Invent. math. 160, 97–144 (2005)
DOI: 10.1007/s00222-004-0406-z

*Inventiones mathematicae*

# On the ramification of Hecke algebras at Eisenstein primes

**Frank Calegari**[1,⋆], **Matthew Emerton**[2,⋆⋆]

[1] Department of Mathematics, Harvard University, Cambridge, MA 02138, USA
(e-mail: fcale@math.harvard.edu)
[2] Department of Mathematics, Northwestern University, Evanston, IL 60208-2730, USA
(e-mail: emerton@math.northwestern.edu)

Oblatum 5-VIII-2003 & 31-VIII-2004
Published online: 11 January 2005 – 

## 1. Introduction

Fix a prime $p$, and a modular residual representation $\overline{\rho} : G_{\mathbf{Q}} \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$. Suppose $f$ is a normalized cuspidal Hecke eigenform of some level $N$ and weight $k$ that gives rise to $\overline{\rho}$, and let $K_f$ denote the extension of $\mathbf{Q}_p$ generated by the $q$-expansion coefficients $a_n(f)$ of $f$. The field $K_f$ is a finite extension of $\mathbf{Q}_p$. What can one say about the extension $K_f/\mathbf{Q}_p$? Buzzard [1] has made the following conjecture: if $N$ is fixed, and $k$ is allowed to vary, then the degree $[K_f : \mathbf{Q}_p]$ is bounded independently of $k$.

Little progress has been made on this conjecture so far; indeed, very little seems to have been proven at all regarding the degrees $[K_f : \mathbf{Q}_p]$. The goal of this paper is to consider a question somewhat orthogonal to that of Buzzard, namely, to fix the weight and vary the level. Moreover, we only consider certain *reducible* representations $\overline{\rho}$ that arise in Mazur's study of the Eisenstein Ideal [7]. Our results suggest that the degrees $[K_f : \mathbf{Q}_p]$ are, in fact, arithmetically significant.

Suppose that $N \geq 5$ is prime, and that $p$ is a prime which exactly divides the numerator of $(N-1)/12$. Mazur ([7], Prop. 9.6, p. 96 and Prop. 19.1, p. 140) has shown that there is a weight two normalized cuspidal Hecke eigenform defined over $\overline{\mathbf{Q}}_p$, unique up to conjugation by $G_{\mathbf{Q}_p}$ (the Galois group of $\overline{\mathbf{Q}}_p$ over $\mathbf{Q}_p$), satisfying the congruence

$$a_\ell(f) \equiv 1 + \ell \mod \mathfrak{p} \tag{1}$$

⋆ F.C. acknowledges the partial support of the AIM.
⋆⋆ M.E. acknowledges the partial support of the NSF grant nos. DMS-0241562 and DMS-0401545.

(where $\mathfrak{p}$ is the maximal ideal in the ring of integers of $K_f$, and $\ell$ ranges over primes distinct from $N$). It follows moreover from [7] (Prop. 19.1, p. 140) that $K_f$ is a *totally ramified* extension of $\mathbf{Q}_p$, and thus that the degree $[K_f : \mathbf{Q}_p]$ is equal to the (absolute) ramification degree of $K_f$. Denote this ramification degree by $e_p$.

In this paper we prove the following theorem, in the case when $p = 2$.

**Theorem 1.1.** *Suppose that $p = 2$ and that $N \equiv 9 \mod 16$, and let $f$ be a weight two eigenform on $\Gamma_0(N)$ satisfying the congruence (1). If $2^m$ is the largest power of 2 dividing the class number of the field $\mathbf{Q}(\sqrt{-N})$, then $e_2 = 2^{m-1} - 1$.*

When $p$ is odd, we establish the following less definitive result.

**Theorem 1.2.** *Suppose that $p$ is an odd prime exactly dividing the numerator of $(N-1)/12$. Let $f$ be a weight two eigenform on $\Gamma_0(N)$ satisfying the congruence (1).*

*(i) Suppose that $p = 3$. (Our hypothesis on $N$ thus becomes $N \equiv 10$ or $19 \mod 27$). Then $e_3 = 1$ if and only if the 3-part of the class group of $\mathbf{Q}(\sqrt{-3}, N^{1/3})$ is cyclic.*

*(ii) Suppose that $p \geq 5$. (Our hypothesis on $N$ thus becomes $p \| N - 1$). Then $e_p = 1$ if the $p$-part of the class group of $\mathbf{Q}(N^{1/p})$ is cyclic.*

The question of computing $e_p$ has been addressed previously, in the paper [9] of Merel. In this work, Merel establishes a necessary and sufficient criterion for $e_p = 1$. Merel's criterion for $e_p = 1$ is *not* expressed in terms of class groups; rather, it is expressed in terms of whether or not the congruence class modulo $N$ of a certain explicit expression is a $p$th power.

When $p = 2$, Merel, using classical results from algebraic number theory, was able to reinterpret his explicit criterion for $e_2 = 1$ so as to prove that $e_2 = 1$ if and only if $m = 2$. (It is known that $m \geq 2$ if and only if $N \equiv 1 \mod 8$; see Proposition 4.1 below.) Theorem 1.1 strengthens this result, by relating the value of $e_2$ in all cases to the order of the 2-part of the class group of $\mathbf{Q}(\sqrt{-N})$.

When $p$ is odd, Merel was not able to reinterpret his explicit criterion in algebraic number theoretic terms. However, combining Merel's result with Theorem 1.2 (and the analogue of this theorem for more general primes $N$, i.e. those for which $p$ divides $N - 1$, but not necessarily exactly) yields the following result.

**Theorem 1.3.** *Let $N \geq 5$ be prime.*

*(i) Let $N \equiv 1 \mod 9$. The 3-part of the class group of $\mathbf{Q}(\sqrt{-3}, N^{1/3})$ is cyclic if and only if $\left(\frac{N-1}{3}\right)!$ is not a cube modulo $N$. Equivalently, if we let $N = \pi\bar{\pi}$ denote the factorization of $N$ in $\mathbf{Q}(\sqrt{-3})$, then the*

*3-part of the class group of* $\mathbf{Q}(N^{1/3}, \sqrt{-3})$ *is cyclic if and only if the 9th power residue symbol* $\left(\frac{\pi}{\bar{\pi}}\right)_9$ *is non-trivial.*[1]

*Furthermore, if these equivalent conditions hold, then the 3-part of the class group of* $\mathbf{Q}(N^{1/3})$ *(which a fortiori is cyclic of order divisible by three) has order exactly three.*

*(ii) Let* $p \geq 5$*, and let* $N \equiv 1 \mod p$*. If the p-part of the class group of* $\mathbf{Q}(N^{1/p})$ *is cyclic then*

$$\prod_{\ell=1}^{(N-1)/2} \ell^{\ell}$$

*is not a pth power modulo N.*

The proofs of Theorems 1.1 and 1.2 depend on arguments using deformations of Galois representations. Briefly, if $\mathbf{T}$ denotes the completion at its $p$-Eisenstein ideal of the Hecke algebra acting on weight two modular forms on $\Gamma_0(N)$, then we identify $\mathbf{T}$ with the universal deformation ring for a certain deformation problem. The theorems are then proved by an explicit analysis of this deformation problem over Artinian $\mathbf{F}_p$-algebras.

It may be of independent interest to note that our identification of $\mathbf{T}$ as a universal deformation ring also allows us to recover *all* the results of Mazur proved in the reference [7] regarding the structure of $\mathbf{T}$ and the Eisenstein ideal: for example, that $\mathbf{T}$ is monogenic over $\mathbf{Z}_p$ (and hence Gorenstein); that the Eisenstein ideal is principal, and is generated by $T_\ell - (1 + \ell)$ if and only if $\ell \neq N$ is a good prime; and also that $T_N = 1$ in $\mathbf{T}$.

Let us now give a more detailed explanation of our method. For the moment, we relax our condition on $N$, assuming simply that $N$ and $p$ are distinct primes. We begin by defining a continuous representation $\overline{\rho} : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F}_p)$. If $p$ is odd, we let

$$\overline{\rho} = \begin{pmatrix} \overline{\chi}_p & 0 \\ 0 & 1 \end{pmatrix},$$

where $\overline{\chi}_p$ is the mod $p$ reduction of the cyclotomic character. If $p$ is even, we let

$$\overline{\rho} = \begin{pmatrix} 1 & \phi \\ 0 & 1 \end{pmatrix},$$

where $\phi : G_{\mathbf{Q}} \to \mathbf{F}_2$ is the unique $\mathbf{F}_2$-valued homomorphism inducing an isomorphism $\mathrm{Gal}(\mathbf{Q}(\sqrt{-1})/\mathbf{Q}) \cong \mathbf{F}_2$.

Let $\overline{V}$ denote the two dimensional vector space on which $\overline{\rho}$ acts, and fix a line $\overline{L}$ in $\overline{V}$ that is *not* invariant under $G_{\mathbf{Q}}$ (equivalently, $G_{\mathbf{Q}_p}$).

[1] The claimed equivalence follows from the formula $\left(\left(\frac{N-1}{3}\right)!\right)^3 \equiv \pi \mod \bar{\pi}$, which was pointed out to us by Noam Elkies. René Schoof has told us that one can prove part (i) of Theorem 1.3 using class field theory. It is not apparent, however, that (ii) can be proved in this way.

Fix once and for all a choice of inertia group $I_N$ at $N$. If $A$ is an Artinian local ring with residue field $\mathbf{F}_p$, consider the set of triples $(V, L, \rho)$, where $V$ is a free $A$-module, $L$ is a direct summand of $V$ that is free of rank one over $A$, and $\rho$ is a continuous homomorphism $G_{\mathbf{Q}} \to \mathrm{GL}(V)$, satisfying the following conditions:

Def1. The triple $(V, L, \rho)$ is a deformation of $(\overline{V}, \overline{L}, \overline{\rho})$.
Def2. The representation $\rho$ is unramified away from $p$ and $N$, and is finite at $p$ (i.e. $V$, regarded as a $G_{\mathbf{Q}_p}$-module, arises as the generic fibre of a finite flat group scheme over $\mathbf{Z}_p$).
Def3. The inertia subgroup at $N$ acts trivially on the submodule $L$ of $V$.
Def4. The determinant of $\rho$ is equal to the composition of the cyclotomic character $\chi_p : G_{\mathbf{Q}} \to \mathbf{Z}_p^\times$ with the natural map $\mathbf{Z}_p^\times \to A^\times$.

If we let $\mathrm{Def}(A)$ denote the collection of such triples modulo strict equivalence ([8] §8, p. 257), then Def defines a deformation functor on the category of Artinian local rings $A$.

Note that the representation $\overline{\rho}$ is reducible, and is either the direct sum of two characters (if $p$ is odd) or an extension of the trivial character by itself (if $p = 2$). Nevertheless, one has the following result.

**Proposition 1.4.** *The deformation functor* Def *is pro-representable by a complete Noetherian local* $\mathbf{Z}_p$*-algebra* $R$.

The proposition follows directly from that fact that the only endomorphisms of the triple $(\overline{V}, \overline{L}, \overline{\rho})$ are the scalars. (See for example [13], Prop. 1.2.) (The authors learned the idea of introducing a locally invariant line to rigidify an otherwise unrepresentable deformation problem from Mark Dickinson, who has applied it to analyse the deformation theory of residually irreducible representations that are ordinary, but not $p$-distinguished, locally at $p$.)

Having defined a universal deformation ring, we now introduce the corresponding Hecke algebra. As indicated above, we let $\mathbf{T}$ denote the completion at its $p$-Eisenstein ideal of the $\mathbf{Z}$-algebra of Hecke operators acting on the space of all modular forms (i.e. the cuspforms together with the Eisenstein series) of level $\Gamma_0(N)$ and weight two. (The $p$-Eisenstein ideal is the maximal ideal in the Hecke algebra generated by the elements $T_\ell - (1 + \ell)$ $(\ell \neq N)$, $T_N - 1$, and $p$).

The following result relates $R$ and $\mathbf{T}$.

**Theorem 1.5.** *If* $\rho^{\mathrm{univ}}$ *denotes the universal deformation of* $\overline{\rho}$ *over the universal deformation ring* $R$*, then there is an isomorphism of* $\mathbf{Z}_p$*-algebras* $R \cong \mathbf{T}$*, uniquely determined by the requirement that the trace of Frobenius at* $\ell$ *under* $\rho^{\mathrm{univ}}$ *(for primes* $\ell \neq p, N$*) maps to the Hecke operator* $T_\ell \in \mathbf{T}$.

Let us now return to the setting of Theorems 1.1 and 1.2. Thus we suppose again that $p$ exactly divides the numerator of $(N - 1)/12$, and let $f$ be as in the statements of the theorems. If $\mathcal{O}$ denotes the ring of integers

in $K_f$, and $\mathfrak{p}$ its maximal ideal, then the results of [7] imply (taking into account the congruence satisfied by $N$) that the Hecke algebra $\mathbf{T}$ admits the following description:

$$\mathbf{T} = \{(a, b) \in \mathbf{Z}_p \times \mathcal{O} \mid a \bmod p = b \bmod \mathfrak{p}\}.$$

From this description of $\mathbf{T}$, one easily computes that $\mathbf{T}/p$ is isomorphic to $\mathbf{F}_p[X]/X^{e_p+1}$. Theorem 1.5 thus yields the following characterization of $e_p$.

**Corollary 1.6.** *The natural number $e_p$ is the largest integer $e$ for which we may find a triple $(V, L, \rho)$ in $\mathrm{Def}(\mathbf{F}_p[X]/X^{e+1})$ such that the induced map $R \to \mathbf{F}_p[X]/X^{e+1}$ is surjective.*

Theorems 1.1 and 1.2 are a consequence of this corollary, together with an explicit analysis of the deformations of $(\overline{V}, \overline{L}, \overline{\rho})$ over Artinian local rings of the form $\mathbf{F}_p[X]/X^n$.

If $p^2$ divides the numerator of $(N-1)/12$, then the residually Eisenstein cusp forms of level $N$ need not be mutually conjugate. However, one still has an isomorphism of the form $\mathbf{T}/p = \mathbf{F}_p[x]/x^{g_p+1}$, where $g_p + 1$ denotes the rank of $\mathbf{T}$ over $\mathbf{Z}_p$. (Thus $g_p$ is the rank over $\mathbf{Z}_p$ of the cuspidal quotient of $\mathbf{T}$.) In particular, the cuspidal Hecke algebra localized at the Eisenstein prime is isomorphic to $\mathbf{Z}_p$ if and only if $g_p = 1$. In this way our analysis of deformations over $\mathbf{F}_p[X]/X^n$ suffices to prove Theorem 1.3. More generally, our paper can be seen as providing a partial answer to Mazur's question ([7], p. 140): "*Is there anything general that can be said ... about $g_p$?*".

The organization of the paper is as follows. In Sect. 2 we develop some results about group schemes that will be required in our study of the deformation functor Def. In Sect. 3 we prove Theorem 1.5, using the numerical criterion of Wiles [17] (subsequently strengthened by Lenstra [6]). As in [16], we use the class field theory of cyclotomic fields to obtain the required upper bound for the size of an appropriate Galois cohomology group; the numerical criterion is then established by comparing this upper bound with the congruence modulus of the weight two Eisenstein series on $\Gamma_0(N)$ (which is known by [7] to equal the numerator of $(N-1)/12$). Finally in Sects. 4 (respectively 5) we perform the analysis necessary to deduce Theorem 1.1 (respectively 1.2 and 1.3) from Corollary 1.6.

Let us close this introduction by emphasising that the only result of [7] required for the proof of Theorem 1.5 is the computation of the congruence modulus between the Eisenstein and cuspidal locus in the Hecke algebra of weight two and level $N$. (Namely, that this congruence modulus is equal to the numerator of $(N-1)/12$.) As remarked upon above, we are then able to deduce all the results of [7] regarding $\mathbf{T}$ and its quotient $\mathbf{T}^0$ from Theorem 1.5. The necessary arguments are presented at the end of Sect. 3.

*Acknowledgements.* The authors would like to thank Brian Conrad for his close reading of an earlier version of this paper. His many remarks not only improved the exposition, but also saved us from a blunder or two. The authors are also grateful for the comments of the anonymous referee; these too were helpful in improving the exposition of the paper.

## 2. Some group scheme-theoretic calculations

Let us fix a prime $p$, and a natural number $n$. We begin with some generalities on finite flat group schemes. All group schemes to be considered here and below will be assumed commutative, whether or not this is explicitly noted.

For any scheme $S$ we let $\mathcal{G}r(S)$ denote the category of (commutative, in light of the convention signalled above) finite flat group schemes over the base $S$. Passing from an object of $\mathcal{G}r(S)$ to the corresponding *fppf* sheaf that it represents embeds $\mathcal{G}r(S)$ as a full additive subcategory of the abelian category of abelian sheaves on the *fppf* site of $S$. We let $\mathcal{S}h(S)$ denote this latter category, and in this way we regard $\mathcal{G}r(S)$ as a full subcategory of $\mathcal{S}h(S)$. A key point is that $\mathcal{G}r(S)$ is closed under extensions in $\mathcal{S}h(S)$ (see Lemma 2.3) and so is an exact category in the sense of Quillen [12].

We suppose from now on that $S = \operatorname{Spec} \mathcal{O}$ with $\mathcal{O}$ a Dedekind domain whose field of fractions $K$ is of characteristic zero. We let $\eta$ denote $\operatorname{Spec} K$, fix an algebraic closure $\overline{K}$ of $K$, and write $G_K := \operatorname{Gal}(\overline{K}/K)$. Since $K$ is of characteristic zero, passing to $\overline{K}$-valued points induces an equivalence between the category $\mathcal{G}r(\eta)$ and the category of finite discrete $G_K$-modules (and we will freely identify an object of $\mathcal{G}r(\eta)$ with the corresponding $G_K$-module). In particular, this category is abelian. Since any object of $\mathcal{G}r(S)$ is equal to the scheme theoretic closure of its generic fibre, restriction from $\mathcal{G}r(S)$ to $\mathcal{G}r(\eta)$ is a faithful functor (although typically not fully faithful).

If $M_{/K}$ is a $G_K$-module, we will refer to an object $M$ of $\mathcal{G}r(S)$ whose generic fibre is isomorphic to $M_{/K}$ as a finite flat prolongation of $M_{/K}$ over $S$. The collection of such prolongations form a category in an evident way (morphisms being morphisms in $\mathcal{G}r(S)$ that restrict to the identity on the generic fibre). Note that there is at most one morphism between any two prolongations of $M_{/K}$ (since restriction to the generic fibre is faithful). In particular, if $M_{/K}$ admits a prolongation that is unique up to isomorphism, then it is unique up to unique isomorphism.

We now describe some simple but crucial aspects of the homological algebra of the exact category $\mathcal{G}r(S)$.

**Lemma 2.1.** *If $S$ is a Dedekind scheme of generic characteristic zero, then the category $\mathcal{G}r(S)$ admits kernels, cokernels, images, and coimages. Furthermore, the formation of each of these is compatible with passage to the generic fibre.*

*Proof.* Let $f : G \to H$ be a morphism in the category $\mathcal{G}r(S)$. Since for a Dedekind domain, flat coincides with torsion free, we see that the scheme-theoretic closure of the kernel of $f_{/K}$ is a finite flat subgroup scheme of $G$, while the scheme-theoretic closure of the image of $f_{/K}$ in $H$ is a finite flat subgroup scheme of $H$. One checks that these are the kernel and image respectively of $f$ in the category $\mathcal{G}r(S)$. The quotient of $G$ by the kernel of $f$ is then a coimage of $f$ in the category $\mathcal{G}r(S)$, while the quotient of $H$ by the image of $f$ is then a cokernel of $f$ in the category $\mathcal{G}r(S)$. □

Note that the constructions of the preceding lemma typically do not coincide with the corresponding constructions in the larger category $\mathcal{Sh}(S)$. For example, take $S = \operatorname{Spec} \mathbf{Z}$, and let $f : (\mathbf{Z}/2)_{/\mathbf{Z}} \to (\mu_2)_{/\mathbf{Z}}$ be the map that induces the identity on generic fibres. Then $f$ has zero kernel, zero cokernel, coimage equal to $(\mathbf{Z}/2)_{/\mathbf{Z}}$, and image equal to $(\mu_2)_{/\mathbf{Z}}$.

Suppose now that $G$ is an object of $\mathcal{G}r(S)$ with endomorphisms by a ring $A$, and suppose that $M$ is a finitely presented right $A$-module. We may define the object $M \otimes_A G$ of $\mathcal{G}r(S)$ in the following way: Choose a presentation $A^r \xrightarrow{\phi} A^s \longrightarrow M \to 0$ of $M$, and define $M \otimes_A G$ to be the cokernel of the induced map $G^r \xrightarrow{\phi \otimes \mathrm{id}_G} G^s$.

**Lemma 2.2.** *The object $M \otimes_A G$ of $\mathcal{G}r(S)$ is well-defined, up to natural isomorphism, independent of the choice of presentation of $M$.*

*Proof.* We leave the easy proof to the reader. □

Since the formation of cokernels is compatible with passage to the generic fibre, we see that there is a natural isomorphism of $G_K$-modules $(M \otimes_A G)_{/K} \cong M \otimes_A (G_{/K})$. We also record here the following lemma used implicitly throughout the rest of the text:

**Lemma 2.3.** *The category $\mathcal{G}r(S)$ is closed under extensions in $\mathcal{Sh}(S)$.*

*Proof.* This follows from [10], Cor. 17.5, III.17-7.

The following result is useful for obtaining finite flat $A$-module schemes. The authors thank Brian Conrad for providing the proof.

**Lemma 2.4.** *Suppose that $M_{/K}$ is a finite discrete $G_K$-module that has a unique (up to isomorphism) finite flat prolongation $M$ over $S$. If $M_{/K}$ admits an $A$-module structure (compatible with its $G_K$-module structure), then this extends uniquely to an $A$-module scheme structure on $M$.*

*Proof.* Since restriction to the generic fibre is a faithful functor on $\mathcal{G}r(S)$, it suffices to show that for each $a \in A$, the corresponding endomorphism of $M_{/K}$ extends to an endomorphism of $M$. These extensions will then necessarily be unique, and induce an $A$-module scheme structure on $M$.

If $a \in A$, let $(\Gamma_a)_{/K} \subset (M \times M)_{/K}$ denote the graph of the endomorphism of $M_{/K}$ induced by $a$. This is then a Galois submodule of $(M \times M)_{/K}$ that maps isomorphically to $M_{/K}$ under the first projection. The Zariski closure of $(\Gamma_a)_{/K}$ in $M \times M$ is thus a closed finite flat subgroup scheme $\Gamma_a$ of $M \times M$ prolonging $(\Gamma_a)_{/K}$. Our assumption that $M_{/K}$ has a unique prolongation over $S$ up to isomorphism implies that the first projection from $\Gamma_a$ to $M$ is again an isomorphism, and hence that $\Gamma_a$ is (as the notation suggests) the graph of an endomorphism of $M$, which extends multiplication by $a$ on $M_{/K}$. □

There is one more homological algebra result that we will need.

**Proposition 2.5.** *Let $V_{/K}$ be a finite discrete $G_K$-module, and suppose that $V_{/K}$ has a unique (up to isomorphism) prolongation to an object $V$ of $\mathcal{G}r(S)$. If $M_{/K}$ is any finite discrete $G_K$-module that admits a filtration by $G_K$-submodules whose subquotients are isomorphic to $V_{/K}$, and that admits a prolongation to a finite flat group scheme $M$ over $S$, then this prolongation is unique up to isomorphism. (The above discussion shows that this isomorphism is then also necessarily unique.) Furthermore, any composition series of $M_{/K}$ with successive quotients isomorphic to $V_{/K}$ prolongs to a composition series for $M$ consisting of closed finite flat subgroup schemes whose subquotients are isomorphic to $V$.*

*Proof.* Let $M$ and $M'$ be two choices of a finite flat group scheme over $S$ prolonging $M_{/K}$. The results of [14] show that we may find a prolongation of $M_{/K}$ that maps (in the category of such prolongations) to each of $M$ and $M'$. Thus we may assume we are given a map $M \to M'$ that induces the identity on generic fibres. By assumption we may find an embedding $V_{/K} \subset M_{/K}$. Passing to scheme theoretic closures in each of $M$ and $M'$, and taking into our assumption on the uniqueness of $V$ (up to isomorphism), this prolongs to an embedding of $V$ into each of $M$ and $M'$, so that the map $M \to M'$ restricts to the identity map between these two copies of $V$. Replacing $M_{/K}$ by $M_{/K}/V_{/K}$, $M$ by $M/V$, and $M'$ by $M'/V$, and arguing by induction on the order of $M$, the proposition follows from the 5-lemma (applied, for example, in the category of sheaves on the *fppf* site over $S$). □

For any prime power $p^n$, we let $\mathcal{G}r(p^n, S)$ denote the full, exact subcategory of $\mathcal{G}r(S)$ consisting of finite flat group schemes of exponent $p^n$. We are primarily interested in finite flat group schemes of exponent $p^n$ (for various $p$ and $n$) that are extensions of $\mathbf{Z}/p^n$ by $\mu_{p^n}$, and so we work in the categories $\mathcal{G}r(p^n, S)$ from now on. We write $\mathrm{Ext}^1_{S,p^n}(-,-)$ to denote the first Yoneda Ext bifunctor on the exact category $\mathcal{G}r(p^n, S)$. (Note in particular, then, that by stipulation, for any objects $G$ and $H$ of $\mathcal{G}r(p^n, S)$, elements of $\mathrm{Ext}^1_{S,p^n}(G, H)$ correspond to extensions of the group scheme $G$ by $H$ that are of exponent $p^n$.) Our base scheme $S$ will typically be either an open subset of $\mathrm{Spec}\,\mathbf{Z}$, or else $\mathrm{Spec}\,\mathbf{Z}_p$.

**Lemma 2.6.** *The natural map $\mathrm{Ext}^1_{\mathbf{Z}_p,p^n}(\mathbf{Z}/p^n, \mu_{p^n}) \to \mathrm{Ext}^1_{\mathbf{Q}_p,p^n}(\mathbf{Z}/p^n, \mu_{p^n})$, induced by restricting to the generic fibre, is injective.*

*Proof.* Kummer theory identifies the map in the statement of the lemma with the obviously injective map $\mathbf{Z}_p^\times/(\mathbf{Z}_p^\times)^{p^n} \to \mathbf{Q}_p^\times/(\mathbf{Q}_p^\times)^{p^n}$. □

If $p = 2$, we let $V_n^{\min}$ denote the extension of $\mathbf{Z}/2^n$ by $\mu_{2^n}$ in the category $\mathcal{G}r(2^n, \mathbf{Q})$ corresponding by Kummer theory to the element $-1 \in \mathbf{Q}^\times/(\mathbf{Q}^\times)^{2^n}$. If $p$ is odd, we let $V_n^{\min}$ denote the direct sum $\mathbf{Z}/p^n \bigoplus \mu_{p^n}$ in the category $\mathcal{G}r(p^n, \mathbf{Q})$. We may (and do) regard $V_n^{\min}$ as an object of the category of $G_{\mathbf{Q}}$-modules annihilated by $p^n$.

More explicitly, let $\chi_p$ denote the $p$-adic cyclotomic character. Then if $p = 2$, the $G_{\mathbf{Q}}$-module $V_n^{\min}$ corresponds to the representation

$$\rho_n^{\min} : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Z}/2^n)$$

given by

$$\sigma \mapsto \begin{pmatrix} \chi_2(\sigma) & (\chi_2(\sigma) - 1)/2 \\ 0 & 1 \end{pmatrix} \mod 2^n,$$

whilst if $p$ is odd, the $G_{\mathbf{Q}}$-module $V_n^{\min}$ corresponds to the representation

$$\rho_n^{\min} : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Z}/p^n)$$

given by

$$\sigma \mapsto \begin{pmatrix} \chi_p(\sigma) & 0 \\ 0 & 1 \end{pmatrix} \mod p^n.$$

(Here we have denoted by $\sigma$ an element of $G_{\mathbf{Q}}$.)

**Proposition 2.7.** *For any natural number $M$, the $G_{\mathbf{Q}}$-module $V_n^{\min}$ has a unique prolongation to an object of $\mathcal{G}r(p^n, \mathbf{Z}[1/M])$.*

*Proof.* The Galois module $V_n^{\min}$ is unramified away from $p$, and so $V_n^{\min}$ has a unique prolongation to a finite étale group scheme over $\mathbf{Z}[1/Mp]$. It thus suffices to show that $V_n^{\min}$, regarded as a $G_{\mathbf{Q}_p}$-module, has a unique prolongation to an object of $\mathcal{G}r(p^n, \mathbf{Z}_p)$. If $p$ is odd, then this is a direct consequence of [2], Thm. 2. Thus we assume for the remainder of the proof that $p = 2$. In this case, $V_n^{\min}$ is defined to be the extension of $\mathbf{Z}/2^n$ by $\mu_{2^n}$ corresponding to $-1 \in \mathbf{Q}_2^{\times}$. Since $-1$ in fact lies in $\mathbf{Z}_2^{\times}$, $V_n^{\min}$ does prolong to a finite flat group scheme over $\mathbf{Z}_2$. We must show that this prolongation is unique.

We begin with the case $n = 1$. Suppose that $G$ is a finite flat group scheme over $\mathbf{Z}_2$ having $(V_1^{\min})_{/\mathbf{Q}_2}$ as its associated Galois representation. The scheme-theoretic closure of the fixed line in $V_1^{\min}$ yields an order two finite flat subgroup scheme $H$ of $G$. Both $H$ and $G/H$ are thus finite flat group schemes of order two. The results of [11] show that $\mathbf{Z}/2$ and $\mu_2$ are the only group schemes of order 2 over $\mathbf{Z}_2$. Thus $G$ is an extension of either $\mathbf{Z}/2$ or $\mu_2$ by either $\mathbf{Z}/2$ or $\mu_2$. Since neither $G$ nor its Cartier dual are unramified (since $V_1^{\min}$ is self-dual and ramified at 2), we see that both $\mathbf{Z}/2$ and $\mu_2$ must appear. Since $V_1^{\min}$ is a non-trivial $G_{\mathbf{Q}_2}$-module, a consideration of the connected-étale exact sequence attached to $G$ shows that in fact $G$ is an extension of $\mathbf{Z}/2$ by $\mu_2$. The fact that $G$ is determined uniquely by $V_1^{\min}$ now follows from Lemma 2.6. The uniqueness in the case of arbitrary $n$ follows from the result of the preceding paragraph, together with Proposition 2.5. □

**Lemma 2.8.** *Let $D_n$ denote the (uniquely determined, by Proposition 2.7) prolongation of $V_n^{\min}$ to an object of $\mathcal{G}r(p^n, \mathbf{Z})$. We have* $\mathrm{Ext}^1_{\mathbf{Z}, p^n}(\mathbf{Z}/p^n, D_n) = \mathrm{Ext}^1_{\mathbf{Z}, p^n}(D_n, \mu_{p^n}) = 0$.

*Proof.* Writing $D_n$ as an extension of $\mathbf{Z}/p^n$ by $\mu_{p^n}$, we obtain the exact sequence of Yoneda Ext groups

$$\mathrm{Ext}^1_{\mathbf{Z},p^n}(\mathbf{Z}/p^n, \mu_{p^n}) \to \mathrm{Ext}^1_{\mathbf{Z},p^n}(\mathbf{Z}/p^n, D_n) \to \mathrm{Ext}^1_{\mathbf{Z},p^n}(\mathbf{Z}/p^n, \mathbf{Z}/p^n).$$

The third of these groups always vanishes, since $\mathbf{Z}$ has no non-trivial finite étale covers. The first group is isomorphic to $\mathbf{Z}^\times/\mathbf{Z}^{\times p}$, so if $p$ is odd it vanishes, and if $p = 2$ it has order two, with the non-trivial element corresponding by Kummer theory to $-1 \in \mathbf{Z}^\times$. Since $D_n$ is itself classified by this same element when $p = 2$, we see that the first arrow vanishes in all cases, and thus so does the middle group. □

**Corollary 2.9.** *Suppose that $A$ is an Artinian local ring with maximal ideal $\mathfrak{p}$ and residue field $\mathbf{F}_p$, that $V$ is a free $A$-module of rank two, and that $\rho : G_{\mathbf{Q}_p} \to \mathrm{GL}(V)$ is a deformation of $(V_1^{\min})_{/\mathbf{Q}_p}$ that is finite flat at $p$. Then there is a unique up to unique isomorphism finite flat group scheme $M$ over $\mathbf{Z}_p$ whose generic fibre equals $V$. Furthermore, the $A$-action on $V$ prolongs to an $A$-action on $M$, the connected-étale sequence of $M$ realizes $M$ as the extension of an étale finite flat $A$-module scheme of $A$-rank one by a multiplicative finite flat $A$-module scheme of $A$-rank one, and $M$ admits a filtration by closed finite flat sub-$A$-module schemes with successive quotients isomorphic to $D_1$.*

*Proof.* If we choose a Jordan-Hölder filtration of $A$ as a module over itself, then this induces a filtration of $V$ with successive quotients isomorphic to $V_1^{\min}$. Thus we are in the situation of Proposition 2.5, and the uniqueness of $M$ follows, as does the existence of the required filtration of $M$. (Note that this uniqueness result, together with Lemma 2.4, shows that the $A$-actions on $V$ and on each of the members of its filtration extend respectively to an $A$-action on $M$ and on the members of its filtration.) Finally, let $0 \to M^0 \to M \to M^{\text{ét}} \to 0$ be the connected-étale sequence of $M$. The functorial nature of its construction implies that it is an exact sequence of closed finite flat $A$-submodule schemes of $M$. Thus the exact sequence $0 \to M^0_{/\mathbf{Q}_p} \to V \to M^{\text{ét}}_{/\mathbf{Q}_p} \to 0$ obtained by restricting to $\mathbf{Q}_p$ yields a two-step filtration of $V$ by $A$-submodules. The formation of this filtration is clearly functorial in $A$. Thus if we tensor $M$ with $A/\mathfrak{p}$ over $A$, and take into account that $A/\mathfrak{p} \otimes_A M = D_1$, we find that $A/\mathfrak{p} \otimes_A M^0 = D_1^0 = \mu_p$ and that $A/\mathfrak{p} \otimes_A M^{\text{ét}} = D_1^{\text{ét}} = \mathbf{Z}/p$. Thus each of $M^0_{/\mathbf{Q}_p}$ and $M^{\text{ét}}_{/\mathbf{Q}_p}$ are cyclic $A$-modules. Since $M_{/\mathbf{Q}_p}$ is free of rank two over $A$, they must both be free $A$-modules of rank one, as claimed. We also see that $M^0$ is multiplicative, as claimed. □

**Proposition 2.10.** *Let $A$ be an Artinian local $\mathbf{Z}/p^n$-algebra with maximal ideal $\mathfrak{p}$ and residue field $\mathbf{F}_p$. If $V$ is a free $A$-module of rank two and $\rho : G_{\mathbf{Q}_p} \to \mathrm{GL}(V)$ is a deformation of $(V_1^{\min})_{/\mathbf{Q}_p}$ that is finite at $p$, then the coinvariants of $V$ with respect to the inertia group $I_p$ are free of rank one over $A$.*

*Proof.* The preceding corollary shows that $V$ admits a two-step filtration, with rank one free quotients, corresponding to the connected-étale sequence of the prolongation of $V$ to a group scheme over $\mathbf{Z}_p$. In particular, the inertial coinvariants $V_{I_p}$ admit a surjection onto a free $A$-module of rank one. On the other hand, if $\mathfrak{p}$ is the maximal ideal of $A$, then $(V_{I_p})/\mathfrak{p} = (V/\mathfrak{p})_{I_p} = (V_1^{\min})_{I_p}$. This latter space is directly checked to be one dimensional over $\mathbf{F}_p$, implying that $V_{I_p}$ is a cyclic $A$-module. Altogether, we find that $V_{I_p}$ is free of rank one over $A$, as claimed. □

**Proposition 2.11.** *Let $A$ be an Artinian local $\mathbf{Z}/p^n$-algebra with maximal ideal $\mathfrak{p}$ and residue field $\mathbf{F}_p$. If $V$ is a free $A$-module of rank two and $\rho : G_{\mathbf{Q}} \to \mathrm{GL}(V)$ is a deformation of $V_1^{\min}$ that is unramified away from $p$ and finite at $p$, then there is an $A$-linear isomorphism of $G_K$-modules $V \cong A \otimes_{\mathbf{Z}/p^n} V_n^{\min}$. (Note that we ignore for the moment the question of whether this isomorphism can be taken to be an isomorphism of deformations of $V_1^{\min}$.)*

*Proof.* Corollary 2.9 shows that $V$ prolongs to a finite flat $A$-module scheme $M$ over $\mathrm{Spec}\,\mathbf{Z}$, which admits a Jordan-Hölder filtration by closed finite flat subgroup schemes, with successive quotients isomorphic to $D_1$.

If $p$ is odd, then Proposition I.4.5 of [7] shows that $M$ is the product of a constant finite flat closed subgroup scheme and a $\mu$-type finite flat closed subgroup scheme. (Recall that a finite flat group scheme is said to be of $\mu$-type if it is Cartier dual to a constant group scheme). Furthermore, these subgroup schemes are unique (and hence this direct product decomposition of $M$ is unique), since when $p$ is odd, there are non-zero morphisms from a constant étale group scheme to a $\mu$-type group scheme (over $\mathbf{Q}$, and hence over $\mathbf{Z}$). Each of these subgroups is thus an $A$-submodule scheme of $M$, and we easily conclude that $V \cong A \otimes_{\mathbf{Z}/p^n} V_n^{\min}$.

If $p = 2$, then Propositions I.2.1 and I.3.1 of [7] show that $M$ is the extension of a constant group scheme by a $\mu$-type group. Again, each of these groups is seen to be an $A$-module scheme, and we easily conclude that $M$ is in fact an extension of the constant $A$-module scheme $A$ by the $\mu$-type $A$-module scheme $A \otimes_{\mathbf{Z}/2^n} \mu_{2^n}$. The group of all such extensions is classified by

$$H^1(\mathrm{Spec}\,\mathbf{Z}, A \otimes_{\mathbf{Z}/2^n} \mu_{2^n}) \cong A \otimes_{\mathbf{Z}/2^n} \mathbf{Z}^\times/(\mathbf{Z}^\times)^{2^n} \cong A/2 \otimes_{\mathbf{F}_2} \{\pm 1\}.$$

We thus see that this cohomology group is free of rank one over $A/2$. Since $V_1^{\min}$ corresponds by Kummer theory to the non-trivial element of $\{\pm 1\}$, we see that the elements of this cohomology group corresponding to deformations of $V_1^{\min}$ form a principal homogeneous space under $(A/2)^\times$. The action of $A^\times$ on $H^1(\mathrm{Spec}\,\mathbf{Z}, A \otimes_{\mathbf{Z}/2^n} \mu_{2^n})$ corresponds simply to "changing the basis" of $A \otimes_{\mathbf{Z}/2^n} \mu_{2^n}$. Thus it does not change the isomorphism class of the finite flat group scheme underlying a given extension, and so we see that there is is a unique finite flat group scheme over $\mathbf{Z}$ that deforms $V_1^{\min}$ over $A$ (which must then be $A \otimes_{\mathbf{Z}/2^n} V_n^{\min}$). □

We leave it to the reader to verify the following lemma.

**Lemma 2.12.** *If $A$ is an Artinian local $\mathbf{Z}/p^n$-algebra with maximal ideal $\mathfrak{p}$, then the ring of Galois equivariant endomorphisms of $A \otimes_{\mathbf{Z}/p^n} V^{\min}$ admits the following description:*

*(i) If $p = 2$, then* $\mathrm{End}_{A[G_{\mathbf{Q}}]}(A \otimes_{\mathbf{Z}/2^n} V_n^{\min}) = \{\begin{pmatrix} a & b \\ 0 & a-2b \end{pmatrix} \mid a, b \in A\}$.

*(ii) If $p$ is odd, then* $\mathrm{End}_{A[G_{\mathbf{Q}}]}(A \otimes_{\mathbf{Z}/p^n} V_n^{\min}) = \{\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a, d \in A\}$.

## 3. Proving that $R = \mathbf{T}$

We let Def denote the deformation problem described in the introduction. We begin by describing some equivalent formulations of condition 4 in the definition of Def.

**Lemma 3.1.** *If $A$ is an Artinian local ring with residue field $\mathbf{F}_p$, and if $(V, L, \rho)$ is a triple satisfying conditions Def1, Def2, and Def3 in the definition of* Def*, then the following conditions are equivalent:*

*Def4. The determinant of $\rho$ is equal to the cyclotomic character $\chi_p$.*
*Def4a. The determinant of $\rho$ is unramified away from $p$.*
*Def4b. The inertia subgroup at $N$ acts trivially on the quotient $V/L$.*

*Proof.* It is obvious that Def4 implies Def4a and Def4b. By assumption $\rho$ is unramified away from $p$ and $N$, and $I_N$ (inertia at $N$) acts trivially on $L$, from which it also follows that Def4a and Def4b are equivalent. If Def4a holds, then (by the Kronecker-Weber theorem) the determinant of $\rho$ is determined by its action on inertia at $p$. Corollary 2.9 shows that the finite flat group scheme over $\mathbf{Z}_p$ that prolongs $V$ is the extension of an étale $A$-module scheme of rank one over $A$ by a multiplicative $A$-module scheme of rank one over $A$. Consequently, the determinant of $\rho$, restricted to inertia at $p$, is equal to $\chi_p$, and so Def4a implies Def4. □

Our proof of Theorem 1.5 employs the technique introduced in [17]: namely, we first consider a minimal deformation $\rho^{\min}$ of $(\overline{V}, \overline{L}, \overline{\rho})$ over $\mathbf{Z}_p$, and then verify the numerical criterion of [17].

Let us define the minimal deformation problem $\mathrm{Def}^{\min}$, as the subfunctor of Def consisting of those deformations of $(\overline{V}, \overline{L}, \overline{\rho})$ that are unramified away from $p$. Let us also define $(\mathrm{Def}^{\min})'$ to be the functor that classifies all deformations of $(\overline{V}, \overline{\rho})$ that are unramified away from $p$ and finite at $p$. Forgetting the $I_N$-fixed line $L$ gives a natural transformation $\mathrm{Def}^{\min} \to (\mathrm{Def}^{\min})'$.

Let us now define the triple $(V^{\min}, L^{\min}, \rho^{\min})$. We take $V^{\min} = \mathbf{Z}_p \bigoplus \mathbf{Z}_p$. If $p = 2$, then we let $\rho^{\min}$ denote the representation

$$\sigma \mapsto \begin{pmatrix} \chi_2(\sigma) & (\chi_2(\sigma) - 1)/2 \\ 0 & 1 \end{pmatrix}$$

(here $\sigma$ denotes an element of $G_{\mathbf{Q}}$), while if $p$ is odd, we let $\rho^{\min}$ denote the direct sum of $\chi_p$ (the $p$-adic cyclotomic character) and 1 (the trivial character). In each case, the pair $(V^{\min}, \rho^{\min})$ is certainly a lifting of $(\overline{V}, \overline{\rho})$. We take $L^{\min}$ to be any free of rank one $\mathbf{Z}_p$-submodule of $V^{\min}$ lifting the line $\overline{L}$ in $\overline{V}$.

Note that for any natural number $n$, we have $V^{\min}/p^n = V_n^{\min}$ (the Galois module introduced in the preceding section).

**Proposition 3.2.** *The natural transformation* $\mathrm{Def}^{\min} \to (\mathrm{Def}^{\min})'$ *is an isomorphism of functors. Moreover, the deformation functor* $\mathrm{Def}^{\min}$ *is pro-represented by* $(V^{\min}, L^{\min}, \rho^{\min})$ *in* $\mathrm{Def}^{\min}(\mathbf{Z}_p)$.

*Proof.* Let $A$ be an Artinian local $\mathbf{Z}_p$-algebra, and let $(V, \rho)$ be an object of $(\mathrm{Def}^{\min})'(A)$. Proposition 2.11 shows that there is an isomorphism $V \cong A \otimes_{\mathbf{Z}_p} V^{\min}$. The explicit description of the endomorphisms of $A \otimes_{\mathbf{Z}_p} V^{\min}$ provided by Lemma 2.12 shows that we may furthermore choose this isomorphism so that it is strict. Thus we see that $(\mathrm{Def}^{\min})'$ is pro-represented by $\mathbf{Z}_p$, with $(V^{\min}, \rho^{\min})$ as universal object.

Now suppose that $(V, L, \rho)$ is an object of $\mathrm{Def}^{\min}(A)$. Using Lemma 2.12 again, we see that we may choose the strict endomorphism $V \cong A \otimes_{\mathbf{Z}_p} V^{\min}$ of the preceding paragraph in such a way that $L$ is identified with $A \otimes_{\mathbf{Z}_p} L^{\min}$. Thus $\mathbf{Z}_p$ also pro-represents $\mathrm{Def}^{\min}$, with universal object $(V^{\min}, L^{\min}, \rho^{\min})$. This establishes the proposition. □

Note that the preceding lemma implies in particular that the class of $(V^{\min}, L^{\min}, \rho^{\min})$ in $\mathrm{Def}(\mathbf{Z}_p)$ is independent of the choice of $L^{\min}$ (provided that it lifts $\overline{L}$).

Let $R$ denote the universal deformation ring that pro-represents the functor Def, and let $(V^{\mathrm{univ}}, L^{\mathrm{univ}}, \rho^{\mathrm{univ}})$ denote the universal deformation of $(\overline{V}, \overline{L}, \overline{\rho})$ over $R$. Corresponding to $(V^{\min}, L^{\min}, \rho^{\min})$ there is a homomorphism $R \to \mathbf{Z}_p$ of $\mathbf{Z}_p$-algebras. We let $I$ denote the kernel of this homomorphism. The following more explicit description of $I$ will be useful.

**Proposition 3.3.** *If $S$ is any finite set of primes containing $p$ and $N$, then $I$ is generated by the set*

$$\{1 + \ell - \mathrm{Trace}(\rho^{\mathrm{univ}}(\mathrm{Frob}_\ell)) \mid \ell \notin S\}.$$

*Proof.* Let $I_S$ denote the ideal generated by the stated set. Clearly $I_S \subset I$. We will show that the Galois representation $G_{\mathbf{Q}} \to \mathrm{GL}_2(R/I_S)$ obtained by reducing $\rho^{\mathrm{univ}}$ modulo $I_S$ is unramified at $N$. It will follow from Proposition 3.2 that $I \subset I_S$, and the proposition will be proved. The argument is a variation of that used to prove Prop. 2.1 of [16].

Suppose first that $p$ is odd. Let us choose a basis for $V^{\mathrm{univ}}$, and write

$$\rho^{\mathrm{univ}}(\sigma) = \begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix},$$

for $\sigma \in G_{\mathbf{Q}}$. We may assume that if $c \in G_{\mathbf{Q}}$ denotes complex conjugation, then

$$\rho^{\mathrm{univ}}(c) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

We find that

$$a(\sigma) = \frac{1}{2}\left(\mathrm{Trace}(\rho^{\mathrm{univ}}(\sigma)) - \mathrm{Trace}(\rho^{\mathrm{univ}}(c\sigma))\right),$$

and that

$$d(\sigma) = \frac{1}{2}\left(\mathrm{Trace}(\rho^{\mathrm{univ}}(\sigma)) + \mathrm{Trace}(\rho^{\mathrm{univ}}(c\sigma))\right).$$

Since by construction $\mathrm{Trace}(\rho^{\mathrm{univ}}(\sigma)) \equiv 1 + \chi_p(\sigma) \mod I_S$, we find that

$$a(\sigma) \equiv \chi_p(\sigma) \mod I_S,$$

whilst

$$d(\sigma) \equiv 1 \mod I_S.$$

In particular, if $\sigma$ is an element of the inertia group $I_N$, then

$$\rho^{\mathrm{univ}}(\sigma) \equiv \begin{pmatrix} 1 & b(\sigma) \\ c(\sigma) & 1 \end{pmatrix} \mod I_S.$$

The universal $I_N$-fixed line is spanned by a vector of the form $(1, x)$, where $x \in R^\times$. We conclude that if $\sigma \in I_N$ then

$$(1 + b(\sigma)x, c(\sigma) + x) \equiv (1, x) \mod I_S,$$

and thus that

$$b(\sigma) \equiv c(\sigma) \equiv 0 \mod I_S.$$

This implies that $\rho^{\mathrm{univ}} \mod I_S$ is unramified at $N$, as required.

Consider now the case $p = 2$. Again, we write

$$\rho^{\mathrm{univ}}(\sigma) = \begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix},$$

for $\sigma \in G_{\mathbf{Q}}$. We may assume that if $c \in G_{\mathbf{Q}}$ denotes complex conjugation, then

$$\rho^{\mathrm{univ}}(c) = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}.$$

We may also assume that the universal $I_N$-fixed line is spanned by the vector $(0, 1)$. By considering $\mathrm{Trace}(\rho^{\mathrm{univ}}(c\sigma))$, for $\sigma \in G_{\mathbf{Q}}$, we find that

$$-a(\sigma) - c(\sigma) + d(\sigma) \equiv 1 - \chi_2(\sigma) \mod I_S.$$

If $\sigma \in I_N$, then since $\sigma$ fixes $(0, 1)$, we find that

$$b(\sigma) = 0, \quad d(\sigma) = 1.$$

The preceding equations, the fact that $\det \rho^{univ} = \chi_2$, and the fact that $\chi_2(\sigma) = 1$ for $\sigma \in I_N$, imply that also

$$a(\sigma) \equiv 1, \quad c(\sigma) \equiv 0 \mod I_S.$$

Altogether, we conclude that $\rho^{\text{univ}} \mod I_S$ is unramified at $N$, as required. □

The preceding result has the following important corollary.

**Corollary 3.4.** *If $S$ is any finite set of primes containing $p$ and $N$, then the complete local $\mathbf{Z}_p$-algebra $R$ is topologically generated by the elements* $\text{Trace}(\rho^{\text{univ}}(\text{Frob}_\ell))$, *for $\ell \notin S$.*

*Proof.* This follows immediately from the description of $I$ provided by Proposition 3.3, the fact that $R$ is $I$-adically complete, and the fact that $R/I \cong \mathbf{Z}_p$. □

We now compute the order of $I/I^2$, which is one of the two ingredients we will eventually use in our verification of the Wiles-Lenstra numerical criterion.

**Theorem 3.5.** *The order of $I/I^2$ (which is a power of $p$) divides $(N^2-1)/24$.*

*Proof.* As usual, the first step of the argument involves identifying the Pontrjagin dual of $I/I^2$ with a certain (inductive limit of) Ext groups. We begin by describing the relevant extensions.

Let $n$ be a natural number, and let $(V_n^{\min}, L_n^{\min}, \rho_n^{\min})$ denote the reduction modulo $p^n$ of $(V^{\min}, L^{\min}, \rho^{\min})$. We consider extensions of Galois modules

$$0 \to \left(V_n^{\min}, L_n^{\min}\right) \to (E, F) \to \left(V_n^{\min}, L_n^{\min}\right) \to 0;$$

here the notation indicates that $E$ is a $\mathbf{Z}/p^n[G_{\mathbf{Q}}]$-module that extends $V_n^{\min}$ by itself, and that $F$ is a submodule of $E$ (not assumed to be Galois invariant) that provides an extension of $L_n^{\min}$ by itself.

We let $\mathcal{A}_n$ denote the additive category of such extensions for which $E$ is annihilated by $p^n$, is unramified away from $p$ and $N$, is finite at $p$, and for which both $F$ and $E/F$ are fixed (element-wise) by the inertia group $I_N$. Morphisms between two objects $(E_1, F_1)$ and $(E_2, F_2)$ of the category $\mathcal{A}_n$ are given by isomorphisms of Galois modules $E_1 \to E_2$ that take $F_1$ to $F_2$, and that make the diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & V_n^{\min} & \longrightarrow & E_1 & \longrightarrow & V_n^{\min} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \mathrm{id}_{V_n^{\min}}} & & \downarrow & & \downarrow{\scriptstyle \mathrm{id}_{V_n^{\min}}} & & \\
0 & \longrightarrow & V_n^{\min} & \longrightarrow & E_2 & \longrightarrow & V_n^{\min} & \longrightarrow & 0
\end{array}$$

commute. The direct sum is given by the usual Baer sum of extensions.

We let $A_n$ denote the Grothendieck group of isomorphism classes of objects of $\mathcal{A}_n$. There are natural Galois equivariant maps $(V_{n+1}^{\min}, L_{n+1}^{\min}) \to (V_n^{\min}, L_n^{\min})$ and $(V_n^{\min}, L_n^{\min}) \to (V_{n+1}^{\min}, L_{n+1}^{\min})$, the first being given by reduction modulo $p^n$, and the second by regarding the sources as the $p^n$-torsion in the target. Pulling back by the first of these maps, and pushing forward by the second, we obtain a functor $F_n : \mathcal{A}_n \to \mathcal{A}_{n+1}$. Thus $F_n$ induces a homomorphism $A_n \to A_{n+1}$ of Grothendieck groups. The usual identification of the relative tangent space to a deformation functor with an appropriate Ext-group in an appropriate category of Galois modules shows that

$$\mathrm{Hom}\left(I/I^2, \mathbf{Q}_p/\mathbf{Z}_p\right) \cong \varinjlim A_n. \tag{2}$$

(Note that we are using the equivalence of conditions Def4 and Def4b in the definition of Def provided by Lemma 3.1.)

We will prove the lemma by showing that the right hand side of this isomorphism has order dividing $(N^2 - 1)/24$. In fact, we will not work directly with the rather complicated Ext groups $A_n$. Rather, we fill construct an injection of inductive systems $\{A_n\}_{n\geq 1} \to \{B_n\}_{n\geq 1}$, with each $B_n$ being a simpler Ext group, and investigate the limit $\varinjlim B_n$ instead.

If $(E, F)$ is an object of $A_n$, then since $\mathbf{Z}/p^n$ (with the trivial $G_{\mathbf{Q}}$-action) is a quotient of $V_n^{\min}$, whilst $\mu_{p^n}$ (with its natural $G_{\mathbf{Q}}$-action) is a submodule of $V_n^{\min}$, the extension $E$ determines an extension $E'$ of $G_{\mathbf{Q}}$ modules

$$0 \to \mathbf{Z}/p^n \to E' \to \mu_{p^n} \to 0. \tag{3}$$

Let $B_n$ denote the group of isomorphism classes of extensions of $G_{\mathbf{Q}}$-modules of the form (3) that are unramified away from $p$ and $N$, and that prolong over $\mathbf{Z}_p$ to an extension of the finite flat group scheme $\mu_{p^n}$ by the finite flat group scheme $\mathbf{Z}/p^n$. The natural maps $\mu_{p^{n+1}} \to \mu_{p^n}$ and $\mathbf{Z}/p^n \to \mathbf{Z}/p^{n+1}$, given respectively by raising to the $p$th power and by multiplication by $p$, induce a map $B_n \to B_{n+1}$. Thus the $B_n$ form an inductive system. The passage from $E$ to $E'$ gives rise to a homomorphism of inductive sequences

$$\{A_n\}_{n\geq 1} \to \{B_n\}_{n\geq 1}, \tag{4}$$

which we will next show is injective.

**Lemma 3.6.** *If $(E, F)$ is an object of $\mathcal{A}_n$ for which $E$ is a trivial extension, then the pair $(E, F)$ is also a trivial extension.*

*Proof.* Let us remind the reader that if $E$ is the trivial extension of $V_n^{\min}$ by itself, then the automorphisms of $E$ (as an object of $\mathcal{A}_n$) are of the form $\begin{pmatrix} \mathrm{Id} & A \\ 0 & \mathrm{Id} \end{pmatrix}$, where $A$ is an element of $\mathrm{End}_{G_{\mathbf{Q}}}(V_n^{\min})$. This being said, the lemma is easily checked using Lemma 2.12.

Alternatively, we may appeal to Proposition 3.2. Since $E$ is assumed to be a trivial extension, it is in particular unramified at $N$, and thus corresponds to a deformation for the subproblem $\mathrm{Def}^{\mathrm{min}}$ of Def. The triviality of $E$ implies that this deformation is trivial, when regarded as an deformation for the problem $(\mathrm{Def}^{\mathrm{min}})'$. Since $\mathrm{Def}^{\mathrm{min}}$ maps isomorphically to $(\mathrm{Def}^{\mathrm{min}})'$, we obtain the assertion of the lemma. □

**Lemma 3.7.** *If $(E, F)$ is an object of $\mathcal{A}_n$ for which the corresponding extension $E'$ in $B_n$ is trivial, then $E$ is also a trivial extension.*

*Proof.* We begin by pointing out the category $\mathcal{A}_n$ has a natural involution, given by passing to Cartier duals. Indeed, since $V_n^{\mathrm{min}}$ is Cartier self-dual by construction, if $(E, F)$ is an object of $\mathcal{A}_n$, then the Cartier dual $E^*$ is itself an extension of $V_n^{\mathrm{min}}$ by itself in a natural way. We define $F^*$ to be the annihilator of $F$ in $E^*$; our assumptions then make it clear that $(E^*, F^*)$ is again an object of $\mathcal{A}_n$. (Note that $V_n^{\mathrm{min}}$ is identified with its Cartier dual $(V_n^{\mathrm{min}})^*$ via the alternating pairing $\wedge : V_n^{\mathrm{min}} \times V_n^{\mathrm{min}} \to \det(V_n^{\mathrm{min}}) \cong \chi_p \bmod p^n$, which implies that $(L_n^{\mathrm{min}})^* = L_n^{\mathrm{min}}$.) It is clear that the extension $(E^*)'$ of $\mu_{p^n}$ by $\mathbf{Z}/p^n$ arising from $E^*$ is obtained by taking the Cartier dual of the extension $E'$ arising from $E$. Thus if $E'$ is trivial, so is $(E^*)'$.

We now prove the lemma. Let $D_n$ denote the (unique, by Proposition 2.7) prolongation of $V_n^{\mathrm{min}}$ to a finite flat group scheme over $\mathbf{Z}[1/N]$. Proposition 2.5 shows that $E$ has a unique prolongation to a finite flat group scheme $\mathcal{E}$ over $\mathbf{Z}[1/N]$, that provides an extension of $D_n$ by itself. We let $D_n^{(1)}$ denote the copy of $D_n$ that appears as a submodule of $\mathcal{E}$, and let $D_n^{(2)}$ denote the copy of $D_n$ that appears as a quotient. Also, we let $\mu_{p^n}^{(i)}$ (respectively $(\mathbf{Z}/p^n)^{(i)}$) denote the copy of $\mu_{p^n}$ (respectively $\mathbf{Z}/p^n$) that appears as a subgroup scheme (respectively a quotient group scheme) of $D_n^{(i)}$, for $i = 1, 2$. The extension (3) corresponding to $E$ thus prolongs to an extension $\mathcal{E}'$ of $\mu_{p^n}$ by $\mathbf{Z}/p^n$ as finite flat groups schemes over $\mathbf{Z}[1/N]$.

We begin by observing that our hypothesis that $E'$ is a trivial extension implies that $\mathcal{E}'$ is also a trivial extension. Indeed, since $\mathcal{E}'$ is étale over $\mathbf{Z}[1/Np]$, the splitting of the extension of Galois modules $E'$ implies the splitting of the corresponding extension of group schemes $\mathcal{E}'$ over $\mathbf{Z}[1/Np]$. Also, a consideration of the connected-étale sequence shows that $\mathcal{E}'_{|\mathbf{Z}_p}$ is a split extension (for any $E'$!). Thus $\mathcal{E}'$ splits over $\mathbf{Z}[1/N]$, as claimed.

The quotient $\mathcal{E}/\mu_{p^n}^{(1)}$ is an extension of $D_n^{(2)}$ by $(\mathbf{Z}/p^n)^{(1)}$. Thus it yields a class $e \in \mathrm{Ext}_{\mathbf{Z}[1/N], p^n}(D_n^{(2)}, (\mathbf{Z}/p^n)^{(1)})$. This latter group sits in the exact sequence

$$\begin{aligned} \mathrm{Ext}_{\mathbf{Z}[1/N], p^n}((\mathbf{Z}/p^n)^{(2)}, (\mathbf{Z}/p^n)^{(1)}) &\to \mathrm{Ext}_{\mathbf{Z}[1/N], p^n}\left(D_n^{(2)}, (\mathbf{Z}/p^n)^{(1)}\right) \\ &\to \mathrm{Ext}_{\mathbf{Z}[1/N], p^n}\left(\mu_{p^n}^{(2)}, (\mathbf{Z}/p^n)^{(1)}\right). \end{aligned} \tag{5}$$

The image of $e$ under the second arrow of (5) classifies the extension $\mathcal{E}'$, and thus vanishes. Thus there is a class $e' \in \mathrm{Ext}_{\mathbf{Z}[1/N], p^n}((\mathbf{Z}/p^n)^{(2)}, (\mathbf{Z}/p^n)^{(1)})$

that maps to $e$ under the first arrow of (5). We can construct such an extension class $e'$ concretely as follows: Since the image of $e$ vanishes, we may choose a lift of $\mu_{p^n}^{(2)}$ to a subgroup scheme $\mu$ of $\mathcal{E}/\mu_{p^n}^{(1)}$. The quotient $(\mathcal{E}/\mu_{p^n}^{(1)})/\mu$ is then an extension of $(\mathbf{Z}/p^n)^{(2)}$ by $(\mathbf{Z}/p^n)^{(1)}$, which gives a realization of a class $e'$ mapping to $e$. Our assumption on the submodule $F$ of $E$ implies that it maps surjectively onto $(E/\mu_{p^n}^{(1)})/\mu$ (the generic fibre of $(\mathcal{E}/\mu_{p^n}^{(1)})/\mu$), and thus that the action of inertia at $N$ on $(E/\mu_{p^n}^{(1)})/\mu$ is trivial. Thus $(\mathcal{E}/\mu_{p^n}^{(1)})/\mu$ has a prolongation to a finite flat group scheme over $\mathbf{Z}$, yielding an extension of $\mathbf{Z}/p^n$ by itself. There are no such non-trivial extensions that are finite flat over $\mathbf{Z}$, and thus the extension class $e'$ is trivial. Hence the extension class $e$ is also trivial, and so $\mathcal{E}/\mu_{p^n}^{(1)}$ is a split extension of $D_n^{(2)}$ by $(\mathbf{Z}/p^n)^{(1)}$.

If $\tilde{\mathcal{E}}$ denotes the preimage in $\mathcal{E}$ of the subgroup $\mu_{p^n}^{(2)} \subset D_n^{(2)}$, then we find that $\tilde{\mathcal{E}}$ is Cartier dual to $\mathcal{E}^*/\mu_{p^n}^{(1)}$. (Where we are momentarily applying the notation $\mu_{p^n}^{(1)}$ not to $\mathcal{E}$, but to its Cartier dual $\mathcal{E}^*$.) The observations at the beginning of the argument show that the reasoning of the preceding paragraph applies equally well to $E^*$, and thus that $\mathcal{E}^*/\mu_{p^n}^{(1)}$ is a split extension of $D_n^{(2)}$ by $(\mathbf{Z}/p^n)^{(1)}$. Consequently, passing back from $\mathcal{E}^*$ to $\mathcal{E}$, we conclude that $\tilde{\mathcal{E}}$ is a split extension of $\mu_{p^n}^{(2)}$ by $D_n^{(1)}$. Consider the exact sequence

$$\begin{aligned} \mathrm{Ext}_{\mathbf{Z}[1/N],p^n}\left((\mathbf{Z}/p^n)^{(2)}, D_n^{(1)}\right) &\to \mathrm{Ext}_{\mathbf{Z}[1/N],p^n}\left(D_n^{(2)}, D_n^{(1)}\right) \\ &\to \mathrm{Ext}_{\mathbf{Z}[1/N],p^n}\left(\mu_{p^n}^{(2)}, D_n^{(1)}\right). \end{aligned} \tag{6}$$

If $e''$ denotes the class of $\mathcal{E}$ in the middle group, then we have just seen that its image under the second arrow of (6) vanishes. Thus we may find a class $e''' \in \mathrm{Ext}_{\mathbf{Z}[1/N],p^n}((\mathbf{Z}/p^n)^{(2)}, D_n^{(1)})$ mapping to $e''$ under the first arrow of (6). We can construct such a class $e'''$ concretely as follows: Since the image of $e''$ vanishes, we may lift $\mu_{p^n}^{(2)}$ to a subgroup scheme $\mu'$ of $\tilde{\mathcal{E}}$. The quotient $\mathcal{E}/\mu'$ then provides an extension of $(\mathbf{Z}/p^n)^{(2)}$ by $D_n^{(1)}$ whose extension class $e'''$ maps to $e''$. Our assumption on $F$ implies that its image in $E/\mu'$ (the generic fibre of $\mathcal{E}/\mu'$) projects isomorphically onto $(\mathbf{Z}/p^n)^{(2)}$, and thus that inertia at $N$ acts trivially on $E/\mu'$, and so $\mathcal{E}/\mu'$ has a prolongation to a finite flat group scheme over $\mathbf{Z}$ that extends $\mathbf{Z}/p^n$ by $D_n$. Lemma 2.8 shows that any such extension is split, and thus that $e'''$ vanishes. Consequently $e''$ also vanishes, and so $E$ is a split extension, as claimed. □

The preceding two results show that the map (4) is injective for each $n$, as claimed. Passing to the direct limit in $n$ yields an injective map

$$\varinjlim A_n \to \varinjlim B_n. \tag{7}$$

**Lemma 3.8.** *The group* $\varinjlim B_n$ *is finite, of order at most the p-power part of* $(N^2-1)/24$.

*Proof.* It suffices to show that $B_n$ is of order at most the $p$-power part of $(N^2-1)/24$ for sufficiently large values of $n$. Let $\Sigma = \{p, N, \infty\}$, and let $G_\Sigma$ denote the Galois group of the maximal extension of $\mathbf{Q}$ in $\overline{\mathbf{Q}}$ unramified away from the elements of $\Sigma$. Extensions of the form (3) are classified by the Galois cohomology group $H^1(G_\Sigma, \mu_{p^n}^{\otimes -1})$. If such an extension prolongs to an extension of finite flat groups over $\mathbf{Z}_p$, then it is in fact trivial locally at $p$, since the connected group scheme $\mu_{p^n}$ cannot have a non-trivial extension over the étale group scheme $\mathbf{Z}/p^n$. Thus $B_n$ is equal to the kernel of the natural map

$$H^1\big(G_\Sigma, \mu_{p^n}^{\otimes -1}\big) \to H^1\big(G_{\mathbf{Q}_p}, \mu_{p^n}^{\otimes -1}\big).$$

Let $K_n$ denote the extension of $\mathbf{Q}$ obtained by adjoining all $p^n$th roots of unity in $\overline{\mathbf{Q}}$. Let $H$ denote the normal subgroup of $G_\Sigma$ which fixes $K_n$; the quotient $G_\Sigma/H$ is naturally isomorphic to $(\mathbf{Z}/p^n)^\times$. The prime $p$ is totally ramified in $K_n$. Thus, if $\pi$ denotes the unique prime of $K_n$ lying over $p$, the quotient $G_{\mathbf{Q}_p}/G_{K_{n,\pi}}$ also maps isomorphically to $(\mathbf{Z}/p^n)^\times$. The inflation-restriction exact sequence gives a diagram

$$\begin{array}{ccccccc}
0 \to & H^1\big((\mathbf{Z}/p^n)^\times, \mu_{p^n}^{\otimes -1}\big) & \to & H^1\big(G_\Sigma, \mu_{p^n}^{\otimes -1}\big) & \longrightarrow & H^1\big(H, \mu_{p^n}^{\otimes -1}\big)^{(\mathbf{Z}/p^n)^\times} \\
& \| & & \downarrow & & \downarrow \\
0 \to & H^1\big((\mathbf{Z}/p^n)^\times, \mu_{p^n}^{\otimes -1}\big) & \to & H^1\big(G_{\mathbf{Q}_p}, \mu_{p^n}^{\otimes -1}\big) & \to & H^1\big(G_{K_{n,\pi}}, \mu_{p^n}^{\otimes -1}\big)^{(\mathbf{Z}/p^n)^\times}.
\end{array}$$

Taking into account the discussion of the preceding paragraph, this diagram in turn induces an injection

$$B_n \hookrightarrow \ker\Big(H^1\big(H, \mu_{p^n}^{\otimes -1}\big)^{(\mathbf{Z}/p^n)^\times} \to H^1\big(G_{K_{n,\pi}}, \mu_{p^n}^{\otimes -1}\big)^{(\mathbf{Z}/p^n)^\times}\Big).$$

Since $H$ acts trivially on $\mu_{p^n}^{\otimes -1}$, there is an isomorphism

$$H^1\big(H, \mu_{p^n}^{\otimes -1}\big)^{(\mathbf{Z}/p^n)^\times} \cong \mathrm{Hom}_{(\mathbf{Z}/p^n)^\times}\big(H, \mu_{p^n}^{\otimes -1}\big).$$

Thus $B_n$ injects into the subgroup of $\mathrm{Hom}_{(\mathbf{Z}/p^n)^\times}(H, \mu_{p^n}^{\otimes -1})$ consisting of homomorphisms that are trivial on $G_{K_{n,\pi}}$.

Any element of $\mathrm{Hom}_{(\mathbf{Z}/p^n)^\times}(H, \mu_{p^n}^{\otimes -1})$ that is trivial on $G_{K_{n,\pi}}$ factors through the Galois group $\mathrm{Gal}(L_n/K_n)$, where $L_n$ is the extension of $K_n$ defined in the statement of the following lemma. Lemma 3.8 is now seen to follow from the conclusion of that lemma. □

**Lemma 3.9.** *Let $L_n$ denote the maximal abelian extension of $K_n$ of exponent dividing $p^n$ that is unramified away from $N$, in which the prime lying over $p$ splits completely, and on whose Galois group $(\mathbf{Z}/p^n)^\times = \mathrm{Gal}(K_n/\mathbf{Q})$ acts via $\chi_p^{-1}$. Then $L_n$ is a cyclic extension of $K_n$, and the degree $[L_n : K_n]$ divides the $p$-power part of $(N^2-1)/24$.*

*Proof.* In the following proof, for an abelian group $G$, let $G/\{m\} = G/G^m$ denote the quotient of $G$ by all $m$th powers in $G$. For integers $a$, $b$ let $G/\{(a,b)\} = G/\{m\}$, where $m$ is the greatest common divisor of $a$ and $b$. Let $\zeta$ be a choice of primitive $p^n$ th root of unity. If $\mathcal{O}_n$ denotes the ring of integers in $K_n$, then $1-\zeta$ generates the unique prime ideal of $\mathcal{O}_n$ lying above $p$. Let $((\mathcal{O}_n/N)^\times/\{p^n\})_{(-1)}$ denote the maximal quotient of $(\mathcal{O}_n/N)^\times/\{p^n\}$ on which $\mathrm{Gal}(K_n/\mathbf{Q})$ acts via $\chi_p^{-1}$. Since Herbrand's criterion shows that the $\chi_p^{-1}$-eigenspace in the $p$-part of the class group of $K_n$ vanishes, global class field theory shows that the Galois group of $L_n/K_n$ is equal to the cokernel of the composite

$$\mathcal{O}_n[(1-\zeta)^{-1}]^\times \to (\mathcal{O}_n/N)^\times \to \left((\mathcal{O}_n/N)^\times/\{p^n\}\right)_{(-1)}.$$

Fix a prime $\mathfrak{n}$ of $K_n$ lying over $N$. We first claim that the injection $(\mathcal{O}_n/\mathfrak{n})^\times \hookrightarrow (\mathcal{O}_n/N)^\times$ (coming from the Chinese remainder theorem) induces an isomorphism

$$(\mathcal{O}_n/\mathfrak{n})^\times/\{(p^n, N^2-1)\} \cong \left((\mathcal{O}_n/N)^\times/\{p^n\}\right)_{(-1)}. \tag{8}$$

To see this, we first recall that $\chi_p$ induces an isomorphism $\mathrm{Gal}(K_n/\mathbf{Q}) \cong (\mathbf{Z}/p^n)^\times$; we will write $\sigma_a$ to denote the Galois element corresponding to $a \in (\mathbf{Z}/p^n)^\times$ via $\chi_p$. The group $\mathrm{Gal}(K_n/\mathbf{Q})$ acts transitively on the primes of $K_n$ lying over $N$, and the stabilizer of any one of these primes (and so in particular of $\mathfrak{n}$) is identified by $\chi_p$ with the cyclic subgroup $\langle N\rangle$ generated by $N$ of $(\mathbf{Z}/p^n)^\times$. Thus if $\{a_1, \dots, a_r\}$ is a set of coset representatives for $\langle N\rangle$ in $\mathbf{Z}/p^n$ (labelled so that $a_1$ represents the identity coset), then (taking into account that $\{a_1^{-1}, \dots, a_r^{-1}\}$ also gives a set of coset representatives) the Chinese remainder theorem provides an isomorphism

$$\prod_{i=1}^{r} (\mathcal{O}_n/\sigma_{a_i^{-1}}(\mathfrak{n}))^\times \cong (\mathcal{O}_n/N)^\times. \tag{9}$$

If $x, y \in (\mathcal{O}_n/N)^\times/p^n$, write $x \sim y$ if $x$ and $y$ have the same image in $((\mathcal{O}_n/N)^\times/\{p^n\})_{(-1)}$. Using the isomorphism (9) to write $x = (x_1, \dots, x_r)$, with $x_i \in (\mathcal{O}_n/\sigma_{a_i^{-1}}(\mathfrak{n}))^\times/\{p^n\}$, we see that

$$x = (x_1, \dots, x_r) \sim \Big(\prod_{i=1}^{r} \sigma_{a_i}(x_i)^{a_i}, 1, \dots, 1\Big).$$

Taking into account the fact that $\sigma_N$ acts on $(\mathcal{O}_n/N)^\times$ as the Frobenius automorphism, i.e. via raising to $N$th powers, we see that (8) is indeed an isomorphism, and that the inverse isomorphism is given by the map

$$\begin{aligned} &\text{image of } x = (x_1, \dots, x_r) \text{ in } ((\mathcal{O}_n/N)/p^n)_{(-1)} \\ &\qquad \mapsto \text{image of } \prod_{i=1}^{r} \sigma_{a_i}(x_i)^{a_i} \text{ in } (\mathcal{O}_n/\mathfrak{n})^\times/\{(p^n, N^2-1)\}. \end{aligned} \tag{10}$$

Of course, this map is independent of the particular choice of coset representatives $\{a_i\}$.

Since $(\mathcal{O}_n/\mathfrak{n})^\times$ is a cyclic group, the isomorphism (8) shows that $((\mathcal{O}_n/N)^\times/\{p^n\})_{(-1)}$ has order bounded by the $p$-part of $N^2-1$. Thus if $p \geq 5$ the lemma is proved.

We now perform a more refined analysis, which will prove the lemma in the remaining cases (i.e. $p = 2$ or 3). The formula (10) shows that under the isomorphism (8), the subgroup of

$$((\mathcal{O}_n/N)^\times/\{p^n\})_{(-1)}$$

generated by $(1-\zeta)$ corresponds to the subgroup of $(\mathcal{O}_n/\mathfrak{n})^\times/\{(p^n, N^2-1)\}$ generated by

$$\prod_{a\in(\mathbf{Z}/p^n)^\times/\langle N\rangle} (1-\zeta^a)^a.$$

(Here and below, in expressions such as this, we will suppress the particular choice of coset representatives for elements of $(\mathbf{Z}/p^n)^\times/\langle N\rangle$; the product is well-defined as an element of $(\mathcal{O}_n/\mathfrak{n})^\times/\{(p^n, N^2-1)\}$, independently of this choice.)

Suppose first that $p$ is odd, and write $N = \omega(N)N_1$ in $\mathbf{Z}_p$, where $\omega(N)$ is the Teichmüller lift and $N_1$ is a 1-unit. Let $c$ denote the order of $(\mathbf{Z}/p)/\langle\omega(N)\rangle$; note that $c$ is prime to $p$. If $p^f$ denotes the exact power of $p$ dividing $N^2-1$, and $p^{f'}$ denotes the exact power of $p$ dividing $N_1-1$, then $f' \geq f$, with equality if $p = 3$. Let us assume that $n \geq f'$, so that $(\mathcal{O}_n/\mathfrak{n})^\times/\{(p^n, N^2-1)\}$ is cyclic of order $p^f$, generated by the image of $\zeta$, or of $-\zeta$.

Since $2c$ is prime to $p$, the subgroup of $(\mathcal{O}_n/\mathfrak{n})^\times/\{(p^n, N^2-1)\}$ generated by

$$\prod_{a\in(\mathbf{Z}/p^n)^\times/\langle N\rangle} (1-\zeta^a)^a$$

coincides with the subgroup generated by

$$\left(\prod_{a\in(\mathbf{Z}/p^n)^\times/\langle N\rangle} (1-\zeta^a)^a\right)^{2c} = \left(\prod_{a\in(\mathbf{Z}/p^n)^\times/\langle N_1\rangle} (1-\zeta^a)^a\right)^2$$

$$= \prod_{a\in(\mathbf{Z}/p^n)^\times/\langle N_1\rangle} (1-\zeta^a)^a(1-\zeta^{-a})^{-a} = \prod_{a\in(\mathbf{Z}/p^{f'})^\times} (-\zeta)^{a^2}.$$

(The above expressions are all well-defined as elements of, and the equalities all hold in, the quotient $(\mathcal{O}_n/\mathfrak{n})^\times/\{(p^n, N^2-1)\}$.)

If $p \geq 5$, then since there are quadratic residues distinct from 1 in $(\mathbf{Z}/p)^\times$, we compute that $\sum_{a\in(\mathbf{Z}/p^{f'})^\times} a^2 \equiv 0 \bmod p^{f'}$, and so $\prod_{a\in(\mathbf{Z}/p^n)^\times/\langle N\rangle}(1-\zeta^a)^a$ generates the trivial subgroup of the group $(\mathcal{O}_n/\mathfrak{n})^\times/\{(p^n, N^2-1)\}$. In this case, our "refined analysis" adds no further

restrictions to the degree of $L_n$ over $K_n$. However, if $p = 3$, then 1 is the only quadratic residue in $(\mathbf{Z}/3)^\times$, and one computes that the power of 3 dividing $\sum_{a\in(\mathbf{Z}/p^{f'})^\times} a^2$ is exactly $3^{f'-1} = 3^{f-1}$. Thus we find that the degree $[L_n : K_n]$ is bounded above by $3^{f-1}$. This is the exact power of 3 dividing $(N^2-1)/24$, and thus we have proved the lemma in the case $p = 3$.

Suppose now that $p = 2$. Write $N = \pm 1 \cdot N_1$, where $N_1 \equiv 1 \mod 4$. Let $2^f$ be the exact power of 2 dividing $N^2 - 1$, and let $2^{f'}$ be the exact power of 2 dividing $N_1 - 1$. Note that $f = f' + 1$. Also, assume that $n \geq f$. In particular, $n \geq 2$, and so $-\zeta$ is also a primitive $2^n$th root of unity. The quotient $(\mathcal{O}_n/\mathfrak{n})^\times/\{(2^n, N^2-1)\}$ is then cyclic of order $2^f$, generated by $\zeta$, or by $-\zeta$.

We may rewrite $\prod_{a\in(\mathbf{Z}/2^n)^\times/\langle N\rangle}(1-\zeta^a)^a$ in the form

$$\prod_{a\in(\mathbf{Z}/2^n)^\times/\langle N\rangle}(1-\zeta^a)^a = \prod_{a\in(1+4\mathbf{Z}/2^n)/\langle N_1\rangle}(1-\zeta^a)^a(1-\zeta^{-a})^{-a}$$
$$= \prod_{a\in(1+4\mathbf{Z}/2^n)/(1+2^{f'}\mathbf{Z}/2^n)}(-\zeta)^{a^2}.$$

(The above expressions are all well-defined as elements of, and the equalities all hold in, the quotient $(\mathcal{O}_n/\mathfrak{n})^\times/\{(2^n, N^2-1)\}$.) One computes that the largest power of 2 dividing $\sum_{a\in(1+4\mathbf{Z}/2^n)/(1+2^{f'}\mathbf{Z}/2^n)} a^2$ is $2^{f'-2} = 2^{f-3}$. Thus the degree $[L_n : K_n]$ is bounded above by $2^{f-3}$. This is the exact power of 2 dividing $(N^2-1)/24$, and so we have proved the lemma in the case $p = 2$. □

*Conclusion of proof of Theorem 3.5:* The theorem follows from the isomorphism (2), the injectivity of (7), and Lemma 3.8. □

The reduced Zariski tangent space of the deformation ring $R$ can be computed via a calculation similar to that used to prove Theorem 3.5. We state the result here, but postpone the details of the calculation to the following sections. (See Proposition 4.11 for the case $p = 2$, and Proposition 5.5 for the case of odd $p$.)

**Proposition 3.10.** *If $\mathfrak{p}$ denotes the maximal ideal of $R$, then the reduced Zariski tangent space $\mathfrak{p}/(\mathfrak{p}^2, p)$ of $R$ is of dimension at most one over $\mathbf{F}_p$. More precisely, $\mathfrak{p}/(\mathfrak{p}^2, p)$ vanishes unless $p$ divides the numerator of $(N-1)/12$, in which case it has dimension one over $\mathbf{F}_p$.*

Having introduced the deformation ring $R$, we now turn to constructing the corresponding Hecke ring $\mathbf{T}$. We consider the space $M_2(N)$ of all modular forms of weight two on $\Gamma_0(N)$ defined over $\overline{\mathbf{Q}}_p$, and the commutative $\mathbf{Z}_p$-algebra $H$ of endomorphisms of $M_2(N)$ generated by the Hecke operators $T_n$. We define the $p$-Eisenstein maximal ideal of the algebra $H$ to be the ideal generated by the elements $T_n - \sigma^*(n)$ (where $\sigma^*(n) = \sum_{\substack{0<d|n\\(d,N)=1}} d$

for any positive integer $n$) together with the prime $p$, and let $\mathbf{T}$ denote the completion of $H$ at its $p$-Eisenstein maximal ideal. Then $\mathbf{T}$ is a reduced $\mathbf{Z}_p$-algebra. We let $J$ denote the kernel of the surjection $\mathbf{T} \to \mathbf{Z}_p$ describing the action of $\mathbf{T}$ on the Eisenstein series $E_2^*$, where

$$E_2^* = 1 - N - 24 \sum_{n=1}^{\infty} q^n \sigma^*(n).$$

Let $\mathbf{T}^0$ denote the quotient of $\mathbf{T}$ that acts faithfully on cuspforms, and let $J^0$ denote the image of $J$ in $\mathbf{T}^0$. (This is the localization at $p$ of the famous Eisenstein ideal of [7].)

**Lemma 3.11.** *The order of* $\mathbf{T}^0/J^0$ (*which is a power of* $p$) *is equal to the* $p$*-power part of the numerator of* $(N-1)/12$.

*Proof.* This is Proposition II.9.7 of [7]. □

**Proposition 3.12.** *There is an object* $(V, L, \rho)$ *of* $\mathrm{Def}(\mathbf{T})$*, uniquely determined by the property that* $\mathrm{Trace}(\rho(\mathrm{Frob}_\ell)) = T_\ell$*, for* $\ell \neq p, N$*. Furthermore, the diagram*

$$\begin{array}{ccc} R & \longrightarrow & \mathbf{T} \\ \downarrow & & \downarrow \\ R/I & = & \mathbf{Z}_p & = & \mathbf{T}/J \end{array}$$

*is commutative.*

*Proof.* Since, by Corollary 3.4, the universal deformation ring $R$ is topologically generated by the traces $\mathrm{Trace}(\rho^{\mathrm{univ}}(\mathrm{Frob}_\ell))$, there is at most one object $(V, L, \rho)$ of $\mathrm{Def}(\mathbf{T})$ satisfying the condition $\mathrm{Trace}(\rho(\mathrm{Frob}_\ell)) = T_\ell$ for $\ell \neq p, N$. This gives the uniqueness statement of the proposition. In order to construct the required object $(V, L, \rho)$, we proceed in several steps.

**Lemma 3.13.** *Let* $\overline{V}'$ *be a two dimensional discrete* $G_{\mathbf{Q}}$*-module over a finite extension* $k$ *of* $\mathbf{F}_p$*. Suppose that* $\overline{V}'$ *is finite at* $p$*, unramified away from* $p$ *and* $N$*, contains an* $I_N$*-fixed line that is* not $G_{\mathbf{Q}}$*-stable, and has semi-simplification isomorphic to the semi-simplification of* $k \otimes_{\mathbf{F}_p} \overline{V}$*. Then* $\overline{V}' \cong k \otimes_{\mathbf{F}_p} \overline{V}$.

*Proof.* Since $\overline{V}'$ and $k \otimes_{\mathbf{F}_p} \overline{V}$ have isomorphic semi-simplifications, we see that $\overline{V}'$ is an extension of one of $k \otimes_{\mathbf{F}_p} \mu_p$ or $k \otimes_{\mathbf{F}_p} \mathbf{Z}/p$ (thought of as étale groups schemes over $\mathbf{Q}$, or equivalently as $G_{\mathbf{Q}}$-representations) by the other. Both these one dimensional representations are unramified at $N$, and $\overline{V}'$ contains one or the other as a $G_{\mathbf{Q}}$-submodule. It also contains an $I_N$-fixed line which is *not* a $G_{\mathbf{Q}}$-submodule. Thus $\overline{V}'$ is in fact spanned by $I_N$-fixed

lines, and so is unramified at $N$. By assumption it is finite at $p$, and so it has a prolongation to a finite flat group scheme over $\mathbf{Z}$.

If $p$ is odd, then $\overline{V}$ must prolong to an extension of one of $k \otimes_{\mathbf{F}_p} \mu_p$ or $k \otimes_{\mathbf{F}_p} \mathbf{Z}/p$ by the other as a group scheme over $\operatorname{Spec} \mathbf{Z}$ (since by [2], Thm. 2, $p$-power order group schemes over $\mathbf{Z}$ are determined by their associated Galois representations). There are no such non-trivial extensions ([7], Ch. I for $k = \mathbf{F}_p$, from which the result can easily be deduced), and thus $\overline{V}' \cong k \otimes_{\mathbf{F}_p} \overline{V}$. In the case that $p = 2$, note first that since both $k \otimes_{\mathbf{F}_2} \mu_2$ and $k \otimes_{\mathbf{F}_2} \mathbf{Z}/2$ yield the trivial character of $G_{\mathbf{Q}}$, the module $\overline{V}$ cannot be the direct sum of these two characters; if it were, every line (including the $I_N$-fixed line appearing in the statement of the lemma) would be $G_{\mathbf{Q}}$-stable. Taking this into account, it is easily seen (again using the results of [7], Ch. I) that $\overline{V}' \cong k \otimes_{\mathbf{F}_2} \overline{V}$. □

**Lemma 3.14.** *Let $K$ be a finite extension of $\mathbf{Q}_p$, with ring of integers $\mathcal{O}$. Let $k$ denote the residue field of $\mathcal{O}$, and let $\mathcal{O}'$ denote the order in $\mathcal{O}$ consisting of elements whose image in $k$ lies in the prime subfield $\mathbf{F}_p$ of $k$. Suppose one is given a two dimensional $K$-vector space $W$, and a continuous representation $G_{\mathbf{Q}} \to \mathrm{GL}(W)$ that is finite at $p$ (in the sense that one, or equivalently any, $G_{\mathbf{Q}}$-invariant $\mathcal{O}$-lattice in $W$ is finite at $p$), semistable at $N$ (in the sense that $W$ contains an $I_N$-fixed line), unramified away from $p$ and $N$, such that the semi-simple residual representation attached to $W$ is isomorphic to the direct sum of the trivial character and the mod $p$ cyclotomic character.*

*If $W$ is irreducible, then we may find a free $\mathcal{O}'$-module of rank two $V$, equipped with a continuous representation $\rho : G_{\mathbf{Q}} \to \mathrm{GL}(V)$, and containing an $I_N$-fixed line $L$, such that the triple $(V, L, \rho)$ deforms $(\overline{V}, \overline{L}, \overline{\rho})$, and such that $K \otimes_{\mathcal{O}'} V \cong W$ as $G_{\mathbf{Q}}$-modules.*

*Proof.* Choose any $G_{\mathbf{Q}}$-stable lattice $V'$ in $W$, and let $L'$ denote the intersection of $V'$ with the $I_N$-fixed line in $W$. Since $W$ is irreducible, the line $L'$ is not $G_{\mathbf{Q}}$-stable. Thus we may find a non-negative integer $n$ such that $L'/p^n$ is $G_{\mathbf{Q}}$-stable in $V'/p^n$, but such that $L'/p^{n+1}$ is *not* $G_{\mathbf{Q}}$-stable in $V'/p^{n+1}$. If we define $V''$ to be the preimage in $V'$ of $L'/p^n$, then we see that $L'/p$, when regarded as a subspace of $V''/p$, is not $G_{\mathbf{Q}}$-stable. Lemma 3.13 implies that $V''/p \cong k \otimes_{\mathbf{F}_p} \overline{V}$. Using the description of the automorphisms of $k \otimes_{\mathbf{F}_p} \overline{V}$ afforded by Lemma 2.12, we deduce easily that in fact there is an isomorphism of pairs $(V''/p, L'/p) \cong k \otimes_{\mathbf{F}_p} (\overline{V}, \overline{L})$. If we choose a basis for $(V'', L')$ over $\mathcal{O}$ that reduces to an $\mathbf{F}_p$ basis for $(\overline{V}, \overline{L})$, then the $\mathcal{O}'$-span of this basis gives rise to the required pair $(V, L)$. □

If $\widetilde{\mathbf{T}}$ denotes the normalization of $\mathbf{T}$, then we may write $\widetilde{\mathbf{T}} = \prod_{i=1}^{d} \mathcal{O}_i$, where each $\mathcal{O}_i$ is a discrete valuation ring, of finite index over $\mathbf{Z}_p$. The rings $\mathcal{O}_i$ are in bijection with the conjugacy classes of normalized eigenforms $f_i$ in $M_2(N)$ that satisfy the congruence $f_i \equiv E_2^* \mod \mathfrak{p}_i$ (where $\mathfrak{p}_i$ denotes the maximal ideal of $\mathcal{O}_i$); as before, $E_2^*$ denotes the weight two Eisenstein

series on $\Gamma_0(N)$. The ring $\mathcal{O}_i$ is the ring of integers in the subfield of $\overline{\mathbf{Q}}_p$ generated by the Fourier coefficients of $f_i$. The injection $\mathbf{T} \to \widetilde{\mathbf{T}} = \prod_{i=1}^{d} \mathcal{O}_i$ is characterised by the property $T_n \mapsto (a_n(f_i))_{i=1,\dots,d}$. Note that $E_2^*$ is one such form $f_i$. We may choose the labeling so that $E_2^* = f_1$; then $\mathcal{O}_1 = \mathbf{Z}_p = \mathbf{T}/J$.

As in the statement of Lemma 3.14, for each $i = 1, \dots, d$, define $\mathcal{O}_i'$ to be the order in $\mathcal{O}_i$ obtained as the preimage under the map to the residue field of the prime subfield $\mathbf{F}_p$. By construction $\mathcal{O}_i'$ is a complete Noetherian local ring with residue field $\mathbf{F}_p$. Also, the natural map $\mathbf{T} \to \mathcal{O}_i$ factors through $\mathcal{O}_i'$.

**Lemma 3.15.** *For each $i = 1, \dots, d$, we may construct an object $(V_i, L_i, \rho_i) \in \mathrm{Def}(\mathcal{O}_i')$ with the property that $\mathrm{Trace}(\rho_i(\mathrm{Frob}_\ell))$ is equal to the image of $T_\ell$ in $\mathcal{O}_i'$, for each $\ell \neq p, N$.*

*Proof.* If $i = 1$, so that $\mathcal{O}_i' = \mathbf{Z}_p$, we take $(V_1, L_1, \rho_1)$ to be the triple $(V^{\min}, L^{\min}, \rho^{\min})$. Suppose now that $i \geq 2$, so that $\mathcal{O}_i$ corresponds to a cuspform $f_i$. If we consider the usual irreducible Galois representation into $\mathrm{GL}_2(\mathbf{Q}_p \otimes_{\mathbf{Z}_p} \mathcal{O}_i)$ attached to $f_i$, and apply Lemma 3.14, then we again obtain the required triple. □

*Conclusion of proof of Proposition 3.12:* Each of the triples $(V_i, L_i, \rho_i)$ constructed in the previous lemma corresponds to a homomorphism $\phi_i : R \to \mathcal{O}_i'$. The product of all these yields a homomorphism $\phi : R \to \prod_{i=1}^{d} \mathcal{O}_i'$. Since $R$ is topologically generated by the elements $\mathrm{Trace}(\rho^{\mathrm{univ}}(\mathrm{Frob}_\ell))$ $(\ell \neq p, N)$, we see that $\phi$ factors through $\mathbf{T}$. The map $\phi$ in turn corresponds to a triple $(V, L, \rho) \in \mathrm{Def}(\mathbf{T})$, satisfying the requirements of the proposition. By construction, the diagram appearing in the statement of the proposition commutes. □

Let $\mathbf{T}'$ denote the image in $\mathbf{T}$ of the map constructed in Proposition 3.12. Our ultimate goal is to prove that this map is an isomorphism, and so in particular that $\mathbf{T}' = \mathbf{T}$. However, we will proceed in stages.

Write $J' = \mathbf{T}' \bigcap J$, let $(\mathbf{T}')^0$ denote the image of $\mathbf{T}'$ in $\mathbf{T}^0$, and let $(J')^0$ denote the image of $J'$ in $(\mathbf{T}')^0$. We have the morphism of short exact sequences

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbf{T}' & \longrightarrow & \mathbf{Z}_p \bigoplus (\mathbf{T}')^0 & \xrightarrow{(x,y)\mapsto x-y} & (\mathbf{T}')^0/(J')^0 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathbf{T} & \longrightarrow & \mathbf{Z}_p \bigoplus \mathbf{T}^0 & \xrightarrow{(x,y)\mapsto x-y} & \mathbf{T}^0/J^0 & \longrightarrow & 0.
\end{array}$$

Applying the snake lemma we obtain the following exact sequence:

$$\begin{aligned}
0 \longrightarrow \ker((\mathbf{T}')^0/(J')^0 \to \mathbf{T}^0/J^0) \longrightarrow \mathrm{coker}(\mathbf{T}' \to \mathbf{T}) \\
\longrightarrow \mathrm{coker}((\mathbf{T}')^0 \to \mathbf{T}^0) \longrightarrow \mathrm{coker}((\mathbf{T}')^0/(J')^0 \to \mathbf{T}^0/J^0) \longrightarrow 0.
\end{aligned}$$

We also have the following tautological exact sequence:

$$0 \longrightarrow \ker((\mathbf{T}')^0/(J')^0 \to \mathbf{T}^0/J^0) \longrightarrow (\mathbf{T}')^0/(J')^0 \\ \longrightarrow \mathbf{T}^0/J^0 \longrightarrow \operatorname{coker}((\mathbf{T}')^0/(J')^0 \to \mathbf{T}^0/J^0) \longrightarrow 0.$$

Thus we find that

$$\#(\mathbf{T}')^0/(J')^0 - \#(\mathbf{T}^0/J^0) = \#\operatorname{coker}(\mathbf{T}' \to \mathbf{T}) - \#\operatorname{coker}((\mathbf{T}')^0 \to \mathbf{T}^0). \tag{11}$$

Since $\mathbf{T} \to \mathbf{T}^0$ is surjective, we conclude that the right hand side of (11) is non-negative, and thus that the order of $(\mathbf{T}')^0/(J')^0$ is at least equal to that of $\mathbf{T}^0/J^0$. By Lemma 3.11, the order of this latter group has order equal to the $p$-power part of the numerator of $(N-1)/12$. Thus the order of $(\mathbf{T}')^0/(J')^0$ is at least equal to this number.

Suppose now that $N \not\equiv -1 \mod 2p$. The $p$-power part of $(N^2-1)/24$ is then equal to the $p$-power part of the numerator of $(N-1)/12$. Theorem 3.5 thus shows that the numerical criterion of [17] (as strengthened in [6]) applies to prove that the surjection $R \to \mathbf{T}'$ of the preceding proposition is an isomorphism of local complete intersections. Furthermore, we conclude that in fact $(\mathbf{T}')^0/(J')^0$ has order exactly equal to the power of $p$ dividing the numerator of $(N-1)/12$, that is, to the order of $\mathbf{T}^0/J^0$. The equation (11) then shows that $\mathbf{T}' = \mathbf{T}$ if and only if $(\mathbf{T}')^0 = \mathbf{T}^0$.

**Lemma 3.16.** *The inclusion $\mathbf{T}' \to \mathbf{T}$ is an isomorphism.*

*Proof.* It follows from Corollary 3.4, together with the construction of the map $R \to \mathbf{T}$ of Proposition 3.12, that $\mathbf{T}'$ contains $T_\ell$ for all $\ell \neq N, p$. Proposition 2.10 shows that $\rho^{\mathrm{univ}}$ has a rank one space of $I_p$-coinvariants, on which $\mathrm{Frob}_p$ then acts as multiplication by a unit. It follows from the construction of $R \to \mathbf{T}$, and the known structure of Galois representations attached to weight two modular forms, that the image of this unit in $\mathbf{T}$ is equal to the Hecke operator $T_p$. Thus $\mathbf{T}'$ contains $T_p$.

It remains to show that $T_N$ lies in $\mathbf{T}'$. By the remark preceding the statement of the lemma, it in fact suffices to show that $T_N$ lies in $(\mathbf{T}')^0$. The surjection $R \to (\mathbf{T}')^0$ induces an object $(V^0, L^0, \rho^0) \in \mathrm{Def}((\mathbf{T}')^0)$. The concrete construction of the map $R \to \mathbf{T}$ (and hence the map $R \to \mathbf{T}^0$) shows that this representation is built out of Galois representations attached to weight two cuspforms on $\Gamma_0(N)$, which are (so to speak) genuinely semi-stable at $N$. In particular, the line $L^0$ is not only fixed by $I_N$, but is stable under the decomposition group at $N$. Standard properties of Galois representations attached to weight two cusp forms show that the eigenvalue of $\mathrm{Frob}_N$ on this line is furthermore equal to $T_N$. Thus $T_N \in (\mathbf{T}')^0$, and so we see that $(\mathbf{T}')^0 = \mathbf{T}^0$, as required. □

The preceding lemma completes the proof of Theorem 1.5 in the case when $N \not\equiv -1 \mod 2p$. If, on the other hand, we have $N \equiv -1 \mod 2p$,

then Proposition 3.10 shows that the Zariski tangent space of $R$ is trivial. In this case, the map $R \to \mathbf{Z}_p$ is an isomorphism. Also, Lemma 3.11 then implies that $\mathbf{T}^0 = 0$, and hence that $\mathbf{T} = \mathbf{Z}_p$. Thus the map $R \to \mathbf{T}$ is certainly an isomorphism in this case, and we have completely proved Theorem 1.5 of the introduction.

Let us make two remarks:

(A) An alternative approach to proving Proposition 3.12 is as follows. The results of [7], Sect. II.16, show that if $V^0$ denotes the $p$-Eisenstein part of the $p$-adic Tate module of $J_0(N)$, then $V^0$ is free of rank two over $\mathbf{T}^0$, and the $G_{\mathbf{Q}}$-action on $V^0$ yields a deformation $\rho^0$ of $\overline{\rho}$ over $\mathbf{T}^0$. The $I_N$-invariants in this representation form a rank one free submodule $L^0$ of this representation. The discussion of [7], Sect. II.11 shows that both the cuspidal and Shimura subgroup map isomorphically onto the connected component group of the fibre over $N$ of the Néron model of $J_0(N)$, and this in turn implies that $(V^0, L^0, \rho^0)$ provides an object of $\mathrm{Def}(\mathbf{T}^0)$. Thus we obtain a corresponding map $R \to \mathbf{T}^0$. Taking the product of this with the map $R \to R/I = \mathbf{Z}_p$, we obtain the required map $R \to \mathbf{T}$ of Proposition 3.12. Finally, the explicit description of $\mathbf{T}^0$ provided by [7], Cor. II.16.2 assures us that the map $R \to \mathbf{T}$ is surjective.

We have chosen to present the alternative argument above both because it is more elementary (the only ingredient required from [7], Ch. II, is the computation of the order of $\mathbf{T}^0/J^0$), and because we are then able to recover the results of [7], Sects. II.16, II.17, as we explain below.

(B) In the proof of Lemma 3.16, we have struggled slightly to prove that $T_N$ in fact lies in $\mathbf{T}'$. This is somewhat amusing, since actually $T_N = 1$ in $\mathbf{T}$! This follows from [7], Prop. II.17.10. When $p$ is odd, the argument is straightforward: namely, since $T_N^2 = 1$ for general reasons (the Galois representations attached to modular forms of weight two on $\Gamma_0(N)$ are semi-stable at $N$ and Cartier self-dual), it suffices to note that $T_N \equiv 1$ modulo the maximal ideal of $\mathbf{T}$. When $p = 2$, Mazur's proof of this result depends on his detailed analysis of the 2-Eisenstein torsion in $J_0(N)$. We present an alternative proof below, using the deformation theoretic techniques of this paper.

We close this section by explaining how Theorem 1.5 allows us to recover the main results of Sect. II of [7].

**Corollary 3.17.** *The $\mathbf{Z}_p$-algebra $\mathbf{T}$ (and consequently also its quotient $\mathbf{T}^0$) is generated by a* single *element over $\mathbf{Z}_p$. In particular, both $\mathbf{T}$ and $\mathbf{T}^0$ are local complete intersections, and hence Gorenstein.*

*Proof.* Theorem 1.5 shows that it suffices to verify the analogous statement for the deformation ring $R$. Proposition 3.10 shows that if $\mathfrak{p}$ denotes the maximal ideal of $R$, then $\mathfrak{p}/(\mathfrak{p}^2, p)$ has dimension at most one over $\mathbf{F}_p$, and the corollary follows. □

The fact that $\mathbf{T}^0$ is monogenic over $\mathbf{Z}_p$ was originally proved by Mazur ([7], Cor. 16.2). Since $\mathbf{T}$ is reduced, finite flat, and monogenic over $\mathbf{Z}_p$, and is equipped with a map $\mathbf{T} \to \mathbf{T}/J \cong \mathbf{Z}_p$, we see that we may write $\mathbf{T} \cong \mathbf{Z}_p[X]/Xf(X)$, where $X$ generates the ideal $J$ in $\mathbf{T}$, the monic polynomial $f(X) \in \mathbf{Z}_p[X]$ satisfies $f(X) \equiv X^{g_p} \mod p$, and there is an isomorphism $\mathbf{T}^0 \cong \mathbf{Z}_p[X]/f(X)$. (Here we follow [7] in letting $g_p$ denote the rank of $\mathbf{T}^0$ over $\mathbf{Z}_p$.) The image of $X$ in $\mathbf{Z}_p[X]/f(X)$ generates the ideal $J^0$ in $\mathbf{T}^0$.

In [7], Prop. II.18.10, Mazur treats the questions of exhibiting explicit generators of $J^0$ (or equivalently, explicit choices for the element "$X$" of the preceding paragraph). We recall his result here, and give a deformation-theoretic proof.

**Proposition 3.18.** *Suppose that $p$ divides the numerator of $(N-1)/12$. Let $\ell$ be a prime different from $N$. Say that $\ell$ is* good *(with respect to the pair $(p, N)$) if (i) one of $\ell$ or $p$ is odd, $\ell$ is not a $p$th power modulo $N$, and $(\ell-1)/2 \not\equiv 0 \mod p$ (note that this last expression makes sense, since either $\ell$ is odd, in which case $(\ell-1)/2$ is an integer, or else $p$ is odd, in which case $1/2$ is well-defined modulo $p$); or (ii) $\ell = p = 2$ and $-4$ is not an 8th power modulo $N$.*[2] *Then $T_\ell - (1+\ell)$ generates the ideal $J^0$ if and only if $\ell$ is a good prime.*

*Proof.* Let $R \cong \mathbf{T} \to \mathbf{F}_p[X]/X^2$ be a map that classifies a (unique up to scaling, by Proposition 3.10) non-trivial element in the reduced Zariski tangent space of $R$. If $\ell$ is distinct from $p$, then we must show that $T_\ell - (1+\ell) = \mathrm{Trace}(\rho^{\mathrm{univ}}(\mathrm{Frob}_\ell)) - (1+\ell)$ has non-zero image under this map if and only if $\ell$ is a good prime. If $\alpha_p \in R \cong \mathbf{T}$ denotes the scalar by which $\mathrm{Frob}_p$ acts on the rank one quotient module of $I_p$-coinvariants of $V^{\mathrm{univ}}$, then $T_p = \alpha_p$, and so we must also show that $\alpha_p - (1+p)$ has non-zero image under this map if and only if $p$ is a good prime. Both cases follow from Proposition 4.11 in the case when $p = 2$, and from Proposition 5.5 in the case of odd $p$. □

As was remarked upon above, the next result (and the final result of this section) is also originally due to Mazur.

**Proposition 3.19.** *In* $\mathbf{T}$ *we have the equality $T_N = 1$.*

---

[2] This definition originally appeared in [7], p. 124. However, condition (ii) is misstated there. In particular, on p. 139 Mazur writes that (for $\ell = 2$ and $\overline{\ell} = x^2 \mod N$)

$$\left(\frac{\ell-1}{2}\right)\varphi(\overline{\ell}) = \varphi(x).$$

In reality this equality is only valid up to an element of $H^+/\mathcal{I}H^+$ killed by 2 (recall there is a non-canonical isomorphism $H^+/\mathcal{I}H^+ \simeq \mathbf{Z}/n\mathbf{Z}$). This ambiguity can not be avoided by replacing $x$ by $-x$, since $\varphi(-1) = 0$. If $4|n$, however, then this equality suffices to determine when $\epsilon^+(2)$ generates the 2-primary subgroup of $H^+/\mathcal{I}H^+$; thus our criterion agrees with Mazur's when $N \equiv 1 \mod 16$.

*Proof.* As we recalled above, this result is straightforward when $p$ is odd. Thus we assume that $p = 2$. The $T_N$-eigenvalue of $E_2^*$ is equal to 1. Thus, in order to show that $T_N = 1$, it suffices to show that for each cuspform $f_i$ ($i = 2, \ldots, d$ – we are using the notation introduced during the proof of Proposition 3.12), the image of $T_N$ in $\mathcal{O}_i$ is equal to 1. If $N \not\equiv 1 \mod 8$, then there are no cuspforms to consider (by Proposition 3.10 and Theorem 1.5, for example, or by Proposition II.9.7 of [7]), and hence there is nothing to prove. Thus we assume for the remainder of the argument that $N \equiv 1 \mod 8$.

Fix a cuspform $f_i$, and let $S$ denote the local ring

$$S = \{(a, b) \in \mathbf{Z}/4 \times \mathcal{O}_i/2\mathfrak{p}_i \mid a \bmod 2 = b \bmod \mathfrak{p}_i\}.$$

The objects $(V_2^{\min}, L_2^{\min}, \rho_2^{\min}) \in \mathrm{Def}(\mathbf{Z}/4)$ and the object in $\mathrm{Def}(\mathcal{O}_i'/2\mathfrak{p}_i)$ obtained by reducing modulo $2\mathfrak{p}_i$ the object $(V_i, L_i, \rho_i) \in \mathrm{Def}(\mathcal{O}_i')$ (the latter was constructed in the course of proving Proposition 3.12) glue to yield an object $(V, L, \rho) \in \mathrm{Def}(S)$. Since $N \equiv 1 \mod 8$, we see that $G_{\mathbf{Q}_N}$ acts trivially on $V_2^{\min}$. Since $(V_i, L_i, \rho_i)$ is constructed from the Galois representation attached to the cuspform $f_i$, we see that $G_{\mathbf{Q}_N}$ stabilizes $L_i$, and $\mathrm{Frob}_N$ acts as multiplication by $T_N$ on $L_i$. Thus the line $L$ is stabilized by $G_{\mathbf{Q}_N}$ (in addition to being fixed by $I_N$), and $\mathrm{Frob}_N$ acts as multiplication by the image of $T_N$ in $S$. If the image of $T_N$ in $\mathcal{O}_i$ is equal to $-1$, then we see that the image of $T_N$ in $S$ is equal to $(1, -1)$. Now $(1, -1) \not\equiv (1, 1) \mod 2S$. Thus the object $(V/2, L/2, \rho/2) \in \mathrm{Def}(S/2)$ obtained by reducing $(V, L, \rho)$ modulo 2 has the property that $L$ is stable, but not trivial, under the action of $G_{\mathbf{Q}_N}$. On the other hand, Theorem 4.4, together with Lemma 4.2, shows that there are no such elements of $\mathrm{Def}(S/2)$. This contradiction proves the proposition. □

## 4. Explicit deformation theory: $p = 2$

Let us begin by fixing an odd prime $N$, and recalling some class field theory of the field $K = \mathbf{Q}(\sqrt{(-1)^{(N+1)/2}N})$. We let $H$ denote the 2-power part of the strict class group $\mathrm{Cl}(\mathcal{O}_K)$ of the ring of integers $\mathcal{O}_K$ of $K$, and let $E$ denote the corresponding cyclic 2-power extension of $K$, which is unramified at all finite primes. Genus theory shows that $H$ is cyclic, and non-trivial. Thus $E$ is a non-trivial cyclic 2-power extension of $K$; its unique quadratic subextension is equal to $K(\sqrt{-1})$. We let $\pi_K$ denote the unique prime of $K$ lying over 2; its image in $H$ generates the two-torsion subgroup $H[2]$ of $H$, if $N \not\equiv -1 \mod 8$.

The following result is classical, but we will recall a proof for the benefit of the reader.

**Proposition 4.1.** *The order of $H$ is divisible by four if and only if $N \equiv 1 \mod 8$. The order of $H$ is divisible by eight if and only if furthermore $-4$ is an 8th power modulo $N$.*

*Proof.* If $N \equiv -1 \mod 4$, then $K$ is a real quadratic field. If $E^+$ denotes the 2-Hilbert class field of $K$ (so $E^+$ is the maximal totally real subextension of $E$), then we see that $E$ is equal to the compositum of $E^+$ and $K(\sqrt{-1})$. Since $E$ is cyclic over $K$, we deduce that $E^+$ must in fact be trivial. Thus in this case $H$ is of order two.

Suppose now that $N \equiv 1 \mod 4$, and that $E$ contains a degree four sub-extension. Since $E/K$ is cyclic, this sub-extension is unique, and hence Galois over $\mathbf{Q}$. It must contain $\mathbf{Q}(\sqrt{-1})$, and one sees easily that it is in fact a biquadratic extension of $\mathbf{Q}(\sqrt{-1})$, unramified away from $N$. Since it is Galois over $\mathbf{Q}$, it must be of the form $\mathbf{Q}(\sqrt{-1}, \sqrt{\nu}, \sqrt{\bar{\nu}})$, where $\nu$ is an element of $\mathbf{Z}[\sqrt{-1}]$ (and $\bar{\nu}$ is its conjugate) satisfying $\nu\bar{\nu} = N$.

However, for the extension $\mathbf{Q}(\sqrt{-1}, \sqrt{\nu}, \sqrt{\bar{\nu}})/\mathbf{Q}(\sqrt{-1})$ to actually be unramified at 2, it must be that $\nu \equiv 1 \mod 4$. The element $\nu$ can be chosen in this manner if and only if $N \equiv 1 \mod 8$. Thus we see that $E$ has a degree four subfield if and only if $N$ satisfies this congruence.

Finally, let us consider the question of whether the order of $H$ is divisible by eight. This is the case if and only if the two-torsion subgroup $H[2]$ of $H$ has trivial image in $H/4$; equivalently, if and only if $\pi_K$ has trivial image in $H/4$. This holds, in turn, if and only if $\pi_K$ splits completely in $\mathbf{Q}(\sqrt{-1}, \sqrt{\nu}, \sqrt{\bar{\nu}})$. Clearly, this is true if and only if the ideal $(1+i)$ splits completely in this field, regarded as an extension of $\mathbf{Q}(\sqrt{-1})$. This holds, in turn, if and only if $(1+i)$ is a quadratic residue modulo $\nu$ (or equivalently module $\bar{\nu}$). Raising to 4th powers, and taking into account the isomorphism $\mathbf{Z}/N \cong \mathbf{Z}[\sqrt{-1}]/\nu$, we see that this is equivalent to $-4$ being an 8th power modulo $N$. □

The following lemma is used in the proof of Proposition 3.19.

**Lemma 4.2.** *If $N \equiv 1 \mod 4$, the inertia group $I_N$ and the decomposition group $G_{\mathbf{Q}_N}$ have the same image in* $\mathrm{Gal}(E/\mathbf{Q})$.

*Proof.* There is a unique prime lying above $N$ in $K$, and it is principal. Thus this prime splits completely in the 2-Hilbert class field $E$ of $K$, and so $I_N$ and $G_{\mathbf{Q}_N}$ both have trivial image in $\mathrm{Gal}(E/K)$. Since $N$ is ramified in $K/\mathbf{Q}$, the lemma follows. □

Let $H'$ denote the 2-power part of the strict ray class group of $K$ of conductor $\pi_K^2$, and let $H''$ denote the 2-power part of the strict ray class group of $K$ of conductor $\pi_K^3$. (Here "strict" means that in the case when $K$ is real quadratic, we allow ramification at infinity.) We let $E'$ and $E''$ denote the corresponding abelian extensions of $K$.

**Proposition 4.3.** *(i) The natural surjection $H'' \to H'$ is an isomorphism.*
*(ii) If $N \equiv -1 \mod 4$, the natural surjection $H' \to H$ is an isomorphism and $E = E'$. If $N \equiv 1 \mod 4$, the kernel of this surjection has order two and $E'/E$ is a quadratic extension that is ramified at two.*

*(iii) The group $H'$ is cyclic.*

*(iv) Let $D_2(E'/\mathbf{Q})$ denote the decomposition group of some prime of $E'$ lying over 2, and let $I_2(E'/\mathbf{Q})$ denote the inertia subgroup of $D_2(E'/\mathbf{Q})$. Then $I_2(E'/\mathbf{Q})$ has index at most two in $D_2(E'/\mathbf{Q})$. If furthermore $E'/E$ is a quadratic extension, then $D_2(E'/\mathbf{Q})$ is dihedral of order 8.*

*Proof.* The groups $H'$ and $H''$ sit inside the following exact diagram:

$$\begin{array}{ccccccc}
\mathcal{O}_K^\times & \longrightarrow & \left(\mathcal{O}_K/\pi_K^3\right)^\times & \longrightarrow & H'' & \longrightarrow & H \longrightarrow 0 \\
\| & & \downarrow{\scriptstyle \psi} & & \downarrow & & \| \\
\mathcal{O}_K^\times & \longrightarrow & \left(\mathcal{O}_K/\pi_K^2\right)^\times & \longrightarrow & H' & \longrightarrow & H \longrightarrow 0.
\end{array}$$

To prove that the map $H'' \to H'$ is an isomorphism, it suffices to show that the kernel of $\psi$ maps to zero in $H''$; in other words, that the kernel of $\psi$ consists of the images of global units. Since $\pi_K^2 = (2)$, we see that the kernel of $\psi$ is equal to $\{\pm 1\}$; this completes the proof of (i).

The proof of (ii) is even more straightforward: it follows immediately from a consideration of the units in $\mathcal{O}_K^\times$ and the exact sequence

$$\mathcal{O}_K^\times \to \left(\mathcal{O}_K/\pi_K^2\right)^\times = (\mathcal{O}_K/2)^\times \to H' \to H \to 0.$$

We now turn to proving (iii). For this, it suffices to prove that $H'/2 \cong \mathbf{Z}/2$. Note that since the non-trivial element of $\mathrm{Gal}(K/\mathbf{Q})$ acts on $H'$ via $h \mapsto h^{-1}$, we see that the extension $K'$ of $K$ corresponding by class field theory to $H'/2$ is abelian over $\mathbf{Q}$. If $H'/2$ were isomorphic to $\mathbf{Z}/2 \oplus \mathbf{Z}/2$ (rather than $\mathbf{Z}/2$), then since $H$ is cyclic, this would imply that there exists a subextension of $K'$, quadratic over $K$ and of conductor 2. Such an extension would again be abelian over $\mathbf{Q}$. Using the Kronecker-Weber theorem, it is easy to check that there are no such quadratic extensions of $K$. Thus $H'$ must be cyclic, as claimed.

If $N \equiv -1 \mod 4$ then $E' = E = K(\sqrt{-1})$ and (iv) is obvious. If $E'/E$ is a quadratic extension, then $N \equiv 1 \mod 4$ and the class of $\pi_K$ has order two in $H$. Thus the decomposition group $D_2(E/K)$ at 2 in the Hilbert class field has order exactly 2. Since $K/\mathbf{Q}$ is ramified at 2, we see that the decomposition group $D_2(E/\mathbf{Q})$ has order four, and that the inertia subgroup $I_2(E/\mathbf{Q})$ has order two. If instead $E'/E$ is quadratic, then $E'/E$ is ramified at 2, implying that $D_2(E'/\mathbf{Q})$ has order 8, and that $I_2(E'/\mathbf{Q})$ has order 4. Since $D_2(E'/K) \subseteq \mathrm{Gal}(E'/K) \cong H'$ is cyclic, by (iii), and since $\mathrm{Gal}(E'/\mathbf{Q})$ is dihedral, it follows that $D_2(E'/\mathbf{Q})$ is dihedral of order 8. □

Let $(V, L, \rho)$ be an object of $\mathrm{Def}(A)$ for some Artinian local $\mathbf{F}_2$-algebra, and let $F$ denote the compositum of $K$ with the fixed field of the kernel of $\rho$. The following result greatly restricts the possibilities for $F$.

**Theorem 4.4.** *The field $F$ is contained in the strict 2-Hilbert class field $E$ of $K$.*

*Proof.* Since $A$ is assumed to be of characteristic 2, the natural map $\mathbf{Z}_2^\times \to A^\times$ has trivial image, and thus the image of $\rho$ is contained in $\mathrm{SL}_2(A)$. Since $I_N$ acts trivially on both $L$ and $V/L$, we deduce that inertia at $N$ acts through an abelian group of exponent 2, and thus through a cyclic group of order at most 2.

**Lemma 4.5.** *The extension $F/K$ is unramified at all finite primes outside $\pi_K$. Moreover, if $K^{ab}/K$ is the maximal abelian extension of $K$ contained in $F$, then the finite part of the conductor of $K^{ab}/K$ divides $\pi_K^3$.*

*Proof.* The Galois group $\mathrm{Gal}(F/\mathbf{Q})$ embeds into $\mathrm{Gal}(K/\mathbf{Q}) \times \rho(G_{\mathbf{Q}})$. In particular, it is of 2-power order, and so the image of an inertia group $I_N$ at $N$ in $\mathrm{Gal}(F/\mathbf{Q})$ is cyclic of two-power order. As observed above, $\rho(I_N)$ is a quotient of $I_N$ of order at most two. On the other hand, since $K/\mathbf{Q}$ is a quadratic extension that is ramified at $N$, we see that $I_N$ surjects onto the order two group $\mathrm{Gal}(K/\mathbf{Q})$. It follows that the image of $I_N$ in $\mathrm{Gal}(F/\mathbf{Q})$ has trivial intersection with $\mathrm{Gal}(F/K)$, and so $F/K$ is unramified at the prime above $N$.

By definition, $\rho$ is unramified outside 2 and $N$, and so it remains to prove the result about the conductor of $K^{ab}/K$. Since the compositum of extensions of conductor dividing $\pi_K^3$ has conductor at most $\pi_K^3$, it suffices to prove the result for extensions $K'/K$ with *cyclic* Galois group. Suppose such an extension $K'/K$ with Galois group $\mathbf{Z}/2^k\mathbf{Z}$ had conductor divisible by $\pi_K^4$. Then the conductor discriminant formula says that the discriminant $\Delta_{K'/K}$ is the product over all characters of $\mathbf{Z}/2^k\mathbf{Z}$ of the corresponding conductor:

$$\Delta_{K'/K} = \prod_\chi \mathfrak{f}_\chi.$$

Since $\mathbf{Z}/2^k\mathbf{Z}$ has exactly $2^{k-1}$ faithful characters, restricting the product to this set we find that the discriminant is divisible by at least $(\pi_K)^{4\cdot 2^{k-1}}$. Recall that the root discriminant of a number field $L/\mathbf{Q}$ is defined to be the positive real number $\delta_L := |\Delta_{L/\mathbf{Q}}|^{1/[L:\mathbf{Q}]}$. Let $\Delta_{L/\mathbf{Q},p}$ be the largest power of $p$ diving $\Delta_{L/\mathbf{Q}}$. Define the $p$-root discriminant $\delta_{L,p}$ of $L/\mathbf{Q}$ to be $|\Delta_{L/\mathbf{Q},p}|^{1/[L:\mathbf{Q}]}$. The divisibility of discriminants proved above implies a lower bound for the 2-root discriminant of $K'$, and thus of $F$. Explicitly,

$$\delta_{F,2} \geq \delta_{K',2} = \delta_{K,2} N_{K/\mathbf{Q}}(\Delta_{K'/K})^{1/[K':\mathbf{Q}]} \geq 2 \cdot 2 = 4.$$

Yet the Fontaine bound ([3], Theorem 1) for finite flat group schemes over $\mathbf{Z}_2$ killed by 2 implies that $\delta_{F,2} < 2^{1+\frac{1}{2-1}} = 4$. Thus the result follows by contradiction. □

We will strengthen this lemma step-by-step, until we eventually establish the theorem.

**Lemma 4.6.** *The extension $F/K$ is cyclic, and is contained in the field $E'$.*

*Proof.* The preceding lemma, together with part (i) of Proposition 4.3, shows that the extension of $K$ cut out by any abelian quotient of $\mathrm{Gal}(F/K)$ is contained in $E'' = E'$. Part (iii) of the same proposition then implies that any such quotient is cyclic. Thus $\mathrm{Gal}(F/K)$ is a 2-group with no non-cyclic abelian quotients, and so is itself cyclic. The result follows. □

We now turn to a more careful study of the ramification at 2. Corollary 2.9 shows that $V_{/\mathbf{Q}_2}$ has a unique prolongation to a finite flat group scheme $M_{/\mathbf{Z}_2}$, that the action of $A$ on $V$ prolongs to an action of $A$ on $M$, and that the connected-étale sequence

$$0 \to M^0 \to M \to M^{\text{ét}} \to 0$$

induces a two-step filtration of $V$ by free $A$-modules of rank one.

**Lemma 4.7.** *The action of inertia at* 2 *on* $M^0(\overline{\mathbf{Q}}_2)$ *and* $M^{ét}(\overline{\mathbf{Q}}_2)$ *is trivial.*

*Proof.* This is clear for $M^{\text{ét}}(\overline{\mathbf{Q}}_2)$, since étale implies unramified. It follows for $M^0(\overline{\mathbf{Q}}_2)$ from the Cartier self-duality of $M_{/\overline{\mathbf{Q}}_2}$. □

**Lemma 4.8.** *If* $\sigma \in G_{\mathbf{Q}_2}$ *then* $\sigma^2$ *acts trivially on* $V$.

*Proof.* Let us choose a basis of $V$ compatible with its filtration arising from the connected-étale sequence of $M$, and write the action of $\sigma$ on $V$ as a matrix over $A$ in terms of this basis:

$$\sigma = \begin{pmatrix} 1+a & b \\ 0 & 1+c \end{pmatrix}.$$

Part (iv) of Proposition 4.3 implies that $\sigma^2$ lies in the inertia subgroup. Thus it must fix $M^0(\overline{\mathbf{Q}}_2)$ and $M^{\text{ét}}(\overline{\mathbf{Q}}_2)$. Computing $\sigma^2$, we find that $(1+a)^2 = (1+c)^2 = 1$, and so $a^2 = c^2 = 0$. Since the determinant of $\sigma$ is 1, we see that $(1+c) = (1+a)^{-1} = 1+a$. Now computing $\sigma^2$ we find that it is trivial. □

*Conclusion of proof of Theorem 4.4:* If $E' = E$, then by Lemma 4.6 there is nothing more to prove. Otherwise, Proposition 4.3 implies that the $D_2(E'/\mathbf{Q})$ is dihedral of order 8. We have seen that for any $\sigma \in G_{\mathbf{Q}_2}$, the element $\sigma^2$ acts trivially. Thus the image $\rho_{|G_{\mathbf{Q}_2}}$ factors through an exponent 2 group, which is therefore abelian. Yet the dihedral group of order 8 is not abelian, and hence $F$ is contained in a proper subfield of $E'$ that is Galois over $\mathbf{Q}$. All such subfields lie inside $E$. □

**Corollary 4.9.** *If* $2^m$ *denotes the order of* $H$, *then there exists a surjection* $R \to \mathbf{F}_2[X]/X^n$ *if and only if* $n \leq 2^{m-1}$. *Furthermore, any such surjection is unique up to applying an automorphism of* $\mathbf{F}_2[X]/X^n$.

*Proof.* Corollary 3.4 implies that there exists a surjection $R \to \mathbf{F}_2[X]/X^n$ if and only if there exits $(V, L, \rho) \in \mathrm{Def}(\mathbf{F}_2[X]/X^n)$ with the property that the traces of $\rho$ generate $\mathbf{F}_2[X]/X^n$ as an $\mathbf{F}_2$-algebra (or equivalently, with the property that there is an element of $G_{\mathbf{Q}}$ whose image under $\rho$ has trace congruent to $X \mod X^2$.)

**Lemma 4.10.** *Let $A$ be an $\mathbf{F}_2$-algebra, and let $U \in \mathrm{SL}_2(A)$.*

*(i)* $U^2 = I + \mathrm{Trace}(U)U$.
*(ii) For any $k \geq 1$, we have that* $\mathrm{Trace}(U^k) \in \mathrm{Trace}(U)A$.
*(iii) If $U \in \mathrm{SL}_2(A)$, then*

$$U^{2^k} = \left( \sum_{i=0}^{k-1} \mathrm{Trace}(U)^{2^k - 2^{k-i}} \right) I + \mathrm{Trace}(U)^{2^k - 1} U,$$

*for any $k \geq 1$.*

*Proof.* Any $2 \times 2$ matrix $U$ over the ring $A$ satisfies the identity $U^2 = \mathrm{Det}(U)I + \mathrm{Trace}(U)U$. Part (i) is a particular case of this identity, and parts (ii) and (iii) follow by induction. □

Theorem 4.4 shows that $\rho$ factors as

$$G_{\mathbf{Q}} \to \mathrm{Gal}(E/\mathbf{Q}) \to \mathrm{SL}_2\big(\mathbf{F}_2[X]/X^n\big).$$

Now $\mathrm{Gal}(E/\mathbf{Q})$ is a dihedral group of order $2^{m+1}$; indeed, we may write

$$\mathrm{Gal}(E/\mathbf{Q}) = \langle \sigma, \tau | \sigma^{2^m} = \tau^2 = (\sigma\tau)^2 = 1 \rangle, \tag{12}$$

where $\sigma$ generates $\mathrm{Gal}(E/K)$, and $\tau$ generates the image of $I_N$ in $\mathrm{Gal}(E/\mathbf{Q})$.

Part (i) of Lemma 4.10 shows that any element of order two in the image of $\rho$ has vanishing trace. Since any element of $\mathrm{Gal}(E/\mathbf{Q})$ that is not of order two is a power of $\sigma$, we conclude from part (ii) of the same lemma that all the traces of $\rho$ lie in the ideal of $\mathbf{F}_2[X]/X^n$ generated by $\mathrm{Trace}(\rho(\sigma))$. Since the trace of any element in the image of $\overline{\rho}$ is zero, we see that this ideal is contained in the maximal ideal of $\mathbf{F}_2[X]/X^n$. Applying part (iii) of Lemma 4.10, we deduce that $\mathrm{Tr}(\rho(\sigma))^{2^{m-1}} = 0$ (since $\sigma^{2^m} = 1$, and so $\rho(\sigma^{2^m}) = I$).

Thus, on the one hand, the only way that $X$ can arise as a trace of $\rho$ is if $\mathrm{Tr}(\rho(\sigma)) \equiv X \mod X^2$. On the other hand, if this condition holds, then $X^{2^{m-1}} = 0$, and hence $n \leq 2^{m-1}$. This proves one direction of the "if and only if" statement of the corollary.

Let us now prove the uniqueness assertion, assuming that we are given a surjective map $R \to \mathbf{F}_2[X]/X^n$. Since the corresponding triple $(V, L, \rho)$ deforms $(\overline{V}, \overline{L}, \overline{\rho})$, and since $\sigma$ has non-trivial image in $\mathrm{Gal}(\mathbf{Q}(\sqrt{-1})/\mathbf{Q})$,

while $\tau$ generates the image of $I_N$ in $\mathrm{Gal}(E/\mathbf{Q})$, we may choose a basis of $V$ such that $\sigma$ and $\tau$ act through matrices in $\mathrm{SL}_2(\mathbf{F}_2[X]/X^n)$ of the form

$$\rho(\sigma) = \begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix} \equiv \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \mod X,$$

$$\rho(\tau) = \begin{pmatrix} a(\tau) & 0 \\ c(\tau) & d(\tau) \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod X.$$

Now conjugating by matrices in $\ker(\mathrm{GL}_2(\mathbf{F}_2[X]/X^n) \to \mathrm{GL}_2(\mathbf{F}_2))$ of the form

$$\begin{pmatrix} \alpha & 0 \\ \gamma & \delta \end{pmatrix},$$

it is easy to show that we may change our basis so that

$$\rho(\sigma) = \begin{pmatrix} 1 + uX & 1 \\ uX & 1 \end{pmatrix}, \qquad \rho(\tau) = \begin{pmatrix} 1 & 0 \\ uX & 1 \end{pmatrix},$$

for some $u \in (\mathbf{F}_2[X]/X^n)^\times$. Thus, after applying the inverse of the automorphism of $\mathbf{F}_2[X]/X^n$ induced by the map $X \mapsto uX$, we see that we may put $\rho$ in the form

$$\rho(\sigma) = \begin{pmatrix} 1 + X & 1 \\ X & 1 \end{pmatrix}, \qquad \rho(\tau) = \begin{pmatrix} 1 & 0 \\ X & 1 \end{pmatrix}. \tag{13}$$

This proves the uniqueness statement.

Finally, one checks that the preceding formula gives a well-defined homomorphism $\rho : \mathrm{Gal}(E/\mathbf{Q}) \to \mathrm{SL}_2(\mathbf{F}_2[X]/X^n)$, so long as $n \leq 2^{m-1}$, and that it deforms $\overline{\rho}$. It is certainly finite flat at 2, since the inertia group at two acts through its image in $\mathrm{Gal}(\mathbf{Q}(\sqrt{-1})/\mathbf{Q})$. Thus, if we let $L$ denote the line spanned by the vector $(0, 1)$, then we obtain an object of $\mathrm{Def}(\mathbf{F}_2[X]/X^n)$ of the required sort (since $\mathrm{Trace}(\rho(\sigma)) = X$). This completes the proof of the corollary. □

Let us consider the particular case $n = 2$ of the preceding corollary.

**Proposition 4.11.** *If* $N \not\equiv 1 \mod 8$, *then* $\mathrm{Def}(\mathbf{F}_2[X]/X^2) = 0$. *If* $N \equiv 1 \mod 8$, *then* $\mathrm{Def}(\mathbf{F}_2[X]/X^2)$ *is one dimensional over* $\mathbf{F}_2$. *Furthermore, if* $(V, L, \rho)$ *corresponds to the non-trivial element, then we have the following formulas for the traces of* $\rho$*:*

*(i) If* $\ell$ *is an odd prime distinct from* $N$, *then*

$$\mathrm{Trace}(\rho(\mathrm{Frob}_\ell)) = \begin{cases} 0 \text{ if } \ell \equiv 1 \mod 4 \text{ or } \ell \text{ is a square} \mod N \\ X \text{ otherwise} \end{cases}.$$

*(ii) If $\alpha_2$ denotes the eigenvalue of* $\mathrm{Frob}_2$ *on the rank one* $\mathbf{F}_2[X]/X^2$*-module of* $I_2$*-coinvariants of* $V$*, then*

$$\alpha_2 = \begin{cases} 1 \text{ if } -4 \text{ is an 8th power mod } N \\ 1 + X \text{ if not} \end{cases}.$$

*Proof.* If $N \not\equiv 1 \mod 8$ then Proposition 4.1 shows that $H$ has order two, and Corollary 4.9 shows that any map $R \to \mathbf{F}_2[X]/X^2$ factors through the map $R \to \mathbf{F}_2$. Thus in this case $\mathrm{Def}(\mathbf{F}_2[X]/X^2) = 0$, as claimed.

If $N \equiv 1 \mod 8$, then conversely we conclude from Proposition 4.1 that $H$ has order divisible by 4. Corollary 4.9 then shows that there is a unique surjection $R \to \mathbf{F}_2[X]/X^2$, and thus that $\mathrm{Def}(\mathbf{F}_2[X]/X^2)$ is one dimensional over $\mathbf{F}_2$. If $F$ denotes the subextension of $E$ over $K$ cut out by this non-trivial deformation, then $F$ is a dihedral extension of $\mathbf{Q}$ of degree 8, unramified over $K$, containing $K(\sqrt{-1})$. (Concretely, as we saw in the proof of Proposition 4.1, the field $F$ has the form $\mathbf{Q}(\sqrt{-1}, \sqrt{\nu}, \sqrt{\bar{\nu}})$, for appropriate $\nu$, $\bar{\nu}$.)

Recall the presentation (12) of $\mathrm{Gal}(E/\mathbf{Q})$. If we let $\bar{\sigma}$ and $\bar{\tau}$ denote the image of $\sigma$ and $\tau$ under the surjection $\mathrm{Gal}(E/\mathbf{Q}) \to \mathrm{Gal}(F/\mathbf{Q})$, then $\mathrm{Gal}(F/\mathbf{Q})$ has the following presentation:

$$\mathrm{Gal}(F/\mathbf{Q}) = \langle \bar{\sigma}, \bar{\tau} | \bar{\sigma}^4 = \bar{\tau}^2 = (\bar{\sigma}\bar{\tau})^2 = 1 \rangle.$$

Recall from the proof of Corollary 4.9 that the only elements of $\mathrm{Gal}(F/\mathbf{Q})$ whose images under $\overline{\rho}$ have non-zero trace (which is then equal to $X$) are $\bar{\sigma}^{\pm 1}$; that is, the elements of $\mathrm{Gal}(F/\mathbf{Q})$ that are of order 4.

If $\ell$ is an odd prime distinct from $N$, then $\ell$ is unramified in $F$. The final remark of the preceding paragraph shows that

$$\mathrm{Trace}(\rho(\mathrm{Frob}_\ell)) = \begin{cases} 0 \text{ if } \mathrm{Frob}_\ell \text{ has order 1 or 2} \\ X \text{ if } \mathrm{Frob}_\ell \text{ has order 4} \end{cases}.$$

Now $K$ is the maximal subfield of $F$ fixed by $\bar{\sigma}$, while one checks that any element of $\mathrm{Gal}(F/\mathbf{Q})$ of order two fixes at least one of the subfields $\mathbf{Q}(\sqrt{-1})$ or $\mathbf{Q}(\sqrt{N})$ of $F$. Thus we see that $\rho(\mathrm{Frob}_\ell)$ has trace zero (as opposed to trace $X$) if and only if $\ell$ splits in at least one of the fields $\mathbf{Q}(\sqrt{-1})$ or $\mathbf{Q}(\sqrt{N})$. This establishes (i).

Again referring to the presentation (12) of $\mathrm{Gal}(E/\mathbf{Q})$, one easily checks that $D_2(E/\mathbf{Q})$ is generated by $\sigma\tau$ and $\sigma^{2^{m-1}}$, with $I_2(E/\mathbf{Q})$ being generated by $\sigma\tau$. (Recall that $2^m$ denotes the order of $H$.) Thus $D_2(F/\mathbf{Q})$ is generated by $\bar{\sigma}\bar{\tau}$ and $\bar{\sigma}^{2^{m-1}}$. Thus if $m \geq 3$, then we see that $D_2(F/\mathbf{Q}) = I_2(F/\mathbf{Q})$, while if $m = 2$, then $D_2(F/\mathbf{Q})/I_2(F/\mathbf{Q})$ is generated by the image of $\bar{\sigma}^2$.

In terms of the explicit model (13) for $\rho$, we see that the coinvariants of $I_2(F/\mathbf{Q}) = \langle \bar{\sigma}\bar{\tau} \rangle$ on $V$ are spanned by the image of the basis vector $(0, 1)$, and that $\bar{\sigma}^2$ (which is central in $\mathrm{Gal}(F/\mathbf{Q})$, and so does act on the space of coinvariants) acts on the image of this vector as multiplication by $1 + X$.

Combining this computation with the discussion of the previous paragraph proves part (ii), once we recall from Proposition 4.1 that $m \geq 3$ if and only if $-4$ is an 8th power modulo $N$. □

The quotient $R/2$ is the universal deformation ring classifying deformations of $(\overline{V}, \overline{L}, \overline{\rho})$ in characteristic 2. The preceding two results together imply that $R/2 \cong \mathbf{F}_2[X]/X^{2^{m-1}}$, where $2^m$ is the order of $H$; formula (13) then gives an explicit model for the universal deformation over $R/2$.

We close this section by observing that Theorem 1.1 follows from Corollaries 1.6 and 4.9 taken together. More generally, we see that $g_2 = 2^{m-1} - 1$.

## 5. Explicit deformation theory: $p$ odd

In this section we suppose that $p \geq 3$, and that $N$ is prime to $p$. We begin by considering the problem of analyzing deformations $(V, L, \rho) \in \mathrm{Def}(A)$, where $A$ is an Artinian local $\mathbf{F}_p$-algebra with residue field $\mathbf{F}_p$. Our results will be less definitive than those obtained in the case of $p = 2$.

Let $\Delta$ denote the following subgroup of $\mathrm{GL}_2(\mathbf{F}_p) \subset \mathrm{GL}_2(A)$:

$$\Delta = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix} \mid \alpha \in \mathbf{F}_p^\times \right\},$$

and let $G'$ denote the kernel of the map $\mathrm{SL}_2(A) \to \mathrm{SL}_2(\mathbf{F}_p)$ induced by reduction modulo $\mathfrak{p}$ (the maximal ideal of $A$); note that $G'$ is a normal subgroup of $\mathrm{GL}_2(A)$. If we let $G$ denote the subgroup of $\mathrm{GL}_2(A)$ generated by $G'$ and $\Delta$, then $G$ is isomorphic to the semi-direct product $G' \rtimes \Delta$, where $\Delta$ acts on $G'$ via conjugation. Explicitly, one computes that

$$\begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \alpha^{-1} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & \alpha b \\ \alpha^{-1} c & d \end{pmatrix}. \tag{14}$$

**Lemma 5.1.** *Let $(V, L, \rho)$ be an object of $\mathrm{Def}(A)$, and let $M$ denotes the finite flat group scheme over $\mathbf{Z}_p$ whose generic fibre equals $V$. If $0 \to M^0 \to M \to M^{ét} \to 0$ denotes the connected-étale exact sequence of $M$, then there is a basis for $V$ over $A$ such that*

*(i) The representation $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(A)$ has image lying in $G$.*
*(ii) The submodule $M^0(\overline{\mathbf{Q}}_p)$ of $V$ (which is free of rank one, by Corollary 2.9) is spanned by the vector $(1, 0)$.*
*(iii) The line $L$ is spanned by the vector $(1, 1)$.*

*Proof.* By definition of the deformation problem Def, the determinant of $\rho$ is equal to $\overline{\chi}_p$. Thus $\mathrm{im}(\rho)$ sits in the exact sequence of groups

$$0 \to G' \cap \mathrm{im}(\rho) \to \mathrm{im}(\rho) \to \mathbf{F}_p^\times \to 0.$$

The order of $\mathbf{F}_p^\times$ is coprime to the order of $G'$, and so this exact sequence splits. If we fix a splitting $s$, then one easily sees that we may choose an eigenbasis for the action of $s(\mathbf{F}_p^\times)$ so that this group acts via the matrices in $\Delta$. Thus condition (i) is satisfied for this basis. Condition (ii) follow directly from condition (i). The stipulations of the deformation problem Def then imply that $L$ is spanned by a vector of the form $(1, u)$, for some unit $u \in A^\times$. Rescaling the second basis vector by $u$, we may assume that $L$ is in fact spanned by $(1, 1)$. □

From now on, we fix an object $(V, L, \rho) \in \mathrm{Def}(A)$, and choose a basis of $V$ as in the preceding lemma. Thus we may regard $\rho$ as a homomorphism $G_{\mathbf{Q}} \to G \subset \mathrm{GL}_2(A)$.

**Lemma 5.2.** *If $(V, L, \rho)$ is a non-trivial deformation, then the image of $I_N$ under $\rho$ is a cyclic subgroup of $G'$ of order $p$. Furthermore, if $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is a generator of this cyclic group, then neither $b$ nor $c$ vanishes, and neither $a$ nor $d$ equals* 1.

*Proof.* Since the image under $\rho$ of inertia at $N$ acts trivially on each of the lines $L$ and $V/L$ (the determinant of $\rho$ equals $\overline{\chi}_p$, which is trivial on $I_N$), we see that $I_N$ acts via an abelian group of exponent $p$. Since tame inertia is pro-cyclic, inertia at $N$ must act through a group of order dividing $p$. If $I_N$ has trivial image, then Proposition 3.2 shows that $V = A \otimes_{\mathbf{F}_p} \overline{V}$, and thus that $(V, L, \rho)$ is the trivial deformation, contradicting our assumption. Thus $I_N$ has image of order $p$.

The line $L$ is spanned by the vector $(1, 1)$. Thus if $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is a generator of the image of $I_N$, it fixes such a vector. Since the determinant of $\rho$ equals $\overline{\chi}_p$, we see that $\det(\gamma) = 1$. If $a$ (respectively $d$) equals 1 then we conclude that $b$ (respectively $c$) equals 0. If either $b$ or $c$ vanishes, one easily checks that $\gamma$ must be the identity, contradicting the fact that $I_N$ has non-trivial image. □

If $F$ denotes the extension of $\mathbf{Q}$ cut out by the kernel of $\rho$, then $F$ contains $\mathbf{Q}(\zeta_p)$ (where $\zeta_p$ denotes a primitive $p$th root of unity), since $\det(\rho) = \overline{\chi}_p$. We let $F^{ab}$ denote the maximal subextension of $F$ abelian over $\mathbf{Q}(\zeta_p)$.

**Lemma 5.3.** *The $p$-part of the conductor of $F^{ab}/\mathbf{Q}(\zeta_p)$ divides $\pi^2$, where $\pi = (1 - \zeta_p)\mathbf{Z}[\zeta_p]$, and the extension $F/\mathbf{Q}(\zeta_p)$ has inertial degree dividing $p$ at $N$ and is unramified outside $N$ and $\pi$.*

*Proof.* Lemma 5.2 shows that the image under $\rho$ of inertia at $N$ is a cyclic group of order dividing $p$. Therefore it suffices to prove the conductor bound at $\pi$.

The image under $\rho$ of $G_{\mathbf{Q}(\zeta_p)}$ lies in $G'$, a $p$-group, and so we see that $\mathrm{Gal}(F^{ab}/\mathbf{Q}(\zeta_p))$ is an abelian $p$-group. Thus it is a compositum of

cyclic extensions of $p$-power degree. The conductor of a compositum of cyclic extensions is equal to the g.c.d. of the conductors of the individual cyclic extensions, and thus it suffices to bound the conductor of a cyclic subextension of $F^{ab}$ of degree $p^k$, for some $k \geq 1$.

Let $F'$ be such a subextension, and suppose that the conductor of $F'$ is divisible by $\pi^3$. There are $(p-1)p^{k-1}$ faithful characters of $\mathbf{Z}/p^k$, and so by the conductor discriminant formula, the discriminant $\Delta_{F'/\mathbf{Q}(\zeta_p)}$ is divisible by $\pi^{3(p-1)p^{k-1}}$. Thus the $p$-root discriminant of $F'$ (as defined in the proof of Lemma 4.5) satisfies

$$\delta_{F',p} \geq \delta_{\mathbf{Q}(\zeta_p)} N_{\mathbf{Q}(\zeta_p)/\mathbf{Q}}(\pi^{3(p-1)p^{k-1}})^{1/[F':\mathbf{Q}]} = p^{(p-2)/(p-1)} \cdot p^{3(p-1)/(p(p-1))}$$

and thus

$$v_p(\delta_{F',p}) \geq 1 + \frac{1}{p-1} + \frac{p-3}{p(p-1)}.$$

This violates Fontaine's bound [3] when $p \geq 3$. The result follows for $F^{ab}$. □

In order to apply this result, we will need to classify the relevant class fields of $\mathbf{Q}(\zeta_p)$ that can arise in the situation of the preceding lemma.

**Proposition 5.4.** *Let $p$ be an odd prime, and let $N$ be a prime distinct from $p$. For any value of $i$, let $K_{(i)}$ denote the maximal abelian extension of $\mathbf{Q}(\zeta_p)$ satisfying the following conditions: $K_{(i)}$ has conductor dividing $\pi^2 N$; the Galois group $\mathrm{Gal}(K_{(i)}/\mathbf{Q}_p(\zeta_p))$ has exponent $p$; the Galois group $\mathrm{Gal}(\mathbf{Q}_p(\zeta_p)/\mathbf{Q})$ acts on $\mathrm{Gal}(K_{(i)}/\mathbf{Q}_p(\zeta_p))$ through the $i$th power of the mod $p$ cyclotomic character $\overline{\chi}_p$. Then:*

*(i)* $K_{(1)} = \mathbf{Q}(\zeta_p, N^{1/p})$;

*(ii)* $$K_{(0)} = \begin{cases} \text{the degree } p \text{ subextension of } \mathbf{Q}_p(\zeta_p, \zeta_N)/\mathbf{Q}_p(\zeta_p) \\ \qquad\qquad \text{if } N \equiv 1 \mod p \\ \mathbf{Q}(\zeta_p) \text{ otherwise} \end{cases};$$

*(iii)* $$K_{(-1)} = \begin{cases} \text{a degree } p \text{ extension of } \mathbf{Q}_p(\zeta_p) \text{ if } N^2 \equiv 1 \mod p \\ \mathbf{Q}(\zeta_p) \text{ otherwise} \end{cases}.$$

*Proof.* Let $E_{(i)}$ denote the unramified extension of $\mathbf{Q}(\zeta_p)$ of exponent $p$ corresponding to the maximal elementary $p$-abelian quotient of the class group of $\mathbf{Q}(\zeta_p)$ on which $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$ acts through $\overline{\chi}_p^i$. Then we have the short exact sequence of abelian Galois groups

$$0 \to \mathrm{Gal}(K_{(i)}/E_{(i)}) \to \mathrm{Gal}(K_{(i)}/\mathbf{Q}(\zeta_p)) \to \mathrm{Gal}(E_{(i)}/\mathbf{Q}(\zeta_p)) \to 0.$$

Global class field theory allows us to compute the group $\mathrm{Gal}(K_i/E_{(i)})$. Indeed, it sits in the exact sequence

$$(\mathbf{Z}[\zeta_p])^\times \longrightarrow \left( \left( \mathbf{Z}[\zeta_p]/\pi^2 \times \mathbf{Z}[\zeta_p]/N \right)^\times / \{p\} \right)_{(i)} \longrightarrow \mathrm{Gal}(K_{(i)}/E_{(i)}) \longrightarrow 0;$$

here the subscript $(i)$ denotes the maximal quotient on which $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$ acts via $\overline{\chi}_p^i$, and $G/\{m\}$ denotes $G/G^m$.

Since the reduction mod $\pi^2$ of the global unit $\zeta_p = 1 + (\zeta_p - 1)$ generates the $p$-power part of $(\mathbf{Z}[\zeta_p]/\pi^2)^\times$, we may eliminate this factor from the second term of the preceding exact sequence. If we fix a prime $\mathfrak{n}$ over $N$ in $\mathbf{Z}[\zeta_p]$, then as in the proof of Lemma 3.9, we obtain a surjection

$$(\mathbf{Z}[\zeta_p]/\mathfrak{n})^\times/\{(p, N^{1-i} - 1)\} \to \mathrm{Gal}(K_{(i)}/E_{(i)}).$$

Consequently, we find that $\mathrm{Gal}(K_{(i)}/E_{(i)})$ is either trivial (when $N^{(1-i)} \not\equiv 1 \mod p$) or of order $p$ (when $N^{(1-i)} \equiv 1 \mod p$).

Let us now consider the particular cases $i = 1, 0, -1$. The 1, 0 and $-1$ eigenspaces inside the class group of $\mathbf{Q}(\zeta_p)$ are trivial by Kummer theory, abelian class field theory and Herbrand's theorem respectively. Thus for these values of $i$, we have $E_i = \mathbf{Q}(\zeta_p)$, and so the preceding paragraph yields a computation of $\mathrm{Gal}(K_{(i)}/\mathbf{Q}(\zeta_p))$. The explicit descriptions of $K_{(i)}$ in the case when $i = 1$ or 0 are easily verified, and so we leave this verification to the reader. □

We are now in a position to determine the reduced Zariski tangent space to the deformation functor Def. We will also record some useful information regarding non-trivial elements of this tangent space (assuming that they exist).

**Proposition 5.5.** *If $p$ does not divide the numerator of $(N-1)/12$, then $\mathrm{Def}(\mathbf{F}_p[X]/X^2) = 0$; otherwise, $\mathrm{Def}(\mathbf{F}_p[X]/X^2)$ is one dimensional over $\mathbf{F}_p$. Suppose for the remainder of the statement of the proposition that we are in the second case, and let $(V, L, \rho)$ correspond to a non-trivial element of $\mathrm{Def}(\mathbf{F}_p[X]/X^2)$.*

*(i) If as above $F$ denotes the extension of $\mathbf{Q}$ cut out by the kernel of $\rho$, then $F$ is equal to the compositum $K_{(1)}K_{(0)}K_{(-1)}$ (where the class fields $K_{(i)}$ of $\mathbf{Q}(\zeta_p)$ are defined as in the statement of the previous proposition).*

*(ii) If $p = 3$, then $\mathrm{Gal}(F/\mathbf{Q}(\zeta_p)) \cong \mathrm{Gal}(K_1/\mathbf{Q}(\zeta_p)) \times \mathrm{Gal}(K_0/\mathbf{Q}(\zeta_p))$, and the image of an appropriately chosen generator of the first (respectively second) factor under $\rho$ has the form $\begin{pmatrix} 1 & -rX \\ rX & 1 \end{pmatrix}$ (respectively $\begin{pmatrix} 1+rX & 0 \\ 0 & 1-rX \end{pmatrix}$) for some $r \in \mathbf{F}_p^\times$.*

*(iii) If $p \geq 5$, then $\mathrm{Gal}(F/\mathbf{Q}(\zeta_p)) \cong \mathrm{Gal}(K_1/\mathbf{Q}(\zeta_p)) \times \mathrm{Gal}(K_0/\mathbf{Q}(\zeta_p)) \times \mathrm{Gal}(K_1/\mathbf{Q}(\zeta_p))$, and the image of an appropriately chosen generator of the first (respectively second, respectively third) factor under $\rho$ has the form $\begin{pmatrix} 1 & -rX \\ 0 & 1 \end{pmatrix}$ (respectively $\begin{pmatrix} 1+rX & 0 \\ 0 & 1-rX \end{pmatrix}$, respectively $\begin{pmatrix} 1 & 0 \\ rX & 1 \end{pmatrix}$) for some $r \in \mathbf{F}_p^\times$.*

*(iv) We have the following formulas for the traces of $\rho$:*
*(iv.i) If $\ell$ is a prime distinct from $N$ and $p$, then*

$$\mathrm{Trace}(\rho(\mathrm{Frob}_\ell)) = \begin{cases} 1+\ell \text{ if } \ell \equiv 1 \mod p \text{ or } \ell \text{ is} \\ \qquad\qquad \text{a } p\text{th power} \mod N; \\ 1+\ell+uX \text{ otherwise} \end{cases}$$

*here $u$ denotes an element of $\mathbf{F}_p^\times$.*

*(iv.ii) If $\alpha_p$ denotes the eigenvalue of $\mathrm{Frob}_p$ on the rank one $\mathbf{F}_p[X]/X^2$-module of $I_p$-coinvariants of $V$, then*

$$\alpha_p = \begin{cases} 1 \text{ if } p \text{ is a } p\text{th power mod } N \\ 1+uX \text{ if not} \end{cases};$$

*again, $u$ denotes an element of $\mathbf{F}_p^\times$.*

*Proof.* Let $(V, L, \rho)$ be a non-trivial element of $\mathrm{Def}(\mathbf{F}_p[X]/X^2)$, cutting out the extension $F$ of $\mathbf{Q}$. As above, we choose the basis of $V$ so that the conditions of Lemma 5.1 are satisfied. Since $G'$ is abelian, we see that $F = F^{ab}$. Equation (14), together with Lemma 5.3, thus shows that $F$ is contained in the compositum $K_{(1)}K_{(0)}K_{(-1)}$. Lemma 5.2 then shows that in fact $F$ must be equal to this compositum, proving part (i) of the proposition; that furthermore, each of the extensions $K_{(1)}$, $K_{(0)}$ and $K_{(-1)}$ of $\mathbf{Q}(\zeta_p)$ must be non-trivial, and thus that $N \equiv 1 \mod p$, by Proposition 5.4; and that either part (ii) or part (iii) of the proposition is satisfied, depending on whether $p = 3$ or $p \geq 5$. (We choose the generator of each group $\mathrm{Gal}(K_{(i)}/\mathbf{Q}(\zeta_p))$ to be the image of some fixed generator of the inertia group $I_N$.)

Suppose conversely that $N \equiv 1 \mod p$, so that each of $K_{(1)}$, $K_{(0)}$ and $K_{(-1)}$ is a non-trivial extension of $\mathbf{Q}(\zeta_p)$. Write $F = K_{(1)}K_{(0)}K_{(-1)}$. If we fix an element $r \in \mathbf{F}_p^\times$, then we may use the formulas of parts (ii) and (iii) to define a representation $\rho : \mathrm{Gal}(F/\mathbf{Q}) \to G \subset \mathrm{GL}_2(\mathbf{F}_p[X]/X^2)$. If we let $L$ denote the line spanned by $(1, 1)$, then this representation will deform the representation $(V, L)$. Thus it will provide an element of $\mathrm{Def}(\mathbf{F}_p[X]/X^2)$ provided that it is finite at $p$. An argument as in the proof of Lemmas 3.8 and 3.9 shows that this is automatically the case when $p \geq 5$, and holds provided $p$ divides $(N-1)/12$, when $p = 3$. This establishes the initial claim of the proposition.

It remains to prove part (iv) of the proposition. Suppose first that $\ell$ is a prime distinct from $p$ and $N$. We may write

$$\rho(\mathrm{Frob}_\ell) = \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1+aX & bX \\ cX & 1-aX \end{pmatrix},$$

for some elements $a, b, c \in \mathbf{F}_p$. Thus $\mathrm{Trace}(\rho(\mathrm{Frob}_\ell)) = 1+\ell+(\ell-1)aX$. This is distinct from $1+\ell$ if and only if $\ell \not\equiv 1 \mod p$ and $a \neq 0$. The

latter occurs if and only if the primes over $\ell$ are not split in the extension $K_{(0)}/\mathbf{Q}(\zeta_p)$, which in turn is the case if and only if $\ell$ is not a $p$th power mod $N$. (Here we have taken into account the explicit description of $K_{(0)}$ provided by Proposition 5.4.) Thus we have proved part (iv.i).

Since the vector $(1, 0)$ spans the subspace $M^0(\overline{\mathbf{Q}}_p)$ of $V$, the space of $I_p$-inertial coinvariants is spanned by the image of the vector $(0, 1)$. The Frobenius element $\mathrm{Frob}_p$ acts non-trivially on the image of this vector if and only if the prime over $p$ is not split in the extension $K_{(0)}$ of $\mathbf{Q}(\zeta_p)$, which is the case if and only if $p$ is not a $p$th power mod $N$. This proves part (iv.ii). □

As we will see below, for $p \geq 3$, the rank $g_p + 1$ of $\mathbf{T}/p$ over $\mathbf{F}_p$ is no longer explained by an abelian extension of number fields (and hence by a single class group), as it is in the case $p = 2$, but by certain more complicated solvable extensions. However, the question of whether or not $g_p = 1$ is somewhat tractable. Indeed, from Corollary 1.6 we deduce the following criterion.

**Lemma 5.6.** *The rank $g_p$ of the parabolic Hecke algebra $\mathbf{T}^0/p$ over $\mathbf{F}_p$ is greater than one (equivalently, $\mathbf{T}^0 \neq \mathbf{Z}_p$) if and only if there exists a $(V, L, \rho)$ in $\mathrm{Def}(\mathbf{F}_p[X]/X^3)$ whose traces generate $\mathbf{F}_p[X]/X^3$.*

In order to apply this lemma, we now assume that $A = \mathbf{F}_p[X]/X^3$, so that $(V, L, \rho)$ lies in $\mathrm{Def}(\mathbf{F}_p[X]/X^3)$. As always, we assume that the basis of $V$ is chosen so as to satisfy the conditions of Lemma 5.1. We let $\rho_n$ denote the composition of $\rho$ with the natural surjection $\mathrm{GL}_2(\mathbf{F}_p[X]/X^3) \to \mathrm{GL}_2(\mathbf{F}_p[X]/X^n)$, for $n \leq 3$. Requiring the traces of $\rho$ to generate $\mathbf{F}_p[X]/X^3$ is equivalent to requiring the traces of $\rho_2$ to generate $\mathbf{F}_p[X]/X^2$, which in turn is equivalent is to requiring that $\rho_2$ be a non-trivial deformation. We assume this to be the case. Also, we let $F_n$ denote the extension cut out by the kernel of $\rho_n$. Thus $F_1 = \mathbf{Q}(\zeta_p)$, and $F_3 = F$.

Since we are assuming that $\rho_2$ is non-trivial, Proposition 5.5 shows that $p$ divides the numerator of $(N-1)/12$, and that $F_2$ is equal to the compositum of the class fields $K_{(i)}$ (for $i = 1, 0, -1$).

**Lemma 5.7.** *(i) We have $F_2 = F^{ab}$, and $\mathrm{Gal}(F_2/F_1) \cong (\mathbf{Z}/p)^2$ (respectively $(\mathbf{Z}/p)^3$) if $p = 3$ (respectively $p \geq 5$).*
*(ii) $F/F_2$ is unramified at $N$.*

*Proof.* Since $p \geq 3$, we see that $G'$ has exponent $p$. Lemma 5.3 and equation (14) then imply that $F^{ab} \subset K_{(1)}K_{(0)}K_{(-1)} = F_2$. Certainly $F_2 \subset F^{ab}$, and so we have the equality stated in (i). The claims regarding $\mathrm{Gal}(F_2/F_1)$ follow from parts (ii) and (iii) of Proposition 5.5.

Part (ii) follows from the Lemma 5.2 and the fact that $F_2/F_1$ is ramified at $N$. □

We now separate our analysis into two cases: $p = 3$, and $p \geq 5$.

*5.1.* $p = 3$

Throughout this subsection we set $p = 3$.

**Lemma 5.8.** *The extension $F/F_2$ is unramified everywhere and has degree exactly three.*

*Proof.* The image of $\rho_{|G_{\mathbf{Q}(\sqrt{-3})}}$ is a subgroup of $G' = \ker(\mathrm{GL}_2(\mathbf{F}_3[X]/X^3) \to \mathrm{GL}_2(\mathbf{F}_3))$ whose image in $\mathrm{GL}_2(\mathbf{F}_3[X]/X^2)$ is isomorphic to $(\mathbf{Z}/3)^2$, by Lemma 5.7. Thus the commutator subgroup of the image of $\rho_{|G_{\mathbf{Q}(\sqrt{-3})}}$ is either trivial or cyclic of order three. Thus the extension $F/F_2$ has degree at most three.

Consider the representation $\rho_2$, which factors through $\mathrm{Gal}(F_2/\mathbf{Q})$. By assumption this yields a non-trivial element of $\mathrm{Def}(\mathbf{F}_3[X]/X^2)$. Part (ii) of Lemma 5.5 thus shows that the image under $\rho_2$ of the element of order three coming from the $\overline{\chi}_p^1$ extension $K_{(1)} = \mathbf{Q}(\sqrt{-3}, \sqrt[3]{N})$ of $\mathbf{Q}(\sqrt{-3})$ must be of the form

$$\begin{pmatrix} 1 & -rX \\ rX & 1 \end{pmatrix},$$

and that the image under $\rho_2$ of the element of order three coming from the $\overline{\chi}_p^0$ extension $K_{(0)}$ of $\mathbf{Q}(\sqrt{-3})$ is of the form

$$\begin{pmatrix} 1 + rX & 0 \\ 0 & 1 - rX \end{pmatrix},$$

for some $r \in \mathbf{F}_3^\times$. Lifting these two elements (in any way) to $\mathrm{GL}_2(\mathbf{F}_3[X]/X^3)$ and taking their commutator, we produce a new element in $\mathrm{Gal}(F/\mathbf{Q})$ which has a lower left-hand entry equal to $r^2X^2 = X^2$. This element cannot be in the decomposition group at 3 because it doesn't preserve $M^0(\overline{\mathbf{Q}}_3)$, which is generated by $(1, 0)$. Thus $F/F_2$ has order exactly three and is unramified at all primes above three. Part (ii) of Lemma 5.7 shows that the extension $F/F_2$ is also unramified at all primes above $N$, and the lemma is proved. □

Let $K = \mathbf{Q}(\sqrt[3]{N})$, and as above write $K_{(1)} = K^{gal} = K(\sqrt{-3})$. The extension $F/K_{(1)}$ has degree 9, and $\mathrm{Gal}(F/K_{(1)}) = (\mathbf{Z}/3\mathbf{Z})^2$. Moreover, $F/K_{(1)}$ is unramified everywhere. The following lemma shows that the existence of such an extension $F$ is sufficient for the construction of a deformation $\rho$ of the type considered here. This completes the proof of part one of each of Theorems 1.2 and 1.3.

**Lemma 5.9.** *If $N \equiv 1 \mod 9$, then the class group of $K_{(1)} = \mathbf{Q}(\sqrt{-3}, \sqrt[3]{N})$ has 3-rank greater than or equal (equivalently, equal) to two if and only if there exists a surjection $R \to \mathbf{F}_3[X]/X^3$; the kernel of the corresponding deformation $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F}_p[X]/X^3)$ then cuts out the $(3, 3)$ unramified class field $F$ of $K_{(1)}$.*

*Proof.* The preceding discussion establishes the "if" claim, and so it suffices to prove the "only if" claim. Genus theory and a consideration of the ambiguous class predicts that the 3-rank of the class group of $K_{(1)}$ is either one or two, and hence by assumption this rank is exactly two (see for example [4]). We let $F$ denote the corresponding unramified (3, 3)-extension of $K_{(1)}$, and (as above) let $F^{ab}$ denote the unique subextension of $F$ abelian over $\mathbf{Q}(\sqrt{-3})$. It is easily checked that $F^{ab}$ is in fact the maximal abelian 3-power extension of $\mathbf{Q}(\sqrt{-3})$ that is unramified over $K_{(1)}$, and that $F^{ab} = K_{(1)}K_{(0)}$.

Proposition 5.5 yields a Galois representation $\mathrm{Gal}(F^{ab}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{F}_3[X]/X^2)$, while Lemma 5.10 below shows that $\mathrm{Gal}(F/\mathbf{Q}(\sqrt{-3}))$ is the unique non-abelian group of order 27 and of exponent three. It is then easy to see that one can lift the representation of $\mathrm{Gal}(F^{ab}/\mathbf{Q})$ to a representation $\rho : \mathrm{Gal}(F/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{F}_3[X]/X^3)$. Furthermore one checks that for any such lift, the image of $I_N$ fixes an appropriate line.

To show that we have constructed an element of $\mathrm{Def}(\mathbf{F}_3[X]/X^3)$, as required, it remains to show that this representation extends to a finite flat group scheme at 3, For this, it suffices to work over the maximal unramified extension of $\mathbf{Q}_3$. Since $F/\mathbf{Q}(\sqrt{-3})$ is unramified at 3 (because $N \equiv 1 \mod 9$), the representation $\rho|_{\mathbf{Q}_3^{ur}}$ factors through a group of order two, and explicitly prolongs to a product of trivial and multiplicative group schemes. Thus $\rho$ is indeed finite at the prime 3. □

**Lemma 5.10.** *The Galois group* $\mathrm{Gal}(F/\mathbf{Q}(\sqrt{-3}))$ *is the (unique up to isomorphism) non-abelian group of order* 27 *and of exponent three.*

*Proof.* Let $\Gamma = \mathrm{Gal}(K_{(1)}/\mathbf{Q}(\sqrt{-3})) = \langle\gamma\rangle$. The 3-class group $H$ of $K_{(1)}$ is naturally a $\mathbf{Z}_3[\Gamma]$-module. From class field theory we have that $H/(\gamma - 1)H$ is isomorphic to the Galois group over $K_{(1)}$ of the maximal abelian 3-extension of $\mathbf{Q}(\sqrt{-3})$ that is unramified over $K_{(1)}$; that is, to $\mathrm{Gal}(F^{ab}/K_{(1)})$, a cyclic group of order 3. Thus by Nakayama's lemma $H$ is a cyclic $\mathbf{Z}_3[\Gamma]$-module. By class field theory, the quotient $H/3$ is isomorphic to $\mathrm{Gal}(F/K_{(1)})$.

Note that $\mathrm{Gal}(F/\mathbf{Q}(\sqrt{-3}))$ sits in the exact sequence:

$$0 \to \mathrm{Gal}(F/K_{(1)}) \longrightarrow \mathrm{Gal}(F/\mathbf{Q}(\sqrt{-3})) \longrightarrow \mathrm{Gal}(K_{(1)}/\mathbf{Q}(\sqrt{-3})) \longrightarrow 0,$$

which is an extension of $\Gamma \cong \mathbf{Z}/3\mathbf{Z}$ by $H/3 \cong (\mathbf{Z}/3\mathbf{Z})^2$. The action via conjugation of $\Gamma$ on $H/3$ is non-trivial, since otherwise $H$ could not be cyclic as a $\Gamma$-module. Already this shows that $\mathrm{Gal}(F/\mathbf{Q}(\sqrt{-3}))$ is one of the two non-abelian groups of order 27. To pin down the group precisely, we must show that it has exponent three. For this, it suffices to find a splitting of the above exact sequence (a section from $\Gamma = \mathrm{Gal}(K_{(1)}/\mathbf{Q}(\sqrt{-3}))$ back to $\mathrm{Gal}(F/\mathbf{Q}(\sqrt{-3}))$). Since the inertia group above $N$ in $\mathrm{Gal}(F/\mathbf{Q}(\sqrt{-3}))$ has order exactly three, and maps isomorphically to $\Gamma$, the required splitting exists. □

The final result of this section provides a relation between the rank of the 3-class group of $K_{(1)}$ and the power of 3 dividing the class number of $K$.

**Lemma 5.11.** *The 3-class group of* $K_{(1)} = \mathbf{Q}(\sqrt{-3}, \sqrt[3]{N})$ *has three rank two if the 3-class group of* $K = \mathbf{Q}(\sqrt[3]{N})$ (*which is cyclic*) *is divisible by nine.*

*Proof.* One has a class number relation between $K$ and $K_{(1)}$ given by $h_{K_{(1)}} = h_K^2/3 \cdot q$, where $q$ is the index of the units in $K_{(1)}$ coming from $K$, $K^\gamma$, and $\mathbf{Q}(\sqrt{-3})$ inside the full unit group. This was initially proven using analytic means by Scholz [15] (for a more recent algebraic proof, see [5]). Here, as above, $\gamma$ denotes a generator of the cyclic group $\Gamma = \mathrm{Gal}(K_{(1)}/\mathbf{Q}(\sqrt{-3}))$. If $9|h_K$, then $27|h_{K_{(1)}}$. Recall from the proof of the previous lemma that the 3-part $H$ of the class group of $K_{(1)}$ is a cyclic $\mathbf{Z}_3[\Gamma]$-module, and satisfies the condition that $H/(\gamma - 1)H$ is cyclic of order 3.

Now $\mathbf{Z}_3[\Gamma]$ admits no quotients $H'$ that are cyclic groups of order 27 with the property that $H'/(\gamma - 1)H'$ is of order 3. It follows that if $H$ is of order divisible by 27, then it must be non-cyclic, as claimed. □

We conjecture that the converse to the preceding lemma is also true. To prove this, it would suffice to show that whenever $3\|h_K$, the unit index $q$ is always equal to one. We have verified this for all primes less than 50,000 for which $3\|h_K$.

### 5.2. $p \geq 5$

Throughout this section we assume that $p \geq 5$, and that we are given a deformation to $\mathbf{F}_p[X]/X^3$ as in the discussion following Lemma 5.6. Proposition 5.5 and Lemma 5.7 together show that $F_2 = K_{(1)}K_{(0)}K_{(-1)}$, that $\mathrm{Gal}(F_2/F_1) = (\mathbf{Z}/p)^3$, and that $F_2 = F^{ab}$. We see that $F_2/F_1$ is unramified at $p$ if and only if $N \equiv 1 \mod p^2$.

It follows from our determination of $F_2$ that $\mathrm{Gal}(F/F_1)$ is the full kernel of the map from $\mathrm{SL}_2(\mathbf{F}_p[x]/x^3)$ to $\mathrm{SL}_2(\mathbf{F}_p)$, since all the elements of

$$\mathrm{Ker}(\mathrm{SL}_2(\mathbf{F}_p[x]/x^3) \to \mathrm{SL}_2(\mathbf{F}_p[x]/x^2))$$

are generated by commutators of lifts of elements of $\mathrm{Ker}(\mathrm{SL}_2(\mathbf{F}_p[x]/x^2) \to \mathrm{SL}_2(\mathbf{F}_p))$.

**Lemma 5.12.** *If $E$ is a degree $p$ Galois extension of $F_2$ inside $F_3$ on which the matrix*

$$\begin{pmatrix} 1+x^2 & 0 \\ 0 & 1-x^2 \end{pmatrix}$$

*acts non-trivially, then $E/F_2$ is everywhere unramified.*

*Proof.* Part (ii) of Lemma 5.7 shows that this extension is unramified at primes above $N$. To see that it is unramified at primes above $p$, it suffices to note that the matrix $\begin{pmatrix} 1+x^2 & 0 \\ 0 & 1-x^2 \end{pmatrix}$ does not fix the vector $(1,0)$ (which spans $M^0(\overline{\mathbf{Q}}_p)$). □

Let $K = \mathbf{Q}(N^{1/p})$ and $L = K^{gal} = K(\zeta_p) = K_{(1)}$.

**Lemma 5.13.** *The Hilbert class field of $K$ has $p$-rank at least two.*

*Proof.* Let us first consider the extension $\mathrm{Gal}(F/K)$. One sees that $\mathrm{Gal}(F/K)^{ab} \cong (\mathbf{Z}/p\mathbf{Z})^2 \times (\mathbf{Z}/p)^\times$ is explicitly generated by the images of

$$\begin{pmatrix} 1+x^k & 0 \\ 0 & (1+x^k)^{-1} \end{pmatrix},$$

for $k = 1, 2$, together with the image of $\Delta$. We let $H$ be the $(p, p)$-extension of $K$ contained in $F$ that is fixed by $\Delta$. We will show that $H$ is unramified over $K$.

We may write $H$ as a compositum $H = H_1 H_2$, where for each of $k = 1, 2$, we let $H_k$ denote a $p$-extension of $K$ contained in $F$, on which the matrix $\begin{pmatrix} 1+x^k & 0 \\ 0 & (1+x^k)^{-1} \end{pmatrix}$ acts non-trivially. If we let $\zeta_N^+$ denote an element of $\mathbf{Q}(\zeta_N)$ that generates the degree $p$ subextension over $\mathbf{Q}$ (so that $K_{(0)} = \mathbf{Q}(\zeta_p, \zeta_N^+)$), then we may take $H_1$ to be $K(\zeta_N^+)$, which is clearly unramified everywhere over $K$ (it is the genus field). We will show that $H_2$ is is also unramified everywhere over $K$. Lemma 5.2 takes care of the primes above $N$, and so it remains to treat the primes above $p$.

We begin by proving that $H_2(\zeta_p)/L$ is unramified. Lemma 5.12 shows that the extension $H_2 \cdot F_2/F_2$ is unramified. Since $F_2/L$ is unramified, it follows that $H_2(\zeta_p)/L$ is unramified, as claimed. We now use the fact that $H_2(\zeta_p)/L$ is unramified to show that $H_2/K$ is unramified. We consider two cases. Suppose first that $p \| N - 1$. Then $K$ is totally ramified at $p$, and thus if $H_2/K$ is ramified we deduce that since $H_2$ is *Galois* over $K$, $e_p(H_2) = p^2$, contradicting the fact that $H_2(\zeta_p)/L$ is unramified. If instead $N \equiv 1 \mod p^2$, then things are even easier: If $H_2/K$ is ramified at at least one prime $\mathfrak{p}$ above $p$, then again using the fact that $H_2/K$ is Galois we deduce that $p | e_{\mathfrak{p}}(H_2)$. Yet $p$ is tamely ramified in $L$ and therefore also in $H_2(\zeta_p)$. Thus $H_2/K$ is unramified everywhere, and $K$ has $p$-rank at least two. □

This completes the proof of parts two of Theorems 1.2 and 1.3. We expect (based on the numerical evidence) that the condition that the class group of $K$ has $p$-rank two is equivalent to the existence of an appropriate group scheme, and thus to $g_p > 1$. Part of this could perhaps be proved by more sophisticated versions of Lemmas 5.9, 5.10, and 5.11.

## 6. Examples

The first example in Mazur's table [7] where $e_2 > 1$ occurs when $N = 41$. The class group of $\mathbf{Q}(\sqrt{-41})$ is $\mathbf{Z}/8\mathbf{Z}$. Thus one has $e_2 = 3$. Using gp one finds that that the class group of $\mathbf{Q}(\sqrt{-21929})$ is $\mathbf{Z}/256\mathbf{Z}$. Independently, using William Stein's programmes, one finds that $e_2 = 127$ for $N = 21929$. In Mazur's table, $e_3$ always equals 1 or 2. One has to go quite some distance before finding an example where $e_3 > 2$. For $N = 2143$, however, one has $e_3 = 3$. This is related to the fact that 2143 is the smallest prime congruent to 1 mod 9 such that the class group of the corresponding extension $K_{(0)}$ of $\mathbf{Q}(\sqrt{-3})$ (in the terminology of Proposition 5.4) has an element of order 9. The corresponding class field contributes to the maximal unramified *solvable* extension of $K = \mathbf{Q}(\sqrt[3]{2143})$. Finally, let us note that when $p = 3$, Lemmas 5.9 and 5.11 show that the value of $g_p$ is related to the *size* of the 3-power part of the class group of $\mathbf{Q}(\sqrt[3]{N})$, whereas for $p \geq 5$, Lemma 5.13 shows that this value is related to the $p$-rank of the class group of $\mathbf{Q}(\sqrt[p]{N})$. As an illustration, when $N = 4261$, one computes that the class group of $\mathbf{Q}(\sqrt[5]{4261})$ is $\mathbf{Z}/25\mathbf{Z}$. However, since the 5-rank of $\mathbf{Z}/25\mathbf{Z}$ is one, it follows that $e_5 = 1$.

## References


1. Buzzard, K.: Questions about slopes of modular forms. To appear in Astérisque
2. Fontaine, J.M.: Groupes finis commutatifs sur les vecteurs de Witt. C. R. Acad. Sci., Paris, Sér. A **280**, 1423–1425 (1975)
3. Fontaine, J.: Il n'y a pas de variété abélienne sur **Z**. Invent. Math. **81**, 515–538 (1985)
4. Gerth III, F.: Ranks of 3-class groups of non-Galois cubic fields. Acta Arith. **30**, 307–322 (1976)
5. Halter–Koch, F.: Einheiten und Divisorenklassen in Galois'schen algebraischen Zahlkörpern mit Diedergruppe der Ordnung $2l$ für eine ungerade Primzahl $l$. Acta Arith. **33**, 355–364 (1977)
6. Lenstra Jr., H.W.: Complete intersections and Gorenstein rings. In: Elliptic curves, modular forms and Fermat's Last Theorem, ed. by J. Coates, S.T. Yau. Cambridge: International Press 1995
7. Mazur, B.: Modular curves and the Eisenstein ideal. Publ. Math., Inst. Hautes Étud. Sci. **47**, 33–186 (1977)
8. Mazur, B.: An introduction to the deformation theory of Galois representations. In: Modular forms and Fermat's last theorem (Boston, MA, 1995), pp. 243–311. New York: Springer 1997
9. Merel, L.: L'accouplement de Weil entre le sous-groupe de Shimura et le sous-groupe cuspidal de $J_0(p)$. J. Reine Angew. Math. **477**, 71–115 (1996)
10. Oort, F.: Commutative group schemes. Lect. Notes Math., vol. 15. Springer 1966
11. Oort, F., Tate, J.: Group schemes of prime order. Ann. Sci. Éc. Norm. Supér., IV. Sér. **3**, 1–21 (1970)
12. Quillen, D.: Higher algebraic $K$-theory. I. In: Algebraic $K$-theory, I: Higher $K$-theories (Proc. Conf., Battelle Memorial Inst., Seattle, Wash., 1972). Lect. Notes Math., vol. 341, pp. 85–147. Berlin: Springer 1973
13. Ramakrishna, R.: On a variation of Mazur's deformation functor. Compos. Math. **87**, 269–286 (1993)

14. Raynaud, M.: Schémas en groupes de type $(p, \ldots, p)$. Bull. Soc. Math. Fr. **102**, 241–280 (1974)
15. Scholz, A.: Idealklassen und Einheiten in kubischen Körpern. Monatsh. Math. Phys. **40**, 211–222 (1933)
16. Skinner, C., Wiles, A.: Ordinary representations and modular forms. Proc. Natl. Acad. Sci. USA **94**, 10520–10527 (1997)
17. Wiles, A.: Modular elliptic curves and Fermat's Last Theorem. Ann. Math. **141**, 443–551 (1995)