Compositio Math. 142 (2006) 63–83
doi:10.1112/S0010437X05001661

Eisenstein deformation rings

Frank Calegari

Abstract

We prove $R = \mathbf{T}$ theorems for certain reducible residual Galois representations. We answer in the positive a question of Gross and Lubin on whether certain Hecke algebras $\mathbf{T}$ are discrete valuation rings. In order to prove these results we determine (using the theory of Breuil modules) when two finite flat group schemes $\mathscr{G}$ and $\mathscr{H}$ of order p over an arbitrarily tamely ramified discrete valuation ring admit an extension not killed by p.

1. Introduction

In a previous paper [CE05], Emerton and the author studied modular deformation problems associated to certain *reducible* representations. In particular, for odd primes p we considered the totally split representation $\overline{\rho}$ given by

$$\begin{pmatrix} 1 & 0 \\ 0 & \chi \end{pmatrix} \mod p,$$

where χ was the p-adic cyclotomic character. It was proved in [CE05] that deformations of $\overline{\rho}$ finite flat at p and satisfying a certain 'semistability' condition at an auxiliary prime N were modular of level $\Gamma_0(N)$, and the associated universal deformation ring R was isomorphic to $\mathbf{T}_{\mathfrak{I}}$, where $\mathbf{T}$ was the full Hecke algebra of level $\Gamma_0(N)$ and $\mathfrak{I}$ was the p-Eisenstein ideal. This enabled us to study the Eisenstein ideal by directly studying deformations of $\overline{\rho}$. In this paper, which can be seen as a sequel to [CE05], we study *non-split* reducible representations $\overline{\rho}$ which are ramified only at p. Under certain natural hypotheses, these representations are modular, and arise from cuspidal modular forms of weight 2 and level $\Gamma_1(p)$ or $\Gamma_0(p^2)$. We define certain deformation problems for $\overline{\rho}$ such that the associated universal deformation ring can be identified with the appropriate Hecke algebra localized at the Eisenstein ideal, and use this to deduce properties of the Hecke algebras in these cases.

There are several important differences in the techniques of this paper from those of [CE05]. In [CE05], the residual Eisenstein representation of level $\Gamma_0(N)$ is not minimal – it has Serre conductor 1. Thus one could play off the minimal and non-minimal deformation problems using techniques of Wiles. In this paper, $\overline{\rho}$ is minimal of the appropriate level, and the minimal deformation problem is not trivially $\mathbf{Z}_p$, as it was in [CE05]. The techniques used to prove modularity in this paper are quite different. One ingredient is the following trivial observation. Suppose the following are true:

(i) $R \to \mathbf{T}$ is surjective;

(ii) $\mathbf{T} \neq \mathbf{T}/p^n$ for any n;

(iii) R is a discrete valuation ring.

Received 9 September 2004, accepted in final form 25 February 2005.
2000 Mathematics Subject Classification 11F80.
Keywords: Galois representations, modular forms.
The author is supported in part by the American Institute of Mathematics.

Then $R = \mathbf{T}$. By considering some very general properties of residual representations we establish a criterion that allows us to establish in many cases that R *is* a discrete valuation ring. For universal deformation rings R for which this criterion does not apply, we construct another universal deformation ring R' (corresponding to certain modular forms of level 1) such that we may apply our criterion to deduce that R' is a discrete valuation ring. We then prove that $R/p = R'/p = \mathbf{T}/p$, and deduce from this that $R = \mathbf{T}$.

In our deformation problems we consider finite flat group schemes over bases $\mathcal{O}_K$ such that $e(K) > p-1$, and thus we are forced to utilize the theory of Breuil modules [Bre00]. In particular, we need to consider finite flat group schemes $\mathscr{G}/\mathcal{O}_K$ that are not killed by p, which leads to certain delicate computations with modules over divided power rings. As a consequence, however, we prove an independently interesting result about certain group schemes of order p^2 (see Theorem 2.7).

As in [CE05], the results of Skinner and Wiles [SW97] proving $R = \mathbf{T}$ theorems for reducible representations do not apply, since our representations $\overline{\rho}$ are either locally split or are associated to non-ordinary deformation problems.

For the case of representations $\overline{\rho}$ of level $\Gamma_1(p)$, we are forced to make certain divisibility assumptions on Bernoulli numbers. Probabilistically, these assumptions should fail at most finitely often, but we have no proof of this fact. It is clear that certain assumptions are required, however. For example, without the assumption that the χ^{1-k}-eigenspace of the class group of $\mathbf{Q}(\zeta_p)$ is cyclic, it is not even clear that the residual representations $\overline{\rho}$ we consider are modular. These assumptions play no role in the $\Gamma_0(p^2)$ case, however.

2. Results

Let p be an odd prime, let $K = \mathbf{Q}(\zeta_p)$, and let $K^+ = \mathbf{Q}(\zeta_p)^+$ be the totally real subfield of K. Fix once and for all an embedding $\overline{\mathbf{Q}} \to \overline{\mathbf{Q}}_p$, and let K_p and K_p^+ denote the respective localizations of K and K^+ inside $\overline{\mathbf{Q}}_p$. Let $2 < k < p-1$ be an even integer, and suppose that the χ^{1-k}-eigenspace of the class group of K is cyclic. This is a well known consequence of Vandiver's conjecture (see for example [Gre01]). Let χ be the cyclotomic character, and let $\omega \equiv \chi \bmod p$ be the Teichmüller character. Let B_n denote the classical Bernoulli numbers, defined as follows:

$$\frac{te^t}{e^t - 1} = \sum_{n=0}^{\infty} \frac{B_n t^n}{n!}.$$

If φ is a character of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ of conductor p then one may also define Leopoldt's generalized Bernoulli numbers $B_{n,\varphi}$ by the following generating series:

$$\sum_{k=0}^{p-1} \frac{\varphi(k) t e^{kt}}{e^{pt} - 1} = \frac{B_{n,\varphi} t^n}{n!}.$$

For integral $n \geqslant 1$ one has the following congruence [Lan78, Theorem 2.3]:

$$\frac{1}{n} B_{n,\omega^{k-n}} \equiv \frac{1}{k} B_k \mod p.$$

Let $\overline{\rho}$ be the unique non-split representation

$$\begin{pmatrix} 1 & \star \\ 0 & \chi^{k-1} \end{pmatrix} \mod p$$

that is unramified over K. It follows from [Rib76] that $\overline{\rho}$ is modular of weight 2 and level $\Gamma_1(p)$. Let $\overline{V}$ be the two-dimensional vector space on which $\overline{\rho}$ acts. We consider the following deformation problem for $\overline{\rho}$: for a local artinian ring A with residue field $\mathbf{F}_p$, let $\mathcal{D}(A)$ denote the set of deformations (ρ, V)

of $(\overline{\rho}, \overline{V})$ satisfying the following properties:

(i) the determinant of ρ is $\chi \cdot \omega^{k-2}$;

(ii) the representation ρ is unramified outside p;

(iii) the representation $\rho_{K_p^+}$ on V is the generic fibre of a finite flat group scheme $\mathscr{G}/\mathcal{O}_{K_p^+}$.

Since $e(K_p^+) = \frac{1}{2}(p-1) < p-1$, the finite flat group scheme $\mathscr{G}$ is determined up to isomorphism by ρ. The following result is standard.

Theorem 2.1. *The functor $\mathcal{D}$ is (pro)-representable by a universal deformation ring R.*

Definition 2.2. Fix k. Let $\mathbf{T}$ be the cuspidal Hecke algebra of weight 2 and level $\Gamma_1(p)$ generated by T_ℓ for $\ell \neq p$. Then the (p,k)-Eisenstein ideal $\mathfrak{I}$ is the maximal ideal of $\mathbf{T}$ containing $T_\ell - 1 - \ell^{k-1}$ for all $\ell \neq p$.

Since it will be clear from the context, we usually refer to $\mathfrak{I}$ as the Eisenstein ideal. Note that we define $\mathfrak{I}$ to be maximal, contrary to the usual definition. Since we are only interested in $\mathbf{T}_\mathfrak{I}$, however, there should hopefully be no confusion. We prove the following theorem.

Theorem 2.3. *Suppose that either $p \| B_{2,\omega^{k-2}}$ or $p \| B_k$. Then there is a natural isomorphism $R \simeq \mathbf{T}_\mathfrak{I}$. The ring R is monogenic over $\mathbf{Z}_p$, and if $p \| B_{2,\omega^{k-2}}$, then R is a discrete valuation ring.*

The other residual representations we consider in this paper are wildly ramified, and arise from level $\Gamma_0(p^2)$. Let p be prime, and let $k < p-1$ be a positive integer such that

$$k \neq 0,\ 1,\ \frac{p-1}{2},\ \frac{p+1}{2}.$$

Let $k' < p-1$ be the unique positive integer such that $k' + k \equiv \frac{1}{2}(p+1) \bmod p-1$, and assume that $p \nmid B_{2k}$ and $p \nmid B_{p+1-2k}$. Let $\overline{\rho}$ be the unique non-split representation of the form

$$\begin{pmatrix} \chi^k & \star \\ 0 & \chi^{1-k} \end{pmatrix} \mod p$$

that is unramified away from p. The Bernoulli condition ensures that any non-split representation is wildly ramified at p. The existence and uniqueness of $\overline{\rho}$ is a simple exercise in class field theory. The representation $\overline{\rho}$ is modular of weight 2 and level $\Gamma_0(p^2)$, and if $2k > p+1$ actually occurs as a subrepresentation of the Jacobian $J_0(p^2)$ (see [GL86]). The Bernoulli number condition also ensures that $\overline{\rho}$ is not a twist of a representation coming from $\Gamma_1(p)$ (necessarily of the other residual representations we are considering), and thus $\overline{\rho}$ is 'genuinely' of level p^2. Let $K/\mathbf{Q}_p$ denote a tamely ramified extension of degree $p+1$. Let $\overline{V}$ be the two-dimensional vector space on which $\overline{\rho}$ acts. We consider the following deformation problem for $\overline{\rho}$: for a local artinian ring A with residue field $\mathbf{F}_p$, let $\mathcal{D}(A)$ denote the set of deformations (V, ρ) of $(\overline{V}, \overline{\rho})$ to A satisfying the following properties:

(i) the determinant of ρ is χ;

(ii) the representation ρ is unramified outside p;

(iii) the representation $\rho|_K$ on V is the generic fibre of a finite flat group scheme $\mathscr{G}/\mathcal{O}_K$.

Since $e(K) = p+1 \geqslant p-1$, finite flat group schemes are typically not determined by their generic fibre. It transpires, however, that for the choice of k above (in particular $2k \not\equiv 0, 2 \bmod p-1$) that $\overline{\rho}$ *does* uniquely determine a finite flat group scheme $\mathscr{G}/\mathcal{O}_K$. We have the following theorem.

Theorem 2.4. *The functor $\mathcal{D}$ is (pro)-representable by a universal deformation ring R.*

Definition 2.5. Let $\mathbf{T}$ be the cuspidal Hecke algebra of weight 2 and level $\Gamma_0(p^2)$. Then the (p,k)-Eisenstein ideal is the maximal ideal $\mathfrak{I}$ of $\mathbf{T}$ containing $T_\ell - \ell^k - \ell^{p-k}$ for all $\ell \neq p$.

We prove the following theorem.

Theorem 2.6. *There is a natural isomorphism $R \simeq \mathbf{T}_\mathfrak{I}$. The ring R is a discrete valuation ring. If $p \equiv 3 \bmod 4$ and $k = k' = (3p-1)/4$, then $R \simeq \mathbf{Z}_p$.*

This theorem was the main motivation for this paper. It answers a question of Gross and Lubin [GL86, p. 310], who asked whether $\mathbf{T}_\mathfrak{I}$ was always a discrete valuation ring.

Our last result is a consequence of finite flat group scheme calculations required to prove Theorem 2.6, although it is interesting in its own right. First recall that (after choosing a uniformizer $\pi \in \mathcal{O}_K$) a finite flat group scheme $\mathscr{G}/\mathcal{O}_K$ of order p is specified by its Oort–Tate parameters, a pair (r,a) with $r \in \mathbf{Z}$ satisfying $0 \leqslant r \leqslant e = e(K/\mathbf{Q})$, and $a \in \mathcal{O}_K/\mathfrak{m}$.

Theorem 2.7. *Let $K/\mathbf{Q}_p$ be a finite extension of ramification degree e, where $(e,p) = 1$. Consider an exact sequence of finite flat group schemes:*

$$0 \to \mathscr{H}' \to \mathscr{H} \to \mathscr{H}'' \to 0$$

and suppose that $\mathscr{H}'$ and $\mathscr{H}''$ are finite flat group schemes of order p. Then one of the following holds:

(i) *$\mathscr{H}$ is killed by p;*

(ii) *$\mathscr{H}$ is étale or multiplicative, and $\mathscr{H}[p]$ is finite flat;*

(iii) *there exists a non-trivial morphism $\mathscr{H}'' \to \mathscr{H}'$ that is* not *an isomorphism, and $\mathscr{H}[p]$ is not a finite flat group scheme.*

Moreover, given a non-trivial morphism $\mathscr{H}'' \to \mathscr{H}'$ there exists an extension $\mathscr{H} \in \mathrm{Ext}(\mathscr{H}'', \mathscr{H}')$ such that $\mathscr{H} \neq \mathscr{H}[p]$ if and only if the Oort–Tate parameters (s,b) of $\mathscr{H}'$ and (r,a) of $\mathscr{H}''$ satisfy either of the following inequalities: $r \geqslant ps$ or $(e-s) \geqslant p(e-r)$.

3. Generalities on Eisenstein representations

The main reference for this section is the paper of Bellaïche and Chenevier [BC05]. In this section we record some general remarks about residually reducible representations. Let $(A, \mathfrak{m}, k)$ be a local p-adically complete ring. Given a representation $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(A)$ such that

$$\overline{\rho} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(A/\mathfrak{m}) = \mathrm{GL}_2(k)$$

is reducible and unramified outside p and ∞, we shall derive a sufficient criterion for A to be a discrete valuation ring. The results of this section should not be considered original, and follow almost directly from the arguments of [BC05]. The spirit of these arguments is also very similar to the work of Ribet and Papier [RP81]. We shall use the notation of [BC05], however.

Let G be a quotient of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ such that ρ factors through G. We may consider ρ as a representation of G into $\mathrm{GL}_2(A)$. Let $T : G \to A$ denote the composite of ρ with the trace map. Suppose that the semi-simplification $(\overline{\rho})^{\mathrm{ss}}$ is given by $\chi_1 \oplus \chi_2$. We shall assume that $\chi_1 \neq \chi_2$. Fix $s \in G$ such that $\chi_1(s) \neq \chi_2(s)$. The characteristic polynomial of $\rho(s)$ has two distinct roots modulo $\mathfrak{m}$, and thus by Hensel's Lemma has roots λ_1 and λ_2 with $\lambda_i \equiv \chi_i(s) \bmod \mathfrak{m}$. Choose a basis of the representation ρ such that $\rho(s)e_i = \lambda_i e_i$. Let a, b, c, d be the matrix entries of ρ with respect to this basis, and let B and C be the A-ideals generated by $b(g)$ and $c(g)$ respectively, for $g \in G$. Let $I \subset A$ be a proper ideal such that $T \bmod I$ can be written as the sum of two characters ψ_1, ψ_2 such that $\psi_i \bmod \mathfrak{m} = \chi_i$.

Lemma 3.1. *For all g, $g' \in G$, $a(g) - \psi_1(g) \in I$, $b(g) - \psi_2(g) \in I$, and $b(g)c(g') \in I$.*

Proof. This is Lemme 1 of [BC05]. □

Lemma 3.2. *There is an injection of A-modules*

$$\mathrm{Hom}_A(B/IB, A/I) \to \mathrm{Ext}^1_{(A/I)[G]}(\psi_2, \psi_1).$$

Definition 3.3. The ideal of reducibility of A is the largest ideal of A such that $T \bmod I$ is the sum of two characters. There is an equality $I = BC$.

Lemma 3.4. *Suppose that A is noetherian, that the ideal of reducibility is maximal, and that*

$$\dim_k \mathrm{Ext}^1_{k[G]}(\chi_2, \chi_1) = \dim_k \mathrm{Ext}^1_{k[G]}(\chi_2, \chi_1) = 1.$$

Then the maximal ideal $\mathfrak{m}$ of A is principal. If moreover A admits a surjective map to a ring of characteristic zero, then A is a discrete valuation ring.

Proof. One has $\dim_k B \otimes_A k \leqslant 1$. Thus by Nakayama's Lemma, B is a cyclic A-module, and hence principal. A similar argument applies to C, and thus $\mathfrak{m} = I = BC$ is principal. Let $\mathfrak{m} = (\pi)$. By Krull's Intersection Theorem each element of A is of the form $u\pi^k$ for some unit $u \in A$. Since A admits a surjective map to a ring of characteristic zero, π is not nilpotent. Thus A is a discrete valuation ring. □

3.1 The general strategy

Let us now explain the general strategy of this paper. In both cases we are considering a reducible representation $\overline{\rho}$, and a suitable universal deformation

$$\rho^{\mathrm{univ}} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(R)$$

unramified outside p and ∞. If $\mathbf{Q}_{\{p,\infty\}}$ denotes the maximal extension of $\mathbf{Q}$ unramified outside p and ∞, then ρ^{univ} *a fortiori* factors through $\mathrm{Gal}(\mathbf{Q}_{\{p,\infty\}}/\mathbf{Q})$. Moreover, in either case χ_1/χ_2 is some non-trivial power of the cyclotomic character, and so of the form χ^i for some $i \neq 0$. Our assumptions regarding Vandiver's conjecture (in the case of $\Gamma_1(p)$, and automatically in the case of $\Gamma_0(p^2)$) imply that $\mathrm{Ext}^1_{\mathbf{F}_p[G]}(1, \chi^i)$ and $\mathrm{Ext}^1_{\mathbf{F}_p[G]}(1, \chi^{-i})$ are one-dimensional, where $G = \mathrm{Gal}(\mathbf{Q}_{\{p,\infty\}}/\mathbf{Q})$. The universal deformation rings are topologically finitely generated over $\mathbf{Z}_p$ and thus noetherian. Thus if I is the ideal of reducibility of R, then I is principal. Providing R admits a surjection to $\mathbf{T}$, we infer that R is a discrete valuation ring whenever the ideal of reducibility is maximal. The following lemma is trivial.

Lemma 3.5. *The ideal I of R is maximal if and only if there does not exist a surjection $R/I \to \mathbf{F}_p[x]/x^2$ or $R/I \to \mathbf{Z}/p^2\mathbf{Z}$.*

In view of the description of R as a universal deformation ring, it therefore suffices to show that $\overline{\rho}$ does not admit any non-trivial deformations to $\mathrm{GL}_2(\mathbf{F}_p[x]/x^2)$ or $\mathrm{GL}_2(\mathbf{Z}/p^2\mathbf{Z})$ that are upper triangular. For the representations we consider of level $\Gamma_0(p^2)$, it turns out that there are never any such deformations. For level $\Gamma_1(p)$, however, their may exist upper triangular deformations to $\mathbf{Z}/p^2\mathbf{Z}$. This happens whenever $p^2 | B_{2,\omega^{k-2}}$ (I do not know any example where this happens, although it is conjectured to happen infinitely often). To deal with this possibility, we switch to another deformation ring R' corresponding to deformations of $\overline{\rho}$ that arise from modular forms of weight k and level $\Gamma_0(1)$. The ring R' is a discrete valuation ring whenever $p^2 \nmid B_k$ by the same proof as in Lemma 3.4. By our assumptions on Bernoulli number divisibility this is always the case. Thus the failure of R to be a discrete valuation ring forces R' to be a discrete valuation ring. In this situation we find that $R' \simeq \mathbf{T}'$, where $\mathbf{T}'$ is the cuspidal Hecke algebra of weight k and level $\Gamma_0(1)$

localized at the Eisenstein ideal. One knows, however, that $\mathbf{T}'/p \simeq \mathbf{T}/p$. Moreover, by purely local considerations it follows that $R'/p \simeq R/p$. From these facts (along with the observation that $\mathbf{T}$ is torsion free) we may conclude that $R = \mathbf{T}$.

One of the main technical difficulties of the paper is determining the upper triangular deformations of $\overline{\rho}$ to $\mathbf{F}_p[x]/x^2$ and $\mathbf{Z}/p^2\mathbf{Z}$. Note that it is *not* always the case that the 'Eisenstein ideal' as defined by Mazur (and others) is the ideal of reducibility. Indeed, for $J_0(N)$ this is never the case. For example, for $N = 11$, the Hecke algebra $\mathbf{T} \simeq \mathbf{Z}$ and the Eisenstein ideal $\mathfrak{I} \simeq (5)$. However, one easily finds that the ideal of reducibility is (25). This was noted by Serre, and in the optic of the Eisenstein ideal was pointed out by Mazur (see for example the discussion in [Maz77, Proposition 18.9, pp. 138–139]).

As a computational observation, it is typically the case that $R = \mathbf{T}_{\mathfrak{I}} = \mathbf{Z}_p$. This is not always true, however. For example, when $p = 547$ and $k = 486$, and $\overline{\rho}$ is the residual representation of level $\Gamma_1(547)$, then using William Stein's Modular Forms Database one finds that

$$\mathbf{T}_{\mathfrak{I}}/p \simeq \mathbf{F}_p[x]/x^2.$$

Similarly, although I know of no examples, there is no reason why p^2 cannot divide $B_{2,\omega^{k-2}}$. Note, however, that if both conditions occur simultaneously, then R *cannot* be a discrete valuation ring. This follows from the fact that the ideal of reducibility $I = (a)$ is principal, and the only discrete valuation ring R that admits a surjection $R/a \to \mathbf{Z}/p^n$ for some $n \geqslant 2$ is $\mathbf{Z}_p$.

4. Deformations of level $\Gamma_1(p)$ and $\Gamma_0(p^2)$

4.1 Eisenstein deformations at level $\Gamma_1(p)$

Let $2 \leqslant k < p-1$. The residual representations considered in this section were studied by Ribet [Rib76], who proved that, whenever $p|B_k$ for even k, the χ^{1-k}-eigenspace of the class group of $K = \mathbf{Q}(\zeta_p)$ is non-trivial (the converse of this statement is a more classical theorem of Herbrand). Moreover, given such a p and k, there exists a non-split representation

$$\begin{pmatrix} 1 & \star \\ 0 & \chi^{k-1} \end{pmatrix} \mod p$$

that is unramified over K. The arguments of Ribet may be summarized as follows. Since $B_2 = 1/6$, $k \neq 2$ and thus $\chi^{k-1} \neq \chi$. Inside some variety J isogenous to $J_1(p)/J_0(p)$ one may find a non-split representation $\overline{\rho}$ of the shape above. Now J acquires everywhere good reduction over the totally real subfield K^+ of K. The results of Raynaud [Ray74] imply that group schemes over a base of ramification $e < p-1$ are determined by their generic fibre. Thus the representation $\overline{\rho}$ over K_p^+ is seen to arise from a finite flat group scheme over $\mathcal{O}_{K_p^+}$ that is an extension of a local group scheme by an étale group scheme. The connected–étale sequence therefore splits this extension of group schemes, and thus $\overline{\rho}$ is locally split at p over K. This implies that $\overline{\rho}$ is the representation considered above. Let $\overline{V}$ be the two-dimensional representation corresponding to $\overline{\rho}$. For a local artinian ring A with residue field $\mathbf{F}_p$, let $\mathcal{D}(A)$ denote the set of deformations (V, ρ) of $(\overline{V}, \overline{\rho})$ to A satisfying the following properties:

(i) the determinant of ρ is $\chi \cdot \omega^{k-2}$;

(ii) the representation ρ is unramified outside p;

(iii) the representation $\rho|_{K_p^+}$ on V arises from a finite flat group scheme over $\mathcal{O}_{K_p^+}$.

Theorem 4.1. *The functor $\mathcal{D}$ is (pro)-representable by a universal deformation ring R.*

Proof. This result can now be considered relatively standard (see for example [CDT99] and [BCDT01]). Let us make a few remarks, however. First note that $\mathrm{End}_{\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})}(\overline{V}) = \mathbf{F}_p$, and thus

the 'unadorned' universal deformation ring exists. Let us make precise what is meant by saying that $\rho_{K_p^+}$ arises from a finite flat group scheme over $\mathcal{O}_{K_p^+}$. Essentially it stipulates the existence of a group scheme $\mathscr{G}/\mathcal{O}_{K_p^+}$ such that the induced representation of $\mathrm{Gal}(\overline{\mathbf{Q}}_p/K_p^+)$ on the generic fibre gives rise to $\rho|_{K_p^+}$. Since ρ is defined over $\mathbf{Q}_p$, this implies that the generic fibre of $\mathscr{G}$ also descends to $\mathbf{Q}$. Thus we automatically obtain a pair $(\mathscr{G}, \phi)$, where $\mathscr{G}$ is a finite flat group scheme over K^+, and ϕ is an action of $\mathrm{Gal}(K^+/\mathbf{Q})$ on the generic fibre of $\mathscr{G}$ (which extends to an action on $\mathscr{G}$). One calls such a pair $(\mathscr{G}, \phi)$ a group scheme with *generic fibre descent data*. Note that since $e < p-1$, the group schemes $\mathscr{G}$ are uniquely determined by the deformations ρ. □

Lemma 4.2. *There is no non-trivial element of $\mathcal{D}(F_p[x]/x^2)$ such that ρ is upper triangular. The ring R is generated as a $\mathbf{Z}_p$-algebra by traces.*

Proof. Suppose that $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{F}_p[x]/x^2)$ is upper triangular, and let $\mathscr{G}/\mathcal{O}_{K_p^+}$ be the associated finite flat group scheme. Let ψ be the character corresponding to the upper left-hand corner of the representation. Then the Galois representation $\psi|_{K_p^+}$ gives rise to a subrepresentation of the generic fibre of $\mathscr{G}$, and thus to a finite flat subgroup scheme $\mathscr{H}$ of $\mathscr{G}$. The generic fibre of $\mathscr{H}$ has a filtration by constant Galois modules. Since $e = \frac{1}{2}(p-1) < p-1$, $\mathscr{H}$ is therefore an extension of constant group schemes. Thus $\mathscr{H}$ is an extension of étale group schemes, and therefore $\mathscr{H}$ is étale. Thus ψ considered as a character of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ is unramified at p and thus unramified everywhere. By simple class field theory it follows that ψ is trivial. In particular, ρ must have the shape:

$$\begin{pmatrix} 1 & \star \\ 0 & \chi^{k-1} \end{pmatrix} \in \mathrm{GL}_2(\mathbf{F}_p[x]/x^2).$$

As in Ribet [Rib76], the connected–étale sequence implies that $\mathscr{G}$ splits over $\mathcal{O}_{K_p^+}$, and thus that ρ is unramified over K^+. If ρ defines a non-trivial representation to $\mathrm{GL}_2(\mathbf{F}_p[x]/x^2)$, we see that its kernel must cut out a $(\mathbf{Z}/p\mathbf{Z})^2$ unramified extension of $\mathbf{Q}(\zeta_p)$. Since this contradicts our assumptions on $\overline{\rho}$, the result follows. To show that R is generated by traces, it suffices to show that any non-trivial deformation of $\overline{\rho}$ to $\mathrm{GL}_2(\mathbf{F}_p[x]/x^2)$ is generated by traces. This follows in a standard way from the fact that (by Nakayama's Lemma) R is generated as a $\mathbf{Z}_p$-algebra by the generators of $\mathfrak{m}_R/(\mathfrak{m}_R^2, p)$. Let ρ be a deformation of $\overline{\rho}$ to $\mathrm{GL}_2(\mathbf{F}_p[x]/x^2)$ that cannot be written as an upper triangular representation. Write the matrix entries of ρ as functions a, b, xc and d of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Then if $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}(\zeta_p))$, then $\mathrm{Det}(\rho(\sigma)) - \mathrm{Trace}(\rho(\sigma)) = xb(\sigma)c(\sigma)$. Since c is non-trivial (by assumption), the Cebotarev density theorem implies there exists a σ such that $b(\sigma)c(\sigma) \neq 0$. Since $\mathrm{Det}(\rho(\sigma)) = 1$, it follows that the traces of ρ generate $\mathbf{F}_p[x]/x^2$. □

Definition 4.3. Let $\mathbf{T}$ be the cuspidal Hecke algebra of weight 2 and level $\Gamma_1(p)$. Then the (p,k)-Eisenstein ideal $\mathfrak{J}$ is the maximal ideal of $\mathbf{T}$ containing $T_\ell - 1 - \ell^{k-1}$ for all $\ell \neq p$.

Lemma 4.4. *There exists a surjective map $R \to \mathbf{T}_\mathfrak{J}$.*

Proof. If $\widetilde{\mathbf{T}}_\mathfrak{J}$ denotes the normalization of $\mathbf{T}_\mathfrak{J}$, then we may write $\widetilde{\mathbf{T}}_\mathfrak{J} = \prod_{i=1}^d \mathcal{O}_i$, where each $\mathcal{O}_i$ is a discrete valuation ring finite over $\mathbf{Z}_p$. The rings $\mathcal{O}_i$ are in bijection with normalized newforms f of level $\Gamma_1(p)$ such that if ρ_f is an integral p-adic Galois representation associated to f, then $(\overline{\rho}_f)^{\mathrm{ss}} = (\overline{\rho})^{\mathrm{ss}}$. Arguing as in Ribet [Rib76], for each form f, there exists a lattice such that the reduction $\overline{\rho}_f$ is a non-split extension of χ^{k-1} by 1. Since f has level $\Gamma_1(p)$ this implies that $\overline{\rho}_f$ splits over K_p and thus is unramified after restriction to K. By assumption (on the cyclicity of the χ^{1-k}-eigenspace of the class group) this uniquely determines $\overline{\rho}_f$, and thus $\overline{\rho}_f = \overline{\rho}$. It follows that ρ_f is a deformation of $\overline{\rho}$, and thus there exists a map $R \to \mathcal{O}_i$. In particular, we obtain a map $R \to \prod_{i=1}^d \mathcal{O}_i = \widetilde{\mathbf{T}}_\mathfrak{J}$. Since R is generated by traces, the image R is also generated by traces. The image of $\mathrm{Trace}(\rho^{\mathrm{univ}}(\mathrm{Frob}_\ell))$ for $\ell \neq p$ is $T_\ell \in \mathbf{T}$. Since Frobenius elements are dense in $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, the image of R is exactly $\mathbf{T}_\mathfrak{J}$. □

Lemma 4.5. *If $p^2 \nmid B_{2,\omega^{k-2}}$ then there are no deformations of $\overline{\rho}$ in $\mathcal{D}(\mathbf{Z}/p^2\mathbf{Z})$ that are upper triangular.*

Proof. As in Lemma 4.2, the character ψ corresponding to the upper left-hand corner must be trivial, and thus ρ is of the form

$$\begin{pmatrix} 1 & \star \\ 0 & \chi\omega^{k-2} \end{pmatrix} \in \mathrm{GL}_2(\mathbf{Z}/p^2\mathbf{Z}),$$

where $\rho|_{\mathbf{Q}_p(\zeta_{p^2})}$ is totally split. Thus this defines a degree p^2 unramified extension of $\mathbf{Q}(\zeta_{p^2})$, which implies the divisibility of Bernoulli numbers. □

Corollary 4.6. *Suppose that $p^2 \nmid B_{2,\omega^{k-2}}$. Then R is a discrete valuation ring and $R = \mathbf{T}$.*

Proof. By Lemmas 4.2 and 4.5, we conclude that the ideal of reducibility I of R is maximal. Since $R \to \mathbf{T}$, p is not nilpotent in R, and thus R is a discrete valuation ring. That $R \simeq \mathbf{T}$ is then obvious, since $\mathbf{T}$ is non-trivial and has characteristic zero. □

Thus to complete the proof of Theorem 2.3 we are now left to consider the case that $p^2 | B_{2,\omega^{k-2}}$. We may therefore assume that $p \| B_k$. Note that, for any p, the naive probability that there exists a $2 \leqslant k < p-1$ such that $p^2 \| B_{2,\omega^{k-2}}$ is approximately $1/p$. The further condition that $p^2 \| B_k$ decreases this probability to $1/p^2$. Thus one might suppose that the divisibilities $p^2 | B_k$ and $p^2 | B_{2,\omega^{k-2}}$ occur at most finitely often for all p. I do not know of any examples in which either condition is satisfied.

Let us now assume that $p \| B_k$. Instead of proving the modularity of R directly, we shall switch to another deformation problem. We note, firstly, that the representation $\overline{\rho}$ is modular of level 1 and weight k. Certainly there exists a non-split representation $\overline{\rho}'$ of that level with $(\overline{\rho}')^{\mathrm{ss}} = (\overline{\rho})^{\mathrm{ss}}$. On the other hand, $\overline{\rho}'$ is crystalline (in the sense of Fontaine and Laffaille [FL82]) with Hodge–Tate weights $[0, k-1]$, which must necessarily be split locally over K_p. By our assumptions such a representation is unique, so it must equal $\overline{\rho}$. We define the following deformation problem $\mathcal{D}'$.

(i) The determinant of ρ is χ^{k-1}.

(ii) The representation ρ is unramified outside p.

(iii) The representation ρ is ordinary at p, i.e. there exists an exact sequence

$$0 \to V' \to V \to V'' \to 0,$$

where V' and V'' are free A-modules of rank 1, and $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ acts on V'' via an unramified character.

Theorem 4.7. *The functor $\mathcal{D}'$ is representable by a universal deformation ring R'. Moreover, if A is an artinian ring killed by p, then $\mathcal{D}(A) \subseteq \mathcal{D}'(A)$, and thus there is a surjection $R'/p \to R/p$.*

Proof. The existence of R' is standard. One could also try to define $\mathcal{D}'$ to be deformations that are crystalline with Hodge–Tate weights $[0, k-1]$ and presumably this would define an equivalent functor. Let (ρ, V) be a deformation in $\mathcal{D}(A)$. Consider the connected–étale sequence attached to the finite flat group scheme associated to ρ. On generic fibres, it induces an exact sequence

$$0 \to V' \to V \to V'' \to 0.$$

Since $\overline{V}''$ and $\overline{V}'$ are one-dimensional it follows from Nakayama's Lemma that V'' and V' are cyclic. By a counting argument it follows that V' and V'' are free. Since $e = \frac{1}{2}(p-1) < p$, this splitting descends to $\mathbf{Q}_p$, and it follows that V is ordinary. The existence of a surjection $R'/p \to R/p$ follows by Yoneda's Lemma. □

Note that this argument also implies that deformations $\rho \in \mathcal{D}(A)$ are in general ordinary. If ρ^{mod} is the representation

$$\rho^{\mathrm{mod}} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{T}_{\mathfrak{J}}),$$

it follows that T_p is given by the action of Frobenius on the unramified quotient. Thus $T_p \in \mathbf{T}_{\mathfrak{J}}$.

Lemma 4.8. *If $p \| B_k$ then R' is a discrete valuation ring.*

Proof. Let I' be the ideal of reducibility of R'. The case of upper triangular deformations to $\mathrm{GL}_2(\mathbf{F}_p[x]/x^2)$ is essentially the same argument as for R, except that now the splitting of Galois modules over K_p comes from the ordinary hypothesis rather than the connected–étale sequence. Consider a reducible deformation $\rho \in \mathcal{D}'(\mathbf{Z}/p^2\mathbf{Z})$. Let ψ be the character corresponding to the upper left-hand corner of the representation. Then $\psi|_{\mathbf{Q}_p}$ is an extension of a trivial representation by a trivial representation. If ψ is ramified at p then ρ can certainly not be ordinary, so ψ is unramified at p and thus trivial. Hence ρ is of the form

$$\begin{pmatrix} 1 & \star \\ 0 & \chi^{k-1} \end{pmatrix} \in \mathrm{GL}_2(\mathbf{Z}/p^2\mathbf{Z}).$$

Moreover the ordinary hypothesis implies that the representation must split locally over K_p. The kernel of ρ defines a degree p^2 unramified χ^{1-k} extension of $\mathbf{Q}(\zeta_{p^2})$, and in particular implies that $p^2 | B_k$. This contradicts our assumption. Thus I is maximal in R', and thus R' is a discrete valuation ring. □

Let $\mathbf{T}'$ be the cuspidal Hecke algebra of level 1 and weight k, and let $\mathfrak{J}$ be the Eisenstein ideal. Since $k < p-1$, the cuspidal Eisenstein deformations are ordinary and in the usual way we obtain a surjection $R' \to \mathbf{T}'_{\mathfrak{J}}$, which must be an isomorphism. Note that this is expected since ordinary representations of weight $k > 2$ are automatically crystalline. There is a standard identification $\mathbf{T}'_{\mathfrak{J}}/p \simeq \mathbf{T}_{\mathfrak{J}}/p$ which follows from the identification $S_2(\Gamma_1(p), \omega^{k-2}, \mathbf{Z}/p\mathbf{Z}) = S_k(\Gamma_0(1), \mathbf{Z}/p\mathbf{Z})$. Thus $R'/p = \mathbf{T}'_{\mathfrak{J}}/p = \mathbf{T}_{\mathfrak{J}}/p = \mathbf{F}_p[x]/x^e$ for some e (recall that R' is a discrete valuation ring, so monogenic over $\mathbf{Z}_p$). Since R'/p surjects onto R/p by Theorem 4.7 and R/p surjects onto $\mathbf{T}_{\mathfrak{J}}/p$, it follows that $R/p = \mathbf{F}_p[x]/x^e$ also. Thus there exists the following diagram.

$$\begin{array}{ccccc} \mathbf{Z}_p[[x]] & \twoheadrightarrow & R & \twoheadrightarrow & R/p \simeq \mathbf{F}_p[x]/x^e \\ & & \downarrow & & \| \\ & & \mathbf{T}_{\mathfrak{J}} & \twoheadrightarrow & \mathbf{T}_{\mathfrak{J}}/p \simeq \mathbf{F}_p[x]/x^e \end{array}$$

Since $\mathbf{T}_{\mathfrak{J}}$ is a monogenic and torsion free, it must be isomorphic to $\mathbf{Z}_p[[x]]/f$ for some polynomial $f(x) \equiv x^e \bmod p$ of degree $\leqslant e-1$. Thus $R \simeq \mathbf{Z}[[x]]/I$ with $I = Jf$. Since $R/p \simeq \mathbf{F}_p[x]/x^e$, it follows that the image of the ideal J in $\mathbf{F}_p[x]/x^e$ contains 1. Thus J contains 1, and $R \simeq \mathbf{T}_{\mathfrak{J}}$. This completes the proof of Theorem 2.3.

It was observed by Stein [CS05] that, although p can divide the discriminant of the Hecke algebra of weight 2 and level $\Gamma_0(p)$ (for example when $p = 389$), it never appears to divide the index. Equivalently, if $\mathbf{T}_{\mathfrak{m}}$ is a localization of the Hecke algebra $\mathbf{T}$ of weight 2 and level $\Gamma_0(p)$, then $\mathbf{T}_{\mathfrak{m}}$ is a discrete valuation ring. Computations of Stein also suggest this conjecture may be true at level $\Gamma_1(p)$. Although we do not prove this conjecture in the Eisenstein case, there are some interesting connections that arise. If E is an elliptic curve of conductor p then the associated Hecke algebra is an integral domain if and only if p does not divide the modular degree. As Stein notes, a result of Flach implies that the modular degree annihilates a certain Selmer group [Fla92], which can in turn be considered a form of generalized class group. Thus the conjecture that $\mathbf{T}_{\mathfrak{m}}$ is an integral domain translates into the conjecture that p does not divide the order of a certain 'class group',

and so resembles the statement of Vandiver's conjecture. For Eisenstein representations of level $\Gamma_1(p)$, we see that the same question is intimately related to the actual Vandiver's conjecture.

4.2 Eisenstein deformations at level $\Gamma_0(p^2)$

Let p be prime, and let $k < p-1$ be a positive integer such that

$$k \neq 0,\ 1,\ \frac{p-1}{2},\ \frac{p+1}{2}.$$

Let $k' < p-1$ be the positive integer such that $k + k' = \frac{1}{2}(p+1) \bmod p-1$, and assume that $p \nmid B_{2k}$ and $p \nmid B_{p+1-2k}$. Under these conditions, there is a unique representation $\overline{\rho}$ of the form

$$\begin{pmatrix} \chi^k & \star \\ 0 & \chi^{1-k} \end{pmatrix} \mod p$$

that is wildly ramified at p and unramified outside p. It follows from [GL86] that $\overline{\rho}$ is modular of weight 2 and level $\Gamma_0(p^2)$. Let $K/\mathbf{Q}_p$ denote a tamely ramified extension of degree $p+1$. We shall study deformations of $\overline{\rho}$ that arise from finite flat group schemes over K. Since $e(K) = p+1 > p-1$, however, a Galois module that arises from a finite flat group scheme does not necessarily determine a *unique* finite flat group scheme. We prove, however, the following result (see Lemma 5.18).

Theorem 4.9. *Let k be as above, and let V be the representation corresponding to $\overline{\rho}$. Then there exists a unique finite flat group scheme $\mathscr{G}/\mathcal{O}_K$ with generic fibre descent data to $\mathbf{Q}_p$ isomorphic to V.*

To prove this theorem, we need to study the category of finite flat group schemes over K. An explicit theory of finite flat group schemes over discrete valuation rings of arbitrary ramification was constructed by Breuil [Bre00].

For a local artinian ring A with residue field $\mathbf{F}_p$, let $\mathcal{D}(A)$ denote the set of deformations (V, ρ) of $(\overline{V}, \overline{\rho})$ to A satisfying the following properties:

(i) the determinant of ρ is χ;
(ii) the representation ρ is unramified outside p;
(iii) the representation $\rho|_K$ on V is the generic fibre of a finite flat group scheme $\mathscr{G}/\mathcal{O}_K$.

Note that finite flat group schemes over $\mathcal{O}_K$ do not form an abelian category. However, throughout this paper we implicitly use the following lemma.

Lemma 4.10. *Let*

$$0 \to H' \to H \to H'' \to 0$$

be a short exact sequence of finite Galois modules such that H is the generic fibre of a finite flat group scheme $\mathscr{H}/\mathcal{O}_K$. Then there exist (unique) finite flat group schemes $\mathscr{H}'$ and $\mathscr{H}''/\mathcal{O}_K$ which fit into a short exact sequence

$$0 \to \mathscr{H}' \to \mathscr{H} \to \mathscr{H}'' \to 0,$$

and such that taking generic fibres in this sequence yields the exact sequence of Galois modules above.

This lemma is proved in [Con99, § 1.1]. The group scheme $\mathscr{H}'$ will be the scheme theoretic closure of H' inside $\mathscr{H}$. Note however that, even if the map $H \to H''$ is 'multiplication by p', this does not identify $\mathscr{H}'$ with $\mathscr{H}[p]$. Indeed, it might be the case that $\mathscr{H}[p]$ is not even a finite flat group scheme. However, in view of Lemma 4.10 one certainly has the following theorem.

Theorem 4.11. *The representation $\mathcal{D}$ is representable by a universal deformation ring R.*

Proof. This follows in the standard way. □

LEMMA 4.12. *There is no non-trivial element of $\mathcal{D}(\mathbf{F}_p[x]/x^2)$ such that ρ is upper triangular. The ring R is generated by traces, and moreover there exists a surjective map $R \to \mathbf{T}_{\mathfrak{J}}$.*

Proof. Our proof is along the same lines as Lemma 4.2. Suppose that $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{F}_p[x]/x^2)$ is upper triangular, and let $\mathscr{G}/\mathcal{O}_K$ be the associated finite flat group scheme. Let ψ be the character corresponding to the upper left-hand corner of the representation. Then the Galois representation $\psi|_K$ gives rise to a subrepresentation of the generic fibre of $\mathscr{G}$, and thus to a finite flat subgroup scheme $\mathscr{H}$ of $\mathscr{G}$. The generic fibre of the group scheme $\mathscr{H}$ has a filtration by two copies of the Galois module $\mathbf{F}_p(\omega^k)$. Since $\mathbf{F}_p(\omega^k)$ extends to a unique group scheme $\mathscr{H}'$ over $\mathcal{O}_K$ by Corollary 5.17, the scheme $\mathscr{H}$ is an element of $\mathrm{Ext}^1(\mathscr{H}', \mathscr{H}')$. Moreover, $\mathscr{H}$ admits generic fibre descent data to $\mathbf{Q}_p$. It follows from Corollary 5.20 that all such extensions split over the maximal unramified extension K^{ur}. In particular, we see that the character $\psi : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{F}_p[x]/x^2$ must be the kth power of the cyclotomic character. Thus ρ must have the shape:

$$\begin{pmatrix} \chi^k & \star \\ 0 & \chi^{1-k} \end{pmatrix} \in \mathrm{GL}_2(\mathbf{F}_p[x]/x^2).$$

The kernel of ρ therefore defines a $(\mathbf{Z}/p\mathbf{Z})^2$ extension of $\mathbf{Q}(\zeta_p)$ on which $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$ acts via χ^{2k-1}. Yet since the χ^{2k-1}-eigenspace of the class group of $\mathbf{Q}(\zeta_p)$ is trivial (by assumption), the maximal χ^{2k-1} extension of $\mathbf{Q}(\zeta_p)$ has order p. Thus we have a contradiction, and no non-trivial upper triangular deformation of $\overline{\rho}$ to $\mathrm{GL}_2(\mathbf{F}_p[x]/x^2)$ exists. That R is generated by traces follows as in Lemma 4.2, and that there exists a surjective map $R \to \mathbf{T}_{\mathfrak{J}}$ follows similarly as in Lemma 4.4. It suffices to prove that the representations ρ_f do actually come from (inverse limits of) finite flat group schemes over K. This follows from [GL86, Corollary 12.5], since the associated abelian varieties acquire good reduction over the extension (there denoted by) M of ramification degree $e|p+1$. □

LEMMA 4.13. *There is no non-trivial element of $\mathcal{D}(\mathbf{Z}/p^2\mathbf{Z})$ such that ρ is upper triangular.*

Proof. Consider such a representation ρ. As in Lemma 4.12, consider the character $\psi|_K$, and the (uniquely) associated finite flat group scheme $\mathscr{H}/\mathcal{O}_K$. By considering the filtration on the generic fibre of $\mathscr{H}$, we once more infer that $\mathscr{H} \in \mathrm{Ext}^1(\mathscr{H}', \mathscr{H}')$. Since the generic fibre of $\mathscr{H}$ is not killed by p, it follows that $\mathscr{H}$ itself is not killed by p. But by Corollary 5.2, there are no extensions at all of $\mathscr{H}'$ by $\mathscr{H}'$ not killed by p! Thus we are done. □

We conclude from Lemmas 4.12 and 4.13 that the ideal of reducibility I is maximal, and thus that R is a discrete valuation ring, and $R \simeq \mathbf{T}_{\mathfrak{J}}$. To complete the proof of Theorem 2.6, we must prove that $\mathbf{T}_{\mathfrak{J}} \simeq \mathbf{Z}_p$ when $p \equiv 3 \bmod 4$ and $k = (3p-1)/4$. Since R is a $\mathbf{Z}_p$-algebra of characteristic zero, it suffices to prove that R does not admit a surjective map to $\mathbf{F}_p[x]/x^2$, or equivalently that $\mathcal{D}(\mathbf{F}_p[x]/x^2)$ is empty. We have already seen that $\mathcal{D}(\mathbf{F}_p[x]/x^2)$ does not contain any upper triangular elements. Suppose that it contains an irreducible representation ρ. Let ϱ be the twist of ρ by χ^{-k}. Then $\overline{\varrho}$ is the representation

$$\begin{pmatrix} 1 & \star \\ 0 & \omega^{(p-1)/2} \end{pmatrix}.$$

Thus the kernel of $\overline{\varrho}$ is a degree p extension of $F = \mathbf{Q}(\sqrt{-p})$, the quadratic subfield of $\mathbf{Q}(\zeta_p)$. Let $L = F.\mathbf{Q}(\zeta_p)$ be the kernel of $\overline{\varrho}$, and H the kernel of ϱ. There is an exact sequence

$$0 \to \mathrm{Gal}(H/L) \to \mathrm{Gal}(H/\mathbf{Q}) \to \mathrm{Gal}(L/\mathbf{Q}) \to 0.$$

We claim this sequence is a semidirect product. The element of order 2 in $\mathrm{Gal}(L/\mathbf{Q})$ lifts uniquely. Since $\mathrm{Gal}(L/\mathbf{Q}) \subset \mathrm{GL}_2(\mathbf{F}_p[x]/x^2)$, we see that the 2-Sylow subgroup acts an involution. Any lifting of the order p element of $\mathrm{Gal}(H/\mathbf{Q})$ (which will have order p) therefore provides a splitting.

By assumption $\varrho|_L$ is not upper triangular. It follows that $\mathrm{Gal}(H/L)$ has order p^3, and moreover H must have a subfield E such that $\mathrm{Gal}(E/F)$ has order p^2 and $\mathrm{Gal}(F/\mathbf{Q})$ acts on $\mathrm{Gal}(E/F)$ as -1. Yet this is a contradiction, since F admits at most (in fact exactly) one extension of degree p of this form. Thus ϱ and ρ must be upper triangular, a contradiction.

In general we have not ruled out the possibility that $\mathbf{T}_{\mathfrak{J}}$ is always $\mathbf{Z}_p$, but one suspects that this is a feature of the limited range of computation available.

5. Breuil modules

Throughout this section we shall freely refer to the results and notation of [Bre00]. A reference for Breuil modules killed by p as $k[u]/u^{ep}$-modules is [BCDT01], and we also use some theorems of Savitt [Sav04] to determine certain extensions killed by p of finite flat group schemes that admit generic fibre descent data to $\mathbf{Q}_p$. Our general approach will be to prove some statements about extensions of a finite flat group scheme over an arbitrary tamely ramified discrete valuation ring. The techniques and technology are essentially due to Breuil [Bre00], following results of Fontaine. Let $K/\mathbf{Q}_p$ be a tamely ramified extension (of arbitrary degree).

Theorem 5.1. *Let $\mathscr{G}$ be a finite flat group scheme of order p^2 over $\mathcal{O}_K$. Then $\mathscr{G}$ sits inside an exact sequence*

$$0 \to \mathscr{G}_{s,b} \to \mathscr{G} \to \mathscr{G}_{r,a} \to 0$$

of Oort–Tate group schemes. If $\mathscr{G}$ is not killed by p then there exists a non-trivial morphism of group schemes $\mathscr{G}_{r,a} \to \mathscr{G}_{s,b}$. Moreover, if $\mathscr{G}$ is not killed by p then $\mathscr{G}[p]$ is finite flat if and only if $\mathscr{G}$ is étale or multiplicative, or equivalently if and only if $\mathscr{G}$ is isomorphic to $\mathbf{Z}/p^2\mathbf{Z}$ or μ_{p^2} over $\mathcal{O}_{K^{\mathrm{ur}}}$. For any pairs (r,a) and (s,b) for which there does exist a non-trivial map $\mathscr{G}_{r,a} \to \mathscr{G}_{s,b}$ that is not an isomorphism, there exists a corresponding extension $\mathscr{G}$ not killed by p if and only if $r \geqslant ps$ or $(e-s) \geqslant p(e-r)$.

This is a combination of Lemma 4.10, Corollary 5.14 and Lemma 5.15. As an application, we have the following corollary.

Corollary 5.2. *Let K be a tamely ramified extension of degree $e = p+1$. Let $\mathscr{G}$ be a finite flat group scheme of order p^2 such that the generic fibre is an extension of $\mathbf{F}_p(\omega^k)$ by $\mathbf{F}_p(\omega^k)$. Suppose moreover that $k \not\equiv 0,\ 1,\ (p-1)/2,\ (p+1)/2 \bmod p-1$. Then $\mathscr{G}$ is killed by p. In particular, the generic fibre is killed by p.*

Proof. From the classification of group schemes of order p (see for example [BCDT01, Example 5.2], Theorem 5.16 and Corollary 5.17) we find that, for k outside the exceptional listed set, the Galois representation $\mathbf{F}_p(\omega^k)$ arises from a unique finite flat group scheme of order p. It follows from Theorem 5.1 that either $\mathscr{G} = \mathscr{G}[p]$ or $\mathscr{G}$ is étale or multiplicative. Since $\mathbf{F}_p(\omega^k)$ is not étale or multiplicative, the result follows. □

5.1 Definitions

We rely extensively on [Bre00]. Let p be an odd prime, and let e be an integer coprime to p. Let $\mathbf{F} \subset \overline{\mathbf{F}}_p$, $W = W(\mathbf{F})$, $K_0 = W \otimes \mathbf{Q}_p$. Let K be a totally tamely ramified extension of K_0. Let π be a uniformizer of $\mathcal{O}_K$ with minimal polynomial $E(u) = u^e + p$. Let $v_n = v(p^n!)$. Let S be the p-adic completion of

$$W[u, X_n], \quad \text{where } X_n = \frac{u^{ep^n}}{p^{v_n}} \text{ for } n \geqslant 1.$$

Let $\mathrm{Fil}^1 S$ be the W-submodule of S topologically generated by $Y_n = E(u)^{p^n}/p^{v_n}$ for all n. There is an isomorphism

$$S/\mathrm{Fil}^1 S \simeq \mathcal{O}_K, \quad u \mapsto \pi.$$

Let ϕ be the unique additive map $S \to S$, semilinear with respect to the absolute Frobenius on W, continuous for the p-adic topology, compatible with the divided powers, and satisfying $\phi(u) = u^p$. Let

$$\phi_1 = \frac{\phi}{p}\bigg|_{\mathrm{Fil}^1 S},$$

and let $S_n = S/p^n$.

Definition 5.3. The category of Breuil modules (denoted by $'(Mod/S)$) consists of triples $(\mathcal{M}, \mathrm{Fil}^1\mathcal{M}, \phi_1)$ such that:

(i) $\mathcal{M}$ is an S-module;
(ii) $\mathrm{Fil}^1\mathcal{M}$ is an S-submodule of $\mathcal{M}$ containing $\mathrm{Fil}^1 S \cdot \mathcal{M}$;
(iii) ϕ_1 is a ϕ-semilinear map $\mathrm{Fil}^1\mathcal{M} \to \mathcal{M}$ such that for all $s \in \mathrm{Fil}^1 S$ and $x \in \mathcal{M}$, $\phi_1(sx) = \phi_1(s)\varphi(x)$, where $\varphi(x) = \phi_1(E(u)x)/\phi_1(E(u))$.

A map between Breuil modules is a map $\mathcal{M} \to \mathcal{M}'$ such that the induced map on $\mathrm{Fil}^1\mathcal{M}$ has image in $\mathrm{Fil}^1\mathcal{M}'$, and commutes with ϕ_1. The category (Mod/S_1) is the category of Breuil modules with $\mathcal{M}$ a free $S_1 = S/p$-module of finite rank such that $\phi_1(\mathcal{M})$ generates $\mathcal{M}$ as an S-module.

Note that in our case, $E(u) = u^e + p$ and $\phi_1(E(u)) = 1 + u^{ep}/p = 1 + X_1$ (which is a unit in S). If $\mathcal{M}$ is killed by p^n it is still important that one take $s \in \mathrm{Fil}^1 S$ in this last condition rather than $s \in \mathrm{Fil}^1 S \cdot S/p^n$. This is because $\phi_1(s) \bmod p$ does not depend only on $s \bmod p$. For example, '$\phi_1(u^e)$' $= X_1 \neq \phi_1(u^e + p) \bmod p$.

We use the notation φ instead of ϕ used in [Bre00] to avoid any confusion with the map ϕ defined on S.

Theorem 5.4. *Let (Mod/S) be the subcategory of $'(Mod/S)$ generated from extensions by (Mod/S_1). Then (Mod/S) is anti-equivalent to the category of finite flat group schemes over $\mathcal{O}_K$.*

Note that $S_1 \simeq \mathbf{F}[u, X_n]/(u^{ep}, X_n^p)$. Moreover, $\mathrm{Fil}^1 S_1 = \mathrm{Fil}^1 S \cdot S_1 = (u^e, X_n)S_1$, so

$$S_1/\mathrm{Fil}^1 S_1 \simeq \mathcal{O}_K/p \simeq \mathbf{F}[u]/u^e.$$

5.2 Rank 1 Breuil modules

Let $\mathcal{A}(r, a)$ be the Breuil module corresponding to the following data:

$$\mathcal{A}(r, a) = S_1\mathbf{e}, \quad \mathrm{Fil}^1\mathcal{A}(r, a) = (u^r, X_n)\mathbf{e}, \quad \phi_1(u^r\mathbf{e}) = a\mathbf{e}.$$

Lemma 5.5. *Any rank 1 Breuil module killed by p is isomorphic to $\mathcal{A}(r, a)$ for some $r \leqslant e$ and $a \in \mathbf{F}$. Moreover, there exists a non-trivial map $\mathcal{A}(s, b) \to \mathcal{A}(r, a)$ if and only if $s \equiv r \bmod p - 1$ and $a/b \in \mathbf{F}^{\times(p-1)}$, and an isomorphism if and only if $s = r$ and $a/b \in \mathbf{F}^{\times(p-1)}$.*

Proof. This is essentially [BCDT01, Example 5.2] and [Bre00, Proposition 2.1.2.2], except for the claim that $\phi(u^r\mathbf{e}_1)$ can be chosen to equal $a\mathbf{e}_1$ rather than $ax\mathbf{e}_1$ for some unit $x \in S_1$ satisfying $x \equiv 1 \bmod (X_n)$. Changing variables by $\mathbf{e}' = y\mathbf{e}$, it suffices to solve the equation

$$\frac{y}{\phi(y)} = x.$$

Since $x \equiv 1 \bmod (X_n)$, $\phi^{(n)}(x) = 1$ for sufficiently large n. Thus one can choose

$$y = \prod_{n=0}^{\infty} \phi^{(n)}(x). \qquad \square$$

Group schemes of order p are also classified by their Oort–Tate parameters [OT70]. The following lemma records that these parameters are (essentially) (r, a).

Lemma 5.6. *The Breuil module $\mathcal{A}(r,a)$ corresponds to the Oort–Tate group scheme $\mathscr{G}_{r,a}$ over $\mathcal{O}_K$ where the affine algebra of $\mathscr{G}_{k,a}$ is equal to*

$$\mathcal{O}_K[X]/(X + \pi^{e-k}\widetilde{a}),$$

where $\widetilde{a}$ is a lift of a to $W(\mathbf{F})$.

Proof. See for example [Bre00, Proposition 3.1.2]. □

5.3 An example

Recall that the category $(Mod\ FI/S)$ is the subcategory of (Mod/S) consisting of Breuil modules such that $\mathcal{M} \simeq \bigoplus S_{n_i}$. The category $(Mod\ FI/S)$ corresponds to finite flat group schemes $\mathscr{G}$ such that $\mathscr{G}[p^i]$ is finite flat for all i. We now construct an explicit example of a Breuil module in (Mod/S) that does not lie in $(Mod\ FI/S)$. This example is in [Bre00], but we feel that it serves as a useful example of the modules that will be considered in the next section. Let $e = p-1$. Recall that $\mathcal{A}(e,1)$ and $\mathcal{A}(0,1)$ are the rank 1 Breuil modules given by the following data:

$$\begin{aligned} &\mathcal{A}(e,1) = S_1\mathbf{e}_1, \quad \mathrm{Fil}^1\mathcal{A}(e,1) = \mathrm{Fil}^1 S \cdot \mathbf{e}_1 = (u^e, X_i)\mathbf{e}_1, \quad \phi(u^e\mathbf{e}_1) = \mathbf{e}_1, \\ &\mathcal{A}(0,1) = S_1\overline{\mathbf{e}}_2, \quad \mathrm{Fil}^1\mathcal{A}(0,1) = S_1\overline{\mathbf{e}}_2, \qquad\qquad\qquad \phi_1(\overline{\mathbf{e}}_2) = \overline{\mathbf{e}}_2. \end{aligned}$$

In addition, let $\mathcal{B}(0,1)$ be the Breuil module given by

$$\mathcal{B}(0,1) = S_2\mathbf{e}_2, \quad \mathrm{Fil}^1\mathcal{B}(0,1) = S_1\mathbf{e}_2, \quad \phi_1(\mathbf{e}_2) = \mathbf{e}_2.$$

We use the notation $\overline{\mathbf{e}}_2$ for a generator of $\mathcal{A}(0,1)$ to highlight the fact that $\mathcal{A}(0,1)$ is a quotient of $\mathcal{B}(0,1)$ where the quotient map (multiplication by p) sends $\mathbf{e}_2$ to $\overline{\mathbf{e}}_2$. The Breuil module $\mathcal{A}(e,1)$ corresponds to the finite flat constant group scheme $\mathbf{Z}/p\mathbf{Z}$, whilst the module $\mathcal{A}(0,1)$ corresponds to μ_p (see Lemma 5.6 for an identification of rank 1 Breuil modules with Oort–Tate group schemes). Define $\psi : \mathcal{A}(0,1) \to \mathcal{A}(e,1)$ by $\psi(\overline{\mathbf{e}}_2) = u^p\mathbf{e}_1 = u^{e+1}\mathbf{e}_1$. We check that

$$\phi_1(\psi(\overline{\mathbf{e}}_2)) = \phi_1(u^p\mathbf{e}_1) = \phi_1(u \cdot u^e\mathbf{e}_1) = \phi(u)\mathbf{e}_1 = u^p\mathbf{e}_1 = \psi(\overline{\mathbf{e}}_2) = \psi(\phi_1(\overline{\mathbf{e}}_2)).$$

The Breuil module $\mathcal{B}(0,1)$ is an extension of $\mathcal{A}(0,1)$ by $\mathcal{A}(0,1)$ (corresponding to μ_{p^2}), and there is a natural map $\iota : \mathcal{A}(0,1) \to \mathcal{B}(0,1)$ given by $\mathbf{e}_2 \to \overline{\mathbf{e}}_2$. Consider the map

$$\iota + \psi : \mathcal{A}(0,1) \to \mathcal{B}(0,1) \oplus \mathcal{A}(e,1), \quad \mathbf{e}_2 \mapsto p\mathbf{e}_2 - u^p\mathbf{e}_1,$$

and let $\mathcal{L}$ be the cokernel. Abstractly it is the quotient of $S_2 \oplus S_1$ by the element $(p, -u^p)$. There is an injective map $\mathcal{A}(e,1) \to \mathcal{L}$ given by $\mathbf{e}_1 \mapsto \mathbf{e}_1$, which extends to a map of Breuil modules. The quotient of $\mathcal{L}$ by $\mathcal{A}(e,1)$ is the quotient of $S_2 \oplus S_1$ by $\mathbf{e}_1$ and $p\mathbf{e}_2 - u^p\mathbf{e}_1$. Since together these elements generate the module $((p\mathbf{e}_2, 0), (0, \mathbf{e}_1))$, the quotient is $\mathcal{B}(0,1)/p \simeq \mathcal{A}(0,1)$. Thus we have an exact sequence of Breuil modules:

$$0 \to \mathcal{A}(e,1) \to \mathcal{L} \to \mathcal{A}(0,1) \to 0.$$

This extension of Breuil modules corresponds to an exact sequence of group schemes (note the anti-equivalence):

$$0 \to \mu_p \to \mathscr{G} \to \mathbf{Z}/p\mathbf{Z} \to 0.$$

5.4 Extension classes

Suppose that $\mathscr{H}_1$ and $\mathscr{H}_2$ are finite flat group schemes over $\mathcal{O}_K$ of order p. Let $\mathscr{G}$ be an extension of $\mathscr{H}_1$ by $\mathscr{H}_2$, and let $\mathcal{M}$ be the associated Breuil module.

Lemma 5.7. *$\mathcal{M}$ is generated by (at most) two elements as an S-module. $\mathcal{M}$ is a quotient of $S_2 \oplus S_1$.*

Proof. Let $\mathcal{A}_i$ be the Breuil module associated to $\mathscr{H}_i$. There is an exact sequence

$$0 \to \mathcal{A}_1 \to \mathcal{M} \to \mathcal{A}_2 \to 0.$$

Call the quotient map ψ. Suppose that $\mathcal{A}_1$ and $\mathcal{A}_2$ are generated by $\mathbf{e}_1$ and $\overline{\mathbf{e}}_2$. Then $\mathcal{M}$ is generated by $\mathbf{e}_1$ and $\mathbf{e}_2 := \psi^{-1}\overline{\mathbf{e}}_2$. Moreover, $p\mathbf{e}_1 = 0$, and $p\mathbf{e}_2 \in S_1\mathbf{e}_1$ so $p^2\mathbf{e}_2 = 0$. □

We conclude that

$$\mathcal{M} = (\mathbf{e}_1 S_1 \oplus \mathbf{e}_2 S_2)/I$$

for some S-submodule I.

Lemma 5.8. *I is generated by $p\mathbf{e}_2 - \eta\mathbf{e}_1$ for some $\eta \in S_1$.*

Proof. The element $p\mathbf{e}_2$ lies in the kernel of $\mathcal{M} \to \mathcal{A}_2$. Thus $p\mathbf{e}_2$ lies in the image of $\mathcal{A}_1$, and thus $p\mathbf{e}_2 = \eta\mathbf{e}_1$ for some $\eta \in S_1$. Suppose that $\beta\mathbf{e}_2 = \alpha\mathbf{e}_1$. If $\beta = p\gamma$, then

$$\gamma(p\mathbf{e}_2 - \eta\mathbf{e}_1) = \beta\mathbf{e}_2 - \gamma\eta\mathbf{e}_1 = (\beta\mathbf{e}_2 - \alpha\mathbf{e}_1) + (\alpha - \gamma\eta)\mathbf{e}_1$$

and so $(\alpha - \gamma\eta)\mathbf{e}_1 = 0$ in $\mathcal{M}$. Yet $\mathcal{A}_1$ injects into $\mathcal{M}$, so $\gamma\eta = \alpha$, and

$$(\beta\mathbf{e}_2 - \alpha\mathbf{e}_1) = \gamma(p\mathbf{e}_2 - \eta\mathbf{e}_1).$$

Thus we may assume that $p \nmid \beta$. As an abstract abelian group, $S_2 \simeq (\mathbf{Z}/p^2\mathbf{Z})^\infty$, and thus the image of β is non-zero in S_1. The map from $\mathcal{M} \to \mathcal{A}_2$ sends $\mathbf{e}_1$ to 0. Thus the image $\overline{\mathbf{e}}_2$ of $\mathbf{e}_2$ is killed by $\overline{\beta}$, which is a contradiction, since $\mathcal{M}$ is surjective and $\mathcal{A}_2$ is free. □

Thus we have an isomorphism of S-modules

$$\mathcal{M} = (S_1 \oplus \mathbf{e}_2 S_2)/(p\mathbf{e}_2 - \eta\mathbf{e}_1).$$

Recall that the category $(Mod\ FI/S)$ consists of Breuil modules such that $\mathcal{M} \simeq \bigoplus S_{n_i}$. The category $(Mod\ FI/S)$ corresponds to finite flat group schemes $\mathscr{G}$ such that $\mathscr{G}[p^i]$ is finite flat for all i. We conclude that $\mathscr{G} = \mathscr{G}[p]$ if and only if $\eta = 0$, and that if $\mathscr{G}[p] \neq \mathscr{G}$, then $\mathscr{G}[p]$ is finite flat if and only if η is a unit in S.

Let us now choose $\mathcal{A}_1 = \mathcal{A}(r, a)$ and $\mathcal{A}_2 = \mathcal{A}(s, b)$, where r and s are integers $\leqslant e$. There is an induced exact sequence

$$0 \to (u^r, X_n)\mathcal{A}(r, a) \to \mathrm{Fil}^1\mathcal{M} \to (u^s, X_n)\mathcal{A}(s, b) \to 0.$$

Recall that $\mathrm{Fil}^1 S_2$ is generated by $Y_n = E(u)^{p^n}/p^{v_n}$ for all n, where $v_n = v(p^n!)$.

Lemma 5.9. *Suppose that $p > 2$. Let $X_0 = u^e$, and let $X_n = u^{ep^n}/p^{v_n}$. Then*

$$Y_n \equiv X_n + p\prod_{i=0}^{n-1} X_i^{p-1} \mod p^2 S.$$

In the module $\mathcal{M}$, $X_n\mathbf{e}_2 \in \mathrm{Fil}^1\mathcal{M}$ for all $n \geqslant 1$.

Proof. The congruence follows by induction from the identity

$$\frac{(a+bp)^p}{p} = \frac{a^p}{p} + a^{p-1}bp \mod p^2$$

and the fact that $Y_{n+1} = Y_n^p/p$. Since $e(p-1) \geqslant e \geqslant r$, and since $u^r\mathbf{e}_1 \in \mathrm{Fil}^1\mathcal{M}$, it follows that

$$pX_0^{p-1}\mathbf{e}_2 = u^{e(p-1)}\eta\mathbf{e}_1 \in \mathcal{M}.$$

Thus as $Y_n\mathbf{e}_2$ is automatically in $\mathrm{Fil}^1\mathcal{M}$, the inclusion $X_n\mathbf{e}_2 \in \mathrm{Fil}^1\mathcal{M}$ follows from the congruence by induction. □

Lemma 5.10. *If $\mathcal{M}$ is an extension of $\mathcal{A}(s,b)$ by $\mathcal{A}(r,a)$ then*

$$\mathcal{M} = S_1 \oplus S_2/(p\mathbf{e}_2 - \eta\mathbf{e}_1).$$

Moreover,

$$\mathrm{Fil}^1\mathcal{M} = (u^r\mathbf{e}_1, u^s\mathbf{e}_2 + x\mathbf{e}_1, X_n\mathbf{e}_1, X_n\mathbf{e}_2), \quad i \geqslant 1,$$

and ϕ_1 is defined as follows:

$$\phi_1(u^r\mathbf{e}_1) = a\mathbf{e}_1, \quad \phi_1(u^s\mathbf{e}_2 + x\mathbf{e}_1) = b\mathbf{e}_2.$$

Proof. We clearly have that $\mathrm{Fil}^1\mathcal{M} \cap \mathcal{A}(r,a) = (u^r, X_n)\mathbf{e}_1$, and $u^s\mathbf{e}_2 + x\mathbf{e}_1 \in \mathrm{Fil}^1\mathcal{M}$ for some $x \in S$. Consider a general element γ of $\mathrm{Fil}^1 S$. Since $X_n\mathbf{e}_2 \in \mathrm{Fil}^1\mathcal{M}$, we may assume after subtracting some element of $(X_n)\mathbf{e}_2$ that $\gamma = \alpha u^s\mathbf{e}_2 + \beta\mathbf{e}_1$. Then

$$\alpha u^s\mathbf{e}_2 + \beta\mathbf{e}_1 - \alpha(u^s\mathbf{e}_2 + x\mathbf{e}_1) = (\beta - \alpha x)\mathbf{e}_1 \in \mathrm{Fil}^1\mathcal{M}.$$

Thus $(\beta - \alpha x)\mathbf{e}_1 = \mathrm{Fil}^1\mathcal{A}(r,a)$, and γ is in the span of $u^s\mathbf{e}_2 + x\mathbf{e}_1$, $(X_n)\mathbf{e}_2$, and $\mathrm{Fil}^1\mathcal{A}(r,a)$. Hence

$$\mathrm{Fil}^1\mathcal{M} = (u^r\mathbf{e}_1, u^s\mathbf{e}_2 + x\mathbf{e}_1, X_n\mathbf{e}_1, X_n\mathbf{e}_2), \quad i \geqslant 1.$$

Moreover,

$$\phi_1(u^r\mathbf{e}_1) = a\mathbf{e}_1, \phi_1(u^s\mathbf{e}_2 + x\mathbf{e}_1) = b\mathbf{e}_2 + z\mathbf{e}_1.$$

Replacing $\mathbf{e}_2$ by $\mathbf{e}_2 + y\mathbf{e}_1$ for suitable y we may assume (having changed x and η appropriately) that $z = 0$. This proves the lemma. □

We also note that $\phi_1(\mathrm{Fil}^1\mathcal{M})$ as defined above generates $\mathcal{M}$ as an S-module. However, we have not shown that ϕ_1 is well defined, and so we have not yet constructed a Breuil module. In fact, the obstructions to defining ϕ_1 will severely limit the possible extension classes.

Fix once and for all an element $y = \eta - u^{e-s}x$.

Let us compute $\varphi(\mathbf{e}_2)$ and $\varphi(\mathbf{e}_1)$. Recalling that $y = \eta - u^{e-s}x$ we find that

$$(u^e + p)\mathbf{e}_2 = u^e\mathbf{e}_2 + \eta\mathbf{e}_1 = u^{e-s}(u^s\mathbf{e}_2 + x\mathbf{e}_1) - u^{e-s}x\mathbf{e}_1 + \eta\mathbf{e}_1 = u^{e-s}(u^s\mathbf{e}_2 + x\mathbf{e}_1) + y\mathbf{e}_1.$$

It follows that $y\mathbf{e}_1 \in \mathrm{Fil}^1\mathcal{A}(r,a)$. We find that

$$\phi_1(E(u)\mathbf{e}_2) = bu^{p(e-s)}\mathbf{e}_2 + \phi_1(y\mathbf{e}_1),$$

and so

$$\varphi(\mathbf{e}_2) = \frac{\phi_1(E(u)\mathbf{e}_2)}{\phi_1(E(u))} = \frac{bu^{p(e-s)}\mathbf{e}_2 + \phi_1(y\mathbf{e}_1)}{1 + X_1}.$$

A similar computation shows that

$$\varphi(\mathbf{e}_1) = \frac{\phi_1(E(u)\mathbf{e}_1)}{\phi_1(E(u))} = \frac{\phi_1(u^{e-r}u^r\mathbf{e}_1)}{1 + u^{ep}/p} = \frac{au^{p(e-r)}\mathbf{e}_1}{1 + X_1}.$$

When $\mathcal{M} = \mathcal{L}$, we see that $\mathrm{Fil}^1\mathcal{L}$ is generated by $\mathbf{e}_2$ and $u^r\mathbf{e}_1$. Moreover, $\phi_1(\mathbf{e}_2) = \mathbf{e}_2$ and $\phi_1(u^r\mathbf{e}_1) = \mathbf{e}_1$. Thus $y = \eta = u^p$, and $x = 0$. Moreover, $s = 0$ and $b = 1$ and so

$$\varphi(\mathbf{e}_2) = \frac{u^{pe}\mathbf{e}_2 + u^p\mathbf{e}_1}{1 + X_1} = \frac{pX_1\mathbf{e}_2 + u^p\mathbf{e}_1}{1 + X_1} = \frac{X_1\eta\mathbf{e}_1 + u^p\mathbf{e}_1}{1 + X_1} = \frac{(1 + X_1)u^p\mathbf{e}_1}{1 + X_1} = u^p\mathbf{e}_1.$$

Returning now to the general situation, we shall derive some relations between η, x and y by computing $\phi_1(u^sY_n\mathbf{e}_2 + xY_n\mathbf{e}_1)$ in two different ways. On the one hand we have that

$$\phi_1(u^sY_n\mathbf{e}_2) = \phi(u^s)\phi_1(Y_n)\varphi(\mathbf{e}_2) = u^{ps}Y_{n+1}\frac{bu^{p(e-s)}\mathbf{e}_2 + \phi_1(y\mathbf{e}_1)}{1 + X_1}$$

and

$$\phi_1(xY_n\mathbf{e}_1) = \phi(x)\phi_1(Y_n)\varphi(\mathbf{e}_1) = \phi(x)Y_{n+1}\frac{au^{p(e-r)}\mathbf{e}_1}{1+X_1}.$$

On the other hand, $u^sY_n\mathbf{e}_2 + xY_n\mathbf{e}_1 = Y_n(u^s\mathbf{e}_2 + x\mathbf{e}_1)$, and so

$$\phi_1(Y_n(u^s\mathbf{e}_2 + x\mathbf{e}_1)) = \phi(Y_n)b\mathbf{e}_2.$$

Now $\phi(Y_n) = Y_n^p = pY_{n+1}$, and $p\mathbf{e}_2 = \eta\mathbf{e}_1$. Thus we find that

$$Y_{n+1}b\eta\mathbf{e}_1 = Y_{n+1}\left(\frac{bu^{pe}\mathbf{e}_2 + u^{ps}\phi_1(y\mathbf{e}_1) + a\phi(x)u^{p(e-r)}\mathbf{e}_1}{1+X_1}\right).$$

We make two simplifications. First, $u^{ep}\mathbf{e}_2 = X_1p\mathbf{e}_2 = X_1\eta\mathbf{e}_1$. Thus both sides are multiples of $\mathbf{e}_1$, and we may replace Y_{n+1} by X_{n+1}. Second, the annihilator of X_n in S_1 is X_n^{p-1}. Thus the annihilator of $(X_n)_{n=k}^m$ is $\prod_{n=k}^m X_n^{p-1}$ and the annihilator of $(X_n)_{n=k}^\infty$ is trivial. Thus if $X_{n+1}\alpha = X_{n+1}\beta$ for all sufficiently large n, $\alpha = \beta$. Applying this to our formula, and multiplying through by $(1+X_1)$ we find that

$$b\eta(1+X_1)\mathbf{e}_1 = X_1b\eta\mathbf{e}_1 + u^{ps}\phi_1(y\mathbf{e}_1) + a\phi(x)u^{p(e-r)}\mathbf{e}_1$$

or

$$b\eta\mathbf{e}_1 = u^{ps}\phi_1(y\mathbf{e}_1) + a\phi(x)u^{p(e-r)}\mathbf{e}_1.$$

Thus we have proven the following theorem.

Theorem 5.11. *If $\mathcal{M}$ is well defined as a Breuil module then*

$$b\eta\mathbf{e}_1 = u^{ps}\phi_1(y\mathbf{e}_1) + a\phi(x)u^{p(e-r)}\mathbf{e}_1.$$

Moreover η is divisible by $(u^p)^{\min\{s,e-r\}}$.

Suppose that $\mathcal{M} = \mathcal{L}$. Then $x = 0$, $e = p-1$, and $y = \eta = u^p$. Thus the theorem is consistent with the identity $u^p = \eta = \phi_1(\eta\mathbf{e}_1)$.

Lemma 5.12. *There is an inclusion $\eta \in \mathbf{F}[u]/u^{ep}$.*

Proof. We divide our proof into two cases. First we consider the case where $(r,s) \neq (e,0)$. Since $\phi(X_n) = X_n^p = 0$, it is clear that $\phi(x) \in \mathbf{F}[u]/u^{ep}$. Moreover, $\phi_1(X_iX_j\mathbf{e}_1) = \phi(X_i)\phi_1(X_j\mathbf{e}_1) = X_n^p\phi(X_j\mathbf{e}_1) = 0$ for the same reason. Thus the only terms that contribute to coefficients of η that do not lie in $\mathbf{F}[u]/u^{ep}$ are of the form u^mX_n. Let m be the infimum (minimum) over all $n \geqslant 1$ such that the coefficient of u^mX_n in y is non-zero. The corresponding coefficient of η is $u^{p(e-r+s+m)}X_{n+1}$, and thus if $m \geqslant r-s$ we are done. Suppose otherwise. Then the minimum m over all $n \geqslant 1$ such that the coefficient of u^mX_n in η is non-zero is $p(e+s-r+m)$. The minimum m over all $n \geqslant 1$ such that the coefficient of u^mX_n in $u^{e-s}x$ is non-zero is trivially at least $e-s$. Since $y = \eta - u^{e-s}x$ we conclude that

$$m \geqslant \min\{p(e+s-r+m), e-s\}.$$

Since $m < r-s \leqslant e-s$, it must be the first inequality that is satisfied. Equivalently,

$$(1-p)m \geqslant p(e+s-r).$$

Since $e \geqslant r$, the right-hand side is non-negative unless $r = e$ and $s = 0$. On the other hand, the left-hand side is negative unless $m \geqslant 0$. Thus either we are done or $(r,s) = (e,0)$ and $m = 0$. Let us now assume we are in that case. There is an identity $y = \eta - u^ex$. Since $y\mathbf{e}_1 \in \mathrm{Fil}^1\mathcal{A}(e,a)$ and $u^e \in \mathrm{Fil}^1S_1$, it follows that $\eta \in \mathrm{Fil}^1S_1$. Now $\phi_1(y\mathbf{e}_1) = \phi_1(\eta\mathbf{e}_1) - a\phi(x)$ and so

$$b\eta\mathbf{e}_1 = \phi_1(y\mathbf{e}_1) + a\phi(x) = \phi_1(\eta\mathbf{e}_1).$$

As above, since $\phi_1(X_iX_j\mathbf{e}_1) = \phi(X_i)\phi(X_j\mathbf{e}_1) = 0$, the only terms contributing to η that do not lie in $\mathbf{F}[u]/u^{ep}$ are coefficients of y of the form u^mX_n with $n \geqslant 1$. Let n be the smallest integer such that u^mX_n is a non-zero coefficient of η. Then since

$$\phi_1(u^iX_j) = u^{ip}\phi_1(Y_{j+1})\varphi(\mathbf{e}_1) = \frac{X_{j+1}u^{ip}}{1+X_1},$$

we see (since $j+1 > m$) that $\phi_1(\eta)$ does not have any coefficients of the form u^nX_m, a contradiction. Thus $\eta \in \mathbf{F}[u]/u^{ep}$. □

Write

$$x = \sum_{k=0}^{ep-1} \alpha_k u^k \bmod (X_n), \quad y = \sum_{k=0}^{ep-1} \beta_k u^k \bmod (X_n).$$

Then (noting by Lemma 5.12 that $\eta \in \mathbf{F}[u]/u^{ep}$) the equality $\eta = y + u^{e-s}x$ becomes

$$\sum_{k=0}^{ep-1} \gamma_k u^k = \eta = \sum_{k=0}^{ep-1} u^k(\beta_k + \gamma_{k+s-e}).$$

Since $y\mathbf{e}_1 \in \mathrm{Fil}^1\mathcal{A}(r,a)$, we must have $\beta_k = 0$ for $k < r$. Applying the equality of Theorem 5.11 we find that

$$b\eta = \sum_{k=0}^{ep-1} au^{pk}(\phi(\beta_{k+r-s}) + \phi(\alpha_{k+r-e})) = a\sum_{k=0}^{ep-1} u^{pk}\phi(\beta_{k+r-s} + \alpha_{k+r-e}),$$

where ϕ is Frobenius on $\mathbf{F}$. The two expressions for η lead to the following relations:

(i) $\gamma_k = \beta_k + \alpha_{k+s-e}$;
(ii) $\gamma_k = 0$ if $p \nmid k$;
(iii) $b\gamma_{pk} = a\phi(\beta_{k+r-s} + \alpha_{k+r-e})$.

In particular we see that $b\gamma_{pk} = a\phi(\gamma_{k+r-s})$.

Lemma 5.13. *If $\mathcal{M}$ is a Breuil module, then $\eta = 0$ unless $(r-s) = k(p-1)$ for some $k \geqslant 0$ and $a/b \in \mathbf{F}^{\times(p-1)}$. If $r = s$, then $\eta = 0$ unless $s = 0$ or $r = e$. If η is non-zero, then up to an element of $\mathbf{F}^\times$, $\eta = u^{kp}$. Finally, there is an inequality $k \geqslant \min\{s, e-r\}$.*

Proof. First note that γ_{pk} is non-zero if and only if $\gamma_{k+(r-s)}$ is non-zero, since Frobenius is injective in $\mathbf{F}$. Let k be the smallest integer such that $\gamma_{pk} \neq 0$. Then $k \geqslant 0$ and k is the smallest integer such that $\gamma_{k+(r-s)} \neq 0$. It follows that $k + (r-s) = pk$, and so $(r-s) = k(p-1)$. The equality $b\gamma_{pk} = a\phi(\gamma_{pk}) \neq 0$ implies that $a/b = \phi(c)/c \in \mathbf{F}^{\times(p-1)}$. One finds (by considering the *second* smallest k such that $\gamma_{pk} \neq 0$) that no other coefficients of η are non-zero, and thus η is a multiple of u^{pk}. If $r = s$ then Theorem 5.11 implies that η is divisible by u (unless $s = 0$ or $r = e$), but the k satisfying $(r-s) = k(p-1)$ is $k = 0$, thus $\eta = 0$. The final inequality follows from Theorem 5.11. □

Corollary 5.14. *Suppose that $\mathscr{G}$ is an extension*

$$0 \to \mathscr{G}_{s,b} \to \mathscr{G} \to \mathscr{G}_{r,a} \to 0$$

of Oort–Tate group schemes that is not *killed by p. Then there is a non-trivial morphism $\mathscr{G}_{r,a} \to \mathscr{G}_{s,b}$.*

Proof. Suppose there existed such an exact sequence. Then there must exist an exact sequence of Breuil modules

$$0 \to \mathcal{A}(r,a) \to \mathcal{M} \to \mathcal{A}(s,b) \to 0.$$

If $\mathscr{G}$ is not killed by p, then $\mathcal{M}$ is not killed by p, and thus $\eta \neq 0$. By Lemma 5.13 then the restrictions on (r,s) and (a,b) are exactly the requirements that there exist a map $\mathcal{A}(s,b) \to \mathcal{A}(r,a)$

(see [BCDT01, Lemma 5.2.1]). Moreover, this map cannot be an isomorphism unless $r = s$, which (from Lemma 5.13) implies that $r = s = 0$ or $r = s = e$. In this case $\mathscr{G}_{r,a}$ and $\mathscr{G}_{s,b}$ are either both multiplicative or both étale, which implies that $\mathscr{G}$ is either multiplicative or étale. □

If r and s are both 0 or both e there exist extensions not killed by p: one can take μ_{p^2} and $\mathbf{Z}/p^2\mathbf{Z}$ respectively.

LEMMA 5.15. *Suppose that r and s are integers $\leqslant e$ such that $(r-s) = k(p-1)$ and $k \geqslant \min\{s, e-r\}$. Let a and b be elements of $\mathbf{F}$ such that $(b/a) = (c)^{p-1}$. Then there exists a non-trivial extension of the form*

$$0 \to \mathscr{G}_{s,b} \to \mathscr{G} \to \mathscr{G}_{r,a} \to 0.$$

Proof. Suppose that $k \geqslant s$. Then one may explicitly let $\mathcal{M} = S_1 \oplus S_2/(p\mathbf{e}_2 - cu^{pk}\mathbf{e}_1)$. Since $kp = r + k - s \geqslant r$, it follows that $u^{kp}\mathbf{e}_1$ is a multiple of $u^r\mathbf{e}_1$. Let

$$\mathrm{Fil}^1\mathcal{M} = (u^r\mathbf{e}_1, u^s\mathbf{e}_2, X_n\mathbf{e}_1, X_n\mathbf{e}_2),$$

and finally define ϕ_1 as follows:

$$\phi_1(u^r\mathbf{e}_1) = a\mathbf{e}_1, \quad \phi_1(u^s\mathbf{e}_2) = b\mathbf{e}_2.$$

If $k \geqslant e - r$ then we still define $\mathcal{M} = S_1 \oplus S_2/(p\mathbf{e}_2 - cu^{pk}\mathbf{e}_1)$. Now that $k \geqslant e - r$ we define $\mathrm{Fil}^1\mathcal{M}$ as

$$\mathrm{Fil}^1\mathcal{M} = (u^r\mathbf{e}_1, u^s\mathbf{e}_2 + cu^{k-e+r}\mathbf{e}_1, X_n\mathbf{e}_1, X_n\mathbf{e}_2),$$

where

$$\phi_1(u^r\mathbf{e}_1) = a\mathbf{e}_1, \quad \phi_1(u^s\mathbf{e}_2 + cu^{k-e+r}\mathbf{e}_1) = b\mathbf{e}_2.$$

Note that $u^{e-s}(u^s\mathbf{e}_2 + cu^{k-e+r}\mathbf{e}_1) = u^e\mathbf{e}_2 + cu^{pk}\mathbf{e}_1 = (u^e + p)\mathbf{e}_2$. One verifies in both cases that $\mathcal{M}$ defines a Breuil module. □

5.5 Finite flat group schemes killed by p

If one restricts to finite flat group schemes killed by p, the theory of Breuil modules can be significantly simplified. In particular, instead of working with S_1-modules, it suffices to work with $S_1/(X_n) = k[u]/u^{ep}$ modules, and replace $\mathcal{M}$ by $\mathcal{M} \otimes_{S_1} k[u]/u^{ep}$.

What Breuil modules $\mathcal{A}(r, a)$ admit generic descent data to $\mathbf{Q}_p$? The answer for a general tamely ramified extension is provided in [Sav04]. We restrict the statement to the case of interest, namely when $K/\mathbf{Q}_p$ is a tamely ramified Galois extension of $\mathbf{Q}_p$ with $e = p + 1$. We have the following theorem.

THEOREM 5.16. *The Breuil module $\mathcal{A}(r, a)$ admits generic fibre descent data to $\mathbf{Q}_p$ if and only if 2 divides r and $a \in \mathbf{F}_p^\times$. Let ξ_a be the unramified character of $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ given by $\xi(\sigma) = \sigma a^{1/(p-1)}/a^{1/(p-1)}$. Then the associated Galois representation on the (descended) generic fibre is given by $\xi_a\mathbf{F}_p(\omega^k)$, where $r \equiv 2 - 2k \bmod (p-1)$.*

Proof. This follows from the calculations in [Sav04], in particular Definition 5.1, Proposition 5.3, and Theorem 6.3. Note that in our setting and Savitt's notation we have $U = -1$, $V = -1$, and $x' = x/(e, p-1) = 2$. □

COROLLARY 5.17. *If $k \neq 0$, 1, $(p-1)/2$, $(p+1)/2$, then there is a unique finite flat group scheme of order p with generic fibre given by $\mathbf{F}_p(\omega^k)$.*

Proof. Any such finite flat group scheme obviously has generic fibre descent data. We see that such a representation forces a to be 1, and $r \not\equiv 0, 2 \bmod (p-1)$. Yet since r is even and less than $p+1$, this determines r exactly. □

Lemma 5.18. *Let $\overline{\rho}$ be as in § 4.2. Then $\overline{\rho}$ uniquely determines a finite flat group scheme $\mathscr{G}/\mathcal{O}_K$.*

Proof. Since $\mathbf{F}_p(\omega^k)$ and $\mathbf{F}_p(\omega^{1-k})$ correspond to unique finite flat group schemes, the lemma follows from a standard application of the 5-Lemma (see [BCDT01], in particular the proof of Lemma 4.1.2). □

Now we turn to extensions of Breuil modules killed by p. An easy computation [BCDT01, Sav04] shows that the extensions of $\mathcal{A}(r,a)$ by itself are classified by an element $h \in u^{\max(0,2r-e)}k[u]/u^{r+1}$. In general, these will correspond to finite flat group schemes whose generic fibre does not descend to $\mathbf{Q}_p$. However, we have the following theorem.

Theorem 5.19. *The space of extensions* $\mathrm{Ext}^1(\mathcal{A}(r,a),\mathcal{A}(r,a))$ *killed by p has dimension* 1 *over* $\mathbf{F}_p$.

Proof. It follows from [Sav04, Theorem 7.5] that h can be taken to have degree less than r. Moreover (since $k_1 = k_2$ in the notation of [Sav04]) the only possible non-zero term is u^r (which is zero) or the constant term which lies in $\mathbf{F}_p$. □

Corollary 5.20. *Suppose that K is tamely ramified of degree $p+1$, that $k \neq 0$, 1, $(p-1)/2$, $(p+1)/2$. Let $\mathscr{H}/\mathcal{O}_K$ be a finite flat group scheme over $\mathcal{O}_K$ with generic fibre $\mathbf{F}_p(\omega^k)$. Then the only extensions of $\mathscr{H}$ by itself which admit generic fibre descent data to $\mathbf{Q}_p$ become unramified over some finite unramified extension of K.*

Proof. The space of extensions is one-dimensional by Theorem 5.19. Thus it suffices to observe that the Galois module $\mathbf{F}_p(\omega^k)$ (over $\mathbf{Q}_p$) admits an extension by itself that splits over the degree p unramified extension of $\mathbf{Q}_p$. Thus if F denotes this unramified extension, then by faithfully flat descent from $\mathcal{O}_{F.K}$ to $\mathcal{O}_K$ we obtain a non-trivial (in fact, $p-1$ non-trivial) extensions of $\mathscr{H}$ by $\mathscr{H}$ in the category of finite flat group schemes with generic fibre descent data, which splits over some unramified extension of K, and thus we are done. □

Acknowledgements

I would like to thank Brian Conrad and Christophe Breuil for answering some technical questions about finite flat group schemes and Breuil modules, respectively. I would also like to thank Matthew Emerton for our frequent conversations, during which several of the ideas of this paper had their genesis.

References

BC05 J. Bellaïche and G. Chenevier, *Lisseté de la courbe de Hecke de* GL_2 *aux points Eisenstein critiques*, Preprint (2005).

BCDT01 C. Breuil, B. Conrad, F. Diamond and R. Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$*: wild* 3*-adic exercises*, J. Amer. Math. Soc. **14** (2001), 843–939.

Bre00 C. Breuil, *Groups p-divisibles, groupes finis et modules filtrés*, Ann. of Math. (2) **152** (2000), 489–549.

CDT99 B. Conrad, F. Diamond and R. Taylor, *Modularity of certain potentially Barsotti–Tate Galois representations*, J. Amer. Math. Soc. **12** (1999), 521–567.

CE05 F. Calegari and M. Emerton, *Ramification of Hecke algebras at Eisenstein primes*, Invent. Math. **160** (2005), 97–144.

CS05 F. Calegari and W. Stein, *Conjectures about discriminants of Hecke algebras*, in *Proc. of ANTS VI*, Lecture Notes in Computer Science (Springer, Berlin) to appear (2005).

Con99 B. Conrad, *Ramified deformation problems*, Duke Math. J. **97** (1999), 439–513.

Fla92 M. Flach, *A finiteness theorem for the symmetric square of an elliptic curve*, Invent. Math. **109** (1992), 307–327.

FL82 J. Fontaine and G. Laffaille, *Construction de représentations p-adiques*, Ann. Sci. École Norm. Sup. (4) **15** (1982), 547–608.

Gre01 R. Greenberg, *Iwasawa theory – past and present*, in *Class field theory – its centenary and prospect*, Tokyo, 1998, Adv. Stud. Pure Math., vol. 30 (Math. Soc. Japan, Tokyo, 2001), 335–385.

GL86 D. Gross and J. Lubin, *The Eisenstein descent on $J_0(N)$*, Invent. Math. **83** (1986), 303–319.

Lan78 S. Lang, *Cyclotomic fields*, Graduate Texts in Mathematics, vol. 59 (Springer, Berlin, 1978).

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

OT70 F. Oort and J. Tate, *Group schemes of prime order*, Ann. Sci. École Norm. Sup. (4) **3** (1970), 1–21.

Ray74 M. Raynaud, *Schémas en groupes de type* $(p, \ldots, p)$, Bull. Soc. Math. France **102** (1974), 241–280.

Rib76 K. Ribet, *A modular construction of unramified p-extensions of* $\mathbf{Q}(\zeta_p)$, Invent. Math. **34** (1976), 151–162.

RP81 K. Ribet and E. Papier, *Eisenstein ideals and λ-adic representations*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28** (1981), 651–665.

Sav04 D. Savitt, *Modularily of some potentially Barsotti–Tate representations*, Compositio Math. **140** (2004), 31–63.

SW97 C. Skinner and A. Wiles, *Ordinary representations and modular forms*, Proc. Natl. Acad. Sci. USA **94** (1997), 10520–10527.

Frank Calegari fcale@math.harvard.edu
Department of Mathematics, Harvard University, 432 Science Center, 1 Oxford Street, Cambridge, MA 02138, USA