THE EISENSTEIN IDEAL WITH SQUAREFREE LEVEL

PRESTON WAKE AND CARL WANG-ERICKSON

Abstract. We use deformation theory of pseudorepresentations to study the analogue of Mazur's Eisenstein ideal with squarefree level. Given a prime number $p > 3$ and a squarefree number N satisfying certain conditions, we study the Eisenstein part of the p-adic Hecke algebra for $\Gamma_0(N)$, and show that it is a local complete intersection and isomorphic to a pseudodeformation ring. We also show that, in certain cases, the Eisenstein ideal is not principal and that the cuspidal quotient of the Hecke algebra is not Gorenstein. As a corollary, we prove that "multiplicity one" fails for the modular Jacobian $J_0(N)$ in these cases. In a particular case, this proves a conjecture of Ribet.

Contents

1. Introduction

In his landmark study [Maz77] of the Eisenstein ideal with prime level, Mazur named five "special settings" in which "it would be interesting to develop the theory of the Eisenstein ideal in a broader context" [pg. 39, *loc. cit.*], the first of which is the setting of squarefree level. In this paper, we develop such a theory in certain cases.

1.1. **Mazur's results and their squarefree analogues.** Let $p \geq 3$ and ℓ be primes, and let $\mathbb{T}_\ell$ be the p-adic Eisenstein completion of the Hecke algebra acting on modular forms of weight 2 and level ℓ, and let $\mathbb{T}_\ell \twoheadrightarrow \mathbb{T}_\ell^0$ be the cuspidal quotient. Let $I_\ell^0 \subset \mathbb{T}_\ell^0$ be the Eisenstein ideal, and let $\mathfrak{m}_\ell^0 = (p, I_\ell^0)$ be the maximal ideal. Mazur proved the following results [Maz77]:

(1) $\mathbb{T}_\ell^0/I_\ell^0 \cong \mathbb{Z}_p/(\frac{\ell-1}{12})\mathbb{Z}_p$,

Date: January 19, 2021.

(2) I_ℓ^0 is principal,
(3) $\mathbb{T}_\ell^0$ is Gorenstein,
(4) if $q \neq \ell$ is a prime such that $q \not\equiv 1 \pmod{p}$ and such that q is not a p-th power modulo ℓ, then $T_q - (q+1)$ generates I_ℓ^0.

Mazur calls a prime q as in (4) a *good prime for* (ℓ, p). We note that, of course, (4) implies (2) implies (3). We also note that (2) implies that $\mathbb{T}_\ell$ is Gorenstein also.

The analogue of (1) has been proven for squarefree levels by Ohta [Oht14]. However, as has been noted by many authors, notably Ribet and Yoo [Rib15, Yoo19b], the statements (2)-(4) are not true in the squarefree setting. Still, in this paper, we prove, in certain cases, analogues of (2)-(4). Namely, we count the minimal number of generators of the Eisenstein ideal, count the dimension of the Eisenstein kernel of the Jacobian, and give sufficient (and sometimes also necessary) conditions for a list of elements $T_q - (q+1)$ to generate the Eisenstein ideal. As a corollary, we produce new level-raising results for modular forms congruent to Eisenstein series.

1.2. **Motivation and applications.** As applications of his results on the structure of the prime level Hecke algebra $\mathbb{T}_\ell$, Mazur proves the following arithmetic results:

(i) $J_0(\ell)(\mathbb{Q})_{\mathrm{tors}}$ is a cyclic group of order n, where n is the numerator of $\frac{\ell-1}{12}$, generated by the class of the divisor $(0) - (\infty)$.
(ii) The dimension of $J_0(\ell)[\mathfrak{m}_\ell^0]$ over $\mathbb{F}_p$ is 2.

Part (i) was conjectured by Ogg. As Mazur points out [Maz77, Remark, pg. 143], if one ignores the 2-torsion, part (i) is much easier and does not require the results (1)-(4) on the Hecke algebra. Indeed, Ohta has proven the squarefree analog of (i) (ignoring 2-torsion) [Oht14]. When we pass to squarefree level, the dimension in (ii) is no longer 2 in general; Ribet and Yoo [Rib15, Yoo19b] have partial results and conjectures as to what the dimension is. We count this dimension exactly, using our results on the Hecke algebra.

Just as Mazur's results on $\mathbb{T}_\ell$ have had many arithmetic applications, we expect that our results about the structure of $\mathbb{T}_N$ for squarefree level N will find more applications. We mention a few directions that are of particular interest to us:

- Connecting the rank of $\mathbb{T}_N$ with Massey products, class groups, and Mazur-Tate L-functions, in analogy to our previous work [WWE20] and the works of Merel [Mer96] and Lecouturier [Lec20] in the prime level case. This should have application to Venkatesh's conjectures for derived Hecke algebras in the case of weight 1 forms with squarefree level, just as Merel's work is applied in the prime level case by Harris and Venkatesh [HV19].
- Implications of the Gorenstein property of $\mathbb{T}_N$ for the arithmetic of cyclotomic fields and Iwasawa theory, as in the works of Ohta [Oht05] and Sharifi [Sha11].
- Applications to the Iwasawa theory of residually reducible modular forms, esspecially conjectures of Greenberg [Gre99, Conj. 1.11] and Vatsal [Vat05, Conj. 1.14] on μ-invariants.

It is also interesting to consider applications of our results in the setting of Hida theory (see §1.8 for a discussion of this). We hope to return to these applications in future work.

1.3. **Techniques of pseudomodularity.** Our main technical result is an $R = \mathbb{T}$ theorem, where R is a deformation ring for Galois pseudorepresentations and $\mathbb{T}$ is the Eisenstein part of the Hecke algebra. Although we consider this result

to be secondary to our results on the structure of the Hecke algebra, we believe that the proof techniques we develop may be of independent interest, and are a step toward integral refinement of the modularity results of Skinner–Wiles [SW99]. Therefore we describe them here. The strategy is similar to that of our previous works [WWE20, WWE19], where we gave new proofs and refinements of Mazur's results. However, there are several points of interest that are new in this setting.

(a) In the case of prime level ℓ, Calegari and Emerton [CE05] have already applied deformation theory to study Mazur's Eisenstein ideal. Their method is to rigidify the deformation theory of Galois representations using auxiliary data coming from the prime level ℓ. In the case of squarefree level, a similar strategy will not work: the deformation problem at prime level is already rigid, and cannot be further rigidified to account for the additional primes.
(b) In the case of squarefree level, there are multiple Eisenstein series, and one has to account for the possibility of congruences among them.
(c) At squarefree level, unlike prime level, the Tate module of the Jacobian may not be free over the Hecke algebra. Since this Tate module is the natural way to construct Galois representations, it is really necessary to work with pseudorepresentations.
(d) We prove $R = \mathbb{T}$ even in some cases where the Galois cohomology groups controlling the tangent space of R are all non-cyclic (see Remark 1.5.8). In this case, the universal pseudodeformation cannot arise from a representation.

To address issue (a), we have to develop a theory of Cayley–Hamilton representations and pseudorepresentations with squarefree level, which has the required flexibility; for this, we drew inspiration from our previous joint works [WWE18, WWE20, WWE19] and the work of Calegari–Specter [CS19]. The ideas are discussed later in this introduction in §1.9. To address issue (b), we make extensive use of an idea of Ohta [Oht14]: we use the Atkin–Lehner involutions at $\ell \mid N$ to define $\mathbb{T}$, rather than the usual Hecke operators U_ℓ.

1.4. **Setup.** We introduce notation in order to state our main results precisely. Throughout the paper we fix a prime p and let N denote a squarefree integer with distinct prime factors $\ell_0, \ell_1, \dots, \ell_r$. The case $p \mid N$ is not excluded.

1.4.1. *Assumption on p.* Throughout the paper we assume that $p > 3$. The assumption that $p \neq 2$ is used crucially throughout the paper in several ways. First, we use the fact that there is no primitive pth root of unity in $\mathbb{Q}$, so the mod-p cyclotomic character is non-trivial. Second, we use the fact that a local ring with residue characteristic p cannot have a non-trivial involution, so p-adic modules with a Hecke action admit a direct sum decomposition according to the Aktin–Lehner eigenvalues. Finally – and this is the only place where we also need $p \neq 3$ – we use the fact that $\zeta(-1) = \frac{-1}{12}$ is a p-adic unit. This is reflected in the Galois cohomology computation that we quote from [WWE20] as the fact that $K_i(\mathbb{Z}) \otimes \mathbb{Z}_p = 0$ for $i = 2, 3$. It is also used to say that a non-zero constant cannot be a mod-p modular form of weight 2. Because these do not seem to be crucial points, it is plausible that our techniques could be adapted to include the case $p = 3$. However, we do not pursue this here.

1.4.2. *Eisenstein series and Hecke algebras.* The Eisenstein series of weight two and level $\Gamma_0(N)$ have a basis $\{E_{2,N}^{\epsilon}\}$, labeled by elements $\epsilon = (\epsilon_0, \dots, \epsilon_r)$ in the

set $\mathcal{E} = \{\pm 1\}^{r+1} \setminus \{(1,1,\dots,1)\}$. The $E^\epsilon_{2,N}$ are characterized in terms of Hecke eigenvalues by the properties that

(1) $T_n E^\epsilon_{2,N} = \left(\sum_{0<t|n} t\right) E^\epsilon_{2,N}$ for all n with $\gcd(n,N)=1$, and
(2) $w_{\ell_i} E^\epsilon_{2,N} = \epsilon_i E^\epsilon_{2,N}$ for the Atkin–Lehner involutions $w_{\ell_0},\dots,w_{\ell_r}$,

together with the normalization $a_1(E^\epsilon_{2,N}) = 1$. The constant coefficients satisfy

$$a_0(E^\epsilon_{2,N}) = -\frac{1}{24}\prod_{i=0}^{r}(\epsilon_i \ell_i + 1). \tag{1.4.1}$$

(See §2.1.3 for more about these Eisenstein series.) Based on the philosophy that congruences between Eisenstein series and cusp forms should happen when the constant term is divisible by p, we expect the most interesting congruences to occur when $\ell_i \equiv -\epsilon_i \pmod p$ for many i. (Note that we do not have to consider constant terms at other cusps: if a modular form f of level $\Gamma_0(N)$ is an eigenform for all the Atkin–Lehner involutions, and $a_0(f) = 0$, then f is a cusp form.)

Consider the Hecke algebra of weight 2 and level $\Gamma_0(N)$ generated by all T_n with $\gcd(n,N) = 1$ and by all Atkin–Lehner involutions $w_{\ell_0},\dots,w_{\ell_r}$. Let $\mathbb{T}^\epsilon_N$ denote the completion of this algebra at the maximal ideal generated by p together with the annihilator of $E^\epsilon_{2,N}$.

Let I^ϵ denote the annihilator of $E^\epsilon_{2,N}$ in $\mathbb{T}^\epsilon_N$, so $\mathbb{T}^\epsilon_N/I^\epsilon = \mathbb{Z}_p$, and let $\mathfrak{m}^\epsilon = (I^\epsilon, p)$ be the maximal ideal of $\mathbb{T}^\epsilon_N$. For a Hecke module M, let $M^\epsilon_{\mathrm{Eis}}$ denote the tensor product of M with $\mathbb{T}^\epsilon_N$ over the Hecke algebra. In particular, let $M_2(N)^\epsilon_{\mathrm{Eis}}$ (resp. $S_2(N)^\epsilon_{\mathrm{Eis}}$) denote the resulting module of modular forms (resp. cuspidal forms). Let $\mathbb{T}^{\epsilon,0}_N$ denote the cuspidal quotient of $\mathbb{T}^\epsilon_N$, and let $I^{\epsilon,0}$ be the image of I^ϵ in $\mathbb{T}^{\epsilon,0}_N$.

1.4.3. *Another Hecke algebra.* In contrast with our approach, one often studies a different Hecke algebra $\mathbb{T}^\epsilon_{N,U}$, containing the operators U_ℓ instead of w_ℓ, and with Eisenstein ideal I^ϵ_U generated by $T_q - (q+1)$ for $q \nmid N$ and $U_{\ell_i} - \ell_i^{\frac{\epsilon_i+1}{2}}$ for $i = 0,\dots,r$. We prove that $\mathbb{T}^\epsilon_{N,U} = \mathbb{T}^\epsilon_N$ in some of the cases that we consider — see Appendix A. Our main results together with Appendix A can be used to prove results about $\mathbb{T}^\epsilon_{N,U}$ that are closely related to the results of authors including Ribet [Rib10, Rib15], Yoo ([Yoo19b, Yoo19a, Yoo17] and others) and Hsu [Hsu19].

We take the point of view that the reason to consider Hecke operators at primes dividing N is to distinguish various oldforms modulo p. When $\mathbb{T}^\epsilon_N \neq \mathbb{T}^\epsilon_{U,N}$, it is because there are multiple oldforms that have congruent U_ℓ-eigenvalues for some $\ell \mid N$. Because this multiplicity does not occur among w_ℓ-eigenvalues, such multiplicity causes $\mathbb{T}^\epsilon_{U,N}$ to have larger rank than $\mathbb{T}^\epsilon_N$. Therefore, we think of $\mathbb{T}^\epsilon_N$ as a superior to $\mathbb{T}^\epsilon_{U,N}$ as a superior desingularization of the unramified Hecke algebra (that is, the Hecke algebra generated by T_n for $(N,n) = 1$). We mostly consider $\mathbb{T}^\epsilon_N$, but see Appendix A for a comparison of $\mathbb{T}^\epsilon_N$ and $\mathbb{T}^\epsilon_{U,N}$.

1.4.4. *The number fields K_i.* Let ℓ be a prime such that $\ell \equiv \pm 1 \pmod p$. Then there is a unique degree p Galois extension $K_\ell/\mathbb{Q}(\zeta_p)$ such that

(1) $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ acts on $\mathrm{Gal}(K_\ell/\mathbb{Q}(\zeta_p))$ via the character ω^{-1},
(2) the prime $(1-\zeta_p)$ of $\mathbb{Q}(\zeta_p)$ splits completely in K_ℓ, and
(3) only the primes above ℓ ramify in $K_\ell/\mathbb{Q}(\zeta_p)$.

For each i such that $\ell_i \equiv \pm 1 \pmod{p}$, let $K_i = K_{\ell_i}$ (see also Definition 3.10.4).

1.5. **Structure of the Hecke algebra.** Our main results concern the structure of the Hecke algebra $\mathbb{T}_N^\epsilon$.

Theorem 1.5.1. *Assume that* $\epsilon = (-1, 1, \dots, 1)$. *Let*

$$\mathcal{S} = \{i \in \{1, \dots, r\} \mid \ell_i \equiv -1 \pmod{p}\}$$

and let $s = \#\mathcal{S}$. *Then*

(1) $\mathbb{T}_N^\epsilon$ *is a complete intersection ring.*
(2) $\mathbb{T}_N^{0,\epsilon}$ *is Gorenstein if and only if* I^ϵ *is principal.*
(3) There is a short exact sequence

$$0 \to \bigoplus_{i=1}^{r} \mathbb{Z}_p/(\ell_i + 1)\mathbb{Z}_p \to I^\epsilon/I^{\epsilon 2} \to \mathbb{Z}_p/(\ell_0 - 1)\mathbb{Z}_p \to 0. \tag{1.5.2}$$

(4) The minimal number of generators of I^ϵ *is* $s + \delta$ *where*

$$\delta = \begin{cases} 1 & \text{if } \ell_0 \text{ splits completely in } K_i \text{ for all } i \in \mathcal{S}, \text{ or} \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Parts (1) and (3) are proved in §5 (see especially Theorem 5.2.6). It is known to experts that Part (2) follows from (1) (see Lemma 2.4.2). Part (4) is Theorem 7.1.1. □

Remark 1.5.3. In fact, we show that, unless $s = r$, there are no newforms in $M_2(N)^\epsilon_{\mathrm{Eis}}$, so we can easily reduce to the case $s = r$ (i.e. the case that $\ell_i \equiv -1 \pmod{p}$ for all $i > 0$). When $s = r$, one could use this theorem to prove that there are newforms in $M_2(N)^\epsilon_{\mathrm{Eis}}$, but this is known (see [Rib15], [Yoo19a, Thm. 1.3(3)]).

Remark 1.5.4. The criterion of Part (4) determines whether or not the extension class defined by the sequence (1.5.2) is p-cotorsion. In fact, one can describe this extension class exactly in terms of algebraic number theory, but we content ourselves with the simpler statement (4).

Theorem 1.5.5. *Assume* $r = 1$ *and* $\epsilon = (-1, -1)$ *and that* $\ell_0 \equiv 1 \pmod{p}$ *but* $\ell_1 \not\equiv 1 \pmod{p}$. *If* ℓ_1 *is not a* p*-th power modulo* ℓ_0, *then there are no newforms in* $M_2(N)^\epsilon_{\mathrm{Eis}}$. *In particular,* I^ϵ *is principal, and generated by* $T_q - (q + 1)$ *where* q *is a good prime (of Mazur) for* (ℓ_0, p).

Proof. This is Theorem 6.3.1. □

Remark 1.5.6. In the case $\ell_1 \neq p$, this is a theorem of Ribet [Rib10] and Yoo [Yoo19a, Thm. 2.3]. Yoo has informed us that the method should work for the case $\ell_1 = p$ as well. In any case, our method is completely different.

Theorem 1.5.7. *Assume* $r = 1$ *and* $\epsilon = (-1, -1)$ *and that* $\ell_0 \equiv \ell_1 \equiv 1 \pmod{p}$. *Assume further that*

$$\ell_i \text{ is not a } p\text{-th power modulo } \ell_j \text{ for } (i, j) \in \{(0, 1), (1, 0)\}.$$

Then

(1) there are newforms in $M_2(N)^\epsilon_{\mathrm{Eis}}$.
(2) $\mathbb{T}_N^\epsilon$ *is a complete intersection ring.*
(3) $\mathbb{T}_N^{\epsilon,0}$ *is not a Gorenstein ring.*
(4) $I^{\epsilon,0}/I^{\epsilon,0\,2} \cong \mathbb{Z}_p/(\ell_0 - 1)\mathbb{Z}_p \oplus \mathbb{Z}_p/(\ell_1 - 1)\mathbb{Z}_p$.

Proof. Parts (2) and (4) are proven in Theorem 6.4.1. Part (1), the precise meaning of which is given in Definition 6.4.3, follows from Part (2) by Theorem 6.4.4. Part (3) follows from (2) and (4) by Lemma 2.4.2. □

Remark 1.5.8. The proof of this theorem may be of particular interest for experts in the deformation theory of Galois representations. The proof is the first (as far as we are aware) example of an $R = \mathbb{T}$ theorem, where R is a universal pseudodeformation ring, and where we do not rely on certain Galois cohomology groups being cyclic. (This cyclicity ensures that the pseudorepresentations come from true representations.) In fact, with the assumptions of the theorem, the relevant cohomology groups are not cyclic. However, see [BK15, Thm. 8.2], where $R' = \mathbb{T}$ is proved, where R' is a certain quotient of a universal pseudodeformation ring.

Remark 1.5.9. Outside of the cases considered in these theorems, we cannot expect that $\mathbb{T}^{\epsilon}_N$ is a complete intersection ring, as Remark 1.5.10 and the examples in §1.10 below illustrate. Our method, which applies Wiles's numerical criterion [Wil95], proves that $\mathbb{T}^{\epsilon}_N$ is a complete intersection ring as a byproduct. A new idea is needed to proceed beyond these cases. The authors along with C. Hsu are currently working out such an idea [HWWE21].

Remark 1.5.10. Consider the case $\epsilon = (-1, -1, \dots, -1)$ with $\ell_i \equiv 1 \pmod{p}$ for $i = 0, \dots, r$. There is a numerological reason why our arguments work for $r = 1$, but not for $r > 1$. To see that $\mathbb{T}^{\epsilon}_N$ satisfies the numerical criterion, its cotangent module $I^{\epsilon}/I^{\epsilon 2}$ must not be any bigger than its reducible quotient contributed by Lemma 4.2.3. In order for the irreducible submodule of $I^{\epsilon}/I^{\epsilon 2}$ to vanish, we have to show that there are $(r+1)^2$ relations which kill off all of the $(r+1)^2$ generators. We can always see that $(r+1)$ of them hold, and when certain additional conditions (like the assumptions in Theorem 1.5.7) on the ℓ_i hold, we show that another $(r+1)$ relations hold (see Lemma 6.2.1). This gives a total of $2(r+1)$, and only when $r = 1$ do we have $(r+1)^2 = 2(r+1)$.

1.6. **Applications to multiplicity one.** For an application of the main result, we let $J_0(N)$ be the Jacobian of the modular curve $X_0(N)$.

Corollary 1.6.1. *In the following cases, we can compute* $\dim_{\mathbb{F}_p} J_0(N)(\overline{\mathbb{Q}}_p)[\mathfrak{m}^{\epsilon}]$*:*

(1) With the assumptions of Theorem 1.5.1, we have

$$\dim_{\mathbb{F}_p} J_0(N)(\overline{\mathbb{Q}}_p)[\mathfrak{m}^{\epsilon}] = 1 + s + \delta,$$

where s and δ are as in Theorem 1.5.1.

(2) With the assumptions of Theorem 1.5.5, we have $\dim_{\mathbb{F}_p} J_0(N)(\overline{\mathbb{Q}}_p)[\mathfrak{m}^{\epsilon}] = 2$.

(3) With the assumptions of Theorem 1.5.7, we have $\dim_{\mathbb{F}_p} J_0(N)(\overline{\mathbb{Q}}_p)[\mathfrak{m}^{\epsilon}] = 3$.

Proof. This follows from the named theorems together with Lemma 2.4.3 (which is known to experts). □

One says that "multiplicity one holds" if $\dim_{\mathbb{F}_p} J_0(N)(\overline{\mathbb{Q}}_p)[\mathfrak{m}^{\epsilon}] = 2$. This corollary implies that multiplicity one holds in case (1) if and only if $s + \delta = 1$, always holds in case (2), and always fails in case (3).

1.6.1. *Ribet's Conjecture.* Previous works on multiplicity one have used a different Hecke algebra $\mathbb{T}^{\epsilon}_{N,U}$, defined in §1.4.3 (see, for example, [Yoo19b]). Let $\mathfrak{m}^{\epsilon}_U = (I^{\epsilon}_U, p) \subset \mathbb{T}^{\epsilon}_{N,U}$ be its maximal ideal. The previous corollary together with Proposition A.2.3 give the following.

Corollary 1.6.2 (Generalized Ribet's Conjecture)**.** *With the assumptions of Theorem 1.5.1, assume in addition that $\ell_i \not\equiv 1 \pmod{p}$ for $i > 0$. Then*

$$\dim_{\mathbb{F}_p} J_0(N)(\overline{\mathbb{Q}}_p)[\mathfrak{m}_U^\epsilon] = 1 + s + \delta,$$

where s and δ are as in Theorem 1.5.1.

The case $s = r = 1$ of Corollary 1.6.2 was conjectured by Ribet [Rib15] (see also [Yoo17, pg. 4]).

Remark 1.6.3. After we told Yoo about the results of this paper, he found an alternate proof of this corollary in the case $s = r = 1$. His proof involves a delicate study of the geometry of $J_0(N)$, and relies on the following particular results of this paper:

(i) I^ϵ is principal if and only if $\mathbb{T}_N^{0,\epsilon}$ is Gorenstein, from Theorem 1.5.1(2), and
(ii) $\mathbb{T}_{N,U}^{0,\epsilon} = \mathbb{T}_N^{0,\epsilon}$ under the assumption $s = r = 1$, from Proposition A.2.3, so that the conclusion of (i) can be applied to the ideal $I_U^\epsilon \subset \mathbb{T}_{N,U}^{0,\epsilon}$.

In particular, Yoo's proof does not make use of our formula for the number of generators for I^ϵ in Theorem 1.5.1(4), and we believe that his methods could be used to give a new proof of that result in this case.

In contrast, our proof is immediate from the ring-theoretic properties given in Theorem 1.5.1 and a standard argument (found in [Maz77], for example), and no additional geometric argument is needed. The fact that our proof is almost completely ring-theoretic demonstrates the power of the Gorenstein property and is a reason for our interest in using $\mathbb{T}_N^\epsilon$ rather than $\mathbb{T}_{N,U}^\epsilon$.

1.6.2. *Gorensteinness, and multiplicity one for the generalized Jacobian.* The following observations are not used (nor proven) in this paper (although they are familiar to experts), but we include them to illustrate the the arithmetic significance of the Gorenstein property for $\mathbb{T}_N^\epsilon$ proved in Theorems 1.5.1, 1.5.5 and 1.5.7. We learned this point of view from papers of Ohta, especially [Oht05].

As is well-known, and as we explain in §2.4, multiplicity one holds if and only if $\mathbb{T}_N^{0,\epsilon}$ is Gorenstein. The nomenclature "multiplicity one" comes from representation theory. It is related to the question of whether $H^1_{\text{ét}}(X_0(N)_{\overline{\mathbb{Q}}}, \mathbb{Z}_p(1))^\epsilon_{\text{Eis}}$ is a free $\mathbb{T}_N^{0,\epsilon}$-lattice in the free $\mathbb{T}_N^{0,\epsilon}[\frac{1}{p}]$-module $H^1_{\text{ét}}(X_0(N)_{\overline{\mathbb{Q}}}, \mathbb{Q}_p(1))^\epsilon_{\text{Eis}}$.

There is another natural lattice to consider, namely $H^1_{\text{ét}}(Y_0(N)_{\overline{\mathbb{Q}}}, \mathbb{Z}_p(1))_{\mathfrak{m}^\epsilon,\text{DM}}$, the image of $H^1_{\text{ét}}(Y_0(N)_{\overline{\mathbb{Q}}}, \mathbb{Z}_p(1))^\epsilon_{\text{Eis}}$ under the Drinfeld-Manin splitting

$$H^1_{\text{ét}}(Y_0(N)_{\overline{\mathbb{Q}}}, \mathbb{Q}_p(1))^\epsilon_{\text{Eis}} \longrightarrow H^1_{\text{ét}}(X_0(N)_{\overline{\mathbb{Q}}}, \mathbb{Q}_p(1))^\epsilon_{\text{Eis}}.$$

In a similar manner to the proof of Lemma 2.4.1, one can show that $\mathbb{T}_N^\epsilon$ is Gorenstein if and only if $H^1_{\text{ét}}(Y_0(N)_{\overline{\mathbb{Q}}}, \mathbb{Z}_p(1))_{\mathfrak{m}^\epsilon,\text{DM}}$ is a free $\mathbb{T}_N^{0,\epsilon}$-module, if and only if

$$\dim_{\mathbb{F}_p} GJ_0(N)(\overline{\mathbb{Q}}_p)[\mathfrak{m}^\epsilon] = 2,$$

where $GJ_0(N)$ is the generalized Jacobian of $J_0(N)$ relative to the cusps (see e.g. [Oht99, §3] for a discussion of generalized Jacobians). Hence our result that $\mathbb{T}_N^\epsilon$ is Gorenstein can be thought of as a multiplicity one result for $GJ_0(N)$.

Finally, we note that these ideas illustrate why the failure of multiplicity one in Corollary 1.6.1 is related to the failure of I^ϵ to be principal: if $\mathbb{T}_N^\epsilon$ is Gorenstein,

$$H^1_{\text{ét}}(X_0(N)_{\overline{\mathbb{Q}}}, \mathbb{Z}_p(1))^\epsilon_{\text{Eis}} \hookrightarrow H^1_{\text{ét}}(Y_0(N)_{\overline{\mathbb{Q}}}, \mathbb{Z}_p(1))_{\mathfrak{m}^\epsilon,\text{DM}}$$

has the form, as $\mathbb{T}_N^{0,\epsilon}$-modules, of

$$\mathbb{T}_N^{0,\epsilon} \oplus I^{0,\epsilon} \hookrightarrow \mathbb{T}_N^{0,\epsilon} \oplus \mathbb{T}_N^{0,\epsilon}.$$

Hence $H^1_{\text{ét}}(X_0(N)_{\overline{\mathbb{Q}}}, \mathbb{Z}_p(1))^{\epsilon}_{\text{Eis}}$ is free if and only if $I^{0,\epsilon}$ is principal.

1.7. **Good primes.** We also prove analogues of Mazur's good prime criterion (statement (5) of §1.1).

In the situation of Theorem 1.5.7, our good prime criterion is necessary and sufficient, exactly analogous to Mazur's. To state it, we let

$$\log_\ell : (\mathbb{Z}/\ell\mathbb{Z})^\times \twoheadrightarrow \mathbb{F}_p$$

denote an arbitrary surjective homomorphism, for any prime ℓ that is congruent to 1 modulo p (the statement below will not depend on the choice).

Theorem 1.7.1. *With the assumptions of Theorem 1.5.7, fix primes q_0, q_1 not dividing N (but possibly dividing p). Then the elements $T_{q_0} - (q_0+1)$ and $T_{q_1} - (q_1+1)$ together generate I^ϵ if and only if*

$$(q_0-1)(q_1-1)\det\begin{pmatrix} \log_{\ell_0}(q_0) & \log_{\ell_0}(q_1) \\ \log_{\ell_1}(q_0) & \log_{\ell_1}(q_1) \end{pmatrix} \in \mathbb{F}_p^\times.$$

Remark 1.7.2. For a single prime ℓ, Mazur's criterion for q to be a good prime can be written as $(q-1)\log_\ell(q) \in \mathbb{F}_p^\times$, so this is a natural generalization.

In the situation of Theorem 1.5.1, we only give a sufficient condition, and even this is cumbersome to state.

Definition 1.7.3. Assume that $\epsilon = (-1, 1, \dots, 1)$, and order the primes ℓ_i so that $\ell_i \equiv -1 \pmod{p}$ for $i = 1, \dots, s$ and $\ell_i \not\equiv -1 \pmod{p}$ for $s < i \le r$. We use the number fields K_i set up in §1.4.4.

Consider an ordered set of primes $\mathcal{Q}' = \{q_0, q_1, \dots, q_s\}$ disjoint from the primes dividing N and satisfying the following conditions:

(1) $q_0 \not\equiv 1 \pmod{p}$, and
(2) q_0 not a p-th power modulo ℓ_0;

and, for $i = 1, \dots, s$,

(3) $q_i \equiv 1 \pmod{p}$,
(4) ℓ_0 is not a p-th power modulo q_i,
(5) q_i does not split completely in K_i, and
(6) q_i does split completely in each K_j for $j = 1, \dots, s$ with $j \neq i$.

In the following cases, the described ordered subset $\mathcal{Q}$ of $\mathcal{Q}'$ is called a *good set of primes for* (N, p, ϵ):

- if $\delta = 1$, $\mathcal{Q} := \mathcal{Q}'$,
- if $\delta = 0$ and $\ell_0 \equiv 1 \pmod{p}$, then $\mathcal{Q} := \mathcal{Q}' \setminus \{q_j\}$ for an index $j > 0$ such that $b_0 \cup c_j \neq 0$,
- if $\ell_0 \not\equiv 1 \pmod{p}$, then $\mathcal{Q} := \mathcal{Q}' \setminus \{q_0\}$.

Remark 1.7.4. Note that, by Chebotarev density, there is an infinite set of primes q_0 satisfying (1)-(2), and, for each i, there is an infinite set of primes q_i satisfying (3)-(6). Note that when $p \nmid N$ and $\ell_0 \equiv 1 \pmod{p}$, it is possible that $p \in \mathcal{Q}$.

Theorem 1.7.5. *Let $\mathcal{Q}$ be a good set of primes for (N, p, ϵ). Then $\{T_q - (q+1) \mid q \in \mathcal{Q}\} \subset \mathbb{T}_N^\epsilon$ is a minimal set of generators for I^ϵ.*

Remark 1.7.6. We can also write down a necessary and sufficient condition, but cannot compute with it, so we doubt its practical use.

1.8. **Relation to Hida Hecke algebras.** The reader will note that we have allowed for the possibility that $p \mid N$. When $p \mid N$, in Appendix A, we also consider a related Hecke algebra $\mathbb{T}^{\epsilon}_{N,H}$ that contains U_p instead of w_p (but still has all other w_ℓ for $\ell \mid \frac{N}{p}$) and show that, in many cases we consider, $\mathbb{T}^{\epsilon}_{N,H} = \mathbb{T}^{\epsilon}_{N}$.

This is related to Hida theory assuming that (as is well-known for the Hecke algebra $\mathbb{T}^{\epsilon}_{N,U}$) there is a Hida-theoretic Hecke algebra $\mathbb{T}^{\epsilon}_{\Lambda}$ that is a free module of finite rank over $\Lambda \simeq \mathbb{Z}_p[\![T]\!]$ that satisfies a control theorem with respect to $\mathbb{T}^{\epsilon}_{N,H}$: there is an element $\omega_2 \in \Lambda$ such that $\mathbb{T}^{\epsilon}_{N,H} = \mathbb{T}^{\epsilon}_{\Lambda}/\omega_2\mathbb{T}^{\epsilon}_{\Lambda}$.

Then our results about $\mathbb{T}^{\epsilon}_{N}$ (including its Gorensteinness and the number of generators of its Eisenstein ideal) translate directly to $\mathbb{T}^{\epsilon}_{\Lambda}$. Subsequently, these results can be specialized into higher weights, as is usual in Hida theory.

1.9. **Method of pseudodeformation theory.** Like our previous work [WWE20], the method of proof of the theorems in §1.5 is to construct a pseudodeformation ring R and prove that $R = \mathbb{T}$ using the numerical criterion. The ring R is the deformation ring of the residual pseudorepresentation $\bar{D} = \psi(\omega \oplus 1)$ associated to $E^{\epsilon}_{2,N}$ that is universal subject to certain conditions (here ψ is the functor associating a pseudorepresentation to a representation, and ω is the mod p cyclotomic character). These conditions include the conditions considered in our previous works [WWE18, WWE20] (having cyclotomic determinant, being flat at p, being ordinary at p), but they also include new conditions at ℓ dividing N that are of a different flavor, as we now explain.

1.9.1. *The Steinberg at ℓ condition.* Fix $\ell = \ell_i \mid N$, assume $\ell \neq p$, and let $G_\ell \subset G_{\mathbb{Q}}$ be a decomposition group at ℓ. Let f be a normalized cuspidal eigenform of weight 2 and level $\Gamma_0(N)$. Let $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O}_f)$ be the associated Galois representation, where $\mathcal{O}_f$ is a finite extension of $\mathbb{Z}_p$.

If f is old at ℓ, then $\rho_f|_{G_\ell}$ is unramified. If f is new at ℓ, we have

$$\rho_f|_{G_\ell} \sim \begin{pmatrix} \lambda(a_\ell(f))\kappa_{\mathrm{cyc}} & * \\ 0 & \lambda(a_\ell(f)) \end{pmatrix} \tag{1.9.1}$$

where $\lambda(x)$ is the unramified character of G_ℓ sending a Frobenius element σ_ℓ to x, and $a_\ell(f)$ is the coefficient of q^ℓ in the q-expansion of f (see Lemma 2.3.1). Note that since $\det(\rho_f) = \kappa_{\mathrm{cyc}}$, we have $\lambda(a_\ell(f))^2 = 1$. In fact, $a_\ell(f)$ is the negative of the w_ℓ-eigenvalue of f. We call such representations (1.9.1) "$\pm$1-Steinberg at ℓ", where $\pm 1 = \mp a_\ell(f)$ is the w_ℓ-eigenvalue of f.

Now assume in addition that $f \in S_2(N)^{\epsilon}_{\mathrm{Eis}}$, so that the semi-simplification of the residual representation of ρ_f is $\omega \oplus 1$ and $w_\ell f = \epsilon f$, where $\epsilon = \epsilon_i$. We want to impose a condition on pseudorepresentations that encapsulates the condition that $\rho_f|_{G_\ell}$ is either unramified or ϵ-Steinberg. The main observation is the following, and is inspired by the work of Calegari–Specter [CS19].

Observation 1.9.2. Suppose that $\rho : G_\ell \to \mathrm{GL}_2(\mathcal{O})$ is either unramified or ϵ-Steinberg. Then

$$(\rho(\sigma) - \lambda(-\epsilon)\kappa_{\mathrm{cyc}}(\sigma))(\rho(\tau) - \lambda(-\epsilon)(\tau)) = 0 \tag{1.9.3}$$

for all $\sigma, \tau \in G_\ell$ with at least one of σ or τ in the inertia group I_ℓ.

This is clear if ρ is unramified: the factor involving the one of σ or τ that is in I_ℓ will be zero. If ρ is ϵ-Steinberg, then the given product (1.9.3) will have the form

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

and any such product is zero (note that the order is important!).

To impose the unramified-or-ϵ-Steinberg condition on the pseudodeformation ring R, we impose the condition (1.9.3) on the universal Cayley–Hamilton algebra, using the theory of [WWE19] (see §3).

1.9.2. *The ordinary at p condition.* When $p \mid N$ and $f \in S_2(N)^\epsilon_{\mathrm{Eis}}$ is a newform, then $\epsilon_p = -1$ and the representation $\rho_f|_{G_p}$ is ordinary. In this paper, we define "ordinary pseudorepresentation" exactly as we define the unramified-or-ϵ-Steinberg, following ideas of Calegari–Specter. In our previous paper [WWE18], we gave a different definition of ordinary, and we prove in this paper that the two definitions coincide (see Lemma 3.7.4). This gives an answer to a question of Calegari–Specter [CS19, pg. 2].

1.10. **Examples.** We conclude this introduction with examples that illustrate the theorems and show that the hypotheses are necessary. For examples where we show that $\mathbb{T}^\epsilon_N$ is not Gorenstein, it is helpful to note that $\mathbb{T}^\epsilon_N$ is Gorenstein if and only if $\mathrm{Soc}(\mathbb{T}^\epsilon_N/p\mathbb{T}^\epsilon_N)$ is 1-dimensional, where $\mathrm{Soc}(\mathbb{T}^\epsilon_N/p\mathbb{T}^\epsilon_N)$ is the annihilator of the maximal ideal (see §C.1).

All computations are using algorithms we have written for the Sage computer algebra software [S+18].

1.10.1. *Examples illustrating Theorem 1.5.1.*

Example 1.10.1. Let $p = 5$, $\ell_0 = 41$, $\ell_1 = 19$, so $N = 19 \cdot 41$, and let $\epsilon = (-1, 1)$. In this case, we compute that K_{19} is the field cut out by

$$\begin{aligned} x^{20} - x^{19} - 7x^{18} + 21x^{17} + 22x^{16} + 223x^{15} - 226x^{14} - 1587x^{13} + 4621x^{12} \\ + 5202x^{11} - 91x^{10} - 3142x^9 - 439x^8 - 2143x^7 - 2156x^6 - 58x^5 \\ + 1237x^4 + 414x^3 + 148x^2 + 56x + 16 \end{aligned}$$

and that 41 splits completely in K_{19}. The theorem says that I^ϵ has 2 generators. Moreover, Theorem 1.7.5 says, in this case, that I^ϵ is generated by $T_{q_0} - (q_0 + 1)$ and $T_{q_1} - (q_1 + 1)$ where q_0 is a good prime for $(41, 5)$ and where q_1 satisfies

(a) q_1 is a prime such that $q_1 \equiv 1 \pmod 5$,
(b) 41 is not a 5-th power modulo q_1, and
(c) q_1 does not split completely in K_{19}.

A quick search yields that $q_0 = 2$ and $q_1 = 11$ satisfy these criteria. And indeed, we compute that there is an isomorphism

$$\frac{\mathbb{F}_5[x, y]}{(y^2 - 2x^2, xy)} \xrightarrow{\sim} \mathbb{T}^\epsilon_N/5\mathbb{T}^\epsilon_N, \quad (x, y) \mapsto (T_2 - 3, T_{11} - 12).$$

Example 1.10.2. Let $p = 5$, $\ell_0 = 11$, $\ell_1 = 19$, $\ell_2 = 29$, so $N = 11 \cdot 19 \cdot 29$, and let $\epsilon = (-1, 1, 1)$. In this case, 11 does not split completely in either of the fields K_{19}, K_{29}, and the theorem says that I^ϵ has 2 generators. Moreover, Theorem 1.7.5 says, in this case, that I^ϵ is generated by $T_{q_0} - (q_0 + 1)$ and $T_{q_1} - (q_1 + 1)$ where q_0 is a good prime for $(11, 5)$ (for example $q_0 = 2$) and where the prime q_1 satisfies:

(a) $q_1 \equiv 1 \pmod 5$,
(b) 11 is not a 5-th power modulo q_1,
(c) q_1 does not split completely in K_{19}, and
(d) q_1 does split completely in K_{29}.

In this case, K_{19} is the field computed in the previous example and K_{29} is the field cut out by

$$\begin{aligned} x^{20} - x^{19} - 11x^{18} + 9x^{17} + 124x^{16} - 223x^{15} - 1244x^{14} + 2111x^{13} + 14291x^{12} \\ - 19804x^{11} + 7169x^{10} + 7938x^9 - 10937x^8 + 15603x^7 - 9472x^6 \\ - 2582x^5 + 8233x^4 - 3732x^3 + 1808x^2 - 832x + 256. \end{aligned}$$

A quick search finds that $q_1 = 181$ satisfies the conditions (a)-(d). And indeed, we compute that there is an isomorphism

$$\frac{\mathbb{F}_5[x,y]}{(x^3+2x^2, y^3, xy+y^2)} \xrightarrow{\sim} \mathbb{T}_N^\epsilon/5\mathbb{T}_N^\epsilon, \quad (x,y) \mapsto (T_2 - 3, T_{181} - 182).$$

Note that these conditions are far from necessary. For example $T_2 - 3$ and $T_7 - 8$ also generate the Eisenstein ideal.

1.10.2. *Examples related to Theorem 1.5.5.* We give examples illustrating that the assumption is necessary. In fact, it seems that the assumption is necessary even for the Gorensteinness of $\mathbb{T}_N^\epsilon$.

Example 1.10.3. Let $p = 5$, $\ell_0 = 11$, $\ell_1 = 23$, so $N = 11 \cdot 23$, and let $\epsilon = (-1,-1)$. Then $\ell_1 \equiv 1 \pmod{11}$ is a 5-th power so the theorem does not apply. We can compute that

$$\frac{\mathbb{F}_5[x,y]}{(x^2, xy, y^2)} \xrightarrow{\sim} \mathbb{T}_N^\epsilon/5\mathbb{T}_N^\epsilon, \quad (x,y) \mapsto (T_2 - 3, T_3 - 4)$$

has dimension 3. Since $\mathbb{T}_{11}^0 = \mathbb{Z}_5$, we see that the space of oldforms has dimension 2, so there must be a newform at level N. Moreover, $\mathrm{Soc}(\mathbb{T}_N^\epsilon/5\mathbb{T}_N^\epsilon) = x\mathbb{F}_5 \oplus y\mathbb{F}_5$, so $\mathbb{T}_N^\epsilon$ is not Gorenstein.

Example 1.10.4. Let $p = 5$, $\ell_0 = 31$, $\ell_1 = 5$, so $N = 5 \cdot 31$, and let $\epsilon = (-1,-1)$. Then note that $\ell_1 = 5 \equiv 7^5 \pmod{31}$, so the theorem does not apply. We can compute that

$$\frac{\mathbb{F}_5[x,y]}{(x^3, xy, y^2)} \xrightarrow{\sim} \mathbb{T}_N^\epsilon/5\mathbb{T}_N^\epsilon, \quad (x,y) \mapsto (T_2 - 3, 2T_2 + T_3)$$

has dimension 4. Since $\mathrm{rank}_{\mathbb{Z}_5}(\mathbb{T}_{31}^0) = 2$, we see that the space of oldforms has dimension 3, and there must be a newform at level N. Moreover, $\mathrm{Soc}(\mathbb{T}_N^\epsilon/5\mathbb{T}_N^\epsilon) = x^2\mathbb{F}_5 \oplus y\mathbb{F}_5$, so $\mathbb{T}_N^\epsilon$ is not Gorenstein.

In this last example, the reader may think that $\ell_0 = 31$ is special because the rank of $\mathbb{T}_{31}^0$ is 2. However, we can take $p = \ell_1 = 5$ and $\ell_0 = 191$ (note that $\mathbb{T}_{191}^0 = \mathbb{Z}_p$). Noting that $5 \equiv 18^5 \pmod{191}$, we again see that the theorem does not apply, and we can compute that $\mathbb{T}_N^\epsilon$ is also not Gorenstein in this case.

1.10.3. *Examples related to Theorem 1.5.7.* First, we give examples illustrating that the assumption is necessary. Again, it seems that the assumption is necessary even for the Gorenstein property of $\mathbb{T}_N^\epsilon$.

Example 1.10.5. Let $p = 5$, $\ell_0 = 11$, $\ell_1 = 61$, so $N = 11 \cdot 61$, and let $\epsilon = (-1, -1)$. Then note that $11 \equiv 8^5 \pmod{61}$ so the theorem does not apply (but note that 61 is not a 5-th power modulo 11). We can compute that

$$\frac{\mathbb{F}_5[x,y]}{(x^2, xy, y^3)} \xrightarrow{\sim} \mathbb{T}_N^\epsilon / 5\mathbb{T}_N^\epsilon, \quad (x,y) \mapsto (T_3 - T_2 - 1, T_2 - 3).$$

We see that $\mathrm{Soc}(\mathbb{T}_N^\epsilon / 5\mathbb{T}_N^\epsilon) = x\mathbb{F}_5 \oplus y^2\mathbb{F}_5$, so $\mathbb{T}_N^\epsilon$ is not Gorenstein.

Example 1.10.6. Let $p = 5$, $\ell_0 = 31$, $\ell_1 = 191$, so $N = 31 \cdot 191$, and let $\epsilon = (-1, -1)$. We have $191 \equiv 7^5 \pmod{31}$ and $31 \equiv 61^5 \pmod{191}$, so the assumption of the theorem fails most spectacularly. We can compute that

$$\frac{\mathbb{F}_5[x,y]}{((x,y)^4, 2x^3 + xy^2 + 3y^3, x^3 - x^2y + 2y^3)} \xrightarrow{\sim} \mathbb{T}_N^\epsilon / 5\mathbb{T}_N^\epsilon,$$
$$(x,y) \mapsto (T_2 - 3, T_7 - 8).$$

Letting $\bar{\mathfrak{m}}^\epsilon$ denote the maximal ideal of $\mathbb{T}_N^\epsilon / 5\mathbb{T}_N^\epsilon$, we see that $(\bar{\mathfrak{m}}^\epsilon)^4 = 0$ but that $(\bar{\mathfrak{m}}^\epsilon)^3$ is 2-dimensional, so $\dim_{\mathbb{F}_5} \mathrm{Soc}(\mathbb{T}_N^\epsilon / 5\mathbb{T}_N^\epsilon) > 1$ and $\mathbb{T}_N^\epsilon$ is not Gorenstein.

Finally, we give an example illustrating Theorem 1.7.1.

Example 1.10.7. Let $p = 5$, $\ell_0 = 11$, $\ell_1 = 41$, so $N = 11 \cdot 41$, and let $\epsilon = (-1, -1)$. We see that neither of 11 or 41 is a 5-th power modulo the other, so Theorem 1.7.1 applies. We consider the primes $2, 3, 7$ and 13, none of which are congruent to 1 modulo 5.

q	Is 5-th power modulo 11?	Is 5-th power modulo 41?
2	No	No
3	No	Yes
7	No	No
13	No	No

From this we see that

$$\det \begin{pmatrix} \log_{11}(3) & \log_{11}(q) \\ \log_{41}(3) & \log_{41}(q) \end{pmatrix} = \log_{11}(3) \cdot \log_{41}(q) \neq 0.$$

for any $q \in \{2, 7, 13\}$. By Theorem 1.7.1, $\{T_3 - 4, T_q - (q+1)\}$ generates I^ϵ for any $q \in \{2, 7, 13\}$, and we can see by direct computation that this is true.

More subtly, we can compute that

$$\det \begin{pmatrix} \log_{11}(2) & \log_{11}(7) \\ \log_{41}(2) & \log_{41}(7) \end{pmatrix} \neq 0, \quad \det \begin{pmatrix} \log_{11}(2) & \log_{11}(13) \\ \log_{41}(2) & \log_{41}(13) \end{pmatrix} = 0.$$

By Theorem 1.7.1, this implies that $\{T_2 - 3, T_7 - 8\}$ generates I^ϵ, but that $\{T_2 - 3, T_{13} - 14\}$ does not, and we again verify this by direct computation.

1.11. **Acknowledgements.** We thank Akshay Venkatesh for interesting questions that stimulated this work, and Ken Ribet for his inspiring talk [Rib15]. We thank Hwajong Yoo for bringing our attention to his work on the subject, and Frank Calegari for clarifying the provenance of Ribet's Conjecture. We thank Shekhar Khare for helpful discussions about the Steinberg condition, Matt Emerton for encouragement and for asking us about implications for newforms, and Rob Pollack for asking us about the case $p \mid N$.

We thank Joël Bellaïche, Tobias Berger, Frank Calegari, Kęstutis Česnavičius, Emmanuel Lecouturier, Barry Mazur, Rob Pollack, Ken Ribet, and Hwajong Yoo

for comments on and corrections to an early draft. We also thank the referee for helpful comments and suggestions.

P.W. was supported by the National Science Foundation under the Mathematical Sciences Postdoctoral Research Fellowship No. 1606255, as well as the grants DMS-1638352 and DMS-1901867. C.W.E. was supported by Engineering and Physical Sciences Research Council grant EP/L025485/1.

1.12. **Notation and Conventions.** We let ∂_{ij} denote the Kronecker symbol, which is 1 if $i = j$ and 0 otherwise.

For each prime $\ell \mid Np$, we fix $G_\ell \subset G_{\mathbb{Q}}$, a decomposition group at ℓ, and let $I_\ell \subset G_\ell$ denote the inertia subgroup. We fix elements $\sigma_\ell \in G_\ell$ whose image in $G_\ell/I_\ell \cong \mathrm{Gal}(\overline{\mathbb{F}}_\ell/\mathbb{F}_\ell)$ is the Frobenius. For $\ell \neq p$, we fix elements $\gamma_\ell \in I_\ell$ such that the image in the maximal pro-p-quotient $I_\ell^{\mathrm{pro}-p}$ (which is well-known to be pro-cyclic) is a topological generator. Let $\gamma_p \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p^{\mathrm{nr}}(\zeta_p)) \subset I_p$ be an element such that the image of γ_p in $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{nr}}(\zeta_p, \sqrt[p]{p})/\mathbb{Q}_p^{\mathrm{nr}}(\zeta_p))$ is non-trivial. When $\ell = \ell_i$ for $i \in \{0, \dots, r\}$ (i.e. $\ell \mid N$), we also write $\sigma_i := \sigma_{\ell_i}$ and $\gamma_i := \gamma_{\ell_i}$ for these elements. We write $G_{\mathbb{Q},S}$ for the Galois group of the maximal extension of $\mathbb{Q}$ unramified outside of the set places S of $\mathbb{Q}$ supporting $Np\infty$, and use the induced maps $G_\ell \to G_{\mathbb{Q},S}$. For primes $q \nmid Np$, we write $\mathrm{Fr}_q \in G_{\mathbb{Q},S}$ for a Frobenius element at q.

As in the theory of representations, Cayley–Hamilton representations, actions on modules, pseudorepresentations, and cochains/cocycles/cohomology of profinite groups G discussed in [WWE19], these objects and categories are implicitly meant to be continuous without further comment. Here all of the targets are finitely generated A-modules for some Noetherian local (continuous) $\mathbb{Z}_p$-algebra A with ideal of definition I, and the I-adic topology is used on the target. Profinite groups used in the sequel satisfy the Φ_p-finiteness condition (i.e. the maximal pro-p quotient of every finite-index subgroup is topologically finitely generated), which allows the theory of [WWE19] to be applied.

We write

$$H^i(\mathbb{Z}[1/Np], M) = H^i(C^\bullet(\mathbb{Z}[1/Np], M)) = \frac{Z^i(\mathbb{Z}[1/Np], M)}{B^i(\mathbb{Z}[1/Np], M)}$$

for (continuous) cohomology of a $G_{\mathbb{Q},S}$-module M, together with this notation for cochains, cocycles, and coboundaries. We write $x_1 \smile x_2 \in C^*(\mathbb{Z}[1/Np], M_1 \otimes M_2)$ for the cup product of $x_i \in C^*(\mathbb{Z}[1/Np], M_i)$, and $a_1 \cup a_2 \in H^*(\mathbb{Z}[1/Np], M_1 \otimes M_2)$ for cup product of cohomology classes $a_i \in H^*(\mathbb{Z}[1/Np], M_i)$.

2. Modular forms

In this section, we recall some results about modular curves and modular forms. Our reference is the paper of Ohta [Oht14].

2.1. **Modular curves, modular forms, and Hecke algebras.** The statements given here are all well-known. We review them here to fix notation.

2.1.1. *Modular curves.* Let $Y_0(N)_{/\mathbb{Z}_p}$ be the coarse moduli space of pairs (E, C), where E is an elliptic curve over S and $C \subset E[N]$ is a finite-flat subgroup scheme of rank N and cyclic (in the sense of Katz-Mazur [KM85]). Let $X_0(N)_{/\mathbb{Z}_p}$ be the usual compactification of $Y_0(N)_{/\mathbb{Z}_p}$, and let $\{\mathrm{cusps}\}$ denote the complement of $Y_0(N)_{/\mathbb{Z}_p}$

in $X_0(N)_{/\mathbb{Z}_p}$, considered as an effective Cartier divisor on $X_0(N)_{/\mathbb{Z}_p}$. Finally, let $X_0(N) = X_0(N)_{/\mathbb{Z}_p} \otimes \mathbb{Q}_p$.

2.1.2. *Modular forms and Hecke algebras.* The map $X_0(N)_{/\mathbb{Z}_p} \to \mathrm{Spec}(\mathbb{Z}_p)$ is known to be LCI, and we let Ω be the sheaf of regular differentials. Let

$$S_2(N;\mathbb{Z}_p) = H^0(X_0(N)_{/\mathbb{Z}_p}, \Omega), \quad M_2(N;\mathbb{Z}_p) = H^0(X_0(N)_{/\mathbb{Z}_p}, \Omega(\{\text{cusps}\}))$$

Let $\mathbb{T}'_N$ and $\mathbb{T}'^0_N$ be the subalgebras of

$$\mathrm{End}_{\mathbb{Z}_p}(M_2(N;\mathbb{Z}_p)), \quad \mathrm{End}_{\mathbb{Z}_p}(S_2(N;\mathbb{Z}_p)),$$

respectively, generated by the standard Hecke operators T_n with $(N,n)=1$, and all Atkin–Lehner operators w_ℓ for $\ell \mid N$ (we do not include any U_ℓ for $\ell \mid N$). These are semi-simple commutative $\mathbb{Z}_p$-algebras (see e.g. [AL70]).

2.1.3. *Eisenstein series and Eisenstein parts.* For each $\epsilon \in \{\pm 1\}^{r+1} \backslash \{(1,1,\dots,1)\}$, there is a element $E^\epsilon_{2,N} \in M_2(N;\mathbb{Z}_p)$ that is an eigenform for all T_n with $(N,n)=1$, and has q-expansion

$$E^\epsilon_{2,N} = -\frac{1}{24}\prod_{i=0}^{r}(\epsilon_i \ell_i + 1) + \sum_{n=1}^{\infty} a_n q^n \tag{2.1.1}$$

where $a_n = \sum_{0<d|n} t$ when $\gcd(n,N)=1$ (in particular, $a_1 = 1$), and $w_{\ell_i} E^\epsilon_{2,N} = \epsilon_i E^\epsilon_{2,N}$ (see [Oht14, Lem. 2.3.4]).

Let $I'^\epsilon = \mathrm{Ann}_{\mathbb{T}'_N}(E^\epsilon_{2,N})$, and let $\mathbb{T}^\epsilon_N$ be the completion of $\mathbb{T}'_N$ at the maximal ideal (I'^ϵ, p), and let $\mathbb{T}^{0,\epsilon}_N = \mathbb{T}'^0_N \otimes_{\mathbb{T}'_N} \mathbb{T}^\epsilon_N$. Let $I^\epsilon = I'^\epsilon \mathbb{T}^\epsilon_N$ and let $I^{0,\epsilon}$ be the image of I^ϵ in $\mathbb{T}^{0,\epsilon}_N$. For a $\mathbb{T}'_N$-module M, let $M^\epsilon_{\mathrm{Eis}} = M \otimes_{\mathbb{T}'_N} \mathbb{T}^\epsilon_N$. The map $\mathbb{T}^\epsilon_N \twoheadrightarrow \mathbb{Z}_p$ induced by $E^\epsilon_{2,N}$ is a surjective ring homomorphism with kernel I^ϵ. We refer to this as the *augmentation map* for $\mathbb{T}^\epsilon_N$.

Note that we have $w_{\ell_i} = \epsilon_i$ as elements of $\mathbb{T}^\epsilon_N$. Indeed, this follows from $w^2_{\ell_i} = 1$, $w_{\ell_i} - \epsilon_i \in I^\epsilon$, and $p \neq 2$: consider $(w_{\ell_i} - \epsilon_i)(w_{\ell_i} + \epsilon_i) = 0$ and observe that $w_{\ell_i} + \epsilon_i \in (\mathbb{T}^\epsilon_N)^\times$. Consequently, $\mathbb{T}^\epsilon_N$ is generated as a $\mathbb{Z}_p$-algebra by T_q for $q \nmid N$.

If $p \nmid N$, let $U_p \in \mathbb{T}^\epsilon_N$ denote the unit root of the polynomial

$$X^2 - T_p X + p = 0,$$

which exists and is unique by Hensel's lemma. Since $T_p - (p+1) \in I^\epsilon$, we see that $U_p - 1 \in I^\epsilon$. Moreover, we see that $T_p = U_p + pU_p^{-1}$.

2.1.4. *Duality.* As in [Oht14, Thm. 2.4.6], there are perfect pairings of free $\mathbb{Z}_p$-modules

$$M_2(N;\mathbb{Z}_p)^\epsilon_{\mathrm{Eis}} \times \mathbb{T}^\epsilon_N \longrightarrow \mathbb{Z}_p, \quad S_2(N;\mathbb{Z}_p)^\epsilon_{\mathrm{Eis}} \times \mathbb{T}^{0,\epsilon}_N \longrightarrow \mathbb{Z}_p \tag{2.1.2}$$

given by $(f,t) \mapsto a_1(t \cdot f)$, where $a_1(-)$ refers to the coefficient of q in the q-expansion. In particular, $M_2(N;\mathbb{Z}_p)^\epsilon_{\mathrm{Eis}}$ (resp. $S_2(N;\mathbb{Z}_p)^\epsilon_{\mathrm{Eis}}$) is a dualizing $\mathbb{T}^\epsilon_N$-module (resp. $\mathbb{T}^{0,\epsilon}_N$-module).

2.1.5. *Oldforms and stabilizations.* If $\ell \mid N$ is a prime and $f \in S_2(N/\ell;\mathbb{Z}_p)$ is an eigenform for all T_n with $(n, N/\ell) = 1$, then the subspace

$$\{g \in S_2(N;\mathbb{Z}_p) \ : \ a_n(g) = a_n(f) \text{ for all } (n, N/\ell) = 1\}$$

has rank two, with basis $f(z), f(\ell z)$. If we let $f_\pm(z) = f(z) \pm \ell f(\ell z)$, then $w_\ell f_\pm(z) = \pm f_\pm(z)$. Note that, since $p \neq 2$, we have $f_+ \not\equiv f_- \pmod p$. In particular, if $\epsilon' \in \{\pm 1\}^r$ is the tuple obtained from ϵ by deleting the entry corresponding to ℓ, then there are injective homomorphisms given by $f \mapsto f_{\epsilon_\ell}$,

$$M_2(N/\ell;\mathbb{Z}_p)^{\epsilon'}_{\mathrm{Eis}} \hookrightarrow M_2(N;\mathbb{Z}_p)^{\epsilon}_{\mathrm{Eis}} \quad \text{and} \quad S_2(N/\ell;\mathbb{Z}_p)^{\epsilon'}_{\mathrm{Eis}} \hookrightarrow S_2(N;\mathbb{Z}_p)^{\epsilon}_{\mathrm{Eis}}.$$

2.2. **Congruence number.** We recall this theorem of Ohta, and related results.

Theorem 2.2.1 (Ohta)**.** *There is an isomorphism $\mathbb{T}^{\epsilon,0}_N/I^{\epsilon,0} \cong \mathbb{Z}_p/a_0(E^\epsilon_{2,N})\mathbb{Z}_p$.*

This is [Oht14, Thm. 3.1.3]. His method of proof actually can be used to give the following stronger result, exactly as in [WWE20, Lem. 3.2.2]. See Lemma C.2.1 for a discussion of fiber products of rings.

Lemma 2.2.2. *The composition of the augmentation map $\mathbb{T}^\epsilon_N \to \mathbb{Z}_p$ with the quotient map $\mathbb{Z}_p \to \mathbb{Z}_p/a_0(E^\epsilon_{2,N})\mathbb{Z}_p$ factors through $\mathbb{T}^{0,\epsilon}_N$ and induces an isomorphism*

$$\mathbb{T}^\epsilon_N \xrightarrow{\sim} \mathbb{T}^{0,\epsilon}_N \times_{\mathbb{Z}_p/a_0(E^\epsilon_{2,N})\mathbb{Z}_p} \mathbb{Z}_p.$$

In particular, $\ker(\mathbb{T}^\epsilon_N \to \mathbb{T}^{0,\epsilon}_N) = \mathrm{Ann}_{\mathbb{T}^\epsilon_N}(I^\epsilon)$.

2.3. **Eigenforms and associated Galois representations.** Let $\nu : \mathbb{T}^{0,\epsilon}_N \hookrightarrow \tilde{\mathbb{T}}^{0,\epsilon}_N$ denote the normalization of $\mathbb{T}^{0,\epsilon}_N$.

Lemma 2.3.1. *We record facts about $\tilde{\mathbb{T}}^{0,\epsilon}_N$ and associated Galois representations.*

(1) Letting q vary over primes $q \nmid Np$, there is an isomorphism

$$h : \tilde{\mathbb{T}}^{0,\epsilon}_N \xrightarrow{\sim} \bigoplus_{f\in\Sigma} \mathcal{O}_f, \quad \nu(T_q) \mapsto (a_q(f))_{f\in\Sigma},$$

where $\Sigma \subset S_2(N;\overline{\mathbb{Q}}_p)^\epsilon_{\mathrm{Eis}}$ is the set of normalized eigenforms, and $\mathcal{O}_f$ is the valuation ring of the finite extension $\mathbb{Q}_p(a_q(f)_{q\nmid Np})/\mathbb{Q}_p$.

(2) For each $f \in \Sigma$, there is an absolutely irreducible representation $\rho_f : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathcal{O}_f[1/p])$ such that the characteristic polynomial of $\rho_f(\mathrm{Fr}_q)$ is $X^2 - a_q(f)X + q$ for any $q \nmid Np$.

(3) Assume $\ell_i \neq p$. The representation $\rho_f|_{G_{\ell_i}}$ is unramified if f is old at ℓ_i. Otherwise, f is new at ℓ_i and there is an isomorphism

$$\rho_f|_{G_{\ell_i}} \simeq \begin{pmatrix} \lambda(a_{\ell_i}(f))\kappa_{\mathrm{cyc}} & * \\ 0 & \lambda(a_{\ell_i}(f)) \end{pmatrix}, \tag{2.3.2}$$

where $a_{\ell_i}(f) = -\epsilon_i$.

(4) There is an isomorphism

$$\rho_f|_{G_p} \simeq \begin{pmatrix} \lambda(a_p(f)^{-1})\kappa_{\mathrm{cyc}} & * \\ 0 & \lambda(a_p(f)) \end{pmatrix}. \tag{2.3.3}$$

Moreover,

(a) $\rho_f|_{G_p}$ is finite-flat if and only if either
(i) $p \nmid N$, in which case $h : \nu(U_p) \mapsto (a_p(f))_{f\in\Sigma}$, or
(ii) $p \mid N$ and f is old at p.

(b) If $p \mid N$ and f is new at p, then $a_p(f) = -\epsilon_p = +1$, i.e. $\epsilon_p = -1$.

Proof. For (1)-(3) and (4a) see, for example, [DDT94, Thm. 3.1]. In (4b), the fact that $a_p(f) = -\epsilon_p$ is [AL70, Thm. 3]. To see that $\epsilon_p = -1$, note that the semi-simple residual representation $\bar{\rho}_f^{\mathrm{ss}}$ is $\omega \oplus 1$, but (2.3.3) implies $\bar{\rho}_f^{\mathrm{ss}}|_{G_p} = \lambda(-\epsilon_p)\omega \oplus \lambda(-\epsilon_p)$. Since $\omega|_{G_p}$ is ramified, this implies that $\lambda(-\epsilon_p) = 1$, so $\epsilon_p = -1$. □

Combining Lemmas 2.2.2 and 2.3.1, we obtain an injective homomorphism

$$\mathbb{T}_N^{\epsilon} \to \mathbb{Z}_p \oplus \mathbb{T}_N^{0,\epsilon} \to \mathbb{Z}_p \oplus \bigoplus_{f \in \Sigma} \mathcal{O}_f \tag{2.3.4}$$

determined by sending T_q to $(q+1, a_q(f)_{f\in\Sigma})$ for $q \nmid Np$ and, if $p \nmid N$, sending U_p to $(1, a_p(f)_{f\in\Sigma})$.

2.4. **The kernel of $\mathfrak{m}^{\epsilon}$ on the modular Jacobian and the Gorenstein condition.** In this section, we use some results of Ohta (following ideas of Mazur) to relate the structure of the rings $\mathbb{T}_N^{\epsilon}$ and $\mathbb{T}_N^{0,\epsilon}$ to the geometry of the Néron model $J_0(N)_{/\mathbb{Z}_p}$ of the Jacobian of $X_0(N)$. Let $J_0(N) = J_0(N)_{/\mathbb{Z}_p} \otimes \mathbb{Q}_p$.

For a $\mathbb{Z}_p$-module M, let $\mathrm{Ta}_p(M) = \mathrm{Hom}(\mathbb{Q}_p/\mathbb{Z}_p, M)$ be the Tate module of M, let $M^* = \mathrm{Hom}_{\mathbb{Z}_p}(M, \mathbb{Q}_p/\mathbb{Z}_p)$ be the Pontrjagin dual, and let $M^\vee = \mathrm{Hom}_{\mathbb{Z}_p}(M, \mathbb{Z}_p)$ be the $\mathbb{Z}_p$-dual. If M is p-divisible, then there is an identification $M^* \cong \mathrm{Ta}_p(M)^\vee$.

Let $\mathcal{T} = H^1_{\text{ét}}(X_0(N)_{\overline{\mathbb{Q}}}, \mathbb{Z}_p(1)) \cong \mathrm{Ta}_p(J_0(N)(\overline{\mathbb{Q}}_p))$.

Lemma 2.4.1. *There is an exact sequence of $\mathbb{T}_N^{0,\epsilon}[I_p]$-modules*

$$0 \longrightarrow \mathbb{T}_N^{0,\epsilon}(1) \longrightarrow \mathcal{T}_{\mathrm{Eis}}^{\epsilon} \longrightarrow (\mathbb{T}_N^{0,\epsilon})^\vee \longrightarrow 0.$$

The sequence splits as $\mathbb{T}_N^{0,\epsilon}$-modules. In particular, we have

$$\dim_{\mathbb{F}_p} J_0(N)[\mathfrak{m}^{\epsilon}](\overline{\mathbb{Q}}_p) = \dim_{\mathbb{F}_p}(\mathcal{T}/\mathfrak{m}^{\epsilon}\mathcal{T}) = 2 + \delta(\mathbb{T}_N^{0,\epsilon})$$

where $\delta(\mathbb{T}_N^{0,\epsilon})$ is the Gorenstein defect of $\mathbb{T}_N^{0,\epsilon}$. (See §C.1 for a discussion of Gorenstein defect.)

Proof. Ohta has shown in [Oht14, Prop. 3.5.4 and Prop. 3.5.9] that

$$\dim_{\mathbb{F}_p} J_0(N)_{/\mathbb{Z}_p}(\overline{\mathbb{F}}_p)[\mathfrak{m}^{\epsilon}] \leq 1.$$

This implies the result, following [Maz77, §§II.7-II.8] (see also [Maz97]). □

Lemma 2.4.2. *Suppose that $\mathbb{T}_N^{\epsilon}$ is Gorenstein. Then there is an isomorphism of $\mathbb{T}_N^{\epsilon}$-modules*

$$I^{\epsilon} \xrightarrow{\sim} (\mathbb{T}_N^{0,\epsilon})^\vee.$$

In particular, the minimal number of generators of I^{ϵ} is $\delta(\mathbb{T}_N^{0,\epsilon}) + 1$, and I^{ϵ} is principal if and only if $\mathbb{T}_N^{0,\epsilon}$ is Gorenstein.

Proof. Like the proof of [Oht14, Lem. 3.2.5], there is an exact sequence of $\mathbb{T}_N^{\epsilon}$-modules

$$0 \longrightarrow S_2(N;\mathbb{Z}_p)_{\mathrm{Eis}}^{\epsilon} \longrightarrow M_2(N;\mathbb{Z}_p)_{\mathrm{Eis}}^{\epsilon} \xrightarrow{\mathrm{Res}} \mathbb{Z}_p \longrightarrow 0$$

where $\mathbb{T}_N^{\epsilon}$ acts on $\mathbb{Z}_p$ via the augmentation map $\mathbb{T}_N^{\epsilon} \to \mathbb{T}_N^{\epsilon}/I^{\epsilon} = \mathbb{Z}_p$. Since we assume that $\mathbb{T}_N^{\epsilon}$ is Gorenstein, we see by the duality (2.1.2) that $M_2(N;\mathbb{Z}_p)_{\mathrm{Eis}}^{\epsilon}$ is a free $\mathbb{T}_N^{\epsilon}$-module of rank 1. We may choose a generator f of $M_2(N;\mathbb{Z}_p)_{\mathrm{Eis}}^{\epsilon}$ such that $\mathrm{Res}(f) = 1$. Then we obtain a surjective $\mathbb{T}_N^{\epsilon}$-module homomorphism

$$\mathbb{T}_N^{\epsilon} \twoheadrightarrow \mathbb{Z}_p, \quad T \mapsto \mathrm{Res}(Tf)$$

whose kernel is isomorphic to $S_2(N;\mathbb{Z}_p)^\epsilon_{\mathrm{Eis}}$. This is a $\mathbb{T}^\epsilon_N$-module homomorphism that sends 1 to 1, so it is the augmentation map $\mathbb{T}^\epsilon_N \twoheadrightarrow \mathbb{Z}_p$. Thus $I^\epsilon \cong S_2(N;\mathbb{Z}_p)^\epsilon_{\mathrm{Eis}}$, so duality (2.1.2) yields the isomorphism of the lemma. The remaining parts follow from §C.1. □

Combining the preceding two lemmas, we obtain the following

Lemma 2.4.3. *Assume that $\mathbb{T}^\epsilon_N$ is Gorenstein. Then*

$$\dim_{\mathbb{F}_p} J_0(N)[\mathfrak{m}^\epsilon](\overline{\mathbb{Q}}_p) = 1 + \dim_{\mathbb{F}_p}(I^\epsilon/\mathfrak{m}^\epsilon I^\epsilon).$$

3. The pseudodeformation ring

In this section, we set up the deformation theory of Galois pseudorepresentations modeling those that arise from Hecke eigenforms of weight 2 and level N that are congruent to the Eisenstein series $E^\epsilon_{2,N}$. These are the Galois representations of Lemma 2.3.1. See §1.9 for further introduction.

3.1. **Theory of Cayley–Hamilton representations.** This section is a summary of [WWE19]. Only for this section, we work with a general profinite group G satisfying condition Φ_p (of §1.12). All pseudorepresentations are assumed to have dimension 2, for simplicity.

3.1.1. *Pseudorepresentations.* A pseudorepresentation $D : E \to A$ is the data of an associative A-algebra E along with a homogeneous multiplicative polynomial law D from E to A. This definition is due to Chenevier [Che14]; see [WWE19] and the references therein. Despite the notation, the pseudorepresentation D includes the data of a multiplicative function $D : E \to A$, but is not characterized by this function alone. It is characterized by the pair of functions $\mathrm{Tr}_D, D : E \to A$, where Tr_D is defined by the *characteristic polynomial*:

$$D(x - t) = t^2 - \mathrm{Tr}_D(x)t + D(x) \in A[t]. \tag{3.1.1}$$

A pseudorepresentation $D : E \to A$ is said to be *Cayley–Hamilton* if, for every commutative A-algebra B, every element $x \in E \otimes_A B$ satisfies its characteristic polynomial. We also denote by $D : G \to A$ a pseudorepresentation $D : A[G] \to A$.

3.1.2. *Cayley–Hamilton representations.* In the category of *Cayley–Hamilton representations of a profinite group G*, an object is a triple

$$(\rho : G \to E^\times, E, D : E \to A),$$

and sometimes referred to more briefly as "ρ." Here ρ is a homomorphism (continuous, as always), E is an associative A-algebra that is finitely generated as an A-module, $(A, \mathfrak{m}_A)$ is a Noetherian local $\mathbb{Z}_p$-algebra, and D is a Cayley–Hamilton pseudorepresentation. We call A the *scalar ring* of E. The *induced pseudorepresentation of ρ* is $D \circ \rho : G \to A$, also denoted $\psi(\rho)$. The functor ψ is essentially surjective. The Cayley–Hamilton representation ρ is said to be *over* $\psi(\rho) \otimes_A A/\mathfrak{m}_A$, and $\psi(\rho)$ is said to be a *pseudodeformation* of $\psi(\rho) \otimes_A A/\mathfrak{m}_A$. If (ρ, E, D) is a Cayley–Hamilton representation of G and $x \in A[G]$, then we abuse notation and write $D(x)$ for $D(\rho(x))$ (where we also abuse notation and write $\rho : A[G] \to E$ for the linearization of ρ).

Given a pseudorepresentation $\bar{D} : G \to \mathbb{F}$ for a field $\mathbb{F}$, there is a universal object in the category of Cayley–Hamilton representations over $\bar{D}$. This is denoted by

$$(\rho^u_{\bar{D}} : G \longrightarrow (E^u_{\bar{D}})^\times, E^u_{\bar{D}}, D_{E^u_{\bar{D}}} : E^u_{\bar{D}} \to R^u_{\bar{D}}),$$

and the induced pseudorepresentation $D^u_{\bar{D}} := \psi(\rho^u_{\bar{D}})$ is the universal pseudodeformation of $\bar{D}$.

3.1.3. *Generalized matrix algebras (GMA).* An important example of a Cayley–Hamilton algebra is a *generalized matrix algebra (GMA)*. An A-GMA E is given by the data (B, C, m) where B and C are finitely-generated R-modules, $m : B \otimes_R C \to R$ is an R-module homomorphism satisfying certain conditions, and $E = \left(\begin{smallmatrix} R & B \\ C & R \end{smallmatrix}\right)$ (see [WWE19, Example 3.1.7]). There is a Cayley–Hamilton pseudorepresentation $D : E \to A$ given by the usual formula for characteristic polynomial. We write a homomorphism $\rho : G \to E^\times$ as $\rho = \left(\begin{smallmatrix} \rho_{1,1} & \rho_{1,2} \\ \rho_{2,1} & \rho_{2,2} \end{smallmatrix}\right)$.

If $\bar{D}$ is multiplicity-free (see [WWE19, Defn. 3.2.1]), then $E^u_{\bar{D}}$ has a GMA structure whose associated pseudorepresentation is $D_{E^u_{\bar{D}}}$ [WWE19, Thm. 3.2.2].

3.1.4. *Reducibility.* We will refer to the condition that a Cayley–Hamilton representation or a pseudorepresentation is *reducible*. We also refer to the *reducibility ideal* in rings receiving a pseudorepresentations. For these definitions, see [WWE19, §4.2] or [WWE18, §5.7]. The important case for this paper is that, if $(\rho, E, D : E \to A)$ is a Cayley–Hamilton representation where E is the GMA associated to (B, C, m), then the reducibility ideal of D is the image of m. There are also universal objects, denoted ρ^{red}, etc.

3.1.5. *Conditions on Cayley–Hamilton representations.* We consider two flavors of conditions $\mathcal{P}$ imposed on Cayley–Hamilton representations of G:

(1) $\mathcal{P}$ is a condition that certain elements vanish, e.g. Definition 3.4.1.
(2) $\mathcal{P}$ is a property applying to finite-length $\mathbb{Z}_p[G]$-modules and satisfying a basic stability condition, e.g. §3.5.

In case (1), one produces a universal Cayley–Hamilton $\rho^{\mathcal{P}}_{\bar{D}}$ representation of G satisfying $\mathcal{P}$ by taking the quotient by the two-sided ideal of $E_{\bar{D}}$ generated by the relevant elements, and then taking a further quotient so that a pseudorepresentation exists. This final quotient is known as the *Cayley–Hamilton quotient of $\rho^u_{\bar{D}}$ for $\mathcal{P}$*. See [WWE19, Defn. 2.4.7] for details; cf. also [WWE18, Defn. 5.9.5].

In case (2), we consider $E^u_{\bar{D}}$ as a G-module using its left action on itself by multiplication, and find in [WWE19, §2.4] that the maximal left quotient module satisfying $\mathcal{P}$ can be defined and is an algebra quotient. The subsequent Cayley–Hamilton quotient is then shown to satisfy the desired properties of $\rho^{\mathcal{P}}_{\bar{D}}$.

3.1.6. *Conditions on pseudorepresentations.* As discussed in [WWE19, §2.5], one says that a pseudorepresentation D of G satisfies $\mathcal{P}$ if there exists a Cayley–Hamilton representation ρ of G such that $\psi(\rho) = D$ and ρ satisfies $\mathcal{P}$. Then the universal pseudodeformation of $\bar{D}$ with property $\mathcal{P}$ turns out to be $\psi(\rho^{\mathcal{P}}_{\bar{D}})$.

3.2. **Universal Cayley–Hamilton representations of Galois groups.** Let $\ell \mid Np$ be a prime. Recall from §1.12 the decomposition group $G_\ell \to G_{\mathbb{Q},S}$. Let $\bar{D} : G_{\mathbb{Q},S} \to \mathbb{F}_p$ denote the pseudorepresentation $\psi(\mathbb{F}_p(1) \oplus \mathbb{F}_p)$.

We denote by

$$(\rho_{\bar{D}} : G_{\mathbb{Q},S} \longrightarrow E^\times_{\bar{D}}, E_{\bar{D}}, D_{E_{\bar{D}}} : E_{\bar{D}} \to R_{\bar{D}})$$

the universal Cayley–Hamilton representation of $G_{\mathbb{Q},S}$ over $\bar{D}$. The scalar ring $R_{\bar{D}}$ is the universal pseudodeformation ring of $\bar{D}$, with universal pseudorepresentation

$D_{\bar{D}} := \psi(\rho_{\bar{D}})$. Similarly, we let the triple

$$(\rho_\ell : G_\ell \to E_\ell^\times, E_\ell, D_{E_\ell} : E_\ell \to R_\ell)$$

denote the universal Cayley–Hamilton representation of G_ℓ over $\bar{D}|_{G_\ell}$, so that $D_\ell := \psi(\rho_\ell) : G_\ell \to R_\ell$ is the universal pseudodeformation of $\bar{D}|_{G_\ell}$.

Definition 3.2.1. Note that $\bar{D}$ is multiplicity-free, and that, if $\ell \not\equiv 1 \pmod{p}$, then $\bar{D}|_{G_\ell}$ is multiplicity-free. In this case, E_ℓ and $E_{\bar{D}}$ have the structure of a GMA. In this paper, whenever we fix such a structure, we assume that $(\rho_\ell)_{1,1} \otimes_{R_\ell} \mathbb{F}_p \cong \omega|_{G_\ell}$ (resp. $(\rho_{\bar{D}})_{1,1} \otimes_{R_{\bar{D}}} \mathbb{F}_p \cong \omega$).

3.3. **Case $\ell \nmid Np$: unramified.** For $\ell \nmid Np$, we want Galois representations to be unramified at ℓ. We impose this by considering representations of $G_{\mathbb{Q},S}$, as opposed to $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

3.4. **Case $\ell \neq p$ and $\ell \mid N$: the unramified-or-Steinberg condition.** In this subsection, we write ℓ for one of the factors of N referred to elsewhere in this manuscript as ℓ_i. Likewise, we write ϵ_ℓ for ϵ_i.

Definition 3.4.1. Let $(\rho : G_\ell \to E, E, D_E : E \to A)$ be a Cayley–Hamilton representation of G_ℓ over $\bar{D}|_{G_\ell}$. We call ρ *unramified-or-ϵ_ℓ-Steinberg* (or $\mathrm{US}_\ell^{\epsilon_\ell}$) if

$$V_\rho^{\epsilon_\ell}(\sigma,\tau) := (\rho(\sigma) - \lambda(-\epsilon_\ell)(\sigma)\kappa_{\mathrm{cyc}}(\sigma))(\rho(\tau) - \lambda(-\epsilon_\ell)(\tau)) \in E \tag{3.4.2}$$

is equal to 0 for all (σ,τ) ranging over the set

$$I_\ell \times G_\ell \cup G_\ell \times I_\ell \ \subset \ G_\ell \times G_\ell.$$

Write $V_\rho^{\epsilon_\ell}$ for the set of all elements $V_\rho^{\epsilon_\ell}(\sigma,\tau)$ over this range.

A pseudodeformation $D : G_\ell \to A$ of $\bar{D}|_{G_\ell}$ is called $\mathrm{US}_\ell^\epsilon$ if there exists a $\mathrm{US}_\ell^\epsilon$ Cayley–Hamilton representation ρ of G_ℓ such that $\psi(\rho) = D$.

Definition 3.4.3. Let $(E_\ell^{\epsilon_\ell}, D_{E_\ell^{\epsilon_\ell}} : E_\ell^{\epsilon_\ell} \to R_\ell^{\epsilon_\ell})$ be the Cayley–Hamilton quotient of (E_ℓ, D_ℓ) by $V_{\rho_\ell}^{\epsilon_\ell}$. Let

$$(\rho_\ell^{\epsilon_\ell} : G_\ell \to (E_\ell^{\epsilon_\ell})^\times, E_\ell^{\epsilon_\ell}, D_{E_\ell^{\epsilon_\ell}} : E_\ell^{\epsilon_\ell} \to R_\ell^{\epsilon_\ell}),$$

be the corresponding Cayley–Hamilton representation, with induced pseudorepresentation of G_ℓ denoted $D_\ell^{\epsilon_\ell} := \psi(\rho_\ell^{\epsilon_\ell}) : G_\ell \to R_\ell^{\epsilon_\ell}$.

By the theory of §3.1.5, $\rho_\ell^{\epsilon_\ell}$ is the universal $\mathrm{US}_\ell^{\epsilon_\ell}$ Cayley–Hamilton representation over $\bar{D}|_{G_\ell}$, and $D_\ell^{\epsilon_\ell}$ is the universal $\mathrm{US}_\ell^{\epsilon_\ell}$ pseudodeformation of $\bar{D}|_{G_\ell}$.

Lemma 3.4.4. *If $\ell \neq p$, then, for any ϵ_ℓ, we have $D_\ell^{\epsilon_\ell}(\tau) = 1$ and $\mathrm{Tr}_{D_\ell^{\epsilon_\ell}}(\tau) = 2$ for all $\tau \in I_\ell$. That is, $(D_\ell^{\epsilon_\ell})|_{I_\ell} = \psi(1 \oplus 1)$.*

Proof. Let $\tau \in I_\ell$. We see in (3.4.2) that $V_{\rho_\ell^{\epsilon_\ell}}^{\epsilon_\ell}(\tau,\tau) = (\rho_\ell^{\epsilon_\ell}(\tau) - 1)^2 = 0$. Thus by [Che14, Lem. 2.7(iv)], we see $\mathrm{Tr}_{D_\ell^{\epsilon_\ell}}(\tau - 1) = D_\ell^{\epsilon_\ell}(\tau - 1) = 0$. As traces are additive, we have $\mathrm{Tr}_{D_\ell^{\epsilon_\ell}}(\tau) = \mathrm{Tr}_{D_\ell^{\epsilon_\ell}}(1) = 2$. Applying (3.1.1) with $x = \tau$ and using the naturality of $D_\ell^{\epsilon_\ell}$ with respect to the morphism $R_\ell^{\epsilon_\ell}[t] \to R_\ell^{\epsilon_\ell}$ given by $t \mapsto 1$, we find that $D_\ell^{\epsilon_\ell}(\tau) = 1$. □

Lemma 3.4.5. *Suppose that $\epsilon_\ell = +1$ and $\ell \not\equiv -1, 0 \pmod{p}$. Then $\rho_\ell^{\epsilon_\ell}$ is unramified (i.e. $\rho_\ell^{\epsilon_\ell}|_{I_\ell} = 1$).*

Proof. Let $\sigma \in G_\ell$ be the element σ_ℓ defined in §1.12. By definition of $E_\ell^{\epsilon_\ell}$,

$$V_{\rho_\ell^{\epsilon_\ell}}^{\epsilon_\ell}(\tau, \sigma) = (\rho_\ell^{\epsilon_\ell}(\tau) - 1)(\rho_\ell^{\epsilon_\ell}(\sigma) + 1) = 0,$$

for any $\tau \in I_\ell$. To prove the lemma, it suffices to show that $(\rho_\ell^{\epsilon_\ell}(\sigma) + 1) \in (E_\ell^{\epsilon_\ell})^\times$.

By the Cayley–Hamilton property, we know that any element $x \in E_\ell^{\epsilon_\ell}$ satisfies $x^2 - \mathrm{Tr}_{D_\ell^{\epsilon_\ell}}(x)x + D_\ell^{\epsilon_\ell}(x) = 0$. In particular, we see that $x \in (E_\ell^{\epsilon_\ell})^\times$ if $D_\ell^{\epsilon_\ell}(x) \in (R_\ell^{\epsilon_\ell})^\times$. Hence it will suffice to show that $D_\ell^{\epsilon_\ell}(\sigma + 1) \in (R_\ell^{\epsilon_\ell})^\times$.

Writing $\mathfrak{m} \subset R_\ell^{\epsilon_\ell}$ for the maximal ideal, we know that $D_\ell^{\epsilon_\ell} \equiv \bar{D} \pmod{\mathfrak{m}}$, so it will suffice to show that $\bar{D}(\sigma+1) \in \mathbb{F}_p^\times$. Because $\ell \neq p$ and $\bar{D} = \psi(\omega \oplus 1)$, we apply (3.1.1) with $x = \sigma$ and $t = -1$, calculating that $\bar{D}(\sigma + 1) = 2(\ell + 1) \in \mathbb{F}_p$. This is a unit because p is odd and $\ell \not\equiv -1 \pmod{p}$. □

3.5. **The finite-flat case: $\ell = p$ and $p \nmid N$.** A finite-length $\mathbb{Z}_p[G_p]$-module V is said to be *finite-flat* when it arises as $\mathcal{G}(\overline{\mathbb{Q}}_p)$, where $\mathcal{G}$ is a finite flat group scheme over $\mathbb{Z}_p$. In [WWE19, §5.2] we check that the theory of §3.1.5 can be applied to the finite-flat condition. This theory gives us

$$(\rho_p^{\mathrm{flat}} : G_p \to (E_p^{\mathrm{flat}})^\times, E_p^{\mathrm{flat}}, D_{E_p^{\mathrm{flat}}} : E_p^{\mathrm{flat}} \to R_p^{\mathrm{flat}}),$$

the universal finite-flat Cayley–Hamilton representation of G_p over $\bar{D}|_{G_p}$. The pseudorepresentation $D_p^{\mathrm{flat}} := \psi(\rho_p^{\mathrm{flat}}) : G_p \to R_p^{\mathrm{flat}}$ is the universal finite-flat pseudodeformation of $\bar{D}|_{G_p}$.

Consider a GMA structure on E_p^{flat} as in Definition 3.2.1, which we write as

$$\rho_p^{\mathrm{flat}} = \begin{pmatrix} \rho_{p,1,1}^{\mathrm{flat}} & \rho_{p,1,2}^{\mathrm{flat}} \\ \rho_{p,2,1}^{\mathrm{flat}} & \rho_{p,2,2}^{\mathrm{flat}} \end{pmatrix} : G_p \longrightarrow \begin{pmatrix} R_p^{\mathrm{flat}} & B_p^{\mathrm{flat}} \\ C_p^{\mathrm{flat}} & R_p^{\mathrm{flat}} \end{pmatrix}^\times.$$

Lemma 3.5.1. *For any such GMA structure on E_p, $C_p^{\mathrm{flat}} = 0$.*

Proof. The proof is implicit in [WWE20] but not stated in this form there. One simply combines the following facts. See [WWE20, §B.4] for the notation.

- As the maximal ideal of R_p^{flat} contains the reducibility ideal, we have $\mathrm{Hom}_{R_p^{\mathrm{flat}}}(C_p^{\mathrm{flat}}, \mathbb{F}_p) = \mathrm{Ext}^1_{\mathrm{ffgs}/\mathbb{Z}_p}(\mu_p, \mathbb{Z}/p\mathbb{Z})$, where $\mathrm{ffgs}/\mathbb{Z}_p$ is the category of finite flat groups schemes over $\mathbb{Z}_p$, by [WWE19, Thm. 4.3.5].
- We see in [WWE20, Lem. 6.2.1(1)] that $\mathrm{Ext}^1_{\mathrm{ffgs}/\mathbb{Z}_p}(\mu_p, \mathbb{Z}/p\mathbb{Z}) = 0$.

As C_p^{flat} is a finitely-generated R_p^{flat}-module, this implies that $C_p^{\mathrm{flat}} = 0$. □

Now that we know that $C_p^{\mathrm{flat}} = 0$, $\rho_{p,i,i}^{\mathrm{flat}}$ are R_p^{flat}-valued characters of G_p, for $i = 1, 2$. Similarly to [WWE20, §5.1], using the fact that $\omega|_{G_p} \neq 1$, we see the following

Lemma 3.5.2. *A pseudodeformation D of $\bar{D}|_{G_p}$ is finite-flat if and only if $D = \psi(\kappa_{\mathrm{cyc}}\chi_1 \oplus \chi_2)$ where χ_1, χ_2 are unramified deformations of the trivial character.*

3.6. **The finite-flat case: $\ell = p$, $p \mid N$, and $\epsilon_p = +1$.** By Lemma 2.3.1(4), we see that, if $\epsilon_p = +1$, then the residually Eisenstein cusp forms are old at p with associated $G_{\mathbb{Q},S}$-representation being finite-flat at p. We impose this condition exactly as in §3.5. Namely, we say that a Cayley–Hamilton representation of G_p is *unramified-or-(+1)-Steinberg* (or US_p^{+1}) if it is finite-flat.

3.7. **The ordinary case: $\ell = p$, $p \mid N$, and $\epsilon_p = -1$.** Based on the form of Galois representations arising from p-ordinary eigenforms given in Lemma 2.3.1(4), we proceed exactly as in the case $\ell \neq p$ given in §3.4.

Definition 3.7.1. We say that a Cayley–Hamilton representation or a pseudodeformation over $\bar{D}|_{G_p}$ is *ordinary* (or US_p^{-1}) when it satisfies Definition 3.4.1, simply letting $\ell = p$.

Similarly to Definition 3.4.3, let $(E_p^{\mathrm{ord}}, D_{E_p^{\mathrm{ord}}})$ be the Cayley–Hamilton quotient of (E_p, D_{E_p}) by $V_{\rho_p}^{-1}$, and let $(\rho_p^{\mathrm{ord}}, E_p^{\mathrm{ord}}, D_{E_p^{\mathrm{ord}}} : E_p^{\mathrm{ord}} \to R_p^{\mathrm{ord}})$ be the corresponding Cayley–Hamilton representation. As per §3.1.5, ρ_p^{ord} is the universal ordinary Cayley–Hamilton representation over $\bar{D}|_{G_p}$, and $D_p^{\mathrm{ord}} := \psi(\rho_p^{\mathrm{ord}}) : G_p \to R_p^{\mathrm{ord}}$ is the universal ordinary pseudodeformation of $\bar{D}|_{G_p}$.

Remark 3.7.2. If one applies $V_{\rho_p}^{+1} = 0$ in the case $\epsilon_p = +1$, one does not get the the desired finite-flat condition of §3.6 that agrees with Lemma 2.3.1(4b). Instead, one finds that $E_p^{+1} = 0$ (i.e. no deformations of $\bar{D}$ satisfy this condition).

We set up the following notation, which includes all cases: $\epsilon_p = \pm 1$ or $p \nmid N$.

Definition 3.7.3. For any N and ϵ, we establish notation

$$(\rho_p^{\epsilon_p}, E_p^{\epsilon_p}, D_{E_p^{\epsilon_p}}, R_p^{\epsilon_p}, D_p^{\epsilon_p}) := \begin{cases} (\rho_p^{\mathrm{ord}}, E_p^{\mathrm{ord}}, D_{E_p^{\mathrm{ord}}}, R_p^{\mathrm{ord}}, D_p^{\mathrm{ord}}) & \text{if } p \mid N, \epsilon_p = -1, \\ (\rho_p^{\mathrm{flat}}, E_p^{\mathrm{flat}}, D_{E_p^{\mathrm{flat}}}, R_p^{\mathrm{flat}}, D_p^{\mathrm{flat}}) & \text{otherwise.} \end{cases}$$

In [WWE18, §5], we developed an alternative definition of ordinary Cayley–Hamilton algebra. (This definition applies to general weight, which we specialize to weight 2 here.) Choose a GMA structure on E_p, as in Definition 3.2.1. Let $J_p^{\mathrm{ord}} \subset E_p$ be the two-sided ideal generated by the subset

$$\rho_{p,2,1}(G_p) \bigcup (\rho_{p,1,1} - \kappa_{\mathrm{cyc}})(I_p) \bigcup (\rho_{p,2,2} - 1)(I_p).$$

As in [WWE18, Lem. 5.9.3], J_p^{ord} is independent of the choice of GMA-structure.

Lemma 3.7.4. *The Cayley–Hamilton quotient of E_p by J_p^{ord} is equal to E_p^{ord}.*

Proof. Let $(V_{\rho_p}^{\mathrm{ord}})$ denote the kernel of $E_p \twoheadrightarrow E_p^{\mathrm{ord}}$, which contains (but may not be generated by) V_p^{ord} (see §3.1.5). It will suffice to show that $(V_{\rho_p}^{\mathrm{ord}}) = J_p^{\mathrm{ord}}$. The inclusion $(V_{\rho_p}^{\mathrm{ord}}) \subset J_p^{\mathrm{ord}}$ is straightforward: see the calculations in [WWE18, §5.9], from which it is evident that the Cayley–Hamilton quotient of ρ_p by J_p^{ord} is a Cayley–Hamilton representation that is ordinary (in the sense of Definition 3.4.1). It remains to show that $J_p^{\mathrm{ord}} \subset (V_{\rho_p}^{\mathrm{ord}})$.

First we will show that $D_p^{\mathrm{ord}}|_{I_p} = \psi(\kappa_{\mathrm{cyc}} \oplus 1)|_{I_p} \otimes_{\mathbb{Z}_p} R_p^{\mathrm{ord}}$. For any $\tau \in I_p$, $\rho_p^{\mathrm{ord}}(\tau)$ satisfies both polynomials

$$T^2 - \mathrm{Tr}_{D_p^{\mathrm{ord}}}(\tau) T - D_p^{\mathrm{ord}}(\tau) \quad \text{and} \quad (T - \kappa_{\mathrm{cyc}}(\tau))(T - 1),$$

the first by the Cayley–Hamilton condition and the second by Definition 3.7.1. If $\omega(\tau) \neq 1$, Hensel's lemma implies that these two polynomials are identical. For such τ, we have $D_p^{\mathrm{ord}}(\tau) = \kappa_{\mathrm{cyc}}(\tau)$ and $\mathrm{Tr}_{D_p^{\mathrm{ord}}}(\tau) = \kappa_{\mathrm{cyc}}(\tau) + 1$. Now choose an arbitrary element of I_p and write it as $\sigma\tau$ with $\omega(\sigma), \omega(\tau) \neq 1$. We immediately

see that $D_p^{\mathrm{ord}}(\sigma\tau) = \kappa_{\mathrm{cyc}}(\sigma\tau)$, since both sides are multiplicative. Let $r_\sigma = \rho_p^{\mathrm{ord}}(\sigma)$ and $r_\tau = \rho_p^{\mathrm{ord}}(\tau)$. Since E_p^{ord} is Cayley–Hamilton, we have

$$(t_\sigma r_\sigma + t_\tau r_\tau)^2 - \mathrm{Tr}_{D_p^{\mathrm{ord}}}(t_\sigma r_\sigma + t_\tau r_\tau)(t_\sigma r_\sigma + t_\tau r_\tau) + D_p^{\mathrm{ord}}(t_\sigma r_\sigma + t_\tau r_\tau) = 0$$

in the polynomial ring $E_p^{\mathrm{ord}}[t_\sigma, t_\tau]$. We can expand $D_p^{\mathrm{ord}}(t_\sigma r_\sigma + t_\tau r_\tau)$ using [Che14, Example 1.8]. Taking the coefficient of $t_\sigma t_\tau$ and writing $\mathrm{Tr} = \mathrm{Tr}_{D_p^{\mathrm{ord}}}$ for brevity,

$$r_\sigma r_\tau + r_\tau r_\sigma - \mathrm{Tr}(\sigma) r_\tau - \mathrm{Tr}(\tau) r_\sigma - \mathrm{Tr}(\sigma\tau) + \mathrm{Tr}(\sigma)\mathrm{Tr}(\tau) = 0.$$

Substituting for $r_\sigma r_\tau$ using $V_{\rho_p}^{\mathrm{ord}}(\sigma, \tau) = 0$ and for $r_\tau r_\sigma$ using $V_{\rho_p}^{\mathrm{ord}}(\tau, \sigma) = 0$, one obtains the desired conclusion $\mathrm{Tr}(\sigma\tau) = \kappa_{\mathrm{cyc}}(\sigma\tau) + 1$.

Let $\sigma \in I_p$, and let $\tau \in I_p$ be such that $\omega(\tau) \neq 1$. Using the fact that $\rho_p^{\mathrm{ord}}|_{I_p}$ is reducible, we see that the $(1,1)$-coordinate of $V_{\rho_p^{\mathrm{ord}}}^{\mathrm{ord}}(\sigma, \tau)$ is

$$(\rho_{p,1,1}^{\mathrm{ord}}(\sigma) - \kappa_{\mathrm{cyc}}(\sigma))(\rho_{p,1,1}^{\mathrm{ord}}(\tau) - 1) = 0$$

Since $\rho_{p,1,1}^{\mathrm{ord}}$ is a deformation of ω, we have $\rho_{p,1,1}^{\mathrm{ord}}(\tau) - 1 \in (R_p^{\mathrm{ord}})^\times$, so this implies $\rho_{p,1,1}^{\mathrm{ord}}(\sigma) - \kappa_{\mathrm{cyc}}(\sigma) = 0$. This shows that $(\rho_{p,1,1} - \kappa_{\mathrm{cyc}})(I_p) \subset (V_{\rho_p}^{\mathrm{ord}})$, and a similar argument gives $(\rho_{p,2,2}^{\mathrm{ord}} - 1)(I_p) \subset (V_{\rho_p}^{\mathrm{ord}})$.

It remains to show that $\rho_{p,2,1}^{\mathrm{ord}}(G_p) = 0$. Let $\mathfrak{m} \subset R_p^{\mathrm{ord}}$ be the maximal ideal. In fact, we will show that $C_p^{\mathrm{ord}}/\mathfrak{m}C_p^{\mathrm{ord}} = 0$, which is equivalent because $\rho_{p,2,1}^{\mathrm{ord}}(G_p)$ generates the finitely generated R_p^{ord}-module C_p^{ord}. We work with $\bar{\rho}^{\mathrm{ord}} := \rho_p^{\mathrm{ord}} \pmod{\mathfrak{m}}$. Since $\bar{\rho}^{\mathrm{ord}}$ is reducible, we can consider $\bar{\rho}_{2,1}^{\mathrm{ord}} \in Z^1(G_p, C_p^{\mathrm{ord}}/\mathfrak{m}C_p^{\mathrm{ord}} \otimes_{\mathbb{F}_p} \mathbb{F}_p(-1))$, and [BC09, Thm. 1.5.5] implies that there is an injection

$$\mathrm{Hom}_{\mathbb{F}_p}(C_p^{\mathrm{ord}}/\mathfrak{m}C_p^{\mathrm{ord}}, \mathbb{F}_p) \hookrightarrow H^1(G_p, \mathbb{F}_p(-1))$$

sending ϕ to the class of the cocycle $\phi \circ \bar{\rho}_{2,1}^{\mathrm{ord}}$. So to show that $C_p^{\mathrm{ord}}/\mathfrak{m}C_p^{\mathrm{ord}}$ is zero, it is enough to show that $\bar{\rho}_{2,1}^{\mathrm{ord}}$ is a coboundary, or, equivalently, that $\bar{\rho}_{2,1}^{\mathrm{ord}}(\sigma) = 0$ for all $\sigma \in \ker(\omega) \subset G_p$. However, we compute that the $(2,1)$-entry of $V_{\rho_p}^{\mathrm{ord}}(\sigma, \tau)$ is

$$\rho_{p,2,1}^{\mathrm{ord}}(\sigma)(\rho_{p,1,1}^{\mathrm{ord}}(\tau) - 1) + (\rho_{p,2,2}^{\mathrm{ord}}(\sigma) - \kappa_{\mathrm{cyc}}(\sigma))\rho_{p,2,1}^{\mathrm{ord}}(\tau).$$

Taking $\sigma \in \ker(\omega)$ and $\tau \in I_p$ such that $\omega(\tau) \neq 1$, we see that $\rho_{p,1,1}^{\mathrm{ord}}(\tau) - 1 \equiv \omega(\tau) - 1 \not\equiv 0 \pmod{\mathfrak{m}}$ and $\rho_{p,2,2}^{\mathrm{ord}}(\sigma) - \kappa_{\mathrm{cyc}}(\sigma) \in \mathfrak{m}$, so this implies $\bar{\rho}_{2,1}^{\mathrm{ord}}(\sigma) = 0$. □

We have the following consequence, following [WWE18, §5.9].

Proposition 3.7.5. *A Cayley–Hamilton representation $(\rho : G_p \to E^\times, E, D : E \to A)$ over $\bar{D}|_{G_p}$ is ordinary if and only if it admits a GMA structure such that*

1. *it is upper triangular, i.e. $\rho_{2,1} = 0$, and*
2. *the diagonal character $\rho_{1,1}$ (resp. $\rho_{2,2}$) is the product of $\kappa_{\mathrm{cyc}} \otimes_{\mathbb{Z}_p} A$ (resp. the constant character A) and an unramified A-valued character.*

Corollary 3.7.6. *Any finite-flat Cayley–Hamilton representation of G_p over $\bar{D}|_{G_p}$ is ordinary. The resulting morphism of universal Cayley–Hamilton representations of G_p, $(\rho_p^{\mathrm{ord}}, E_p^{\mathrm{ord}}, D_{E_p^{\mathrm{ord}}}) \to (\rho_p^{\mathrm{flat}}, E_p^{\mathrm{flat}}, D_{E_p^{\mathrm{flat}}})$, induces an isomorphism on universal pseudodeformation rings $R_p^{\mathrm{ord}} \xrightarrow{\sim} R_p^{\mathrm{flat}}$. The universal pseudodeformations $D_p^{\mathrm{ord}} \cong D_p^{\mathrm{flat}}$ of $\bar{D}|_{G_p}$ have the form $\psi(\kappa_{\mathrm{cyc}}\chi_1 \oplus \chi_2)$, where χ_1, χ_2 are unramified deformations of the trivial character $1 : G_p \to \mathbb{F}_p^\times$.*

Proof. The Cayley–Hamilton representation ρ_p^{flat} satisfies conditions (1) and (2) of Proposition 3.7.5 by Lemmas 3.5.1 and 3.5.2, respectively. The isomorphism of universal pseudorepresentations becomes evident by comparing Lemma 3.5.2 and Proposition 3.7.5(2). □

3.8. **Global formulation.** We now combine the local constructions to define what it means for a global Cayley–Hamilton representation or pseudorepresentation to be unramified-or-Steinberg of level N and type ϵ.

Definition 3.8.1. Let $(\rho : G_{\mathbb{Q},S} \to E^\times, E, D_E : E \to A)$ be a Cayley–Hamilton representation over $\bar{D}$. We say that ρ is *unramified-or-Steinberg of level N and type ϵ* (or US_N^ϵ) when $\rho|_{G_\ell}$ is $\mathrm{US}_\ell^{\epsilon_\ell}$ for all primes $\ell \mid N$, and, if $p \nmid N$, $\rho|_{G_p}$ is finite-flat.

Let $D : G_{\mathbb{Q},S} \to A$ be a pseudodeformation of $\bar{D}$. We say that D is *unramified-or-Steinberg of level N and type ϵ* (or US_N^ϵ) when there exists a Cayley–Hamilton representation $(\rho : G_{\mathbb{Q},S} \to E^\times, E, D_E : E \to A)$ such that $D = \psi(\rho)$ and ρ is US_N^ϵ.

Recall the Cayley–Hamilton representation $\rho_{\bar{D}}$ set up in §3.2. There are maps of Cayley–Hamilton algebras $\iota_\ell : (E_\ell, D_{E_\ell}) \to (E_{\bar{D}}, D_{E_{\bar{D}}})$ arising from the fact that $\rho_{\bar{D}}|_{G_\ell}$ is a Cayley–Hamilton representation of G_ℓ over $\bar{D}|_{G_\ell}$. For any $\ell \mid Np$, write J_ℓ^ϵ for the kernel of $E_\ell \to E_\ell^{\epsilon_\ell}$ (refer to Definition 3.7.3 for $E_p^{\epsilon_p}$).

Definition 3.8.2. Let $(E_N^\epsilon, D_{E_N^\epsilon})$ denote the Cayley–Hamilton algebra quotient of $E_{\bar{D}}$ by the union of $\iota_\ell(J_\ell^\epsilon)$ over all primes $\ell \mid Np$. We denote the quotient Cayley–Hamilton representation of $G_{\mathbb{Q},S}$ by

$$(\rho_N^\epsilon : G_{\mathbb{Q},S} \longrightarrow (E_N^\epsilon)^\times, E_N^\epsilon, D_{E_N^\epsilon} : E_N^\epsilon \longrightarrow R_N^\epsilon)$$

and its induced pseudorepresentation by $D_N^\epsilon = \psi(\rho_N^\epsilon) : G_{\mathbb{Q},S} \to R_N^\epsilon$.

Using §3.1.5, we see that ρ_N^ϵ (resp. D_N^ϵ) is the universal US_N^ϵ Cayley–Hamilton representation (resp. pseudodeformation) over $\bar{D}$. In particular, a homomorphism $R_{\bar{D}} \to A$ factors through R_N^ϵ if and only if the corresponding pseudodeformation $D : G_{\mathbb{Q},S} \to A$ of $\bar{D}$ satisfies US_N^ϵ.

Proposition 3.8.3. *Let $D : G_{\mathbb{Q},S} \to A$ be a pseudodeformation of $\bar{D}$ satisfying US_N^ϵ. Then $D(\tau) = \kappa_{\mathrm{cyc}}(\tau)$ for all $\tau \in G_{\mathbb{Q},S}$.*

Proof. It suffices to show that $D(\tau) = \kappa_{\mathrm{cyc}}(\tau)$ for all $\tau \in I_\ell$ and all $\ell \mid Np$, since this will show that $G_{\mathbb{Q},S} \ni \sigma \mapsto D(\sigma)\kappa_{\mathrm{cyc}}^{-1}(\sigma) \in A^\times$ is a character of $G_{\mathbb{Q},S}$ that is unramified everywhere and hence trivial. For $\ell \neq p$, this follows from Lemma 3.4.4, and for $\ell = p$ this follows from Corollary 3.7.6. □

3.9. **Information about B_N^ϵ and C_N^ϵ.** Recall that we fixed a GMA structure on E_p in §3.7. This defines a GMA structure on $E_p^{\epsilon_p}$ and E_N^ϵ via the Cayley–Hamilton algebra morphisms $E_p \to E_p^{\epsilon_p}$ and $E_p^{\epsilon_p} \to E_N^\epsilon$ (see [WWE19, Theorem 3.2.2]). We write this GMA structure as

$$E_N^\epsilon = \begin{pmatrix} R_N^\epsilon & B_N^\epsilon \\ C_N^\epsilon & R_N^\epsilon \end{pmatrix}, \quad \rho_N^\epsilon(\tau) = \begin{pmatrix} a_\tau & b_\tau \\ c_\tau & d_\tau \end{pmatrix}. \tag{3.9.1}$$

3.9.1. *Computation of $B_{\mathrm{flat}}^{\mathrm{min}}$ and $C_{\mathrm{flat}}^{\mathrm{min}}$.* First we work in the case that either $p \nmid N$ or $\epsilon_p = +1$, so $E_p^{\epsilon_p} = E_p^{\mathrm{flat}}$, with a GMA structure chosen. Let $(E_{\mathrm{flat}}, D_{E_{\mathrm{flat}}})$

represent the Cayley–Hamilton quotient of $E_{\bar{D}}$ by $\iota_p(J_p^\epsilon)$, with a GMA structure coming from $E_p^{\mathrm{flat}} \to E_{\mathrm{flat}}$. Write this GMA structure as

$$E_{\mathrm{flat}} \cong \begin{pmatrix} R_{\mathrm{flat}} & B_{\mathrm{flat}} \\ C_{\mathrm{flat}} & R_{\mathrm{flat}} \end{pmatrix}, \quad \rho_{\mathrm{flat}}(\tau) = \begin{pmatrix} a_{\mathrm{flat},\tau} & b_{\mathrm{flat},\tau} \\ c_{\mathrm{flat},\tau} & d_{\mathrm{flat},\tau} \end{pmatrix}. \tag{3.9.2}$$

Let $J_{\mathrm{flat}}^{\mathrm{min}} = \ker(R_{\mathrm{flat}} \to \mathbb{Z}_p)$, where $R_{\mathrm{flat}} \to \mathbb{Z}_p$ corresponds to $\psi(\mathbb{Z}_p(1) \oplus \mathbb{Z}_p)$, which is obviously finite-flat. Let

$$B_{\mathrm{flat}}^{\mathrm{min}} = B_{\mathrm{flat}}/J_{\mathrm{flat}}^{\mathrm{min}} B_{\mathrm{flat}}, \quad C_{\mathrm{flat}}^{\mathrm{min}} = C_{\mathrm{flat}}/J_{\mathrm{flat}}^{\mathrm{min}} C_{\mathrm{flat}}.$$

By [WWE20, Prop. 2.5.1], we have, for any finitely-generated $\mathbb{Z}_p$-module M, isomorphisms

$$\begin{aligned} \mathrm{Hom}_{\mathbb{Z}_p}(B_{\mathrm{flat}}^{\mathrm{min}}, M) &\cong H^1_{\mathrm{flat}}(\mathbb{Z}[1/Np], M(1)) \\ \mathrm{Hom}_{\mathbb{Z}_p}(C_{\mathrm{flat}}^{\mathrm{min}}, M) &\cong H^1_{(p)}(\mathbb{Z}[1/Np], M(-1)). \end{aligned} \tag{3.9.3}$$

where $H^1_{\mathrm{flat}}(\mathbb{Z}[1/Np], M(1))$ equals

$$\ker\left(H^1(\mathbb{Z}[1/Np], M(1)) \to \frac{H^1(\mathbb{Q}_p, M(1))}{\mathrm{Ext}_{\mathrm{ffgs}/\mathbb{Z}_p}(\mathbb{Z}_p, M \otimes_{\mathbb{Z}_p} \mathrm{Ta}_p(\mu_{p^\infty}))} \right)$$

and

$$H^1_{(p)}(\mathbb{Z}[1/Np], M(-1)) = \ker(H^1(\mathbb{Z}[1/Np], M(-1)) \to H^1(\mathbb{Q}_p, M(-1))).$$

Here $\mathrm{ffgs}/\mathbb{Z}_p$ is the category of locally-free group schemes of finite rank over $\mathbb{Z}_p$, which maps to the category of G_p-modules by taking generic fiber. In other words, a class in $H^1_{\mathrm{flat}}(\mathbb{Z}[1/Np], M(1))$ (resp. $H^1_{(p)}(\mathbb{Z}[1/Np], M(-1))$) is represented by a Galois representation ρ that is an extension of $\mathbb{Z}_p$ by $M(1)$ (resp. $M(-1)$), such that $\rho|_{G_p}$ is isomorphic to the generic fiber of a locally-free group scheme of finite rank over $\mathbb{Z}_p$ (resp. $\rho|_p$ is a trivial extension). The Galois cohomology computations of [WWE20, §6.3] allow us to compute these.

Lemma 3.9.4. *Recall that $N = \ell_0\ell_1\cdots\ell_r$, and recall the elements $\gamma_i \in I_{\ell_i}$ for $i = 0, \ldots, r$ defined in §1.12. There are isomorphisms*

$$\mathbb{Z}_p^{\oplus r+1} \xrightarrow{\sim} B_{\mathrm{flat}}^{\mathrm{min}}, \quad \bigoplus_{i=0}^{r} \mathbb{Z}_p/(\ell_i^2 - 1)\mathbb{Z}_p \xrightarrow{\sim} C_{\mathrm{flat}}^{\mathrm{min}}$$

given by $e_i \mapsto b_{\mathrm{flat},\gamma_i}$ and $e_i \mapsto c_{\mathrm{flat},\gamma_i}$, where $e_i \in \mathbb{Z}_p^{\oplus r+1}$ is the i-th standard basis vector.

3.9.2. *Computation of $B_{\mathrm{ord}}^{\mathrm{min}}$ and $C_{\mathrm{ord}}^{\mathrm{min}}$.* Next we compute in the case $p \mid N$ and $\epsilon_p = -1$, so $E_p^{\epsilon_p} = E_p^{\mathrm{ord}}$. Let $(E_{\mathrm{ord}}, D_{E_{\mathrm{ord}}})$ be the Cayley–Hamilton quotient of $E_{\bar{D}}$ by $\iota_p(J_p^\epsilon)$, receiving a GMA structure via $E_p^{\mathrm{ord}} \to E_{\mathrm{ord}}$. Write this GMA structure as

$$E_{\mathrm{ord}} \cong \begin{pmatrix} R_{\mathrm{ord}} & B_{\mathrm{ord}} \\ C_{\mathrm{ord}} & R_{\mathrm{ord}} \end{pmatrix}, \quad \rho_{\mathrm{ord}}(\tau) = \begin{pmatrix} a_{\mathrm{ord},\tau} & b_{\mathrm{ord},\tau} \\ c_{\mathrm{ord},\tau} & d_{\mathrm{ord},\tau} \end{pmatrix}. \tag{3.9.5}$$

Let $J_{\mathrm{ord}}^{\mathrm{min}} = \ker(R_{\mathrm{ord}} \to \mathbb{Z}_p)$, where $R_{\mathrm{ord}} \to \mathbb{Z}_p$ corresponds to $\psi(\mathbb{Z}_p(1) \oplus \mathbb{Z}_p)$, which is obviously ordinary. Let

$$B_{\mathrm{ord}}^{\mathrm{min}} = B_{\mathrm{ord}}/J_{\mathrm{ord}}^{\mathrm{min}} B_{\mathrm{flat}}, \quad C_{\mathrm{ord}}^{\mathrm{min}} = C_{\mathrm{ord}}/J_{\mathrm{ord}}^{\mathrm{min}} C_{\mathrm{ord}}.$$

Just as in [WWE17, Lem. 4.1.5], we have, for any finitely-generated $\mathbb{Z}_p$-module M, isomorphisms

$$\begin{aligned} \mathrm{Hom}_{\mathbb{Z}_p}(B^{\min}_{\mathrm{ord}}, M) &\cong H^1(\mathbb{Z}[1/Np], M(1)), \\ \mathrm{Hom}_{\mathbb{Z}_p}(C^{\min}_{\mathrm{ord}}, M) &\cong H^1_{(p)}(\mathbb{Z}[1/Np], M(-1)). \end{aligned} \tag{3.9.6}$$

The Galois cohomology computations of [WWE20, §6.3] allow us to compute these. Recall that γ_i is defined in §1.12, even when $\ell_i = p$.

Lemma 3.9.7. *There are isomorphisms*

$$\mathbb{Z}_p^{\oplus r+1} \xrightarrow{\sim} B^{\min}_{\mathrm{ord}}, \quad \bigoplus_{i=0}^{r} \mathbb{Z}_p/(\ell_i^2-1)\mathbb{Z}_p \xrightarrow{\sim} C^{\min}_{\mathrm{ord}}$$

given by $e_i \mapsto b_{\mathrm{ord},\gamma_i}$ and $e_i \mapsto c_{\mathrm{ord},\gamma_i}$, where $e_i \in \mathbb{Z}_p^{\oplus r+1}$ is the i-th standard basis vector.

3.9.3. *Information about $B_N^{\epsilon,\min}$ and $C_N^{\epsilon,\min}$.* Let $J^{\min} := \ker(R_N^{\epsilon} \to \mathbb{Z}_p)$, where this homomorphism is induced by the US_N^{ϵ} pseudodeformation $\psi(\mathbb{Z}_p(1) \oplus \mathbb{Z}_p)$ of $\bar{D}$.

Lemma 3.9.8. *We consider $B_N^{\epsilon,\min} = B_N^{\epsilon}/J^{\min} B_N^{\epsilon}$ and $C_N^{\epsilon,\min} = C_N^{\epsilon}/J^{\min} C_N^{\epsilon}$.*

(1) If $\epsilon_i = 1$ and $\ell_i \neq p$, then the image of b_{γ_i} in $B_N^{\epsilon,\min}$ is 0.

(2) If $\epsilon_i + \ell_i \not\equiv 0 \pmod{p}$, then the image of c_{γ_i} in $C_N^{\epsilon,\min}$ is 0.

Moreover, there are surjections

$$\bigoplus_{i=0}^{r} \mathbb{Z}_p/(\epsilon_i+1)\mathbb{Z}_p \twoheadrightarrow B_N^{\epsilon,\min}, \qquad \bigoplus_{i=0}^{r} \mathbb{Z}_p/(\ell_i+\epsilon_i)\mathbb{Z}_p \twoheadrightarrow C_N^{\epsilon,\min}.$$

given by $e_i \mapsto b_{\gamma_i}$ and $e_i \mapsto c_{\gamma_i}$, respectively.

Proof. Note that for $\rho_N^{\epsilon,\min} = \rho_N^{\epsilon} \otimes_{R_N^{\epsilon}} R_N^{\epsilon}/J^{\min}$, in the GMA structure, we have

$$\rho_N^{\epsilon,\min} = \begin{pmatrix} \kappa_{\mathrm{cyc}} & b \\ c & 1 \end{pmatrix}.$$

Note that we have

$$V^{\epsilon_i}_{\rho_N^{\epsilon,\min}}(\gamma_i, \sigma_i) = (\rho_N^{\epsilon,\min}(\gamma_i) - 1)(\rho_N^{\epsilon,\min}(\sigma_i) + \epsilon_i) = 0.$$

In GMA notation, this is

$$0 = \begin{pmatrix} 0 & b_{\gamma_i} \\ c_{\gamma_i} & 0 \end{pmatrix} \begin{pmatrix} \ell_i + \epsilon_i & b_{\sigma_i} \\ c_{\sigma_i} & 1+\epsilon_i \end{pmatrix} = \begin{pmatrix} 0 & (1+\epsilon_i) b_{\gamma_i} \\ (\ell_i+\epsilon_i) c_{\gamma_i} & 0 \end{pmatrix}.$$

In case (1), $(1+\epsilon_i)$ is invertible, so $b_{\gamma_i} = 0$. In case (2), $(\ell_i + \epsilon_i)$ is invertible, so $c_{\gamma_i} = 0$.

The final statement follows from (1) and (2) and Lemma 3.9.7 if $p \mid N$ and $\epsilon_p = -1$; otherwise, it follows from Lemma 3.9.4. □

3.10. **Labeling some cohomology classes.** Later, in §7, it will be convenient to have notation for the extension classes, taken as Galois cohomology classes, arising from homomorphisms $B_N^{\epsilon,\min} \to \mathbb{F}_p$ and $C_N^{\epsilon,\min} \to \mathbb{F}_p$.

Definition 3.10.1. We call a cohomology class $x \in H^1(\mathbb{Z}[1/Np], M)$ *ramified at a prime ℓ* when its image in $H^1(I_\ell, M)$ is non-zero. For certain i with $0 \le i \le r$, we designate b_i and c_i as follows.

- For $i = 0, \dots, r$, let $\tilde{b}_i$ denote the $\mathbb{F}_p^\times$-scaling of the Kummer cocycle of ℓ_i such that $\tilde{b}_i(\gamma_i) = 1$, and let $b_i \in H^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1))$ be the class of $\tilde{b}_i$.
- Let $T = \{0 \leq j \leq r \ : \ell_i \equiv \pm 1 \pmod{p}\}$. For $i \in T$, let $c_i \in H^1_{(p)}(\mathbb{Z}[1/Np], \mathbb{F}_p(-1))$ be an element that is ramified exactly at ℓ_i and such that $\tilde{c}_i(\gamma_i) = 1$ for any cocycle $\tilde{c}_i$ representing c_i.

Lemma 3.10.2. *The sets $\{b_i\}_{i=0}^r$ and $\{c_i\}_{i \in T}$ are well-defined and satisfy the following properties:*

(i) b_i is characterized up to $\mathbb{F}_p^\times$-scaling by being ramified at ℓ_i, unramified outside $\{\ell_i, p\}$, and finite-flat at p if $\ell_i \neq p$.
(ii) If $p \mid N$, the set $\{b_i\}_{i=0}^r$ is a basis of $H^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1))$.
(iii) The subset $\{b_i \ : \ \ell_i \neq p\}$ is a basis of $H^1_{\mathrm{flat}}(\mathbb{Z}[1/Np], \mathbb{F}_p(1))$.
(iv) The set $\{c_i\}_{i \in T}$ is a basis of $H^1_{(p)}(\mathbb{Z}[1/Np], \mathbb{F}_p(-1))$.

Proof. The value of $\tilde{b}_i(\gamma_i)$ is well-defined for the same reason when $\ell_i \neq p$, and $b_p(\gamma_p)$ is well-defined by the choice of γ_p (in §1.12). Parts (i), (ii), and (iii) follow from Kummer theory (note that the Kummer class of p is not finite-flat at p).

For part (iv), note that the module $C_N^{\epsilon,\min}$ is computed in [WWE20, Prop. 6.3.3]. Together with (3.9.3), this computation implies the existence of $c_i \in H^1_{(p)}(\mathbb{F}_p(-1))$ characterized up to $\mathbb{F}_p^\times$-scaling by being ramified exactly at ℓ_i. These statements also imply part (iv). Because $\omega|_{I_{\ell_i}} = 1$, $\tilde{c}_i|_{I_{\ell_i}} : I_{\ell_i} \twoheadrightarrow \mathbb{F}_p$ is a homomorphism not dependent on the choice of $\tilde{c}_i$. □

The stated bases are almost dual bases, with the exception arising from the possibility that b_i is ramified at p even when $\ell_i \neq p$.

Lemma 3.10.3. *Under the perfect pairings*

(1) $B_{\mathrm{flat}} \otimes_{R_{\mathrm{flat}}} \mathbb{F}_p \times H^1_{\mathrm{flat}}(\mathbb{Z}[1/Np], \mathbb{F}_p(1)) \longrightarrow \mathbb{F}_p$,
(2) $C_{\mathrm{ord}} \otimes_{R_{\mathrm{ord}}} \mathbb{F}_p \times H^1_{(p)}(\mathbb{Z}[1/Np], \mathbb{F}_p(-1)) \longrightarrow \mathbb{F}_p$
(3) $C_{\mathrm{flat}} \otimes_{R_{\mathrm{flat}}} \mathbb{F}_p \times H^1_{(p)}(\mathbb{Z}[1/Np], \mathbb{F}_p(-1)) \longrightarrow \mathbb{F}_p$,

defined by (3.9.3) and (3.9.6), the following are respective dual basis pairs

(1) $\{b_{\mathrm{flat},\gamma_i} \ : \ i = 0, \dots, r$ if $\ell_i \neq p\}$ and $\{b_i \ : \ i = 0, \dots, r$ if $\ell_i \neq p\}$
(2) $\{c_{\mathrm{ord},\gamma_i} \ : \ i \in T\}$ and $\{c_i \ : \ i \in T\}$
(3) $\{c_{\mathrm{flat},\gamma_i} \ : \ i \in T\}$ and $\{c_i \ : \ i \in T\}$

Also, for $0 \leq i, j \leq r$ such that $\ell_i = p$ or $\ell_j \neq p$, we have $b_i(b_{\mathrm{ord},\gamma_j}) = \partial_{ij}$.

Proof. We give the proof for (1), the other parts being similar. The pairing (3.9.3) sends a class $x \in H^1_{\mathrm{flat}}(\mathbb{Z}[1/Np], \mathbb{F}_p(1))$ to a homomorphism $B_{\mathrm{flat}} \to \mathbb{F}_p$ that sends b_τ to $\tilde{x}(\tau)$, where $\tilde{x}$ is a particular cocycle representing x (the choice is determined by the choice of GMA structure on E_{flat}). However, if $\omega(\tau) = 1$, the value of $\tilde{x}(\tau)$ is independent of the choice of cocycle, and we may write this value as $x(\tau)$. Hence we see that $b_i(b_{\mathrm{flat},\gamma_j}) = b_i(\gamma_j) = \partial_{ij}$. □

Definition 3.10.4. For each $i \in T$, let K_i be the fixed field of $\ker(\tilde{c}_i|_{G_{\mathbb{Q}(\zeta_p),S}})$, where $\tilde{c}_i$ is any cocycle $\tilde{c}_i : G_{\mathbb{Q},S} \to \mathbb{F}_p(-1)$ representing c_i.

One readily verifies that K_i is the unique extension of $\mathbb{Q}(\zeta_p)$ satisfying the properties of §1.4.4.

4. Toward $R = \mathbb{T}$

4.1. **The map $R_N^\epsilon \to \mathbb{T}_N^\epsilon$.** We prove the following proposition, following the construction technique of Calegari–Emerton [CE05, Prop. 3.12].

Proposition 4.1.1. *There is a surjective homomorphism $R_N^\epsilon \twoheadrightarrow \mathbb{T}_N^\epsilon$ of augmented $\mathbb{Z}_p$-algebras. Moreover, $\mathbb{T}_N^\epsilon$ is generated as a $\mathbb{Z}_p$-algebra by T_q for any cofinite set of primes q not dividing Np.*

Proof. For this proof, it is important to note that the elements $\mathrm{Tr}_{D_N^\epsilon}(\mathrm{Fr}_q)$ for any such set of primes q generate R_N^ϵ as a $\mathbb{Z}_p$-algebra. This follows the fact that R_N^ϵ is a quotient of the (unrestricted) universal pseudodeformation ring $R_{\bar{D}}$, that traces $\{\mathrm{Tr}_{D_{\bar{D}}}(\sigma) : \sigma \in G_{\mathbb{Q},S}\}$ of the universal pseudodeformation generate $R_{\bar{D}}$ (because the residue characteristic is not 2, see [Che14, Prop. 1.29]), and Chebotarev density.

In the rest of the proof, we use the notation Σ, ρ_f and $\mathcal{O}_f$ established in Lemma 2.3.1. We proceed in three steps:

Step 1. Construct a homomorphism $R_N^\epsilon \to \mathcal{O}_f$ for each $f \in \Sigma$ that sends $\mathrm{Tr}_{D_N^\epsilon}(\mathrm{Fr}_q)$ to $a_q(f)$ for each prime $q \nmid Np$.

Step 2. Show that the resulting map $R_N^\epsilon \to \mathbb{Z}_p \oplus \bigoplus_f \mathcal{O}_f$ sends $\mathrm{Tr}_{D_N^\epsilon}(\mathrm{Fr}_q)$ to the image of T_q under the map $\mathbb{T}_N^\epsilon \to \mathbb{Z}_p \oplus \bigoplus_f \mathcal{O}_f$ of (2.3.4), for each $q \nmid Np$. This gives a homomorphism $R_N^\epsilon \to \mathbb{T}_N^\epsilon$ whose image is the $\mathbb{Z}_p$-subalgebra generated by the T_q for all $q \nmid Np$. This completes the proof if $p \mid N$.

Step 3. In the case that $p \nmid N$, show that the image of $R_N^\epsilon \to \mathbb{T}_N^\epsilon$ contains U_p and U_p^{-1}. This shows both that $R_N^\epsilon \to \mathbb{T}_N^\epsilon$ is surjective and that $\mathbb{T}_N^\epsilon$ is generated as a $\mathbb{Z}_p$-algebra by T_q for $q \nmid Np$.

Proof of Step 1. Let $f \in \Sigma$. Then $\psi(\bar{\rho}_f) = \bar{D}$, so $\psi(\rho_f)$ induces a map $R_{\bar{D}} \to \mathcal{O}_f$. For each prime $q \nmid Np$, we have $\mathrm{Tr}(\rho_f(\mathrm{Fr}_q)) = a_q(f)$, so $R_{\bar{D}} \to \mathcal{O}_f$ sends $\mathrm{Tr}_{D_{\bar{D}}}(\mathrm{Fr}_q)$ to $a_q(f)$.

In order to show that $R_{\bar{D}} \to \mathcal{O}_f$ factors through R_N^ϵ, we prove that $\psi(\rho_f)$ and ρ_f are US_N^ϵ by verifying local conditions, as per Definition 3.8.1.

- For $\ell \mid N$ with $\ell \neq p$, $\rho_f|_{G_\ell}$ is $\mathrm{US}_\ell^{\epsilon_\ell}$ by Lemma 2.3.1(3).
- If $p \nmid N$, or if $p \mid N$ and f is old at p, then $\rho_f|_{G_p}$ is finite-flat by Lemma 2.3.1(4a). Also, when $p \mid N$, this implies that $\rho_f|_{G_p}$ is $\mathrm{US}_p^{\epsilon_p}$ by definition if $\epsilon_p = +1$ and by Corollary 3.7.6 if $\epsilon_p = -1$.
- If f is new at p, then $\epsilon_p = -1$ and $\rho_f|_{G_p}$ is US_p^{-1} by Lemma 2.3.1(4b). □

Proof of Step 2. By construction, the map $R_N^\epsilon \to \mathbb{Z}_p \oplus \bigoplus_f \mathcal{O}_f$ sends $\mathrm{Tr}_{D_N^\epsilon}(\mathrm{Fr}_q)$ to $(1+q, \bigoplus_f a_q(f))$, which, by (2.3.4), is the image of T_q. □

Proof of Step 3. Let $\tau \in I_p$ be an element such that $\omega(\tau) \neq 1$. Let $x = \kappa_{\mathrm{cyc}}(\tau) \in \mathbb{Z}_p$, so that $1 - x \in \mathbb{Z}_p^\times$. Let $\sigma_p \in G_p$ be the element defined in §1.12 and let $z = \kappa_{\mathrm{cyc}}(\sigma_p)$. By Lemma 2.3.1(4), we see that $\mathrm{Tr}(\rho_f(\sigma_p)) = z a_p(f)^{-1} + a_p(f)$ and $\mathrm{Tr}(\rho_f(\tau\sigma_p)) = xz a_p(f)^{-1} + a_p(f)$. Hence we have

$$a_p(f) = \frac{1}{x-1}\big(x\mathrm{Tr}(\rho_f(\sigma_p)) - \mathrm{Tr}(\rho_f(\tau\sigma_p))\big) \quad \text{and}$$
$$a_p(f)^{-1} = \frac{1}{z-xz}\big(\mathrm{Tr}(\rho_f(\sigma_p)) - \mathrm{Tr}(\rho_f(\tau\sigma_p))\big).$$

We see that U_p is the image of $\frac{1}{x-1}(x\mathrm{Tr}_{D_N^\epsilon}(\sigma_p) - \mathrm{Tr}_{D_N^\epsilon}(\tau\sigma_p))$ and U_p^{-1} is the image of $\frac{1}{z-xz}(\mathrm{Tr}_{D_N^\epsilon}(\sigma_p) - \mathrm{Tr}_{D_N^\epsilon}(\tau\sigma_p))$. Since $\mathbb{T}_N^\epsilon$ is generated by T_q for $q \nmid Np$ along with $T_p = U_p + pU_p^{-1}$, we see that $R_N^\epsilon \to \mathbb{T}_N^\epsilon$ is surjective. □

4.2. **Computation of $(R_N^\epsilon)^{\mathrm{red}}$.** In this section, we will frequently make use of the elements σ_i and γ_i defined in §1.12. We denote by $M^{p\text{-part}}$ the maximal p-primary quotient of a finite abelian group M.

Consider the group $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})^{p\text{-part}}$. We have isomorphisms

$$\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})^{p\text{-part}} \xrightarrow{\sim} \prod_{i=0}^{r} \mathrm{Gal}(\mathbb{Q}(\zeta_{\ell_i})/\mathbb{Q})^{p\text{-part}} \xrightarrow{\sim} \prod_{i=0}^{r} \mathbb{Z}_p/(\ell_i - 1)\mathbb{Z}_p.$$

Since $\mathbb{Q}(\zeta_{\ell_i})/\mathbb{Q}$ is totally ramified at ℓ_i, we can and do choose the second isomorphism so that the image of γ_i is $(0, \dots, 0, 1, 0, \dots, 0)$ (with 1 in the i-th factor). We define α_j^i to be the j-th factor of the image of σ_i, so that $\sigma_i \mapsto (\alpha_0^i, \alpha_1^i, \dots, \alpha_r^i)$ (we can and do assume that $\alpha_i^i = 0$).

Remark 4.2.1. Note that if $\ell_j \equiv 1 \pmod{p}$, we may choose a surjective homomorphism $\log_{\ell_j} : (\mathbb{Z}/\ell_j\mathbb{Z})^\times \twoheadrightarrow \mathbb{F}_p$ such that $\log_{\ell_j}(\ell_i) \equiv \alpha_j^i \pmod{p}$. By abuse of notation, we denote by $\log_j = \log_{\ell_j}$ a $\mathbb{F}_p$-valued character of $G_{\mathbb{Q},S}$ produced by composition with the canonical surjection $G_{\mathbb{Q},S} \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_{\ell_j})/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/\ell_j)^\times$.

This isomorphism determines an isomorphism of group rings

$$\mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})^{p\text{-part}}] \xrightarrow{\sim} \mathbb{Z}_p\left[\prod_{i=0}^{r} \mathbb{Z}_p/(\ell_i - 1)\mathbb{Z}_p\right] \cong \mathbb{Z}_p[y_0, \dots, y_r]/(y_i^{p^{v_i}} - 1)$$

where $v_i = v_p(\ell_i - 1)$, and where the second isomorphism sends y_i to the group-like element $(0, \dots, 0, 1, 0, \dots, 0)$ (with 1 in the i-th factor). Let

$$\langle - \rangle : G_{\mathbb{Q},S} \to (\mathbb{Z}_p[y_0, \dots, y_r]/(y_i^{p^{v_i}} - 1))^\times$$

be the character obtained by the quotient $G_{\mathbb{Q},S} \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})^{p\text{-part}}$ followed by this isomorphism. Note that

$$\langle \gamma_i \rangle = y_i, \qquad \langle \sigma_i \rangle = \prod_{j=0}^{r} y_j^{\alpha_j^i}.$$

Let $R^{\mathrm{red}}_{\mathrm{flat}}(\kappa_{\mathrm{cyc}})$ (resp. $R^{\mathrm{red}}_{\mathrm{ord}}(\kappa_{\mathrm{cyc}})$) be the quotient of the finite-flat global deformation ring R_{flat} (resp. ordinary global deformation ring R_{ord}) defined in §3.9.1 (resp. §3.9.2) by the ideal generated by the reducibility ideal along with $\{D_{\bar{D}}(\gamma) - \kappa_{\mathrm{cyc}}(\gamma) : \gamma \in G_{\mathbb{Q},S}\}$. That is, we are insisting that the determinant is κ_{cyc}.

Lemma 4.2.2. *The surjection $R_{\mathrm{ord}} \twoheadrightarrow R_{\mathrm{flat}}$ induces an isomorphism $R^{\mathrm{red}}_{\mathrm{ord}}(\kappa_{\mathrm{cyc}}) \xrightarrow{\sim} R^{\mathrm{red}}_{\mathrm{flat}}(\kappa_{\mathrm{cyc}})$. Moreover, they are both isomorphic as rings to*

$$\mathbb{Z}_p[y_0, \dots, y_r]/(y_i^{p^{v_i}} - 1)$$

and the universal reducible pseudorepresentation pulls back to $D^{\mathrm{red}} = \psi(\kappa_{\mathrm{cyc}}\langle - \rangle^{-1} \oplus \langle - \rangle)$ via these isomorphisms.

Proof. The quotient map $R_{\mathrm{ord}} \twoheadrightarrow R_{\mathrm{flat}}$ comes from the first part of Corollary 3.7.6, and the two rings differ only in the local condition at p. After imposing the reducibility and determinant conditions, the universal pseudodeformations both have the form $\psi(\kappa_{\mathrm{cyc}}\chi^{-1} \oplus \chi)$ for a character χ that deforms the trivial character. By the

latter parts of the corollary, the finite-flat and ordinary conditions on such pseudo-deformations are identical. The last statement is proven just as in [WWE20, Lem. 5.1.1]. □

Let $Y_i = y_i - 1$.

Lemma 4.2.3. *There is an isomorphism*

$$(R_N^\epsilon)^{\mathrm{red}} \cong \mathbb{Z}_p[Y_0, \dots, Y_r]/\mathfrak{a}$$

where $\mathfrak{a}$ *is the ideal generated by the elements*

$$Y_i^2, (\ell_i - 1)Y_i, (\epsilon_i + 1)Y_i, Y_i \left(\prod_{j=0}^{r} (1 - \tilde{\alpha}_i^j Y_j) - 1 \right),$$

for $i = 0, \dots, r$*, where* $\tilde{\alpha}_i^j \in \mathbb{Z}_p$ *is any lift of* $\alpha_i^j \in \mathbb{Z}_p/(\ell_j - 1)\mathbb{Z}_p$ *(note that* $\mathfrak{a}$ *is independent of the choice of this lift).*

Proof. We consider $(E_N^\epsilon)^{\mathrm{red}} = E_N^\epsilon \otimes_{R_N^\epsilon} (R_N^\epsilon)^{\mathrm{red}}$. We write the base-change of ρ_N^ϵ to this algebra as ρ^{red}, for simplicity. Write $\overline{\langle - \rangle} : G_{\mathbb{Q},S} \to ((R_N^\epsilon)^{\mathrm{red}})^\times$ for the composite of $\langle - \rangle$ with the quotient $R^{\mathrm{red}}_{\mathrm{flat}}(\kappa_{\mathrm{cyc}}) \to (R_N^\epsilon)^{\mathrm{red}}$, which exists by Proposition 3.8.3. (We use $R^{\mathrm{red}}_{\mathrm{flat}}(\kappa_{\mathrm{cyc}})$ even in the ordinary case, in light of Lemma 4.2.2.)

First we show that the map $R^{\mathrm{red}}_{\mathrm{flat}}(\kappa_{\mathrm{cyc}}) \to (R_N^\epsilon)^{\mathrm{red}}$ factors through $\mathbb{Z}_p[Y_0, \dots, Y_r]/\mathfrak{a}$. We can write ρ^{red} in GMA notation as

$$\rho^{\mathrm{red}} = \begin{pmatrix} \kappa_{\mathrm{cyc}} \overline{\langle - \rangle}^{-1} & * \\ * & \overline{\langle - \rangle} \end{pmatrix}.$$

Since $V^{\epsilon_i}_{\rho^{\mathrm{red}}}(\gamma_i, \gamma_i) = (\rho^{\mathrm{red}}(\gamma_i) - 1)^2 = 0$ in $(E_N^\epsilon)^{\mathrm{red}}$, we see that $Y_i^2 = 0$ in $(R_N^\epsilon)^{\mathrm{red}}$. Since $(1 + Y_i)^{p^{v_i}} - 1 = 0$, this implies that $p^{v_i} Y_i = 0$ in $(R_N^\epsilon)^{\mathrm{red}}$. Moreover, by Lemma 3.4.5, if $\epsilon_i = +1$ and $v_i > 0$, then $\rho^{\mathrm{red}}(\gamma_i) = 1$; for such i, this implies that $Y_i = 0$ in $(R_N^\epsilon)^{\mathrm{red}}$. We can rephrase this as $(\epsilon_i + 1)Y_i = 0$ for all i.

From now on, consider i such that $\epsilon_i = -1$. Already, we see that

$$\overline{\langle \sigma_i \rangle} = \prod_{j=0}^{r} y_j^{\alpha_j^i} = \prod_{j=0}^{r} (1 + \tilde{\alpha}_j^i Y_j)$$

Since $V^{\epsilon_i}_{\rho^{\mathrm{red}}}(\gamma_i, \sigma_i) = (\rho^{\mathrm{red}}(\gamma_i) - 1)(\rho^{\mathrm{red}}(\sigma_i) - 1) = 0$ in $(E_N^\epsilon)^{\mathrm{red}}$, we obtain

$$(\overline{\langle \gamma_i \rangle}^{-1} - 1)(\ell_i \overline{\langle \sigma_i \rangle}^{-1} - 1) = 0, \quad (\overline{\langle \gamma_i \rangle} - 1)(\overline{\langle \sigma_i \rangle} - 1) = 0.$$

These imply

$$0 = Y_i \left(\prod_{j=0}^{r} (1 - \tilde{\alpha}_i^j Y_j) - 1 \right) = Y_i \left(\prod_{j=0}^{r} (1 + \tilde{\alpha}_i^j Y_j) - 1 \right).$$

However, this last equation is redundant because

$$\left(- \prod_{j=0}^{r} (1 + \tilde{\alpha}_i^j Y_j) \right) \left(\prod_{j=0}^{r} (1 - \tilde{\alpha}_i^j Y_j) - 1 \right) \equiv \left(\prod_{j=0}^{r} (1 + \tilde{\alpha}_i^j Y_j) - 1 \right) \pmod{Y_0^2, \dots, Y_r^2}.$$

This shows that $R^{\mathrm{red}}_{\mathrm{flat}}(\kappa_{\mathrm{cyc}}) \to (R^{\epsilon}_N)^{\mathrm{red}}$ factors through $\mathbb{Z}_p[Y_0,\dots,Y_r]/\mathfrak{a}$. It remains to verify that the pseudorepresentation $D : G_{\mathbb{Q},S} \to \mathbb{Z}_p[Y_0,\dots,Y_r]/\mathfrak{a}$ defined by $\psi(\kappa_{\mathrm{cyc}}\overline{\langle - \rangle}^{-1} \oplus \overline{\langle - \rangle})$ is US^{ϵ}_N. This is checked easily. □

5. The case $\epsilon = (-1, 1, 1, \dots, 1)$

In this section, we consider the case where $\epsilon_0 = -1$ and $\epsilon_i = 1$ for $0 < i \leq r$. Without loss of generality, we can and do, for this section, assume that the primes $\{\ell_i\}_{i=0}^r$ are ordered so that $\ell_i \equiv -1 \pmod{p}$ for $i = 1, \dots, s$ and $\ell_i \not\equiv -1 \pmod{p}$ for $s < i \leq r$. Here s is an integer, $0 \leq s \leq r$. The most interesting case is $s = r$, and, in fact, we immediately reduce to this case.

5.1. **Reduction to the case $s = r$.** Let $N(s) = \prod_{i=0}^{s} \ell_i$ and $\epsilon(s) \in \{\pm 1\}^{s+1}$ be defined by $\epsilon(s)_0 = -1$ and $\epsilon(s)_i = 1$ for $0 < i \leq s$. There is a natural map $\mathbb{T}^{\epsilon}_N \twoheadrightarrow \mathbb{T}^{\epsilon(s)}_{N(s)}$ by restricting to the space of forms that are old at ℓ_i for $s < i \leq r$. There is also a natural surjection $R^{\epsilon}_N \twoheadrightarrow R^{\epsilon(s)}_{N(s)}$, since $\rho^{\epsilon(s)}_{N(s)}$ is unramified (resp. finite-flat) at ℓ_i when $\ell_i \neq p$ (resp. $\ell_i = p$) and $s < i \leq r$.

Lemma 5.1.1. *The natural map $R^{\epsilon}_N \twoheadrightarrow R^{\epsilon(s)}_{N(s)}$ is an isomorphism. Moreover, if the map $R^{\epsilon(s)}_{N(s)} \twoheadrightarrow \mathbb{T}^{\epsilon(s)}_{N(s)}$ is an isomorphism, then the surjections $R^{\epsilon}_N \twoheadrightarrow \mathbb{T}^{\epsilon}_N$ and $\mathbb{T}^{\epsilon}_N \twoheadrightarrow \mathbb{T}^{\epsilon(s)}_{N(s)}$ of Proposition 4.1.1 are isomorphisms.*

Proof. The isomorphy of $R^{\epsilon}_N \twoheadrightarrow R^{\epsilon(s)}_{N(s)}$ can be rephrased as saying that, for all $s < i \leq r$, ρ^{ϵ}_N is unramified (resp. finite-flat) at ℓ_i if $\ell_i \neq p$ (resp. if $\ell_i = p$). This follows from Lemma 3.4.5 and §3.6. For the second statement, consider the commutative diagram of surjective ring homomorphisms

$$\begin{array}{ccc} R^{\epsilon}_N & \longrightarrow & \mathbb{T}^{\epsilon}_N \\ \downarrow \wr & & \downarrow \\ R^{\epsilon(s)}_{N(s)} & \longrightarrow & \mathbb{T}^{\epsilon(s)}_{N(s)}. \end{array}$$

□

5.2. **The case $s = r$.** Now we assume that $s = r$ (i.e. that $\ell_i \equiv -1 \pmod{p}$ for $i = 1, \dots, r$). We write $J^{\min} \subset R^{\epsilon}_N$ for the augmentation ideal, and $J^{\mathrm{red}} = \ker(R^{\epsilon}_N \twoheadrightarrow (R^{\epsilon}_N)^{\mathrm{red}})$. We have the following consequence of Wiles's numerical criterion [Wil95, Appendix].

Proposition 5.2.1. *The surjection $R^{\epsilon}_N \twoheadrightarrow \mathbb{T}^{\epsilon}_N$ is a isomorphism of complete intersection rings if and only if*

$$\#J^{\min}/{J^{\min}}^2 \leq p^{v_p(\ell_0 - 1)} \cdot \prod_{i=1}^{r} p^{v_p(\ell_i + 1)}.$$

If this is the case, then equality holds.

Proof. The surjection comes from Proposition 4.1.1. Note that

$$p^{v_p(\ell_0 - 1)} \cdot \prod_{i=1}^{r} p^{v_p(\ell_i + 1)} = \#\mathbb{Z}_p/a_0(E^{\epsilon})\mathbb{Z}_p.$$

The proposition follows from Theorem 2.2.1 and the numerical criterion, as in [WWE20, Thm. 7.1.1]. □

Lemma 5.2.2. *There is an isomorphism*

$$J^{\min}/J^{\mathrm{red}} \cong \mathbb{Z}_p/(\ell_0-1)\mathbb{Z}_p$$

sending $d_{\gamma_0}-1$ *to* 1, *and* ${J^{\min}}^2 \subset J^{\mathrm{red}}$.

Proof. By Lemma 4.2.3, we have

$$(R_N^\epsilon)^{\mathrm{red}} = \mathbb{Z}_p[Y_0]/((\ell_0-1)Y_0, Y_0^2),$$

and we can easily see that $d_{\gamma_0}-1$ maps to Y_0 and generates the image of $J^{\min}$. Since $Y_0^2=0$, we have the second statement. □

Lemma 5.2.3. *There is a surjection*

$$\mathbb{Z}_p/(\ell_0-1)\mathbb{Z}_p \oplus \left(\bigoplus_{i=1}^r \mathbb{Z}_p/(\ell_i+1)\mathbb{Z}_p\right) \twoheadrightarrow J^{\mathrm{red}}/J^{\min}J^{\mathrm{red}}$$

given by $e_i \mapsto b_{\gamma_0}c_{\gamma_i}$.

Proof. By Lemma 3.9.8, we have surjections

$$\mathbb{Z}_p \twoheadrightarrow B_N^{\epsilon,\min}, \quad 1 \mapsto b_{\gamma_0}$$

and

$$\mathbb{Z}_p/(\ell_0-1)\mathbb{Z}_p \oplus \left(\bigoplus_{i=1}^r \mathbb{Z}_p/(\ell_i+1)\mathbb{Z}_p\right) \twoheadrightarrow C_N^{\epsilon,\min}, \quad e_i \mapsto c_{\gamma_i}.$$

By [BC09, Prop. 1.5.1], in any A-GMA $E = \left(\begin{smallmatrix} A & B \\ C & A \end{smallmatrix}\right)$, the structure map $B\otimes_A C \to A$ has image equal to the reducibility ideal of E. Applying this to the R_N^ϵ-GMA E_N^ϵ of (3.9.1) we have an R_N^ϵ-module surjection $B_N^\epsilon \otimes_{R_N^\epsilon} C_N^\epsilon \twoheadrightarrow J^{\mathrm{red}}$. Tensoring this by $R_N^\epsilon/J^{\min} = \mathbb{Z}_p$, we have a surjection

$$B_N^{\epsilon,\min} \otimes_{\mathbb{Z}_p} C_N^{\epsilon,\min} \twoheadrightarrow J^{\mathrm{red}}/J^{\min}J^{\mathrm{red}}, \quad b\otimes c \mapsto bc. \tag{5.2.4}$$

Combining these, we have the lemma. □

Lemma 5.2.5. *The element* $b_{\gamma_0}c_{\gamma_0} \in R_N^\epsilon$ *is in* ${J^{\min}}^2$.

Proof. Since $V^{\epsilon_0}_{\rho_N^\epsilon}(\gamma_0,\gamma_0) = (\rho_N^\epsilon(\gamma_0)-1)^2 = 0$, we see that $(a_{\gamma_0}-1)^2 + b_{\gamma_0}c_{\gamma_0} = 0$. Since $a_{\gamma_0}-1 \in J^{\min}$, we have the lemma. □

We have arrived at the main theorem.

Theorem 5.2.6. *Let* $N = \ell_0\ell_1\cdots\ell_r$ *and* $\epsilon = (-1,1,\dots,1)$. *Then the map* $R_N^\epsilon \twoheadrightarrow \mathbb{T}_N^\epsilon$ *is a isomorphism of augmented* $\mathbb{Z}_p$*-algebras, and both rings are complete intersection. The ideal* $J^{\min}$ *is generated by the elements* $b_{\gamma_0}c_{\gamma_i}$ *for* $i=1,\dots,r$ *together with* $d_{\gamma_0}-1$. *There is an exact sequence*

$$0 \to \bigoplus_{i=1}^r \mathbb{Z}_p/(\ell_i+1)\mathbb{Z}_p \to I^\epsilon/{I^\epsilon}^2 \to \mathbb{Z}_p/(\ell_0-1)\mathbb{Z}_p \to 0. \tag{5.2.7}$$

Proof. By Lemma 5.2.2, there is an exact sequence

$$0 \to J^{\mathrm{red}}/{J^{\min}}^2 \to J^{\min}/{J^{\min}}^2 \to \mathbb{Z}_p/(\ell_0-1)\mathbb{Z}_p \to 0 \tag{5.2.8}$$

Combining Lemmas 5.2.3 and 5.2.5, we see that there is a surjection

$$\bigoplus_{i=1}^r \mathbb{Z}_p/(\ell_i+1)\mathbb{Z}_p \twoheadrightarrow J^{\mathrm{red}}/{J^{\min}}^2 \tag{5.2.9}$$

given by $e_i \mapsto b_{\gamma_0} c_{\gamma_i}$. This shows that

$$\#J^{\min}/{J^{\min}}^2 \leq p^{v_p(\ell_0-1)} \cdot \prod_{i=1}^{r} p^{v_p(\ell_i+1)}.$$

By Proposition 5.2.1, this shows that $R_N^\epsilon \twoheadrightarrow \mathbb{T}_N^\epsilon$ is an isomorphism of complete intersection rings, and that this inequality is actually equality. This implies that (5.2.9) is an isomorphism. Using Lemma 5.2.2 and Nakayama's lemma, this shows that $J^{\min}$ is generated by the stated elements. Since $J^{\min}$ maps isomorphically onto I^ϵ, the desired sequence follows from (5.2.8). □

6. The case $\epsilon = (-1,-1)$

In this section, we assume that $r = 1$ and also that $\epsilon = (-1,-1)$.

6.1. **No interesting primes.** If $\ell_i \not\equiv 1 \pmod{p}$ for $i = 0, 1$, then there are no cusp forms congruent to the Eisenstein series.

Theorem 6.1.1. *If $\ell_i \not\equiv 1 \pmod{p}$ for $i = 0, 1$, then $\mathbb{T}_N^\epsilon = \mathbb{Z}_p$ and $\mathbb{T}_N^{\epsilon,0} = 0$.*

Proof. It is enough to show that $R_N^\epsilon = \mathbb{Z}_p$. By Lemma 4.2.3, we have $R_N^{\epsilon,\mathrm{red}} = \mathbb{Z}_p$ and by Lemma 3.9.8 we have $C_N^\epsilon = 0$, so $J^{\mathrm{red}} = 0$. This implies $R_N^\epsilon = \mathbb{Z}_p$. □

6.2. **Generators of B_N^ϵ.** Since nothing interesting happens if there are no interesting primes, we now assume that $\ell_0 \equiv 1 \pmod{p}$. We emphasize that, in this section, we do not assume that $\ell_1 \neq p$. Recall the notation $a_\tau, b_\tau, c_\tau, d_\tau$ for $\tau \in G_{\mathbb{Q},S}$ from (3.9.1) and the elements $\gamma_i, \sigma_i \in G_{\mathbb{Q},S}$ from §1.12.

Lemma 6.2.1. *Assume that ℓ_1 is not a p-th power modulo ℓ_0. Then the subset $\{b_{\gamma_0}, b_{\sigma_0}\} \subset B_N^\epsilon$ generates B_N^ϵ as a R_N^ϵ-module.*

Proof. We give the proof in the case $\ell_1 = p$; the case $\ell_1 \neq p$ is exactly analogous, changing 'ordinary' to 'finite-flat' everywhere. Because $B_{\mathrm{ord}}^{\min}$ surjects onto B_N^ϵ and by Nakayama's lemma, it is enough to show that the images $\bar{b}_{\mathrm{ord},\gamma_0}, \bar{b}_{\mathrm{ord},\sigma_0}$ of $b_{\mathrm{ord},\gamma_0}, b_{\mathrm{ord},\sigma_0}$ in $B_{\mathrm{ord}}^{\min}/pB_{\mathrm{ord}}^{\min}$ generate $B_{\mathrm{ord}}^{\min}/pB_{\mathrm{ord}}^{\min}$.

Using b_i, $\tilde{b}_i$ defined in §3.10 and the lemmas there, we know that $\{\bar{b}_{\mathrm{ord},\gamma_0}, \bar{b}_{\mathrm{ord},\gamma_1}\}$ is a basis for $B_{\mathrm{ord}}^{\min}/pB_{\mathrm{ord}}^{\min}$ and $b_1(\bar{b}_{\mathrm{ord},\gamma_j}) = \partial_{1j}$ for $j = 0, 1$. Hence it is enough to show that $b_1(\bar{b}_{\mathrm{ord},\sigma_0}) \neq 0$. As in the proof of Lemma 3.10.3, the fact that $\omega(\sigma_0) = 1$ implies that $b_1(\bar{b}_{\mathrm{ord},\sigma_0}) = \tilde{b}_1(\sigma_0)$. Because ℓ_1 is not a p-th power modulo ℓ_0, class field theory implies that $\tilde{b}_1(\sigma_0) \neq 0$. □

Proposition 6.2.2. *Assume that ℓ_1 is not a p-th power modulo ℓ_0. Then*

$$b_{\gamma_0} c_{\gamma_0},\ b_{\gamma_1} c_{\gamma_1},\ b_{\gamma_1} c_{\gamma_0} \in {J^{\min}}^2.$$

If, in addition, $\ell_1 \equiv 1 \pmod{p}$ and ℓ_0 is not a p-th power modulo ℓ_1, then $b_{\gamma_0} c_{\gamma_1} \in {J^{\min}}^2$ as well.

Proof. The proof for $b_{\gamma_0} c_{\gamma_0}, b_{\gamma_1} c_{\gamma_1}$ is just as in Lemma 5.2.5. If we prove that $b_{\gamma_1} c_{\gamma_0} \in {J^{\min}}^2$, then we get $b_{\gamma_0} c_{\gamma_1} \in {J^{\min}}^2$ in the second statement by symmetry. So it suffices to prove $b_{\gamma_1} c_{\gamma_0} \in {J^{\min}}^2$.

Let $X = a_{\sigma_0} - \ell_0$ and $W = a_{\gamma_0} - 1$, and note that $X, W \in J^{\min}$. From the $(1,1)$-coordinate of the equation $V_{\rho_N^\epsilon}^{\epsilon_{\ell_0}}(\sigma_0, \gamma_0) = 0$ defined in (3.4.2), we see that $XW + b_{\sigma_0} c_{\gamma_0} = 0$. In particular, $b_{\sigma_0} c_{\gamma_0} \in {J^{\min}}^2$.

By Lemma 6.2.1, we know that b_{γ_1} is in the R_N^ϵ-linear span of b_{σ_0} and b_{γ_0}. Because both $b_{\sigma_0}c_{\gamma_0}$ and $b_{\gamma_0}c_{\gamma_0}$ lie in ${J^{\min}}^2$, so does $b_{\gamma_1}c_{\gamma_0}$. □

6.3. **One interesting prime.** We assume that $\ell_0 \equiv 1 \pmod p$ and $\ell_1 \not\equiv 1 \pmod p$ (including the possibility that $\ell_1 = p$). There is a natural surjective homomorphism $\mathbb{T}_N^\epsilon \twoheadrightarrow \mathbb{T}_{\ell_0}$ by restricting to forms that are old at ℓ_1.

Theorem 6.3.1. *Assume that $\ell_0 \equiv 1 \pmod p$, that $\ell_1 \not\equiv 1 \pmod p$, and that ℓ_1 is not a p-th power modulo ℓ_0. Then the natural map $\mathbb{T}_N^\epsilon \twoheadrightarrow \mathbb{T}_{\ell_0}$ is an isomorphism. In particular, I^ϵ is principal, $\mathbb{T}_N^\epsilon$ and $\mathbb{T}_N^{\epsilon,0}$ are complete intersections, and there are no newforms in $S_2(N)^\epsilon_{\mathrm{Eis}}$.*

Proof. Just as in the proof of Lemma 5.1.1, it suffices to show that the map $R_N^\epsilon \twoheadrightarrow \mathbb{T}_{\ell_0}$ is an isomorphism. By Lemma 4.2.3, there is an isomorphism

$$R_N^{\epsilon,\mathrm{red}} \cong \mathbb{Z}_p[Y_0]/(Y_0^2, (\ell_0 - 1)Y_0),$$

where the image of $J^{\min}$ is the ideal generated by Y_0. This implies that ${J^{\min}}^2 \subset J^{\mathrm{red}}$ and that there is an isomorphism

$$\mathbb{Z}_p/(\ell_0 - 1)\mathbb{Z}_p \xrightarrow{\sim} J^{\min}/J^{\mathrm{red}}, \quad 1 \mapsto Y_0.$$

On the other hand, we know that J^{red} is generated by the set $\{b_{\gamma_0}c_{\gamma_0}, b_{\gamma_1}c_{\gamma_0}\}$ by Lemma 3.9.8 and the surjection (5.2.4). By Proposition 6.2.2, we see that this set is contained in ${J^{\min}}^2$. Hence $J^{\mathrm{red}} \subset {J^{\min}}^2$, and so $J^{\mathrm{red}} = {J^{\min}}^2$.

Now we have $\#J^{\min}/{J^{\min}}^2 = p^{v_p(\ell_0-1)}$ and, by the numerical criterion (Proposition 5.2.1), $R_N^\epsilon \twoheadrightarrow \mathbb{T}_{\ell_0}$ is an isomorphism. □

Remark 6.3.2. The assumption that ℓ_1 is not a p-th power modulo ℓ_0 is necessary: see the examples in §1.10.2.

6.4. **Two interesting primes.** We consider the case $\ell_i \equiv 1 \pmod p$ for $i = 0, 1$.

Theorem 6.4.1. *Let $N = \ell_0\ell_1$ and $\epsilon = (-1, -1)$. Assume that $\ell_i \equiv 1 \pmod p$ for $i = 0, 1$ and assume that neither prime is a p-th power modulo the other. Then the map $R_N^\epsilon \twoheadrightarrow \mathbb{T}_N^\epsilon$ is an isomorphism of complete intersection rings augmented over $\mathbb{Z}_p$, and there is an isomorphism*

$$I^\epsilon/I^{\epsilon 2} \cong \mathbb{Z}_p/(\ell_0 - 1)\mathbb{Z}_p \oplus \mathbb{Z}_p/(\ell_1 - 1)\mathbb{Z}_p.$$

Proof. By Lemma 4.2.3, we see that there is an isomorphism

$$R_N^{\epsilon,\mathrm{red}} \cong \mathbb{Z}_p[Y_0, Y_1]/(Y_0^2, Y_0Y_1, Y_1^2, (\ell_0 - 1)Y_0, (\ell_1 - 1)Y_1)$$

and that the image of $J^{\min}$ is the ideal generated by (Y_0, Y_1). In particular ${J^{\min}}^2 \subset J^{\mathrm{red}}$ and

$$J^{\min}/J^{\mathrm{red}} \cong \mathbb{Z}_p/(\ell_0 - 1)\mathbb{Z}_p \oplus \mathbb{Z}_p/(\ell_1 - 1)\mathbb{Z}_p.$$

Moreover, by Proposition 6.2.2 and Lemma 3.9.8, we see that $J^{\mathrm{red}} \subset {J^{\min}}^2$ so we have

$$J^{\min}/{J^{\min}}^2 = J^{\min}/J^{\mathrm{red}} \cong \mathbb{Z}_p/(\ell_0 - 1)\mathbb{Z}_p \oplus \mathbb{Z}_p/(\ell_1 - 1)\mathbb{Z}_p.$$

In particular, $\#J^{\min}/{J^{\min}}^2 = p^{v_p(\ell_0-1)+v_p(\ell_1-1)}$.

Now the numerical criterion of Proposition 5.2.1 implies that $R_N^\epsilon \twoheadrightarrow \mathbb{T}_N^\epsilon$ is a isomorphism of complete intersection augmented $\mathbb{Z}_p$-algebras. It follows that $I^\epsilon = J^{\min}$, and so the description of $I^\epsilon/I^{\epsilon 2}$ also follows. □

Remark 6.4.2. Again, the assumptions are necessary. See the examples in §1.10.3.

Definition 6.4.3. We say there are *no newforms in* $M_2(N;\mathbb{Z}_p)^\epsilon_{\mathrm{Eis}}$ if

$$M_2(N;\mathbb{Z}_p)^\epsilon_{\mathrm{Eis}} = M_2(\ell_0;\mathbb{Z}_p)_{\mathrm{Eis}} + M_2(\ell_1;\mathbb{Z}_p)_{\mathrm{Eis}},$$

where the later are considered submodules of the former via the stabilizations in §2.1.5. Otherwise, we say there are *newforms in* $M_2(N;\mathbb{Z}_p)^\epsilon_{\mathrm{Eis}}$.

Theorem 6.4.4. *Let* $N = \ell_0\ell_1$ *and* $\epsilon = (-1,-1)$ *and assume that* $\ell_i \equiv 1 \pmod p$ *for* $i = 0, 1$. *If there are no newforms in* $M_2(N;\mathbb{Z}_p)^\epsilon_{\mathrm{Eis}}$, *then* $\mathbb{T}^\epsilon_N$ *is not Gorenstein. In particular, if neither prime* ℓ_i *is a* p*-th power modulo the other, then there are newforms in* $M_2(N;\mathbb{Z}_p)^\epsilon_{\mathrm{Eis}}$.

Proof. The second statement follows from the first statement by Theorem 6.4.1. Now assume that there are no newforms in $M_2(N;\mathbb{Z}_p)^\epsilon_{\mathrm{Eis}}$. We count that

$$\mathrm{rank}_{\mathbb{Z}_p}(M_2(N;\mathbb{Z}_p)^\epsilon_{\mathrm{Eis}}) = \mathrm{rank}_{\mathbb{Z}_p}(M_2(\ell_0;\mathbb{Z}_p)_{\mathrm{Eis}}) + \mathrm{rank}_{\mathbb{Z}_p}(M_2(\ell_1;\mathbb{Z}_p)_{\mathrm{Eis}}) - 1$$

(by Lemma 2.3.1, for example).

We claim that, under this assumption, we have an isomorphism $\mathbb{T}^\epsilon_N \xrightarrow{\sim} \mathbb{T}_{\ell_0} \times_{\mathbb{Z}_p} \mathbb{T}_{\ell_1}$. To see this, consider the commutative diagram of free $\mathbb{Z}_p$-modules, where the right square consists of canonical surjective homomorphisms of commutative $\mathbb{Z}_p$-algebras and the rows are exact:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathfrak{a}_1 & \longrightarrow & \mathbb{T}^\epsilon_N & \twoheadrightarrow & \mathbb{T}_{\ell_1} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & I_0 & \longrightarrow & \mathbb{T}_{\ell_0} & \twoheadrightarrow & \mathbb{Z}_p & \longrightarrow & 0. \end{array}$$

By Lemma C.2.1, it is enough to show that $\mathfrak{a}_1 \to I_0$ is an isomorphism. From this diagram and the above rank count, we see that $\mathrm{rank}_{\mathbb{Z}_p}(\mathfrak{a}_1) = \mathrm{rank}_{\mathbb{Z}_p}(I_0)$. Thus it suffices to show that the $\mathbb{Z}_p$-dual map is surjective. By duality (2.1.2), the dual map is identified with the map

$$M_2(\ell_0;\mathbb{Z}_p)_{\mathrm{Eis}}/\mathbb{Z}_p E_{2,\ell_0} \to M_2(N;\mathbb{Z}_p)^\epsilon_{\mathrm{Eis}}/M_2(\ell_1;\mathbb{Z}_p)_{\mathrm{Eis}}$$

induced by stabilization, which is surjective by our assumption $M_2(N;\mathbb{Z}_p)^\epsilon_{\mathrm{Eis}} = M_2(\ell_0;\mathbb{Z}_p)_{\mathrm{Eis}} + M_2(\ell_1;\mathbb{Z}_p)_{\mathrm{Eis}}$. This proves that $\mathfrak{a}_1 \to I_0$ is an isomorphism.

Using this isomorphism $\mathbb{T}^\epsilon_N \xrightarrow{\sim} \mathbb{T}_{\ell_0} \times_{\mathbb{Z}_p} \mathbb{T}_{\ell_1}$ and Mazur's results (§1.1) on the structure of $\mathbb{T}_{\ell_i}$, it is then a simple computation to see that

$$\mathbb{T}^\epsilon_N/p\mathbb{T}^\epsilon_N \cong \mathbb{F}_p[y_0,y_1]/(y_0^{e_0+1}, y_1^{e_1+1}, y_0y_1), \quad \text{for some } e_0, e_1 > 0.$$

Thus $\mathrm{Soc}(\mathbb{T}^\epsilon_N/p\mathbb{T}^\epsilon_N) = \mathbb{F}_p y_0^{e_0} \oplus \mathbb{F}_p y_1^{e_1}$. By Lemma C.1.3, $\mathbb{T}^\epsilon_N$ is not Gorenstein. □

7. Generators of the Eisenstein ideal

In this section, we prove Part (4) of Theorem 1.5.1 about the number of generators of the Eisenstein ideal, as well as Theorems 1.7.5 and 1.7.1, about specific generators.

7.1. **Determining the number of generators of I^ϵ when $\varepsilon = (-1, 1, \dots, 1)$.** In this subsection, we prove Part (4) of Theorem 1.5.1. Assume we are in the setting of that theorem, so $\epsilon = (-1, 1, \dots, 1)$. Recall the fields K_i of Definition 3.10.4.

Theorem 7.1.1. *Assume that $\ell_i \equiv -1 \pmod p$ for $i = 1, \dots, r$. The minimal number of generators of I^ϵ is $r + \delta$ where*

$$\delta = \begin{cases} 1 & \text{if } \ell_0 \text{ splits completely in } K_i \text{ for } i = 1, \dots, r \\ 0 & \text{otherwise.} \end{cases} \tag{7.1.2}$$

This immediately implies Part (4) of Theorem 1.5.1 by Lemma 5.1.1. For the rest of §7.1, we assume that $r > 0$ and $\ell_i \equiv -1 \pmod p$ for $i = 1, \dots, r$, and we use δ to refer to the integer (7.1.2).

7.1.1. *Outline of the proof.* By Theorem 5.2.6, we see that $R^\epsilon_N \to \mathbb{T}^\epsilon_N$ is an isomorphism and that it induces an isomorphism $J^{\min} \xrightarrow{\sim} I^\epsilon$. Hence we are reduced to computing the number of generators of $J^{\min}$. Moreover, (5.2.7) implies that this number of generators is either r or $r + 1$, and we are reduced to showing that it is $r + 1$ if and only if the splitting condition in (7.1.2) holds.

We do some initial reductions in §7.1.2. We use class field theory to show that the splitting condition in (7.1.2) is equivalent to the vanishing of certain cup products in Galois cohomology. The number of generators of $J^{\min}$ is the same as the dimension of the tangent space of $R^\epsilon_N/pR^\epsilon_N$, and this is related to cup products. Explicitly, Bellaïche proved in [Bel12, Thm. A] that the the tangent space $\mathfrak{t}_{\bar D}$ of $R_{\bar D}/pR_{\bar D}$ (where $R_{\bar D}$ is the unrestricted pseudodeformation ring of $\bar D$ – without any local conditions) fits in an exact sequence

$$\mathfrak{t}_{\bar D} \xrightarrow{\iota} H^1(\mathbb{F}_p(1)) \otimes_{\mathbb{F}_p} H^1(\mathbb{F}_p(-1)) \xrightarrow{b' \otimes c' \mapsto (b' \cup c', c' \cup b')} H^2(\mathbb{F}_p) \oplus H^2(\mathbb{F}_p).$$

In other words, the tangent space is larger as more cup products vanish. We show that this immediately implies one implication of Theorem 7.1.1: if the number of generators of $J^{\min}$ is $r + 1$, this forces the tangent space of $\mathfrak{t}_{\bar D}$ to be large, which can only happen if the cup products vanish.

The other implication is more delicate. If we assume that the cup products vanish, then Bellaïche's theory only tells us that the tangent space of the unrestricted deformation ring is large. We have to show that these first-order deformations can be made to satisfy the right local conditions at primes dividing Np. To do this, we construct in §7.1.3 a particular GMA representation ρ_M that realizes Bellaïche's tangent space computation, and show that ρ_M satisfies the US^ϵ_N local conditions. In §7.1.4, we show that ρ_M indeed realizes the tangent space of $R^\epsilon_N/pR^\epsilon_N$, and this completes the proof.

7.1.2. *First reductions.* Note that because $\mathfrak{m} = J^{\min} + pR^\epsilon_N \subset R^\epsilon_N$ is the maximal ideal, we have

$$J^{\min}/\mathfrak{m}J^{\min} \cong \mathfrak{m}/(p, \mathfrak{m}^2).$$

By Nakayama's lemma, the minimal cardinality of a generating subset of $J^{\min}$ is $\dim_{\mathbb{F}_p} \mathfrak{m}/(p, \mathfrak{m}^2)$. By Theorem 5.2.6 we have $I^\epsilon \cong J^{\min}$, so, to prove Theorem 7.1.1, it suffices to show that $\dim_{\mathbb{F}_p} \mathfrak{m}/(p, \mathfrak{m}^2) = r + \delta$, and this is what we will prove.

Recall the notation of §3.10, in particular, the class $b_0 \in H^1(\mathbb{Z}[1/Np], \mathbb{F}_p(1))$ and the representing cocycle $\tilde b_0$, as well as the classes $c_0, \dots, c_r \in H^1_{(p)}(\mathbb{Z}[1/Np], \mathbb{F}_p(-1))$

(note that c_0 is only defined if $\ell_0 \equiv \pm 1 \pmod{p}$). The starting point is the following proposition, which is proven in Appendix B.

Proposition 7.1.3. *Let $i \in \{1, \dots, r\}$. Then ℓ_0 splits completely in K_i if and only if $\ell_0 \equiv 1 \pmod{p}$ and $b_0 \cup c_i$ vanishes in $H^2(\mathbb{Z}[1/Np], \mathbb{F}_p)$.*

We can now prove one implication of Theorem 7.1.1.

Proposition 7.1.4. *Suppose that the minimal number of generators of I^ϵ is $r+1$. Then $\delta = 1$.*

Proof. By Theorem 5.2.6, we see that minimal number of generators of I^ϵ is $r+1$ if and only if $\ell_0 \equiv 1 \pmod{p}$ and the images of the elements $b_{\gamma_0} c_{\gamma_i}$ for $i = 1, \dots, r$ in $\mathfrak{m}/(p, \mathfrak{m}^2)$ are linearly independent. In particular, for each i, the image of $b_{\gamma_0} c_{\gamma_i}$ in $\mathfrak{m}/(p, \mathfrak{m}^2)$ is non-zero. Fix such an i, and let (writing $\mathbb{F}_p[\varepsilon]$ for $\mathbb{F}_p[\varepsilon]/(\varepsilon^2)$)

$$\alpha : R_N^\epsilon/(p, \mathfrak{m}^2) \to \mathbb{F}_p[\varepsilon]$$

be a ring homomorphism sending $b_{\gamma_0} c_{\gamma_i}$ to ε.

Let $E = \left(\begin{smallmatrix} \mathbb{F}_p[\varepsilon] & \mathbb{F}_p \\ \mathbb{F}_p & \mathbb{F}_p[\varepsilon] \end{smallmatrix}\right)$ be the $\mathbb{F}_p[\varepsilon]$-GMA with data $(\mathbb{F}_p, \mathbb{F}_p, m)$ where $m : \mathbb{F}_p \times \mathbb{F}_p \to \mathbb{F}_p[\varepsilon]$ is the map $(x, y) \mapsto xy\varepsilon$. By Lemma 3.10.3, we have a homomorphism of GMAs $A : E_N^\epsilon \to E$ given by

$$A = \begin{pmatrix} \alpha & \tilde{b}_0 \\ \tilde{c}_i & \alpha \end{pmatrix}.$$

Let $D_A = \psi(A \circ \rho_N^\epsilon) : G_{\mathbb{Q},S} \to \mathbb{F}_p[\varepsilon]$ be the corresponding deformation of $\bar{D}$. Then D_A contributes a non-zero element to the tangent space $\mathfrak{t}_{\bar{D}}$ of $R_{\bar{D}}/pR_{\bar{D}}$. Examining [Bel12], the image of D_A under ι in the exact sequence of [Bel12, Thm. A]

$$\mathfrak{t}_{\bar{D}} \xrightarrow{\iota} H^1(\mathbb{F}_p(1)) \otimes_{\mathbb{F}_p} H^1(\mathbb{F}_p(-1)) \xrightarrow{b' \otimes c' \mapsto (b' \cup c', c' \cup b')} H^2(\mathbb{F}_p) \oplus H^2(\mathbb{F}_p)$$

is $b_0 \otimes c_i$, and hence $b_0 \cup c_i = 0$. Since this is true for all i, Proposition 7.1.3 implies that $\delta = 1$. □

The remainder of the proof of Theorem 7.1.1 relies on the following construction.

7.1.3. *Construction of a maximal first-order pseudodeformation.* Let H be the kernel of the map

$$H^1_{(p)}(\mathbb{Z}[1/Np], \mathbb{F}_p(-1)) \longrightarrow H^2(\mathbb{Z}[1/Np], \mathbb{F}_p) \oplus H^1(I_{\ell_0}, \mathbb{F}_p(-1)),$$
$$x \mapsto (b_0 \cup x,\ x|_{I_{\ell_0}}).$$

Lemma 7.1.5. *If $\ell_0 \equiv 1 \pmod{p}$ and $\delta = 0$, then $b_0 \cup c_i \neq 0$ for some i. In that case, there are elements $\alpha_j \in \mathbb{F}_p$ such that the set $\{c_j - \alpha_j c_i\}$ for $j \in \{1, \dots, r\} \setminus \{i\}$ is a basis for H. Otherwise, the set $\{c_1, \dots, c_r\}$ is a basis for H.*

Proof. The first statement follows from Proposition 7.1.3. Recall that c_i is ramified at ℓ_0 if and only if $i = 0$, so H is contained in the span of the linearly independent set $\{c_1, \dots, c_r\}$. Since

$$\dim_{\mathbb{F}_p} H^2(\mathbb{Z}[1/Np], \mathbb{F}_p) = \begin{cases} 1 & \text{when } \ell_0 \equiv 1 \pmod{p} \\ 0 & \text{when } \ell_0 \not\equiv 1 \pmod{p}, \end{cases}$$

the lemma follows. □

Lemma 7.1.6. *If $\ell_0 \neq p$ and $h \in H$, the image $h|_{G_{\ell_0}} \in H^1(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(-1))$ is zero.*

Proof. If $\ell_0 \not\equiv \pm 1 \pmod{p}$, then $H^1(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(-1)) = 0$. If $\ell_0 \equiv -1 \pmod{p}$, then $H^1(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(-1)) = H^1(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(1))$, and so this follows from Lemma B.1.1. Now assume $\ell_0 \equiv 1 \pmod{p}$. Then, since $h \cup b_0 = 0$ in $H^2(\mathbb{Z}[1/Np], \mathbb{F}_p)$, b_0 is ramified at ℓ_0, and h is unramified at ℓ_0, Lemma B.1.3 implies that $h|_{G_{\ell_0}} = 0$. □

Construction 7.1.7. We construct a cocycle $C : G_{\mathbb{Q},S} \to H^*(-1)$, where $H^* = \mathrm{Hom}_{\mathbb{F}_p}(H, \mathbb{F}_p)$ with trivial $G_{\mathbb{Q},S}$-action, and a cochain $F : G_{\mathbb{Q},S} \to H^*$ such that:

(1) $C|_{G_p} = 0$,
(2) if $\ell_0 \neq p$, then $C|_{G_{\ell_0}}$ is a coboundary,
(3) $dF = \tilde{b}_0 \smile C$,
(4) $F|_{I_p} = 0$,
(5) For any cocycle $\tilde{h}$ whose cohomology class h is in H, and any $\tau \in G_{\mathbb{Q},S}$ with $\omega(\tau) = 1$, we have $C(\tau)(h) = \tilde{h}(\tau)$.

Proof. For any $G_{\mathbb{Q},S}$-module X, let

$$Z^1_{(p)}(\mathbb{Z}[1/Np], X) = \{(a, x) \in Z^1(\mathbb{Z}[1/Np], X) \times X \mid a(\tau) = (\tau - 1)x,\ \forall\, \tau \in G_p\}.$$

There is a surjection $Z^1_{(p)}(\mathbb{Z}[1/Np], \mathbb{F}_p(-1)) \twoheadrightarrow H^1_{(p)}(\mathbb{Z}[1/Np], \mathbb{F}_p(-1))$ sending (a, x) to the class of a. Choose a linear section $s : H \hookrightarrow Z^1_{(p)}(\mathbb{Z}[1/Np], \mathbb{F}_p(-1))$, and write $s(h) = (s(h)_1, s(h)_2) \in Z^1(\mathbb{Z}[1/Np], \mathbb{F}_p(-1)) \times \mathbb{F}_p(-1)$.

Define an element $(C', x) \in C^1(\mathbb{Z}[1/Np], H^*(-1)) \times H^*(-1)$ by $C'(\tau)(h) = s(h)_1(\tau)$ and $x(h) = s(h)_2$ for $h \in H$. One observes $(C', x) \in Z^1_{(p)}(\mathbb{Z}[1/Np], H^*(-1))$. Then let $C = C' - dx$, so that $C|_{G_p} = 0$ and (1) holds. We also see that (5) holds, since the value $\tilde{h}(\tau)$ is independent of the choice of cocycle. Computing with dual vector spaces, it is easy to see that $b_0 \cup C = 0$ in $H^2(\mathbb{Z}[1/Np], H^*)$ and that Lemma 7.1.6 implies (2).

Finally, to see (3) and (4), let y be any cochain such that $dy = \tilde{b}_0 \smile C$. Note that the restriction map

$$H^1(\mathbb{Z}[1/Np], H^*) \to H^1(I_p, H^*)$$

is surjective, and that, since H^* has trivial action, we may and do identify a cohomology class with its representing cocycle. Since $C|_{I_p} = 0$ and $dy = \tilde{b}_0 \smile C$, we see that $y|_{I_p} \in H^1(I_p, H^*)$. Hence there is a cocycle $y' \in H^1(\mathbb{Z}[1/Np], H^*)$ with $y'|_{I_p} = y|_{I_p}$. Letting $F = y - y'$, we have $dF = dy = \tilde{b}_0 \smile C$ and $F|_{I_p} = 0$. □

Let $M = H^* \oplus \mathbb{Z}/(p, \ell_0 - 1)$, and let $\mathbb{F}_p[M]$ be the vector space $\mathbb{F}_p \oplus M$ thought of as a local $\mathbb{F}_p$-algebra with square-zero maximal ideal M. We write elements of $\mathbb{F}_p[M]$ as triples (x, y, z) with $x \in \mathbb{F}_p$, $y \in H^*$ and $z \in \mathbb{Z}/(p, \ell_0 - 1)\mathbb{Z}$.

Let E_M be the $\mathbb{F}_p[M]$-GMA given by the data $(\mathbb{F}_p, H^*, m)$ where m is the homomorphism

$$m : \mathbb{F}_p \otimes_{\mathbb{F}_p} H^* \cong H^* \xrightarrow{\sim} H^* \oplus \{0\} \subset M \hookrightarrow \mathbb{F}_p[M].$$

Let $\rho_M : G_{\mathbb{Q},S} \longrightarrow E_M^\times$ be the function

$$\rho_M(\tau) = \begin{pmatrix} \omega(\tau)(1, F(\tau), \log_{\ell_0}(\tau)) & \tilde{b}_0(\tau) \\ \omega(\tau)C(\tau) & (1, \tilde{b}_0(\tau)C(\tau) - F(\tau), -\log_{\ell_0}(\tau)) \end{pmatrix}. \tag{7.1.8}$$

Then ρ_M is a homomorphism by Construction 7.1.7. Let $D_M : G_{\mathbb{Q},S} \to \mathbb{F}_p[M]$ denote the pseudorepresentation $D_M := \psi(\rho_M)$.

Lemma 7.1.9. *ρ_M satisfies* US^ϵ_N.

Proof. As per Definition 3.8.1, we verify US_N^{ϵ} by proving that $\rho_M|_{G_p}$ is finite-flat if $\ell_0 \neq p$, and that $\rho_M|_{G_\ell}$ satisfies condition $\mathrm{US}_\ell^{\epsilon_\ell}$ for all $\ell \mid N$.

If $\ell_0 \neq p$, $\rho_M|_{G_p}$ is finite-flat: For this, we will make frequent use of the notion of a Cayley–Hamilton module, developed in [WWE19, §2.6].

Let E'_M be the $\mathbb{F}_p[M]$-sub-GMA of E_M given by $E'_M = \left(\begin{smallmatrix} \mathbb{F}_p[M] & \mathbb{F}_p \\ 0 & \mathbb{F}_p[M] \end{smallmatrix}\right)$. Since $C|_{G_p} = 0$, we see that the action of G_p on E_M via ρ_M factors through E'_M. Hence $(\rho_M|_{G_p} : G_p \to E'^{\times}_M, E'_M, D_{E'_M} : E'_M \to \mathbb{F}_p[M])$, which we denote by $\rho'_{M,p}$ for convenience, is a Cayley–Hamilton representation of G_p. Then E_M is a faithful Cayley–Hamilton module of $\rho'_{M,p}$; by [WWE19, Thm. 2.6.3], it is enough to show that $\rho'_{M,p}$ is finite-flat.

Consider the extension $\mathcal{E}_{\tilde{b}_0}$ defined by $\tilde{b}_0$:

$$0 \longrightarrow \mathbb{F}_p(1) \longrightarrow \mathcal{E}_{\tilde{b}_0} \longrightarrow \mathbb{F}_p \longrightarrow 0,$$

which is finite-flat by Kummer theory. Let $W_\omega = \mathbb{F}_p[M]$ and $W_1 = \mathbb{F}_p[M]$ with G_p acting by the characters $\omega(1, F, \log_{\ell_0})$ and $(1, -F, -\log_{\ell_0})$, respectively. Since $F|_{I_p}$ and $\log_{\ell_0}|_{I_p}$ are zero, W_ω and W_1 are finite-flat. We have exact sequences of $\mathbb{F}_p[M][G_p]$-modules

$$0 \to M(1) \to W_\omega \to \mathbb{F}_p(1) \to 0, \qquad 0 \to M \to W_1 \to \mathbb{F}_p \to 0.$$

Let $l : \mathbb{F}_p \hookrightarrow M$ be an injective linear map. This induces a injection $\mathbb{F}_p(1) \hookrightarrow W_\omega$ of $\mathbb{F}_p[M][G_p]$-modules. Taking the pushout of $\mathcal{E}_{\tilde{b}_0}$ by this injection, we obtain an exact sequence

$$0 \longrightarrow W_\omega \longrightarrow \mathcal{E}_{\tilde{b}_0,\omega} \longrightarrow \mathbb{F}_p \longrightarrow 0.$$

Pulling back this sequence by $W_1 \twoheadrightarrow \mathbb{F}_p$, we obtain an exact sequence

$$0 \longrightarrow W_\omega \longrightarrow \mathcal{E}_{\tilde{b}_0,\omega,1} \longrightarrow W_1 \longrightarrow 0.$$

Following [WWE20, App. C], we see that $\mathcal{E}_{\tilde{b}_0,\omega,1}$ is finite-flat and that there is an isomorphism $\mathcal{E}_{\tilde{b}_0,\omega,1} \cong \mathbb{F}_p[M]^{\oplus 2}$ under which the action of G_p is given by

$$\left.\begin{pmatrix} \omega(1, F, \log_{\ell_0}) & (0, \tilde{b}_0 \cdot l(1)) \\ 0 & (1, -F, -\log_{\ell_0}) \end{pmatrix}\right|_{G_p} : G_p \to \mathrm{GL}_2(\mathbb{F}_p[M]). \tag{7.1.10}$$

We now use this isomorphism $\mathcal{E}_{\tilde{b}_0,\omega,1} \cong \mathbb{F}_p[M]^{\oplus 2}$ as an identification.

We have an injective $\mathbb{F}_p[M]$-GMA homomorphism $l' : E'_M \to \mathrm{End}_{\mathbb{F}_p[M]}(\mathcal{E}_{\tilde{b}_0,\omega,1}) = M_{2\times 2}(\mathbb{F}_p[M]))$ given by

$$l' = \begin{pmatrix} \mathrm{id}_{\mathbb{F}_p[M]} & l \\ 0 & \mathrm{id}_{\mathbb{F}_p[M]} \end{pmatrix}.$$

By (7.1.10), we see that action of G_p-action on $\mathcal{E}_{\tilde{b}_0,\omega,1}$ factors through l'. In other words, $\mathcal{E}_{\tilde{b}_0,\omega,1}$ is a faithful Cayley–Hamilton module of $\rho'_{M,p}$. Since $\mathcal{E}_{\tilde{b}_0,\omega,1}$ is finite-flat, $\rho'_{M,p}$ is finite-flat by [WWE19, Thm. 2.6.3].

If $\ell_0 = p$, then $\rho_M|_{G_p}$ is ordinary: This follows from Proposition 3.7.5 and Construction 7.1.7.

If $\ell_0 \equiv 1 \pmod{p}$, then $\rho_M|_{G_{\ell_0}}$ is $\mathrm{US}_{\ell_0}^{-1}$: Since $\ell_0 \equiv 1 \pmod{p}$, $\omega|_{G_{\ell_0}} = 1$. By Construction 7.1.7, we have $C|_{G_{\ell_0}} = 0$. Then, for any $\sigma, \tau \in G_{\ell_0}$, we have

$$V_{\rho_M}^{-1}(\sigma, \tau) := (\rho_M(\sigma) - \omega(\sigma))(\rho(\tau) - 1) = \begin{pmatrix} \varepsilon_1 & \tilde{b}_0(\sigma) \\ 0 & \varepsilon_2 \end{pmatrix} \begin{pmatrix} \varepsilon_3 & \tilde{b}_0(\tau) \\ 0 & \varepsilon_4 \end{pmatrix} = 0,$$

where $\varepsilon_i \in M \subset \mathbb{F}_p[M]$.

If $\ell_0 \not\equiv 0, 1 \pmod{p}$, then $\rho_M|_{G_{\ell_0}}$ is $\mathrm{US}^{-1}_{\ell_0}$: By assumption, we have $M = H^*$ and $\log_{\ell_0} = 0$, so we write elements of $\mathbb{F}_p[M]$ as pairs (x, y) with $x \in \mathbb{F}_p$ and $y \in H^*$. Since $C|_{G_{\ell_0}}$ is a coboundary, there exists $z \in H^*$ such that $C(\tau) = (\omega^{-1}(\tau) - 1)z$ for all $\tau \in G_{\ell_0}$.

Let $\rho'_M : G_{\mathbb{Q},S} \to E_M^\times$ be the composite of ρ_M with the automorphism $E_M \xrightarrow{\sim} E_M$ given by conjugation by $\left(\begin{smallmatrix} 1 & 0 \\ z & 1 \end{smallmatrix}\right) \in E_M^\times$. By explicit computation, we see that

$$\rho'_M = \begin{pmatrix} \omega(1, F_a) & \tilde{b}_0 \\ \omega(C - (\omega^{-1} - 1)z) & (1, F_d) \end{pmatrix},$$

where $F_a = F - \omega^{-1}\tilde{b}_0 z$ and $F_d = \tilde{b}_0 C - F + \omega\tilde{b}_0 z$; in particular, the $(2,1)$-coordinate of $\rho'_M|_{G_{\ell_0}}$ is zero. This implies that $F_a|_{G_{\ell_0}}, F_d|_{G_{\ell_0}} : G_{\ell_0} \to H^*$ are homomorphisms. Because $\ell_0 \not\equiv 0, 1 \pmod{p}$ and H^* has exponent p, they are unramified.

For any $(\sigma, \tau) \in G_{\ell_0} \times I_{\ell_0}$, we compute that

$$V^{-1}_{\rho'_M}(\sigma, \tau) = \begin{pmatrix} \varepsilon & * \\ 0 & * \end{pmatrix} \begin{pmatrix} 0 & * \\ 0 & 0 \end{pmatrix} = 0$$

where $\varepsilon \in M$. Equivalently, $V^{-1}_{\rho_M} = 0$. A similar computation shows that $V^{-1}_{\rho_M}(\sigma, \tau) = 0$ for $(\sigma, \tau) \in I_{\ell_0} \times G_{\ell_0}$.

If $\ell \mid N$ and $\ell \neq \ell_0$, then $\rho_M|_{G_\ell}$ is US^{+1}_ℓ: In this case we have $\ell \equiv -1 \pmod{p}$, and hence $\omega|_{G_\ell} = \lambda(-1)$. Since $\ell \neq \ell_0$, we have $b_0|_{I_\ell} = 0$, so $b_0|_{G_\ell} = 0$ by Lemma B.1.1. Hence there exists $z \in \mathbb{F}_p$ such that $\tilde{b}_0(\tau) = (\omega(\tau) - 1)z$ for all $\tau \in G_\ell$. Exactly as in the previous case, we can show that $V^{+1}_{\rho_M}(\sigma, \tau) = 0$ for all $(\sigma, \tau) \in G_\ell \times I_\ell \cup I_\ell \times G_\ell$ by conjugating ρ_M by $\left(\begin{smallmatrix} 1 & z \\ 0 & 1 \end{smallmatrix}\right) \in E_M^\times$. □

7.1.4. *End of the proof.* We will show that D_M is, in a sense, the universal US^ϵ_N first-order deformation of $\bar{D}$.

Proposition 7.1.11. *The pseudodeformation D_M of $\bar{D}$ induces an isomorphism $R^\epsilon_N/(p, \mathfrak{m}^2) \xrightarrow{\sim} \mathbb{F}_p[M]$.*

Proof. By Lemma 7.1.9, ρ_M is US^ϵ_N, so D_M is also US^ϵ_N by Definition 3.8.1, and there is an induced map $E^\epsilon_N \to E_M$. This gives us a local homomorphism $R^\epsilon_N \to \mathbb{F}_p[M]$, and any such map factors through $R^\epsilon_N/(p, \mathfrak{m}^2) \to \mathbb{F}_p[M]$. Let f denote the restriction $\mathfrak{m}/(p, \mathfrak{m}^2) \to M$. It suffices to show that f is an isomorphism.

Assume that the GMA structure on E^ϵ_N is chosen so that $E^\epsilon_N \to E_M$ is a morphism of GMAs (such a GMA structure is known to exist by [WWE19, Thm. 3.2.2]). By Theorem 5.2.6, we see that the elements $b_{\gamma_0} c_{\gamma_i}$ for $i = 1, \dots, r$ together with the element $d_{\gamma_0} - 1$ generate $\mathfrak{m}/(p, \mathfrak{m}^2)$, and, moreover, if $\ell_0 \not\equiv 1 \pmod{p}$, the elements $b_{\gamma_0} c_{\gamma_i}$ for $i = 1, \dots, r$ are a basis.

By construction, we see that $f(b_{\gamma_0} c_{\gamma_i}) = (0, \tilde{b}_0(\gamma_0) C(\gamma_i), 0) = (0, C(\gamma_i), 0)$, and that $f(d_{\gamma_0} - 1) = (0, 0, -\log_{\ell_0}(\gamma_0))$ (which is non-zero if $\ell_0 \equiv 1 \pmod{p}$). By Lemma 7.1.13 below, f is surjective.

Now we count dimensions. By Theorem 5.2.6 and Proposition 7.1.4, we have

$$\dim_{\mathbb{F}_p}(\mathfrak{m}/(p, \mathfrak{m}^2)) = \begin{cases} r & \text{if } \delta = 0 \\ r \text{ or } r + 1 & \text{if } \delta = 1. \end{cases}$$

By Lemma 7.1.5, we have

$$\dim_{\mathbb{F}_p}(M) = \begin{cases} r & \text{if } \delta = 0 \\ r + 1 & \text{if } \delta = 1. \end{cases} \tag{7.1.12}$$

Since f is surjective, this implies that f is an isomorphism in all cases. □

Lemma 7.1.13. *Let $\tau_1, \dots, \tau_r \in G_{\mathbb{Q},S}$ be any elements such that:*

- $\omega(\tau_i) = 1$ *for* $i = 1, \dots, r$, *and*
- $\tilde{c}_j(\tau_i) = \partial_{ij}$ *for all* $1 \leq i, j \leq r$.

If $\delta = 1$ or $\ell_0 \not\equiv 1 \pmod{p}$, then the set $\{C(\tau_i) \ : \ i = 1, \dots, r\}$ is a basis for H^*. Otherwise $b_0 \cup c_j \neq 0$ for some j and the set $\{C(\tau_i) \ : \ i = 1, \dots, r, i \neq j\}$ is a basis for H^*.

Proof. Indeed, if $c_j - \alpha c_k \in H$ for some $\alpha \in \mathbb{F}_p$ and $j, k \in \{1, \dots, r\}$, then by Construction 7.1.7(5) we have

$$C(\tau_i)(c_j - \alpha c_k) = \tilde{c}_j(\tau_i) - \alpha \tilde{c}_k(\tau_i) = \partial_{ij} - \alpha \partial_{ik}.$$

Using the explicit basis of H constructed in Lemma 7.1.5, the lemma follows. □

Proof of Theorem 7.1.1. By Proposition 7.1.11, we have $\mathfrak{m}/(p, \mathfrak{m}^2) \xrightarrow{\sim} M$, and the dimension of M is given by (7.1.12). This completes the proof. □

7.2. **Good sets of primes in the case $\epsilon = (-1, 1, \dots, 1)$.** In this section, we prove Theorem 1.7.5. Recall Definition 1.7.3 for the meaning of the set of good primes $\mathcal{Q}$.

Proof of Theorem 1.7.5. We freely refer to ρ_M and related objects in this proof (see (7.1.8)). Let J be the index set of $\mathcal{Q}$ (i.e. $J = \{0, \dots, s\}$, $J = \{0, \dots, s\} \setminus \{j\}$ or $J = \{1, \dots, s\}$ in the three cases of Definition 1.7.3, respectively).

By Theorem 5.2.6, Proposition 7.1.11, and Nakayama's lemma, it suffices to show that the projection $\Upsilon(q)$ of $T_q - (q+1)$ under $\mathbb{T}_N^\epsilon \xrightarrow{\sim} R_N^\epsilon \twoheadrightarrow \mathbb{F}_p[M]$ comprise a basis $\{\Upsilon(q)\}_{q \in \mathcal{Q}}$ of M. The conditions (1)-(6) on $\mathcal{Q}$ have been chosen so that:

(i) If $0 \in J$ and $q_0 \neq p$, then $\omega(\mathrm{Fr}_{q_0}) \neq 1$ and $\log_{\ell_0}(\mathrm{Fr}_{q_0}) \neq 0$. This follows from (1) and (2).
(ii) $\omega(\mathrm{Fr}_{q_i}) = 1$ for $i \in J$ with $i > 0$. This follows from condition (3).
(iii) $\tilde{b}_0(\mathrm{Fr}_{q_i}) \neq 0$ for $i \in J$ with $i > 0$. This follows from (4) by class field theory.
(iv) $\{C(\mathrm{Fr}_{q_i}) : i \in J, i > 0\}$ is a basis for H^*. This follows from Lemma 7.1.13 by (ii), (5), and (6).

When $q_i \neq p$, it is clear that $\Upsilon(q_i) = \mathrm{Tr}\rho_M(\mathrm{Fr}_{q_i}) - (q_i + 1)$, and we calculate:

(a) By (ii), $\Upsilon(q_i) = (0, \tilde{b}_0(\mathrm{Fr}_{q_i}) \cdot C(\mathrm{Fr}_{q_i}), 0) \in \mathbb{F}_p[M]$ for $i \in J$ with $i > 0$. By (iii) and (iv), these elements form a basis of H^*.
(b) If $0 \in J$ and $q_0 \neq p$, then $\Upsilon(q_0) \in \mathbb{F}_p[M]$ lies in M and projects via $M \twoheadrightarrow \mathbb{Z}/(p, \ell_0 - 1)$ to $(\omega(\mathrm{Fr}_{q_0}) - 1)\log_{\ell_0}(\mathrm{Fr}_{q_0})$. This is non-zero, by (i).
(c) If $0 \in J$ and $q_0 = p$, we claim that $\Upsilon(p) \in \mathbb{F}_p[M]$ lies in M and maps to $\log_{\ell_0} p \neq 0$ under the summand projection $M \twoheadrightarrow \mathbb{Z}/(p, \ell_0 - 1)$. This follows from the same argument as in Case $q_0 = p$ of the proof in §7.3, but is simpler. □

Remark 7.2.1. The reader will note that, in this proof, our conditions are used to ensure that a certain matrix is diagonal with non-zero diagonal entries. Of course, the necessary and sufficient condition is simply that this same matrix is invertible.

7.3. **Good pairs of primes in the case $\epsilon = (-1, -1)$.** In this section, we prove Theorem 1.7.1. We assume we are in the setting of Theorem 6.4.1.

Proof of Theorem 1.7.1. By Theorem 6.4.1 and Nakayama's lemma, $\mathbb{T}_N^\epsilon$ is generated by $\{T_{q_i} - (q_i + 1)\}_{i=0,1}$ if and only if their images $\{\Upsilon(q_i)\}_{i=0,1}$ via $\mathbb{T}_N^\epsilon \xrightarrow{\sim}$

$R_N^\epsilon \twoheadrightarrow R_N^\epsilon/(p,\mathfrak{m}^2)$ are a basis of $\mathfrak{m}/(p,\mathfrak{m}^2)$. We see in the proof of Theorem 6.4.1 that $J^{\mathrm{red}} = J^{\min\,2}$. In particular, as $\mathfrak{m} = J^{\min} + (p) \subset R_N^\epsilon$, there are isomorphisms

$$R_N^\epsilon/(p,\mathfrak{m}^2) \xrightarrow{\sim} R_N^{\epsilon,\mathrm{red}}/(p) \cong \mathbb{F}_p[Y_0,Y_1]/(Y_0^2, Y_0Y_1, Y_1^2), \quad \mathfrak{m}/(p,\mathfrak{m}^2) \xrightarrow{\sim} (Y_0,Y_1),$$

which we use as identifications. Then D_N^ϵ pulls back to the pseudorepresentation $D = \psi(\omega\langle-\rangle^{-1} \oplus \langle-\rangle) : G_{\mathbb{Q},S} \to R_N^{\epsilon,\mathrm{red}}/(p)$, where, for particular choices of $\log_{\ell_i}$,

$$G_{\mathbb{Q},S} \ni \tau \mapsto \langle\tau\rangle := 1 + \log_{\ell_0}(\tau)Y_0 + \log_{\ell_1}(\tau)Y_1 \in (R_N^{\epsilon,\mathrm{red}}/(p))^\times.$$

We see that if $q_i \neq p$, then $\Upsilon(q_i) = \mathrm{Tr}_D(\mathrm{Fr}_{q_i}) - (q_i+1)$.

Case $q_0, q_1 \neq p$**.** One computes that the matrix expressing $\{\Upsilon(q_0), \Upsilon(q_1)\}$ in the basis $\{Y_0,Y_1\}$ of $\mathfrak{m}/(p,\mathfrak{m}^2) \cong (Y_0,Y_1)$ is

$$\begin{pmatrix} (q_0-1)\log_{\ell_0} q_0 & (q_1-1)\log_{\ell_0} q_1 \\ (q_0-1)\log_{\ell_1} q_0 & (q_1-1)\log_{\ell_1} q_1 \end{pmatrix} \in M_2(\mathbb{F}_p),$$

which completes the proof.

Case $q_0 = p$**.** We note that the images of $T_p - (p+1)$ and $U_p - 1$ in $I^\epsilon/\mathfrak{m}I^\epsilon$ are equal, so we may replace $T_p - (p+1)$ by $U_p - 1$ in the statement. We recall from Step 3 of the proof of Proposition 4.1.1 that U_p is the image under $R_N^\epsilon \xrightarrow{\sim} \mathbb{T}_N^\epsilon$ of $\frac{1}{x-1}(x\mathrm{Tr}(\rho_N^\epsilon)(\sigma_p) - \mathrm{Tr}(\rho_N^\epsilon)(\tau\sigma_p))$, where $\tau \in I_p$ is such that $\omega(\tau) \neq 1$ and $x = \kappa_{\mathrm{cyc}}(\tau)$. We compute that

$$\Upsilon(p) = \frac{1}{x-1}\big(x\mathrm{Tr}_D(\sigma_p) - \mathrm{Tr}_D(\tau\sigma_p)\big) - 1 = \log_{\ell_0}(p)Y_0 + \log_{\ell_1}(p)Y_1.$$

Thus, the matrix expressing $\{\Upsilon(p), \Upsilon(q_1)\}$ in the basis $\{Y_0,Y_1\}$ of $\mathfrak{m}/(p,\mathfrak{m}^2)$ is

$$\begin{pmatrix} \log_{\ell_0} p & (q_1-1)\log_{\ell_0} q_1 \\ \log_{\ell_1} p & (q_1-1)\log_{\ell_1} q_1 \end{pmatrix} \in M_2(\mathbb{F}_p). \qquad \square$$

Appendix A. Comparison with the Hecke algebra containing U_ℓ

In order to compare our results with existing results and conjectures, in this appendix we consider a Hecke algebra that contains the U_ℓ operators rather than the w_ℓ operators. We prove comparison results between Eisenstein completions of this algebra and the Eisenstein completions $\mathbb{T}_N^\epsilon$ studied in this paper. Throughout this appendix, we drop the subscripts 'N' on all Hecke algebras to avoid cumbersome notation.

Recall that we have the normalization map of Lemma 2.3.1

$$\mathbb{T}^\epsilon \hookrightarrow \mathbb{Z}_p \oplus \left(\bigoplus_{f\in\Sigma} \mathcal{O}_f\right),$$

where $\Sigma, \mathcal{O}_f$ were defined there. For each $f \in \Sigma$, there is a unique pair $(N_f, \tilde{f})$ of a divisor N_f of N and a newform $\tilde{f}$ of level N_f such that $a_q(f) = a_q(\tilde{f})$ for all primes q not dividing N_f and $a_\ell(\tilde{f}) = -\epsilon_\ell$ for primes ℓ dividing N_f. For this $\tilde{f}$, we have $a_q(\tilde{f}) \equiv 1 + q \pmod{\mathfrak{m}_f}$ for all $q \nmid N_f$.

A.1. **Oldforms and stabilizations.** Just as in §2.1.5, if $\ell \mid N$ and $f \in S_2(N/\ell;\mathbb{Z}_p)$ is an eigenform for all T_n with $(n, N/\ell) = 1$, then there are two ways to stabilize f to be a U_ℓ-eigenform in $S_2(N;\mathbb{Z}_p)$. Let $\alpha_\ell(f), \beta_\ell(f)$ denote the roots of $x^2 - a_\ell(f)x + \ell$. Then $f_{\alpha_\ell}(z) = f(z) - \beta_\ell(f)f(\ell z)$ and $f_{\beta_\ell}(z) = f(z) - \alpha_\ell(f)f(\ell z)$ satisfy $U_\ell f_{\alpha_\ell} = \alpha_\ell(f)f_{\alpha_\ell}$ and $U_\ell f_{\beta_\ell} = \beta_\ell(f)f_{\beta_\ell}$. Note that, unlike in §2.1.5, it may happen that $\alpha_\ell(f) \equiv \beta_\ell(f) \pmod{p}$.

A.2. **The case $p \nmid N$.** For this section, assume $p \nmid N$. Let $\mathbb{T}'_U$ and $\mathbb{T}'^0_U$ be the $\mathbb{Z}_p$-subalgebras of

$$\mathrm{End}_{\mathbb{Z}_p}(M_2(N;\mathbb{Z}_p)) \quad \text{and} \quad \mathrm{End}_{\mathbb{Z}_p}(S_2(N;\mathbb{Z}_p)),$$

respectively, generated by the Hecke operators T_ℓ for $\ell \nmid N$ and U_ℓ for $\ell \mid N$. These are semi-simple commutative algebras (see [CE98] for the semi-simplicity).

For each $\epsilon \in \mathcal{E}$ as in §1.4.2, we let $I'^\epsilon_U \subset \mathbb{T}'_U$ be the ideal generated by the set

$$\{T_q - (q+1),\ U_\ell - \ell^{\frac{\epsilon_\ell+1}{2}} : q \nmid N,\ \ell \mid N \text{ primes}\}.$$

Note that $U_\ell - 1 \in I'^\epsilon_U$ if $\epsilon_\ell = -1$ and $U_\ell - \ell \in I'^\epsilon_U$ if $\epsilon_\ell = 1$, so the ideal I'^ϵ_U is the annihilator of a certain stabilization of the Eisenstein series $E_{2,1}$ (but generally not $E^\epsilon_{2,N}$). Let $\mathbb{T}^\epsilon_U$ and $\mathbb{T}^{0,\epsilon}_U$ denote the completions of $\mathbb{T}'_U$ and $\mathbb{T}'^0_U$ respectively, at the maximal ideal $(p, I'^\epsilon_U) \subset \mathbb{T}'_U$. Let $\mathfrak{m}^\epsilon_U \subset \mathbb{T}^\epsilon_U$ and $\mathfrak{m}^{0,\epsilon}_U \subset \mathbb{T}^{0,\epsilon}_U$ be the maximal ideals.

A.2.1. *The normalization of $\mathbb{T}^\epsilon_U$.* Since $\mathbb{T}^\epsilon_U$ and $\mathbb{T}^{0,\epsilon}_U$ are semi-simple, the standard description of prime ideals in terms of eigenforms allows us to describe their normalizations, just as for $\mathbb{T}^\epsilon$. For newforms f, we know that $U_\ell f = -w_\ell f$ for all $\ell \mid N$. For oldforms, we can use the stabilization formulas from §2.1.5 and §A.1 to describe the eigenforms for $\mathbb{T}^\epsilon_U$ in terms of the set Σ. We write down the result of this description explicitly in Lemma A.2.1.

We require the following notation. Let $L_N = \{\ell \mid N \ :\ \ell \equiv 1 \pmod{p}\}$. For each $f \in \Sigma$ and each $\ell \mid \frac{N}{N_f}$, let $\alpha_\ell(f)$ and $\beta_\ell(f)$ be the roots of $x^2 - a_\ell(\tilde{f})x + \ell$. Assume that $\alpha_\ell(f) \equiv \ell^{\frac{\epsilon_\ell+1}{2}} \pmod{p}$ and let $L_f = \{\ell \mid \frac{N}{N_f} : \ell \equiv 1 \pmod{p}\}$. Let $\tilde{\mathcal{O}}_f$ be the extension of $\mathcal{O}_f$ generated by $\alpha_\ell(f)$ and $\beta_\ell(f)$. If $\ell \not\equiv 1 \pmod{p}$, then the congruence condition determines $\alpha_\ell(f)$ ($\beta_\ell(f)$) uniquely, and $\tilde{\mathcal{O}}_f = \mathcal{O}_f$; in this case, only stabilizations of $\tilde{f}_{\alpha_\ell}$ can appear in the completion $S_2(N;\mathbb{Z}_p) \otimes_{\mathbb{T}'^0_U} \mathbb{T}^\epsilon_U$. If $\ell \equiv 1 \pmod{p}$, then we label the two roots arbitrarily (in this situation, below, we will use the two roots symmetrically), and $\tilde{\mathcal{O}}_f$ may be a quadratic extension of $\mathcal{O}_f$; in this case the stabilizations of both $\tilde{f}_{\alpha_\ell}$ and $\tilde{f}_{\beta_\ell}$ can appear in the completion $S_2(N;\mathbb{Z}_p) \otimes_{\mathbb{T}'^0_U} \mathbb{T}^\epsilon_U$.

Lemma A.2.1. *The normalization of $\mathbb{T}^\epsilon_U$ is the injection*

$$\mathbb{T}^\epsilon_U \hookrightarrow \left(\mathop{\oplus'}_{L \subset L_N} \mathbb{Z}_p\right) \oplus \left(\bigoplus_{f \in \Sigma} \left(\bigoplus_{L \subset L_f} \tilde{\mathcal{O}}_f\right)\right),$$

where the primed summation in the first factor indicates that we omit the subset $L = L_N$ if $\epsilon_\ell = 1$ for all $\ell \notin L_N$. The map is given by

$$T_q \mapsto ((1+q)_{L \subset L_N}, a_q(f)_{f \in \Sigma, L \subset L_f}) \text{ for all } q \nmid N,$$

and sending U_ℓ for $\ell \mid N$ as follows. In the factor $\mathbb{T}_U^\epsilon \to \mathbb{Z}_p$ for $L \subset L_N$, we have

$$U_\ell \mapsto \ 1 \quad \text{if} \quad \begin{cases} \ell \notin L_N \text{ and } \epsilon_\ell = -1, \text{ or} \\ \ell \in L_N - L \text{ and } \epsilon_\ell = -1, \text{ or} \\ \ell \in L \text{ and } \epsilon_\ell = 1 \end{cases}$$

and

$$U_\ell \mapsto \ \ell \quad \text{if} \quad \begin{cases} \ell \notin L_N \text{ and } \epsilon_\ell = 1, \text{ or} \\ \ell \in L_N - L \text{ and } \epsilon_\ell = 1, \text{ or} \\ \ell \in L \text{ and } \epsilon_\ell = -1 \end{cases}$$

for all $\ell \mid N$. In the factor $\mathbb{T}_U \to \tilde{\mathcal{O}}_f$ corresponding to $f \in \Sigma$ and $L \subset L_f$, we have

$$U_\ell \mapsto u_\ell(f) := \begin{cases} -\epsilon_\ell & \text{if} \quad \ell \mid N_f \\ \alpha_\ell(f) & \text{if} \quad \ell \mid N, \ell \nmid N_f, \ell \notin L \\ \beta_\ell(f) & \text{if} \quad \ell \mid N, \ell \nmid N_f, \ell \in L \end{cases}$$

for all $\ell \mid N$.

The only part of the lemma that is not completely standard is the factor $\left(\bigoplus'_{L \subset L_N} \mathbb{Z}_p\right)$, which corresponds to the Eisenstein series in $M_2(N)^\epsilon_{\mathrm{Eis}}$. For $\ell \mid N$, if $\ell \notin L_N$, then the U_ℓ-eigenvalue of any such Eisenstein series must be $\ell^{\frac{\epsilon_\ell+1}{2}}$, but if $\ell \in L_N$, then the possible U_ℓ-eigenvalues 1 and ℓ are congruent, and so both appear, regardless of what ϵ_ℓ is. We need to omit $L = L_N$ in the case that $\epsilon_\ell = 1$ for all $\ell \notin L_N$ because that factor corresponds to the Eisenstein series with U_ℓ-eigenvalue ℓ for all $\ell \mid N$, which is the non-holomorphic one.

The normalization of $\mathbb{T}_U^{0,\epsilon}$ is the same, but without the Eisenstein factor $\left(\bigoplus_{L \subset L_N} \mathbb{Z}_p\right)$

A.2.2. *Comparisons.* We now compare the algebras $\mathbb{T}_U^{0,\epsilon}$ and $\mathbb{T}^{0,\epsilon}$. The following proposition gives a necessary and sufficient condition for the algebras to coincide.

Proposition A.2.2. *Suppose that both of the following are true:*

(1) for each $f \in \Sigma$, we have $L_f = \emptyset$; and

(2) $\mathbb{T}_U^{\epsilon,0}$ is generated as a $\mathbb{Z}_p$-algebra by $\{T_q \ : \ q \nmid Np\}$.

Then $\mathbb{T}_U^{\epsilon,0} = \mathbb{T}^{\epsilon,0}$. Moreover, if one of these conditions is false, then $\mathbb{T}_U^{\epsilon,0} \neq \mathbb{T}^{\epsilon,0}$.

Proof. The first condition ensures that $\mathbb{T}_U^{\epsilon,0}$ and $\mathbb{T}^{\epsilon,0}$ have the same normalization, so it is certainly necessary. The second condition is true for $\mathbb{T}^{\epsilon,0}$ by Proposition 4.1.1, so it is necessary. Furthermore, if we assume (1) and (2), then $\mathbb{T}_U^{\epsilon,0}$ and $\mathbb{T}^{\epsilon,0}$ are identified with the subalgebra of $\bigoplus_{f \in \Sigma} \mathcal{O}_f$ generated by $\{(a_q(f)_f) : q \nmid Np\}$. □

We now verify these conditions in certain cases considered in this paper.

Proposition A.2.3. *Assume that $\ell_i \not\equiv 1 \pmod{p}$ for $0 < i \leq r$ and assume that $\epsilon = (-1, 1, \ldots, 1)$. Then $\mathbb{T}_U^{\epsilon,0} = \mathbb{T}^{\epsilon,0}$.*

Proof. We verify the conditions (1) and (2) of Proposition A.2.2.

To verify (1), assume, for a contradiction, that there is an $f \in \Sigma$ with $L_f \neq \emptyset$. By our assumptions on ℓ_i, we must have $L_f = \{\ell_0\}$. Then the newform $\tilde{f} \in S_2(N_f; \overline{\mathbb{Q}}_p)$ satisfies $a_q(\tilde{f}) \equiv 1 + q \pmod{p}$ for all $q \nmid N_f$ and $a_\ell(\tilde{f}) = -1$ for all $\ell \mid N_f$ (since $\ell_0 \nmid N_f$ by assumption). But this is impossible by a theorem of Ribet (see [BD14, Thm. 2.6(ii)(b)]), so (1) holds.

We now turn to (2). Just as in the proof of Proposition 4.1.1, we have a homomorphism $R_N^\epsilon \to \mathbb{T}_U^{0,\epsilon}$ sending $\mathrm{Tr}(\rho_N^\epsilon(\mathrm{Fr}_q))$ for $q \nmid Np$ to T_q, and whose image is

the subalgebra of $\mathbb{T}^0_U$ generated by $\{T_q : q \nmid Np\}$. Note that, by (1), for each $f \in \Sigma$ we have $\ell_0 \mid N_f$, so $u_{\ell_0}(f) = 1$. This implies $U_{\ell_0} = 1$ in $\mathbb{T}^0_U$. Hence to verify (2), we need only show that U_ℓ is in the image of $R^\epsilon_N \to \mathbb{T}^{0,\epsilon}_U$ for all $\ell \mid N$ with $\ell \neq \ell_0$.

Now fix such an ℓ and note that, by assumption, $\ell \not\equiv 1 \pmod p$ and $\epsilon_\ell = 1$. Let $\tilde{U} \in R^\epsilon_N$ be the root of the polynomial $x^2 - \mathrm{Tr}(\rho^\epsilon_N(\sigma_\ell))x + \ell$ such that $\tilde{U} - \ell \in \mathfrak{m}_R$; such a $\tilde{U}$ exists and is unique by Hensel's Lemma. We claim that the image of $\tilde{U}$ in $\mathbb{T}^{0,\epsilon}_U$ is U_ℓ. To prove the claim, it suffices to show that $\tilde{U} \mapsto u_\ell(f)$ under the map $R^\epsilon_N \to \mathcal{O}_f$ for each $f \in \Sigma$.

First assume that $\ell \mid N_f$. By (2.3.2), $\mathrm{Tr}(\rho_f(\sigma_\ell)) = -(\ell + 1)$. So $\tilde{U}$ is sent to the root of

$$x^2 + (\ell + 1)x + \ell = (x + 1)(x + \ell)$$

(that is, either -1 or $-\ell$) that is congruent to ℓ modulo $\mathfrak{m}_f$. Since $\ell \not\equiv -\ell \pmod p$, we see that $\tilde{U}$ is sent to -1. (Note that this shows that if $\ell \mid N_f$, then $\ell \equiv -1 \pmod p$, corroborating Lemma 5.1.1.)

Next assume that $\ell \mid N$ and $\ell \nmid N_f$, so $\mathrm{Tr}(\rho_f(Fr_\ell)) = a_\ell(\tilde{f})$. Then $\tilde{U}$ is sent to the root of

$$x^2 - a_\ell(\tilde{f})x + \ell$$

that is congruent to ℓ modulo $\mathfrak{m}_f$, which is $\alpha_\ell(f)$ by definition.

This shows that, for $f \in \Sigma$ the map $R^\epsilon_N \to \mathcal{O}_f$ sends $\tilde{U}$ to

$$\begin{cases} -1 & \text{if} \quad \ell \mid N_f \\ \alpha_\ell(f) & \text{if} \quad \ell \nmid N_f \end{cases}$$

which is equal to $u_\ell(f)$. Hence U_ℓ is the image of $\tilde{U}$ in $\mathbb{T}^{0,\epsilon}_U$ and the map $R^\epsilon_N \to \mathbb{T}^{0,\epsilon}_U$ is surjective, verifying (2). □

The proof of the first part of the following proposition is almost identical, but simpler, so we leave it to the reader. The second part is an application of Theorem 6.3.1.

Proposition A.2.4. *Assume that $N = \ell_0\ell_1$, that $\ell_1 \not\equiv 1 \pmod p$, and that $\epsilon = (-1, -1)$. Then $\mathbb{T}^{0,\epsilon} = \mathbb{T}^{0,\epsilon}_U$. If, in addition, ℓ_1 is not a p-th power modulo ℓ_0, then $\mathbb{T}^{0,\epsilon}$ and $\mathbb{T}^{0,\epsilon}_U$ are both identical to the Hecke algebra at level ℓ_0 considered by Mazur.*

A.3. **The case $p \mid N$.** In this section, we maintain the notation of the previous section, but we assume that $\ell_0 = p$ and that $\epsilon_0 = -1$ (for $0 < i \leq r$, ϵ_i is arbitrary).

We consider a variant $\mathbb{T}^\epsilon_H$ of the Hecke algebra that is intermediate to $\mathbb{T}^\epsilon$ and $\mathbb{T}^\epsilon_U$. Namely, $\mathbb{T}^\epsilon_H$ is the completion of the Hecke algebra generated by the T_q for $q \nmid N$, together with U_p and w_{ℓ_i} for $0 < i \leq r$, at the ideal generated by p, $\mathbb{T}_q - (q + 1)$, $U_p - 1$, and $w_{\ell_i} - \epsilon_i$. Note that, as in the case of $\mathbb{T}^\epsilon$, we have $w_{\ell_i} = \epsilon_i$ in $\mathbb{T}^\epsilon_H$. For each $f \in \Sigma$, if $p \nmid N_f$, we let $\alpha_p(f) \in \mathcal{O}_f$ be the (unique) unit root of $x^2 - a_p(\tilde{f})x + p$.

Just as in Lemma A.2.1, we can compute the normalization of $\mathbb{T}^\epsilon_H$. It is the injective map

$$\mathbb{T}^\epsilon_H \hookrightarrow \mathbb{Z}_p \oplus \left(\bigoplus_{f \in \Sigma} \mathcal{O}_f \right)$$

sending T_q to $(1 + q, a_q(f)_f)$ for $q \nmid N$ and U_p as follows. The component $\mathbb{T}^\epsilon_H \to \mathbb{Z}_p$ sends U_p to 1. The component $\mathbb{T}^\epsilon_H \to \mathcal{O}_f$ sends U_p to $u_p(f)$ defined by

$$u_p(f) := \begin{cases} 1 & \text{if} \quad p \mid N_f \\ \alpha_p(f) & \text{if} \quad p \nmid N_f. \end{cases}$$

Proposition A.3.1. *With the assumptions that $\ell_0 = p$ and $\epsilon_0 = -1$, we have $\mathbb{T}^{\epsilon}_H = \mathbb{T}^{\epsilon}$ as subalgebras of $\mathbb{Z}_p \oplus \left(\bigoplus_{f\in\Sigma} \mathcal{O}_f\right)$ and $\mathbb{T}^{\epsilon,0}_H = \mathbb{T}^{\epsilon,0}$ as subalgebras of $\left(\bigoplus_{f\in\Sigma} \mathcal{O}_f\right)$.*

Proof. The proof is just as in the proof of Proposition A.2.3, so we will be brief. We have a map $R^{\epsilon}_N \to \mathbb{T}^{\epsilon}_H$ and we need only show that U_p is in the image of this map. Now choose $\sigma_p \in G_p$ to be a Frobenius element such that $\omega(\sigma_p) = 1$, and let $\tilde{U} \in R^{\epsilon}_N$ be the unique unit root of $x^2 - \mathrm{Tr}(\rho^{\epsilon}_N(\sigma_p))x + p$. We see that $\tilde{U}$ maps to U_p. □

Corollary A.3.2. *Let $N = p\ell$ with $\ell \equiv 1 \pmod p$ and $\epsilon = (-1,-1)$. Assume that p is not a p-th power modulo ℓ. Then the Eisenstein ideal of $\mathbb{T}^{\epsilon}_H$ is generated by $U_p - 1$. In particular, $\mathbb{T}^{\epsilon}_H$ and $\mathbb{T}^{0,\epsilon}_H$ are Gorenstein.*

Proof. Combine the previous proposition with Theorem 6.3.1 and Mazur's good prime criterion (§1.1). □

Appendix B. Computation of some cup products

B.1. Cohomology calculations.

Lemma B.1.1. *If $\ell \not\equiv 0, 1 \pmod p$, then the restriction map*

$$H^1(\mathbb{Q}_\ell, \mathbb{F}_p(1)) \to H^1(I_\ell, \mathbb{F}_p(1))$$

is injective.

Proof. Under the isomorphisms of Kummer theory, this map corresponds to the map $\mathbb{Q}_\ell^\times \otimes \mathbb{F}_p \to \mathbb{Q}_\ell^{\mathrm{ur}\,\times} \otimes \mathbb{F}_p$ induced by the inclusion. Since $\ell \not\equiv 0, 1 \pmod p$, $\mathbb{Q}_\ell^\times \otimes \mathbb{F}_p$ is generated by the class of ℓ, which maps the class of ℓ in $\mathbb{Q}_\ell^{\mathrm{ur}\,\times} \otimes \mathbb{F}_p$, which is nonzero. □

Lemma B.1.2. *Let $N = \ell_0 \cdots \ell_r$ be squarefree and assume $p \nmid N$. Let $V = \{i \ : \ p \mid (\ell_i - 1)\}$. The local restriction maps induce an isomorphism*

$$H^2(\mathbb{Z}[1/Np], \mathbb{F}_p) \xrightarrow{\sim} \bigoplus_{i=1}^{r} H^2(\mathbb{Q}_{\ell_i}, \mathbb{F}_p) \cong \bigoplus_{i\in V} H^2(\mathbb{Q}_{\ell_i}, \mathbb{F}_p).$$

of vector spaces of dimension $\#V$.

Proof. Just as in [WWE20, Lem. 12.1.1], we know that

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

is a surjection because $H^3_{(c)}(\mathbb{Z}[1/Np], \mathbb{F}_p) \cong H^0(\mathbb{Z}[1/Np], \mathbb{F}_p(1))^* = 0$. By Tate duality, $H^2(\mathbb{Q}_\ell, \mathbb{F}_p) = H^0(\mathbb{Q}_\ell, \mathbb{F}_p(1))^*$, which is one-dimensional if $\ell \equiv 1 \pmod p$ and zero otherwise. It remains to verify that $H^2(\mathbb{Z}[1/Np], \mathbb{F}_p)$ has the same dimension. This follows from the global Tate Euler characteristic computation of [WWE20, Lem. 12.1.1]. □

The following is a consequence of Tate duality.

Lemma B.1.3. *Assume that $\ell \equiv 1 \pmod{p}$ is prime. Then $H^1(\mathbb{Q}_\ell, \mathbb{F}_p(-1)) = H^1(\mathbb{Q}_\ell, \mathbb{F}_p(1))$. This cohomology group is 2-dimensional, the unramified subspace is 1-dimensional, and the cup product pairing*

$$\cup : H^1(\mathbb{Q}_\ell, \mathbb{F}_p(-1)) \times H^1(\mathbb{Q}_\ell, \mathbb{F}_p(1)) \longrightarrow H^2(\mathbb{Q}_\ell, \mathbb{F}_p)$$

is non-degenerate and symplectic. In particular, the cup product of two unramified classes vanishes, and the cup product of a ramified class with a non-trivial unramified class does not vanish.

B.2. **Proof of Proposition 7.1.3.** By the description of the number fields K_i in Definition 3.10.4, ℓ_0 splits completely in K_i if and only if $\ell_0 \equiv 1 \pmod{p}$ and the image $c_i|_{G_{\ell_0}}$ of c_i in $H^1(\mathbb{Q}_{\ell_0}, \mathbb{F}_p(-1))$ is zero. Since $b_0|_{G_{\ell_0}}$ is ramified and $c_i|_{G_{\ell_0}}$ is unramified, Lemma B.1.3 implies that $c_i|_{G_{\ell_0}} = 0$ if and only if $b_0|_{G_{\ell_0}} \cup c_i|_{G_{\ell_0}} = 0$. By Lemma B.1.2, this happens if and only if $b_0 \cup c_i = 0$.

Appendix C. Algebra

C.1. **Some comments about Gorenstein defect.** Let $(A, \mathfrak{m}_A, k)$ be a regular Noetherian local ring, and let $(R, \mathfrak{m}_R)$ be a finite, flat, local A-algebra.

More generally, for an A-module M, let $M^\vee = \mathrm{Hom}_A(M, A)$. Also, let $\bar{M} = M/\mathfrak{m}_A M$. For a k-vector space M, let $M^* = \mathrm{Hom}_k(M, k)$. For an R-module M, give $M^\vee$ the R-module structure given by $(r \cdot f)(x) = f(rx)$ for $f \in M^\vee$ and $r \in R$, and let $g_R(M) = \dim_k(M/\mathfrak{m}_R M)$ be the minimal number of generators of M. The assumptions on A and R imply that R is a Cohen–Macaulay ring with dualizing module $R^\vee$.

Define the *Gorenstein defect* $\delta(R)$ of R to be the integer $\delta(R) = g_R(R^\vee) - 1$. Then R is Gorenstein if and only if $\delta(R) = 0$ [BH93, Thm. 3.3.7, pg. 111]. If R is complete intersection, then R is Gorenstein [BH93, Prop. 3.2.1, pg. 95]. Kilford and Wiese [KW08, Defn. 1.4] define the Gorenstein defect of R to be $\dim_k \mathrm{Soc}(\bar{R}) - 1$, where $\mathrm{Soc}(\bar{R}) = \mathrm{Ann}_{\bar{R}}(\mathfrak{m}_{\bar{R}})$. Our goal is Lemma C.1.3; these definitions amount to the same thing. The proofs of the following lemmas are elementary, but we include them for completeness.

Lemma C.1.1. *Assume that $A = k$. Then the canonical pairing $R \times R^\vee \to k$ induces a perfect pairing $\mathrm{Ann}_R(\mathfrak{m}_R) \times R^\vee/\mathfrak{m}_R R^\vee \to k$. In particular, $\delta(R) = \dim_k(\mathrm{Ann}_R(\mathfrak{m}_R)) - 1$.*

Proof. By restriction, there is a surjective homomorphism of R-modules

$$R^\vee \twoheadrightarrow \mathrm{Ann}_R(\mathfrak{m}_R)^\vee$$

which is easily seen to factor through $R^\vee/\mathfrak{m}_R R^\vee$. This gives the pairing. To show it is perfect, it is enough to show that the dual map $\mathrm{Ann}_R(\mathfrak{m}_R) \to (R^\vee/\mathfrak{m}_R R^\vee)^\vee$ is surjective as well. This map is induced by the canonical isomorphism $R \to R^{\vee\vee}$ given by $x \mapsto \mathrm{ev}_x$, where $\mathrm{ev}_x(f) = f(x)$ for $f \in R^\vee$.

Let $g \in (R^\vee/\mathfrak{m}_R R^\vee)^\vee$ be an arbitrary element. Then g is induced by a R-module homomorphism $\tilde{g} : R^\vee \to k$ such that $\tilde{g}(r.f) = 0$ for all $r \in \mathfrak{m}_R$ and $f \in R^\vee$. By duality, we have $\tilde{g} = \mathrm{ev}_x$ for some $x \in R$. Then we have

$$0 = \tilde{g}(r.f) = \mathrm{ev}_x(r.f) = f(rx)$$

for all $r \in \mathfrak{m}_R$ and $f \in R^\vee$. This implies that $rx = 0$ for all $r \in \mathfrak{m}_R$, so $x \in \mathrm{Ann}_R(\mathfrak{m}_R)$. Hence g is in the image of $\mathrm{Ann}_R(\mathfrak{m}_R) \to (R^\vee/\mathfrak{m}_R R^\vee)^\vee$, so this map is surjective and the pairing is perfect. □

Lemma C.1.2. *There is a canonical isomorphism of $\bar{R}$-modules $\overline{R^\vee} \cong \bar{R}^*$.*

Proof. Since R is projective as an A-module, the map

$$R^\vee = \mathrm{Hom}_A(R, A) \to \mathrm{Hom}_A(R, k) \cong \mathrm{Hom}_k(\bar{R}, k) = \bar{R}^*$$

is a surjective morphism of R-modules. Since $\mathfrak{m}_A$ annihilates the image, this map must factor through $\overline{R^\vee}$. Since $\overline{R^\vee}$ and $\bar{R}^*$ both have k-dimension equal to $\mathrm{rank}_A(R)$, the map $\overline{R^\vee} \to \bar{R}^*$ is an isomorphism. □

Lemma C.1.3. *We have $\delta(R) = \delta(\bar{R}) = \dim_k \mathrm{Soc}(\bar{R}) - 1$.*

Proof. We have

$$\overline{R^\vee} \otimes_{\bar{R}} \bar{R}/\mathfrak{m}_{\bar{R}} = (R^\vee \otimes_R \bar{R}) \otimes_{\bar{R}} \bar{R}/\mathfrak{m}_{\bar{R}} = R^\vee \otimes_R R/\mathfrak{m}_R$$

so $g_R(R^\vee) = g_{\bar{R}}(\overline{R^\vee})$. By Lemma C.1.2, we have

$$1 + \delta(R) = g_R(R^\vee) = g_{\bar{R}}(\overline{R^\vee}) = g_{\bar{R}}(\bar{R}^*) = 1 + \delta(\bar{R}).$$

This shows that $\delta(R) = \delta(\bar{R})$. The equality $\delta(\bar{R}) = \dim_k \mathrm{Soc}(\bar{R}) - 1$ follows from Lemma C.1.1. □

C.2. **Fiber products of commutative rings.** Note that the category of commutative rings has all limits. The underlying set of the limit of a diagram of commutative rings is the limit of the diagram of underlying sets.

Lemma C.2.1. *Consider a commutative diagram*

$$\begin{array}{ccc} A & \xrightarrow{\pi_B} & B \\ {\scriptstyle \pi_C}\downarrow & & \downarrow{\scriptstyle \phi_B} \\ C & \xrightarrow{\phi_C} & D \end{array}$$

in the category of commutative rings. Assume that all the maps are surjective and that the map $\ker(\pi_B) \to \ker(\phi_C)$ induced by π_C is an isomorphism. Then the canonical map $A \to B \times_D C$ is an isomorphism.

The proof is a diagram chase.

References

[AL70] A. O. L. Atkin and J. Lehner. Hecke operators on $\Gamma_0(m)$. *Math. Ann.*, 185:134–160, 1970.

[BC09] Joël Bellaïche and Gaëtan Chenevier. Families of Galois representations and Selmer groups. *Astérisque*, (324):xii+314, 2009.

[BD14] Nicolas Billerey and Luis V. Dieulefait. Explicit large image theorems for modular forms. *J. Lond. Math. Soc. (2)*, 89(2):499–523, 2014.

[Bel12] Joël Bellaïche. Pseudodeformations. *Math. Z.*, 270(3-4):1163–1180, 2012.

[BH93] Winfried Bruns and Jürgen Herzog. *Cohen-Macaulay rings*, volume 39 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1993.

[BK15] Tobias Berger and Krzysztof Klosin. On lifting and modularity of reducible residual Galois representations over imaginary quadratic fields. *Int. Math. Res. Not. IMRN*, (20):10525–10562, 2015.

[CE98] Robert F. Coleman and Bas Edixhoven. On the semi-simplicity of the U_p-operator on modular forms. *Math. Ann.*, 310(1):119–127, 1998.

[CE05] Frank Calegari and Matthew Emerton. On the ramification of Hecke algebras at Eisenstein primes. *Invent. Math.*, 160(1):97–144, 2005.

[Che14] Gaëtan Chenevier. The p-adic analytic space of pseudocharacters of a profinite group, and pseudorepresentations over arbitrary rings. In *Automorphic Forms and Galois Representations: Vol. I*, volume 414 of *London Mathematical Society Lecture Note Series*, pages 221–285. Cambridge Univ. Press, Cambridge, 2014. We follow the numbering of the online version https://arxiv.org/abs/0809.0415v2, which differs from the print version.

[CS19] Frank Calegari and Joel Specter. Pseudorepresentations of weight one are unramified. *Algebra Number Theory*, 13(7):1583–1596, 2019.

[DDT94] Henri Darmon, Fred Diamond, and Richard Taylor. Fermat's last theorem. In *Current developments in mathematics, 1995 (Cambridge, MA)*, pages 1–154. Int. Press, Cambridge, MA, 1994.

[Gre99] Ralph Greenberg. Iwasawa theory for elliptic curves. In *Arithmetic theory of elliptic curves (Cetraro, 1997)*, volume 1716 of *Lecture Notes in Math.*, pages 51–144. Springer, Berlin, 1999.

[Hsu19] Catherine Hsu. Higher congruences between newforms and Eisenstein series of squarefree level. *J. Théor. Nombres Bordeaux*, 31(2):503–525, 2019.

[HV19] Michael Harris and Akshay Venkatesh. Derived Hecke algebra for weight one forms. *Exp. Math.*, 28(3):342–361, 2019.

[HWWE21] Catherine Hsu, Preston Wake, and Carl Wang-Erickson. Small Eisenstein congruences and explicit non-Gorenstein $R = \mathbb{T}$. In preparation, 2021.

[KM85] Nicholas M. Katz and Barry Mazur. *Arithmetic moduli of elliptic curves*, volume 108 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1985.

[KW08] L. J. P. Kilford and Gabor Wiese. On the failure of the Gorenstein property for Hecke algebras of prime weight. *Experiment. Math.*, 17(1):37–52, 2008.

[Lec20] E. Lecouturier. Higher Eisenstein elements, higher Eichler formulas and rank of Hecke algebras. To appear in *Invent. Math.* https://doi.org/10.1007/s00222-020-00996-1, 2020.

[Maz77] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977.

[Maz97] Barry Mazur. Letter to J. Tilouine and K. Ribet. (Appendix to *Hecke algebras and the Gorenstein property* by J. Tilouine). In *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pages 340–342. Springer, New York, 1997.

[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.

[Oht99] Masami Ohta. Ordinary p-adic étale cohomology groups attached to towers of elliptic modular curves. *Compositio Math.*, 115(3):241–301, 1999.

[Oht05] Masami Ohta. Companion forms and the structure of p-adic Hecke algebras. *J. Reine Angew. Math.*, 585:141–172, 2005.

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

[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.

[Sha11] Romyar Sharifi. A reciprocity map and the two-variable p-adic L-function. *Ann. of Math. (2)*, 173(1):251–300, 2011.

[SW99] C. M. Skinner and A. J. Wiles. Residually reducible representations and modular forms. *Inst. Hautes Études Sci. Publ. Math.*, (89):5–126 (2000), 1999.

[Vat05] V. Vatsal. Multiplicative subgroups of $J_0(N)$ and applications to elliptic curves. *J. Inst. Math. Jussieu*, 4(2):281–316, 2005.

[Wil95] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.

[WWE17] Preston Wake and Carl Wang-Erickson. Ordinary pseudorepresentations and modular forms. *Proc. Amer. Math. Soc. Ser. B*, 4:53–71, 2017.

[WWE18] Preston Wake and Carl Wang-Erickson. Pseudo-modularity and Iwasawa theory. *Amer. J. Math.*, 140(4):977–1040, 2018.

[WWE19] Preston Wake and Carl Wang-Erickson. Deformation conditions for pseudorepresentations. *Forum Math. Sigma*, 7:e20, 44 pp., 2019.

[WWE20] Preston Wake and Carl Wang-Erickson. The rank of Mazur's Eisenstein ideal. *Duke Math. J.*, 169(1):31–115, 2020.

[Yoo17] Hwajong Yoo. The kernel of a rational Eisenstein prime at non-squarefree level. arXiv:1712.01717v1 [math.NT], 2017.

[Yoo19a] Hwajong Yoo. Non-optimal levels of a reducible mod ℓ modular representation. *Trans. Amer. Math. Soc.*, 371(6):3805–3830, 2019.

[Yoo19b] Hwajong Yoo. On rational Eisenstein primes and the rational cuspidal groups of modular Jacobian varieties. *Trans. Amer. Math. Soc.*, 372(4):2429–2466, 2019.

Department of Mathematics, Michigan State University, East Lansing, MI 48824
E-mail address: wakepres@msu.edu

Department of Mathematics, University of Pittsburgh, Pittsburgh, PA 15260
E-mail address: carl.wang-erickson@pitt.edu