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
2. Recollection of pseudodeformation theory 10
3. Additional arithmetic preliminaries 20
4. An explicit first-order deformation 25
5. The pseudodeformation ring $R/pR$ up to second order 30
6. Galois-theoretic implications of $\dim_{\mathbb{F}} R/pR \geq 4$ 34
7. Constructing a second-order $US_N$ deformation $\rho_2$ 41
8. The invariant $\alpha^2 + \beta$ is canonical 51
References 57

1. INTRODUCTION

1.1. Summary. 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, $\omega$ 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 $N$:

1. $\ell_0$ is a prime number with $\ell_0 \equiv 1 \pmod{p}$, and
2. $\ell_1$ is a prime number with $\ell_1 \not\equiv 0, \pm 1 \pmod{p}$, such that $\ell_1$ is a $p$th power modulo $\ell_0$.
3. there is a unique cuspidal $f$ of level $\ell_0$ that is congruent to the Eisenstein series modulo $p$.

By a theorem of Ribet [Rib10, Rib15, Yoo19], restated as Theorem 1.2.1 below, conditions (1) and (2) imply that there is a newform of level $N$ with reducible

---

2020 Mathematics Subject Classification. 11F80, 11F33.
Key words and phrases. Galois representations, modular forms, non-optimal level, $R = \mathbb{T}$ theorem.
residual Galois representation $\bar{\rho}$, and condition (3) ensures that the space of oldforms is as small as possible. Moreover, under these conditions on $N$, the algebra $\mathcal{T}$ is expected to be non-Gorenstein (and this is borne out computationally), and so we focus on this case because it is the simplest situation we can find that exhibits this non-Gorenstein behaviour. We intend that the methods developed here might serve as a prototype for more general residually reducible contexts.

Now, condition (3) is equivalent to the non-vanishing of an easily-computed numerical invariant called Merel’s number, due to a deep theorem of Merel [Mer96] (see Remark 1.2.3). Our main result can be thought of as an analog of Merel’s theorem at level $N$. Indeed, the standard techniques that are used to prove that the surjection $\mathcal{R} \rightarrow \mathcal{T}$ is an isomorphism do not apply in our setting because $\mathcal{T}$ is not a local complete intersection. Instead, we prove $\mathcal{R} = \mathcal{T}$ using rank bounds. The $\mathbb{Z}_p$-rank of $\mathcal{T}$ is at least 3: there is the Eisenstein series, the unique cuspform of level $\ell_0$, and at least one newform of level $N$. We define invariants $a^{(1)}(\text{Fr}_{\ell_1})$ and $\alpha^2 + \beta$ in $\mathbb{F}_p$, discussed more in Section 1.3.1 below, which play the role of Merel’s number in that they control whether or not the newform of level $N$ is unique.

**Theorem 1.1.1** (Theorem 7.3.3). Let $p \geq 5$ and assume that the level $N$ satisfies conditions (1)-(3). The $\mathbb{F}_p$-dimension of $\mathcal{R}/p\mathcal{R}$ is greater than 3 if and only if both

(i) $a^{(1)}(\text{Fr}_{\ell_1}) = 0$
(ii) $\alpha^2 + \beta = 0$.

Moreover if one of (i) or (ii) fails, then the map $\mathcal{R} \rightarrow \mathcal{T}$ is an isomorphism, the $\mathbb{Z}_p$-rank of $\mathcal{T}$ is 3, and there is a unique newform of level $N$ that is congruent to the Eisenstein series modulo $p$.

This method for proving $\mathcal{R} = \mathcal{T}$ is novel. It differs significantly from the method of the paper [WWE21] in which $\mathcal{R}$ is formulated, the surjection $\mathcal{R} \rightarrow \mathcal{T}$ is established, and similar $\mathcal{R} = \mathcal{T}$ results for the representation $\bar{\rho}$ and certain squarefree levels $N$ are proven. In [WWE21], the theorems rely on conditions designed to force the rings $\mathcal{R}$ and $\mathcal{T}$ to be local complete intersections. Then, the crux of the method of [WWE21] is to verify Wiles’s numerical criterion [Wil95, Appendix], which relies on the complete intersection property and only uses information about $\mathcal{R}$ that corresponds to first-order deformations of pseudorepresentations. First-order calculations are also used to give a Galois-deformation-theoretic proof of Merel’s theorem in [WWE20].

To prove Theorem 1.1.1, first order deformations are no longer sufficient: they can be used to prove that $\dim_{\mathbb{F}_p} \mathcal{R}/p\mathcal{R} \geq 3$, but cannot give an upper bound. Instead, we show that $\dim_{\mathbb{F}_p} \mathcal{R}/p\mathcal{R} > 3$ if and only if certain second-order deformations exist. We set up technology that links the existence of second-order deformations of pseudorepresentations to the vanishing of cup products and triple Massey products in Galois cohomology, deploying the framework of tangent and obstruction theory for pseudorepresentations developed by the third-named author in [WE18]. We extract from these products the numerical invariants appearing in Theorem 1.1.1. To establish the theorem, we prove that these invariants are the only obstructions to constructing the required second-order deformations. In this sense, we carry out a fine-grained computation of $\mathcal{R}/p\mathcal{R}$ modulo the cube of the maximal ideal.

---

1Mazur’s theorem [Maz77] implies that there is at least one such cuspform.
In the second paper [HWWE23] in this series, we interpret the vanishing of $a^{(1)}(F_{\ell_1})$ and $\alpha^2 + \beta$ in terms of algebraic number theory and use this description to develop algorithms that determine whether or not these invariants vanish. Specifically, we show that the condition $\alpha^2 + \beta = 0$ can be detected by the splitting behaviour of primes in an explicit three-step solvable extension of $\mathbb{Q}(\zeta_p)$ that has degree $p^4$. We give an implementation of this algorithm in Sage [S+18] and compile data from computer experiments showing that the rank of $R$ is exactly 3 whenever the rank of $T$ is. We regard the second paper as an important proof of feasibility and applicability of the framework for computing with $R$ that is developed in this paper.

1.1.1. Toward $R = T$ beyond rank 3. One potential drawback of our main theorem is that it only establishes $R = T$ when the rank of $T$ is 3. We believe that $R = T$ regardless of the rank of $T$, but proving this will require new results on both the Hecke and Galois sides. To see why, it is instructive to revisit the prime level case.

In the prime level case, Mazur [Maz77] originally raised the question about the arithmetic significance of the rank of the analogous Hecke algebra. Merel used modular symbols—that is, Hecke-theoretic techniques—to prove his criterion for when the rank is one. More recently, Lecouturier [Lec21] gave a Hecke-theoretic interpretation of the rank in general. Calegari and Emerton [CE05] used deformation theory—that is, Galois-theoretic techniques—to give a criterion for when the rank is one, and the work of the second and third-named authors [WWE20] gave a Galois-theoretic interpretation of the rank in general. The fact that the two methods arrive at the same answer is closely related to a case of the equivariant main conjecture of Iwasawa theory (see [Wak23]).

In this paper, the starting point is a Hecke-side result: Ribet’s proof that the rank of $T$ is at least 3. We expect that there is an Hecke-side formula for the rank of $T$ in general, along the lines of [Lec21]. The techniques of this paper could be used to give a Galois-side formula for the dimension of $R/pR$ more generally. The fact that these formulas should give the same answer is an Iwasawa-theory-type phenomenon, but it is not part of any conjectural framework (as far as we are aware). We hope and expect that is part of a rich theory that has yet to be discovered.

1.2. Setup. Let $p \geq 5$ be a prime and let $\bar{\rho}$ be 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. For an integer $M$, we say that $\bar{\rho}$ is modular of level $M$ if there is a (cuspidal) newform $f$ of weight 2 and level $\Gamma_0(M)$ such that the residual pseudorepresentation of $f$ is $\bar{\rho}$. For an irreducible residual representation, the question of which levels it is modular for (if any) is the subject of Serre’s conjecture [Ser87], proven by Khare–Wintenberger [KW09] and of level-raising and level-lowering results of Ribet [Rib84, Rib90]. For reducible residual representations, like $\bar{\rho}$, the situation is much different. For example, in Mazur’s landmark paper on the Eisenstein ideal [Maz77], he proves that, for any prime $\ell$, $\bar{\rho}$ is modular of level $\ell$ 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 with respect to divisibility.
Ribet [Rib10] (see also [Yoo19]) initiated the study of level raising for $\bar{\rho}$. 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 1.2.1** (Ribet). If $\ell_0$ is a prime such that $\ell_0 \equiv 1 \pmod{p}$ and $\ell_1 \neq \pm 1$ is another prime, then $\bar{\rho}$ is modular of level $\ell_0\ell_1$ if and only if $\ell_1$ is a $p$th power modulo $\ell_0$.

The key thing to note about this result is that, unlike in the residually irreducible case [Rib84], the level-raising condition on the prime $\ell_1$ depends not just on $\ell_1$ and $\bar{\rho}$, but also on $\ell_0$.

**Assumption 1.2.2.** Now, and for the rest of the paper, we specialize to level $N = \ell_0\ell_1$, where $\ell_0$ and $\ell_1$ are primes such that

1. $\ell_0 \equiv 1 \pmod{p}$,
2. $\ell_1 \neq 0, \pm 1 \pmod{p}$ and $\ell_1$ is a $p$th power modulo $\ell_0$, and
3. there is a unique cusp form $f$ of level $\ell_0$ that is congruent to the Eisenstein series modulo $p$.

By Ribet’s Theorem 1.2.1, (1) and (2) imply that $\bar{\rho}$ is modular of level $N$.

**Remark 1.2.3.** The number of cusp forms of level $\ell_0$ that are congruent to the Eisenstein series is well understood [Mer96, CE05, Lec21, WWE20] and there is a numerical equivalent to assumption (3) as follows. Let $\log_{\ell_0}: \mathbb{F}_p^\times \to \mathbb{F}_p$ be a surjective homomorphism (that is, a discrete logarithm). Then *Merel’s number* is the quantity

$$\sum_{i=1}^{\ell_0 - 1} i \log_{\ell_0}(i) \in \mathbb{F}_p.$$ 

By Merel’s Theorem [Mer96, Théorème 2], the assumption (3) is equivalent to Merel’s number being non-zero.

1.2.1. *The Hecke algebra and congruence with Eisenstein series.* Note that the trace of $\bar{\rho}(Fr_\ell)$, where $Fr_\ell$ is an arithmetic Frobenius element $Fr_\ell \in G_\mathbb{Q}$ 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 $\ell$th Hecke operator $T_\ell$ on the Eisenstein series $E_2$ of weight 2 and level 1. (Although the form $E_2$ is non-holomorphic, it has a holomorphic stabilization to any level $M$ with $M > 1$.) Hence, for an integer $M > 1$, $\bar{\rho}$ is modular of level $M$ if there is a newform $f$ of level $M$ such that for all $n$ prime to $M$, $a_n(f)$ is congruent to $a_n(\bar{E}_2)$ modulo a prime above $p$. In particular, if $M$ is squarefree with $t \geq 1$ prime divisors, there are $2^t - 1$ Eisenstein series of level $M$, all of which are stabilizations of $E_2$. As such, when $M$ is not prime, we need to specify the eigenvalues of Hecke operators at primes dividing $M$, thereby selecting a single Eisenstein series of level $M$, before setting up a bijection between eigenforms and pseudorepresentations.

Now let $M = N = \ell_0\ell_1$. There is a 3-dimensional space of Eisenstein series of weight 2 and level $\Gamma_0(N)$, all having $T_\ell$-eigenvalue $\ell + 1$ for $\ell \nmid N$. As in the paper [WWE21], we choose a basis of eigenforms for the Atkin–Lehner involutions $w_{\ell_0}$ and $w_{\ell_1}$. The possible pairs of eigenvalues of the Eisenstein series under the Atkin–Lehner operators $(w_{\ell_0}, w_{\ell_1})$ are $(-1, -1), (-1, 1), (1, -1)$. However, it is known that a level $\Gamma_0(N)$ newform that is congruent to an Eisenstein series must have
Let $T'$ be the $\mathbb{Z}_p$-algebra acting on modular forms of weight 2 and level $\Gamma_0(N)$ with coefficients in $\mathbb{Z}_p$ that is generated by the operators $T_\ell$ for $\ell \nmid N$ along with the Atkin–Lehner involutions $w_{\ell_0}$ and $w_{\ell_1}$. Let $\mathbb{T}$ be the completion of $T'$ at the maximal ideal generated by $p$ and the annihilator of $E_{2,N}$, and let $\mathbb{T}^0$ be the largest quotient of $\mathbb{T}$ that acts faithfully on cusp forms. By Ribet’s Theorem 1.2.1, 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 cusp form of level $\ell_0$, specified in (3) above, that has Atkin–Lehner eigenvalues $(-1,-1)$,
- the newform of level $N$ arising from Ribet’s theorem, which has $\mathbb{Z}_p$-rank at least 1.

1.2.2. Residually reducible modularity lifting and imposing conditions at $N$. By Ribet’s Theorem 1.2.1, we know that $\bar{\rho}$ is modular of level $N$, so we can ask about modularity lifting. Let $R_{\text{univ}}$ 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 $R_{\text{univ}} \twoheadrightarrow \mathbb{T}$ (see [WWE21, §4.1]).

To formulate a modularity lifting theorem, we must then define a level $N$ quotient $R_N$ of $R_{\text{univ}}$ 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 $\rho$ to “look modular of level $N$,” we want it to satisfy the following conditions. Such $\rho$ are exactly those parameterized by $R$.

1. $\det(\rho) = \kappa_{\text{cyc}}$, the $p$-adic cyclotomic character (weight 2)
2. $\rho$ is finite-flat at $p$ (geometricity)
3. $\rho$ is unramified or Steinberg at $\ell_0$ and $\ell_1$ (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 indecomposable, and because it involves $p$-integritically interpolating between two conditions, unramified and Steinberg, that do not overlap in characteristic 0.

In [WWE21], a candidate definition of (3), called unramified-or-Steinberg, is made. The rough idea of this definition is as follows. A two-dimensional representation $\rho$ is Steinberg at $\ell$ if there is an isomorphism

$$\rho|_\ell \sim \begin{pmatrix} \kappa_{\text{cyc}} & * \\ 0 & 1 \end{pmatrix}$$

on the restriction $\rho|_\ell$ to a decomposition group at $\ell$. This implies that, for all $\sigma$ and $\tau$ in the decomposition group, the expression

$$\rho(\sigma) - \kappa_{\text{cyc}}(\sigma)(\rho(\tau) - 1)$$

is zero.
is zero. Indeed, the form of the Steinberg representation implies that (1.2.4) is conjugate to a matrix product of the form
\[
\begin{pmatrix}
0 & * \\
0 & *
\end{pmatrix}
\cdot
\begin{pmatrix}
* & * \\
0 & 0
\end{pmatrix}
= 
\begin{pmatrix}
0 & 0 \\
0 & 0
\end{pmatrix}.
\]
On the other hand, if \( \rho \) is unramified at \( \ell \), then the expression (1.2.4) may not be zero because the Frobenius eigenvalues of \( \rho \) need not be \( \ell \) and 1. However, if \( \sigma \) is in the inertia group at \( \ell \), then (1.2.4) is zero, simply because the term \( \rho(\sigma) - \kappa_{\text{cyc}}(\sigma) \) is zero. Similarly, if \( \tau \) is in the inertia group, then \( \rho(\tau) - 1 \) is zero, so (1.2.4) is zero. Hence, if \( \rho \) is either unramified or Steinberg at \( \ell \), then the expression (1.2.4) is zero for all pairs \((\sigma, \tau)\) in the decomposition group with at least one of \( \sigma \) and \( \tau \) in the inertia group. A pseudorepresentation is defined to be unramified-or-Steinberg at \( \ell \) if its determinant character is unramified and it comes from a Cayley-Hamilton representation \( \rho \) satisfying (1.2.4) for all such pairs \((\sigma, \tau)\); this corrects an error in the definition of unramified-or-Steinberg in the second- and third-named authors’ previous paper \[WWE21, \S 3.4\]. See \$2.2.4 for more details of this correction.

As an initial check that the definition of unramified-or-Steinberg is reasonable, it is shown in \[WWE20\] that there is a surjective homomorphism \( R_M \twoheadrightarrow T_M \); that is, Galois representations arising from modular forms of level \( M \) are unramified-or-Steinberg at the primes dividing \( M \). Moreover, several theorems in \[WWE21\] establish that, in many cases at many squarefree levels \( M \), this is the right definition of (3), in that \( R_M \cong T_M \). However, in all of the cases of \( R_M \cong T_M \) proved in \[WWE21\], the rings \( R_M \) and \( T_M \) are local complete intersection. One of the motivations for this paper is to provide evidence that the definition of unramified-or-Steinberg given in \[WWE21\] and clarified in \$2.2.4 is the right one, even in more pathological cases.

1.3. Main results: bounding the rank of \( R \). Our main result shows that \( R \cong T \) under certain, numerically verifiable conditions, thereby supplying evidence that \( R \cong T \) in general.

Since \( T \) 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 \( R \twoheadrightarrow T \) is an isomorphism. Instead, we use a new strategy: we prove that \[
\dim_{\mathbb{F}_p} R/pR \leq \operatorname{rank}_{\mathbb{Z}_p} T.
\]
Because \( R \) is \( p \)-adically separated, a separated version of Nakayama’s lemma then implies that \( R \twoheadrightarrow T \) is an isomorphism. As discussed above, we have made assumptions that ensure that \( \operatorname{rk}_{\mathbb{Z}_p} T \geq 3 \). Hence our goal is to find conditions under which \( \dim_{\mathbb{F}_p} R/pR \leq 3 \), for this will imply that \( R \cong T \).

1.3.1. 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 \( \ell_0 \)) and a “new irreducible vector.”
Under condition (3) in Assumption 1.2.2, we show 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 \( \ell_1 \)
- the cocycle \( c^{(1)} \in Z^1(G_{\mathbb{Q},Np}, \mathbb{F}_p(-1)) \) is ramified only at \( \ell_0 \)
- the cochain \( a^{(1)} : G_{\mathbb{Q},Np} \to \mathbb{F}_p \) satisfies \(-da^{(1)} = b^{(1)} - c^{(1)} \).

To make sense of this (and to explain the notation), we think of a generalized matrix algebra
\[
(1.3.1)\quad p_1 = \begin{pmatrix} \omega(1 + a^{(1)}/(1) + b^{(1)}) & b^{(1)} \\ \omega c^{(1)} & 1 + d^{(1)/2} \end{pmatrix},
\]
where \( d^{(1)} = b^{(1)} - c^{(1)} \), 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 \( \epsilon \) (see §4.1 below for a formal discussion of these generalized matrix algebras). To determine if \( p_1 \) deforms to second order, we write down a putative deformation
\[
(1.3.2)\quad p_2 = \begin{pmatrix} \omega(1 + a^{(1)/2} + a^{(2)/2} + c^{(2)/2}) & b^{(1)/2} + b^{(2)/2} \\ \omega c^{(1)/2} + c^{(2)/2} & 1 + d^{(1)/2} + d^{(2)/2} \end{pmatrix}
\]
with \( \epsilon^3 = 0 \) and write down the conditions that the new cochains \( a^{(2)}, b^{(2)}, c^{(2)}, d^{(2)} \) must satisfy for \( p_2 \) to define a map \( R \to \mathbb{F}_p[\epsilon]/(\epsilon^3) \). We find that, in order for \( p_2 \) to exist as a generalized matrix algebra representation, we must have
- \( a^{(1)/2} |_{\ell_1} = 0 \)
and that if any deformation \( p_2 \) exists, it can be arranged to satisfy
- \( a^{(1)/2} |_{\ell_0} = \alpha c^{(1)/2} |_{\ell_0} \) for some \( \alpha \in \mathbb{F}_p \),
- \( b^{(2)/2} |_{\ell_0} = \beta c^{(1)/2} |_{\ell_0} \) for some \( \beta \in \mathbb{F}_p \),

where “|\( \ell \)” indicates restriction to the decomposition group at \( \ell \). In addition, for \( p_2 \) to be unramified-or-Steinberg at \( \ell_0 \), 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 \( a^2 + \beta = 0 \) are independent of the choices. Actually, in §8, we show more: \( \alpha^2 + \beta \) arises from a canonical element of the 1-dimensional \( \mathbb{F}_p \)-vector space \( \mu_p \otimes \mu_p \), where \( \mu_p \subset \mathbb{Q}^\times \) are the \( p \)th roots of unity.

1.3.2. Main results. The proof of this paper’s main theorem relies on showing that there exists \( p_2 \) as in (1.3.2) 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 \( R/pR \cong \mathbb{F}_p[x, y]/(x^2, xy, y^2) \), with \( \mathbb{F}_p \)-dimension 3. The main result is Theorem 1.1.1, which we restate here for convenience.

**Theorem 1.3.3** (Theorem 7.3.3). Let \( p \geq 5 \). The \( \mathbb{F}_p \)-dimension of \( R/pR \) is greater than 3 if and only if both

(i) \( a^{(1)} |_{\ell_1} (\mathbb{F}_{\ell_1}) = 0 \) and
(ii) \( a^2 + \beta = 0 \),
where \( a^{(1)} \) and \( \alpha^2 + \beta \) are as defined in Section 1.3.1. 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

\[
R \twoheadrightarrow T
\]

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 [HWWE23], 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 1.3.4.** Let \( p = 5 \) and \( \ell_0 = 11 \). Then for

\[
\ell_1 = 23, 67, 263, 307, 373, 593, 857, 967, 1013,
\]

condition (i) of Theorem 1.3.3 holds, but condition (ii) does not. In particular, for these values of \( \ell_1 \), the \( \mathbb{F}_p \)-dimension of \( R/pR \) equals 3 and \( R \cong T \).

For \( \ell_1 = 43, 197, 683, 727 \), conditions (i) and (ii) of Theorem 1.3.3 both hold. Consequently, the \( \mathbb{F}_p \)-dimension of \( R/pR \) exceeds 3 for these values of \( \ell_1 \).

**Remark 1.3.5.** For the values of \( p \) and \( N \) where we found \( \dim_{\mathbb{F}_p} R/pR > 3 \), we also computed \( \dim_{\mathbb{F}_p} T/pT > 3 \). This is consistent with the expectation that \( R \cong T \).

To summarize Theorem 1.3.4, in all of the examples we computed, we find that one of the following cases occurs, witnessing the main Theorem 1.3.3.

- We compute in number field extensions and determine that both (i) and (ii) of Theorem 1.3.3 are true. In addition, we independently compute with modular symbols and determine that \( \rk_{\mathbb{Z}_p}(T) \geq 4 \).
- We compute in number field extensions and determine that, of the conditions of Theorem 1.3.3, (i) is true but (ii) is false. In addition, we independently compute that \( \rk_{\mathbb{Z}_p}T = 3 \). Theorem 1.3.3 tells us that \( R \cong T \) in this case.

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

**Conjecture 1.3.6.** For any prime \( p \) and squarefree level \( M \) as in Section 1.2.2, we have \( R_M \cong T_M \).

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 \( \text{"} R_M^\varepsilon = T_M^\varepsilon \text{"} \) as \( \varepsilon \) varies over sets of Atkin–Lehner eigenvalues, as in [WWE21, §1.9.1].

**1.4. Organization of the paper.** In order to organize non-canonical choices in one place, the notion of *pinning data* is set up in Definition 1.6.1. 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 [WWE21]. Section 3 continues with several lemmas and definitions in arithmetic and Galois representations that extend the content of Section 2, going beyond what appears in [WWE21]. Section 4 sets up the first-order deformation \( \rho_1 \) of (1.3.1) above. Section 5 produces an explicit formula for \( R/pR \) up to
second order, and Section 6 applies this in order to prove the “only if” direction of
the main Theorem 1.3.3. Section 7 proves the other logical direction by construct-
ing by hand a level \( N \) deformation \( \rho_2 \) of \( \rho_1 \) as in (1.3.2). Section 8 proves that the
invariant \( \alpha^2 + \beta \) is canonical by showing that the pinning data does not affect it.

1.5. Acknowledgements. The first-named author would like to thank the Uni-
versity of Bristol and the Heilbronn Institute for Mathematical Research for its
partial support of this project. The second-named author was supported in part
by NSF grant DMS-1901867 and NSF CAREER grant DMS-2337830. The third-
named author was supported in part by Simons Foundation award 846912 and NSF
grant DMS-2401384, 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 Swar-
more College through the computing resources provided. Specifically, this work
used the H2P cluster at the University of Pittsburgh, which is supported by NSF
award number OAC-2117681.

1.6. 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 \( \text{R} \Gamma(G, -) \) denote the class of
\( C^\bullet(G, -) \) in the derived category. Let \( x \mapsto [x] \) denote the quotient map \( \text{Z}^i(G, -) \to 
H^i(G, -) \). Let \( \cup \) denote the cup product on \( C^\bullet(G, -) \) and \( \cup \) for the induced map
on \( H^\bullet(G, -) \).

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 \( \text{Spec}(R) \), and similarly for
\( \text{H}^i(R, -) \), \( \text{Z}^i(R, -) \), \( \text{B}^i(R, -) \), and \( \text{R} \Gamma(R, -) \).

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
\( G_{\mathbb{Q}, Np} := \text{Gal}(\mathbb{Q}_S/\mathbb{Q}) \).

For each prime number \( q \), let \( \overline{\mathbb{Q}}_q/\mathbb{Q}_q \) be an algebraic closure and let \( G_q := 
\text{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q) \). Let \( I_q \subset G_q \) be the inertia group and let \( I_q^{\text{tame}} \) be the tame quotient.
When \( q \neq p \), let \( \gamma_q \in I_q \) denote a lift along \( I_q \to I_q^{\text{tame}} \) of a topological generator
of \( I_q^{\text{tame}} \).

Let \( \mu_p \subset \overline{\mathbb{Q}}^x \) denote the subgroup of \( p \)th roots of unity, and let \( \omega : G_{\mathbb{Q}, Np} \to \mathbb{F}_q^x \)
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 \( \omega \).

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 1.3.3 is independent of the pinning data.

**Definition 1.6.1.** 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 \( p \)th root of unity \( \zeta_p \in \overline{\mathbb{Q}}_q \),
- for \( i = 0, 1 \), a \( p \)th root \( \ell_1^{1/p} \in \overline{\mathbb{Q}}_q \) of \( \ell_1 \), such that, if possible, the image of \( \ell_1^{1/p} \)
in \( \overline{\mathbb{F}}_p \), 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 $N_p$, a decomposition subgroup of $q$ in $G_{Q,N_p}$ and an isomorphism between this subgroup and $G_q$, and
- for each $n \in \mathbb{Z}$, isomorphisms $F_p(\tau) \sim \mu_p \otimes n$.

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

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

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 §1.2.1. Note that since we fix this choice of Atkin–Lehner signs throughout this paper, we omit the superscript $\varepsilon$ found in the notation throughout [WWE21].

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

$$T_q, \text{ for } q \nmid N \text{ prime, and}$$
$$w_\ell, \text{ for } \ell \mid N \text{ prime,}$$

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

As remarked in §1.2.1, the space $\text{Eis}_2(\Gamma_0(N))$ of Eisenstein series of weight 2 and level $\Gamma_0(N)$ is 3-dimensional, and our choice of $(w_{\ell_0}, w_{\ell_1})$-eigenvalues $\varepsilon = (-1, -1)$ specifies a unique normalized Hecke eigenform $E_{2,N}$. It has $T_q$-eigenvalue $q + 1$ for all primes $q \nmid N$, and the constant term of its $q$-expansion at infinity is

$$a_0(E_{2,N}) = \frac{1}{2} \zeta(-1) \prod_{\ell|N} (\ell - 1) = -\frac{1}{24} \prod_{\ell|N} (\ell - 1).$$

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

- Let $\mathcal{T}$ denote the completion of $\mathcal{H}_N$ at its maximal ideal $(p, \text{Ann}_{\mathcal{H}_N}(E_{2,N}))$. Its residue field is $\mathbb{F}_p$, because $\mathcal{H}_N/\text{Ann}_{\mathcal{H}_N}(E_{2,N}) \cong \mathbb{Z}$.
- Let $\mathcal{T}^0$ be the cuspidal quotient of $\mathcal{T}$. 
Let \( I := \text{Ann}_{\mathbb{T}}(E_{2,N}) \cdot \mathbb{T} \), 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 [Oht14, Theorem 3.1.3] has proved that
\[
\mathbb{T}^0/I^0 \cong \mathbb{Z}_p/a_0(E_{2,N})\mathbb{Z}_p.
\]

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

Let \( M_2(N;\mathbb{Z}_p)_{\text{Eis}} \) 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 \( E_{2,N} \). Let \( S_2(N;\mathbb{Z}_p)_{\text{Eis}} \) denote the submodule of \( M_2(N;\mathbb{Z}_p)_{\text{Eis}} \) consisting of cusp forms. We have perfect pairings
\[
(2.1.2) \quad M_2(N;\mathbb{Z}_p)_{\text{Eis}} \times \mathbb{T} \to \mathbb{Z}_p, \quad S_2(N;\mathbb{Z}_p)_{\text{Eis}} \times \mathbb{T}^0 \to \mathbb{Z}_p.
\]

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

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

We will also require the Eisenstein-congruent Hecke algebras of weight 2 and level \( \ell_0 \) 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 \( \mathbb{T} \to \mathbb{T}_{\ell_0} \) and \( \mathbb{T}^0 \to \mathbb{T}^0_{\ell_0} \), because a choice of Atkin–Lehner signature at level \( \ell_0 \) designates a stabilization of level \( \ell_0 \) 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 \( M_2(N;\mathbb{Z}_p)_{\text{Eis}} \). 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 \( G_\ell \), which combine 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

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

When the source and target of a pseudorepresentation $D$ have a topology, $D$ is considered continuous when $\text{Tr}_D$ 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 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 $\gamma \in E \otimes_A B$, $\gamma$ satisfies its $B$-valued characteristic polynomial $X^2 - \text{Tr}_D(\gamma)X + \det_D(\gamma) \in B[X]$.
- 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 $\rho$ 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 $m : B \otimes_A C \to A$ 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 $2 \times 2$-matrix multiplication.
2.2.4. The unramified-or-Steinberg condition, correcting an error in [WWE21]. We now review and correct the unramified-or-Steinberg condition that was introduced in [WWE21, §3]. In [WWE21, §3], this condition is called the “unramified-or-ε-Steinberg condition” or “US^ε_N condition”, to allow for arbitrary choice of Atkin–Lehner signs \( \varepsilon = (\varepsilon_\ell)_{\ell | N} \) indexed by the prime divisors of \( N \). In this paper, we

- We think of a GMA structure on a Cayley–Hamilton algebra as the idempotents \((\frac{1}{0} 0)\) and \((0 \frac{1}{0})\) 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 \( C \) when some Cayley–Hamilton representation inducing it satisfies \( C \). In this section, we overview these deformation-theoretic concepts, first specializing to the particular pseudorepresentation that we will deform.

- Let \( \omega : G_Q \to \mathbb{F}_p^\times \) denote the mod-\( p \) cyclotomic character, which factors through \( G_{Q,N_p} \). It is the reduction modulo \( p \) of the \( p \)-adic cyclotomic character that we denote by \( \kappa : G_Q \to \mathbb{Z}_p^\times \).
- Let \( D : G_{Q,N_p} \to \mathbb{F}_p \) denote the pseudorepresentation \( \psi(\omega \oplus 1) \) of \( G_{Q,N_p} \).
- When \( A \) is a commutative local ring with residue field \( \mathbb{F}_p \), we say that \( D : G_{Q,N_p} \to A \) deforms \( \bar{D} \) if the composite pseudorepresentation \( \bar{G}_{Q,N_p} \to A \) equals \( \bar{D} \).
- Let \( R_D \) denote the universal pseudodeformation ring of \( D \). By [Che14, Proposition E], \( R_D \) is Noetherian, which means that there is a universal pseudodeformation \( D^\alpha_D : G_{Q,N_p} \to R_D \).

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 \((\rho,E,D)\) of \( G \) is over \( \bar{D} \) when the pseudorepresentation \( \bar{D} \circ \rho : G \to A \) deforms \( \bar{D} \).
- There exists a universal Cayley–Hamilton representation of \( G_{Q,N_p} \) over \( \bar{D} \), valued in the universal pseudodeformation ring \( R_D \). It is written

\[
(\rho^\alpha : G_{Q,N_p} \to (E_D^n)^\times, E_D^n, D_E^n : E_D^n \to R_D^n).
\]

- 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 \( G_{Q,N_p} \) over \( \bar{D} \) admits the structure of a GMA representation. (See [WWE19, Theorem 3.2.2] for more details.)
only consider negative Atkin–Lehner signs, so we suppress the $\varepsilon$ from our notation outside of §2.2.4.

However, the second- and third-named authors appreciate the opportunity to correct an error in [WWE21] in the formulation of $\US_N^\varepsilon$ for general $\varepsilon$, which we do in Definition 2.2.2. See Remark 2.2.6 for justification that the results of [WWE21] still hold with precisely this correction to the definition.

The definition of $\US_N^\varepsilon$ 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 $\rho_f : \Gamma_0(N) \to \GL_2(\mathbb{Q}_p)$ 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:

- $\rho_f|_{\ell}$ is non-trivial if and only if $f$ is new at $\ell$. In other words, $\rho_f|_{\ell}$ is unramified if and only if either $f$ is old at $\ell$ or $\ell \nmid N$.
- If $f$ is new at $\ell$ and its $w_\ell$-eigenvalue is $\varepsilon_\ell$, then $\rho_f|_{\ell} : \GL_2(\mathbb{Q}_p)$ has the form

$$\rho_f|_{\ell} \simeq \lambda(-\varepsilon_\ell) \otimes \begin{pmatrix} \kappa & \bar{b}_\ell \\ 0 & 1 \end{pmatrix},$$

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

In either case, if $f$ has $w_\ell$-eigenvalue $\varepsilon_\ell$, then the expression

$$(\rho_f(\sigma) - \lambda(\varepsilon_\ell)\kappa(\sigma)) \cdot (\rho_f(\tau) - \lambda(\varepsilon_\ell)(\tau))$$

is zero for all $\sigma, \tau \in G_\ell$ with at least one of $\sigma$ and $\tau \in I_\ell$. Indeed, if $f$ is old at $\ell$, then $\rho_f$ is unramified and one of the two factors in the expression is zero. Otherwise, $\rho_f|_{\ell}$ has the form (2.2.1), and the expression is of the form

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

and any such product is zero. This motivates the following definition.

**Definition 2.2.2 (Correction of [WWE21, Defn. 3.4.1]).** A Cayley–Hamilton representation $(\rho : \Gamma_0(N) \to \GL_2(\mathbb{Q}_p))$ is unramified-or-$\varepsilon_\ell$-Steinberg at $\ell$ (or $\US_N^\varepsilon$) provided that

1. the determinant of $\rho$, $\det : \GL_2(\mathbb{Q}_p) \to \mathbb{A}^*$, is unramified
2. the following identity

$$\begin{align*}
(\rho(\sigma) - \lambda(\varepsilon_\ell)\kappa(\sigma)) \cdot (\rho(\tau) - \lambda(\varepsilon_\ell)(\tau)) &= 0 \\
\end{align*}$$

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

**Remark 2.2.4.** For the rest of this paper, we will only use the case that $\varepsilon_\ell = -1$.

So we will treat the identity (2.2.3) as

$$\begin{align*}
(\rho(\sigma) - \kappa(\sigma)) \cdot (\rho(\tau) - 1) &= 0 \\
\end{align*}$$

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

**Remark 2.2.6.** The definition of unramified-or-Steinberg in [WWE21, Defn. 3.4.1] assumes only condition (2) and there is an incorrect lemma [WWE21, Lem. 3.4.4] that claims that (2) implies (1). This difference does not affect the results of
Since det(\(\rho\)) = 2, so Tr(\(\rho\)) = 2. By the pseudorepresentation identity in [Che14, Lem. 2.7(iv)],

\[2 \text{det}(\rho) = \text{Tr}(\rho)^2 - \text{Tr}(\rho^2).\]

Since \(\text{det}(\rho) = 1\) and \(\rho(\tau)^2 = 2\rho(\tau) - 1\), this implies

\[2 = \text{Tr}(\rho(\tau)^2) - 2\text{Tr}(\rho(\tau)) + \text{Tr}(1).\]

But Tr(1) = 2, so

\[\text{Tr}(\rho(\tau))(\text{Tr}(\rho(\tau)) - 2) = 0.\]

The reduction of Tr(\(\rho(\tau)\)) modulo the maximal ideal of \(A\) is Tr(\(\rho(\tau)\)) = 2, so Tr(\(\rho(\tau)\)) is a unit in \(A\), and the previous equation implies \(\text{Tr}(\rho(\tau)) = 2\), as desired. \(\square\)

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 2.2.9.** We say that an action of \(G_p\) on a finite cardinality \(\mathbb{Z}_p\)-module \(M\) is finite-flat provided that there exists a finite-flat group scheme \(G/\mathbb{Z}_p\) and an isomorphism of \(\mathbb{Z}_p[G_p]\)-modules \(M \cong G(\mathbb{Q}_p)\).

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 2.2.10.** 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 \( \rho \) 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 \( \rho \) that is finite-flat.

In [WWE19], it is proved that any stable condition cuts out a universal Cayley–Hamilton representation over any residual pseudorepresentation \( \bar{D} : G_p \to F \), 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 \( R_\bar{D} \to R_{\bar{D}}^{\text{flat}} \) 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 \( D|_p \).

**Proposition 2.2.11.** For any finite-flat Cayley–Hamilton representation \( \rho \) of \( G_p \) over \( D|_p : G_p \to \mathbb{F}_p \), with coefficient ring \( A \), there exist unique characters \( \theta_i : G_p \to \mathbb{A}^\times \), \( i = 1, 2 \), and a GMA structure with respect to which it has the form

\[
\rho \simeq \left( \begin{array}{cc} \kappa \theta_1 & \ast \\ 0 & \theta_2 \end{array} \right).
\]

The characters \( \theta_i \) 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 \( \theta_i \), there is a restriction on the extension denoted “\( \ast \)”, cutting out an \( A \)-submodule

\[
\text{Ext}^1_{A[G]}(\theta_2, \theta_1(1))^{\text{flat}} \subset \text{Ext}^1_{A[G]}(\theta_2, \theta_1(1))
\]

consisting of finite-flat extensions of \( \theta_2 \) by \( \kappa \theta_1 \). We will especially be interested in the case where \( A = \mathbb{F}_p \) and the \( \theta_i \) are trivial. In that case, since \( \omega = (\kappa \mod p) \) lifts to \( G_{Q,N_p} \), we construct

\[
\text{Ext}^1_{\mathbb{F}_p[G_{Q,N_p}]}(\mathbb{F}_p, \mathbb{F}_p(1))^{\text{flat}} \subset \text{Ext}^1_{\mathbb{F}_p[G_{Q,N_p}]}(\mathbb{F}_p, \mathbb{F}_p(1))
\]

consisting of those \( G_{Q,N_p} \)-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 \( H_i := \text{Gal}(\mathbb{Q}_{p^i}/\mathbb{Q}_{p^i}) \), so \( H_1 = G_p \). Let \( \mathbb{Z}_{p^i} \) denote the ring of integers of \( \mathbb{Q}_{p^i} \).

**Lemma 2.2.13** (Local Kummer theory). Under the canonical isomorphism

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

and the 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 \( \text{Ext}^1_{\mathbb{F}_p[H_i]}(\mathbb{F}_p, \mu_p)^{\text{flat}} \) 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 \( \text{Ext}^1_{\mathbb{F}_p[G_p]}(\mathbb{F}_p, \mu_p)^{\text{flat}} \) corresponds with the subspace \( \langle 1 + p \rangle \).
Proof. This is well known; see, for example, [Sch12, Prop. 2.2]. \qed

Lemma 2.2.14 (Global Kummer theory).

(1) The subspace
$$\operatorname{Ext}^1_{F_p[G_0,N_p]}(\mathbb{F}_p, \mathbb{F}_p)_{\flat} \subset \operatorname{Ext}^1_{F_p[G_0,N_p]}(\mathbb{F}_p, \mathbb{F}_p)$$
has basis \{\ell_0, \ell_1\} under the canonical isomorphisms
$$\operatorname{Ext}^1_{F_p[G_0,N_p]}(\mathbb{F}_p, \mathbb{F}_p) \cong H^1(\mathbb{Z}[1/Np], \mu_p) \cong \mathbb{Z}[1/Np]^\times / (\mathbb{Z}[1/Np]^\times)^p.$$

(2) The natural map
$$\operatorname{Ext}^1_{F_p[G_0,N_p]}(\mathbb{F}_p, \mathbb{F}_p(1)) \to \operatorname{Ext}^1_{F_p[G_0,N_p]}(\mathbb{F}_p, \mathbb{F}_p(1))$$
has image containing a complement of \(\operatorname{Ext}^1_{F_p[G_0,N_p]}(\mathbb{F}_p, \mathbb{F}_p(1))_{\flat}\). 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 2.2.13 and the fact that \(p, \ell_0, \ell_1\) is a basis for \(\mathbb{Z}[1/Np]^\times / (\mathbb{Z}[1/Np]^\times)^p\). \qed

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

Lemma 2.2.15. Let \(\rho : G_p \to E\) be a Cayley–Hamilton representation with coefficient ring \(A\). Suppose that \(S \subset E\) is a subalgebra containing \(\rho(G_p)\), and let \(V\) be a faithful \(S\)-module. If the \(G_p\)-action on \(V\) induced by \(\rho\) is finite-flat, then \(\rho\) 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]. \qed

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 2.2.16. Let \(G\) be a profinite group, let \(\eta : G \to \operatorname{GL}_2(\mathbb{F}_p)\) be a representation, and let \(s : (A', m_{A'}) \to (A, m_A)\) be a surjection of local Artinian \(\mathbb{F}_p\)-algebras such that \(m_{A'} \cdot \ker s = 0\). Let \(\eta_A\) be a lift of \(\eta\) over \(A \to A/m_A = \mathbb{F}_p\).

(1) If the set of lifts of \(\eta_A\) over \(A' \to A\) is non-empty, then it is a torsor over the group
$$Z^1(G, \operatorname{Ad}(\eta)) \otimes_{\mathbb{F}_p} \ker s$$
under addition of coordinates.

(2) If \(A = \mathbb{F}_p\), then this torsor is canonically isomorphic to \(Z^1(G, \operatorname{Ad}(\eta)) \otimes_{\mathbb{F}_p} \ker s\) due to the base point given by the trivial lift \(\rho \otimes_{\mathbb{F}_p} A\) of \(\rho\) to \(A\).

(3) Conjugation of \(\rho_{A'}\) by \(x \in \ker(\operatorname{GL}_2(A') \to \operatorname{GL}_2(A))\), which is canonically isomorphic to \(C^0(G, \operatorname{Ad}(\rho)) \otimes_{\mathbb{F}_p} \ker s\), amounts to acting by coboundary \(dx \in B^1(G, \operatorname{Ad}(\rho)) \otimes_{\mathbb{F}_p} \ker s\) on \(\rho_{A'}\) (via the torsor structure of (1)).

(4) If \(\eta_A\) has constant determinant (that is, \(\det \eta_A = \det \eta\) under \(\mathbb{F}_p^\times \to A^\times\)), then the set of constant determinant lifts of \(\eta_A\) 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
$$Z^1(G, \operatorname{Ad}^0(\eta)) \otimes_{\mathbb{F}_p} \ker s$$
under addition of coordinates.
Here “addition of coordinates” on \( \rho_A \) means that we add to the function \( \rho_A : G \to \text{GL}_2(A') \) the function \( G \to M_d(\ker s) \subset \text{GL}_2(A') \) given by an element of \( Z^1(G, \text{Ad}(\eta)) \otimes_{\mathbb{F}_p} \ker s \).

**Proposition 2.2.17.** Let \( \eta : G \to \text{GL}_2(\mathbb{F}_p) \) be a finite-flat representation. Let \( s : (A', m_{A'}) \to (A, m_A) \) be a surjection of local Artinian \( \mathbb{F}_p \)-algebras such that \( m_{A'} \cdot \ker s = 0 \). Let \( \eta_A \) be a finite-flat lift of \( \eta \) over \( A \to A/\mathfrak{m}_A = \mathbb{F}_p \).

1. The set of finite-flat lifts of \( \eta_A \) over \( s \) is non-empty, and admits the structure of a torsor over the group
   \[
   Z^1(G, \text{Ad}(\eta))^{\text{flat}} \otimes_{\mathbb{F}_p} \ker s,
   \]
   where \( Z^1(G, \text{Ad}(\eta))^{\text{flat}} \subset Z^1(G, \text{Ad}(\eta)) \) is a sub-vector space that contains \( B^1(G, \text{Ad}(\eta)) \).

2. In particular, if \( A = \mathbb{F}_p \), then this torsor is non-empty and canonically isomorphic to \( Z^1(\mathbb{Q}_p, \text{Ad}(\eta)) \otimes_{\mathbb{F}_p} \ker s \).

3. The analogue of Lemma 2.2.16(3) holds for finite-flat representations.

4. The analogue of Lemma 2.2.16(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 2.2.16 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 2.2.18.** Let \( \rho \) be a Cayley–Hamilton representation over \( \bar{D} : G_{\mathbb{Q}, N \mathbb{p}} \to \mathbb{F}_p \). We say that \( \rho \) is unramified-or-Steinberg of level \( N \), or US\(_N\), when

1. for all \( \ell | N \), \( \rho|_{\ell} \) is US\(_\ell\), and
2. \( \rho|_{\mathbb{p}} \) is finite-flat in the sense of Definition 2.2.10.

When \( D : G_{\mathbb{Q}, N \mathbb{p}} \to A \) is a deformation of \( \bar{D} : G_{\mathbb{Q}, N \mathbb{p}} \to \mathbb{F}_p \), we say that \( D \) is US\(_N\) if there exists some \( A \)-valued Cayley–Hamilton representation \( \rho \) over \( \bar{D} \) such that \( \rho \) is US\(_N\) and \( D = \psi(\rho) \).

We fix notation for the universal objects satisfying US\(_N\), which were produced in [WWE21, §3].

**Definition 2.2.19.**

- Let \( R \) denote the universal pseudodeformation ring of \( \bar{D} \) satisfying the US\(_N\) condition. It admits a natural surjection \( R_{\bar{D}} \to R \).
- Likewise, there exists a universal US\(_N\) Cayley–Hamilton representation of \( G_{\mathbb{Q}, N \mathbb{p}} \) over \( \bar{D} \), denoted
  \[
  \rho_N : G_{\mathbb{Q}, N \mathbb{p}} \to E^\times, E, D_E : E \to R
  \]
  and inducing \( D_N : G_{\mathbb{Q}, N \mathbb{p}} \to R \), the universal US\(_N\) deformation of \( \bar{D} \).
- We fix a \( R_{\bar{D}} \)-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 \( (\rho_N, E, D_E) \) of \( G_{\mathbb{Q}, N \mathbb{p}} \) over \( \bar{D} \), and write its matrix coordinates as
  \[
  E \cong \begin{pmatrix} R & B \\ C & R \end{pmatrix}.
  \]
For $\gamma \in G_{Q,Np}$, we write
\[
\begin{pmatrix}
a_{\gamma} & b_{\gamma} \\
c_{\gamma} & d_{\gamma}
\end{pmatrix}
\]
for its image in $E$ under $\rho_N$. Letting $m \subset R$ denote the maximal ideal, we may and do assume that the GMA structure on $E$ has been chosen such that
\[
(a \mod m) = \omega \quad \text{and} \quad (d \mod m) = 1
\]
as homomorphisms $G_{Q,Np} \to \mathbb{F}_p^\times$.

We will also occasionally refer to $R_{\ell_0}$ as the universal pseudodeformation of $\bar{D}$ satisfying the (global) US$_{\ell_0}$ condition (with Atkin–Lehner sign $-1$ at $\ell_0$).

There is a natural surjection $R \twoheadrightarrow R_{\ell_0}$.

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

**Proposition 2.2.20** ([WWE21, Prop. 4.1.1]). We have a surjection $R \twoheadrightarrow T$ characterized by sending traces of Frobenius elements $\text{Tr}_{D_N}(\text{Fr}_q) \in R$ for primes $q \nmid Np$ to the Hecke operator $T_q$. Similarly, we have $R_{\ell_0} \twoheadrightarrow T_{\ell_0}$.

Note that since $T$ is generated as a $\mathbb{Z}_p$-algebra by the $T_q$, the characterizing property of the map makes its surjectivity visible. The level $\ell_0$ map is known to be an isomorphism $R_{\ell_0} \cong T_{\ell_0}$ [WWE20].

**Remark 2.2.21.** Our hypothesis is that the local US$_N$ 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 $R \xrightarrow{\sim} T$ 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 $J^\text{red}_D \subset R_D$ such that a pseudodeformation $D_A : G \to A$ of $D$ is reducible if and only if $J^\text{red}_D$ vanishes under the corresponding homomorphism $R_D \to A$. And any $D_A$ becomes reducible modulo the image of $J^\text{red}_D$ 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 $J^\text{red}_D$ is equal to the image of the multiplication map $m : B \otimes_R C \to R$.

Another canonical ideal of $R$ is the kernel $J^\text{min}$ of the composition
\[
J^\text{min} := \ker(R \to T \to \mathbb{Z}_p),
\]
that arises from the Eisenstein series $E_{2,N}$. This is characterized by sending $\text{Tr}_{D_N}(\text{Fr}_q) \in R$ 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 $J^\text{red}_D \subset J^\text{min}$ 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 $R_{\text{red}} := R/J_{\text{red}}$. Here we write $\gamma_0 \in I_{\ell_0}$ for then chosen lift of the topological generator of the tame quotient of $I_{\ell_0}$, denoted $\gamma_{\ell_0}$ in §1.6.

Lemma 2.3.2. There is an isomorphism

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

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

$$D_{\text{red}} := \psi(\omega(1 + Ya_0) + (1 - Y a_0)) : G_{\mathbb{Q}, Np} \to \mathbb{F}_p[Y]/(Y^2).$$

In Proposition 5.1.8, we use the local homomorphism $\varphi_{D_{\text{red}}} : R \to \mathbb{F}_p[e]/(e^2)$ induced by $D_{\text{red}}$.

Proof. The first statement is a direct application of the presentation for $R_{\text{red}}$ 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 notation for generators of the tame quotients of inertia groups as in §1.6.

Definition 2.4.1. For a prime $\ell_i$ not equal to $p$, let $\gamma_i \in I_{\ell_i}$ stand for the element $\gamma_{\ell_i} \in I_{\ell_i}$ chosen in §1.6, which is a lift over the tame quotient $I_q \to I_q^{\text{tame}}$ of a topological generator.

Proposition 2.4.2. The elements $b_{\gamma_0}$ and $b_{\gamma_1}$ 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 $J_{\text{min}}^2 \subset J_{\text{red}} \subset J_{\text{min}}$. The element $b_{\gamma_0} \cdot c_{\gamma_0}$ of $J_{\text{red}}$ lies within its submodule $J_{\text{min}}^2$.

Proof. The inclusion of ideals follows from Lemma 2.3.2 because the kernel of $R/J_{\text{red}} = R_{\text{red}} \to \mathbb{Z}_p = R/J_{\text{min}}$ 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 1.6.1 as well as the conditions in Assumption 1.2.2.

3.1. Cocycles determined by the pinning data. We fix some notation for Galois cocycles determined by the pinning data of Definition 1.6.1.

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 $\sigma \mapsto \frac{\sigma n_{1/p}^{1/p}}{n_{1/p}^{1/p}}$ for a choice $n^{1/p} \in \overline{\mathbb{Q}}$ of $p$th 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 $\mu_p \not\in \mathbb{Q}^\times$, each Kummer cocycle of $n$ is given by $\sigma \mapsto \sigma^{n/p}$ for a unique choice of $n/p \in \overline{\mathbb{Q}}_p$ of $p$th root of $n$. We use the isomorphism $\mathbb{F}_p(1) \cong \mu_p$ chosen in §1.6 to value Kummer classes and cocycles in $\mathbb{F}_p(1)$.

**Definition 3.1.1.**

- Let $b^{(1)}_0, b^{(1)}_1 \in Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1))$ be the Kummer cocycles associated to $p$th roots $\ell^{1/p}_0$ and $\ell^{1/p}_1$ of $\ell_0$ and $\ell_1$, respectively, chosen in §1.6. Let $b^{(1)} = b^{(1)}_1$.
- Denote the Kummer classes of $\ell_0, \ell_1, p$, 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 $b^{(1)}_1(\gamma_1) = 1$.
- The cohomology group $H^1_{(p)}(\mathbb{Z}[1/Np], \mathbb{F}_p(-1))$ has $\mathbb{F}_p$-dimension 1 by [WWE21, Lem. 3.10.2]. Let $\tilde{c}_0 \in H^1(\mathbb{Z}[1/Np], \mathbb{F}_p(-1))$ denote the unique class in the image of $H^1_{(p)}(\mathbb{Z}[1/Np], \mathbb{F}_p(-1))$ such that $\tilde{c}_0(\gamma_0) = 1$ for any cycle $\tilde{c}_0 \in Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p(-1))$ representing $c_0$.
- If $\tilde{c}_0 \in Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p(-1))$ is a cocycle representing $c_0$, then every other such cocycle is of the form $\tilde{c}_0 + dx$ for some $x \in \mathbb{F}_p(-1)$. Then
\[(\tilde{c}_0 + dx)(\text{Fr}_{\ell_1}) = \tilde{c}_0(\text{Fr}_{\ell_1}) + (\ell_1^{-1} - 1)x.\]

Then $x = -(\ell_1^{-1} - 1)^{-1}\tilde{c}_0(\text{Fr}_{\ell_1})$ is the unique choice such that $(\tilde{c}_0 + dx)(\text{Fr}_{\ell_1}) = 0$. Let $c^{(1)} \in Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p(-1))$ be $\tilde{c}_0 + dx$ for this choice of $x$. Then $c^{(1)}$ is the unique cocycle with cohomology class $c_0 = [c^{(1)}]$ such that $c^{(1)}|_{\ell_1} = 0$.
- 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 $x_{c^{(1)}} = (\omega(\tau)^{-1} - 1)^{-1}c^{(1)}(\tau)$.
- Let $a_0, a_p \in Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p)$ be non-zero homomorphisms ramified exactly at $\ell_0$ 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 1.6.1:

- The cocycles $b^{(1)}$, $c^{(1)}$, and $a_0$.
- The images of $\gamma_i$ in $I_{\ell_i}^{\text{tame}} \otimes_{\mathbb{Z}} \mathbb{F}_p$. 
3.2. Cup products and congruence conditions. The conditions in this paper’s running assumption, Assumption 1.2.2, 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 (2) in Assumption 1.2.2). Let $\ell_0, \ell_1$ 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. $\ell_1$ is a $p$th power modulo $\ell_0$.
2. $a_{\ell_1}|\ell_0 \equiv 0$ 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 $F/\mathbb{Q}$ be the unique degree-$p$ subextension of $\mathbb{Q}(\zeta_{\ell_0})/\mathbb{Q}$. We see that (2) is true if and only if $\ell_1$ splits completely in $F/\mathbb{Q}$, which, in turn, is equivalent to a Frobenius element $\operatorname{Fr}_{\ell_1}$ for $\ell_1$ becoming trivial in $\operatorname{Gal}(F/\mathbb{Q})$. Then the equivalence of (1) and (2) follows from the standard fact that $\operatorname{Fr}_{\ell_1} \mapsto \ell_1$ under the canonical isomorphism $\operatorname{Gal}(\mathbb{Q}(\zeta_{\ell_0})/\mathbb{Q}) \cong \mathbb{F}_p^\times$.

(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 $\ell_1$.

(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 $\ell_0$-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. $\square$

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 $\ell_1^{1/p} \in \mathbb{Q}$ in the pinning data of Definition 1.6.1 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 $\ell$ be a prime, $\ell \not\equiv p$, and let $b_1 \in H^1(\mathbb{Q}, \mathbb{F}_p(1))$ be the Kummer class of $\ell$. The following conditions are equivalent.

1. $\ell - 1$ is divisible by $p^2$
2. $a_{\ell} \in H^1(\mathbb{Q}_{\ell}, \mathbb{F}_p)$ is trivial
3. $b_{1|p} \in H^1(\mathbb{Q}_p, \mathbb{F}_p(1))$ is trivial
4. $b_{1|p} \in H^1(\mathbb{Q}_p^\times, \mathbb{F}_p(1))$ is trivial
5. $\mathbb{Q}((\ell^{1/p})/\mathbb{Q}$ is not totally ramified at $p$; or, what is the same, tamelyramified 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 $b_i|_{\mathbb{Q}(\zeta_p)}$, which is a surjective homomorphism $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_p)) \to \mathbb{F}_p(1)$. We observe that both (4) and (5) are equivalent to $b_i|_{\mathbb{Q}(\zeta_p)}$ 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. $\square$

We now shift to a discussion of local cup products related to item (1) in Assumption 1.2.2. Indeed, since we have assumed $\ell_0 \equiv 1 \pmod{p}$, our chosen primitive $p$th 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

$$(3.2.3) \quad \mathbb{F}_p(i)|_{\ell_0} \cong \mathbb{F}_p(j)|_{\ell_0}, \quad x \mapsto x \otimes \zeta_p^{-i}$$

of representations of $G_{\ell_0}$ 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

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

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 $i \in \mathbb{Z}$,

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

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

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

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. $\square$

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

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

is injective.

Our proof for $i = -1$ also uses (2) in Assumption 1.2.2, 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 (mod $p$). 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 $H^2(\mathbb{Q}_{\ell_1}, \mathbb{F}_p(-1)) = 0$ for all $j \in \mathbb{Z}_{\geq 1}$, making the exact triangle

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

degenerate.

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

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

has cokernel of dimension 1, since $H^3_c(\mathbb{Z}/Np, \mathbb{F}_p(1)) \cong \mathbb{F}_p$ (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 (3) in Assumption 1.2.2. This assumption states that the Hecke algebra $T_{\ell_0}$, 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 (3) in Assumption 1.2.2). Assume that $\ell_0 \equiv 1 \pmod{p}$ and $\ell_1 \not\equiv \pm 1 \pmod{p}$. The following are equivalent.

1. $\text{rk}_{\mathbb{F}_p} T_{\ell_0} = 2$
2. $b_0 \cup c_0 \neq 0$ in $H^2(\mathbb{Z}/\ell_0p, \mathbb{F}_p)$
3. $b_0 \cup c_0 \neq 0$ in $H^2(\mathbb{Z}/Np, \mathbb{F}_p)$
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 $H^2(\mathbb{Z}/\ell_0p, \mathbb{F}_p(-1))$
6. $a_0 \cup c_0 \neq 0$ in $H^2(\mathbb{Z}/Np, \mathbb{F}_p(-1))$
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 \(D_1 : G_{\mathbb{Q},N_p} \rightarrow \mathbb{F}_p[\epsilon]/(\epsilon^2)\) of \(D : G_{\mathbb{Q},N_p} \rightarrow \mathbb{F}_p\) 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 \(F[\epsilon_n] \rightarrow F[\epsilon_m]\). 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 \(\rho : G \rightarrow \text{GL}_2(F[x])\) 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 \(a, b, c, d : G \rightarrow F[x]\). Suppose we want to check that \(\rho\) is a homomorphism. Equivalently, we can check this in stages labeled by natural numbers \(n\): at each stage \(n\), check that \(\rho \mod x^n\) 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 \(\rho\) is a homomorphism is to consider the conjugate \(\rho' = (x^{-1} 0 \mid 0 1)\rho(\bar{0} 1)\) —that is,

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

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

In the example, if \(\rho\) is a homomorphism, then \(\rho\) and \(\rho'\) 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 \(\rho\) and \(\rho'\) have the same trace and determinant, and that the trace and determinant of \(\rho\) 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
\[ \mathbb{F}_p[\epsilon_{n-1}] \otimes_{\mathbb{F}_p[\epsilon_{n}]} \mathbb{F}_p[\epsilon_{n-1}] \xrightarrow{bc \mapsto hc} \mathbb{F}_p[\epsilon_{n-1}] \xrightarrow{\epsilon x \mapsto \epsilon x} \mathbb{F}_p[\epsilon_{n}]. \]

The image of the multiplication map \( m \) is \( \epsilon \mathbb{F}_p[\epsilon_{n}] \). In particular, if \( \rho : G \to E_n^\infty \) is a Cayley–Hamilton representation such that the induced map \( \mathbb{F}_p[G] \to E_n \) is surjective, then the reducibility ideal of \( \rho \) 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 \( \text{GL}_2(\mathbb{F}_p[\epsilon_{n}]) \). 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 \( k = 2, \ldots, n \), 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 \( (\alpha_0 + \alpha_1 \gamma \delta_0 + \epsilon \delta_1) \) for \( \alpha_0, \beta, \gamma, \delta_0, \delta_1 \in \mathbb{F}_p \), and the multiplication is
\[ \begin{pmatrix} \alpha_0 + \epsilon \alpha_1 & \beta \\ \gamma & \delta_0 + \epsilon \delta_1 \end{pmatrix} \begin{pmatrix} \alpha_0' + \epsilon \alpha_1' & \beta' \\ \gamma' & \delta_0' + \epsilon \delta_1' \end{pmatrix} = \begin{pmatrix} \alpha_0 \alpha_0' + \epsilon (\alpha_0 \alpha_1' + \alpha_0' \alpha_1 + \beta \gamma) & \alpha_0 \beta' + \beta \delta_0' \\ \gamma \alpha_0' + \delta_0 \gamma' & \delta_0 \delta_0' + \epsilon (\delta_0 \delta_1' + \delta_0' \delta_1 + \beta \gamma) \end{pmatrix}. \]

Example 4.1.6. Let \( \rho \) and \( a, b, c, d \) be as in Example 4.1.1 with \( F = \mathbb{F}_p \) and with the variable \( x \) replaced by \( \epsilon \). Suppose that \( \rho \) is a homomorphism. Then, for every \( n > 0 \), the map
\[ g \mapsto \begin{pmatrix} a(g) \pmod{\epsilon^{n-1}} & b(g) \pmod{\epsilon^{n}} \\ c(g) \pmod{\epsilon^{n-1}} & d(g) \pmod{\epsilon^{n}} \end{pmatrix} \]
gives a homomorphism \( G \to E_n^\infty \).

4.1.2. Reduction of 1-reducible GMAs. When \( n \geq m \), the standard surjection \( \mathbb{F}_p[\epsilon_{n}] \to \mathbb{F}_p[\epsilon_{m}], \epsilon \mapsto \epsilon \), extends naturally to 1-reducible GMAs. We have a reduction map
\[ r_{n,m} : E_n \to E_m, \]
simply reducing each of the coordinates under the usual surjections \( \mathbb{F}_p[\epsilon_{n}] \to \mathbb{F}_p[\epsilon_{m}] \) and \( \mathbb{F}_p[\epsilon_{n-1}] \to \mathbb{F}_p[\epsilon_{m-1}] \), which is a \( \mathbb{F}_p[\epsilon_{n}] \)-algebra homomorphism. We will especially apply the case
\[ r_{2,1} : E_2 \to E_1. \]

The reduction map \( r_{n,m} \) is distinct from the tensor reduction map
\[ E_n \to E_n \otimes_{\mathbb{F}_p[\epsilon_{n}]} \mathbb{F}_p[\epsilon_{m}], \quad x \mapsto x \otimes 1, \]
which is also a ring homomorphism. As long as \( n > m \), the latter has the form
\[
\begin{pmatrix}
\mathbb{F}_p[\epsilon_n] & \mathbb{F}_p[\epsilon_n-1]
\end{pmatrix}
\begin{pmatrix}
\mathbb{F}_p[\epsilon_m] & \mathbb{F}_p[\epsilon_m]
\end{pmatrix}
\rightarrow
\begin{pmatrix}
\mathbb{F}_p[\epsilon_m] & \mathbb{F}_p[\epsilon_m]
\end{pmatrix},
\]
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 \( r_{2,1} : E_2 \rightarrow E_1 \)
\[
(4.1.8)
E_2 \rightarrow \begin{pmatrix}
\mathbb{F}_p[\epsilon_m] & \mathbb{F}_p[\epsilon_m] \\
\mathbb{F}_p[\epsilon_m] & \mathbb{F}_p[\epsilon_m]
\end{pmatrix}
\rightarrow E_1,
\]
where the leftmost map is the tensor reduction map for \( (n, m) = (2, 1) \), and the
rightmost map is reduction modulo \( \epsilon \) 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 2.2.11 that they must be upper-triangular, which makes it possible to apply the test of finite-flatness in Lemma 2.2.15 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
\[
U_n := \begin{pmatrix}
\mathbb{F}_p[\epsilon_n] & \mathbb{F}_p[\epsilon_n-1]
\end{pmatrix} \subset E_n.
\]
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-\( \epsilon \)
map, written \( \epsilon : \mathbb{F}_p[\epsilon_n-1] \rightarrow \mathbb{F}_p[\epsilon_n] \).

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 \( \epsilon^n \) 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
\[
\begin{pmatrix}
a & b \\
c & d
\end{pmatrix} \mapsto \begin{pmatrix}
\bar{a} & \bar{b} \\
\bar{c} & \bar{d}
\end{pmatrix},
\]
where \( \bar{a}, \bar{d} \in \mathbb{F}_p[\epsilon_n-1] \) indicates reduction modulo \( \epsilon^n \).

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

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:
\begin{enumerate}
\item \( -a^{(1)} = b^{(1)} - c^{(1)} \),
\item \( (a^{(1)} - b^{(1)} - c^{(1)}|_{t_p}) = 0 \) in \( H^1(\mathbb{Q}_p^\text{nr}, \mathbb{F}_p) \), and
\item the class of \( a^{(1)}|_{t_0} \) in \( H^1(\mathbb{Q}_0, \mathbb{F}_p) \) is on the line spanned by \( \zeta \cup c_0|_{t_0} \) for any
(equivalently, all) non-trivial \( \zeta \in \mu_p(\mathbb{Q}_0) \cong H^0(\mathbb{Q}_0, \mathbb{F}_p(1)) \).
\end{enumerate}
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 1.6.1.

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

For any \(-g\) whose coboundary is \( b^{(1)} \prec c^{(1)} \), we have
\[
-dg|_p = b^{(1)}|_p \prec c^{(1)}|_p = b^{(1)}|_p \prec dx_{c^{(1)}} = -d(b^{(1)}|_p \prec x_{c^{(1)}})
\]
Hence \((g - b^{(1)}|_p \prec x_{c^{(1)}})|_p\) is a cocycle. Since \( H^1(\mathbb{Q}_p, \mathbb{F}_p) \) is generated by its unramified subgroup \( H^1_{un}(\mathbb{Q}_p, \mathbb{F}_p) \) together with \( a_p|_p \), we have
\[
(g - b^{(1)}|_p \prec x_{c^{(1)}})|_p \equiv ya_p|_p \pmod{H^1_{un}(\mathbb{Q}_p, \mathbb{F}_p)}
\]
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
\[
-dg|_{\ell_0} = b^{(1)}|_{\ell_0} \prec c^{(1)}|_{\ell_0} = 0,
\]
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 \( H^1(\mathbb{Q}_p, \mathbb{F}_p) \). 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 \( \gamma \).

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 \( G_{\ell_1} \) to \( \mathbb{F}_p \) is unramified. \( \square \)

Condition (3) in Lemma 4.2.1 provides the invariant \( \alpha \), 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 \( \alpha \) depends only on the pinning data of Definition 1.6.1.

**4.3. An irreducible first-order deformation.** We now produce a first-order 1-reducible GMA representation \( \rho_1 : G_{\mathbb{Q}, N_p} \to E^\times \) deforming \( \omega \oplus 1 \) and satisfying the unramified-or-Steinberg condition \( US_N \) of Definition 2.2.18. The construction uses the cocycles \( b^{(1)} \) and \( c^{(1)} \) fixed in Definition 3.1.1 and the cocycle \( a^{(1)} \) defined in Lemma 4.2.1, together with the cochain \( d^{(1)} \) defined by
\[
d^{(1)} = b^{(1)} \circ c^{(1)} - a^{(1)}.
\]
Note that, since \(-d(b^{(1)}\circ c^{(1)}) = b^{(1)} \circ c^{(1)} + c^{(1)} \circ b^{(1)} \), we have
\[
-dd^{(1)} = c^{(1)} \circ b^{(1)}.
\]

**Lemma 4.3.2.** Let \( E_1 \) be the 1-reducible GMA over \( \mathbb{F}_p[\epsilon] \). Let \( \rho_1 : G_{\mathbb{Q}, S} \to E^\times_1 \) be the function given in coordinates by
\[
(4.3.3) \quad \rho_1 = \begin{pmatrix} \omega(1 + a^{(1)}\epsilon) & b^{(1)} \\ \omega c^{(1)} & 1 + d^{(1)}\epsilon \end{pmatrix}.
\]
Then \( \rho_1 \) is a homomorphism that is \( US_N \). In particular, the associated pseudorepresentation
\[
D_1 := \psi(\rho_1), \quad \text{Tr}D_1 = \omega + 1 + \epsilon(b^{(1)}\circ c^{(1)} + (\omega - 1)a^{(1)}) : G_{\mathbb{Q}, S} \to \mathbb{F}_p(\epsilon)
\]
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 \(\rho_1\) can readily be checked to be equivalent to the following equalities of 2-coboundaries: \(db^{(1)} = 0\), \(dc^{(1)} = 0\), \(-da^{(1)} = b^{(1)} \sim c^{(1)}\) and \(-dd^{(1)} = c^{(1)} \sim b^{(1)}\). 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 \(\rho_1\) by \((-x_{c^{(1)},1})\) we find that

\[
\text{ad}((-1, 0))|_p = \begin{pmatrix}
\omega(1 + (a^{(1)}|_p - b^{(1)}|_p \sim x_{c^{(1)}})c) & b^{(1)}|_p \\
0 & 1 - (a^{(1)}|_p - b^{1}|_p \sim x_{c^{(1)})}c)
\end{pmatrix}
\]

Since \(a^{(1)}|_p - b^{(1)}|_p \sim x_{c^{(1)}}|_p\) is an unramified element of \(\mathbb{Z}^1(\mathbb{Q}_p, \mathbb{F}_p)\) and \(b^{(1)}\) induces a finite-flat extension of \(\mathbb{F}_p\) by \(\mathbb{F}_p(1)\) by Lemma 2.2.13, \(\rho_1|_p\) is finite-flat by Lemmas 2.2.15 and 4.1.9.

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

\[
(\rho_1(\sigma) - \omega(\sigma))|_p(\tau(\tau) - 1) = \begin{pmatrix}
\epsilon a^{(1)}(\sigma) & 0 \\
\epsilon c^{(1)}(\sigma) & \epsilon d^{(1)}(\sigma)
\end{pmatrix} \begin{pmatrix}
\epsilon a^{(1)}(\tau) & 0 \\
\epsilon c^{(1)}(\tau) & \epsilon d^{(1)}(\tau)
\end{pmatrix} = 0
\]

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

\[
(\rho_1(\sigma) - \omega(\sigma))(\rho_1(\tau) - 1) = \begin{pmatrix}
\epsilon a^{(1)}(\sigma) & b^{(1)}(\sigma) \\
0 & 1 - \omega(\sigma) + \epsilon d^{(1)}(\sigma)
\end{pmatrix} \begin{pmatrix}
\omega(\tau) - 1 + \epsilon a^{(1)}(\tau) & b^{(1)}(\tau) \\
(1 - \omega(\sigma))d^{(1)}(\tau)
\end{pmatrix} = 0
\]

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.

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

Note that \(\rho_1, D_1\) and the homomorphism \(R \to \mathbb{F}_p[\epsilon_1]\) depend only on the pinning data of Definition 1.6.1. 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 \((\rho_N, E, D_E)\) from Definition 2.2.19. By the universal property, the representation \(\rho_1\) 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
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 2.2.19) 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]. \(\square\)

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 1.6.1).

### 5. The Pseudodeformation Ring \(R/pR\) Up to Second Order

Recall from Definition 2.2.19 that \(R\) denotes the pseudodeformation ring of \(\omega \oplus 1\) with the US\(N\) condition. Let \(\m \subset R/pR\) denote the maximal ideal. In this section, we prove that \(\dim_{\mathbb{F}_p} R/(p, \m^2) = 3\) while \(\dim_{\mathbb{F}_p} R/(p, \m^3) \leq 4\), also identifying a generator of \(\m^2\). These results are summed up in Corollary 5.3.3. In the sequel, we will use these results to establish a presentation of \(R/(p, \m^3)\) and to distinguish between the cases \(\dim_{\mathbb{F}_p} R/(p, \m^3) = 3\) and \(\dim_{\mathbb{F}_p} R/(p, \m^3) \geq 4\), keeping in mind that we have a surjection \(R \rightarrow \mathbb{T}\) from Proposition 2.2.20. As always, Assumption 1.2.2 is in force.

#### 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 \(R_D\) [Bel12].

Let \(J^\text{red}_D \subset R_D\) denote the reducibility ideal and \(R^\text{red}_D = R_D/J^\text{red}_D\), and let \(E^\text{an}_D = \left( C_{\text{an}}^D, R_D \right)\) be the \(R_D\)-GMA structure on \(E^\text{an}_D\). On the other hand, let \(t^\text{irr}_D\) be the cokernel of the natural map \(t^\text{red}_D \rightarrow t_{R_D}\); define \(t^\text{irr}_R\) analogously as the cokernel of \(t^\text{red}_R \rightarrow t_R\). We will address these tangent spaces mainly through their dual, which is the irreducible subspace of the cotangent space,
\[
(t^\text{irr}_R)^* \subset t^\text{irr}_R, \quad (t^\text{irr}_D)^* \subset t^\text{irr}_D.
\]
We will access these irreducible subspaces as follows. According to Proposition 2.3.1, the GMA-multiplication map induces a surjective $R_D$-module homomorphism

$$B_D \otimes_{R_D} C_D \to J_D^{\text{red}}, \quad b \otimes c \mapsto b \cdot c.$$ 

As a result, there is a composite surjection

$$(5.1.1) \quad B_D/m_B B_D \otimes_{F_p} C_D/m_B C_D \to J_D^{\text{red}}/m_B J_D^{\text{red}} \to (t^{\text{irr}}_{R_D})^*$$

of $F_p$-vector spaces. Bellaïche interprets this surjection in terms of cup products in Galois cohomology.

**Proposition 5.1.2** (Bellaïche [Bel12, Theorem A and §4.1.1]). There is an exact sequence

$$(5.1.3) \quad 0 \to t^{\text{irr}}_{R_D} \to H^1(Z[1/Np], F_p(1)) \otimes_{F_p} H^1(Z[1/Np], F_p(-1)) \cup \to H^2(Z[1/Np], F_p).$$

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

$$(5.1.4) \quad B_D/m_B B_D \cong (H^1(Z[1/Np], F_p(1)))^*, \quad C_D/m_B C_D \cong (H^1(Z[1/Np], F_p(-1)))^*,$$

the map $\iota$ is identified with the dual of $(5.1.1)$.

Applying the proposition under 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 5.1.5.** There is an element of $f \in B_D/m_B B_D \otimes_{F_p} C_D/m_B C_D$ satisfying

(i) under the dualities (5.1.4), $f(b_0 \otimes c_0) \neq 0$ and $f(b_1 \otimes c_0) = 0$ in $F_p$, and

(ii) $f$ maps to 0 under (5.1.1).

**Proof.** Since $b_0 \cup c_0 \neq 0$, it is not in the image of $\iota$, so there is an element $\lambda$ of the dual of $H^1(Z[1/Np], F_p(1)) \otimes_{F_p} H^1(Z[1/Np], F_p(-1))$ such that $\lambda(b_0 \otimes c_0) \neq 0$ and such that $\lambda$ is zero on the image of $\iota$. In particular, since $b_1 \cup c_0$ is zero, $b_1 \otimes c_0$ is in the image of $\iota$ and $\lambda(b_1 \otimes c_0) = 0$. Our identifications give an isomorphism between the dual of $H^1(Z[1/Np], F_p(1)) \otimes_{F_p} H^1(Z[1/Np], F_p(-1))$ and $B_D/m_B B_D \otimes_{F_p} C_D/m_B C_D$, and we can take $f$ to be the image of $\lambda$ under this identification.

Now we apply the computations in $R_D$ above, under the surjection $R_D \to R$, to calculate the irreducible subspace of the mod $p$ cotangent space of $R$. Along the way, we specify minimal sets of generators for $J^{\text{red}} \subset R$ and $J^{\text{red}} \subset \hat{R}.

**Proposition 5.1.6.** The ideal $J^{\text{red}} \subset \hat{R}$ is principal, generated by the non-zero image of $b_{\gamma_1} \cdot c_{\gamma_0}$ under $R \to \hat{R}$. In particular, the image of $b_{\gamma_1} c_{\gamma_0}$ in $t^H_{\hat{R}}$ generates the 1-dimensional subspace $(t_{\hat{R}}^{\text{irr}})^*$. In contrast, the ideal $J^{\text{red}} \subset R$ is not principal, and is generated by $\{b_{\gamma_0} c_{\gamma_0}, b_{\gamma_1} c_{\gamma_0}\}$.

**Proof.** First, we claim that $b_{\gamma_0} c_{\gamma_0}$ and $b_{\gamma_1} c_{\gamma_0}$ generate $J^{\text{red}}$. Due to Proposition 2.3.1 (which applies to any generalized matrix algebra and its scalar ring), 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 $J^{\text{red}}$. Due to the previous claim, it suffices to prove that $b_{\gamma_0} c_{\gamma_0}$ is a multiple of $b_{\gamma_1} c_{\gamma_0}$ in $J^{\text{red}}$. Just as in (5.1.1), there is a
similar map for $J^\text{red}$ fitting into a commutative diagram
\[
\begin{align*}
B_D/m_DB_D \otimes_{\mathbb{F}_p} C_D/m_DC_D & \longrightarrow J_D^\text{red}/m_D J_D^\text{red} \\
B/mB \otimes_{\mathbb{F}_p} C/mC & \longrightarrow J^\text{red}/mJ^\text{red}
\end{align*}
\]
Under the interpretation of $B_D/m_DB_D$ and $C_D/m_DC_D$ as dual vector spaces found in (5.1.4), the left 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 $\{b_{\gamma_0}, b_{\gamma_0}\}$ of $B/mB$ is dual to the basis $\{b_0, b_1\}$ of Galois cohomology; and $\{c_{\gamma_0}\}$ is a basis of $C/mC$, dual to $\{c_0\}$.

Now consider the element $f \in B_D/m_DB_D \otimes_{\mathbb{F}_p} C_D/m_DC_D$ from Lemma 5.1.5. The image of $f$ in $B/mB \otimes_{\mathbb{F}_p} C/mC$ is of the form $(xb_{\gamma_0} + yb_{1}) \otimes c_{\gamma_0}$ 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 diagram (5.1.7) and the fact that $f$ maps to 0 in $(t_D^\text{im})^* \subset t_D^*$ imply that
\[
b_{\gamma_0} \cdot c_{\gamma_0} = -x^{-1}yb_{1} \cdot c_{\gamma_0} = 0
\]
in $t_R^*$, completing the claim that $b_{1} \cdot c_{\gamma_0}$ generates $J^\text{red}$.

Next we prove that $t_R^\text{im} \cong (J^\text{red}/mJ^\text{red})^*$ is 1-dimensional. It remains to show that $t_R^\text{im}$ is not zero. This follows from the existence of the irreducible first-order pseudodeformation $D_1$ of $\psi(\omega \oplus 1)$ of $\mathbb{F}_p[e_1]$ constructed in Lemma 4.3.2, because the lemma showed that $D_1$ satisfies USN.

It remains to show that $J^\text{red}$ is not principal. If it were principal, then the image of $b_{\gamma_0}c_{\gamma_0}$ in $J^\text{red}$ is a generator, $b_{\gamma_0}c_{\gamma_0} \in J^\text{red}$ would be a generator. But $b_{\gamma_0}c_{\gamma_0}$ vanishes under $R \rightarrow R_0$, because the Galois pseudorepresentations parameterized by $R_0$, are unramified at $\ell_1$ (hence $b_{\gamma_0}$ maps to zero in the global level $\ell_0$ $R_0$-GMA). This would imply that the pseudorepresentation supported by $R_0$ is reducible. But this implication is known to be false: the Galois representation supported by the level $\Gamma_0(\ell_0)$ cusp form $f$ of Assumption 1.2.2(3) is irreducible.

Now we can calculate the whole tangent space of $R$.

**Proposition 5.1.8.** The $\mathbb{F}_p$-dimension of $t_R$ is 2, with a basis given by the two maps $\varphi_D^\text{red}, \varphi_{D_1} : R \rightarrow \mathbb{F}_p[e]/(e^2)$ specified in Lemma 2.3.2 and Lemma 4.3.2, respectively. More precisely:

1. The subspace $t_R^\text{red} \subset t_R$ is 1-dimensional and spanned by $D^\text{red}$.
2. The space $t_R^\text{im}$ is one-dimensional and the element $D_1$ of $t_R$ maps to a generator of it under the natural surjection $t_R \rightarrow t_R^\text{im}$.

**Proof.** Since there is an exact sequence
\[
0 \rightarrow t_R^\text{red} \rightarrow t_R \rightarrow t_R^\text{im} \rightarrow 0
\]
it is enough to show (1) and (2). Part (1) follows from the isomorphisms
\[
R^\text{red}/pR^\text{red} \cong \mathbb{F}_p[y]/(y^2)
\]
of Lemma 2.3.2.

Part (2) follows from Proposition 5.1.6 (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. Having characterized $\bar{R}/\bar{m}^2$, we begin toward calculating $\bar{R}/\bar{m}^3$, ultimately showing in Corollary 5.3.3 that $\bar{m}^2/\bar{m}^3$ is at most 1-dimensional. The first step is the following proposition, which will be used to show that lifts of certain cotangent vectors to $\bar{R}/\bar{m}^3$ must have product zero. The idea is that $C$ is a factor of the irreducible cotangent vector under (5.1.7), so it will be useful to show that $C$ is killed by the reducible cotangent vector.

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 $C \otimes_{R, \text{red}} \mathbb{F}_p[\epsilon_1]$ is $\epsilon$ (here the tensor product is with respect to the ring map \( \varphi_{\text{red}} : R \to \mathbb{F}_p[\epsilon_1] \) defined in Lemma 2.3.2).

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

Let $\bar{C} := C \otimes_{R, \text{red}} \mathbb{F}_p[\epsilon_1]$. 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 $c_{\gamma_0}$. Because $D^{\text{red}}$ is reducible, the $B$-coordinate $B_{E'}$ of the $\mathbb{F}_p[\epsilon_1]$-GMA $E' = E \otimes_{R, \text{red}} \mathbb{F}_p[\epsilon_1]$ is a two-sided ideal; indeed, the reducibility implies that $B_{E'} \cdot C_{E'}$ is the reducibility ideal in $\mathbb{F}_p[\epsilon_1]$, which is the zero ideal. The quotient by $B_{E'}$ has the form

$$E'' := \left( \begin{array}{cc} \mathbb{F}_p[\epsilon_1] & \mathbb{F}_p[\epsilon_1] \\ \bar{C} & \mathbb{F}_p[\epsilon_1] \end{array} \right) \xrightarrow{\sim} \left( \begin{array}{cc} \mathbb{F}_p[\epsilon_1] & \mathbb{F}_p[\epsilon_1] \\ \mathbb{F}_p[\epsilon_1] & \mathbb{F}_p[\epsilon_1] \end{array} \right) \subseteq M_2(\mathbb{F}_p[\epsilon_1])$$

(where we used $c_{\gamma_0}$ as a generator of $\bar{C}$ to draw the isomorphism) receiving a homomorphism from $\mathbb{F}_p[\epsilon_1][G_{\bar{C}}]$ of the form

$$\left( \begin{array}{cc} \omega(1 + c_{\gamma_0}) & 0 \\ \omega(c^{(1)} + \epsilon c^{(2)}) & 1 - c_{\gamma_0} \end{array} \right).$$

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, and we use these coordinates under the surjection $E \to E'$.

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

$$-d_c^{(2)} = a_0 - c^{(1)} + c^{(1)} - (-a_0).$$

The right hand side is in the cohomology class of $2a_0 \cup c_0$. But our assumption $\text{rk}_{\mathbb{Z}} T_{\gamma_0} = 2$ 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. \( \square \)

5.3. The ring $S := \bar{R}/\bar{m}^3$. Let $S := \bar{R}/\bar{m}^3$. Because $S$ surjects onto $\bar{R}/\bar{m}^2$ and Proposition 5.1.8 describes the 2-dimensional cotangent space $t^*_R = \bar{m}/\bar{m}^2$, 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. Otherwise, a priori we know that $\dim_{\mathbb{F}_p} S \leq 6$. Our goal is to refine this bound to $\dim_{\mathbb{F}_p} S \leq 4$ and to show that $(J^{\text{red}})^2 = \bar{m}^2$. 


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

**Proposition 5.3.1.** The inclusion of ideals \((J^\text{red}_S)^2 \subset m_SJ^\text{red}_S\) is an equality.

*Proof.* Let \( C_S := C \otimes_R S \), and likewise \( B_S := B \otimes_R S \).

We claim that \( m_S C_S \subset J^\text{red}_S C_S \), 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 \( S^\text{red} \) kills \( C^\text{red} \). Lifting this result from \( S^\text{red} \)-modules to \( S \)-modules, we find that \( m_S C_S \subset J^\text{red}_S C_S \), which is the desired result.

We derive from the equality \( m_S C_S = J^\text{red}_S C_S \) that, for all \( x \in m_S \), there exists some \( z \in J^\text{red}_S \) such that \( xc_{\gamma_0} = zc_{\gamma_0} \), and that every element of \( m_S J^\text{red}_S \) has this form because \( c_{\gamma_0} \) generates \( C_S \). We apply this to the surjection of \( S \)-modules \( C_S \otimes_S B_S \twoheadrightarrow J^\text{red}_S \), also using that \( c_{\gamma_0} b_{\gamma_1} \) is a generator of the principal ideal \( J^\text{red}_S \) (Proposition 5.1.6).

Namely, finding that every element of \( m_S J^\text{red}_S = m_S C_S B_S \) has the form \( x(c_{\gamma_0} b_{\gamma_1} s) = (xc_{\gamma_0})(b_{\gamma_1} s) = z(c_{\gamma_0} b_{\gamma_1}) s \in (J^\text{red}_S)^2 \), for some \( s \in S \), and with \( x \) and \( z \) as in (5.3.2). \(\Box\)

**Corollary 5.3.3.** Either \( \dim_{\mathbb{F}_p} S = 3 \) or \( \dim_{\mathbb{F}_p} S = 4 \). In general, \( \dim_{\mathbb{F}_p} S = \dim_{\mathbb{F}_p} J^\text{red}_S + 2 = \dim_{\mathbb{F}_p}(J^\text{red}_S)^2 + 3 \).

Consequently, \((J^\text{red}_S)^2 = \bar{m}^2 \) in \( \bar{R} \).

*Proof.* Because \( S^\text{red} = S/J^\text{red}_S \) is 2-dimensional, we have \( \dim_{\mathbb{F}_p} S = 2 + \dim_{\mathbb{F}_p} J^\text{red}_S \) in general.

Because \( J^\text{red}_S \subset m_S \) and \( m^3_S = 0 \), we have a filtration \( J^\text{red}_S \supset m_S J^\text{red}_S \supset m^2_S J^\text{red}_S = 0 \).

The principality of \( J^\text{red}_S \) (Proposition 5.1.6) implies that \( \dim_{\mathbb{F}_p} J^\text{red}_S/m_S J^\text{red}_S = 1 \).

The equality \( m_S J^\text{red}_S = (J^\text{red}_S)^2 \) of Proposition 5.3.1 implies that \( \dim_{\mathbb{F}_p} m_S J^\text{red}_S \leq 1 \).

The final claim follows from Nakayama’s lemma. \(\Box\)

### 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 \( S = R/(p, m^3) \)) and derive consequences for Galois cohomology. The main results are Propositions 6.2.9 and 6.4.1, which together essentially prove one direction of Theorem 1.3.3 from the introduction. Of note, Proposition 6.4.1 gives an optimal presentation of \( S \).
6.1. A GMA over $S$ when $\dim_p S = 4$. Henceforth, let $y$ be the image of $b_{\gamma_1} \cdot c_{\gamma_0}$ in $S$, which generates the principal ideal $J_S^{\text{red}} \subset S$. According to Corollary 5.3.3, the $F_p$-dimension of $J_S^{\text{red}}$ is 2. Since $J_S^{\text{red}}$ is principal, its annihilator $\text{Ann}_S(J_S^{\text{red}})$ is also 2-dimensional. Consider the ring homomorphism

$$(6.1.1) \quad S \xrightarrow{\text{Ann}_S(J_S^{\text{red}})} \cong \mathbb{F}_p[\epsilon_1],$$

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

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

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

$$\varphi_{D_y} : R \to S \xrightarrow{\text{Ann}_S(J_S^{\text{red}})} \cong \mathbb{F}_p[\epsilon_1]$$

determined by the isomorphism $S/\text{Ann}_S(J_S^{\text{red}}) \xrightarrow{\sim} \mathbb{F}_p[\epsilon_1]$ above.

- We also allow ourselves to identify $J_S^{\text{red}}$ with $\mathbb{F}_p[\epsilon_1]$, as $S$-modules where $\mathbb{F}_p[\epsilon_1]$ has structure map $\varphi_{D_y}$, under the isomorphism

$$(6.1.1) \quad \mathbb{F}_p[\epsilon_1] \xrightarrow{(6.1.1)} S/\text{Ann}_S(J_S^{\text{red}}) \xrightarrow{\sim} J_S^{\text{red}},$$

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 $m_S J_S^{\text{red}} = y^2 S$ (Proposition 5.1.6), 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 $\dim_p S = 4$. There are surjective $S$-module homomorphisms (which we will call coordinate maps)

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

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

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

Using these surjections $B_S \to \mathbb{F}_p \oplus \mathbb{F}_p[\epsilon_1]$ and $C_S \to \mathbb{F}_p[\epsilon_1]$ and the identification $J_S^{\text{red}} = \mathbb{F}_p[\epsilon_1]$ sending $y$ to 1, the GMA-multiplication map

$$(6.1.4) \quad B_S \otimes_S C_S \to J_S^{\text{red}}$$

induces the map

$$\left( \mathbb{F}_p \oplus \mathbb{F}_p[\epsilon_1] \right) \otimes_{\mathbb{F}_p[\epsilon_1]} \mathbb{F}_p[\epsilon_1] \to \mathbb{F}_p[\epsilon_1]$$

given by

$$(u, v) \otimes z \mapsto \eta uz + vz.$$
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 \(gb_{\gamma_0} + hb_{\gamma_1} = 0 \in B_S\) (for \(g, h \in S\)) must have \(g, h \in m_S\), since \(B_S\) is not cyclic. Therefore, no relation \(gb_{\gamma_0} + hb_{\gamma_1}\) can possibly map to something non-zero under the coordinate map for \(B_S\), since this would imply that
\[
0 = gb_{\gamma_0}c_{\gamma_0} + hb_{\gamma_1}c_{\gamma_0} = g\eta y^2 + hy = hy \text{ in } J_S^{\text{red}},
\]
for some \(h\) such that \(\varphi_{D_y}(h) \neq 0\), contradicting \(\text{Ann}_S(y) = \ker \varphi_{D_y}\). Consequently, the coordinate map for \(B_S\) is well defined.

It remains to verify that the square of surjections
\[
\begin{array}{ccc}
B_S \otimes_S C_S & \rightarrow & J_S^{\text{red}} \\
(F_p \oplus F_p[\epsilon_1]) \otimes_{F_p[\epsilon_1]} F_p[\epsilon_1] & \rightarrow & F_p[\epsilon_1]
\end{array}
\]
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 \(\eta \epsilon \in F_p[\epsilon_1]\); on the other hand, \(b_{\gamma_0}c_{\gamma_0} \in J_S^{\text{red}}\) has the form \(\eta y^2\) by definition of \(\eta\), which also maps to \(\eta \epsilon \in F_p[\epsilon_1]\) under the coordinate map for \(J_S^{\text{red}}\).

The coordinates of \(b_{\gamma_1} \otimes c_{\gamma_0}\) are \((0, 1) \otimes 1\), which maps to \(1 \in F_p[\epsilon_1]\); on the other hand, \(b_{\gamma_1}c_{\gamma_0} \in J_S^{\text{red}}\) equals \(y\), which also maps to \(1 \in F_p[\epsilon_1]\) under the coordinate map \(J_S^{\text{red}} \rightarrow F_p[\epsilon_1]\). \(\square\)

Let \(E_S'\) denote the \(S\)-GMA
\[
(6.1.5) \quad E_S' = \left( \begin{array}{c}
S \\
F_p \oplus F_p[\epsilon_1] \\
S
\end{array} \right)
\]
where \(F_p[\epsilon_1]\) is a \(S\)-module via the map \(\varphi_{D_y} : S \rightarrow F_p[\epsilon_1]\), and where the GMA-multiplication map is given by \((6.1.4)\). By Lemma 6.1.3, the coordinate maps comprise a surjective morphism of \(S\)-GMAs
\[
E \otimes_R S \rightarrow E_S'.
\]

6.2. The coordinates of a \(S\)-GMA valued Galois representation when \(\dim_{F_p} S = 4\). Now consider the Cayley–Hamilton representation \(\rho_S : G_{Q,N_p} \rightarrow (E_S')^\times\) obtained as composition of the universal Cayley–Hamilton representation \(\rho : G_{Q,N_p} \rightarrow E^\times\) with \(E \rightarrow E_S'\). We are interested in endowing it with coordinates and comparing these coordinates to the 1-reducible GMA representation \(\rho_1 : G_{Q,N_p} \rightarrow E_1^\times\) 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 \(\{D^{\text{red}}, D_y\}\) is a basis of \(t_R\) according to Proposition 5.1.8, because \(D^{\text{red}}\) is reducible, \(D_y\) is irreducible, and \(\dim_{F_p} t_R = 2\).

**Definition 6.2.1.** Let \(x \in S\) denote a generator for \(\text{Ann}_S(J_S^{\text{red}})\) whose image \(\bar{x} \in t_R^* = m_S/m_S^2\) makes \(\bar{x}, \bar{y}\) a dual basis to \(\{D^{\text{red}}, D_y\}\).

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 \( S \),

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

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 \( (y^2) = (J_S^{red})^2 \).

Proof. The ideal \( \text{Ann}_S(J_S^{red}) \subset S \) is contained in \( m_S \) because \( J_S^{red} \neq 0 \). On the other hand, \( \text{Ann}_S(J_S^{red}) \) is not contained in \( m_S^2 \) because \( \dim_{\mathbb{F}_p} m_S^2 = 1 \) while \( \dim_{\mathbb{F}_p} \text{Ann}_S(J_S^{red}) = 2 \). Therefore \( \text{Ann}_S(J_S^{red}) \) has 1-dimensional image under the projection \( m_S \to m_S / m_S^2 = \mathfrak{t}_R \). This image is complementary to \( (\mathfrak{t}_R^\mathfrak{r})^* = (\bar{y}) \) because \( y^2 \neq 0 \), yet every element of \( \text{Ann}_S(J_S^{red}) \) kills the generator \( y \) of \( J_S^{red} \).

Similarly, \( \text{Ann}_S(J^{red}) \subset S \) is the kernel of \( \varphi_{D_y} \), so there exists a generator \( x \) of \( \text{Ann}_S(J_S^{red}) \) such that

\[
\{\bar{x}, \bar{y}\} \text{ is a dual basis to } \{D_{\varphi}, D_y\}.
\]

In particular, \( x \) and \( y \) generate \( S \) as an \( \mathbb{F}_p \)-algebra, and we have a surjection \( \phi : \mathbb{F}_p[X, Y] \to S \) 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 \( m_S^3 = 0 \). Likewise, we know that \( XY \in \ker \phi \) because \( x \in S \) satisfies \( xJ_S^{red} = 0 \) 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 \( J_S^{red} = (y^2) \) and the fact that \( m_S^2 = (J_S^{red})^2 = (y^2) \) is 1-dimensional over \( \mathbb{F}_p \) (Propositions 5.1.6 and 5.3.1), since we know from the start that \( x^2 \in m_S^2 \).

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 \( \text{Ann}_S(J_S^{red}) \), 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 \( \mu \) clear, since \( x^2 \) only depends upon \( \bar{x} \). \( \square \)

Combining the coordinates of \( S \) from Lemma 6.2.2 with the coordinates for the off-diagonal parts of \( E^0_\mathbb{C} \) from (6.1.5), we produce a coordinate-wise description of \( \rho_S : G_{\mathbb{Q}, \mathbb{N}_p} \to (E^0)^\times \).

\[
(6.2.3) \quad \rho_S = \left( \begin{array}{ll}
\omega(1 + y a^{(1)'}) & (b_0^{(1)} + y b^{(2)'}) \\
\omega(x a^{(2)'}) & 1 + y d^{(1)' + y d^{(2)' - x a_0}'}
\end{array} \right)
\]

for some cocycles

\[
\begin{align*}
& a^{(1)'} : G_{\mathbb{Q}, \mathbb{N}_p} \to \mathbb{F}_p, \\
& b^{(2)'} : G_{\mathbb{Q}, \mathbb{N}_p} \to \mathbb{F}_p(1), \\
& c^{(2)'} : G_{\mathbb{Q}, \mathbb{N}_p} \to \mathbb{F}_p(-1),
\end{align*}
\]

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 \( D_{\varphi} \in \mathfrak{t}_R \) is dual to \( \bar{x} \in \mathfrak{t}_R \), and we observe that the pseudorepresentation induced by \( \rho_S \otimes_S \varphi \) on \( \mathbb{F}_p(1) \) is exactly \( D_{\varphi} \) (keep in mind that \( \varphi_{D_{\varphi}}(x) = c, \varphi_{D_{\varphi}}(y) = 0 \)).
Proposition 2.2.11 implies the vanishing of \( a G (2) \).

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

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 \( \rho_S' \) onto the \( \rho_1 : G_{Q,Np} \rightarrow E_i^\psi \) 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 \( \rho_S' \) implies that \( a^{(1)}' \) satisfies the differential equation

\[
- da^{(1)}' = b^{(1)} \sim c^{(1)},
\]

which \( a^{(1)} \) also satisfies (Lemma 4.2.1). We note that the fact that \( \rho_S' \) has constant determinant \( \omega \) implies that \( d^{(1)}' = b^{(1)}c^{(1)} - a^{(1)} \), just as in the discussion of \( d^{(1)} \) in \( \S 4.3 \).

There are even more differential equations implied by the fact that \( \rho_S' \) is a homomorphism,

\[
- dc^{(2)}' = a^{(1)} \sim a^{(1)} + d^{(1)}' \sim c^{(1)}
\]

\[
- db^{(2)} = a^{(1)} \sim b^{(1)} + d^{(1)} \sim d^{(1)}.
\]

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

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

**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 \( \mathbb{D} \). 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 \( \rho_S' \) 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 2.2.11 implies the vanishing of \( (a^{(1)}' + b^{(1)} - x_{c^{(1)}})|_{\ell_0} \), 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 \( \ell_0 \), equation (6.2.5) implies that \( a^{(1)}' \big|_{\ell_0} \) is a cocycle and \( 2(c^{(1)} - a^{(1)}') \big|_{\ell_0} \) 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 \( \phi(\rho_S') : G_{Q,Np} \rightarrow S \) induces \( D_1 \) via \( S \rightarrow \mathbb{F}_p[\epsilon_1], x \mapsto 0, y \mapsto \epsilon \).
while, on the other hand, this map \( S \to \mathbb{F}_p[\ell_1] \) is exactly the same as \( \varphi_{D_\rho} \). □

There are even more implications of the differential equations implied by the existence of \( \rho'_S \). 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 \( da^{(1)} = b^{(1)} \sim c^{(1)} \) and \( c^{(1)}|_{\ell_1} = 0 \)).

**Proposition 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

\[
(6.2.10) \quad a^{(1)} \cup b^{(1)} + b^{(1)} \cup d^{(1)}
\]

vanishing in \( H^2(G_{\mathbb{Q}, N_p}, \mathbb{F}_p(1)) \). 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 \( G_{\ell_1} \) 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

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

**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 \( -da^{(1)} = b^{(1)} \sim c^{(1)} \), 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\(_S\) property of \( \rho'_S \). The fact that \( \rho'_S \) is unramified-Steinberg at \( \ell_0 \) 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
\[
\frac{\mathbb{F}_p[X,Y]}{(X^2, XY, Y^2)}
\]

**Remark 6.4.2.** Since \( \alpha \) depends only on the pinning data of Definition 1.6.1, part (1) implies that \( \beta' \) depends only on this data as well.

**Proof.** Since \( \rho_S' \) is obtained as a quotient of the universal \( \text{US}_N \) Cayley–Hamilton representation \( E \), it is also \( \text{US}_N \). Let \( \sigma \in G_{\ell_0} \) and \( \tau \in I_{\ell_0} \). By Definition 2.2.2, the fact that \( \rho_S' \) is \( \text{US}_N \) implies that
\[
(\rho_S'(\sigma) - \omega(\sigma))(\rho_S'(\tau) - 1)
\]
vanishes in \( E_S' \). Consider the top-left coordinate of (6.4.3) in terms of the GMA decomposition (6.2.3) of \( \rho_S' \). 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
\[
(a^{(1)}(\sigma)a^{(1)}(\tau) + (b^{(2)}(\sigma) + \eta b_0^{(1)}(\sigma))c^{(1)}(\tau)) y^2 + a_0(\sigma) a_0(\tau)x^2.
\]
Recall from the presentation given in Lemma 6.2.2 that \( x^2 = \mu y^2 \) in \( S \). Using the relations
\[
a^{(1)}|_{\ell_0} = \alpha - c^{(1)}|_{\ell_0}, \quad (b^{(2)} + \eta b_0^{(1)})|_{\ell_0} = \beta' - c^{(1)}|_{\ell_0}
\]
that define \( \alpha \) and \( \beta' \), (6.4.4) then simplifies to
\[
((\alpha^2 + \beta')c^{(1)}(\tau) + \mu a_0(\tau) a_0(\sigma)) y^2.
\]
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
\[
(\alpha^2 + \beta')c^{(1)}(\tau)|_{\ell_0} + \mu a_0(\tau) a_0|_{\ell_0} = 0,
\]
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 \( c^{(1)}|_{\ell_0} \) and \( a_0|_{\ell_0} \) are nonzero, this gives the result. \( \square \)

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 \( \Upsilon_2(u, v) = \eta u + v \) induces a map of \( \mathbb{F}_p[\epsilon_2] \)-GMAs
\[
E_S' \otimes_S \mathbb{F}_p[\epsilon_2] \xrightarrow{(D_2, \Upsilon_2)} E_2.
\]
In particular, there is an \( \text{US}_N \) Cayley–Hamilton representation \( \rho_2 : G_{Q,Np} \to E_2^\times \) that deforms \( \rho_1 \) along the map \( r_{2,1} : E_2 \to E_1 \) of (4.1.7).
Proof. Given that \( \mu = 0 \), the fact that \( \left( D_2, T_2 \right) \) is ring homomorphism is a simple computation using the formula (6.1.4) for multiplication in \( E_{\beta}^1 \). The representation \( \rho_2 \) is obtained as the composition of \( \rho_2' \) with \( E_{\beta}' \otimes_{\mathbb{F}_p} \mathbb{F}_p[\ell_2] \to E_2 \). \( \Box 
\]

7. Constructing a second-order US\(_N\) deformation \( \rho_2 \)

In this section, we prove the remaining implication of Theorem 1.3.3. 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\(_p\) \( R/pR > 3 \). 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\(_p\) \( R/pR > 3 \) 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

\[
\rho_1 = \left( \begin{array}{cc}
\omega(1 + e^{(1)}) & b^{(1)} \\
\omega c^{(1)} & 1 + e^{(1)}
\end{array} \right) : G_{\mathbb{Q},N_p} \to E_1^\times
\]

of Lemma 4.3.2. Let \( \Pi_2 \) denote the set of second-order 1-reducible Cayley–Hamilton deformations of \( \rho_1 \):

\[
\Pi_2 = \{ \rho_2 : G_{\mathbb{Q},N_p} \to E_2^\times | r_{2,1} \circ \rho_2 = \rho_1 \},
\]

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

Lemma 7.1.1. The set \( \Pi_2 \) is in bijection with the set quadruples of cochains \( a^{(2)}, d^{(2)} : G_{\mathbb{Q},N_p} \to \mathbb{F}_p, b^{(2)} : G_{\mathbb{Q},N_p} \to \mathbb{F}_p(1), \) and \( c^{(2)} : G_{\mathbb{Q},N_p} \to \mathbb{F}_p(-1) \) that satisfy

\[
\begin{align*}
(i) \quad & -da^{(2)} = a^{(1)} + b^{(1)} + c^{(2)} + b^{(2)} - c^{(1)} \\
(ii) \quad & -db^{(2)} = a^{(1)} + b^{(1)} + c^{(2)} - d^{(1)} \\
(iii) \quad & -dc^{(2)} = a^{(1)} + d^{(1)} - c^{(1)} \\
(iv) \quad & -dd^{(2)} = d^{(1)} - d^{(1)} + c^{(1)} - b^{(2)} + c^{(2)} - b^{(1)}.
\end{align*}
\]

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

(1) \( \Pi_2 \) admits the structure of a torsor under the group

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

where

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

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

\[
\begin{align*}
(a, d, 0, 0) \cdot (a^{(2)}, d^{(2)}, b^{(2)}, c^{(2)}) &= (a^{(2)} + a, d^{(2)} + d, b^{(2)} + b, c^{(2)}) \\
(0, 0, b, c) \cdot (a^{(2)}, d^{(2)}, b^{(2)}, c^{(2)}) &= (a^{(2)} + \sigma(b, c), d^{(2)} - \sigma(b, c) + b \cdot c^{(1)} + b^{(1)} \cdot c, b^{(2)} + b, c^{(2)} + c)
\end{align*}
\]
Proof. Every element \( \rho \) of the equations (i)-(iv). Conversely, given cochains satisfying (i)-(iv), the function \( \rho_2 \) defined by (7.1.2) is an element of \( \Pi_2 \). 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 Proposition 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 \( \Pi_2 \) 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

\[
\begin{align*}
c^{(1)} \cup a^{(1)} + d^{(1)} \cup c^{(1)} &= 0 \\
\end{align*}
\]

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 \( \ell_1 \)-local restriction vanishes because \( a^{(1)}|_{\ell_1} = d^{(1)}|_{\ell_1} = 0 \). Since \( d^{(1)}|_{\ell_0} = -a^{(1)}|_{\ell_0} \), the \( \ell_0 \)-local restriction is

\[
\begin{align*}
c^{(1)}|_{\ell_0} \cup a^{(1)}|_{\ell_0} - a^{(1)}|_{\ell_0} \cup c^{(1)}|_{\ell_0},
\end{align*}
\]

which vanishes because \( a^{(1)}|_{\ell_0} = a \cup c^{(1)}|_{\ell_0} \). 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

\[
\begin{align*}
a^{(1)} &\sim a^{(1)} + b^{(1)} \sim c^{(2)} + b^{(2)} \sim c^{(1)}
\end{align*}
\]

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

\[
\begin{align*}
b^{(2)}|_{\ell_0} &\sim c^{(1)}|_{\ell_0}
\end{align*}
\]

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 \( [b^{(1)}]|_{\ell_0} \cup [c^{(1)}]|_{\ell_0} \) by Proposition 3.2.9, there is a constant \( \gamma \in \mathbb{F}_p \) such that

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

- \( \Pi_2 \) 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 \( \Pi_2 \) that acts by addition on the \( b^{(2)} \) and \( c^{(2)} \)-coordinates
- And there exists a linear choice of \( \sigma \), namely
  \[
  Z_b^1 \times Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p(-1)) \ni (b, c) \mapsto -d^{-1}(b \sim c^{(1)} + b^{(1)} \sim c)
  \]

where \( d^{-1} \) is an arbitrarily chosen linear section of the boundary map \( d : C^1(\mathbb{Z}[1/Np], \mathbb{F}_p) \to B^2(\mathbb{Z}[1/Np], \mathbb{F}_p) \). Under this definition of \( \sigma \), 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 \( \Pi_2 \) 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 \( \Pi_2 \) consisting of elements with constant determinant \( \omega \),

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

**Lemma 7.1.4.** Assume \( a^{(1)}|\ell_1 = 0 \). Then \( \Pi_2^{\det} \) is non-empty, an element \( \rho_2 \in \Pi_2^{\det} \) is completely determined by its cochains \( a^{(2)}, b^{(2)} \) and \( c^{(2)} \), and \( \Pi_2^{\det} \) is a torsor for the subgroup \( \mathcal{Z}_2^{\det} \subset \mathcal{Z}_2 \) under the action of \( \mathcal{Z}_2 \) on \( \Pi_2 \) of Lemma 7.1.1, where

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

**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 \( \rho_2 \) 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 \((a, b, c, d) \in \mathcal{Z}_2 \) fixes the determinant if and only if \( a + d = 0 \). This follows from the equations for the action of \( \mathcal{Z}_2 \) given in Lemma 7.1.1. \( \square \)

**7.2. The finite-flat at \( p \) condition on \( \rho_2 \).** 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 \( \Pi_2 \),

\[
\Pi_2^{\text{det}, p} := \{ \rho_2 \in \Pi_2^{\det} \mid \rho_2|p \text{ is finite-flat} \} \subset \Pi_2.
\]
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 $Z^1(\mathbb{Z}[1/N_p], \mathbb{F}_p(1))$ spanned by coboundaries and $b^{(1)}$. In particular, there is a unique $\beta \in \mathbb{F}_p(2)$ such that, for every $\rho_2 \in \Pi_2^{\det,p}$,

$$[b^{(2)}]_{t_0} = \beta \cup [c^{(1)}]_{t_0} \in H^1(\mathbb{Q}_e, \mathbb{F}_p(1)),$$

where $b^{(2)}$ is the cochain associated to $\rho_2$.

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 $\beta$ exists for any single $\rho_2 \in \Pi_2$; our supplemental work will be to show that there is only one $\beta$ 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 $\rho_1$ 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 $x_{c(t)} \in \mathbb{F}_p(1)$ of Definition 3.1.1 satisfying $dx_{c(t)}|_{p} = c^{(1)}|_{p}$. Define $\rho_2' := \text{ad}((-x_{c(t)} + y_{p} 0))^{|\rho_2}$ for $y \in \mathbb{F}_p$ to be chosen later, and write $\rho_2'$ as

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

Explicitly:

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

and

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

Just as in the proof of Lemma 4.3.2, we have

- $a^{(1)'_c}|_{p}$ and $d^{(1)'_c}|_{p}$ are unramified homomorphisms
- $c^{(1)'_c}|_{p} = 0$

Because $\rho_2'$ 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 $(a, -a, b, c) \in \mathcal{S}_2^{\det}$ such that $\rho_2|_{p,new} := (a, -a, b, c) \cdot \rho_2$ has the desired property.

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

$$-dc^{(2)'_c}|_{p} = c^{(1)'_c}|_{p} - a^{(1)'_c}|_{p} + d^{(1)'_c}|_{p} - c^{(1)'_c}|_{p} = 0$$

since $c^{(1)'_c}|_{p} = 0$. Hence $c^{(2)'_c}|_{p}$ is a cocycle.
Sublemma 7.2.6. The \( \mathbb{F}_p \)-dimension of \( H^1(\mathbb{Z}[1/Np], \mathbb{F}_p(-1)) \) is 1. The localization map \( H^1(\mathbb{Z}[1/Np], \mathbb{F}_p(-1)) \rightarrow H^1(\mathbb{Q}_p, \mathbb{F}_p(-1)) \) 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 \( H^\bullet(\mathbb{Z}, \mathbb{F}_p(-1)) \) is \(-1\). For the second claim, consider the exact sequence

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

coming from the definition of \( H^\bullet(\mathbb{Z}) \) 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. \( \square \)

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

Let \( \rho_2 \in \Pi_2^{\text{det}} \) be as in Lemma 7.2.5. Then

\[
(7.2.7) \quad \rho_2|_p = \begin{pmatrix} \chi_2 & (b(1)' + b(2)'|_p) \\ 0 & \chi_2^{-1} \end{pmatrix} : G_p \rightarrow E_2^X,
\]

where

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

Indeed, since \( \rho_2' \) is upper-triangular, \( \chi_2 \) is a homomorphism, and since \( \det(\rho_2') = \omega \), the lower-right coordinate of \( \rho_2'|_p \) must be \( \chi_2^{-1} \). Let \( \chi_1 : G_p \rightarrow \mathbb{F}_p[\epsilon_1]^X \) 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 \( \rho_2' \), bootstrapping from the fact that its reduction \( \rho_1 \) is finite-flat at \( p \). To this end, we induce two representations \( \eta_2 \) and \( \eta_1 \) associated to an element of \( \Pi_2^{\text{det}} \)

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

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

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

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

given by \( \rho_2' \) composed with the map \( E_2 \rightarrow M_2(\mathbb{F}_p[\epsilon_1]) \) of Lemma 4.1.10.

Remark 7.2.10. Note that

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

Also, be aware that \( \eta_1 \) does not equal the reduction of \( \eta_2 \) modulo \( \epsilon^2 \). Rather, one obtains \( \eta_1 \) from \( \eta_2 \) by “dividing the extension class \( \epsilon b(1)' + \epsilon^2 b(2)' \in \text{Ext}^1_{\mathbb{F}_p[\epsilon_2][G_p]}(\chi_2^{-1}, \omega \chi_2)^{\text{flat}} \) by \( \epsilon \),” which will be made rigorous in the proof of Lemma 7.2.11.
Lemma 7.2.11. Assume that $p_2 \in \Pi_{\text{det}}^\text{eff}$ has the property that $p_2|_p$ is upper-triangular, and let $\eta_2$ and $\eta_1$ be the associated representations of Definition 7.2.8. The following are equivalent:

1. The Cayley–Hamilton representation $p_2|_p$ is finite-flat.
2. The homomorphism $\eta_2$ is finite-flat.
3. The homomorphism $\eta_1|_p : G_p \to \text{GL}_2(\mathbb{F}_p[e_1])$ is finite-flat and $\chi_2$ is unramified.

Proof. The equivalence of (1) and (2) follows from the embedding of Lemma 4.1.9 along with Lemma 2.2.15.

Now we assume (2) and prove (3). By Proposition 2.2.11, $\chi_2$ is unramified. We will show that $\eta_1|_p$ is isomorphic to a subquotient representation of $\eta_2$. 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 $\mathbb{F}_p[e_2][G_p]$ with exact rows and columns

$$\begin{array}{cccc}
\text{Ext}^1(\chi_1^{-1}, \epsilon \omega \chi_2) & & & \\
0 & \text{Ext}^1(\chi_2^{-1}, \epsilon \omega \chi_2) & \text{Ext}^1(\chi_2^{-1}, \omega \chi_2) & \text{Ext}^1(\chi_2^{-1}, \omega)
\end{array}$$

The representation $\eta_2$ defines a class in $\text{Ext}^1(\chi_2^{-1}, \omega \chi_2)$, written as $e_b^{(1)'} + e^2 b^{(2)'}$. The fact that this class is a multiple of $\epsilon$ implies that $\eta_2$ maps to zero under both the horizontal and the vertical map out of $\text{Ext}^1(\chi_2^{-1}, \omega \chi_2)$ in the diagram. By a diagram chase, there is a class $W \in \text{Ext}^1(\chi_1^{-1}, \epsilon \omega \chi_2)$ mapping to $\eta_2$. This $W$ is a subquotient of $\eta_2$, 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 $\mathbb{F}_p[e_1]$-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 2.2.17 (the formal smoothness of the finite-flat deformation functor), there is a finite-flat representation $\eta_{2,\text{lift}} : G_p \to \text{GL}_2(\mathbb{F}_p[e_2])$ of the form

$$\eta_{2,\text{lift}} = \begin{pmatrix}
\omega (1 + \epsilon d^{(1)'} + e^2 d^{(2)'}_{\text{lift}}) & b^{(1)'} + e b^{(2)'} + e^2 b^{(3)'}_{\text{lift}} \\
0 & 1 + \epsilon d^{(1)'} + e^2 d^{(2)'}_{\text{lift}}
\end{pmatrix}$$

$$= \begin{pmatrix}
\omega \chi_{2,1,\text{lift}} & b^{(1)'} + e b^{(2)'} + e^2 b^{(3)'}_{\text{lift}} \\
0 & \chi_{2,2,\text{lift}}
\end{pmatrix}.$$ 

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

$$\epsilon \cdot \eta_{2,\text{lift}} = \begin{pmatrix}
\omega \chi_{2,1,\text{lift}} & e b^{(1)'} + e^2 b^{(2)'} \\
0 & \chi_{2,2,\text{lift}}
\end{pmatrix} : G_p \to \text{GL}_2(\mathbb{F}_p[e_2]),$$
which represents the class in $\text{Ext}^1_{\mathbb{F}_p[G]\text{-}[G]}(\chi^{-1}_{2,1\text{lift}}, \omega\chi_{2,1\text{lift}})$ that is the $\epsilon$-multiple of the class of $b^{(2)'} + \epsilon b^{(3)'} + \epsilon^2 b^{(3)'}$. By [WWE20, Rem. C.3.2], since $\eta_{2,\text{lift}}$ is finite-flat, $\epsilon \cdot \eta_{2,\text{lift}}$ is too.

Finally, since $\chi_2$, $\chi_{2,1\text{lift}}$, and $\chi_{2,2\text{lift}}$ are all unramified characters, it follows that

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

are unramified cocycles. Then $\eta_2$ is obtained from the finite-flat representation $\epsilon \cdot \eta_{2,\text{lift}}$ by adding the cocycle $\left( \begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix} \right) \in Z^1(G, \text{End}_{\mathbb{F}_p}(\omega \oplus 1))$, which is in the finite-flat subspace. By Proposition 2.2.17, this implies that $\eta_2$ is also finite-flat. □

**Lemma 7.2.12.** Assume $a^{(1)}|_{\epsilon_1} = 0$. There exists $\rho_2 \in \Pi^\text{det}_2$ such that

- $\rho_2|_p$ is upper-triangular (equivalently, $c^{(2)'}|_p = 0$), and
- the associated homomorphism $\eta_1$ as in Definition 7.2.8 is finite-flat.

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

Let $\eta = (\omega b^{(1)'} = (\eta_1 \mod \epsilon)$; it is finite-flat at $p$ by Lemma 2.2.13. The lift $\eta_1$ of $\eta$ over $\mathbb{F}_p[\epsilon_1] \to \mathbb{F}_p$ can and will be considered to be an element of $Z^1(\mathbb{Z}[1/Np], \text{Ad}^0(\eta))$ by Lemma 2.2.16. We want to examine its coordinates so we set up the following notions.

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

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

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

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

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

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

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

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

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

$$\begin{array}{ccccccc}
0 & \rightarrow & Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1)) & \xrightarrow{\iota} & Z^1(\mathbb{Z}[1/Np], \text{Ad}^0(\eta))^\text{p-UT} \\
\downarrow & & \downarrow & & \downarrow \\
0 & \rightarrow & Z^1(\mathbb{Q}_p, \mathbb{F}_p(1)) & \xrightarrow{\iota_p} & Z^1(\mathbb{Q}_p, U) & \xrightarrow{\kappa_p} & Z^1(\mathbb{Q}_p, \mathbb{F}_p) \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
0 & \rightarrow & Z^1(\mathbb{Q}_p, \mathbb{F}_p(1)) & \xrightarrow{\iota_p^\text{flat}} & Z^1(\mathbb{Q}_p, U)^\text{flat} & \xrightarrow{\kappa^\text{flat}} & Z^1(\mathbb{Q}_p, \mathbb{F}_p)^\text{flat} & \rightarrow & 0
\end{array}$$
where
\[ \iota_* : b \mapsto \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}, \quad \kappa_* : \begin{pmatrix} a_p^{(1)'} & b_p^{(2)'} \\ 0 & -a_p^{(1)'} \end{pmatrix} \mapsto a_p^{(1)'} \cdot \]

**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 \( \iota_p \) and \( \kappa_p \). The final claim of the lemma follows from Proposition 2.2.17 and the exactness of the rows of the diagram. \( \square \)

Since \( \eta_1 | _p \) is upper-triangular, \( \eta_1 \in Z^1(\mathbb{Z}[1/Np], \text{Ad}^0(\eta))_{\text{flat}} \). Moreover \( \kappa_p(\eta_1 | _p) = a^{(1)'} | _p \) is in \( Z^1(\mathbb{Q}_p, \mathbb{F}_p)_{\text{flat}} \). By Lemma 2.2.14, the image of \( \eta_1 \) is finite-flat. Since \( \eta_1 \) is given by \( \eta_1 = \eta_1 \), the snake lemma implies that the class of \( \eta_1 | _p \) is in the image of
\[ \frac{Z^1(\mathbb{Q}_p, \mathbb{F}_p(1))_{\text{flat}}}{Z^1(\mathbb{Q}_p, \mathbb{F}_p(1))_{\text{flat}}} \to Z^1(\mathbb{Q}_p, \mathbb{F}_p(1))_{\text{flat}} \].
By Lemma 2.2.14, the image of \( Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1)) \) generates \( \frac{Z^1(\mathbb{Q}_p, \mathbb{F}_p(1))_{\text{flat}}}{Z^1(\mathbb{Q}_p, \mathbb{F}_p(1))_{\text{flat}}} \). 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 \( Z^1(\mathbb{Q}_p, \mathbb{F}_p(1))_{\text{flat}} \). The commutativity of the diagram implies that \( \iota_p(b | _p) = \eta_1 | _p \).

Let \( b \in Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1)) \) be such that \( \iota_p(b | _p) + \eta_1 | _p \) is in \( Z^1(\mathbb{Q}_p, \mathbb{F}_p(1))_{\text{flat}} \). Moreover, \( \kappa_p(\eta_1 | _p) = a^{(1)'} | _p \) is in \( Z^1(\mathbb{Q}_p, \mathbb{F}_p(1))_{\text{flat}} \). By construction, \( \eta_1 | _p = \eta_1 + \iota_p(b | _p) \), and \( \eta_1 | _p = \eta_1 + \iota_p(b | _p) \) is finite-flat. \( \square \)

**Lemma 7.2.14.** Assume \( a^{(1)'} | _i = 0 \). Then \( \Pi_2^{\text{det.-p}} \) is non-empty.

**Proof.** Let \( \rho_2 \in \Pi_2^{\text{det.-p}} \) be as in Lemma 7.2.12. We claim that there is a cocycle \( a \in Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p) \) 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 \( \eta_1 \), 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 \( a \in Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p) \) such that \( (a^{(2)'} + a) | _p \) is unramified. The fact that \( \chi_2 \) is a character implies
\[ -da^{(2)'} | _p = a^{(1)'} - a^{(1)'} \cdot \]
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
\[ Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p) \to \frac{Z^1(\mathbb{Q}_p, \mathbb{F}_p)}{Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p)} \]
is surjective, there is $a \in Z^1(Z[1/Np], \mathbb{F}_p)$ 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. \hfill \square

Let 

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

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

**Remark 7.2.16.** In fact, the set of differences of the Proposition is equal to $(Z_b^1)^{\mathrm{flat}}$, 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 $\eta|_p$ and $\eta_{\text{alt}}|_p$ are finite-flat.

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

When $x \in \mathbb{F}_p(1)$ is a basis, then $\{dx, b_p, b^{(1)}, b^{(1)}_0\}$ is a basis for $Z^1(Z[1/Np], \mathbb{F}_p(1))$. By Lemma 2.2.14, $\{dx, b^{(1)}, b^{(1)}_0\}$ is a basis for the subspace $Z^1(Z[1/Np], \mathbb{F}_p(1))^{\mathrm{flat}}$. Since $b^{(1)}|_{\ell_i} = 0$ and $dx|_{\ell_i} = 0$, both $b^{(1)}$ and $dx$ are in $(Z_b^1)^{\mathrm{flat}}$. But, by Lemma 3.2.1 and Proposition 3.2.9, $b^{(1)}_0$ is not in $Z_b^1$, so $\{dx, b^{(1)}\}$ is a basis for $(Z_b^1)^{\mathrm{flat}}$. \hfill \square

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 $\rho_2$

Finally, consider the subset $\Pi_2^{\text{US}_N}$ of $\Pi_2^{\det,p}$ consisting of those $\rho_2$ which satisfying the US$_N$ condition. This subset is cut out by local conditions as

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

Indeed, the US$_N$ condition is simply the combination of the finite-flat condition at $p$ along with the two US$_{\ell_i}$ conditions at $\ell_i$, 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 $\Pi_2^{\text{US}_N} = \Pi_2^{\det,p}$, and, in particular, $\Pi_2^{\text{US}_N}$ 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$_{\ell_0}$. Let $\sigma, \tau \in G_{\ell_0}$. It suffices to show that

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

where $\omega$ is a character of $G_{\ell_0}$.

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

Using the equations that
\[
a^{(1)}|_{\ell_0} = \alpha \sim c^{(1)}|_{\ell_0},
\]
all instances of $a^{(1)}$, $d^{(1)}$, and $b^{(2)}$ can be replaced by appropriate multiples of $c^{(1)}$, and the formula simplifies to
\[
(r_2(\sigma) - \omega(\sigma))(r_2(\tau) - 1) = \begin{pmatrix}
  (\alpha^2 + \beta)c^{(1)}(\sigma)c^{(1)}(\tau)\epsilon^2 & 0 \\
  0 & (\alpha^2 + \beta)c^{(1)}(\sigma)c^{(1)}(\tau)\epsilon^2
\end{pmatrix}
\]
which vanishes by the assumption $\alpha^2 + \beta = 0$. This implies that $r_2|_{\ell_0}$ is US$\ell_0$.

It remains to show that $r_2|_{\ell_1}$ is US$\ell_1$. To do so, it will be convenient to change $c^{(2)}$ by adding an element of $B^1(\mathbb{Z}[1/Np], F_p(-1))$ to it. This amounts to conjugating $r_2$ by an element of $E_2^\times$, which does not affect whether the US$\ell_1$-condition holds.

Note that $\omega|_{\ell_1} = 1$ 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 $H^1(\mathcal{Q}_{\ell_1}, F_p(-1))$ vanishes, $c^{(2)}|_{\ell_1}$ is a coboundary. Therefore, by adding an element of $B^1(\mathbb{Z}[1/Np], F_p(-1))$ to $c^{(2)}$ if necessary, we may and do assume $c^{(2)}|_{\ell_1} = 0$.

With this assumption, $r_2|_{\ell_1}$ can be written in coordinates as
\[
r_2|_{\ell_1} = \begin{pmatrix}
  \omega\chi & b^{(1)}|_{\ell_1} + b^{(2)}|_{\ell_1} \\
  0 & \chi^{-1}
\end{pmatrix}
\]
where $\chi = 1 + a^{(2)}|_{\ell_1}\epsilon^2 : G_{\ell_1} \to \mathbb{F}_p[\epsilon_2]^\times$ is a homomorphism. Since $\chi$ has order dividing $p$ and the pro-$p$-abelian quotient of $G_{\ell_1}$ is generated by Frobenius, $\chi$ is unramified.

Let $\sigma \in G_{\ell_1}$, $\tau \in I_{\ell_1}$. Then $\chi(\tau) = 1$ and $\omega(\tau) = 1$, so
\[
(r_2(\sigma) - \omega(\sigma))(r_2(\tau) - 1) = \begin{pmatrix}
  \omega(\sigma)(\chi(\sigma) - 1) & b^{(1)}(\sigma) + b^{(2)}(\sigma)\epsilon \\
  0 & \omega(\sigma)\chi^{-1}(\sigma) - \omega(\sigma)
\end{pmatrix} \begin{pmatrix}
  0 & b^{(1)}(\tau) + b^{(2)}(\tau)\epsilon \\
  0 & 0
\end{pmatrix}
\]
This equals zero because $\omega(\sigma)(\chi(\sigma) - 1) \in \mathbb{F}_p[\epsilon_2]$, which annihilates the $B$-coordinate $\mathbb{F}_p[\epsilon_1]$. On the other hand
\[
(r_2(\tau) - \omega(\tau))(r_2(\sigma) - 1) = \begin{pmatrix}
  0 & b^{(1)}(\tau) + b^{(2)}(\tau)\epsilon \\
  0 & 0
\end{pmatrix} \begin{pmatrix}
  \omega(\sigma)\chi(\sigma) - 1 & b^{(1)}(\sigma) + b^{(2)}(\sigma)\epsilon \\
  0 & \omega(\sigma)\chi^{-1}(\sigma) - 1
\end{pmatrix}.
\]
This equals zero similarly, because $\chi^{-1}(\sigma) - 1 \in \mathbb{F}_p[\epsilon_2]$. Therefore, for all $\sigma, \tau \in G_{\ell_1} \times I_{\ell_1} \cup I_{\ell_1} \times G_{\ell_1}$,
\[
(r_2(\sigma) - \omega(\sigma))(r_2(\tau) - 1) = 0
\]
and so $r_2|_{\ell_1}$ is US$\ell_1$. \hfill $\square$

**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, $\Pi^{USN}_2$ is non-empty. Let $\rho_2 \in \Pi^{USN}_2$, let $D_2 = \psi(\rho_2) : GQ_{N}\rightarrow F_p[\epsilon_2]$ be the associated pseudorepresentation, and let $\phi_2 : R \rightarrow F_p[\epsilon_2]$ be the local homomorphism induced by $D_2$ using the universal property of $R$. By construction, the composition of $\phi_2$ with the quotient $F_p[\epsilon_2] \rightarrow F_p[\epsilon_1]$ is the map $\phi_1$ of Lemma 4.3.2. Since $\phi_1$ is surjective, this implies that $\phi_2$ is surjective.

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

$$\dim F_{\phi_2} S = 3 + \dim F_{\phi_2}(m_S^2) > 3.$$ 

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

**Theorem 7.3.3.** The $F_p$-dimension of $R/pR$ is greater than 3 if and only if

1. $\alpha(1)|_{\ell_0} = 0$ in $H^1(Q_{\ell_0}, F_p)$ and
2. $\alpha^2 + \beta = 0$ in $F_p(2)|_{\ell_0}$.

Moreover, if $\dim F_{\phi_2} R/pR = 3$, the surjection $R \rightarrow T$ of Proposition 2.2.20 is an isomorphism of reduced finite flat $\mathbb{Z}_p$-algebras of rank 3.

**Proof.** We prove the final statement first. Suppose $\dim F_{\phi_2} R/pR = 3$. 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 $\mathbb{Z}_p^3 \rightarrow R$. On the other hand, $T$ is a free $\mathbb{Z}_p$-module, and Ribet’s Theorem 1.2.1 implies that $\text{rk}_{\mathbb{Z}_p} T \geq 3$. The surjectivity of the composition

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

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

Now we prove the first statement. One implication is immediate from Corollary 7.3.2. Conversely, assume $\dim F_{\phi_2} R/pR > 3$. Since $\dim F_{\phi_2} R/(p, m^2) = 3$ by Proposition 5.1.8, this implies $\dim F_{\phi_2} S > 3$ where $S = R/(p, m^2)$. By Corollary 5.3.3, this implies $\dim F_{\phi_2} S = 4$. By Proposition 6.2.9, this implies (1).

It remains to show that (2) holds when $\dim F_{\phi_2} S = 4$. Let $\rho_2 \in \Pi^{USN}_2$ be the element constructed in Corollary 6.4.1. By the construction and by Proposition 7.2.1, the element $\beta' \in F_p(2)$ defined in Lemma 6.3.1 is equal to $\beta$. 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 1.6.1. 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 1.6.1.

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 $F_p(2)$, not of $\mu_p^{\otimes 2}$. Note the difference: $\mu_p \subset \overline{\mathbb{Q}}$ is the group of $p$th roots of unity, and a choice of primitive $p$th root of unity $\zeta \in \overline{\mathbb{Q}}$ defines an isomorphism

\begin{equation}
\phi_\zeta : F_p(2) \rightarrow \mu_p^{\otimes 2}, \quad 1 \mapsto \zeta \otimes \zeta
\end{equation}
of $\mathbb{F}_p[G]$-modules. Since the pinning data includes a choice primitive $p$th 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 1.2.2.

1. The condition $a^{(1)}|_{t_1} = 0$ does not depend on the pinning data.
2. If $a^{(1)}|_{t_1} = 0$, 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 $p$th 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 $\alpha$ and $\beta$ and defined in terms of these cocycles, their values could depend on pinning data. However, in a sense, we can think of $\alpha$ and $\beta$ 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 $\alpha$ and $\beta$ are unchanged. The only change of the pinning data that affects $\alpha^2 + \beta$ is changing the primitive $p$th root of unity $\zeta$, and we show that change behaves as expected for an element of $\mu_p^{\otimes 2}$: changing $\zeta$ to $\zeta^\ell$ multiplies $\alpha^2 + \beta$ by $\alpha^{-2}$.

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 $\rho_1$ and $\rho_2$. By Lemma 7.1.1, the condition $a^{(1)}|_{t_1} = 0$ can be interpreted in terms of the existence of a deformation $\rho_2$ of $\rho_1$, and this is unaffected by conjugation. In general, conjugation changes the value of $\alpha$ and $\beta$, 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 $\alpha$ and $\beta$ change under conjugation. In each of the remaining parts, we focus on a single change to the pinning data, and compute its effect. We will use the following notation scheme:

- We maintain the same notation $\alpha$, $\beta$, $\rho_1$, $\rho_2$, $a^{(1)}$, $b^{(1)}$, . . . , as in the earlier parts of the paper, computed with respect the pinning data fixed in Definition 1.6.1. Here $\rho_2$ denotes an arbitrary element of $\Pi_2^{\text{det},p}$, assuming it exists.
- We use primed notation $\alpha'$, $\beta'$, $\rho'_1$, $\rho'_2$, $a'^{(1)}$, $b'^{(1)}$, . . . , 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 $\rho_1$ and $\rho_2$.

In this section, we compute the effect of conjugation on the representations $\rho_1$ and $\rho_2$ 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 $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$.

The usual formula for inverting a $2 \times 2$-matrix is valid in $E_2$:

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

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

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

Let $M_1 \in E_1^\infty$ 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 $\rho_1$ and $\rho_2$ (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

$$\rho_{2,M} = \begin{pmatrix} \omega(1 + a_1^{(1)} \sigma + a_2^{(2)} \sigma^2) & b_1^{(1)} + b_2^{(2)} \sigma \\ \omega(c_1^{(1)} + c_2^{(2)} \sigma) & 1 + d_1^{(1)} + d_2^{(2)} \sigma^2 \end{pmatrix}$$

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 $M \in E_2^\infty$ and $\rho_{1,M}, \rho_{2,M}$ be as above. Then

(8.2.2) $b_1^{(1)} = A_0^{-1} \left( b^{(1)} + B_0(\omega - 1) \right)$

(8.2.3) $c_1^{(1)} = A_0(c^{(1)} + A_0^{-1}C_0(\omega - 1))$

(8.2.4) $a_1^{(1)} = a^{(1)} + B_0C_0 + A_0^{-1}C_0(\omega - 1) - A_0^{-1}B_0C_0(\omega - 1)$

(8.2.5) $b_2^{(2)} = A_0^{-1} \left( b^{(2)} + (D_1 + A_0^{-1}A_1 + B_0C_0)b^{(1)} + (B_1 - A_0^{-1}A_1B_0 + B_2^2C_0)(\omega - 1) + B_0(\omega a^{(1)} - d^{(1)}) - B_0^2\omega c^{(1)} \right)$.

Using this lemma, we can see how changes to the pinning data that cause $\rho_1$ and $\rho_2$ to be replaced by conjugates affect the values of $a^{(1)}|_{\ell_1}$ and $\alpha^2 + \beta^2$.

**Lemma 8.2.6.** Consider a change to the pinning data that does not alter the decomposition group at $\ell_0$ or the primitive $p$th root of unity $\zeta$, and let $G'_{\ell_1}$ denote the decomposition group at $\ell_1$ that is part of this new data. Suppose that the representation $\rho$ computed with this respect to this new data is of the form $\rho_1 = \rho_{1,M}$ for some $M \in E_2^\infty$ 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 $\alpha^2 + \beta^2 = A_0^{-2}(\alpha^2 + \beta^2)$.

**Proof.** For part (1), note that, by Lemma 7.1.1, $a^{(1)}|_{\ell_1} = 0$ if and only if $\rho_1$ has a deformation $\rho_2$. If $a^{(1)}|_{\ell_1} = 0$, then $\rho_2$ exists, and $\rho_{2,M}$ gives a deformation of $\rho_1$, so $a^{(1)}|_{G'_{\ell_1}} = 0$. This argument is symmetric, so the other implication follows.

Now suppose $a^{(1)}|_{\ell_1} = 0$, so $\rho_2$ exists and we can define $\rho'_2 = \rho_{2,M}$, and $\beta$ and $\beta'$ are defined. Then $\alpha$ and $\beta$ are defined by the formulas

$$a^{(1)}|_{\ell_0} = \alpha \cup c^{(1)}|_{\ell_0}, \quad b^{(2)}|_{\ell_0} = \beta \cup c^{(1)}|_{\ell_0}$$
and similarly for \( \alpha' \) and \( \beta' \). Since both pinning data have the same primitive \( p \)th root of unity \( \zeta \), we can and do use \( \zeta \) to identify twists of \( \mathbb{F}_p \) with \( \mathbb{F}_p \). In this way, we can think of \( \alpha \) and \( \beta \) 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
\[
\begin{align*}
\alpha' |_{\ell_0} &= \alpha |_{\ell_0} - B_0 c^{(1)} |_{\ell_0} \\
\beta' |_{\ell_0} &= A_0 c^{(1)} |_{\ell_0} \\
b^{(2)} |_{\ell_0} &= A_0^{-1} (b^{(2)} |_{\ell_0} - 2B_0 \alpha |_{\ell_0} - B_0^2 (\gamma |_{\ell_0})).
\end{align*}
\]
Rearranging to write everything in terms of \( c^{(1)} |_{\ell_0} \) gives
\[
\begin{align*}
\alpha' |_{\ell_0} &= A_0^{-1} (\alpha - B_0) c^{(1)} |_{\ell_0} \\
b^{(2)} |_{\ell_0} &= A_0^{-2} (\beta + 2B_0 \alpha - B_0^2) c^{(1)} |_{\ell_0}.
\end{align*}
\]
In other words,
\[
\alpha' = A_0^{-1} (\alpha - B_0), \quad \beta' = A_0^{-2} (\beta + 2B_0 \alpha - B_0^2)
\]
so \( \alpha^2 + \beta^2 = A_0^{-2} (\alpha^2 + \beta) \), as desired. \( \square \)

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 \( \ell_0 \) and changes to \( \zeta \) by separate arguments.

8.3. Changes that affect \( \rho_1 \) 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 \( b^{(1)}, b^{(1)} \), \( c^{(1)} \), 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 \( \ell_1 \)). Let \( G'_{\ell_1} \subset G_{Q,N_p} \) be another choice of decomposition group at \( \ell_1 \), and let \( \rho'_1 \) 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 \( \ell_1 \), 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 $\rho'_1$ (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 $\ell_1$ (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 $\ell_1$). Let $G'_p \subset G_{Q,Np}$ 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 $\rho'_1$ 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 $a^2 + \beta$.

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 $\ell_1$, 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 $\ell_0$ only changes the cocycle $b^{(1)}$ and does not affect $b^{(1)}$ or $c^{(1)}$, and consequently does not change $a^{(1)}$, $\alpha$, or $\beta$.

**8.4. Change of decomposition group at $\ell_0$.** Changing the decomposition group at $\ell_0$ 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 $G'_{\ell_0} \subset G_{Q,Np}$ be another choice of decomposition group at $\ell_0$, and let $\rho'_1$ 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
\[
\begin{array}{c}
b^{(2)'} = A b^{(2)}.
\end{array}
\]
In particular, this change does not alter the value of \( \alpha \) or \( \beta \).

**Proof.** The cocycle \( b^{(1)} \) does not depend on the choice of decomposition group at \( \ell_0 \), so \( b^{(1)'} = b^{(1)} \). Let \( \sigma \in G_{\ell_0} \) be such that \( G'_{\ell_0} = \sigma^{-1} G_{\ell_0} \sigma \).

A computation with cocycles\(^2\) 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 \( \alpha_0 = \omega(\sigma) \) and \( \gamma_0 = \sigma^{-1} \gamma_0 \sigma \), 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 \( c^{(1)'} = A c^{(1)} \).

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
\[
\rho_2' = \begin{pmatrix} \omega(1 + A a^{(1)} \epsilon + A^2 a^{(2)} \epsilon^2) & b^{(1)} + A b^{(2)} \epsilon \\ \omega(A c^{(1)} + A c^{(2)} \epsilon) & 1 + A d^{(1)} \epsilon + A^2 d^{(2)} \epsilon^2 \end{pmatrix}
\]
is in \( \Pi_{2}^{\det,p} \). In order to prove the claim, we apply the implication (3) \( \Rightarrow \) (1) of Lemma 7.2.11. The \( \eta'_1 \) produced from \( \rho_2' \) via (7.2.9), considered as an element of \( Z^1(\mathbb{Z}[1/Np], A d^{(1,2)}(\eta')) \) via Lemma 2.2.16 where \( \eta' = \eta_1 \mod \epsilon \), has coordinates \( A \cdot (c^{(1)}, d^{(1)}) \). Since the subset of finite-flat at \( p \) lifts of \( \eta' \) is a subspace containing \( (c^{(1)}, d^{(1)}) \), it contains \( \eta_1' \) as well.

Finally, since \( a^{(1)}, c^{(1)}, \) and \( b^{(2)} \) are all scaled by the same factor, the values of \( \alpha \) and \( \beta \) are left unchanged. \( \square \)

### 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 \( A \in \mathbb{F}_p^* \) be such that \( \zeta = \zeta'^A \). Let \( \rho_1' \) be the representation obtained by this change to the pinning data. Then
\[
\begin{array}{c}
b^{(1)'} = A b^{(1)} \quad c^{(1)'} = A c^{(1)} \quad a^{(1)'} = A^2 a^{(1)}.
\end{array}
\]
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
\[
b^{(2)'} = A b^{(2)}.
\]
In particular, \( \alpha' = A \alpha \) and \( \beta' = A^2 \beta \), and
\[
\phi_\zeta(\alpha'^2 + \beta') = \phi_\zeta(\alpha^2 + \beta).
\]

\(^2\)Note that this is the the same as the conjugation formula (8.2.2), and can also be proven in the same way.
where $\phi_\zeta$ 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 $\sigma \in G_{\Q,N_P}$. Replacing $\zeta$ by $\zeta^A$, 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 $\gamma_0' \in I_{E_0}$ satisfies $b^{(1)'}_0(\gamma_0') = 1$. 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 $a^{(1)} = A^2a^{(1)}$ follows immediately from Lemma 4.2.1. Similarly, it is easy to see that $b^{(2)'} = A^2b^{(2)}$ satisfies differential equation (ii) in Proposition 7.3.1, and the fact that the resulting $\rho_0$ 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
\[
\phi_{\zeta'}(\alpha'^2 + \beta') = \phi_{\zeta'}(A^2(\alpha^2 + \beta)) = \phi_\zeta(\alpha^2 + \beta).
\]

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 pseudomodular forms 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.

[HWWE23] Catherine Hsu, Preston Wake, and Carl Wang-Erickson. Explicit non-Gorenstein $R = \mathbb{T}$ via rank bounds II: Computational aspects. Res. Number Theory, 9(1): Paper No. 16, 52 pp., 2023. Part of the proceedings of the Fifteenth Algorithmic Number Theory Symposium (ANTS-XV).

[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):485–505, 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.

[Oht14] Masami Ohta. Eisenstein ideals and the rational torsion subgroups of modular Jacobian varieties II. Tokyo J. Math., 37(2):273–318, 2014.

[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 Gal($\overline{\mathbb{Q}}/\mathbb{Q}$) 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 Gal($\overline{\mathbb{Q}}/\mathbb{Q}$). Duke Math. J., 54(1):179–230, 1987.

[Wak23] Preston Wake. The Eisenstein ideal for weight $k$ and a Bloch-Kato conjecture for tame families. J. Eur. Math. Soc. (JEMS), 25(7):2815–2861, 2023.

[WE18] Carl Wang-Erickson. Presentations of non-commutative deformation rings via $A_\infty$-algebras and applications to deformations of Galois representations and pseudorepresentations. arXiv:1809.02484v2 [math.NT], 2018.

[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):977–1049, 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