min}$, B and C, set up in §2, we use the following:

- Let $\bar{R} := R/pR$, for convenience.
- If $I \subset R$ is an ideal, let $\bar{I} \subset \bar{R}$ denotes its image in $\bar{R}$. We warn the reader that the natural surjection $I/pI \to \bar{I}$ may not be an isomorphism.
- Let $\mathfrak{m} \subset R$ be the maximal ideal. Notice that $\mathfrak{m} = (J^{\min}, p)$ and that $\bar{\mathfrak{m}} \subset \bar{R}$ is also maximal.

- For a Noetherian local $\mathbb{Z}_p$-algebra $(A, \mathfrak{n})$, let $\mathfrak{t}_A$, the *tangent space of* A, be the set of local ring homomorphisms $\mathrm{Hom}(A, \mathbb{F}_p[\epsilon]/(\epsilon^2))$, which is an $\mathbb{F}_p$-vector space. The dual vector space $\mathfrak{t}_A^*$ is identified with $\mathfrak{n}/(\mathfrak{n}^2, p)$, and called this *cotangent space* of A.[3] It is naturally isomorphic to the cotangent space of $\bar{A} := A/pA$.

5.1. **The tangent space of R.** In this section, we compute the tangent space of R. In order to do this, we first recall Bellaïche's computation of the tangent space of the unrestricted deformation ring $R_{\bar{D}}$ [Bel12].

Let $J_{\bar{D}}^{\mathrm{red}} \subset R_{\bar{D}}$ denote the reducibility ideal and $R_{\bar{D}}^{\mathrm{red}} = R_{\bar{D}}/J_{\bar{D}}^{\mathrm{red}}$, and let $E_{\bar{D}}^u = \left(\begin{smallmatrix} R_{\bar{D}} & B_{\bar{D}} \\ C_{\bar{D}} & R_{\bar{D}} \end{smallmatrix}\right)$ be the $R_{\bar{D}}$-GMA structure on $E_{\bar{D}}^u$. On the other hand, let $\mathfrak{t}_{R_{\bar{D}}}^{\mathrm{irr}}$ be the cokernel of the natural map $\mathfrak{t}_{R_{\bar{D}}^{\mathrm{red}}} \to \mathfrak{t}_{R_{\bar{D}}}$; define $\mathfrak{t}_R^{\mathrm{irr}}$ analogously as the cokernel of $\mathfrak{t}_{R^{\mathrm{red}}} \to \mathfrak{t}_R$. We will address these tangent spaces mainly through their dual, which is the irreducible subspace of the cotangent space,

$$(\mathfrak{t}_R^{\mathrm{irr}})^* \subset \mathfrak{t}_R^*, \qquad (\mathfrak{t}_{R_{\bar{D}}}^{\mathrm{irr}})^* \subset \mathfrak{t}_{R_{\bar{D}}}^*.$$

The following equivalent expression of $\mathfrak{t}_R^{\mathrm{irr}}$ will be used pervasively.

Lemma 5.1.1. *The natural maps*

$$\bar{J}^{\mathrm{red}}/\bar{\mathfrak{m}}\bar{J}^{\mathrm{red}} \to \mathfrak{t}_R^*, \qquad \bar{J}_{\bar{D}}^{\mathrm{red}}/\bar{\mathfrak{m}}_{\bar{D}}\bar{J}_{\bar{D}}^{\mathrm{red}} \to \mathfrak{t}_{R_{\bar{D}}}^*$$

are injective with image equal to $(\mathfrak{t}_R^{\mathrm{irr}})^*$ *and* $(\mathfrak{t}_{R_{\bar{D}}}^{\mathrm{irr}})^*$*, respectively. In other words,*

$$\bar{J}^{\mathrm{red}}/\bar{\mathfrak{m}}\bar{J}^{\mathrm{red}} \cong (\mathfrak{t}_R^{\mathrm{irr}})^* \quad \textit{and} \quad \bar{J}_{\bar{D}}^{\mathrm{red}}/\bar{\mathfrak{m}}_{\bar{D}}\bar{J}_{\bar{D}}^{\mathrm{red}} \cong (\mathfrak{t}_{R_{\bar{D}}}^{\mathrm{irr}})^*.$$

According to Proposition 2.3.1, the GMA-multiplication map induces a surjective $R_{\bar{D}}$-module homomorphism

$$B_{\bar{D}} \otimes_{R_{\bar{D}}} C_{\bar{D}} \twoheadrightarrow J_{\bar{D}}^{\mathrm{red}}, \quad b \otimes c \mapsto b \cdot c$$

This induces a composite surjection

$$B_{\bar{D}}/\mathfrak{m}_{\bar{D}}B_{\bar{D}} \otimes_{\mathbb{F}_p} C_{\bar{D}}/\mathfrak{m}_{\bar{D}}C_{\bar{D}} \twoheadrightarrow J_{\bar{D}}^{\mathrm{red}}/\mathfrak{m}_{\bar{D}}J_{\bar{D}}^{\mathrm{red}} \twoheadrightarrow (\mathfrak{t}_{R_{\bar{D}}}^{\mathrm{irr}})^* \tag{5.1.2}$$

of $\mathbb{F}_p$-vector spaces. Bellaïche interprets this surjection in terms of cup products in Galois cohomology.

Proposition 5.1.3 (Bellaïche [Bel12, Theorem A and §4.1.1])**.** *there is an exact sequence*

(5.1.4)

$$0 \to \mathfrak{t}_{R_{\bar{D}}}^{\mathrm{irr}} \xrightarrow{\iota} H^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1)) \otimes_{\mathbb{F}_p} H^1(\mathbb{Z}[1/Np], \mathbb{F}_p(-1)) \xrightarrow{\cup} H^2(\mathbb{Z}[1/Np], \mathbb{F}_p).$$

where the final map is the cup product. Moreover, under natural identifications

(5.1.5)

$$B_{\bar{D}}/\mathfrak{m}_{\bar{D}}B_{\bar{D}} \cong (H^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1)))^*, \quad C_{\bar{D}}/\mathfrak{m}_{\bar{D}}C_{\bar{D}} \cong (H^1(\mathbb{Z}[1/Np], \mathbb{F}_p(-1)))^*,$$

the map ι *is identified with the dual of* (5.1.2).

Applying the proposition to our running assumptions $b_1 \cup c_0 = 0$ (see Lemma 3.2.1) and $b_0 \cup c_0 \neq 0$ (see Proposition 3.2.9), we have the following

Lemma 5.1.6. *There is an element of* $f \in B_{\bar{D}}/\mathfrak{m}_{\bar{D}}B_{\bar{D}} \otimes_{\mathbb{F}_p} C_{\bar{D}}/\mathfrak{m}_{\bar{D}}C_{\bar{D}}$ *satisfying*

(i) under the dualities (5.1.5), $f(b_0 \otimes c_0) \neq 0$ *and* $f(b_1 \otimes c_0) = 0$ *in* $\mathbb{F}_p$*, and*
(ii) f *maps to* 0 *under* (5.1.2).

[3] The spaces $\mathfrak{t}_A$ and $\mathfrak{t}_A^*$ might more accurately be called the mod-p (co)tangent space of $\mathrm{Spec}(A)$.

Proof. Since $b_0 \cup c_0 \neq 0$, it is not in the image of ι, so there is an element λ of the dual of $H^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1)) \otimes_{\mathbb{F}_p} H^1(\mathbb{Z}[1/Np], \mathbb{F}_p(-1))$ such that $\lambda(b_0 \otimes c_0) \neq 0$ and such that λ is zero on the image of ι. In particular, since $b_1 \cup c_0$ is zero, $b_1 \otimes c_0$ is in the image of ι and $\lambda(b_1 \otimes c_0) = 0$. Our identifications give an isomorphism between the dual of $H^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1)) \otimes_{\mathbb{F}_p} H^1(\mathbb{Z}[1/Np], \mathbb{F}_p(-1))$ and $B_{\bar{D}}/\mathfrak{m}_{\bar{D}}B_{\bar{D}} \otimes_{\mathbb{F}_p} C_{\bar{D}}/\mathfrak{m}_{\bar{D}}C_{\bar{D}}$, and we can take f to be the image of λ under this identification. □

Now we calculate the irreducible subspace of the cotangent space of R, as well as minimal sets of generators for $J^{\mathrm{red}} \subset R$ and $\bar{J}^{\mathrm{red}} \subset \bar{R}$.

Proposition 5.1.7. *The ideal $\bar{J}^{\mathrm{red}} \subset \bar{R}$ is principal, generated by the non-zero image of $b_{\gamma_1} \cdot c_{\gamma_0}$ under $R \twoheadrightarrow \bar{R}$. In particular, the image of $b_{\gamma_1}c_{\gamma_0}$ in $\mathfrak{t}_R^*$ generates the 1-dimensional subspace $(\mathfrak{t}_R^{\mathrm{irr}})^*$. In contrast, the ideal $J^{\mathrm{red}} \subset R$ is not principal, and is generated by $\{b_{\gamma_0}c_{\gamma_0}, b_{\gamma_1}c_{\gamma_0}\}$. Nonetheless, the image of $b_{\gamma_0}c_{\gamma_0}$ in $\mathfrak{t}_R^*$ vanishes.*

Proof. First, we claim that $b_{\gamma_0}c_{\gamma_0}$ and $b_{\gamma_1}c_{\gamma_0}$ generate J^{red}. By Nakayama's lemma, it suffices to show that $J^{\mathrm{red}}/\mathfrak{m}J^{\mathrm{red}}$ is generated by the image of $b_{\gamma_1} \cdot c_{\gamma_0}$ and $b_{\gamma_0} \cdot c_{\gamma_0} = 0$. This follows from the fact that $\{b_{\gamma_0}, b_{\gamma_1}\}$ generate B and $\{c_{\gamma_0}\}$ generates C, as recorded in Proposition 2.4.2.

Next, we claim that $b_{\gamma_1}c_{\gamma_0}$ generates $\bar{J}^{\mathrm{red}}$, which requires us to apply Lemma 5.1.6. Just as in (5.1.2), there is a similar map for J^{red} fitting into a commutative diagram

$$\begin{array}{ccc} B_{\bar{D}}/\mathfrak{m}_{\bar{D}}B_{\bar{D}} \otimes_{\mathbb{F}_p} C_{\bar{D}}/\mathfrak{m}_{\bar{D}}C_{\bar{D}} & \twoheadrightarrow & J_{\bar{D}}^{\mathrm{red}}/\mathfrak{m}_{\bar{D}}J_{\bar{D}}^{\mathrm{red}} \\ \downarrow & & \downarrow \\ B/\mathfrak{m}B \otimes_{\mathbb{F}_p} C/\mathfrak{m}C & \twoheadrightarrow & J^{\mathrm{red}}/\mathfrak{m}J^{\mathrm{red}} \end{array}$$

Under the interpretation of $B_{\bar{D}}/\mathfrak{m}_{\bar{D}}B_{\bar{D}}$ and $C_{\bar{D}}/\mathfrak{m}_{\bar{D}}C_{\bar{D}}$ as dual vector spaces found in (5.1.5), the leftmost vertical arrow is the dual of the inclusion of subspaces of the Galois cohomology groups. By [WWE21, Lem. 3.10.3], we can identify these subspaces: the basis $\{b_{\gamma_0}, b_{\gamma_1}\}$ of $B/\mathfrak{m}B$ is dual to the basis $\{b_0, b_1\}$ of Galois cohomology; and $\{c_{\gamma_0}\}$ is a basis of $C/\mathfrak{m}C$, dual to $\{c_0\}$.

Now consider the element $f \in B_{\bar{D}}/\mathfrak{m}_{\bar{D}}B_{\bar{D}} \otimes_{\mathbb{F}_p} C_{\bar{D}}/\mathfrak{m}_{\bar{D}}C_{\bar{D}}$ from Lemma 5.1.6. The image of f in $B/\mathfrak{m}B \otimes_{\mathbb{F}_p} C/\mathfrak{m}C$ is of the form $(xb_{\gamma_0} + yb_{\gamma_1}) \otimes c_{\gamma_0}$ for some $x, y \in \mathbb{F}_p$. Since $f(b_0 \otimes c_0) \neq 0$ and $f(b_1 \otimes c_0) = 0$ it follows that $x \neq 0$ and $y = 0$. Then the commutativity of the diagram and the fact that f maps to 0 in $(\mathfrak{t}_{\bar{D}}^{\mathrm{irr}})^* \subset \mathfrak{t}_{\bar{D}}^*$ imply

$$b_{\gamma_0} \cdot c_{\gamma_0} = -x^{-1}yb_{\gamma_1} \cdot c_{\gamma_0} = 0$$

in $\mathfrak{t}_R^*$. In particular, the image of $b_{\gamma_1} \cdot c_{\gamma_0}$ in $\bar{R}$ generates $\bar{J}^{\mathrm{red}}$, due to Lemma 5.1.1 and Nakayama's lemma.

There exists an irreducible first-order pseudodeformation D_1 of $\psi(\omega \oplus 1)$ constructed in Lemma 4.3.2, which is evidence that $\mathfrak{t}_R^{\mathrm{irr}} \neq 0$.

In light of Lemma 5.1.1, the conclusions about $\bar{J}^{\mathrm{red}}$ imply the conclusions about $(\mathfrak{t}_R^{\mathrm{irr}})^*$.

It remains to show that J^{red} is not principal. If it were principal, then because the image of $b_{\gamma_1}c_{\gamma_0}$ in $\bar{J}^{\mathrm{red}}$ is a generator, $b_{\gamma_1}c_{\gamma_0} \in J^{\mathrm{red}}$ would be a generator. But $b_{\gamma_1}c_{\gamma_0}$ vanishes under $R \twoheadrightarrow R_{\ell_0}$ because the Galois pseudorepresentations parameterized by R_{ℓ_0} are unramified at ℓ_1 (hence b_{γ_1} maps to zero in the global level ℓ_0 R_{ℓ_0}-GMA).

This would imply that the pseudorepresentation supported by R_{ℓ_0} is reducible, because its reducibility ideal has a single generator which is zero. But this is known not to be the case: the Galois representation supported by the level $\Gamma_0(\ell_0)$ cusp form f of Assumption 1.3.2(4) is irreducible. □

Now we can calculate the whole tangent space of R.

Proposition 5.1.8. *The $\mathbb{F}_p$-dimension of $\mathfrak{t}_R$ is 2, with a basis given by the two maps $D^{\mathrm{red}}, D_1 : R \to \mathbb{F}_p[\epsilon]/(\epsilon^2)$ specified in Lemma 2.3.2 and Lemma 4.3.2, respectively. More precisely:*

1. *The subspace $\mathfrak{t}_{R^{\mathrm{red}}} \subset \mathfrak{t}_R$ is 1-dimensional and spanned by D^{red}.*
2. *The space $\mathfrak{t}_R^{\mathrm{irr}}$ is one-dimensional and the element D_1 of $\mathfrak{t}_R$ maps to a generator of it under the natural surjection $\mathfrak{t}_R \twoheadrightarrow \mathfrak{t}_R^{\mathrm{irr}}$.*

Proof. Since there is an exact sequence

$$0 \to \mathfrak{t}_{R^{\mathrm{red}}} \to \mathfrak{t}_R \to \mathfrak{t}_R^{\mathrm{irr}} \to 0$$

it is enough to show (1) and (2). Part (1) follows from the isomorphisms

$$R^{\mathrm{red}}/pR^{\mathrm{red}} \cong \mathbb{F}_p[y]/(y^2)$$

of Lemma 2.3.2.

Part (2) follows from Proposition 5.1.7 (see the end of its proof) along with the fact that D_1 is irreducible, which is inherent to its construction in Lemma 4.3.2. □

5.2. **The R-module C is torsion.** In Proposition 2.4.2, we saw that C is a cyclic R-module, generated by the element $c_{\gamma_0} \in C$. An important consequence of our running assumption $a_0 \cup c_0 \neq 0$ (see Proposition 3.2.9) is that C is not a free R-module.

Proposition 5.2.1. *The R-module C is cyclic and not free. In fact, the annihilator of $C \otimes_{R,D^{\mathrm{red}}} \mathbb{F}_p[\epsilon_1]$ is ϵ (here the tensor product is with respect to the ring map $D^{\mathrm{red}} : R \to \mathbb{F}_p[\epsilon_1]$ defined in Lemma 2.3.2).*

Proof. Because $BC = J^{\mathrm{red}}$ is non-zero, C is also non-zero.

Let $\bar{C} := C \otimes_{R,D^{\mathrm{red}}} \mathbb{F}_p[\epsilon_1]$. We will show that $\bar{C}$ is not a free $\mathbb{F}_p[\epsilon_1]$-module (in which case it must be isomorphic to $\mathbb{F}_p$), which implies that C is not free as an R-module. To set up a contradiction, assume that $\bar{C}$ is a free $\mathbb{F}_p[\epsilon_1]$-module; we will show that this contradicts the assumption $a_0 \cup c_0 \neq 0$.

We know by Nakayama's lemma and Proposition 2.4.2 that $\bar{C}$ is a cyclic $\mathbb{F}_p[\epsilon_1]$-module with generator c_{γ_0}. Because D^{red} is reducible, there is a quotient $\mathbb{F}_p[\epsilon_1]$-GMA of $E' = E \otimes_{R,D^{\mathrm{red}}} \mathbb{F}_p[\epsilon_1]$ of the form

$$\begin{pmatrix} \mathbb{F}_p[\epsilon_1] & \\ \bar{C} & \mathbb{F}_p[\epsilon_1] \end{pmatrix} \xrightarrow{\sim} \begin{pmatrix} \mathbb{F}_p[\epsilon_1] & \\ \mathbb{F}_p[\epsilon_1] & \mathbb{F}_p[\epsilon_1] \end{pmatrix} \subseteq M_2(\mathbb{F}_p[\epsilon_1])$$

(where we used c_{γ_0} as a generator of $\bar{C}$ to draw the isomorphism) receiving a homomorphism from $\mathbb{F}_p[\epsilon_1][G_{\mathbb{Q}}]$ of the form

$$\begin{pmatrix} \omega(1+\epsilon a_0) & 0 \\ \omega(c^{(1)} + \epsilon c^{(2)}) & 1 - \epsilon a_0 \end{pmatrix}.$$

The quotient map has kernel equal to the B-coordinate $B_{E'} \subset E'$, which is a two-sided ideal because $B_{E'} \cdot C_{E'} = 0$ (which expresses the reducibility of D^{red}).

In the coordinate expression, $c^{(1)}$ appears because we have made a choice of GMA coordinates of E compatible with $E \to E_1$ as in Proposition 4.4.1. The new coordinate $c^{(2)}$ also appears, and the conclusion of the proof applies its existence.

We have an equality of 2-$G_{\mathbb{Q},Np}$-cocycles valued in $\mathbb{F}_p(-1)$,

$$-dc^{(2)} = a_0 \smile c^{(1)} + c^{(1)} \smile (-a_0).$$

The right hand side is in the cohomology class of $2a_0 \cup c_0$. But our assumption $\mathrm{rk}_{\mathbb{Z}_p} \mathbb{T}_{\ell_0} = 2$ implies that $a_0 \cup c_0 \neq 0$ in $H^2(\mathbb{Z}[1/Np], \mathbb{F}_p(-1))$ by Proposition 3.2.9. Therefore such a $c^{(2)}$ cannot exist. □

5.3. **The ring $S := \bar{R}/\bar{\mathfrak{m}}^3$.** Note that the $\mathbb{F}_p$-dimension of $\bar{R}/\bar{\mathfrak{m}}^2$ is $1 + \dim_{\mathbb{F}_p}(\mathfrak{t}_R)$, which is 3 by Proposition 5.1.8. This implies the inequality $\dim_{\mathbb{F}_p} \bar{R} \geq 3$, with equality if and only if $\bar{\mathfrak{m}}^2 = 0$. By Nakayama's lemma, $\dim_{\mathbb{F}_p}(\bar{R}) = 3$ if and only if $\bar{\mathfrak{m}}^3 = \bar{\mathfrak{m}}^2$. Hence the key object to study is the ring $\bar{R}/\bar{\mathfrak{m}}^3$, which we shall denote by S.

Because S surjects onto $\bar{R}/\bar{\mathfrak{m}}^2$ and Proposition 5.1.8 describes the 2-dimensional cotangent space $\mathfrak{t}_R^* = \bar{\mathfrak{m}}/\bar{\mathfrak{m}}^2$, there are equivalences

$$\dim_{\mathbb{F}_p} S = 3 \iff \dim_{\mathbb{F}_p} \bar{R} = 3 \iff \bar{R} \cong S \cong \frac{\mathbb{F}_p[x,y]}{(x^2, xy, y^2)},$$

and Proposition 5.1.8 characterizes $\bar{R}$ completely in this case. Therefore, we are left to deal with the case that

$$\dim_{\mathbb{F}_p} S \geq 4.$$

This section is meant to characterize S in that case.

For an ideal I in R or $\bar{R}$, let $I_S \subset S$ denote its image in S. Note that $\dim_{\mathbb{F}_p} S = 3 + \dim_{\mathbb{F}_p}(\mathfrak{m}_S^2)$.

Proposition 5.3.1. *The inclusion of ideals $(J_S^{\mathrm{red}})^2 \subset \mathfrak{m}_S J_S^{\mathrm{red}}$ is an equality.*

Proof. Let $C_S := C \otimes_R S$, and likewise $B_S := B \otimes_R S$.

We claim that $\mathfrak{m}_S C_S \subset J_S^{\mathrm{red}} C_S$, which we will derive from Proposition 5.2.1. Proposition 5.2.1, translated into our current notation using S, states that the maximal ideal of S^{red} kills C_S^{red}. Lifting this result from S^{red}-modules to S-modules, we find that $\mathfrak{m}_S C_S \subset J_S^{\mathrm{red}} C_S$, which is the desired result.

We derive from the equality $\mathfrak{m}_S C_S = J_S^{\mathrm{red}} C_S$ that, for all $x \in \mathfrak{m}_S$, there exists some $z \in J_S^{\mathrm{red}}$ such that

$$xc_{\gamma_0} = zc_{\gamma_0}, \tag{5.3.2}$$

and that every element of $\mathfrak{m}_S C_S$ has this form because c_{γ_0} generates C_S. We apply this to the surjection of S-modules

$$C_S \otimes_S B_S \twoheadrightarrow J_S^{\mathrm{red}},$$

also using that $c_{\gamma_0} b_{\gamma_1}$ is a generator of the principal ideal J_S^{red} (Proposition 5.1.7). Namely, finding that every element of $\mathfrak{m}_S J_S^{\mathrm{red}} = \mathfrak{m}_S C_S B_S$ has the form

$$x(c_{\gamma_0} b_{\gamma_1} s) = (xc_{\gamma_0})(b_{\gamma_1} s) = z(c_{\gamma_0} b_{\gamma_1}) s \in (J_S^{\mathrm{red}})^2,$$

for some $s \in S$, and with x and z as in (5.3.2). □

Corollary 5.3.3. *Either $\dim_{\mathbb{F}_p} S = 3$ or $\dim_{\mathbb{F}_p} S = 4$. In general,*

$$\dim_{\mathbb{F}_p} S = \dim_{\mathbb{F}_p} J_S^{\mathrm{red}} + 2 = \dim_{\mathbb{F}_p} (J_S^{\mathrm{red}})^2 + 3.$$

Proof. Because $S^{\mathrm{red}} = S/J_S^{\mathrm{red}}$ is 2-dimensional, we have $\dim_{\mathbb{F}_p} S = 2 + \dim_{\mathbb{F}_p} J_S^{\mathrm{red}}$ in general.

Because $J_S^{\mathrm{red}} \subset \mathfrak{m}_S$ and $\mathfrak{m}_S^3 = 0$, we have a filtration

$$J_S^{\mathrm{red}} \supset \mathfrak{m}_S J_S^{\mathrm{red}} \supset \mathfrak{m}_S^2 J_S^{\mathrm{red}} = 0$$

graded by $\mathbb{F}_p$-vector spaces. The principality of J_S^{red} (Proposition 5.1.7) implies that

$$\dim_{\mathbb{F}_p} \frac{J_S^{\mathrm{red}}}{\mathfrak{m}_S J_S^{\mathrm{red}}} = 1.$$

The equality $\mathfrak{m}_S J_S^{\mathrm{red}} = (J_S^{\mathrm{red}})^2$ of Proposition 5.3.1 implies that $\dim_{\mathbb{F}_p} \mathfrak{m}_S J_S^{\mathrm{red}} \leq 1$. □

6. Galois-theoretic implications of $\dim_{\mathbb{F}_p} R/pR \geq 4$

Throughout this section, we assume that $\dim_{\mathbb{F}_p} R/pR \geq 4$ (or, equivalently, that $\dim_{\mathbb{F}_p}(S) = 4$, where $S = R/(p, \mathfrak{m}^3)$) and derive consequences for Galois cohomology. The main results are Lemma 6.2.9 and Proposition 6.4.1, which together essentially prove one direction of Theorem 1.4.3 from the introduction.

6.1. **A GMA over S when $\dim_{\mathbb{F}_p} S = 4$.** From now on, let y be the image of $b_{\gamma_1} \cdot c_{\gamma_0}$ in S, which generates the principal ideal $J_S^{\mathrm{red}} \subset S$. According to Corollary 5.3.3, the $\mathbb{F}_p$-dimension of J_S^{red} is 2. Since J_S^{red} is principal, its annihilator $\mathrm{Ann}_S(J_S^{\mathrm{red}})$ is also 2-dimensional. Consider the ring homomorphism

$$S \twoheadrightarrow \frac{S}{\mathrm{Ann}_S(J_S^{\mathrm{red}})} \cong \mathbb{F}_p[\epsilon_1], \tag{6.1.1}$$

where the isomorphism $S/\mathrm{Ann}_S(J_S^{\mathrm{red}}) \xrightarrow{\sim} \mathbb{F}_p[\epsilon_1]$ is determined by $y \mapsto \epsilon$. This is possible because y^2 spans $(J_S^{\mathrm{red}})^2 = \mathfrak{m}_S^2$, which is non-zero in S under the assumption that $\dim_{\mathbb{F}_p} S = 4$ (Corollary 5.3.3).

Definition 6.1.2. We set up the following coordinates for objects within S.

- We define a $\mathbb{F}_p[\epsilon_1]$-valued pseudorepresentation $D_y : G_{\mathbb{Q},Np} \to \mathbb{F}_p[\epsilon_1]$ by associating it to the local homomorphism

$$\varphi_{D_y} : R \twoheadrightarrow S \twoheadrightarrow \mathbb{F}_p[\epsilon_1]$$

  determined by the isomorphism $\frac{S}{\mathrm{Ann}_S(J_S^{\mathrm{red}})} \xrightarrow{\sim} \mathbb{F}_p[\epsilon_1]$ above.
- We also allow ourselves to identify J_S^{red} with $\mathbb{F}_p[\epsilon_1]$, as S-modules where $\mathbb{F}_p[\epsilon_1]$ has structure map φ_{D_y}, under the isomorphism

$$\mathbb{F}_p[\epsilon_1] \overset{(6.1.1)}{\xrightarrow{\sim}} \frac{S}{\mathrm{Ann}_S(J_S^{\mathrm{red}})} \xrightarrow{\sim} J_S^{\mathrm{red}},$$

  where the rightmost isomorphism is determined by $s \mapsto ys$.
- Since the image of $b_{\gamma_0} \cdot c_{\gamma_0}$ in S is in $\mathfrak{m}_S J_S^{\mathrm{red}} = y^2 S$ (Proposition 5.1.7), we see that there is a unique $\eta \in \mathbb{F}_p$ such that

$$b_{\gamma_0} \cdot c_{\gamma_0} = \eta y^2.$$

We call the map (6.1.1) and the following maps out of B_S and C_S, collectively, *coordinate maps.*

Lemma 6.1.3. *Assume that* $\dim_{\mathbb{F}_p} S = 4$. *There are surjective* S*-module homomorphisms*

$$B_S \twoheadrightarrow \mathbb{F}_p \oplus \mathbb{F}_p[\epsilon_1], \quad s_0 b_{\gamma_0} + s_1 b_{\gamma_1} \mapsto (\bar{s}_0, \varphi_{D_y}(s_1)),$$

where $\bar{s}_0 \in \mathbb{F}_p$ *is the image of* s_0 *under the augmentation* $S \to \mathbb{F}_p$, *and*

$$C_S \twoheadrightarrow \mathbb{F}_p[\epsilon_1], \quad s c_{\gamma_0} \mapsto \varphi_{D_y}(s).$$

Using these surjections $B_S \twoheadrightarrow \mathbb{F}_p \oplus \mathbb{F}_p[\epsilon_1]$ *and* $C_S \twoheadrightarrow \mathbb{F}_p[\epsilon_1]$ *and the identification* $J_S^{\mathrm{red}} = \mathbb{F}_p[\epsilon_1]$, *the GMA-multiplication map*

$$B_S \otimes_S C_S \to J_S^{\mathrm{red}}$$

induces the map

$$(\mathbb{F}_p \oplus \mathbb{F}_p[\epsilon_1]) \otimes_{\mathbb{F}_p[\epsilon_1]} \mathbb{F}_p[\epsilon_1] \to \mathbb{F}_p[\epsilon_1] \tag{6.1.4}$$

given by

$$(u, v) \otimes z \mapsto \eta\epsilon uz + vz.$$

Proof. The only coordinate map that does not obviously exist as defined is that of B_S: B_S is non-cyclic and generated by $\{b_{\gamma_0}, b_{\gamma_1}\}$, and we must show that any relation between the generators is sent by the coordinate map to 0. First, observe that any relation $g b_{\gamma_0} + h b_{\gamma_1} = 0 \in B_S$ (for $g, h \in S$) must have $g, h \in \mathfrak{m}_S$, since B_S is not cyclic. Therefore, no relation $g b_{\gamma_0} + h b_{\gamma_1}$ can possibly map to something non-zero under the coordinate map for B_S, since this would imply that

$$0 = g b_{\gamma_0} c_{\gamma_0} + h b_{\gamma_1} c_{\gamma_0} = g \eta y^2 + hy = hy \text{ in } J_S^{\mathrm{red}},$$

for some h such that $\varphi_{D_y}(h) \neq 0$, contradicting $\mathrm{Ann}_S(y) = \ker \varphi_{D_y}$. Consequently, the coordinate map for B_S is well defined.

It remains to verify that the square of surjections

$$\begin{array}{ccc} B_S \otimes_S C_S & \longrightarrow & J_S^{\mathrm{red}} \\ \downarrow & & \downarrow \\ (\mathbb{F}_p \oplus \mathbb{F}_p[\epsilon_1]) \otimes_{\mathbb{F}_p[\epsilon_1]} \mathbb{F}_p[\epsilon_1] & \longrightarrow & \mathbb{F}_p[\epsilon_1] \end{array}$$

commutes, which we can check on the generating set $\{b_{\gamma_0} \otimes c_{\gamma_0}, b_{\gamma_1} \otimes c_{\gamma_0}\}$ of $B_S \otimes_S C_S$.

The coordinates of $b_{\gamma_0} \otimes c_{\gamma_0}$ are $(1, 0) \otimes 1$, which maps to $\eta\epsilon \in \mathbb{F}_p[\epsilon_1]$; on the other hand, $b_{\gamma_0} c_{\gamma_0} \in J_S^{\mathrm{red}}$ has the form ηy^2 by definition of η, which also maps to $\eta\epsilon \in \mathbb{F}_p[\epsilon_1]$ under the coordinate map for J_S^{red}.

The coordinates of $b_{\gamma_1} \otimes c_{\gamma_0}$ are $(0, 1) \otimes 1$, which maps to $1 \in \mathbb{F}_p[\epsilon_1]$; on the other hand, $b_{\gamma_1} c_{\gamma_0} \in J_S^{\mathrm{red}}$ equals y, which also maps to $1 \in \mathbb{F}_p[\epsilon_1]$ under the coordinate map for J_S^{red}. □

Let E'_S denote the S-GMA

$$E'_S = \begin{pmatrix} S & \mathbb{F}_p \oplus \mathbb{F}_p[\epsilon_1] \\ \mathbb{F}_p[\epsilon_1] & S \end{pmatrix} \tag{6.1.5}$$

where $\mathbb{F}_p[\epsilon_1]$ is a S-module via the map $\varphi_{D_y} : S \to \mathbb{F}_p[\epsilon_1]$, and where the GMA-multiplication map is given by (6.1.4). By the lemma, the coordinate maps comprise a surjective morphism of S-GMAs

$$E \otimes_R S \twoheadrightarrow E'_S.$$

6.2. **The coordinates of a S-GMA valued Galois representation when $\dim_{\mathbb{F}_p} S = 4$.** Now consider the Cayley–Hamilton representation $\rho'_S : G_{\mathbb{Q},Np} \to (E'_S)^\times$ obtained as composition of the universal Cayley–Hamilton representation $\rho : G_{\mathbb{Q},Np} \to E^\times$ with $E \twoheadrightarrow E'_S$. We are interested in endowing it with coordinates and comparing these coordinates to the 1-reducible GMA representation $\rho_1 : G_{\mathbb{Q},Np} \to E_1^\times$ of (4.3.3).

To this end, the coordinates of E'_S suffice, modulo the need for complete coordinates for S, which we now supply. To introduce this definition, we point out that $\{D^{\mathrm{red}}, D_y\}$ is a basis of $\mathfrak{t}_R$ according to Proposition 5.1.8, because D^{red} is reducible, D_y is irreducible, and $\dim_{\mathbb{F}_p} \mathfrak{t}_R = 2$.

Definition 6.2.1. Let $x \in S$ denote a generator for $\mathrm{Ann}_S(J_S^{\mathrm{red}})$ whose image $\bar{x} \in \mathfrak{t}_R^* = \mathfrak{m}_S/\mathfrak{m}_S^2$ makes $\{\bar{x}, \bar{y}\} \subset \mathfrak{t}_R^*$ a dual basis to $\{D^{\mathrm{red}}, D_y\}$.

Here are the important properties of this choice of x; we also justify in this lemma that such a choice of x exists.

Lemma 6.2.2. *Assume $\dim_{\mathbb{F}_p} S = 4$. A choice of $x \in S$ as in Definition 6.2.1 induces a presentation of S,*

$$\frac{\mathbb{F}_p[\![X, Y]\!]}{(X^2 - \mu Y^2, XY, Y^3)} \xrightarrow{\sim} S, \qquad X \mapsto x, Y \mapsto y,$$

for some unique $\mu \in \mathbb{F}_p$. The possible choices of x are a torsor under the 1-dimensional $\mathbb{F}_p$-vector space $(y^2) = (J_S^{\mathrm{red}})^2$.

Proof. The ideal $\mathrm{Ann}_S(J_S^{\mathrm{red}}) \subset S$ is contained in $\mathfrak{m}_S$ because $J_S^{\mathrm{red}} \neq 0$. On the other hand, $\mathrm{Ann}_S(J_S^{\mathrm{red}})$ is not contained in $\mathfrak{m}_S^2$ because $\dim_{\mathbb{F}_p} \mathfrak{m}_S^2 = 1$ while $\dim_{\mathbb{F}_p} \mathrm{Ann}_S(J_S^{\mathrm{red}}) = 2$. Therefore $\mathrm{Ann}_S(J_S^{\mathrm{red}})$ has 1-dimensional image under the projection $\mathfrak{m}_S \twoheadrightarrow \mathfrak{m}_S/\mathfrak{m}_S^2 = \mathfrak{t}_R^*$. This image is complementary to $(\mathfrak{t}_R^{\mathrm{irr}})^* = \langle \bar{y} \rangle$ because $y^2 \neq 0$, yet every element of $\mathrm{Ann}_S(J_S^{\mathrm{red}})$ kills the generator y of J_S^{red}). Similarly, $\mathrm{Ann}_S(J^{\mathrm{red}}) \subset S$ is the kernel of φ_{D_y}, so there exists a generator x of $\mathrm{Ann}_S(J_S^{\mathrm{red}})$ such that

$$\{\bar{x}, \bar{y}\} \text{ is a dual basis to } \{D^{\mathrm{red}}, D_y\}.$$

In particular, x and y generate S as an $\mathbb{F}_p$-algebra, and we have a surjection $\phi : \mathbb{F}_p[\![X, Y]\!] \twoheadrightarrow S$ via $X \mapsto x, Y \mapsto y$.

The next goal is to show the existence of $\mu \in \mathbb{F}_p$ such that $(X^2 - \mu Y^2, XY, Y^3) \subset \ker \phi$. This will suffice to prove the presentation, because the quotient if $\mathbb{F}_p[\![X, Y]\!]$ by this ideal is 4-dimensional over $\mathbb{F}_p$, like S.

Clearly $Y^3 \in \ker \phi$, since $\mathfrak{m}_S^3 = 0$. Likewise, we know that $XY \in \ker \phi$ because $x \in S$ satisfies $xJ_S^{\mathrm{red}} = 0$ by definition, and y is a generator of J_S^{red}. Finally, the existence of $\mu \in \mathbb{F}_p$ such that $X^2 - \mu Y^2 \in \ker \phi$ follows from the principality of $J_S^{\mathrm{red}} = (y)$ and the fact that $\mathfrak{m}_S^2 = (J_S^{\mathrm{red}})^2 = (y^2)$ is 1-dimensional over $\mathbb{F}_p$ (Propositions 5.1.7 and 5.3.1), since we know from the start that $x^2 \in \mathfrak{m}_S^2$.

The claim that the various choices of x satisfying Definition 6.2.1 are a torsor under (y^2) follows from the fact that $\{x, y^2\}$ is an $\mathbb{F}_p$-basis for $\mathrm{Ann}_S(J^{\mathrm{red}})$, and that the projection of $gx + hy^2$ $(g, h \in \mathbb{F}_p)$ to $\mathfrak{t}_R^*$ equals $g\bar{x}$. This also makes the uniqueness of μ clear, since x^2 only depends upon $\bar{x}$. □

Combining the coordinates of S from Lemma 6.2.2 with the coordinates for the off-diagonal parts of E'_S from (6.1.5), we produce a coordinate-wise description of

$\rho'_S : G_{\mathbb{Q},Np} \to (E'_S)^\times$.

$$\rho'_S = \begin{pmatrix} \omega(1 + ya^{(1)'} + y^2a^{(2)'} + xa_0) & (b_0^{(1)}, b^{(1)} + yb^{(2)'}) \\ \omega(c^{(1)} + yc^{(2)'}) & 1 + yd^{(1)'} + y^2d^{(2)'} - xa'_0 \end{pmatrix} \tag{6.2.3}$$

for some cochains

- $a^{(1)'}, a^{(2)'}, d^{(1)'}, d^{(2)'} : G_{\mathbb{Q},Np} \to \mathbb{F}_p$,
- $b^{(2)'} : G_{\mathbb{Q},Np} \to \mathbb{F}_p(1)$,
- $c^{(2)'} : G_{\mathbb{Q},Np} \to \mathbb{F}_p(-1)$,

and cocycles a_0, $b^{(1)} = b_1^{(1)}$, $b_0^{(1)}$, and $c^{(1)}$ defined in Definition 3.1.1. The reason that we find these previously defined cocycles among these coordinates is

- for a_0: the tangent vector $D^{\mathrm{red}} \in \mathfrak{t}_R$ is dual to $\bar{x} \in \mathfrak{t}_R^*$, and we observe that the pseudorepresentation induced by $\rho_S \otimes_{S,\varphi_{D^{\mathrm{red}}}} \mathbb{F}_p[\epsilon_1]$ is exactly D^{red} (keep in mind that $\varphi_{D^{\mathrm{red}}}(x) = \epsilon$, $\varphi_{D^{\mathrm{red}}}(y) = 0$)
- for the remaining cocycles: the presence of dual bases of the dual vector spaces of (5.1.5) (see the proof of Proposition 5.1.7), along with the normalization of both the generators of B_S, C_S and the cocycles $b^{(1)}$, $b_0^{(1)}$, and $c^{(1)}$ in terms of the elements γ_0, γ_1 of inertia groups.

Next, we are interested in identifying $a^{(1)'}$ with the $a^{(1)}$ constructed in Lemma 4.2.1, which implies the similar identification of $d^{(1)'}$ with $d^{(1)} = b^{(1)}c^{(1)} - a^{(1)}$. This will produce a surjection from ρ'_S onto the $\rho_1 : G_{\mathbb{Q},Np} \to E_1^\times$ constructed in Lemma 4.3.2 and implies that $D_y = D_1 := \psi(\rho_1)$. The key is the comparison of differential equations: the homomorphism property of ρ'_S implies that $a^{(1)'}$ satisfies the differential equation

$$-\,da^{(1)'} = b^{(1)} \smile c^{(1)}, \tag{6.2.4}$$

which $a^{(1)}$ also satisfies (Lemma 4.2.1). We note that the fact that ρ'_S has constant determinant ω implies that $d^{(1)'} = b^{(1)}c^{(1)} - a^{(1)}$, just as in the discussion of $d^{(1)}$ in §4.3.

There are even more differential equations implied by the fact that ρ'_S is a homomorphism,

$$-dc^{(2)'} = c^{(1)} \smile a^{(1)'} + d^{(1)'} \smile c^{(1)} \tag{6.2.5}$$

$$-da^{(2)} = a^{(1)} \smile a^{(1)} + b^{(1)} \smile c^{(2)} + (b^{(2)} + \eta b_0^{(1)}) \smile c^{(1)} + \mu a_0 \smile a_0 \tag{6.2.6}$$

$$-db^{(2)} = a^{(1)} \smile b^{(1)} + b^{(1)} \smile d^{(1)}. \tag{6.2.7}$$

In particular, the 2-cocycles on the right-hand-sides of these equations are coboundaries.

Lemma 6.2.8. *The two 1-cochains $a^{(1)}, a^{(1)'} : G_{\mathbb{Q},Np} \to \mathbb{F}_p$ are equal. Consequently, $D_y = D_1 : G_{\mathbb{Q},Np} \to \mathbb{F}_p[\epsilon_1]$.*

Proof. Lemma 4.2.1 has listed characterizing properties (1)-(3) of $a^{(1)}$. We will show that $a^{(1)'}$ satisfies them as well.

Property (1) is satisfied in (6.2.4).

We will deduce property (2) from the finite-flat property that $\rho'_S|_p$, which it satisfies because it is a quotient GMA of the universal US_N GMA over $\bar{D}$. By design, the 0-cochain $x_{c^{(1)}} \in C^0(\mathbb{Z}[1/Np], \mathbb{F}_p(-1))$ conjugates $c^{(1)}$ so that it vanishes on G_p, in the sense that the conjugation of ρ'_S by $\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}$ is upper-triangular on G_p modulo the ideal generated by the image of yC_S in the C-coordinate. Then Proposition 2.2.6 implies the vanishing of $(a^{(1)'} + b^{(1)} \smile x_{c^{(1)}})|_{I_p}$, which is property (2).

Because of the injection $H^2(\mathbb{Z}[1/Np], \mathbb{F}_p(-1)) \hookrightarrow H^2(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(-1))$ of Lemma 3.2.8 and the vanishing of $b^{(1)}$ at ℓ_0, equation (6.2.5) implies that $a^{(1)'}|_{\ell_0}$ is a cocycle and $(2c^{(1)} \smile a^{(1)'})|_{\ell_0}$ is a 2-coboundary. Since the cup product on $H^1(\mathbb{Q}_{\ell_0}, \mathbb{F}_p) \times H^1(\mathbb{Q}_{\ell_0}, \mathbb{F}_p)$ is alternating in the sense of Lemma 3.2.6, we conclude that $[a^{(1)'}|_{\ell_0}]$ and $[c^{(1)}|_{\ell_0}] \cup [\zeta]$ are colinear in $H^1(\mathbb{Q}_{\ell_0}, \mathbb{F}_p)$ for any choice of $\zeta \in H^0(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(1))$, which is property (3).

To deduce that $D_y = D_1$, observe that the equality $a^{(1)'} = a^{(1)}$ implies that the pseudorepresentation $\phi(\rho'_S) : G_{\mathbb{Q},Np} \to S$ induces D_1 via

$$S \to \mathbb{F}_p[\epsilon_1], \quad x \mapsto 0, y \mapsto \epsilon,$$

while, on the other hand, this map $S \to \mathbb{F}_p[\epsilon_1]$ is exactly the same as φ_{D_y}. □

There are even more implications of the differential equations implied by the existence of ρ'_S. In particular, (6.2.7) has the following consequence about the restriction $a^{(1)}|_{\ell_1}$ (note that $a^{(1)}|_{\ell_1}$ is a cocycle since $da^{(1)} = b^{(1)} \smile c^{(1)}$ and $c^{(1)}|_{\ell_1} = 0$).

Lemma 6.2.9. *There exists a cochain $b^{(2)}$ satisfying* (6.2.7) *if and only if $a^{(1)}|_{\ell_1} = 0$. In particular, if $\dim_{\mathbb{F}_p}(S) = 4$, then $a^{(1)}|_{\ell_1} = 0$.*

Proof. Since $a^{(1)}|_{\ell_1}$ is an element of $H^1(\mathbb{Q}_{\ell_1}, \mathbb{F}_p)$, which is Tate-dual to $H^1(\mathbb{Q}_{\ell_1}, \mathbb{F}_p(1))$, and since $b^{(1)}|_{\ell_1}$ is a basis for $H^1(\mathbb{Q}_{\ell_1}, \mathbb{F}_p(1))$, the cup product $a^{(1)}|_{\ell_1} \cup b^{(1)}|_{\ell_1}$ vanishes in $H^2(\mathbb{Q}_{\ell_1}, \mathbb{F}_p(1))$ if and only if $a^{(1)}|_{\ell_1} = 0$.

The existence of a cochain $b^{(2)}$ satisfying (6.2.7) is equivalent to

$$a^{(1)} \cup b^{(1)} + b^{(1)} \cup d^{(1)} \tag{6.2.10}$$

vanishing in $H^2(G_{\mathbb{Q},Np}, \mathbb{F}_p(1))$. By Lemma 3.2.8, it is equivalent that the image of (6.2.10) vanishes in $H^2(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(1))$ and $H^2(\mathbb{Q}_{\ell_1}, \mathbb{F}_p(1))$. Since $b^{(1)}|_{\ell_0} = 0$ in $H^1(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(1))$, it is enough to consider the restriction of (6.2.10) to $H^2(\mathbb{Q}_{\ell_1}, \mathbb{F}_p(1))$.

Since $d^{(1)} = b^{(1)}c^{(1)} - a^{(1)}$ and $c^{(1)}|_{\ell_1} = 0$, it follows that $d^{(1)}|_{\ell_1} = -a^{(1)}|_{\ell_1}$. Restricting (6.2.10) to G_{ℓ_1} then gives

$$a^{(1)}|_{\ell_1} \cup b^{(1)}|_{\ell_1} - b^{(1)}|_{\ell_1} \cup a^{(1)}|_{\ell_1},$$

which vanishes if and only if $a^{(1)}|_{\ell_1} \cup b^{(1)}|_{\ell_1} = 0$ by the skew-symmetry of cup product. □

6.3. **The invariant $\beta' \in \mathbb{F}_p(2)$.** The assumption $\dim_{\mathbb{F}_p}(S) = 4$ implies the equation (6.2.6). We use (6.2.6) to define an element $\beta' \in \mathbb{F}_p(2)$.

Lemma 6.3.1. *Assume $\dim_{\mathbb{F}_p}(S) = 4$. There is a unique element $\beta' \in \mathbb{F}_p(2)$ such that*

$$(b^{(2)} + \eta b_0^{(1)})|_{\ell_0} = \beta' \cup c^{(1)}|_{\ell_0}. \tag{6.3.2}$$

Proof. By Lemma 3.2.6, it is enough to show that the cup product

$$(b^{(2)} + \eta b_0^{(1)})|_{\ell_0} \cup c^{(1)}|_{\ell_0}$$

vanishes in $H^2(\mathbb{Q}_{\ell_0}, \mathbb{F}_p)$. This follows from (6.2.6) by restriction to $H^2(\mathbb{Q}_{\ell_0}, \mathbb{F}_p)$. Indeed, recall from Lemma 3.2.1 that $b^{(1)}|_{\ell_0} = 0$. Since $-da^{(1)} = b^{(1)} \smile c^{(1)}$, this implies that $a^{(1)}|_{\ell_0}$ is a cocycle. By the skew-symmetry of cup product on cohomology, (6.2.6) then implies

$$(b^{(2)} + \eta b_0^{(1)})|_{\ell_0} \cup c^{(1)}|_{\ell_0} = 0.$$

in $H^2(\mathbb{Q}_{\ell_0}, \mathbb{F}_p)$. □

6.4. **Implications of the** US_N **property of** ρ'_S**.** The fact that ρ'_S is unramified-or-Steinberg at ℓ_0 implies a relationship between the invariants $\alpha \in \mathbb{F}_p(1)$, defined in Definition 4.2.2, and $\beta' \in \mathbb{F}_p(2)$, defined in Lemma 6.3.1.

Proposition 6.4.1. *Assume* $\dim_{\mathbb{F}_p} S = 4$. *Then*

(1) $\alpha^2 + \beta' = 0$ *in* $\mathbb{F}_p(2)$.
(2) the invariant $\mu \in \mathbb{F}_p$ *set up in Lemma 6.2.2 is zero.*

In particular, the presentation of S *from Lemma 6.2.2 takes the form*

$$\frac{\mathbb{F}_p[\![X, Y]\!]}{(X^2, XY, Y^3)}.$$

Remark 6.4.2. Since α depends only on the pinning data of Definition 1.7.1, part (1) implies that β' depends only on this data as well.

Proof. Since ρ'_S is obtained as a quotient of the universal US_N Cayley–Hamilton representation E, it is also US_N. Let $\sigma \in G_{\ell_0}$ and $\tau \in I_{\ell_0}$. By Definition 2.2.2, the fact that ρ'_S is US_N implies that

$$(\rho'_S(\sigma) - \omega(\sigma))(\rho'_S(\tau) - 1) \tag{6.4.3}$$

vanishes in E'_S. Consider the top-left coordinate of (6.4.3) in terms of the GMA decomposition (6.2.3) of ρ'_S. Using the facts that $\omega|_{\ell_0} = 1$ and $b^{(1)}|_{\ell_0} = 0$, and the formula for multiplication in E'_S given in (6.1.4), the top-left coordinate in (6.4.3) equals

$$\left(a^{(1)}(\sigma)a^{(1)}(\tau) + (b^{(2)}(\sigma) + \eta b_0^{(1)}(\sigma))c^{(1)}(\tau)\right) y^2 + a_0(\sigma)a_0(\tau)x^2. \tag{6.4.4}$$

Recall from the presentation given in Lemma 6.2.2 that $x^2 = \mu y^2$ in S. Using the relations

$$a^{(1)}|_{\ell_0} = \alpha \smile c^{(1)}|_{\ell_0}, \quad (b^{(2)} + \eta b_0^{(1)})|_{\ell_0} = \beta' \smile c^{(1)}|_{\ell_0}$$

that define α and β', (6.4.4) then simplifies to

$$\left((\alpha^2 + \beta')c^{(1)}(\tau)c^{(1)}(\sigma) + \mu a_0(\tau)a_0(\sigma)\right) y^2. \tag{6.4.5}$$

Since (6.4.3) vanishes in E'_S, this implies that (6.4.5) vanishes in S.

The vanishing of (6.4.5) in S for arbitrary $\sigma \in G_{\ell_0}$ and $\tau \in I_{\ell_0}$ implies

$$(\alpha^2 + \beta')c^{(1)}(\tau)c^{(1)}|_{\ell_0} + \mu a_0(\tau)a_0|_{\ell_0} = 0,$$

for all $\tau \in I_{\ell_0}$. Since $a_0|_{\ell_0}$ and $c^{(1)}|_{\ell_0}$ are linearly independent in $H^1(\mathbb{Q}_{\ell_0}, \mathbb{F}_p)$ by Proposition 3.2.9, this implies

$$(\alpha^2 + \beta')c^{(1)}(\tau) = 0 \text{ and } \mu a_0(\tau) = 0$$

for all $\tau \in I_{\ell_0}$. Since $c^{(1)}|_{I_{\ell_0}}$ and $a_0|_{I_{\ell_0}}$ are nonzero, this gives the result. □

Since $\mu = 0$ in the presentation for S of Lemma 6.2.2, there is a ring homomorphism

$$D_2 : S \to \mathbb{F}_p[\epsilon_2], \quad x \mapsto 0, y \mapsto \epsilon$$

whose composition with the quotient $\mathbb{F}_p[\epsilon_2] \to \mathbb{F}_p[\epsilon_1]$ is D_1. There is also a homomorphism of $\mathbb{F}_p[\epsilon_2]$-GMAs $E'_S \otimes_S \mathbb{F}_p[\epsilon_2] \to E_2$, where E_2 is the 1-reducible GMA over $\mathbb{F}_p[\epsilon_2]$ of Definition 4.1.2.

Corollary 6.4.6. *Assume* $\dim_{\mathbb{F}_p} S = 4$. *The map*

$$\Upsilon_2 : \mathbb{F}_p \oplus \mathbb{F}_p[\epsilon_1] \to \mathbb{F}_p[\epsilon_1]$$

given by $\Upsilon_2(u, v) = \eta\epsilon u + v$ *induces a map of* $\mathbb{F}_p[\epsilon_2]$*-GMAs*

$$E'_S \otimes_S \mathbb{F}_p[\epsilon_2] \xrightarrow{\left(\begin{smallmatrix} D_2 & \Upsilon_2 \\ \mathrm{Id} & D_2 \end{smallmatrix}\right)} E_2.$$

In particular, there is an US_N *Cayley–Hamilton representation* $\rho_2 : G_{\mathbb{Q},Np} \to E_2^\times$ *that deforms* ρ_1 *along the map* $r_{2,1} : E_2 \twoheadrightarrow E_1$ *of* (4.1.7).

Proof. Given that $\mu = 0$, the fact that $\left(\begin{smallmatrix} D_2 & \Upsilon_2 \\ \mathrm{Id} & D_2 \end{smallmatrix}\right)$ is ring homomorphism is a simple computation using the formula (6.1.4) for multiplication in E'_S. The representation ρ_2 is obtained as the composition of ρ'_S with $E'_S \otimes_S \mathbb{F}_p[\epsilon_2] \to E_2$. □

7. Constructing a second-order US_N deformation ρ_2

In this section, we prove the remaining implication of Theorem 1.4.3. Throughout the section, we assume $a^{(1)}|_{\ell_1} = 0$. Under this assumption, we construct an invariant $\beta \in \mathbb{F}_p(2)$, and show that if $\alpha^2 + \beta = 0$, then $\dim_{\mathbb{F}_p} R/pR > 3$. In particular, if $\alpha^2 + \beta = 0$, we can apply the constructions of the previous section to obtain another invariant $\beta' \in \mathbb{F}_p(2)$, and we prove that $\beta' = \beta$.

The proof of $\dim_{\mathbb{F}_p} R/pR > 3$ involves constructing an explicit US_N deformation using the 1-reducible GMAs of Definition 4.1.2. We do this in steps, first constructing an arbitrary deformation, and then imposing the local conditions one at a time. We show that the assumption $a^{(1)}|_{\ell_1} = 0$ implies that a deformation exists. Next, we impose the finite-flat condition, which we show limits the set of deformations enough that there is a well-defined invariant $\beta \in \mathbb{F}_p(2)$. Finally, we show that the unramified-or-Steinberg condition is satisfied if $\alpha^2 + \beta = 0$.

7.1. Construction of a second-order 1-reducible GMA representation without local conditions.

Recall the Cayley–Hamilton representation

$$\rho_1 = \begin{pmatrix} \omega(1 + \epsilon a^{(1)}) & b^{(1)} \\ \omega c^{(1)} & 1 + \epsilon d^{(1)} \end{pmatrix} : G_{\mathbb{Q},Np} \to E_1^\times$$

of Lemma 4.3.2. Let Π_2 denote the set of second-order 1-reducible Cayley–Hamilton deformations of ρ_1:

$$\Pi_2 = \{\rho_2 : \ G_{\mathbb{Q},Np} \ \to \ E_2^\times \mid r_{2,1} \circ \rho_2 = \rho_1\},$$

where $r_{2,1}$ is the reduction map of 1-reducible GMAs $r_{2,1} : E_2 \twoheadrightarrow E_1$ of (4.1.7).

Lemma 7.1.1. *The set* Π_2 *is in bijection with the set quadruples of cochains* $a^{(2)}, d^{(2)} : G_{\mathbb{Q},Np} \to \mathbb{F}_p$, $b^{(2)} : G_{\mathbb{Q},Np} \to \mathbb{F}_p(1)$, *and* $c^{(2)} : G_{\mathbb{Q},Np} \to \mathbb{F}_p(-1)$ *that satisfy*

(i) $-da^{(2)} = a^{(1)} \smile a^{(1)} + b^{(1)} \smile c^{(2)} + b^{(2)} \smile c^{(1)}$
(ii) $-db^{(2)} = a^{(1)} \smile b^{(1)} + b^{(1)} \smile d^{(1)}$

(iii) $-dc^{(2)} = c^{(1)} \smile a^{(1)} + d^{(1)} \smile c^{(1)}$
(iv) $-dd^{(2)} = d^{(1)} \smile d^{(1)} + c^{(1)} \smile b^{(2)} + c^{(2)} \smile b^{(1)}$.

This set is non-empty if and only if $a^{(1)}|_{\ell_1} = 0$. *Moreover, if it is non-empty,*

(1) Π_2 *admits the structure of a torsor under the group*

$$\mathfrak{Z}_2 := Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p) \times Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p) \times Z^1_b \times Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p(-1)),$$

where

$$Z^1_b := \ker\left(Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1)) \to \frac{H^1(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(1))}{\langle \mathbb{F}_p(2)|_{\ell_0} \cup [c^{(1)}]|_{\ell_0}\rangle}\right)$$

and the action of $(a, d, b, c) \in \mathfrak{Z}_2$ *on* $(a^{(2)}, d^{(2)}, b^{(2)}, c^{(2)}) \in \Pi_2$ *has the form*

$$(a, d, 0, 0) \cdot (a^{(2)}, d^{(2)}, b^{(2)}, c^{(2)}) = (a^{(2)} + a, d^{(2)} + d, b^{(2)}, c^{(2)})$$

$$(0, 0, b, c) \cdot (a^{(2)}, d^{(2)}, b^{(2)}, c^{(2)}) =$$
$$(a^{(2)} + \sigma(b, c), d^{(2)} - \sigma(b, c) + b \cdot c^{(1)} + b^{(1)} \cdot c, b^{(2)} + b, c^{(2)} + c)$$

where $\sigma : Z^1_b \times Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p(-1)) \to C^1(\mathbb{Z}[1/Np], \mathbb{F}_p)$ *is a choice of linear map such that* $-d\sigma(b, c) = b \smile c^{(1)} + b^{(1)} \smile c$.

(2) For every $(a^{(2)}, d^{(2)}, b^{(2)}, c^{(2)}) \in \Pi_2$, *the restriction* $b^{(2)}|_{\ell_0}$ *is a cocycle whose cohomology class is a multiple of* $c_0|_{\ell_0} = [c^{(1)}]|_{\ell_0}$.

Proof. Every element ρ_2 of Π_2 can be written in the form

$$\rho_2 = \begin{pmatrix} \omega(1 + a^{(1)}\epsilon + a^{(2)}\epsilon^2) & b^{(1)} + b^{(2)}\epsilon \\ \omega(c^{(1)} + c^{(2)}\epsilon) & 1 + d^{(1)}\epsilon + d^{(2)}\epsilon^2 \end{pmatrix} : G_{\mathbb{Q},Np} \to E_2^\times, \tag{7.1.2}$$

for some cochains $a^{(2)}$, $b^{(2)}$, $c^{(2)}$, $d^{(2)}$. The fact that ρ_2 is a homomorphism implies the equations (i)-(iv). Conversely, given cochains satisfying (i)-(iv), the function ρ_2 defined by (7.1.2) is an element of Π_2. This gives the desired bijection. Now we show that there are cochains satisfying (i)-(iv) if and only if $a^{(1)}|_{\ell_1} = 0$.

Coboundary condition (ii). Note that (ii) is the same equation as (6.2.7). By Lemma 6.2.9, there is a cochain $b^{(2)}$ satisfying (ii) if and only if $a^{(1)}|_{\ell_1} = 0$. The set of cochains $b^{(2)}$ satisfying (ii) is a torsor for $Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1))$; however, we will see that condition (i) can only be satisfied for a subset of the cochains $b^{(2)}$ satisfying (ii).

This shows that $a^{(1)}|_{\ell_1} = 0$ is necessary for Π_2 to be non-empty. Now assume $a^{(1)}|_{\ell_1} = 0$, and we will show this is sufficient.

Coboundary condition (iii). There is a cochain satisfying (iii) if

$$c^{(1)} \cup a^{(1)} + d^{(1)} \cup c^{(1)} = 0$$

in $H^2(G_{\mathbb{Q},Np}, \mathbb{F}_p(-1))$. By Lemma 3.2.8, we only have to check this vanishing after restriction to $H^2(\mathbb{Q}_{\ell_1}, \mathbb{F}_p(-1))$ and $H^2(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(-1))$. The ℓ_1-local restriction vanishes because $a^{(1)}|_{\ell_1} = d^{(1)}|_{\ell_1} = 0$. Since $d^{(1)}|_{\ell_0} = -a^{(1)}|_{\ell_0}$, the ℓ_0-local restriction is

$$c^{(1)}|_{\ell_0} \cup a^{(1)}|_{\ell_0} - a^{(1)}|_{\ell_0} \cup c^{(1)}|_{\ell_0},$$

which vanishes because $a^{(1)}|_{\ell_0} = \alpha \cup c^{(1)}|_{\ell_0}$. The set of cochains satisfying (iii) is a torsor for $Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p(-1))$.

Coboundary condition (i). Note that condition (i) is similar to (6.2.6); this argument follows the same line as in the proof Lemma 6.3.1.

Let $b^{(2)}$ and $c^{(2)}$ be arbitrary cochains satisfying (ii) and (iii), respectively. There is a cochain $a^{(2)}$ satisfying (i) if

$$a^{(1)} \smile a^{(1)} + b^{(1)} \smile c^{(2)} + b^{(2)} \smile c^{(1)} \tag{7.1.3}$$

vanishes in $H^2(G_{\mathbb{Q},Np}, \mathbb{F}_p)$. By Lemma 3.2.8 and since $H^2(\mathbb{Q}_{\ell_1}, \mathbb{F}_p) = 0$, it is enough to check this vanishing after restriction to $H^2(\mathbb{Q}_{\ell_0}, \mathbb{F}_p)$.

Recall from Lemma 3.2.1 that $b^{(1)}|_{\ell_0} = 0$. Since $-da^{(1)} = b^{(1)} \smile c^{(1)}$, this implies that $a^{(1)}|_{\ell_0}$ is a cocycle. Likewise, differential equation (ii) implies that $b^{(2)}|_{\ell_0}$ is a cocycle. By the skew-symmetry of cup product, (7.1.3) vanishes if and only if

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

vanishes in $H^2(\mathbb{Q}_{\ell_0}, \mathbb{F}_p)$. This happens for some choices of $b^{(2)}$, but not others: recall that the set of choices of $b^{(2)}$ satisfying (ii) is a torsor for $Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1))$. Indeed, since $H^2(\mathbb{Q}_{\ell_0}, \mathbb{F}_p)$ has $\mathbb{F}_p$-dimension 1 and is spanned by $[b_0^{(1)}]|_{\ell_0} \cup [c^{(1)}]|_{\ell_0}$ by Proposition 3.2.9, there is a constant $\gamma \in \mathbb{F}_p$ such that

$$[b^{(2)}|_{\ell_0}] \cup [c^{(1)}]|_{\ell_0} = \gamma [b_0^{(1)}]|_{\ell_0} \cup [c^{(1)}|_{\ell_0}.$$

This shows that (7.1.3) vanishes if $b^{(2)}$ is replaced by $b^{(2)} - \gamma b_0^{(1)}$. Moreover, the set of choices for $b^{(2)}$ satisfying (ii) and such that (7.1.3) vanishes is a torsor for the set of $b \in Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1))$ such that $[b]|_{\ell_0} \cup [c^{(1)}]|_{\ell_0} = 0$. By Tate duality (Lemma 3.2.6), this is same as b belonging to the subgroup Z_b^1.

In summary, the set of $b^{(2)}$ that satisfy (ii) and such that (i) has a solution is a torsor for Z_b^1; this is holds for any choice of $c^{(2)}$. For any such $b^{(2)}$, the set of $a^{(2)}$ that satisfy (i) is a torsor for $Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p)$.

Coboundary condition (iv). The same analysis as for (i) applies to (iv).

Combining these analyses, we deduce that

- Π_2 is non-empty if and only if $a^{(1)}|_{\ell_1} = 0$
- There is an action of $Z_b^1 \times Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p(-1))$ on Π_2 that acts by addition on the $b^{(2)}$ and $c^{(2)}$-coordinates
- And there exists a linear choice of σ, namely

  $$Z_b^1 \times Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p(-1)) \ni (b, c) \mapsto -d^{-1}(b \smile c^{(1)} + b^{(1)} \smile c)$$

  where d^{-1} is an arbitrarily chosen linear section of the boundary map $d : C^1(\mathbb{Z}[1/Np], \mathbb{F}_p) \twoheadrightarrow B^2(\mathbb{Z}[1/Np], \mathbb{F}_p)$. Under this definition of σ, one can compute that the differential equations (i) and (iv) are satisfied by $(0, 0, b, c) \cdot (a^{(2)}, b^{(2)}, c^{(2)}, d^{(2)})$. (See the origin of the formula for the $d^{(2)}$-coordinate in the proof of Lemma 7.1.4, below.)
- There is an action of $Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p)^{\oplus 2}$ that acts by addition on the $a^{(2)}$ and $d^{(2)}$-coordinates and fixes the $b^{(2)}$ and $c^{(2)}$-coordinates,

which amounts to claim (1). Claim (2) follows from the analysis of coboundary condition (i) above. □

We will frequently use the bijection between Π_2 and the set of quadruples of cochains $(a^{(2)}, d^{(2)}, b^{(2)}, c^{(2)})$ satisfying (i)-(iv) without comment. Let $\Pi_2^{\det}$ denote the subset of Π_2 consisting of elements with constant determinant ω,

$$\Pi_2^{\det} := \{\rho_2 \in \Pi_2 \mid \det(\rho_2) = \omega\}.$$

Lemma 7.1.4. *Assume $a^{(1)}|_{\ell_0} = 0$. Then $\Pi_2^{\det}$ is non-empty, an element $\rho_2 \in \Pi_2$ is completely determined by its cochains $a^{(2)}$, $b^{(2)}$ and $c^{(2)}$, and $\Pi_2^{\det}$ is a torsor for the subgroup $\mathfrak{Z}_2^{\det} \subset \mathfrak{Z}_2$ under the action of $\mathfrak{Z}_2$ on Π_2 of Lemma 7.1.1, where*

$$\mathfrak{Z}_2^{\det} := \{(a,d,b,c) \in \mathfrak{Z}_2 \mid a + d = 0\} \subset \mathfrak{Z}_2.$$

Proof. Let $a^{(2)}$, $b^{(2)}$, and $c^{(2)}$ be cochains satisfying equations (i), (ii) and (iii), respectively, of Lemma 7.1.1. A straightforward calculation shows that the only choice of cochain $d^{(2)}$ such that the resulting representation ρ_2 satisfies $\det(\rho_2) = \omega$ is

$$d^{(2)} = b^{(1)}c^{(2)} + b^{(2)}c^{(1)} - a^{(1)}d^{(1)} - a^{(2)}.$$

Moreover, a computation shows that this choice of $d^{(2)}$ satisfies equation (iv). The action of an element $(a,b,c,d) \in \mathfrak{Z}_2$ fixes the determinant if and only if $a + d = 0$. This follows from the equations for the action of $\mathfrak{Z}_2$ given in Lemma 7.1.1. □

7.2. **The finite-flat at p condition on ρ_2.** We continue to assume that $a^{(1)}|_{\ell_1} = 0$; consequently, $\Pi_2^{\det}$ is non-empty by Lemma 7.1.4. Consider the subset of Π_2,

$$\Pi_2^{\det,p} = \{\rho_2 \in \Pi_2^{\det} \mid \rho_2|_p \text{ is finite-flat}\} \subset \Pi_2.$$

Proposition 7.2.1. *Assume $a^{(1)}|_{\ell_1} = 0$. Then $\Pi_2^{\det,p}$ is non-empty, and the possibilities for $b^{(2)}$-coordinates of $\rho_2 \in \Pi_2^{\det,p}$ is contained in a torsor under the subgroup of $Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1))$ spanned by coboundaries and $b^{(1)}$. In particular, there is a unique $\beta \in \mathbb{F}_p(2)$ such that, for every $\rho_2 \in \Pi_2^{\det,p}$,*

$$[b^{(2)}|_{\ell_0}] = \beta \cup [c^{(1)}]|_{\ell_0} \quad \in H^1(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(1)),$$

where $b^{(2)}$ is the cochain associated to ρ_2.

Remark 7.2.2. In fact, the phrase "contained in" in the proposition can be replaced by "equal to," but we do not have a use for that result.

Remark 7.2.3. Lemma 7.1.1(2) already implies that some such β exists for any *single* $\rho_2 \in \Pi_2$; our supplemental work will be to show that there is only one β that appears among $\rho_2 \in \Pi_2^{\det,p}$.

We will prove the first claim of Proposition 7.2.1, that $\Pi_2^{\det,p}$ is non-empty, using a series of lemmas to produce an element of $\Pi_2^{\det}$ that is finite-flat at p.

Just as in the proof that ρ_1 is finite-flat in Lemma 4.3.2, it will be convenient to change the basis of $\rho_2 \in \Pi_2^{\det}$ in order to test the finite-flat condition of $\rho_2|_p$. Recall the element $x_{c^{(1)}} \in \mathbb{F}_p(1)$ of Definition 3.1.1 satisfying $dx_{c^{(1)}}|_p = c^{(1)}|_p$. Define $\rho_2' := \mathrm{ad}\left(\begin{pmatrix} 1 & 0 \\ -x_{c^{(1)}}+y\epsilon & 1\end{pmatrix}\right)\rho_2$ for $y \in \mathbb{F}_p$ to be chosen later, and write ρ_2' as

$$\rho_2' = \begin{pmatrix} \omega(1 + a^{(1)'}\epsilon + a^{(2)'}\epsilon^2) & b^{(1)'} + b^{(2)'}\epsilon \\ \omega(c^{(1)'} + c^{(2)'}\epsilon) & 1 + d^{(1)'}\epsilon + d^{(2)'}\epsilon^2 \end{pmatrix}. \tag{7.2.4}$$

Explicitly:

- $a^{(1)'} = a^{(1)} + b^{(1)} \smile x_{c^{(1)}}$
- $b^{(1)'} = b^{(1)}$
- $c^{(1)'} = c^{(1)} - dx_{c^{(1)}}$
- $d^{(1)'} = d^{(1)} - x_{c^{(1)}} \smile b^{(1)}$

and

- $a^{(2)'} = a^{(2)} + b^{(2)} \smile x_{c^{(1)}} + b^{(1)} \smile y$

- $b^{(2)'} = b^{(2)}$
- $c^{(2)'} = c^{(2)} - x_{c^{(1)}} \smile a^{(1)} + d^{(1)} \smile x_{c^{(1)}} - x_{c^{(1)}} \smile b^{(1)} \smile x_{c^{(1)}} - dy$
- $d^{(2)'} = d^{(2)} - x_{c^{(1)}} \smile b^{(2)} - y \smile b^{(1)}$.

Just as in the proof of Lemma 4.3.2, we have

- $a^{(1)'}|_p$ and $d^{(1)'}|_p$ are unramified homomorphisms
- $c^{(1)'}|_p = 0$.

Because ρ_2' is also a homomorphism, the primed cochains also satisfy equations (i)-(iv) of Lemma 7.1.1.

Lemma 7.2.5. *Assume $a^{(1)}|_{\ell_1} = 0$. There exists $\rho_2 \in \Pi_2^{\det}$ such that $\rho_2|_p$ is upper-triangular (in the sense that $c^{(2)'}|_p = 0$).*

Proof. Let $\rho_2 \in \Pi_2^{\det}$ be arbitrary. We will find an element $(a, -a, b, c) \in \mathfrak{Z}_2^{\det}$ such that $\rho_{2,\mathrm{new}} := (a, -a, b, c) \cdot \rho_2$ has the desired property.

By equation (iii) of Lemma 7.1.1 applied to $c^{(2)'}$,

$$-dc^{(2)'}|_p = c^{(1)'}|_p \smile a^{(1)'}|_p + d^{(1)'}|_p \smile c^{(1)'}|_p = 0$$

since $c^{(1)'}|_p = 0$. Hence $c^{(2)'}|_p$ is a cocycle.

Sublemma 7.2.6. *The $\mathbb{F}_p$-dimension of $H^1(\mathbb{Q}_p, \mathbb{F}_p(-1))$ is 1. The localization map $H^1(\mathbb{Z}[1/Np], \mathbb{F}_p(-1)) \to H^1(\mathbb{Q}_p, \mathbb{F}_p(-1))$ is surjective.*

Proof. The first claim is a standard consequence of Tate local duality and local Euler characteristics at p; in particular, the Euler characteristic of $H^\bullet(\mathbb{Q}_p, \mathbb{F}_p(-1))$ is -1. For the second claim, consider the exact sequence

$$0 \to H^1_{(p)}(\mathbb{Z}[1/Np], \mathbb{F}_p(-1)) \to H^1(\mathbb{Z}[1/Np], \mathbb{F}_p(-1)) \to H^1(\mathbb{Q}_p, \mathbb{F}_p(-1))$$

coming from the definition of $H^\bullet_{(p)}$ as a cone. The Euler characteristic of global cohomology $H^\bullet(\mathbb{Z}[1/Np], \mathbb{F}_p(-1))$ is -1 by the global Euler characteristic formula. We also know from the proof of Lemma 3.2.8 that $\dim_{\mathbb{F}_p} H^2(\mathbb{Z}[1/Np], \mathbb{F}_p(-1)) = 1$. Therefore $\dim_{\mathbb{F}_p} H^1(\mathbb{Z}[1/Np], \mathbb{F}_p(-1)) = 2$. The desired surjectivity follow from the fact that $H^1_{(p)}(\mathbb{Z}[1/Np], \mathbb{F}_p(-1))$ has dimension 1. Indeed, c_0 is a basis for it, as discussed in Definition 3.1.1. □

By the sublemma, there exists $z \in Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p(-1))$ such that $z|_p = -c^{(2)'}|_p$. Let $\rho_{2,\mathrm{new}} = (0, 0, 0, z) \cdot \rho_2$. It has $c^{(2)}_{\mathrm{new}} = c^{(2)} + z$. By the formula for $c^{(2)'}$ in terms of $c^{(2)}$ (given after (7.2.4)), we also have $c^{(2)'}_{\mathrm{new}} = c^{(2)'} + z$. Therefore $c^{(2)'}_{\mathrm{new}}|_p = 0$, as desired. □

Let $\rho_2 \in \Pi_2^{\det}$ be as in Lemma 7.2.5. Then

$$\rho_2'|_p = \begin{pmatrix} \omega\chi_2 & (b^{(1)'} + b^{(2)'}\epsilon)|_p \\ 0 & \chi_2^{-1} \end{pmatrix} : G_p \to E_2^\times, \tag{7.2.7}$$

where

$$\chi_2 = (1 + a^{(1)'}\epsilon + a^{(2)'}\epsilon^2)|_p : G_p \to \mathbb{F}_p[\epsilon_2]^\times.$$

Indeed, since $\rho_2'|_p$ is upper-triangular, χ_2 is a homomorphism, and since $\det(\rho_2') = \omega$, the lower-right coordinate of $\rho_2'|_p$ must be χ_2^{-1}. Let $\chi_1 : G_p \to \mathbb{F}_p[\epsilon_1]^\times$ denote the character $\chi_1 := \chi_2 \otimes_{\mathbb{F}_p[\epsilon_2]} \mathbb{F}_p[\epsilon_1]$, which equals $1 + a^{(1)'}\epsilon$. We want to characterize the finite-flat at p property of ρ_2, bootstrapping from the fact that its reduction ρ_1

is finite-flat at p. To this end, we induce two representations η_2 and η_1 associated to an element of $\Pi_2^{\det}$

Definition 7.2.8. Assume that $\rho_2 \in \Pi_2^{\det}$ has the property that $\rho_2'|_p$ is upper-triangular. Then there are two associated representations

$$\eta_2 = \begin{pmatrix} \omega\chi_2 & \epsilon b^{(1)'} + \epsilon^2 b^{(2)'} \\ 0 & \chi_2^{-1} \end{pmatrix} : G_p \to \mathrm{GL}_2(\mathbb{F}_p[\epsilon_2])$$

given by $\rho_2'|_p$ composed with the embedding of Lemma 4.1.9, and

$$\eta_1 = \begin{pmatrix} \omega(1+\epsilon a^{(1)'}) & b^{(1)'} + \epsilon b^{(2)'} \\ \omega\epsilon c^{(1)'} & 1+\epsilon d^{(1)'} \end{pmatrix} : G_{\mathbb{Q},Np} \to \mathrm{GL}_2(\mathbb{F}_p[\epsilon_1]) \tag{7.2.9}$$

given by ρ_2' composed with the map $E_2 \to M_2(\mathbb{F}_p[\epsilon_1])$ of Lemma 4.1.10.

Remark 7.2.10. Note that

$$\eta_1|_p = \begin{pmatrix} \omega\chi_1 & b^{(1)'}|_p + \epsilon b^{(2)'}|_p \\ 0 & \chi_1^{-1} \end{pmatrix}.$$

Also, be aware that η_1 does not equal the reduction of η_2 modulo ϵ^2. Rather, one obtains η_1 from η_2 by "dividing the extension class $\epsilon b^{(1)'} + \epsilon^2 b^{(2)'} \in \mathrm{Ext}^1_{\mathbb{F}_p[\epsilon_2][G_p]}(\chi_2^{-1}, \omega\chi_2)^{\mathrm{flat}}$ by ϵ," which will be made rigorous in the proof of Lemma 7.2.11.

Lemma 7.2.11. *Assume that $\rho_2 \in \Pi_2^{\det}$ has the property that $\rho_2'|_p$ is upper-triangular, and let η_2 and η_1 be the associated representations of Definition 7.2.8. The following are equivalent:*

(1) The Cayley–Hamilton representation $\rho_2|_p$ is finite-flat.
(2) The homomorphism η_2 is finite-flat.
(3) The homomorphism $\eta_1|_p : G_p \to \mathrm{GL}_2(\mathbb{F}_p[\epsilon_1])$ is finite-flat and χ_2 is unramified.

Proof. The equivalence of (1) and (2) follows from the embedding of Lemma 4.1.9 along with Lemma 2.2.10.

Now we assume (2) and prove (3). By Proposition 2.2.6, χ_2 is unramified. We will show that $\eta_1|_p$ is isomorphic to a subquotient representation of η_2. This implies that $\eta_1|_p$ is finite-flat, since the finite-flat property is *stable*, as discussed in §2.2.5.

From the exact sequences

$$0 \to \epsilon\omega\chi_2 \to \omega\chi_2 \to \omega \to 0, \quad 0 \to \epsilon^2\chi_2^{-1} \to \chi_2^{-1} \to \chi_1^{-1} \to 0$$

there is a commutative diagram of Ext groups over $\mathbb{F}_p[\epsilon_2][G_p]$ with exact rows and columns

$$\begin{array}{ccccccc}
 & & \mathrm{Ext}^1(\chi_1^{-1}, \epsilon\omega\chi_2) & & & & \\
 & & \downarrow & & & & \\
0 & \longrightarrow & \mathrm{Ext}^1(\chi_2^{-1}, \epsilon\omega\chi_2) & \longrightarrow & \mathrm{Ext}^1(\chi_2^{-1}, \omega\chi_2) & \longrightarrow & \mathrm{Ext}^1(\chi_2^{-1}, \omega) \\
 & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Ext}^1(\epsilon^2\chi_2^{-1}, \epsilon\omega\chi_2) & \longrightarrow & \mathrm{Ext}^1(\epsilon^2\chi_2^{-1}, \omega\chi_2) & &
\end{array}$$

The representation η_2 defines a class in $\mathrm{Ext}^1(\chi_2^{-1}, \omega\chi_2)$, written as $\epsilon b^{(1)'} + \epsilon^2 b^{(2)'}$. The fact that this class is a multiple of ϵ implies that η_2 maps to zero under both the horizontal and the vertical map out of $\mathrm{Ext}^1(\chi_2^{-1}, \omega\chi_2)$ in the diagram. By a diagram chase, there is a class $W \in \mathrm{Ext}^1(\chi_1^{-1}, \epsilon\omega\chi_2)$ mapping to η_2. This W is a subquotient of η_2, so it is finite-flat. Moreover, a computation of the maps in the diagram in coordinates, as in [WWE20, Appendix C], shows that there is an $\mathbb{F}_p[\epsilon_1]$-basis for W such that the action of G_p on W is given by $\eta_1|_p$. In particular, $\eta_1|_p$ is isomorphic to W as a $\mathbb{F}_p[G_p]$-module, so it is finite-flat.

Finally, we assume (3) and prove (2). By Proposition 2.2.12 (the formal smoothness of the finite-flat deformation functor), there is a finite-flat representation $\eta_{2,\mathrm{lift}} : G_p \to \mathrm{GL}_2(\mathbb{F}_p[\epsilon_2])$ of the form

$$\begin{aligned}\eta_{2,\mathrm{lift}} &= \begin{pmatrix} \omega(1+\epsilon a^{(1)'} + \epsilon^2 a^{(2)'}_{\mathrm{lift}}) & b^{(1)'} + \epsilon b^{(2)'} + \epsilon^2 b^{(3)'}_{\mathrm{lift}} \\ 0 & 1 + \epsilon d^{(1)'} + \epsilon^2 d^{(2)'}_{\mathrm{lift}} \end{pmatrix} \\ &= \begin{pmatrix} \omega\chi_{2,1,\mathrm{lift}} & b^{(1)'} + \epsilon b^{(2)'} + \epsilon^2 b^{(3)'}_{\mathrm{lift}} \\ 0 & \chi_{2,2,\mathrm{lift}} \end{pmatrix}.\end{aligned}$$

deforming $\eta_1|_p$. Let $\epsilon \cdot \eta_{2,\mathrm{lift}}$ denote the homomorphism

$$\epsilon \cdot \eta_{2,\mathrm{lift}} = \begin{pmatrix} \omega\chi_{2,1,\mathrm{lift}} & \epsilon b^{(1)'} + \epsilon^2 b^{(2)'} \\ 0 & \chi_{2,2,\mathrm{lift}} \end{pmatrix} : G_p \to \mathrm{GL}_2(\mathbb{F}_p[\epsilon_2]),$$

which represents the class in $\mathrm{Ext}^1_{\mathbb{F}_p[\epsilon_2][G_p]}(\chi_{2,2,\mathrm{lift}}^{-1}, \omega\chi_{2,1,\mathrm{lift}})$ that is the ϵ-multiple of the class of $b^{(1)'} + \epsilon b^{(2)'} + \epsilon^2 b^{(3)'}$. By [WWE20, Rem. C.3.2], since $\eta_{2,\mathrm{lift}}$ is finite-flat, $\epsilon \cdot \eta_{2,\mathrm{lift}}$ is too.

Finally, since χ_2, $\chi_{2,1,\mathrm{lift}}$, and $\chi_{2,2,\mathrm{lift}}$ are all unramified characters, it follows that

$$a = a^{(2)'} - a^{(2)'}_{\mathrm{lift}}, \text{ and } d = d^{(2)'} - d^{(2)'}_{\mathrm{lift}}$$

are unramified cocycles. Then η_2 is obtained from the finite-flat representation $\epsilon \cdot \eta_{2,\mathrm{lift}}$ by adding the cocycle $\left(\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right) \in Z^1(G_p, \mathrm{End}_{\mathbb{F}_p}(\omega \oplus 1))$, which is in the finite-flat subspace. By Proposition 2.2.12, this implies that η_2 is also finite-flat. ☐

Lemma 7.2.12. *Assume $a^{(1)}|_{\ell_1} = 0$. There exists $\rho_2 \in \Pi_2^{\mathrm{det}}$ such that*

- *$\rho_2'|_p$ is upper-triangular (equivalently, $c^{(2)'}|_p = 0$), and*
- *the associated homomorphism η_1 as in Definition 7.2.8 is finite-flat.*

Proof. Let $\rho_2 \in \Pi_2^{\mathrm{det}}$ be such that $\rho_2|_p$ is upper-triangular (which exists by Lemma 7.2.5). We will find an element $(0,0,b,0) \in \mathfrak{Z}_2^{\mathrm{det}}$ such that $\rho_{2,\mathrm{new}} := (0,0,b,0)\cdot\rho_2$ has $\eta_{1,\mathrm{new}}$ being finite-flat. This $\rho_{2,\mathrm{new}}|_p$ is still upper-triangular because $c^{(2)'}_{\mathrm{new}} = c^{(2)'}$.

Let $\eta = \left(\begin{smallmatrix} \omega & b^{(1)'} \\ 0 & 1 \end{smallmatrix}\right) = (\eta_1 \bmod \epsilon)$; it is finite-flat at p by Lemma 2.2.8. The lift η_1 of η over $\mathbb{F}_p[\epsilon_1] \twoheadrightarrow \mathbb{F}_p$ can and will be considered to be an element of $Z^1(\mathbb{Z}[1/Np], \mathrm{Ad}^0(\eta))$ by Lemma 2.2.11. We want to examine its coordinates so we set up the following notions.

The filtration of $\mathbb{F}_p[G_{\mathbb{Q},Np}]$-modules

$$0 \to \mathbb{F}_p(1) \xrightarrow{\iota} \eta \xrightarrow{\pi} \mathbb{F}_p \to 0$$

induces a filtration of $\mathrm{Ad}^0(\eta)$,

$$0 \subset \mathrm{Hom}_{\mathbb{F}_p}(\mathbb{F}_p, \mathbb{F}_p(1)) \subset U \subset \mathrm{Ad}^0(\eta),$$

where $U := \{f \in \mathrm{Ad}^0(\eta) \mid \pi \circ f \circ \iota = 0\}$ and

$$\frac{U}{\mathrm{Hom}_{\mathbb{F}_p}(\mathbb{F}_p, \mathbb{F}_p(1))} \simeq \mathbb{F}_p, \qquad \frac{\mathrm{Ad}^0(\eta)}{U} \cong \mathrm{Hom}_{\mathbb{F}_p}(\mathbb{F}_p(1), \mathbb{F}_p) \cong \mathbb{F}_p(-1).$$

For any subgroup $G \subset G_{\mathbb{Q},Np}$, it is exactly the cochains in $C^1(G, \mathrm{Ad}^0(\eta))$ that lie in $C^1(G, U)$ that are upper-triangular. Therefore we are interested in $Z^1(\mathbb{Q}_p, U)$, and its finite-flat subspace $Z^1(\mathbb{Q}_p, U)^{\mathrm{flat}}$. We also want to use the subspace of global lifts that are upper-triangular upon restriction to G_p,

$$Z^1(\mathbb{Z}[1/Np], \mathrm{Ad}^0(\eta))^{p\text{-UT}} = \ker\left(Z^1(\mathbb{Z}[1/Np], \mathrm{Ad}^0(\eta)) \to \frac{Z^1(\mathbb{Q}_p, \mathrm{Ad}^0(\eta|_p))}{Z^1(\mathbb{Q}_p, U)}\right).$$

Sublemma 7.2.13. *There is a commutative diagram induced by the filtrations above with exact rows*

$$\begin{array}{ccccccccc}
0 & \to & Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1)) & \xrightarrow{\iota_{\mathbb{Q}}} & Z^1(\mathbb{Z}[1/Np], \mathrm{Ad}^0(\eta))^{p\text{-}UT} & & & & \\
 & & \downarrow & & \downarrow & & & & \\
0 & \to & Z^1(\mathbb{Q}_p, \mathbb{F}_p(1)) & \xrightarrow{\iota_p} & Z^1(\mathbb{Q}_p, U) & \xrightarrow{\kappa_p} & Z^1(\mathbb{Q}_p, \mathbb{F}_p) & & \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \to & Z^1(\mathbb{Q}_p, \mathbb{F}_p(1))^{\mathrm{flat}} & \to & Z^1(\mathbb{Q}_p, U)^{\mathrm{flat}} & \to & Z^1(\mathbb{Q}_p, \mathbb{F}_p)^{\mathrm{flat}} & \to & 0
\end{array}$$

where

$$\iota_* : b \mapsto \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}, \quad \kappa_* : \begin{pmatrix} a_p^{(1)'} & b_p^{(2)'} \\ 0 & -a_p^{(1)'} \end{pmatrix} \mapsto a_p^{(1)'}.$$

Proof. The commutativity follows directly from the filtrations. The exactness of the top two rows follows from standard long exact sequences in Galois cohomology, for $G = G_{\mathbb{Q},Np}, G_p$,

$$0 \to H^0(G, \mathbb{F}_p) \to H^1(G, \mathbb{F}_p(1)) \to H^1(G, U) \to H^1(G, \mathbb{F}_p),$$

and the observation that the kernel of $H^1(G, \mathbb{F}_p(1)) \to H^1(G, U)$ arises from cocycles being sent to coboundaries that are non-zero. The exactness of the third row follows from direct calculation of ι_p and κ_p. The final claim of the lemma follows from Proposition 2.2.12 and the exactness of the rows of the diagram. $\square$

Since $\eta_1|_p$ is upper-triangular, $\eta_1 \in Z^1(\mathbb{Z}[1/Np], \mathrm{Ad}^0(\eta))^{p\text{-UT}}$. Moreover $\kappa_p(\eta_1|_p) = a^{(1)'}|_p$ is in $Z^1(\mathbb{Q}_p, \mathbb{F}_p)^{\mathrm{flat}} = Z^1_{\mathrm{unr}}(\mathbb{Q}_p, \mathbb{F}_p)$ because $a^{(1)'}|_p$ is unramified by construction (see Lemma 4.2.1).

Consider the diagram in the sublemma. Since $\kappa_p(\eta_1|_p) \in Z^1(\mathbb{Q}_p, \mathbb{F}_p)^{\mathrm{flat}}$, the snake lemma implies that the class of $\eta_1|_p$ is in the image of

$$\frac{Z^1(\mathbb{Q}_p, \mathbb{F}_p(1))}{Z^1(\mathbb{Q}_p, \mathbb{F}_p(1))^{\mathrm{flat}}} \xrightarrow{\iota_p} \frac{Z^1(\mathbb{Q}_p, U)}{Z^1(\mathbb{Q}_p, U)^{\mathrm{flat}}}.$$

By Lemma 2.2.9, the image of $Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1))$ generates $\frac{Z^1(\mathbb{Q}_p, \mathbb{F}_p(1))}{Z^1(\mathbb{Q}_p, \mathbb{F}_p(1))^{\mathrm{flat}}}$. This implies that there is $b \in Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1))$ such that $\iota_p(b|_p) + \eta_1|_p$ is in $Z^1(\mathbb{Q}_p, U)^{\mathrm{flat}}$. The commutativity of the diagram implies that $\iota_p(b|_p) = \iota_{\mathbb{Q}}(b)|_p$.

Let $b \in Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1))$ be such that $\iota_{\mathbb{Q}}(b)|_p + \eta_1|_p$ is in $Z^1(\mathbb{Q}_p, U)^{\mathrm{flat}}$ and let $\rho_{2,\mathrm{new}} := (0, 0, b, 0) \cdot \rho_2 \in \Pi_2^{\det}$. By construction, $\eta_{1,\mathrm{new}} = \eta_1 + \iota_{\mathbb{Q}}(b)$, and $\eta_{1,\mathrm{new}}|_p = \eta_1|_p + \iota_{\mathbb{Q}}(b)|_p$ is finite-flat. $\square$

Lemma 7.2.14. *Assume* $a^{(1)}|_{\ell_1} = 0$. *Then* $\Pi_2^{\det,p}$ *is non-empty.*

Proof. Let $\rho_2 \in \Pi_2^{\det}$ be as in Lemma 7.2.12. We claim that there is a cocycle $a \in \mathbb{Z}^1(\mathbb{Z}[1/Np], \mathbb{F}_p)$ such that $(a^{(2)'} + a)|_p$ is unramified. Assume this claim, and let $\rho_{2,\text{new}} = (a, -a, 0, 0) \cdot \rho_2$. As this action only changes $a^{(2)}$ and $d^{(2)}$, the representation $\eta_{1,\text{new}}$ for $\rho_{2,\text{new}}$ is identically equal to η_1, so it is finite-flat. The character $\chi_{2,\text{new}}$ for $\rho_{2,\text{new}}$ is given by

$$\chi_{2,\text{new}} = \left(1 + \epsilon a^{(1)'} + \epsilon^2 (a^{(2)'} + a)\right)|_p$$

and it is unramified because $(a^{(2)'} + a)|_p$ is unramified. By Lemma 7.2.11, $\rho_{2,\text{new}}|_p$ is finite-flat.

It remains to prove the claim that there is a cocycle $a \in \mathbb{Z}^1(\mathbb{Z}[1/Np], \mathbb{F}_p)$ such that $(a^{(2)'} + a)|_p$ is unramified. The fact that χ_2 is a character implies

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

This is the same as the coboundary of $\frac{1}{2}(a^{(1)'}|_p)^2$, so the difference $a' := \frac{1}{2}(a^{(1)'}|_p)^2 - a^{(2)'}|_p$ is a cocycle. Since the map

$$Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p) \to \frac{Z^1(\mathbb{Q}_p, \mathbb{F}_p)}{Z^1_{\text{un}}(\mathbb{Q}_p, \mathbb{F}_p)}$$

is surjective, there is $a \in Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p)$ such that $a' - a|_p$ is unramified. Thus, since $a^{(1)'}|_p$ is unramified, it follows that

$$(a^{(2)'} + a)|_p = \frac{1}{2}(a^{(1)'}|_p)^2 + (a' - a|_p)$$

is unramified. □

Let

$$(Z_b^1)^{\text{flat}} := Z_b^1 \cap Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1))^{\text{flat}} \subset Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1)).$$

Proposition 7.2.15. *For every pair of elements of* $\Pi_2^{\det,p}$, *the difference between their* $b^{(2)}$*-entries is contained in* $(Z_b^1)^{\text{flat}}$. *Moreover,* $(Z_b^1)^{\text{flat}}$ *is the span of* $b^{(1)}$ *and* $B^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1))$. *In particular,* $b|_{\ell_0} = 0$ *for all* $b \in (Z_b^1)^{\text{flat}}$.

Remark 7.2.16. In fact, the set of differences of the Proposition is equal to $(Z_b^1)^{\text{flat}}$, but we have no need of this result.

Proof. Let $\rho_2, \rho_{2,\text{alt}} \in \Pi_2^{\det,p}$. By Lemma 7.2.11, both $\eta_1|_p$ and $\eta_{1,\text{alt}}|_p$ are finite-flat.

As in the proof of Lemma 7.2.12, and with the notation used there, η_1 and $\eta_{1,\text{alt}}$ are identified with elements of $Z^1(\mathbb{Z}[1/Np], \text{Ad}^0(\eta))^{p-UT}$. Since they have equal coordinates other than $b^{(2)'}$, the difference $b^{(2)'} - b^{(2)'}_{\text{alt}}$ is in $Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1))$. As $\eta_1|_p$ and $\eta_{1,\text{alt}}|_p$ are finite-flat, the commutativity of the diagram in Sublemma 7.2.13 implies that $b^{(2)'} - b^{(2)'}_{\text{alt}} \in Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1))^{\text{flat}}$. On the other hand, Lemma 7.1.1(2) implies that $b^{(2)'} - b^{(2)'}_{\text{alt}} \in Z_b^1$. This proves that $b^{(2)} - b^{(2)}_{\text{alt}} \in (Z_b^1)^{\text{flat}}$, as desired.

When $x \in \mathbb{F}_p(1)$ is a basis, then $\{dx, b_p, b^{(1)}, b_0^{(1)}\}$ is a basis for $Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1))$. By Lemma 2.2.9, $\{dx, b^{(1)}, b_0^{(1)}\}$ is a basis for the subspace $Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1))^{\text{flat}}$. Since $b^{(1)}|_{\ell_0} = 0$ and $dx|_{\ell_0} = 0$, both $b^{(1)}$ and dx are in $(Z_b^1)^{\text{flat}}$. But, by Lemma 3.2.1 and Proposition 3.2.9, $b_0^{(1)}$ is not in Z_b^1, so $\{dx, b^{(1)}\}$ is a basis for $(Z_b^1)^{\text{flat}}$. □

The main result of this section, Proposition 7.2.1, follows immediately from Lemma 7.2.14 and Proposition 7.2.15.

7.3. **The US_N condition on ρ_2.** Finally, consider the subset $\Pi_2^{\mathrm{US}_N}$ of $\Pi_2^{\det,p}$ consisting of those ρ_2 which satisfying the US_N condition. This subset is cut out by local conditions as

$$\Pi_2^{\mathrm{US}_N} = \{\rho_2 \in \Pi_2^{\det,p} \mid \rho_2|_{\ell_i} \text{ is } \mathrm{US}_{\ell_i} \text{ for } i = 0,1\}.$$

Indeed, the US_N condition is simply the combination of the finite-flat condition at p along with the two US_{ℓ_i} conditions at ℓ_i, and the constant determinant condition actually follows from the US_N condition according to [WWE21, Prop. 3.8.3].

Recall $\alpha \in \mathbb{F}_p(1)$ from Definition 4.2.2. If $a^{(1)}|_{\ell_1} = 0$, then $\beta \in \mathbb{F}_p(2)$ as in Proposition 7.2.1 is defined.

Proposition 7.3.1. *If $a^{(1)}|_{\ell_1} = 0$ and $\alpha^2 + \beta = 0$, then $\Pi_2^{\mathrm{US}_N} = \Pi_2^{\det,p}$, and, in particular, $\Pi_2^{\mathrm{US}_N}$ is non-empty.*

Proof. By Proposition 7.2.1, $\Pi_2^{\det,p}$ is non-empty. Let $\rho_2 \in \Pi_2^{\det,p}$. We will first show that, if $\alpha^2 + \beta = 0$, then $\rho_2|_{\ell_0}$ is US_{ℓ_0}. Let $\sigma, \tau \in G_{\ell_0}$. It suffices to show that

$$(\rho_2(\sigma) - \omega(\sigma))(\rho_2(\tau) - 1)$$

is zero in E_2. Using the facts that $\omega|_{\ell_0} = 1$ and $b^{(1)}|_{\ell_0} = 0$, this product, written in coordinates, is

$$\begin{pmatrix} a^{(1)}(\sigma)\epsilon + a^{(2)}(\sigma)\epsilon^2 & b^{(2)}(\sigma)\epsilon \\ c^{(1)}(\sigma) + c^{(2)}(\sigma)\epsilon & d^{(1)}(\sigma)\epsilon + d^{(2)}(\sigma)\epsilon^2 \end{pmatrix} \cdot \begin{pmatrix} a^{(1)}(\tau)\epsilon + a^{(2)}(\tau)\epsilon^2 & b^{(2)}(\tau)\epsilon \\ c^{(1)}(\tau) + c^{(2)}(\tau)\epsilon & d^{(1)}(\tau)\epsilon + d^{(2)}(\tau)\epsilon^2 \end{pmatrix}$$
$$= \begin{pmatrix} (a^{(1)}(\sigma)a^{(1)}(\tau) + b^{(2)}(\sigma)c^{(1)}(\tau))\epsilon^2 & 0 \\ (c^{(1)}(\sigma)a^{(1)}(\tau) + d^{(1)}(\sigma)c^{(1)}(\tau))\epsilon & (c^{(1)}(\sigma)b^{(2)}(\tau) + d^{(1)}(\sigma)d^{(1)}(\tau))\epsilon^2 \end{pmatrix}.$$

Using the equations that

$$a^{(1)}|_{\ell_0} = \alpha \smile c^{(1)}|_{\ell_0},\ d^{(1)}|_{\ell_0} = -a^{(1)}|_{\ell_0},\ b^{(2)}|_{\ell_0} = \beta \smile c^{(1)}|_{\ell_0},$$

all instances of $a^{(1)}$, $d^{(1)}$, and $b^{(2)}$ can be replaced by appropriate multiples of $c^{(1)}$, and the formula simplifies to

$$(\rho_2(\sigma) - \omega(\sigma))(\rho_2(\tau) - 1) = \begin{pmatrix} (\alpha^2 + \beta)c^{(1)}(\sigma)c^{(1)}(\tau)\epsilon^2 & 0 \\ 0 & (\alpha^2 + \beta)c^{(1)}(\sigma)c^{(1)}(\tau)\epsilon^2 \end{pmatrix}$$

which vanishes by the assumption $\alpha^2 + \beta = 0$. This implies that $\rho_2|_{\ell_0}$ is US_{ℓ_0}.

It remains to show that $\rho_2|_{\ell_1}$ is US_{ℓ_1}. To do so, it will be convenient to change $c^{(2)}$ by adding an element of $B^1(\mathbb{Z}[1/Np], \mathbb{F}_p(-1))$ to it. This amounts to conjugating ρ_2 by an element of $E_2^\times$, which does not affect whether the US_{ℓ_1}-condition holds.

Note that $\omega|_{I_{\ell_1}} = 1$ and that $a^{(1)}|_{\ell_1}$, $d^{(1)}|_{\ell_1}$, and $c^{(1)}|_{\ell_1}$ are zero. By equation (iii) in Lemma 7.1.1, $c^{(2)}|_{\ell_1}$ is a cocycle. Since $H^1(\mathbb{Q}_{\ell_1}, \mathbb{F}_p(-1))$ vanishes, $c^{(2)}|_{\ell_1}$ is a coboundary. Therefore, by adding an element of $B^1(\mathbb{Z}[1/Np], \mathbb{F}_p(-1))$ to $c^{(2)}$ if necessary, we may and do assume $c^{(2)}|_{\ell_1} = 0$.

With this assumption, $\rho_2|_{\ell_1}$ can be written in coordinates as

$$\rho_2|_{\ell_1} = \begin{pmatrix} \omega\chi & b^{(1)}|_{\ell_1} + b^{(2)}|_{\ell_1}\epsilon \\ 0 & \chi^{-1} \end{pmatrix}$$

where $\chi = 1 + a^{(2)}|_{\ell_1}\epsilon^2 : G_{\ell_1} \to \mathbb{F}_p[\epsilon_2]^\times$ is a homomorphism. Since χ has order dividing p and the pro-p-abelian quotient of G_{ℓ_1} is generated by Frobenius, χ is unramified.

Let $\sigma \in G_{\ell_1}$, $\tau \in I_{\ell_1}$. Then $\chi(\tau) = 1$ and $\omega(\tau) = 1$, so

$$(\rho_2(\sigma) - \omega(\sigma))(\rho_2(\tau) - 1) =$$
$$\begin{pmatrix} \omega(\sigma)(\chi(\sigma)-1) & b^{(1)}(\sigma) + b^{(2)}(\sigma)\epsilon \\ 0 & \chi^{-1}(\sigma) - \omega(\sigma) \end{pmatrix} \cdot \begin{pmatrix} 0 & b^{(1)}(\tau) + b^{(2)}(\tau)\epsilon \\ 0 & 0 \end{pmatrix}$$

This equals zero because $\omega(\sigma)(\chi(\sigma) - 1) \in \epsilon^2 \mathbb{F}_p[\epsilon_2]$, which annihilates the B-coordinate $\mathbb{F}_p[\epsilon_1]$. On the other hand

$$(\rho_2(\tau) - \omega(\tau))(\rho_2(\sigma) - 1) =$$
$$\begin{pmatrix} 0 & b^{(1)}(\tau) + b^{(2)}(\tau)\epsilon \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} \omega(\sigma)\chi(\sigma) - 1 & b^{(1)}(\sigma) + b^{(2)}(\sigma)\epsilon \\ 0 & \chi^{-1}(\sigma) - 1 \end{pmatrix}.$$

This equals zero similarly, because $\chi^{-1}(\sigma) - 1 \in \epsilon^2 \mathbb{F}_p[\epsilon_2]$. Therefore, for all $\sigma, \tau \in G_{\ell_1} \times I_{\ell_1} \cup I_{\ell_1} \times G_{\ell_1}$,

$$(\rho_2(\sigma) - \omega(\sigma))(\rho_2(\tau) - 1) = 0$$

and so $\rho_2|_{\ell_1}$ is US_{ℓ_1}. □

Corollary 7.3.2. *Assume $a^{(1)}|_{\ell_1} = 0$ and $\alpha^2 + \beta = 0$. Then $\dim_{\mathbb{F}_p} R/pR > 3$.*

Proof. By Proposition 7.3.1, $\Pi_2^{\mathrm{US}_N}$ is non-empty. Let $\rho_2 \in \Pi_2^{\mathrm{US}_N}$, let $D_2 = \psi(\rho_2) : G_{\mathbb{Q},Np} \to \mathbb{F}_p[\epsilon_2]$ be the associated pseudorepresentation, and let $\phi_2 : R \to \mathbb{F}_p[\epsilon_2]$ be the local homomorphism induced by D_2 using the universal property of R. By construction, the composition of ϕ_2 with the quotient $\mathbb{F}_p[\epsilon_2] \twoheadrightarrow \mathbb{F}_p[\epsilon_1]$ is the map ϕ_1 of Lemma 4.3.2. Since ϕ_1 is surjective, this implies that ϕ_2 is surjective.

Recall the notation $S = R/(p, \mathfrak{m}^2)$ of Section 5.3; since S is a quotient of R/pR, it is enough to show that $\dim_{\mathbb{F}_p}(S) > 3$. The map ϕ_2 induces a surjective local-ring homomorphism $\phi_2 : S \twoheadrightarrow \mathbb{F}_p[\epsilon_2]$. Any element $y \in \mathfrak{m}_S$ such that $\phi_2(y) = \epsilon$ has $\phi_2(y^2) = \epsilon^2 \neq 0$, so $y^2 \in \mathfrak{m}_S^2$ is non-zero. Since $\dim_{\mathbb{F}_p}(R/(p, \mathfrak{m}^2)) = 3$ by Proposition 5.1.8, this implies

$$\dim_{\mathbb{F}_p}(S) = 3 + \dim_{\mathbb{F}_p}(\mathfrak{m}_S^2) > 3.$$ □

Combining this corollary with Proposition 6.4.1, we can prove the main theorem.

Theorem 7.3.3. *The $\mathbb{F}_p$-dimension of R/pR is greater than 3 if and only if*

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

Moreover, if $\dim_{\mathbb{F}_p} R/pR = 3$, the surjection $R \to \mathbb{T}$ of Proposition 2.2.15 is an isomorphism of reduced finite flat $\mathbb{Z}_p$-algebras of rank 3.

Proof. We prove the final statement first. Suppose $\dim_{\mathbb{F}_p} R/pR = 3$. Since R is complete and separated as a $\mathbb{Z}_p$-module, Nakayama's lemma implies that there is a surjection of $\mathbb{Z}_p$-modules $\mathbb{Z}_p^3 \twoheadrightarrow R$. On the other hand, $\mathbb{T}$ is a free $\mathbb{Z}_p$-module, and Ribet's Theorem 1.3.1 implies that $\mathrm{rk}_{\mathbb{Z}_p} \mathbb{T} \geq 3$. The surjectivity of the composition

$$\mathbb{Z}_p^3 \twoheadrightarrow R \twoheadrightarrow \mathbb{T}$$

then implies that $\mathrm{rk}_{\mathbb{Z}_p} \mathbb{T} = 3$, so the composition is an isomorphism. This implies that $R \twoheadrightarrow \mathbb{T}$ is an isomorphism.

Now we prove the first statement. One implication is immediate from Corollary 7.3.2. Conversely, assume $\dim_{\mathbb{F}_p} R/pR > 3$. Since $\dim_{\mathbb{F}_p} R/(p, \mathfrak{m}^2) = 3$ by Proposition 5.1.8, this implies $\dim_{\mathbb{F}_p} S > 3$ where $S = R/(p, \mathfrak{m}^3)$. By Corollary 5.3.3, this implies $\dim_{\mathbb{F}_p} S = 4$. By Lemma 6.2.9, this implies (1).

It remains to show that (2) holds when $\dim_{\mathbb{F}_p} S = 4$. Let $\rho_2 \in \Pi_2^{\mathrm{US}_N}$ be the element constructed in Corollary 6.4.6. By the construction and by Proposition 7.2.1, the element $\beta' \in \mathbb{F}_p(2)$ defined in Lemma 6.3.1 is equal to β. Since $\alpha^2+\beta' = 0$ by Proposition 6.4.1, this implies (2). □

8. The invariant $\alpha^2 + \beta$ is canonical

In this section, we prove that $\alpha^2+\beta$ is a canonical element of $\mu_p^{\otimes 2}$, when it exists. That is, we will show that it does not depend on the pinning data of Definition 1.7.1. This improves upon Theorem 7.3.3, which only implies that the *vanishing* of $\alpha^2 + \beta$ is independent of the pinning data of Definition 1.7.1.

8.1. **Formulation and outline of the proof.** First, we must make precise what we mean by "$\alpha^2 + \beta$ is a canonical element of $\mu_p^{\otimes 2}$". Up until this point, we have defined $\alpha^2 + \beta$ as an element of $\mathbb{F}_p(2)$, not of $\mu_p^{\otimes 2}$. Note the difference: $\mu_p \subset \overline{\mathbb{Q}}$ is the group of pth roots of unity, and a choice of primitive pth root of unity $\zeta \in \overline{\mathbb{Q}}$ defines an isomorphism

$$\phi_\zeta : \mathbb{F}_p(2) \to \mu_p^{\otimes 2}, \quad 1 \mapsto \zeta \otimes \zeta \tag{8.1.1}$$

of $\mathbb{F}_p[G_{\mathbb{Q}}]$-modules. Since the pinning data includes a choice primitive pth root of unity $\zeta \in \overline{\mathbb{Q}}$, for any choice of pinning data, we have an element $\phi_\zeta(\alpha^2 + \beta) \in \mu_p^{\otimes 2}$. When we say that $\alpha^2+\beta$ is a canonical, we mean that the $\phi_\zeta(\alpha^2+\beta)$ is independent of the choice of pinning data.

Theorem 8.1.2. *Make Assumption 1.3.2.*

(1) The condition $a^{(1)}|_{\ell_1} = 0$ does not depend on the pinning data.
(2) If $a^{(1)}|_{\ell_1} = 0$, then there is an element $\delta \in \mu_p^{\otimes 2}$ such that, for each choice of pinning data, $\alpha^2 + \beta = \phi_\zeta^{-1}(\delta)$, where $\zeta \in \overline{\mathbb{Q}}$ is the primitive pth root of unity given in the pinning data.

We explain the main ideas of the proof. The pinning data is mainly used in the paper in two ways: first, as a normalization factor to choose a particular Galois cohomology class that is only canonical up to scalar, and, second, to select cocycles within those normalized cohomology classes. Since α and β and defined in terms of these cocycles, their values could depend on pinning data. However, in a sense, we can think of α and β as being "ratios" of pairs of cocycles, and we show that, for most changes to the pinning data that affect the normalization, both elements in the pair are scalar by the same factor, and, as a result, the ratios α and β are unchanged. The only change of the pinning data that affects $\alpha^2 + \beta$ is changing the primitive pth root of unity ζ, and we show that change behaves as expected for an element of $\mu_p^{\otimes 2}$: changing ζ to ζ^a multiplies $\alpha^2 + \beta$ by a^{-2}.

The second kind of effect of the pinning data is to change the choice of cocycle within a cohomology class. This kind of change amounts to conjugating the representations ρ_1 and ρ_2. By Lemma 7.1.1, the condition $a^{(1)}|_{\ell_1} = 0$ can be interpreted in terms of the existence of a deformation ρ_2 of ρ_1, and this is unaffected by conjugation. In general, conjugation changes the value of α and β, but we show that the quantity $\alpha^2 + \beta$ is left unchanged.

To prove the theorem, we analyze the effect of changing each datum independently. In Section 8.2, we prove a general lemma about how α and β change under conjugation. In each of the remaining parts, we focus on a single changes to the pinning data, and compute its effect. We will use the following notation scheme:

- We maintain the same notation α, β, ρ_1, ρ_2, $a^{(1)}$, $b^{(1)}$, …, as in the earlier parts of the paper, computed with respect the pinning data fixed in Definition 1.7.1. Here ρ_2 denotes an arbitrary element of $\Pi_2^{\det,p}$, assuming it exists.
- We use primed notation α', β', ρ_1', ρ_2', $a^{(1)'}$, $b^{(1)'}$, …, for the same objects computed with respect to the altered pinning data under consideration at the time.

In particular, be warned that the meaning of the primed objects is variable (and they also differ from the primed objects considered in Section 7.2).

8.2. **Coordinate-wise calculation of conjugation of ρ_1 and ρ_2.** In this section, we compute the affect of conjugation on the representations ρ_1 and ρ_2 and their constituent cochains.

Let $M \in E_2^\times$ be an element of the form

$$M = \begin{pmatrix} A_0 + A_1\epsilon + A_2\epsilon^2 & B_0 + B_1\epsilon \\ C_0 + C_1\epsilon & 1 + D_1\epsilon + D_2\epsilon^2 \end{pmatrix}$$

with $A_i, B_i, C_i, D_i \in \mathbb{F}_p$, such that $\det(M) = A_0$, and also write M as $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$. The usual formula for inverting a 2×2-matrix is valid in E_2:

$$M^{-1} = A_0^{-1} \begin{pmatrix} D & -B \\ -C & A \end{pmatrix}$$

and for $N = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in E_2$, the conjugation $M^{-1}NM$ is given by

$$M^{-1}NM = A_0^{-1} \begin{pmatrix} ADa - \epsilon ABc + \epsilon CDb - \epsilon BCd & D^2b + BD(a-d) - \epsilon B^2c \\ A^2c + AC(d-a) - \epsilon C^2b & ADd - \epsilon CDb - \epsilon BCa + \epsilon ABc \end{pmatrix}$$

Let $M_1 \in E_1^\times$ be the image of M under the map $E_2 \to E_1$, and let $\rho_{1,M}$ and $\rho_{2,M}$ denote the conjugates of ρ_1 and ρ_2 (if it exists)

$$\rho_{1,M}(\sigma) = M_1^{-1}\rho_1(\sigma)M_1, \ \ \rho_{2,M}(\sigma) = M^{-1}\rho_2(\sigma)M.$$

Write these in coordinates as

$$\rho_{2,M} = \begin{pmatrix} \omega(1 + a_M^{(1)}\epsilon + a_M^{(2)}\epsilon^2) & b_M^{(1)} + b_M^{(2)}\epsilon \\ \omega(c_M^{(1)} + c_M^{(2)}\epsilon) & 1 + d_M^{(1)}\epsilon + d_M^{(2)}\epsilon^2 \end{pmatrix}$$

and similarly for $\rho_{1,M}$. Using the explicit formula for conjugation above, we can express these new cochains in terms of the original ones.

Lemma 8.2.1. *Let $M \in E_2^\times$ and $\rho_{1,M}$, $\rho_{2,M}$ be as above. Then*

$$b_M^{(1)} = A_0^{-1}\Big(b^{(1)} + B_0(\omega - 1)\Big) \tag{8.2.2}$$

$$c_M^{(1)} = A_0(c^{(1)} + A_0^{-1}C_0(\omega^{-1} - 1) \tag{8.2.3}$$

$$a_M^{(1)} = a^{(1)} - B_0c^{(1)} + A_0^{-1}C_0\omega^{-1}b^{(1)} - A_0^{-1}B_0C_0(\omega^{-1} - 1) \tag{8.2.4}$$

$$\begin{aligned} b_M^{(2)} &= A_0^{-1}\Big(b^{(2)} + (D_1 + A_0^{-1}A_1 + B_0C_0)b^{(1)} \\ &\quad + (B_1 - A_0^{-1}A_1B_0 + B_0^2C_0)(\omega - 1) + B_0(\omega a^{(1)} - d^{(1)}) - B_0^2\omega c^{(1)}\Big). \end{aligned} \tag{8.2.5}$$

Using this lemma, we can see how changes to the pinning data that cause ρ_1 and ρ_2 to be replaced by conjugates affect the values of $a^{(1)}|_{\ell_1}$ and $\alpha^2 + \beta$.

Lemma 8.2.6. *Consider a change to the pinning data that does not alter the decomposition group at ℓ_0 or the primitive pth root of unity ζ, and let G'_{ℓ_1} denote the decomposition group at ℓ_1 that is part of this new data. Suppose that the representation ρ'_1 computed with this respect to this new data is of the form $\rho'_1 = \rho_{1,M}$ for some $M \in E_2^\times$ as above. Then*

(1) $a^{(1)'}|_{G'_{\ell_1}} = 0$ if and only if $a^{(1)}|_{\ell_1} = 0$.

(2) if $a^{(1)}|_{\ell_1} = 0$, then $\alpha'^2 + \beta' = A_0^{-2}(\alpha^2 + \beta)$.

Proof. For part (1), note that, by Lemma 7.1.1, $a^{(1)}|_{\ell_1} = 0$ if and only if ρ_1 has a deformation ρ_2. If $a^{(1)}|_{\ell_1} = 0$, then ρ_2 exists, and $\rho_{2,M}$ gives a deformation of $\rho'_1 = \rho_{1,M}$, so $a^{(1)'}|_{G_{\ell_1}} = 0$. This argument is symmetric, so the other implication follows.

Now suppose $a^{(1)}|_{\ell_1} = 0$, so ρ_2 exists and we can define $\rho'_2 = \rho_{2,M}$, and β and β' are defined. Then α and β are defined by the formulas

$$a^{(1)}|_{\ell_0} = \alpha \cup c^{(1)}|_{\ell_0},\ b^{(2)}|_{\ell_0} = \beta \cup c^{(1)}|_{\ell_0}$$

and similarly for α' and β'. Since both pinning data have the same primitive pth root of unity ζ, we can and do use ζ to identify twists of $\mathbb{F}_p$ with $\mathbb{F}_p$. In this way, we can think of α and β as elements of $\mathbb{F}_p$ and think of this cup product as scalar multiplication.

Noting that $\omega|_{\ell_0} = 1$, $d^{(1)}|_{\ell_0} = -a^{(1)}|_{\ell_0}$, and $b^{(1)}|_{\ell_0} = 0$, the formulas of Lemma 8.2.1 give

$$\begin{aligned}
a^{(1)'}|_{\ell_0} &= a^{(1)}|_{\ell_0} - B_0 c^{(1)}|_{\ell_0} \\
c^{(1)'}|_{\ell_0} &= A_0 c^{(1)}|_{\ell_0} \\
b^{(2)'}|_{\ell_0} &= A_0^{-1}(b^{(2)}|_{\ell_0} + 2B_0 a^{(1)}|_{\ell_0} - B_0^2 c^{(1)}|_{\ell_0}).
\end{aligned}$$

Rearranging to write everything in terms of $c^{(1)'}|_{\ell_0}$ gives

$$\begin{aligned}
a^{(1)'}|_{\ell_0} &= A_0^{-1}(\alpha - B_0) c^{(1)'}|_{\ell_0} \\
b^{(2)'}|_{\ell_0} &= A_0^{-2}(\beta + 2B_0\alpha - B_0^2) c^{(1)'}.
\end{aligned}$$

In other words,

$$\alpha' = A_0^{-1}(\alpha - B_0), \quad \beta' = A_0^{-2}(\beta + 2B_0\alpha - B_0^2)$$

so $\alpha'^2 + \beta' = A_0^{-2}(\alpha^2 + \beta)$, as desired. ∎

In the next section, we will see that, for any such change to the pinning data, we have $\rho'_1 = \rho_{1,M}$ for an element M with $A_0 = \det(M) = 1$. Then the lemma implies Theorem 8.1.2 for these types of changes. Finally, we will deal with changes to the decomposition group at ℓ_0 and changes to ζ by separate arguments.

8.3. **Changes that affect ρ_1 by conjugation.** In this section, we consider the changes to the pinning data of the types allowed in Lemma 8.2.6. We maintain the same notation $\rho_{1,M}$ as in the previous section. We will often rely on Definition 3.1.1, which describes how the cocycles $b_0^{(1)}$, $b^{(1)}$, $c^{(1)}$, and a_0 as well as the elements $\gamma_0 \in I_{\ell_0}$ and $\gamma_1 \in I_{\ell_1}$ and the 0-cochain $x_{c^{(1)}}$ are determined by the pinning data. We also frequently use Lemma 4.2.1, which describes the cochain $a^{(1)}$.

Lemma 8.3.1 (Change of decomposition group at ℓ_1). *Let $G'_{\ell_1} \subset G_{\mathbb{Q},Np}$ be another choice of decomposition group at ℓ_1, and let ρ'_1 be the representation obtained by this change to the pinning data. Then $\rho'_1 = \rho_{1,M}$ where*

$$M = \begin{pmatrix} 1 & 0 \\ C_0 & 1 \end{pmatrix}$$

for some $C_0 \in \mathbb{F}_p$.

In particular, this change does not affect the condition $a^{(1)}|_{\ell_1} = 0$ and does not change the value of $\alpha^2 + \beta$.

Proof. The cocycle $b^{(1)}$ and the class c_0 of the cocycle $c^{(1)}$ do not depend on the choice of decomposition group at ℓ_1, so $b^{(1)'} = b^{(1)}$ and $c^{(1)'} - c^{(1)}$ is a coboundary. Therefore

$$c^{(1)'} = c^{(1)} + C_0(\omega^{-1} - 1)$$

for some $C_0 \in \mathbb{F}_p$. This implies

$$x_{c^{(1)'}} = x_{c^{(1)}} + C_0.$$

It remains to show that

$$a^{(1)'} = a^{(1)} - C_0\omega^{-1}b^{(1)}.$$

This follows from Lemma 4.2.1, as the defining properties (1)-(3) are easily checked with these values of $b^{(1)'}$, $c^{(1)'}$, and $x_{c^{(1)'}}$. (Alternatively, properties (1) and (2) correspond to properties of the resulting map ρ'_1 (that it be a homomorphism and be finite-flat at p, respectively) that are unchanged by conjugation.) The last statement is clear from Lemma 8.2.6. □

Next we consider the choice of decomposition group at p and the choice of root $\ell_1^{1/p}$ of ℓ_1 (or equivalently, the choice of cocycle $b^{(1)}$ in the class b_1). These cannot be considered completely independently because we insist that $b^{(1)}|_p = 0$ when $b_1|_p = 0$ (note that the condition $b_1|_p = 0$ is independent of the choice of decomposition group).

Lemma 8.3.2 (Change of decomposition group at p and change of root $\ell_1^{1/p}$ of ℓ_1). *Let $G'_p \subset G_{\mathbb{Q},Np}$ be a choice of decomposition group at p and let $b^{(1)'}$ be a choice of cocycle in the class b_1 of $b^{(1)}$ that satisfies*

$$b^{(1)'}|_{G'_p} = 0$$

if $b_1|_p = 0$. Let ρ'_1 be the representation obtained by this change to the pinning data. Then $\rho'_1 = \rho_{1,M}$ where

$$M = \begin{pmatrix} 1 & B_0 \\ 0 & 1 \end{pmatrix}$$

for some $B_0 \in \mathbb{F}_p$.

In particular, this change does not affect the condition $a^{(1)}|_{\ell_1} = 0$ and does not change the value of $\alpha^2 + \beta$.

Proof. The cocycles $b^{(1)'}$ and $b^{(1)}$ have the same class, so $b^{(1)'} = b^{(1)} + B_0(\omega - 1)$ for some $B_0 \in \mathbb{F}_p$. The cocycle $c^{(1)}$ does not depend on the choice of decomposition group at p or on the choice of root $\ell_1^{1/p}$ of ℓ_1, so $c^{(1)'} = c^{(1)}$. It remains to show that

$$a^{(1)'} = a^{(1)} - B_0c^{(1)}.$$

This follows from Lemma 4.2.1 just as in the last lemma. The last statement is clear from Lemma 8.2.6. □

Changing the root $\ell_0^{1/p}$ of ℓ_0 only changes the cocycle $b_0^{(1)}$ and does not affect $b^{(1)}$ or $c^{(1)}$, and consequently does not change $a^{(1)}$, α, or β.

8.4. **Change of decomposition group at ℓ_0.** Changing the decomposition group at ℓ_0 changes the element $\gamma_0 \in I_{\ell_0}$ that is used to normalize $c^{(1)}$. Hence it will scale $c^{(1)}$ by a factor. However, the following lemma shows that it changes $a^{(1)}$ and $b^{(2)}$ by the same factor.

Lemma 8.4.1. *Let $G'_{\ell_0} \subset G_{\mathbb{Q},Np}$ be another choice of decomposition group at ℓ_0, and let ρ'_1 be the representation obtained by this change to the pinning data. Then there is an element $A \in \mathbb{F}_p^\times$ such that*

$$b^{(1)'} = b^{(1)}$$
$$c^{(1)'} = Ac^{(1)}$$
$$a^{(1)'} = Aa^{(1)}.$$

In particular, this change does not affect the condition $a^{(1)}|_{\ell_1} = 0$.

If, moreover, $a^{(1)}|_{\ell_1} = 0$, then there is deformation $\rho'_2 \in {\Pi'}_2^{\det,p}$ such that

$$b^{(2)'} = Ab^{(2)}.$$

In particular, this change does not alter the value of α or β.

Proof. The cocycle $b^{(1)}$ does not depend on the choice of decomposition group at ℓ_0, so $b^{(1)'} = b^{(1)}$. Let $\sigma \in G_{\mathbb{Q}}$ be such that $G'_{\ell_0} = \sigma^{-1} G_{\ell_0} \sigma$.

A computation with cocycles[4] shows that, for all $\tau \in G_{\ell_0}$:

$$b_0^{(1)}(\sigma^{-1}\tau\sigma) = \omega(\sigma)^{-1}\left(b_0^{(1)}(\tau) + b_0^{(1)}(\sigma)(\omega(\tau)-1)\right)$$

In particular, letting $A_0 = \omega(\sigma)$ and $\gamma'_0 = \sigma^{-1}\gamma_0^{A_0}\sigma$, it follows that $b^{(1)}(\gamma'_0) = 1$.

The cocycle $c^{(1)'}$ is normalized so that $c^{(1)'}(\gamma'_0) = 1$. Formula (8.2.3) applied with $M_1 = \rho_1(\sigma)$ gives

$$c^{(1)}(\gamma'_0) = A_0^2$$

so $c^{(1)'} = A_0^{-2} c^{(1)}$. Letting $A = A_0^{-2}$, this gives $c^{(1)'} = Ac^{(1)}$.

Now we claim that

$$a^{(1)'} = Aa^{(1)}.$$

This follows from Lemma 4.2.1. Finally, if $a^{(1)}|_{\ell_1} = 0$, then we claim that

$$\rho'_2 = \begin{pmatrix} \omega(1 + Aa^{(1)}\epsilon + A^2 a^{(2)}\epsilon^2) & b^{(1)} + Ab^{(2)}\epsilon \\ \omega(Ac^{(1)} + Ac^{(2)}\epsilon) & 1 + Ad^{(1)}\epsilon + A^2 d^{(2)}\epsilon^2 \end{pmatrix}$$

is in ${\Pi'}_2^{\det,p}$. In order to prove the claim, we apply the implication (3) ⇒ (1) of Lemma 7.2.11. The η'_1 produced from ρ'_2 via (7.2.9), considered as an element of $Z^1(\mathbb{Z}[1/Np], \mathrm{Ad}^0(\eta'))$ via Lemma 2.2.11 where $\eta' = \eta_1 \pmod{\epsilon}$, has coordinates $A \cdot \left(\begin{smallmatrix} a^{(1)} & b^{(2)} \\ c^{(1)} & d^{(1)} \end{smallmatrix}\right)$. Since the subset of finite-flat at p lifts of η' is a subspace containing $\left(\begin{smallmatrix} a^{(1)} & b^{(2)} \\ c^{(1)} & d^{(1)} \end{smallmatrix}\right)$, it contains η'_1 as well.

[4]Note that this is the the same as the conjugation formula (8.2.2), and can also be proven in the same way.

Finally, since $a^{(1)}$, $c^{(1)}$, and $b^{(2)}$ are all scaled by the same factor, the values of α and β are left unchanged. ☐

8.5. **Changing the root of unity.** Finally, we check that changing the root of unity alters $\alpha^2 + \beta$ in the expected way.

Lemma 8.5.1. *Let $\zeta' \in \overline{\mathbb{Q}}$ denote another choice of primitive root of unity and let $A \in \mathbb{F}_p^\times$ be such that $\zeta = \zeta'^A$. Let ρ_1' be the representation obtained by this change to the pinning data. Then*

$$b^{(1)'} = Ab^{(1)}$$
$$c^{(1)'} = Ac^{(1)}$$
$$a^{(1)'} = A^2 a^{(1)}.$$

In particular, this change does not affect the condition $a^{(1)}|_{\ell_1} = 0$.

If, moreover, $a^{(1)}|_{\ell_1} = 0$, then there is deformation $\rho_2' \in {\Pi'}_2^{\det,p}$ such that

$$b^{(2)'} = A^3 b^{(2)}.$$

In particular, $\alpha' = A\alpha$ and $\beta' = A^2\beta$, and

$$\phi_{\zeta'}(\alpha'^2 + \beta') = \phi_\zeta(\alpha^2 + \beta).$$

where ϕ_ζ is as in (8.1.1)

Proof. Recall that $b^{(1)}$ is defined by the equation

$$\frac{\sigma \ell_1^{1/p}}{\ell_1^{1/p}} = \zeta^{b^{(1)}(\sigma)}$$

for all $\sigma \in G_{\mathbb{Q},Np}$. Replacing ζ by ζ'^A, it follows that $b^{(1)'} = Ab^{(1)}$. Similarly $b_0^{(1)'} = Ab_0^{(1)'}$.

The cocycle $c^{(1)'}$ is a scalar multiple of $c^{(1)}$, normalized such that $c^{(1)'}(\gamma_0') = 1$ where $\gamma_0' \in I_{\ell_0}$ satisfies $b_0^{(1)'}(\gamma_0') = 1$. Since $b_0^{(1)}(\gamma_0) = 1$ and $b_0^{(1)'} = Ab_0^{(1)}$, we can choose $\gamma_0' = \gamma_0^{A^{-1}}$. Given that $c^{(1)}(\gamma_0) = 1$, this shows that $c^{(1)'} = Ac^{(1)}$.

The fact that $a^{(1)'} = A^2 a^{(1)}$ follows immediately from Lemma 4.2.1. Similarly, it is easy to see that $b^{(2)'} = A^3 b^{(2)}$ satisfies differential equation (ii) in Proposition 7.3.1, and the fact that the resulting ρ_2 is finite-flat is clear.

The equations $\alpha' = A\alpha$ and $\beta' = A^2\beta$ follow immediately from the definitions and, since $\phi_\zeta = A^2\phi_{\zeta'}$, this shows that

$$\phi_{\zeta'}(\alpha'^2 + \beta') = \phi_{\zeta'}(A^2(\alpha^2 + \beta)) = \phi_\zeta(\alpha^2 + \beta). \qquad \square$$

References

[Bel12] Joël Bellaïche. Pseudodeformations. *Math. Z.*, 270(3-4):1163–1180, 2012.

[CE05] Frank Calegari and Matthew Emerton. On the ramification of Hecke algebras at Eisenstein primes. *Invent. Math.*, 160(1):97–144, 2005.

[Che14] Gaëtan Chenevier. The p-adic analytic space of pseudocharacters of a profinite group, and pseudorepresentations over arbitrary rings. In *Automorphic Forms and Galois Representations: Vol. I*, volume 414 of *London Mathematical Society Lecture Note Series*, pages 221–285. Cambridge Univ. Press, Cambridge, 2014. We follow the numbering of the online version `https://arxiv.org/abs/0809.0415v2`, which differs from the print version.

[CHT08] Laurent Clozel, Michael Harris, and Richard Taylor. Automorphy for some l-adic lifts of automorphic mod l Galois representations. *Publ. Math. Inst. Hautes Études Sci.*, (108):1–181, 2008. With Appendix A, summarizing unpublished work of Russ Mann, and Appendix B by Marie-France Vignéras.

[HWWE22] Catherine Hsu, Preston Wake, and Carl Wang-Erickson. Explicit non-Gorenstein $R = \mathbb{T}$ via rank bounds II: Computation. Preprint, available at `http://www.math.pitt.edu/~caw203/pdfs/RR3-Part2.pdf`. To appear Res. Number Theory as part of the proceedings of the Fifteenth Algorithmic Number Theory Symposium (ANTS-XV), 2022.

[KW09] Chandrashekhar Khare and Jean-Pierre Wintenberger. Serre's modularity conjecture. I. *Invent. Math.*, 178(3):485–504, 2009.

[Lec21] Emmanuel Lecouturier. Higher Eisenstein elements, higher Eichler formulas and rank of Hecke algebras. *Invent. Math.*, 223(2):485–595, 2021.

[Maz77] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977.

[Mer96] Loïc Merel. 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.

[Oht03] Masami Ohta. Congruence modules related to Eisenstein series. *Ann. Sci. École Norm. Sup. (4)*, 36(2):225–269, 2003.

[Poo17] Bjorn Poonen. *Rational points on varieties*, volume 186 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2017.

[Ram93] Ravi Ramakrishna. On a variation of Mazur's deformation functor. *Compositio Math.*, 87(3):269–286, 1993.

[Rib84] Kenneth A. Ribet. Congruence relations between modular forms. In *Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Warsaw, 1983)*, pages 503–514. PWN, Warsaw, 1984.

[Rib90] K. A. Ribet. On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms. *Invent. Math.*, 100(2):431–476, 1990.

[Rib10] Kenneth A. Ribet. Non-optimal levels of reducible mod ℓ Galois representations. Lecture at CRM, slides available at `https://math.berkeley.edu/~ribet/crm.pdf`, 2010.

[Rib15] Kenneth A. Ribet. Non-optimal levels of reducible mod ℓ Galois representations. Lecture at UCLA Number Theory Seminar, (notes by P. Wake), 2015.

[S$^+$18] W. A. Stein et al. *SageMath, the Sage Mathematics Software System (accessed online through CoCalc)*. The Sage Development Team, 2018. `http://www.sagemath.org`, `https://cocalc.com`.

[Sch12] René Schoof. Semistable abelian varieties with good reduction outside 15. *Manuscripta Math.*, 139(1-2):49–70, 2012.

[Ser87] Jean-Pierre Serre. Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. *Duke Math. J.*, 54(1):179–230, 1987.

[Wil95] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.

[WWE18] Preston Wake and Carl Wang-Erickson. Pseudo-modularity and Iwasawa theory. *Amer. J. Math.*, 140(4):977–1040, 2018.

[WWE19] Preston Wake and Carl Wang-Erickson. Deformation conditions for pseudorepresentations. *Forum Math. Sigma*, 7:e20, 2019.

[WWE20] Preston Wake and Carl Wang-Erickson. The rank of Mazur's Eisenstein ideal. *Duke Math. J.*, 169(1):31–115, 2020.

[WWE21] Preston Wake and Carl Wang-Erickson. The Eisenstein ideal with squarefree level. *Adv. Math.*, 380:Paper No. 107543, 62, 2021.

[Yoo19] Hwajong Yoo. Non-optimal levels of a reducible mod ℓ modular representation. *Trans. Amer. Math. Soc.*, 371(6):3805–3830, 2019.

Department of Mathematics & Statistics, Swarthmore College, Swarthmore, PA 19081, USA
Email address: chsu2@swarthmore.edu

Department of Mathematics, Michigan State University, East Lansing, MI 48824, USA
Email address: wakepres@msu.edu

Department of Mathematics, University of Pittsburgh, Pittsburgh, PA 15260, USA
Email address: carl.wang-erickson@pitt.edu