Compositio Math. 140 (2004) 31–63
DOI: 10.1112/S0010437X03000289

Modularity of some potentially Barsotti–Tate Galois representations

David Savitt

Abstract

We prove a portion of a conjecture of Conrad, Diamond, and Taylor, yielding some new cases of the Fontaine–Mazur conjectures, specifically, the modularity of certain potentially Barsotti–Tate Galois representations. The proof follows the template of Wiles, Taylor–Wiles, and Breuil–Conrad–Diamond–Taylor, and relies on a detailed study of the descent, across tamely ramified extensions, of finite flat group schemes over the ring of integers of a local field. This makes crucial use of the filtered ϕ_1-modules of Breuil.

1. Notation, terminology, and results

Throughout this article, we let l be an odd prime, and we fix an algebraic closure $\overline{\mathbb{Q}}_l$ of $\mathbb{Q}_l$ with residue field $\overline{\mathbb{F}}_l$. The fields K, L, and E will always be finite extensions of $\mathbb{Q}_l$ inside $\overline{\mathbb{Q}}_l$. We denote by G_K the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}_l/K)$, by W_K the Weil group of K, and by I_K the inertia group of K. The group $I_{\mathbb{Q}_l}$ will be abbreviated as I_l. The character $\omega_n : G_{\mathbb{Q}_l} \to \mathbb{F}_{l^n} \subset \overline{\mathbb{F}}_l$ is defined via

$$\omega_n : u \mapsto \frac{u(-l)^{1/(l^n-1)}}{(-l)^{1/(l^n-1)}},$$

and its Teichmüller lift will be denoted $\tilde{\omega}_n$. In particular, $\omega = \omega_1$ is the mod-l reduction of the cyclotomic character ϵ. Recall that if $\rho : G_{\mathbb{Q}_l} \to \mathrm{GL}_2(E)$ or $W_{\mathbb{Q}_l} \to \mathrm{GL}_2(E)$ is continuous and tamely ramified, then $\rho|_{I_l} \otimes_E \overline{E}$ is isomorphic either to $\tilde{\omega}^i \oplus \tilde{\omega}^j$ or to $\tilde{\omega}_2^m \oplus \tilde{\omega}_2^{lm}$, depending on the absolute reducibility or irreducibility of ρ.

If an l-adic representation ρ of $G_{\mathbb{Q}_l}$ is potentially semistable (in the sense of Fontaine [Fon94]), then one associates to ρ a Weil–Deligne representation $WD(\rho)$ over $\overline{\mathbb{Q}}_l$, for example as in [CDT99, § B.1]. Then ρ becomes semistable over K if and only if $WD(\rho)|_{I_K}$ is trivial. The *Galois type* $\tau(\rho)$ associated to such ρ is defined to be the isomorphism class of the representation $WD(\rho)|_{I_l}$ of I_l.

Following [BCDT01] and using the notation of [BM02], we define a collection of deformation rings. Let $\overline{\rho} : G_{\mathbb{Q}_l} \to \mathrm{GL}_2(\mathbb{F})$ be a representation over a finite field $\mathbb{F}$ of characteristic l, and assume that the only matrices which commute with the image of $\overline{\rho}$ are scalar matrices, i.e. that $\overline{\rho}$ has trivial centralizer. Fix a positive integer k, and let τ be a Galois type such that $\det(\tau)$ is tame. We are interested in lifts $\rho : G_{\mathbb{Q}_l} \to \mathrm{GL}_2(\overline{\mathbb{Q}}_l)$ of $\overline{\rho}$ with the following properties:

i) ρ is potentially semistable with Hodge–Tate weights $(0, k-1)$;

ii) $\tau(\rho)$ is isomorphic to τ;

iii) $\det(\rho) = \epsilon^{k-1}\chi$, where χ is a character of finite order prime to l.

Received 1 July 2002, accepted in final form 15 April 2003.
2000 Mathematics Subject Classification 11F80 (primary), 14L15 (secondary).
Keywords: Breuil module, Galois representation, modularity.
This work was supported by an NSERC postdoctoral fellowship and partially conducted by the author for the Clay Mathematics Institute.

https://doi.org/10.1112/S0010437X03000289 Published online by Cambridge University Press

Let $R_{\mathcal{O}}^{\mathrm{univ}}$ denote the universal deformation ring parametrizing deformations of $\overline{\rho}$ over complete local Noetherian $\mathcal{O}$-algebras, where $\mathcal{O}$ is the integer ring of a finite extension of $\mathbb{Q}_l$ inside $\overline{\mathbb{Q}}_l$ which contains both the Witt vectors $W(\mathbb{F})$ and a field of rationality of τ. Let ρ^{univ} be the universal deformation. We say that a prime $\mathfrak{p}$ of $R_{\mathcal{O}}^{\mathrm{univ}}$ has type (k,τ) if there is a field $E \supset \mathcal{O}$ and a map of $\mathcal{O}$-algebras

$$f_{\mathfrak{p}} : R_{\mathcal{O}}^{\mathrm{univ}} \to E \quad \text{with } \mathfrak{p} = \ker(f_{\mathfrak{p}}),$$

such that the pushforward of ρ^{univ} by $f_{\mathfrak{p}}$ satisfies the three desired conditions above. Since $\mathcal{O}$ contains a field of rationality of τ, if $\sigma \in G_E$ then ${}^{\sigma}\tau$ and τ are equivalent, and so the definition of type (k,τ) is independent of the choice of $f_{\mathfrak{p}}$. We define

$$R(\overline{\rho},k,\tau)_{\mathcal{O}} = R_{\mathcal{O}}^{\mathrm{univ}} \Big/ \bigcap_{\mathfrak{p} \text{ type } (k,\tau)} \mathfrak{p}.$$

When $W(\mathbb{F})$ contains a field of rationality of τ, we will often write $R(\overline{\rho},k,\tau)$ for $R(\overline{\rho},k,\tau)_{W(\mathbb{F})}$; we remark in particular that this is always the case for $\tau = \tilde{\omega}_2^m \oplus \tilde{\omega}_2^{lm}$, which is rational over $\mathbb{Q}_l$.

In the case $k=2$, if there is a surjection $\mathcal{O}[[X]] \twoheadrightarrow R(\overline{\rho},2,\tau)_{\mathcal{O}}$ we say that τ is *weakly acceptable* for $\overline{\rho}$. If τ is weakly acceptable for $\overline{\rho}$ and $R(\overline{\rho},2,\tau)_{\mathcal{O}} \neq (0)$, we say that τ is acceptable for $\overline{\rho}$. The above deformation rings are of particular interest because [CDT99] and [BCDT01] use the methods of [Wil95] and [TW95] to prove results of roughly the following form (for a precise statement, see Theorem 1.4.1 of [BCDT01]): if ρ is an l-adic representation of $G_{\mathbb{Q}}$ such that $\rho|_{G_{\mathbb{Q}_l}}$ is potentially semistable with Galois type τ and Hodge–Tate weights $(0,1)$, such that τ is acceptable for $\overline{\rho}$, and with $\overline{\rho}$ modular, then ρ is modular. We remark [BM02, Lemme 2.2.2.3] that

$$R(\overline{\rho},k,\tau)_{\mathcal{O}'} \cong \mathcal{O}' \otimes_{\mathcal{O}} R(\overline{\rho},k,\tau)_{\mathcal{O}},$$

so when τ is defined over the fraction field of $W(\mathbb{F})$ the acceptability and weak acceptability of τ for $\overline{\rho}$ depend only on $R(\overline{\rho},2,\tau)$.

In this article, we will prove the following cases of [CDT99, Conjecture 1.2.3].

Theorem 1.1. *Suppose that $\tau = \tilde{\omega}_2^m \oplus \tilde{\omega}_2^{lm}$, where $m \in \mathbb{Z}/(l^2-1)\mathbb{Z}$ and $m = (l+1)j + i$ with $i = 1,\dots,l$ and $j \in \mathbb{Z}/(l-1)\mathbb{Z}$. Suppose also that $\overline{\rho}|_{G_{\mathbb{Q}_l}} : G_{\mathbb{Q}_l} \to \mathrm{GL}_2(\mathbb{F}_l)$, has centralizer $\mathbb{F}_l$, and is reducible. Then $R(\overline{\rho},2,\tau) \neq (0)$ only if $\overline{\rho}|_{I_l}$ has one of the following forms:*

$$\begin{aligned} \overline{\rho}|_{I_l} &= \begin{pmatrix} \omega^{i+j} & * \\ 0 & \omega^{1+j} \end{pmatrix} \quad \text{and if } i=2,\ * \text{ is peu ramifié,} \\ \overline{\rho}|_{I_l} &= \begin{pmatrix} \omega^{1+j} & * \\ 0 & \omega^{i+j} \end{pmatrix} \quad \text{and if } i=l-1,\ * \text{ is peu ramifié.} \end{aligned} \tag{1.2}$$

In each of these cases, τ is weakly acceptable for $\overline{\rho}$.

Combining Theorem 1.1 with [BCDT01, Theorem 1.4.1], we have the following theorem.

Theorem 1.3. *Let l be an odd prime, E a finite extension of $\mathbb{Q}_l$ in $\overline{\mathbb{Q}}_l$, and $\mathbb{F}$ the residue field of E. Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(E)$ be an odd continuous representation ramified at only finitely many primes. Assume that its reduction $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F})$ is absolutely irreducible after restriction to $\mathbb{Q}(\sqrt{(-1)^{(l-1)/2}l})$ and is modular. Furthermore, suppose that*

- *$\overline{\rho}|_{G_{\mathbb{Q}_l}}$ has centralizer $\mathbb{F}$;*
- *$\overline{\rho}|_{G_{\mathbb{Q}_l}}$ is reducible and has $\mathbb{F}_l$ as a field of definition;*
- *$\rho|_{G_{\mathbb{Q}_l}}$ is potentially Barsotti–Tate, and the associated Weil–Deligne representation $WD(\rho|_{G_{\mathbb{Q}_l}})$ is irreducible and tamely ramified.*

Then ρ is modular.

https://doi.org/10.1112/S0010437X03000289 Published online by Cambridge University Press

Proof. If $WD(\rho|_{G_{\mathbb{Q}_l}})$ satisfies the given hypotheses, then the Galois type of ρ is $\tau = \tilde{\omega}_2^m \oplus \tilde{\omega}_2^{lm}$ for some m not divisible by $l+1$. The hypotheses on ρ guarantee that $\overline{\rho}$ satisfies the conditions of Theorem 1.1, and the very existence of ρ implies that $R(\overline{\rho}, 2, \tau) \neq (0)$. Hence τ is weakly acceptable for $\overline{\rho}$, and $\overline{\rho}$ is of one of the forms (1.2). Once we see that (in the terminology of [BCDT01]) our $\tau = \tilde{\omega}_2^m \oplus \tilde{\omega}_2^{lm}$ *admits* each of the two possibilities for $\overline{\rho}$, then by Theorem 1.4.1 of [BCDT01] we obtain that ρ is modular.

To verify the admittance statement, one first checks that (in the notation of [CDT99] and [BCDT01]) $\sigma_\tau \cong \Theta(\chi)$ where $\chi : \mathbb{F}_{l^2}^\times \to \overline{\mathbb{Q}}_l$ maps $c \mapsto c^{-m}$. (The reason for an exponent of $-m$ instead of an exponent of m is the choice of normalization for the local Langlands correspondence in [CDT99]: namely, in Lemma 4.2.4(3) of [CDT99], we note that since $\eta_{l,2} = \tilde{\omega}_2^{-1}$, the character $\tilde{\omega}_2$ corresponds to $c \mapsto c^{-1}$.) Since $m = i + (l+1)j$ with $i \in \{1, \ldots, l\}$ and $j \in \mathbb{Z}/(l-1)\mathbb{Z}$, we may similarly write $-m = (l+1-i) + (l+1)(-1-j)$. By Lemma 3.1.1 of [CDT99], $\sigma_\tau \otimes \overline{\mathbb{F}}_l$ contains as Jordan–Hölder subquotients (again, in the notation of [BCDT01]) the representation $\sigma_{l-1-i,-j}$ (if $i \neq l$) and $\sigma_{i-2,l-i-j}$ (if $i \neq 1$). From the definitions in [BCDT01, § 1.3], $\sigma_{l-1-i,-j}$ admits $\left(\begin{smallmatrix}\omega^{1+j} & * \\ 0 & \omega^{i+j}\end{smallmatrix}\right)$ with $*$ peu ramifié if $i = l-1$, while $\sigma_{i-2,l-i-j}$ admits $\left(\begin{smallmatrix}\omega^{i+j} & * \\ 0 & \omega^{1+j}\end{smallmatrix}\right)$ with $*$ peu ramifié if $i = 2$, as desired. □

Thus we obtain new cases of the Fontaine–Mazur conjectures [FM95] conditional on the modularity of the residual representation (see [Ser87]). For another approach to these conjectures, see [Tay02].

Remark 1.4. Once a theory of Breuil modules with coefficients (see § 3) is sufficiently well developed, it should allow one to remove from Theorem 1.3 the hypotheses that $\overline{\rho}$ is a representation defined over $\mathbb{F}_l$ (instead of over an arbitrary finite field of characteristic l). One should also then be able to use our methods to address Conjecture 1.2.3 of [CDT99] in the case of irreducible $\overline{\rho}|_{G_{\mathbb{Q}_l}}$.

Example 1.5. Let C be the genus four curve

$$y^2 + (x^3 + x^2 + 1)y = -x^5 - x^4 - 2x^3 - 4x^2 - 2x - 1,$$

and let $J = \mathrm{Jac}(C)$. In [Bru95], Brumer gave families of curves with real multiplication by $\sqrt{5}$ over $\mathbb{Q}$, including the family

$$y^2 + (x^3 + x + 1 + c(x^2 + x))y = b + (1 + 3b)x + (1 - bd + 3b)x^2 + (b - 2bd - d)x^3 - bdx^4.$$

Setting $b = c = d = -1$ and substituting $y = y' + x^2$ yields the curve C. Hence J carries real multiplication by $\sqrt{5}$, and the Galois representation on the five-adic Tate module of J may be regarded as a two-dimensional representation $\rho_{J,5} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Q}_5(\sqrt{5}))$. In computations performed jointly with Stein, we verify that $\rho_{J,5}$ satisfies the hypotheses of Theorem 1.3, and so J is modular. González-Jiménez and González [GJG03] have shown the existence of a non-constant map $X_1(175) \to C$, and so J is also modular for that reason.

The remainder of this article is concerned with the proof of Theorem 1.1.

2. Deformation theory

Henceforth ρ and $\overline{\rho}$ will denote representations of $G_{\mathbb{Q}_l}$. All group schemes in this article are commutative.

2.1 Weil–Deligne representations: the Barsotti–Tate case

When $\rho : G_{\mathbb{Q}_l} \to \mathrm{GL}_d(E)$ is potentially Barsotti–Tate, we provide an alternate description of $WD(\rho)$, directly following Appendix B.3 of [CDT99]. Suppose ρ becomes Barsotti–Tate over a

https://doi.org/10.1112/S0010437X03000289 Published online by Cambridge University Press

finite Galois extension K of $\mathbb{Q}_l$, so that $\rho|_{G_K}$ arises from an l-divisible group Γ over $\mathcal{O}_K$. Write $\mathcal{O}$ for the integers of E, let $\mathbf{k}$ be the residue field of K, and let σ denote the arithmetic Frobenius on $W(\mathbf{k})$.

By Tate's full faithfulness theorem (Theorem 4 of [Tat67]), Γ has an action of $\mathrm{Gal}(K/\mathbb{Q}_l)$ over the action of $\mathrm{Gal}(K/\mathbb{Q}_l)$ on $\mathrm{Spec}(\mathcal{O}_K)$. This reduces to an action on the closed fibre $\Gamma \times \mathbf{k}$. Let ϕ be the Frobenius endomorphism of the closed fibre of Γ; then we produce an action of W_l on $\Gamma_{/\mathbf{k}}$ by letting g act via $g|_K \circ \phi^{-v(g)}$.

This above action of W_l is a right-action. It therefore translates into a left-action on the contravariant Dieudonné module $D(\Gamma_{/\mathbf{k}})$. Then $D(\Gamma_{/\mathbf{k}})$ is a free $W(\mathbf{k})$-module of rank $d[E:\mathbb{Q}_l]$ with an action of the Dieudonné ring $W(\mathbf{k})[F,V]$. (Recall that in this ring we have the relationships: F acts σ-semilinearly on $W(\mathbf{k})$, V acts σ^{-1}-semilinearly on $W(\mathbf{k})$, and $FV = VF = l$.)

Next, we define an action of W_l on

$$D'(\Gamma_{/\mathbf{k}}) = \mathrm{Hom}_{W(\mathbf{k})}(D(\Gamma_{/\mathbf{k}}), W(\mathbf{k})). \tag{2.1}$$

We set $\phi'(f) = \sigma \circ f \circ F^{-1}$ on $D'(\Gamma_{/\mathbf{k}})[1/l]$, and for $g \in \mathrm{Gal}(K/\mathbb{Q}_l)$ we set $g(f) = \overline{g} \circ f \circ g^{-1}$, where $\overline{g}$ is the map g induces on $W(\mathbf{k})$ and g^{-1} is the semilinear action on $D(\Gamma_{/\mathbf{k}})$ coming from the semilinear action on Γ. Finally, as usual, we let W_l act on $D'(\Gamma_{/\mathbf{k}})$ by letting g act as $g|_K \circ (\phi')^{-v(g)}$.

Finally, we note that the action of $\mathcal{O}$ on Γ propagates through all of the above constructions, and we have [CDT99, Proposition B.3.1]

$$WD(\rho) \cong D'(\Gamma_{/\mathbf{k}}) \otimes_{W(\mathbf{k}) \otimes_{\mathbb{Z}_l} \mathcal{O}} \overline{\mathbb{Q}}_l.$$

2.2 Dieudonné module calculations

For the rest of this article, we fix $\tau = \tilde{\omega}_2^m \oplus \tilde{\omega}_2^{lm}$, and the following notation. Let $\mathbb{Q}_{l^2}$ be the copy in $\overline{\mathbb{Q}}_l$ of the field of fractions of the Witt vectors $W(\mathbb{F}_{l^2})$, and let π be a choice of $(-l)^{1/i^2-1}$. Let $H = \mathbb{Q}_l(\pi)$, $H' = \mathbb{Q}_{l^2}(\pi)$. Note that $\tau|_{I_H}$ is trivial. We will regard an element $\zeta \in \mathbb{F}_{l^2}^\times$ as an element in $W(\mathbb{F}_{l^2})$ (and hence in $\mathbb{Q}_{l^2}$) via the Teichmüller lifting map. Let g_ζ denote the element of $\mathrm{Gal}(H'/\mathbb{Q}_l)$ fixing $\mathbb{Q}_{l^2}$ and sending π to $\zeta\pi$. Let φ denote the element of $\mathrm{Gal}(H'/\mathbb{Q}_l)$ fixing π and extending the non-trivial automorphism of $\mathbb{Q}_{l^2}$.

Suppose $\rho : G_{\mathbb{Q}_l} \to \mathrm{GL}_2(E)$ is a potentially Barsotti–Tate representation with Galois type τ and with determinant

$$\det(\rho) = \epsilon \cdot \mathrm{Teich}(\omega^{-1} \det(\overline{\rho})),$$

where 'Teich' denotes the Teichmüller lift.

We now specialize the discussion of § 2.1 to this situation. We know $\tau|_{I_{H'}}$ is trivial, and so ρ becomes Barsotti–Tate when restricted to $G_{H'}$. Consequently, we obtain an l-divisible group Γ over $\mathcal{O}_{H'}$ such that the Tate module of the generic fibre of Γ is $\rho|_{G_{H'}}$. The residue field of H' is $\mathbf{k} = \mathbb{F}_{l^2}$, the Witt vectors $W(\mathbf{k}) = \mathbb{Z}_{l^2}$, σ is the Frobenius automorphism of $\mathbb{Z}_{l^2}$, and in the notation of § 2.1 the map $\overline{g}_\zeta$ is the identity for each ζ, and the map $\overline{\varphi} = \sigma$.

We saw in § 2.1 [CDT99, Proposition B.3.1] that

$$WD(\rho) \cong D'(\Gamma_{/\mathbb{F}_{l^2}}) \otimes_{\mathbb{Z}_{l^2} \otimes_{\mathbb{Z}_l} \mathcal{O}_E} \overline{\mathbb{Q}}_l, \tag{2.2}$$

where $g \in W_l$ acts on the right-hand side via $g|_{H'} \circ (\phi')^{-v(g)}$. In particular, I_l acts via $I_l \twoheadrightarrow \mathrm{Gal}(H'/\mathbb{Q}_{l^2})$, and since $v(I_l) = 0$, no untwisting is needed.

Since $\tau = \tilde{\omega}_2^m \oplus \tilde{\omega}_2^{lm}$, there exist basis elements $\mathbf{v}, \mathbf{w}$ of $D'(\Gamma_{/\mathbb{F}_{l^2}}) \otimes_{\mathbb{Z}_{l^2} \otimes_{\mathbb{Z}_l} \mathcal{O}_E} \overline{\mathbb{Q}}_l$ so that for $g \in I_l$ $g(\mathbf{v}) = \tilde{\omega}_2^m(g)\mathbf{v}$ and $g(\mathbf{w}) = \tilde{\omega}_2^{lm}(g)\mathbf{w}$.

For $\zeta \in \mathbb{F}_{l^2}$, by definition we have

$$\tilde{\omega}_2^m(g_\zeta) = (g_\zeta(\pi)/\pi)^m = \zeta^m,$$

https://doi.org/10.1112/S0010437X03000289 Published online by Cambridge University Press

and similarly $\tilde{\omega}_2^{lm}(g_\zeta) = \zeta^{lm}$. Thus $g_\zeta(\mathbf{v}) = \zeta^m\mathbf{v}$ and $g_\zeta(\mathbf{w}) = \zeta^{lm}\mathbf{w}$. Similarly, we find $g_\zeta^l(\mathbf{v}) = \zeta^{lm}\mathbf{v}$ and $g_\zeta^l(\mathbf{w}) = \zeta^m\mathbf{w}$, from which we conclude that $g_\zeta + g_\zeta^l$ acts on $D'(\Gamma_{/\mathbb{F}_{l^2}}) \otimes_{\mathbb{Z}_{l^2}\otimes_{\mathbb{Z}_l}\mathcal{O}_E} \overline{\mathbb{Q}}_l$ by scalar multiplication by $\zeta^m + \zeta^{lm}$, whereas g_ζ^{l+1} acts by scalar multiplication by $\zeta^{(l+1)m}$. (The action is linear, and not semilinear, since the image of $I_l \to \mathrm{Gal}(H'/\mathbb{Q}_{l^2})$ acts trivially on the coefficients $\mathbb{Z}_{l^2}$.)

We now wish to use Equation (2.1) and the action $g_\zeta(f) = \overline{g}_\zeta \circ f \circ g_\zeta^{-1} = f \circ g_\zeta^{-1}$ on $D'(\Gamma_{/\mathbb{F}_{l^2}})$ to understand the action of g_ζ on $D(\Gamma_{/\mathbb{F}_{l^2}})$.

Since $D'(\Gamma_{/\mathbb{F}_{l^2}})$ is a free module, the actions of g_ζ and g_ζ^l must sum and multiply on $D'(\Gamma_{/\mathbb{F}_{l^2}})$ to scalar multiplication by $\zeta^m + \zeta^{lm}$ and $\zeta^{(l+1)m}$, respectively. If $f \in D'(\Gamma_{/\mathbb{F}_{l^2}})$, we know $g_\zeta(f(x)) = f(g_\zeta^{-1}x)$ with $x \in D(\Gamma_{/\mathbb{F}_{l^2}})$. It follows that $f((g_\zeta^{-1} + g_\zeta^{-l})x) = (g_\zeta + g_\zeta^l)f(x) = (\zeta^m + \zeta^{lm})f(x) = f((\zeta^m + \zeta^{lm})x)$. By freeness, for any non-zero $x \in D(\Gamma_{/\mathbb{F}_{l^2}})$ we can find $f \in D'(\Gamma_{/\mathbb{F}_{l^2}})$ which does not vanish on x, so we conclude that $g_\zeta^{-1} + g_\zeta^{-l}$ acts as scalar multiplication by $\zeta^m + \zeta^{lm}$ on $D(\Gamma_{/\mathbb{F}_{l^2}})$. Replacing ζ by ζ^{-1}, we have found that

$$g_\zeta + g_\zeta^l \text{ acts as scalar multiplication by } \zeta^{-m} + \zeta^{-lm} \text{ on } D(\Gamma_{/\mathbb{F}_{l^2}}). \tag{2.3}$$

Similarly

$$g_\zeta^{l+1} \text{ acts as scalar multiplication by } \zeta^{-(l+1)m} \text{ on } D(\Gamma_{/\mathbb{F}_{l^2}}). \tag{2.4}$$

We next wish to see what the determinant condition tells us about $D(\Gamma_{/\mathbb{F}_{l^2}})$. Let χ_l denotes the one-dimensional unramified character of W_l sending arithmetic Frobenius to l, and let

$$\chi = \mathrm{Teich}(\omega^{-1}\det(\overline{\rho}))|_{W_{\mathbb{Q}_l}} \otimes_E \overline{\mathbb{Q}}_l.$$

By the examples in § B.2 of [CDT99] and since WD is compatible with tensor products, we have $WD(\det(\rho)) = \chi_l\chi$. Let s be any lift of φ to W_l, so s is a lift of arithmetic Frobenius but fixes F. Since WD is compatible with the formation of exterior products, we know $\det(WD(\rho)) = WD(\det(\rho))$, and in particular $\det(WD(\rho)(s)) = lT$, where $T = \mathrm{Teich}(\omega^{-1}\det(\overline{\rho}))(s) = \mathrm{Teich}(\det(\overline{\rho}))(s)$. (We have $\omega(s) = 1$ since s fixes F.) Note that T depends only on $\overline{\rho}$, not on ρ or the choice of s.

We claim that $\mathrm{Trace}(WD(\rho)(s)) = 0$. Since

$$WD(\rho)|_{I_l} = \begin{pmatrix} \tilde{\omega}_2^m & 0 \\ 0 & \tilde{\omega}_2^{lm} \end{pmatrix}$$

and since for any $u \in I_l$ we have the relationship $WD(\rho)(sus^{-1}) = WD(\rho)(u^l)$, a quick calculation shows that $WD(\rho)(s)$ must act via a matrix $\left(\begin{smallmatrix} 0 & * \\ * & 0 \end{smallmatrix}\right)$. Therefore, we have shown that $WD(\rho)(s)$ satisfies the characteristic polynomial $X^2 + lT = 0$. By Equation (2.2), and since $D'(\Gamma_{/\mathbb{F}_{l^2}})$ is free, the action of s on $D'(\Gamma_{/\mathbb{F}_{l^2}})$ must satisfy this same polynomial.

For $D(\Gamma_{/\mathbb{F}_{l^2}})$, note that if $f \in D'(\Gamma_{/\mathbb{F}_{l^2}})[1/l]$ then

$$s(f)(x) = \varphi \circ (\phi')^{-1}(f)(x) = (\sigma(\sigma^{-1} \circ f \circ F) \circ \varphi)(x) = f(F \circ \varphi(x))$$

for $x \in D(\Gamma)$. Then

$$s^2(f)(x) = f(F^2 \circ [\varphi]^2(x)) = f(F^2(x)).$$

Since $s^2 + lT = 0$ on $D'(\Gamma_{/\mathbb{F}_{l^2}})$, we learn that $f((F^2 + lT)x) = 0$ for all x and f, and consequently $F^2 + lT = 0$ on $D(\Gamma_{/\mathbb{F}_{l^2}})$. Applying V to both sides of this equation we see $F(FV) + lTV = lF + lTV = 0$ and since $D(\Gamma_{/\mathbb{F}_{l^2}})$ is free we obtain the relationship

$$F + TV = 0 \tag{2.5}$$

on $D(\Gamma_{/\mathbb{F}_{l^2}})$.

2.3 Deformation problems

We will make use of the following definitions, essentially following § 4 of [BCDT01].

Definition 2.6. If X is a scheme over $\operatorname{Spec} A$ and $g : A \to B$ is a ring homomorphism, let ${}^{g}X$ denote the pullback of X by g. Suppose that K/L is an Galois extension of fields over $\mathbb{Q}_l$, and let $\mathcal{G}$ be a group scheme over $\mathcal{O}_K$. By *generic fibre descent data* from K to L, we mean a collection of isomorphisms

$$[g] : \mathcal{G} \to {}^{g}\mathcal{G}$$

for $g \in \mathrm{Gal}(K/L)$ satisfying the compatibility conditions $[gh] = ({}^{g}[h]) \circ [g]$. The pair $(\mathcal{G}, \{[g]\})$, which we will sometimes abbreviate as $\mathcal{G}$, is a *group scheme with descent data*. Note that since $\mathcal{O}_K/\mathcal{O}_L$ is not necessarily étale, we do not necessarily obtain a descended group scheme over $\mathcal{O}_L$. However, since K/L is étale we can descend the generic fibre as usual, and we denote the descended L-group scheme by $(\mathcal{G}, \{[g]\})_L$. By the descended G_L-representation of $(\mathcal{G}, \{[g]\})_L$, we mean the representation of G_L on $(\mathcal{G}, \{[g]\})_L(\overline{\mathbb{Q}}_l)$.

Definition 2.7. If G is a finite group scheme over a field $L/\mathbb{Q}_l$, then an *integral model* of G is a finite flat group scheme $\mathcal{G}$ over $\mathcal{O}_L$ such that $\mathcal{G} \times_{\mathcal{O}_L} L \cong G$. More generally, if K/L is a Galois extension, then an *integral model of G with descent data* over $\mathcal{O}_K$ is a finite flat group scheme $(\mathcal{G}, \{[g]\})$ over $\mathcal{O}_K$ with descent data to L such that $(\mathcal{G}, \{g]\})_L \cong G$.

Fix $\overline{\rho} : G_{\mathbb{Q}_l} \to \mathrm{GL}_2(\mathbb{F}_l)$ a reducible Galois representation with centralizer $\mathbb{F}_l$, let $M_{\overline{\rho}}$ denote the standard $\mathbb{F}_l$-vector space on which $G_{\mathbb{Q}_l}$ acts via $\overline{\rho}$, and let $T = \mathrm{Teich}(\det(\overline{\rho}))(\mathrm{Frob}_l)$.

We let $\mathcal{S}(\overline{\rho})$ denote the full subcategory of the category of finite length discrete $\mathbb{Z}_l$-modules with $\mathbb{Z}_l$-linear action of $G_{\mathbb{Q}_l}$ consisting of objects which admit a finite filtration such that each graded piece is isomorphic to $M_{\overline{\rho}}$. Let $\mathcal{S}$ be the full subcategory of $\mathcal{S}(\overline{\rho})$ consisting of objects X for which there exists a finite flat $\mathcal{O}_{H'}$-group scheme $(\mathcal{G}, \{[g]\})$ with descent data to $\mathbb{Q}_l$ such that $X \cong (\mathcal{G}, \{[g]\})_{\mathbb{Q}_l}(\overline{\mathbb{Q}}_l)$ as $\mathbb{Z}_l[G_{\mathbb{Q}_l}]$-modules and such that $[\zeta]+[\zeta]^l-(\zeta^{-m}+\zeta^{-lm})$ and $[\zeta]^{l+1}-\zeta^{-(l+1)m}$ for all $\zeta \in \mathbb{F}_{l^2}^{\times}$, as well as $F+TV$, annihilate the Dieudonné module $D(\mathcal{G} \times \mathbb{F}_{l^2})$.

From Lemma 4.1.3 of [BCDT01] it follows that $\mathcal{S}$ is closed under finite products, subobjects, and quotients. Following § 4.3 of [BCDT01], define the set-valued functor $\mathcal{D}^{\mathcal{S}}_{\overline{\rho},\mathbb{Z}_l}$ on the category of complete Noetherian local $\mathbb{Z}_l$-algebras with residue field $\mathbb{F}_l$ by letting $\mathcal{D}^{\mathcal{S}}_{\overline{\rho},\mathbb{Z}_l}(R)$ be the set of conjugacy classes of continuous R-representations such that $\rho \bmod \mathfrak{m}_R$ is conjugate to $\overline{\rho}$ and such that for each open ideal $\mathfrak{a} \subset R$ the action of ρ makes $(R/\mathfrak{a})^2$ into an object of $\mathcal{S}$.

By a theorem of Ramakrishna [Ram93], if $\mathcal{D}^{\mathcal{S}}_{\overline{\rho},\mathbb{Z}_l}(\mathbb{F}_l)$ is non-empty, then the functor $\mathcal{D}^{\mathcal{S}}_{\overline{\rho},\mathbb{Z}_l}$ is representable; in this case, let $R^{\mathcal{S}}_{\overline{\rho},\mathbb{Z}_l}$ denote the resulting deformation ring. We have the following.

Proposition 2.8. *If $\mathcal{D}^{\mathcal{S}}_{\overline{\rho},\mathbb{Z}_l}(\mathbb{F}_l)$ is non-empty, then there is a surjection*

$$R^{\mathcal{S}}_{\overline{\rho},\mathbb{Z}_l} \twoheadrightarrow R(\overline{\rho}, 2, \tau).$$

Proof. Let $R^{\mathrm{univ}}_{\overline{\rho}}$ denote the universal deformation ring for $\overline{\rho}$, and let

$$\mathcal{I} = \ker(R^{\mathrm{univ}}_{\overline{\rho}} \twoheadrightarrow R^{\mathcal{S}}_{\overline{\rho},\mathbb{Z}_l}).$$

It suffices to show

$$\mathcal{I} \subset \ker(R^{\mathrm{univ}}_{\overline{\rho}} \twoheadrightarrow R(\overline{\rho}, 2, \tau)) = \bigcap_{\mathfrak{p}\ \text{type}\ \tau} \mathfrak{p} = \bigcap_{i \geqslant 1, \mathfrak{p}\ \text{type}\ \tau} (\mathfrak{p}, l^i).$$

In other words, we need to show that each map $R^{\mathrm{univ}}_{\overline{\rho}} \twoheadrightarrow R^{\mathrm{univ}}_{\overline{\rho}}/(\mathfrak{p}, l^i)$ factors through $R^{\mathrm{univ}}_{\overline{\rho}} \twoheadrightarrow R^{\mathcal{S}}_{\overline{\rho},\mathbb{Z}_l}$. Let $\tilde{\rho}$ denote the representation arising from $R^{\mathrm{univ}}_{\overline{\rho}} \twoheadrightarrow R^{\mathrm{univ}}_{\overline{\rho}}/(\mathfrak{p}, l^i)$. Since $\mathfrak{p}$ has type τ, there is an extension $E/\mathbb{Q}_l$ and an exact sequence $0 \to \mathfrak{p} \to R^{\mathrm{univ}}_{\overline{\rho}} \to E$ so that the resulting $\rho : G_{\mathbb{Q}_l} \to$

$\mathrm{GL}_2(E)$ is of type τ. The results of § 2.2 produce an l-divisible group $\Gamma/\mathcal{O}_{H'}$ satisfying the desired relations on the Dieudonné module of its closed fibre and whose generic fibre representation is $\rho|_{G_{H'}}$. The l^i-torsion $\Gamma[l^i]$ is the desired finite flat group scheme with descent data which shows that the conjugacy class of $\tilde{\rho}$ is indeed in $\mathcal{D}^{\mathcal{S}}_{\overline{\rho},\mathbb{Z}_l}(R^{\mathrm{univ}}_{\overline{\rho}}/(\mathfrak{p},l^i))$. □

Corollary 2.9. *If $\mathcal{D}^{\mathcal{S}}_{\overline{\rho},\mathbb{Z}_l}(\mathbb{F}_l)$ is non-empty, then the dimension of the tangent space of $R(\overline{\rho},2,\tau)$ is at most the dimension of the tangent space of $R^{\mathcal{S}}_{\overline{\rho},\mathbb{Z}_l}$.*

The rest of this article will be concerned with the proof of the following theorem.

Theorem 2.10. *If $R(\overline{\rho},2,\tau)\neq(0)$, then $\mathcal{D}^{\mathcal{S}}_{\overline{\rho},\mathbb{Z}_l}(\mathbb{F}_l)$ is non-empty. In this case, $\overline{\rho}|_{I_l}$ is of one of the two forms (1.2), and up to isomorphism there is exactly one finite flat group scheme $(\mathcal{G},\{[g]\})$ over $\mathcal{O}_{H'}$ with descent data to $\mathbb{Q}_l$ such that $(\mathcal{G},\{[g]\})_{\mathbb{Q}_l}\cong\overline{\rho}$ and such that $D(\mathcal{G}\times\mathbb{F}_{l^2})$ satisfies the relations (2.3)–(2.5). The space of extensions of $(\mathcal{G},\{[g]\})$ by $(\mathcal{G},\{[g]\})$, in the category of finite flat $\mathcal{O}_{H'}$-group schemes with descent data, whose Dieudonné modules satisfy these relations, is one-dimensional.*

This theorem evidently implies that if $R(\overline{\rho},2,\tau)\neq(0)$ then $R^{\mathcal{S}}_{\overline{\rho},\mathbb{Z}_l}$ exists and has a one-dimensional tangent space, which completes the proof of Theorem 1.1.

2.4 Strategy of the calculation

If $R(\overline{\rho},2,\tau)\neq(0)$, then there exists a prime $\mathfrak{p}$ of type τ. Hence there is a lift ρ of $\overline{\rho}$ which arises from an l-divisible group Γ over $\mathcal{O}_{H'}$ with descent data to $\mathbb{Q}_l$ and satisfying the Dieudonné module relations (2.3)–(2.5). Then the l-torsion $\Gamma[l]$ is filtered by integral models for $\overline{\rho}$ with descent data, so we see that $\mathcal{D}^{\mathcal{S}}_{\overline{\rho},\mathbb{Z}_l}(\mathbb{F}_l)$ is non-empty.

It remains to determine all (reducible) $\overline{\rho}$ for which there exists a group scheme $(\mathcal{G},\{[g]\})$ over $\mathcal{O}_{H'}$ with descent data to $\mathbb{Q}_l$, such that $(\mathcal{G},\{[g]\})_{\mathbb{Q}_l}\cong\overline{\rho}$, and such that the Dieudonné module of $\mathcal{G}$ satisfies relations (2.3)–(2.5); to show that when such a group scheme with descent data exists, there is exactly one of them; and, in this case, to compute the extensions described in Theorem 2.10.

Note that since $\overline{\rho}$ is reducible, any integral model with descent data for $\overline{\rho}$ over $\mathcal{O}_{H'}$ is an extension of rank-one group schemes which are integral models for the sub and quotient characters of $\overline{\rho}|_{G_{H'}}$, and by a scheme-theoretic closure argument (see [Ray74] or Lemma 4.1.3 of [BCDT01]) this is actually an extension in the category of integral models with descent data. In § 3, we describe the category of Breuil modules with descent data, which is anti-equivalent to the category of finite flat l-torsion group schemes with descent data. Breuil modules here will play the role played by the Honda systems in [Con99]. We compute all of the rank-one Breuil modules with descent data over a tamely ramified extension, and identify explicitly the Galois characters to which these Breuil modules with descent data correspond. We next classify all of the (rank-two) extensions, in the category of Breuil modules with descent data, of these rank-one Breuil modules with descent data, after which we may discard from consideration those Breuil modules with descent data which do not correspond to group schemes satisfying relations (2.3)–(2.5) on their Dieudonné modules.

We will indeed see that the only $\overline{\rho}$ for which integral models exist that admit generic fibre descent data satisfying the desired Dieudonné module relations, are exactly those of the form (1.2). Moreover, for each such $\overline{\rho}$ this integral model with descent data will be seen to be unique (up to isomorphism). We complete the proof of Theorem 2.10 by calculating $\mathrm{Ext}^1(\mathcal{M},\mathcal{M})$, in the category of Breuil modules with descent data, for the Breuil modules with descent data $\mathcal{M}$ corresponding to these integral models with descent data, and checking that the space of extensions satisfying the Dieudonné module relations is at most one-dimensional.

https://doi.org/10.1112/S0010437X03000289 Published online by Cambridge University Press

3. Review of Breuil modules with descent data

3.1 Breuil modules

We remind the reader that the prime l is odd. Let $K/\mathbb{Q}_l$ be a finite extension, and suppose K has integers $\mathcal{O}$, ramification index e_K, and residue field $\mathbf{k}$. Fix a uniformizer π of $\mathcal{O}$. A Breuil module $(\mathcal{M}, \mathcal{M}_1, \phi_1)$ for K consists of the following data:

- a finite-rank free $\mathbf{k}[u]/u^{e_K l}$-module $\mathcal{M}$;
- a submodule $\mathcal{M}_1 \subset \mathcal{M}$ such that $\mathcal{M}_1 \supset u^{e_K}\mathcal{M}$;
- an additive map $\phi_1 : \mathcal{M}_1 \to \mathcal{M}$ such that $\phi_1(hv) = h^l \phi_1(v)$ for any $h \in \mathbf{k}[u]/u^{e_K l}$ and $v \in \mathcal{M}_1$, and such that the $\mathbf{k}[u]/u^{e_K l}$-span of $\phi_1(\mathcal{M}_1)$ is all of $\mathcal{M}$.

Morphisms of Breuil modules are $\mathbf{k}[u]/u^{e_K l}$-module homomorphisms which preserve $\mathcal{M}_1$ and commute with ϕ_1. The rank of a Breuil module is defined to be its rank as a $\mathbf{k}[u]/u^{e_K l}$-module.

Breuil [Bre00] has proved the following theorem.

Theorem 3.1. *There is an (additive) contravariant equivalence of categories, depending on the choice of the uniformizer π, between the category of Breuil modules for K and the category of finite flat group schemes over $\mathcal{O}$ which are killed by l. The rank of the Breuil module is the same as the rank of the corresponding group scheme.*

When the field K and uniformizer π are clear from context, by the Breuil module corresponding to a group scheme we will mean the Breuil module obtained from the group scheme via this equivalence (and *vice versa*).

The Breuil module functor has numerous useful properties: for example, a short exact sequence of group schemes maps under the functor to a short exact sequence of Breuil modules, and a sequence of Breuil modules is short-exact if and only if the underlying sequence of $\mathbf{k}[u]/u^{e_K l}$-modules is short-exact [BCDT01, Lemma 5.1.1.]. This will allow us directly to compute the Exts of Breuil modules.

There is a very useful compatibility between Breuil theory and contravariant Dieudonné theory. Let $u^{e_K} - lG_\pi(u)$ be the minimal polynomial of π over $W(\mathbf{k})$, and let $c_\pi = -G_\pi(u)^l \in \mathbf{k}[u]/u^{e_K l}$. On any Breuil module, define $\phi : \mathcal{M} \to \mathcal{M}$ via $\phi(v) = (1/c_\pi)\phi_1(u^{e_K}v)$. Note that $u^{e_K}v \in \mathcal{M}_1$ by definition. Then [BCDT01, Theorem 5.1.3(3)] if $\mathcal{M}_\pi$ is the Breuil module corresponding to the group scheme $\mathcal{G}$ (with π as our fixed uniformizer), there is a canonical $\mathbf{k}$-linear isomorphism

$$D(\mathcal{G}) \otimes_{\mathbf{k},\mathrm{Frob}_l} \mathbf{k} \cong \mathcal{M}_\pi/u\mathcal{M}_\pi, \tag{3.2}$$

under which $F \otimes \mathrm{Frob}_l$ corresponds to ϕ and $V \otimes \mathrm{Frob}_l^{-1}$ corresponds to the composition

$$\mathcal{M}/u\mathcal{M} \xrightarrow{\phi_1^{-1}} \mathcal{M}_1/u\mathcal{M}_1 \to \mathcal{M}/u\mathcal{M}.$$

(One can see that ϕ_1 mod u is always bijective.)

3.2 Rank-one Breuil modules

It is a straightforward exercise [BCDT01, Example 5.2] to check that the rank-one Breuil modules are of the form

$$\mathcal{M} = (\mathbf{k}[u]/u^{e_K l})\mathbf{e}, \quad \mathcal{M}_1 = (\mathbf{k}[u]/u^{e_K l})u^r\mathbf{e}, \quad \phi_1(u^r\mathbf{e}) = a\mathbf{e}$$

with $0 \leqslant r \leqslant e_k$ and $a \in (\mathbf{k}[u]/u^{e_K l})^\times$. We will denote this module as $\mathcal{M}(r, a)$. The reader may verify that non-zero homomorphisms $\mathcal{M}(r, a) \to \mathcal{M}(r_1, a_1)$ exist if and only if $r_1 \geqslant r$, $r_1 \equiv r \pmod{l-1}$, and $a/a_1 \in ((\mathbf{k}[u]/u^{e_K l})^\times)^{l-1}$, and are given exactly by the linear maps $\mathbf{e} \mapsto bu^{l(r_1-r)/(l-1)}\mathbf{e}_1$ where $b^{l-1} = a/a_1$. In particular, any rank-one Breuil module $\mathcal{M}(r, a)$ is isomorphic to $\mathcal{M}(r, a(0))$,

https://doi.org/10.1112/S0010437X03000289 Published online by Cambridge University Press

where $a(0) \in \mathbf{k}^\times$ is the constant term of a. Therefore, in the remainder of this section we will assume that $a \in \mathbf{k}^\times$.

From 3.1.2 of [Bre00], the affine algebra underlying the group scheme corresponding to $\mathcal{M}(r,a)$ is

$$\mathcal{O}[X] \Big/ \left(X^l + \frac{\pi^{e_K - r}\tilde{a}}{G_\pi(\pi)} X \right),$$

where $\tilde{a}$ denotes the Teichmüller lift of a. We note that we may say even more, namely that the comultiplication on this algebra is exactly that which one would expect from the Oort–Tate classification, which leads us to Lemma 3.3.

Lemma 3.3. *Set $C = (\pi^{e_K - r}\tilde{a})/G_\pi(\pi) \in \mathcal{O}$. The group scheme corresponding to $\mathcal{M}(r,a)$ (under the fixed choice of uniformizer π) is isomorphic to the group scheme with affine algebra $\mathcal{O}[X]/(X^l + CX)$ and comultiplication*

$$X \mapsto 1 \otimes X + X \otimes 1 - \frac{l}{C} \sum_{i=1}^{l-1} \frac{X^i}{w_i} \otimes \frac{X^{l-i}}{w_{l-i}}, \tag{3.4}$$

where the units $w_i \in \mathbb{Z}_l^\times$ are as defined in § 2 of [OT70].

Proof. If $r < e_K$, so that C is divisible by π, one simply needs to note that

$$\mathcal{O}[X]/(X^l + CX) \cong \mathcal{O}[X]/(X^l + C'X)$$

if and only if $C/C' \in (\mathcal{O}^\times)^{l-1}$. By the Oort–Tate classification, the group scheme corresponding to $\mathcal{M}(r,a)$ is isomorphic to some $\operatorname{Spec} \mathcal{O}[X]/(X^l + C'X)$ with comultiplication as in Equation (3.4) with C' in place of C. Since $C'/C \in (\mathcal{O}^\times)^{l-1}$, it is therefore also isomorphic to $\operatorname{Spec} \mathcal{O}[X]/(X^l + CX)$ with comultiplication (3.4).

If $r = e_K$, the Dieudonné module compatibility (3.2) shows that the classical Dieudonné module of the closed fibre of the group scheme corresponding to $\mathcal{M}(e_K, a)$ is isomorphic to

$$\mathbf{k}[F,V] \Big/ \left(F + \frac{a}{G_\pi(0)}, V \right),$$

where the ring $\mathbf{k}[F,V]$ is non-commutative if $\mathbf{k} \neq \mathbb{F}_l$, satisfying $Fx = x^l F$, $Vx^l = xV$ for $x \in \mathbf{k}$, and $FV = VF = 0$. We recall from § 3 of [OT70] that the Dieudonné module attached to the group scheme

$$\mathbf{k}[X]/(X^l - \alpha X), \quad X \mapsto 1 \otimes X + X \otimes 1 + \beta \sum_{i=0}^{l-1} \frac{X^i}{i!} \otimes \frac{X^{l-i}}{(l-i)!}$$

with $\alpha\beta = 0$ is $\mathbf{k}[F,V]/(F - \alpha, V - \beta^{1/l})$. If the group scheme corresponding to $\mathcal{M}(e_K, a)$ is isomorphic to $\operatorname{Spec} \mathcal{O}[X]/(X^l + CX)$ for some $C \in \mathcal{O}$ with comultiplication (3.4), it follows that $C \in \mathcal{O}^\times$, and that the image of C in $\mathbf{k}$ differs from that of $-a/G_\pi(0)$ by an $(l-1)$st power. Noting that $G_\pi(0)$ and $G_\pi(\pi)$ have the same image in $\mathbf{k}$, the claim follows using Hensel's lemma. □

3.3 Generic fibre descent data

A group scheme with descent data $(\mathcal{G}, \{[g]\})$ corresponds to a Breuil module with descent data. With the notation of Definition 2.6, in the case where K/L a is tamely ramified Galois extension with relative ramification index $e = e(K/L)$, and the uniformizer π of K satisfies $\pi^e \in L$, the description of the generic fibre descent data is fairly simple. (In the wild case, it is decidedly not.) The following description has not appeared in the literature, but is essentially a transcription from an unpublished preprint of Conrad [Con], included here by permission.

https://doi.org/10.1112/S0010437X03000289 Published online by Cambridge University Press

Theorem 3.5. *If K/L is a tamely ramified Galois extension and $\pi^e \in L$, then giving generic fibre descent data on $(\mathcal{M}, \mathcal{M}_1, \phi_1)$ is equivalent to giving, for each $g \in \mathrm{Gal}(K/L)$, an additive bijection $[g] : \mathcal{M} \mapsto \mathcal{M}$ satisfying:*

- *each $[g]$ preserves $\mathcal{M}_1$ and commutes with ϕ_1;*
- *$[1]$ is the identity and $[g][h] = [gh]$;*
- *$g(au^iv) = g(a)(zu)^ig(v)$, where $g(\pi) = z\pi$ and $a \in \mathbf{k}$ is regarded as being in K via the Teichmüller lift.*

Moreover, this generic fibre descent data is compatible with Dieudonné theory (3.2).

To see that this description follows from the (significantly) more involved description, found in § 5.6 of [BCDT01], of generic fibre descent data over general (i.e. possibly wild) field extensions, we again quote from [Con]: observe, in the notation of [BCDT01], that we can choose $H_g(u) = g(\pi)/\pi$ a root of unity, so $t_g = 0$ for all g, $f_{g_1,g_2} = 0$ for all g_1, g_2, and therefore $\mathbf{1}_{g_1,g_2}$ is the identity.

Given two Breuil modules $\mathcal{M}'$, $\mathcal{M}''$ with descent data, an extension in the category of Breuil modules with descent data is an extension of Breuil modules

$$0 \to \mathcal{M}' \to \mathcal{M} \to \mathcal{M}'' \to 0$$

with generic fibre descent data on $\mathcal{M}$ such that for all $[g]$ the following diagram commutes:

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{M}' \arrow[r] \arrow[d, "{[g]}"] & \mathcal{M} \arrow[r] \arrow[d, "{[g]}"] & \mathcal{M}'' \arrow[r] \arrow[d, "{[g]}"] & 0 \\
0 \arrow[r] & \mathcal{M}' \arrow[r] & \mathcal{M} \arrow[r] & \mathcal{M}'' \arrow[r] & 0
\end{tikzcd}$$

If $\mathcal{M}$ is a Breuil module with descent data corresponding to a group scheme $\mathcal{G}$ with descent data from K to L, then by the descended L-group scheme (respectively G_L-representation) of $\mathcal{M}$, we mean the descended L-group scheme (respectively G_L-representation) of $\mathcal{G}$.

For any further facts about Breuil modules which may be necessary, the reader can refer to § 5 of [BCDT01]. We now begin the computations needed for the proof of Theorem 2.10.

4. A Galois cohomology lemma

Let K/L be a tamely ramified Galois extension of $\mathbb{Q}_l$, let $\mathbf{k}/\mathbf{l}$ be the extension of residue fields, let $e = e(K/L)$ be the ramification index, and let $\pi \in K$ be a uniformizer such that $\pi^e \in L$. For ease of notation, we will identify the elements of $\mathbf{k}$ with their Teichmüller lifts in K.

Lemma 4.1. *With the above notation, let n be a positive integer and let $G = \mathrm{Gal}(K/L)$ act on $\mathbf{k}[u]/u^n$ via ${}^g(\sum_{i=0}^{n-1} a_iu^i) = \sum_{i=0}^{n-1} g(a_i)\,(g\pi/\pi)^i\,u^i$. Under this action:*

- *$H^q(G, \mathbf{k}[u]/u^n) = 0$ for all $q > 0$;*
- *$\#H^1(G, (\mathbf{k}[u]/u^n)^\times) = e$.*

The non-zero elements of $H^1(G, (\mathbf{k}[u]/u^n)^\times)$ are represented by the cocycles $g \mapsto (g\pi/\pi)^i$, for $0 \leqslant i < e$.

Proof. Let $\mathbf{k}_i$ denote the additive group $\mathbf{k}$ with the G-action $g \cdot a = g(a)(g\pi/\pi)^i$. Let I denote the inertia subgroup of G, and let $K_0 = K^I$ be the maximal unramified extension of L inside K. Then $H^q(I, \mathbf{k}_i) = 0$ for all $q > 0$ as $\#\mathbf{k}_i$ is a power of l whereas $\#I$ is prime-to-l (since L/K is tame). As a result, the Hochschild–Serre spectral sequence provides an isomorphism

$$H^q(G/I, \mathbf{k}_i^I) \xrightarrow{\sim} H^q(G, \mathbf{k}_i)$$

https://doi.org/10.1112/S0010437X03000289 Published online by Cambridge University Press

for all q. We compute: $a \in \mathbf{k}_i^I$ if and only if $g(a)(g\pi/\pi)^i = a$ for all $g \in I$, if and only if $a\pi^i \in K_0$. Noting that $a \in K_0$, if $a \neq 0$ then $\pi^i \in K_0$, and in this case we see by considering the valuation that i is divisible by e. Hence either $\mathbf{k}_i^I = 0$ or $\mathbf{k}_i^I = \mathbf{k}$ with the usual action of $G/I = \mathrm{Gal}(\mathbf{k}/\mathbf{l})$. In both cases $H^q(G/I, \mathbf{k}_i^I) = 0$, and so $H^q(G, \mathbf{k}_i) = 0$ for all i and all $q > 0$.

Now the first claim of the lemma follows immediately from the isomorphism $\mathbf{k}[u]/u^n = \bigoplus_{i=0}^{n-1} \mathbf{k}_i$. To see the second claim, observe that we have a short exact sequence of G-modules

$$0 \to \{1 + au^n + u^{n+1}\mathbf{k}[u]/u^n\} \to (\mathbf{k}[u]/u^{n+1})^\times \to (\mathbf{k}[u]/u^n)^\times \to 0 \tag{4.2}$$

and note that the first module in the sequence (4.2) is isomorphic to $\mathbf{k}_n$ when $n \geqslant 1$. From the long exact sequence of cohomology associated with Equation (4.2) and the vanishing of $H^1(G, \mathbf{k}_n)$ and $H^2(G, \mathbf{k}_n)$ we obtain an isomorphism $H^1(G, (\mathbf{k}[u]/u^{n+1})^\times) \cong H^1(G, (\mathbf{k}[u]/u^n)^\times)$ for all $n \geqslant 1$. Hence $H^1(G, \mathbf{k}[u]/u^n) \cong H^1(G, \mathbf{k}^\times)$. By another application of the Hochschild–Serre spectral sequence, we obtain

$$0 \to H^1(G/I, (\mathbf{k}^\times)^I) \to H^1(G, \mathbf{k}^\times) \to H^1(I, \mathbf{k}^\times)^{G/I} \to H^2(G/I, (\mathbf{k}^\times)^I). \tag{4.3}$$

Inertia acts trivially on $\mathbf{k}$, and so the first and last groups in Equation (4.3) vanish by Hilbert's Theorem 90 and by the triviality of the Brauer group of finite fields, respectively. Therefore

$$H^1(G, \mathbf{k}^\times) \cong H^1(I, \mathbf{k}^\times)^{G/I} \cong \mathrm{Hom}(I, \mathbf{k}^\times)^{G/I}.$$

The right-hand side evidently is not bigger than $e = \#I$, and so to complete our proof we need only to show that the cocycles $g \mapsto (g\pi/\pi)^i$ for $0 \leqslant i < e$ lie in distinct cohomology classes. It suffices to show that they are non-trivial if $i \neq 0$. However, if $b \in (\mathbf{k}[u]/u^n)^\times$ is such that $(g\pi/\pi)^i = b/g_b$ for all $g \in G$, then since the left-hand side of this equality has no terms involving u we find $(g\pi/\pi)^i = b(0)/g(b(0))$ for all $g \in G$ as well. Then $b(0)\pi^i \in K^G = L$, and by considering the valuation we see that $e \mid i$, so $i = 0$. □

5. Rank-one modules

We retain our notation from § 4, so in particular K/L is a tamely ramified Galois extension of local fields with ramification index $e = e(K/L)$, and $\pi \in K$ satisfies $\pi^e \in L$. We let $e_K = e(K/\mathbb{Q}_l)$ denote the absolute ramification index of K, and $G = \mathrm{Gal}(K/L)$ acts on $\mathbf{k}[u]/u^{e_K l}$ as in Lemma 4.1. We will frequently need to divide various integers by the greatest common divisor $(l-1, e)$, and so we make the following definition.

Definition 5.1. If x is any integer, then x' will denote $x/(l-1,e)$; moreover, use of the expression x' will implicitly mean that x is divisible by $(l-1,e)$.

It is often useful that $x'y = xy'$. Finally, we choose U an integer which is an inverse of $(l-1)'$ modulo e', and let V satisfy

$$U(l-1)' = 1 + Ve'. \tag{5.2}$$

When $l - 1 \mid e$, for example, we will always choose $U = 1$, $V = 0$.

Proposition 5.3. *Consider the category of Breuil modules for $\mathcal{O}_K$ with π as the fixed choice of uniformizer.*

i) *A rank-one Breuil module $\mathcal{M}(r, a)$ admits generic fibre descent data from K to L if and only if r is divisible by $(l-1, e)$ and $a \in \mathbf{l}^\times((\mathbf{k}[u]/u^{el})^\times)^{l-1}$.*

ii) *For each $0 \leqslant r' \leqslant e'_K$, $a \in \mathbf{l}^\times$, $c \in \mathbb{Z}/(l-1,e)\mathbb{Z}$, define $\mathcal{M}_U(r,a,c)$ to be the Breuil module $\mathcal{M}(r,a)$ with descent data given by $[g]\mathbf{e} = (g\pi/\pi)^{e'c - Ulr'}\mathbf{e}$, extended G-semilinearly to additive bijections on $\mathcal{M}$. Any rank-one Breuil module with descent data from K to L is isomorphic to some $\mathcal{M}_U(r,a,c)$, and $\mathcal{M}_U(r,a,c) \cong \mathcal{M}_U(s,b,d)$ if and only if $r = s$, $c = d$, and $a/b \in (\mathbf{l}^\times)^{l-1}$.*

https://doi.org/10.1112/S0010437X03000289 Published online by Cambridge University Press

Proof. The first statement of the proposition follows immediately from the second, and from our understanding of maps between rank-one Breuil modules. It is straightforward to check that the additive bijections in item ii do indeed define generic fibre descent data.

Suppose now that $\mathcal{M}(r,a)$ admits generic fibre descent data given by $[g]\mathbf{e} = A_g\mathbf{e}$. We make the following observations:

i) We have $[h][g]\mathbf{e} = [h](A_g\mathbf{e}) = {}^hA_gA_h\mathbf{e}$, and so $A_{hg} = {}^hA_gA_h$.

ii) Replacing $\mathbf{e}$ by $\tilde{\mathbf{e}} = b\mathbf{e}$ as the standard basis vector, we find $\phi_1(u^r\tilde{\mathbf{e}}) = b^{l-1}a\tilde{\mathbf{e}}$, and $[g]\tilde{\mathbf{e}} = g_b/bA_g\tilde{\mathbf{e}}$.

Therefore $g \mapsto A_g$ is a cocycle in $H^1(G, (\mathbf{k}[u]/u^{e_K l})^\times)$, while replacing $\mathbf{e}$ by $b\mathbf{e}$ multiplies this cocycle by the coboundary $g \mapsto g_b/b$. As a consequence, by Lemma 4.1 we may make a choice of $\mathbf{e}$ so that $A_g = (g\pi/\pi)^k$ for some k.

Having done this, we calculate

$$\phi_1[g](u^r\mathbf{e}) = \phi_1\left(\left(\frac{g\pi}{\pi}\right)^{k+r} u^r\mathbf{e}\right) = \left(\frac{g\pi}{\pi}\right)^{lk+lr} a\mathbf{e}$$

while

$$[g]\phi_1(u^r\mathbf{e}) = [g]a\mathbf{e} = \left(\frac{g\pi}{\pi}\right)^{k} ({}^ga)\mathbf{e}.$$

Equating these two expressions, we find

$$\left(\frac{g\pi}{\pi}\right)^{(l-1)k+lr} = \frac{{}^ga}{a}.$$

We conclude that $g \mapsto (g\pi/\pi)^{(l-1)k+lr}$ is a coboundary, and therefore $e \mid (l-1)k+lr$ (see the proof of Lemma 4.1). From this, we easily see that $(l-1,e) \mid r$ and therefore that k must be of the form $e'c - Ulr'$ for some $c \in \mathbb{Z}/(l-1,e)\mathbb{Z}$.

Since $e \mid (l-1)k+lr$ it also follows that ${}^ga/a = 1$ for all $g \in G$ and so $a \in ((\mathbf{k}[u]/u^{e_K l})^\times)^G = (\mathbf{l}[u^e]/u^{e_K l})^\times$. We note, however, that replacing $\mathbf{e}$ by $\tilde{\mathbf{e}} = b\mathbf{e}$ with $b \in ((\mathbf{k}[u]/u^{e_K l})^\times)^G$ leaves A_g unchanged but replaces a by ab^{l-1}. Since

$$((\mathbf{l}[u^e]/u^{e_K l})^\times)^{l-1} = (\mathbf{l}^\times)^{l-1}(1 + u^e\mathbf{l}[u^e]/u^{e_K l}),$$

the remaining statements in the proposition follow easily. □

Example 5.4. Recall our notation from § 2.2. We are interested in describing the rank-one Breuil modules over $\mathcal{O}_{H'}$ with descent data from H' to $\mathbb{Q}_l$ using a choice of $\pi = (-l)^{1/(l^2-1)}$ as our uniformizer. In this case the ramification indices are $e = e_{H'} = l^2 - 1$ and the residue field of H' is $\mathbb{F}_{l^2}$, so these are rank-one modules over $\mathbb{F}_{l^2}[u]/u^{l(l^2-1)}$. Since $l-1 \mid e$, we choose $U = 1$ and $V = 0$. Whenever $U = 1$, we drop the subscript U from $\mathcal{M}_U(r,a,c)$.

Recall that $\mathrm{Gal}(H'/\mathbb{Q}_l)$ is generated by φ and the g_ζ, subject to the relations $g_\zeta^{l^2-1} = 1$ and $\varphi g_\zeta \varphi = g_\zeta^l$ for all $\zeta \in \mathbb{F}_{l^2}$. Since $H'/\mathbb{Q}_l$ is tamely ramified and $\pi^e = -l \in \mathbb{Q}_l$, we conclude from Proposition 5.3 that the desired Breuil modules with descent data are the $\mathcal{M}(r,a,c)$ given by

$$\mathcal{M} = \langle \mathbf{e} \rangle, \quad \mathcal{M}_1 = \langle u^{r'(l-1)}\mathbf{e} \rangle, \quad \phi_1(u^{r'(l-1)}\mathbf{e}) = a\mathbf{e}$$

for $a \in \mathbb{F}_l^\times$ and $r = r'(l-1)$ with $0 \leqslant r' \leqslant l+1$, and generic fibre descent data given by $[\varphi](\mathbf{e}) = \mathbf{e}$ and $[\zeta](\mathbf{e}) = \zeta^{(l+1)c-lr'}\mathbf{e}$ with $c \in \mathbb{Z}/(l-1)\mathbb{Z}$. (We will abbreviate $[g_\zeta]$ by $[\zeta]$.) For different triples (r,a,c), $\mathcal{M}(r,a,c)$ are non-isomorphic.

6. Identification of rank-one Breuil modules with descent data

We now give an argument which identifies the Breuil modules with descent data from § 5, in the following sense: the Breuil module $\mathcal{M}_U(r,a,c)$ corresponds to a finite flat group scheme $\mathcal{G}_U(r,a,c)$ over $\mathcal{O}_K$ with descent data, and we wish to determine the finite flat group scheme $\mathcal{G}_{U,L}(r,a,c)$ over L to which the generic fibre $\mathcal{G}_U(r,a,c)_{/K}$ descends. That is, we will compute the character $\chi_{U,L}(r,a,c) : G_L \to \mathbb{F}_l^\times$ obtained as the Galois representation on $\mathcal{G}_{U,L}(r,a,c)(\overline{\mathbb{Q}}_l)$. If L' is any field lying between L and K, we may similarly define the character $\chi_{U,L'}(r,a,c)$ of $G_{L'}$ obtained by restricting descent data to $\mathrm{Gal}(K/L')$. We will sometimes write $\chi_U(r,a,c)$ as shorthand for $\chi_{U,L}(r,a,c)$.

To begin, we note the following lemma.

Lemma 6.1. *There is a non-zero homomorphism from $\mathcal{M}_U(r,a,c)$ to $\mathcal{M}_U(s,b,d)$ if and only if $r \leqslant s$ and $r \equiv s \pmod{l-1}$, $a/b \in (\mathbf{l}^\times)^{l-1}$, and $c \equiv d + V(r-s)/(l-1) \pmod{(l-1,e)}$.*

Note. Henceforth, we will always let $\mathbf{e}$ denote the standard basis vector of $\mathcal{M}_U(s,b,d)$ and $\mathbf{e}'$ the standard basis vector of $\mathcal{M}_U(r,a,c)$.

Proof. Ignoring generic fibre descent data for the moment, the descent dataless analogue of this lemma (e.g. part 2 of Lemma 5.2.1 in [BCDT01]) states that we have a non-zero map from $\mathcal{M}(r,a)$ to $\mathcal{M}(s,b)$ if and only if $r \leqslant s$, $r \equiv s \pmod{l-1}$, and $a/b \in (\mathbf{k}^\times)^{l-1}$, and moreover all such maps are of the form $\mathbf{e}' \mapsto \alpha u^{l((s-r)/(l-1))}\mathbf{e}$ for $\alpha \in \mathbf{k}^\times$. Such a map is exactly compatible with generic fibre descent data when

$$\alpha \left(\frac{g\pi}{\pi}\right)^{e'c-Ulr'} u^{l((s-r)/(l-1))}\mathbf{e} = g(\alpha)\left(\frac{g\pi}{\pi}\right)^{l((s-r)/(l-1))}\left(\frac{g\pi}{\pi}\right)^{e'd-Uls'} u^{l((s-r)/(l-1))}\mathbf{e}$$

for all $g \in G$. This amounts to $\alpha \in \mathbf{l}^\times$ and

$$e'c - Ulr' \equiv e'd - Uls' + l\left(\frac{s-r}{l-1}\right) \pmod{e};$$

this congruence is easily seen to be equivalent to

$$c - d \equiv V\left(\frac{r-s}{l-1}\right) \pmod{(l-1,e)}. \qquad \square$$

Corollary 6.2. *If $r \equiv s \pmod{l-1}$, then $\chi_U(r,a,c) = \chi_U(s,a,c+V((s-r)/(l-1)))$.*

Proof. Put $d = c + V((s-r)/(l-1)) \in \mathbb{Z}/(l-1,e)\mathbb{Z}$. Suppose $r \leqslant s$. A non-zero map $\mathcal{M}_U(r,a,c) \to \mathcal{M}_U(s,a,d)$ exists by the previous lemma, and arises from a non-zero map $\mathcal{G}_U(r,a,c) \to \mathcal{G}_U(s,a,d)$ compatible with generic fibre descent data. Therefore we get a map $\mathcal{G}_{U,L}(r,a,c) \to \mathcal{G}_{U,L}(s,a,d)$ which is non-zero. This amounts to a non-zero map of Galois modules of order l, so is therefore an isomorphism, and we find $\chi_U(r,a,c) = \chi_U(s,a,d)$. If $s < r$, the maps go in the other direction but the conclusion is the same. □

Theorem 6.3. *Let*

$$\lambda = -la(\pi^e)^{Vr'-(l-1)'c} \in L.$$

Then $\chi_U(r,a,c) : G_L \to \mathbb{F}_l^\times$ is the character

$$\eta_\lambda : g \mapsto \frac{g(\lambda^{1/(l-1)})}{\lambda^{1/(l-1)}}.$$

Before we give the proof of Theorem 6.3, we need the following lemma.

https://doi.org/10.1112/S0010437X03000289 Published online by Cambridge University Press

Lemma 6.4. *Let $\mathcal{G}$ be a group scheme of order l over $\mathcal{O}_K$ with descent data from K to L, such that by the Oort–Tate classification $\mathcal{G} \cong \operatorname{Spec} \mathcal{O}_K[X]/(X^l + CX)$ with comultiplication (3.4). If $g \in \operatorname{Gal}(K/L)$, then the generic fibre descent data map $[g]$ sends $X \mapsto \alpha X$ for some α satisfying $\alpha^{l-1} = g(C)/C$.*

Proof. Let $\langle m \rangle$ be the multiplication-by-m endomorphism of $\mathcal{G}$, and let $\chi : \mathbb{F}_l^\times \to \mathbb{Z}_l^\times$ denote the Teichmüller map. Then $\langle m \rangle$ and $[g]$ commute, and so $[g]$ also commutes with the operator

$$e_1 = \frac{1}{l-1} \sum_{m \in \mathbb{F}_l^\times} \frac{1}{\chi(m)} \langle m \rangle,$$

defined by Oort and Tate [OT70]. But in the Oort–Tate construction, e_1 is the projection onto the submodule generated by X, and so

$$[g](X) = [g] \circ e_1(X) = e_1 \circ [g](X) \in \mathcal{O}_K X.$$

Write $[g](X) = \alpha X$ with $\alpha \in \mathcal{O}_K$. Since $[g](X^l) = \alpha^l X^l$ and $[g](CX) = g(C)\alpha X$, it follows that $\alpha^{l-1} = g(C)/C$. □

Now we return to the proof of Theorem 6.3.

Proof of Theorem 6.3. Let K_0 be the maximal unramified extension of L inside K and let $L_1 = L(\pi)$, so that $K = K_0 L_1$. Then it suffices to show

$$\chi_{U,K_0}(r,a,c) = \eta_\lambda|_{G_{K_0}} \tag{6.5}$$

and

$$\chi_{U,L_1}(r,a,c) = \eta_\lambda|_{G_{L_1}}. \tag{6.6}$$

Formula (6.5) is precisely what is obtained by applying this theorem to the totally ramified extension K/K_0. As for Equation (6.6), the extension K/L_1 is unramified, and the parameters U_1 and V_1 for this extension satisfy $U_1(l-1) = 1 + V_1$. Putting

$$\lambda_1 = -la(\pi)^{V_1 r - (l-1)c} = -la(\pi)^{-r + (l-1)(rU_1 - c)},$$

the statement of this theorem for the extension K/L_1 is that $\chi_{U,L_1}(r,a,c) = \eta_{\lambda_1}$. However, it is easily checked that λ_1/λ is a power of π^{l-1}, and so $\eta_{\lambda_1} = \eta_\lambda|_{G_{L_1}}$. We conclude that it suffices to prove the theorem in the cases of K/L an unramified extension and K/L a totally (tamely) ramified extension.

The unramified case is easy, since in that case generic fibre descent data actually descends the group scheme. Specifically, let $\mathcal{M}_L(r,a)$ be the Breuil module for $\mathcal{O}_L$ with chosen uniformizer π and parameters r and a. There is only one way to put generic fibre descent data on $\mathcal{M}(r,a)$, and Corollary 5.4.2 of [BCDT01] tells us that $\mathcal{M}(r,a)$ descends to $\mathcal{M}_L(r,a)$. Then it follows from Lemma 3.3 that the affine algebra underlying $\mathcal{M}_L(r,a)$ is $\mathcal{O}_L[X]/(X^l + (la/\pi^r)X)$ and $\chi_{U,L}(r,a) = \eta_{-la/\pi^r} = \eta_\lambda$, as desired.

We next turn to the situation when L/K is totally (tamely) ramified. We will first consider the case when $e \mid r$. Note that $(g\pi/\pi)^{e'} \in \mathbb{F}_l^\times$, so that in this case g acts as multiplication by $(g\pi/\pi)^{e'c - Ulr'} \in \mathbb{F}_l^\times$ on the standard basis vector of $\mathcal{M}_U(r,a,c)$. Since K/L is totally ramified, the residue fields $\mathbf{l}, \mathbf{k}$ are equal, and part 2 of Theorem 5.6.1 of [BCDT01] tells us that $D([g])$ is the multiplication-by-$(g\pi/\pi)^{e'c-Ulr'}$ endomorphism of the Dieudonné module, $D(\mathcal{G}_U(r,a,c) \times_K \mathbf{k})$. Since $(g\pi/\pi)^{e'c-Ulr'} \in \mathbb{F}_l$, there is an integer n such that $D([g]) = \mathrm{Id} + \cdots + \mathrm{Id}$ (where there are n Id's in the sum). As the Dieudonné functor is additive, it follows that the corresponding action of $[g]$ on $\mathcal{G}_U(r,a,c) \times_K \mathbf{k}$ is also multiplication by n, where $(g\pi/\pi)^{e'c-Ulr'}$ is the mod-l reduction of n.

https://doi.org/10.1112/S0010437X03000289 Published online by Cambridge University Press

Recall from Lemma 3.3 that the affine algebra of $\mathcal{G}_U(r,a,c)$ is $\mathcal{O}_K[X]/(X^l+CX)$ where $C = (\pi^{e_K - r}a)/G_\pi(\pi) = la/\pi^r$, and the comultiplication is

$$X \mapsto 1\otimes X + X\otimes 1 - \frac{l}{C}\sum_{i=1}^{l-1}\frac{X^i}{w_i}\otimes\frac{X^{l-i}}{w_{l-i}}.$$

In any case one can verify that the multiplication-by-n map on the mod-π reduction of this group scheme is $X \mapsto nX$, and using the fact that $n \equiv (g\pi/\pi)^{e'c-Ulr'} \pmod{\pi}$, we therefore know that the action of $[g]$ on $\mathcal{G}_U(r,a,c)$ fits in the commutative diagram

$$\begin{tikzcd}
\mathcal{G}_U(r,a,c) \arrow[r, "{[g]}"] \arrow[d] & \mathcal{G}_U(r,a,c) \arrow[d] \\
\operatorname{Spec}\mathcal{O}_L \arrow[r, "g"'] & \operatorname{Spec}\mathcal{O}_L
\end{tikzcd}$$

and sends $X \mapsto (g\pi/\pi)^{e'c-Ulr'}X + \pi f(X)$ for some polynomial $f(X)$. Since $g(C) = C$ (because $\pi^e \in L$ and $e \mid r$), we conclude from Lemma 6.4 that $[g] : X \mapsto (g\pi/\pi)^{e'c-Ulr'}X$.

We now consider the action of this descent data on the generic fibre. Put $\beta = \pi^{-(e'c-Ulr')}$ and $C_1 = \beta^{l-1}C \in L$. Note that we have a K-algebra isomorphism $\gamma : K[X]/(X^l+C_1X) \to K[X]/(X^l+CX)$ sending $X \mapsto \beta X$, and for each $g \in \operatorname{Gal}(K/L)$ we obtain the commutative diagram

$$\begin{tikzcd}
K[X]/(X^l+C_1X) \arrow[r] \arrow[d, "X\mapsto X"'] & K[X]/(X^l+CX) \arrow[d, "{[g]}"] \\
K[X]/(X^l+C_1X) \arrow[r] & K[X]/(X^l+CX)
\end{tikzcd}$$

where the horizontal maps are γ and the vertical maps are g-semilinear. This shows that, pulling our generic fibre descent data back via the map γ, the generic fibre descent data acts on $K[X]/(X^l + C_1X)$ simply via the action of Galois on K. Furthermore, γ pulls back the comultiplication on $K[X]/(X^l+CX)$ to the following comultiplication on $K[X]/(X^l+C_1X)$:

$$X \mapsto 1\otimes X + X\otimes 1 - \frac{l}{C_1}\sum_{i=1}^{l-1}\frac{X^i}{w_i}\otimes\frac{X^{l-i}}{w_{l-i}}.$$

It follows immediately that the descended group scheme over L corresponding to the above group scheme with descent data over K is $L[X]/(X^l+C_1X)$ with the usual Oort–Tate comultiplication. Therefore the character $\chi_{U,L}(r,a,c)$ is η_{-C_1}. Using $e \mid r$ it is straightforward to check that $-C_1/\lambda$ is an $(l-1)$st power in L, and so $\chi_{U,L}(r,a,c) = \eta_\lambda$ as well.

Now suppose instead that $0 < r < e_K$. Again $\mathcal{G}_U(r,a,c)$ has underlying algebra $\mathcal{O}_K[X]/(X^l + CX)$ with $C = la/\pi^r$. From Lemma 6.4 we have $[g] : X \mapsto \mu_g X$ where μ_g satisfies $\mu_g^{l-1} = (g\pi/\pi)^{-r}$, and we must determine μ_g.

Note that the induced action of $[g]$ on the closed fibre sends $X \mapsto \mu_g X$, and by the identification of the Cartier–Manin Dieudonné module of $\mathcal{G}_U(r,a,c)\otimes_{\mathcal{O}_K}\mathbf{k} \cong \alpha_l$ with its tangent space, we find that $[g]$ induced multiplication by μ_g on the Dieudonné module. We also know that $[g]$ on $\mathcal{M}_U(r,a,c)/u\mathcal{M}_U(r,a,c)$ acts as multiplication by $(g\pi/\pi)^{e'c-lUr'}$, and from the proof of Theorem 5.1.3 in [BCDT01] it follows that $\mu_g^l = (g\pi/\pi)^{e'c-lUr'}$. We conclude that $\mu_g = (g\pi/\pi)^{e'c-lUr'+r}$. (One may check that indeed this μ_g satisfies $\mu_g^{l-1} = (g\pi/\pi)^{-r}$.) Now proceeding exactly as in the case $e \mid r$, we put

$$C_1 = \pi^{-(l-1)(e'c-lUr'+r)}\frac{la}{\pi^r} = la(\pi^e)^{(lVr'-c(l-1)')} \in L$$

and compute that $\chi_U(r,a,c) = \eta_{-C_1} = \eta_\lambda$. □

Example 6.7. We return to the example of particular interest, namely when the extension K/L is $H'/\mathbb{Q}_l$, so $e_K = e = l^2 - 1$, $U = 1$, $V = 0$, and $\pi = (-l)^{1/(l^2-1)}$. Then $(l-1)' = 1$, $\pi^e = -l$, and $\lambda = a(-l)^{1-c}$. Theorem 6.3 now says that $\chi(r,a,c) = \chi_a \omega^{1-c}$, where χ_a is the unramified character sending arithmetic Frobenius to a.

7. Rank-two extensions of rank-one modules

In this section, we classify the extensions, in the category of Breuil modules with descent data, of the rank-one modules in the previous sections by one another. The extensions without descent data are classified in Lemma 5.2.2 of [BCDT01].

Lemma 7.1. *In the category of Breuil modules corresponding to finite flat l-torsion group schemes over $\mathcal{O}_K$ with choice of uniformizer π, we have an isomorphism*

$$\operatorname{Ext}^1(\mathcal{M}(r,a), \mathcal{M}(s,b)) \cong \{h \in u^{\max(0, r+s-e_K)} \mathbf{k}[u]/u^{e_K l}\}/\{u^s t - (b/a) u^r t^l\}$$

given by associating to each $h \in u^{\max(0,r+s-e_K)}\mathbf{k}[u]/u^{e_K l}$ the ϕ_1-module

$$\mathcal{M} = \langle \mathbf{e}, \mathbf{e}' \rangle, \quad \mathcal{M}_1 = \langle u^s \mathbf{e}, u^r \mathbf{e}' + h\mathbf{e} \rangle,$$

with

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

Moreover, replacing the basis element $\mathbf{e}'$ with $\mathbf{e}' + (b/a)t^l\mathbf{e}$ transforms h to $h + (u^s t - (b/a)u^r t^l)$, and all equivalences between extensions are of this form.

We now wish to understand extensions of rank-one modules in the category of Breuil modules with descent data. The underlying Breuil module extension must be of the above form, and generic fibre descent data must act via

$$[g](\mathbf{e}) = \left(\frac{g\pi}{\pi}\right)^{k_1} \mathbf{e}, \quad [g](\mathbf{e}') = \left(\frac{g\pi}{\pi}\right)^{k_2} \mathbf{e}' + A_g \mathbf{e},$$

where for ease of notation we have set

$$k_1 = e'd - Uls', \quad k_2 = e'c - Ulr'.$$

One checks that the relation $[h][g]\mathbf{e}' = [hg]\mathbf{e}'$ is equivalent to

$$\frac{A_{hg}}{(hg\pi/\pi)^{k_2}} = \frac{A_h}{(h\pi/\pi)^{k_2}} + \left(\frac{h\pi}{\pi}\right)^{k_1 - k_2} {}^h\!\left(\frac{A_g}{(g\pi/\pi)^{k_2}}\right)$$

and so the map $g \mapsto A_g/(g\pi/\pi)^{k_2}$ is a cocycle in $H^1(G, \mathbf{k}[u]/u^{e_K l})$ where $h \in G$ acts on $\mathbf{k}[u]/u^{e_K l}$ via $hf = (h\pi/\pi)^{k_1-k_2}({}^h f)$. (The notation ${}^h f$ will always be reserved for the action defined in Lemma 4.1.) By the same method of proof as in Lemma 4.1, this cohomology group vanishes, and so this map is in fact a coboundary.

Now putting $\tilde{\mathbf{e}}' = \mathbf{e}' + (b/a)t^l\mathbf{e}$, one computes

$$\begin{aligned}[g]\tilde{\mathbf{e}}' &= \left(\frac{g\pi}{\pi}\right)^{k_2} \tilde{\mathbf{e}}' + \left(A_g + \left(\frac{g\pi}{\pi}\right)^{k_1} {}^g\!\left(\frac{b}{a}t^l\right) - \left(\frac{g\pi}{\pi}\right)^{k_2} \frac{b}{a}t^l\right)\mathbf{e} \\ &= \left(\frac{g\pi}{\pi}\right)^{k_2} \tilde{\mathbf{e}}' + \left(A_g + \left(\frac{g\pi}{\pi}\right)^{k_2} \left(g \cdot \left(\frac{b}{a}t^l\right) - \frac{b}{a}t^l\right)\right)\mathbf{e}\end{aligned}$$

and so this alters $A_g/(g\pi/\pi)^{k_2}$ by the coboundary of $(b/a)t^l$. Since $A_g/(g\pi/\pi)^{k_2}$ is already a coboundary, to see that in this fashion the A_g may be transformed to 0 by an appropriate choice of t it suffices to show that all non-zero terms of A_g have degree divisible by l.

To this end, we apply the relation $\phi_1[g] = [g]\phi_1$ to the element $u^r\mathbf{e}' + h\mathbf{e} \in \mathcal{M}_1$. One computes that

$$\phi_1[g](u^r\mathbf{e}' + h\mathbf{e}) = \left(\frac{g\pi}{\pi}\right)^{(k_2+r)l} a\mathbf{e}' + \left(\frac{\Delta}{u^s}\right)^l b\mathbf{e},$$

where

$$\Delta = \left(\frac{g\pi}{\pi}\right)^r u^r A_g + {}^g h \left(\frac{g\pi}{\pi}\right)^{k_1} - h\left(\frac{g\pi}{\pi}\right)^{k_2+r}$$

must have lowest term of degree at least s, while

$$[g]\phi_1(u^r\mathbf{e}' + h\mathbf{e}) = \left(\frac{g\pi}{\pi}\right)^{k_2} a\mathbf{e}' + A_g a\mathbf{e}.$$

That the $\mathbf{e}'$-terms are equal follows from the fact that $e \mid (l-1)k_2 + lr$, while the equality between the $\mathbf{e}$-terms shows that A_g is indeed an lth power.

We can suppose, then, that all $A_g = 0$. Since now $(\Delta/u^s)^l$ must be 0, it follows that a necessary and sufficient condition on $h \in u^{\max(0, r+s-e_K)}\mathbf{k}[u]/u^{e_K l}$ for this extension of Breuil modules to admit that the generic fibre descent data is

$$u^{s+e_K} \mid \Delta = {}^g h \left(\frac{g\pi}{\pi}\right)^{k_1} - h\left(\frac{g\pi}{\pi}\right)^{k_2+r}$$

for all $g \in G$. Moreover, two such extensions with descent data with parameters h, h' are equivalent precisely when h' is of the form $h + u^s t - (b/a)u^r t^l$ for some t such that $g((b/a)t^l) = (b/a)t^l$ for all $g \in G$. That is, we have the following necessary and sufficient conditions:

- all monomial terms of h with degree $k < s + e_K$ must have $k \equiv r + k_2 - k_1 \pmod{e}$ and coefficient in $\mathbf{l}$;
- all terms of degree $k < e_K$ of an allowable change-of-variables t must have $k \equiv l^{-1}(k_2 - k_1)$ and coefficient in $\mathbf{l}$.

Before continuing, given $H \in \mathbf{k}[u]/u^{e_K l}$ we describe an inductive procedure to solve the equation $H = u^s T - (b/a)u^r T^l$. Let $H = \sum_i H_i u^i$ and $T = \sum_i T_i u^i$, so that the equation we wish to solve amounts to the system of equations

$$H_i = T_{i-s} - \frac{b}{a} T^l_{(i-r)/l} \tag{7.2}$$

for $0 \leqslant i < le_K$, and where T_j is required to be 0 if j is not a non-negative integer. Set $i_0 = (ls - r)/(l-1)$. We will attempt to solve Equations (7.2) inductively, inducting on the distance of i from i_0. The condition $|i - i_0| < 1/(l-1)$ is an empty condition unless $i = i_0$ is a non-negative integer, in which case the associated equation is

$$H_{(s-r)/(l-1)} = T_{(s-r)/(l-1)} - \frac{b}{a} T^l_{(s-r)/(l-1)}.$$

If this equation can be solved for $T_{(s-r)/(l-1)}$, this is our base case, and then assume the following inductive hypothesis:

- Equations (7.2) can be solved for all i such that $|i - i_0| < N + 1/(l-1)$;
- in doing so, all and only the T_j with $|j - (s-r)/(l-1)| < N + 1/(l-1)$ have been determined.

Now suppose that i satisfies $N + 1/(l-1) \leqslant |i - i_0| < N + (1/(l-1))$. Then $N + 1/(l-1) \leqslant |(i-s) - ((s-r)/(l-1))| < N + (l/(l-1))$ and so by assumption T_{i-s} has not been determined. Alternatively, $|((i-r)/l) - ((s-r)/(l-1))| < (N/l) + (1/(l-1)) \leqslant N + (1/(l-1))$, and so $T_{(i-r)/l}$ *has* been determined. So we may recursively take $T_{i-s} = H_i + (b/a)T_{(i-r)/l}$. This is only a condition if $i < s$, in which case there is a solution only if the T_{i-s} so-obtained is 0. By induction, we conclude that system (7.2) has a solution if and only if:

https://doi.org/10.1112/S0010437X03000289 Published online by Cambridge University Press

- the base case $H_{(ls-r)/(l-1)} = T_{(s-r)/(l-1)} - (b/a)T^l_{(s-r)/(l-1)}$ is either vacuous or is non-vacuous and has a solution;
- in our recursive process, $T_{i-s} = H_i + (b/a)T^l_{(i-r)/l} = 0$ for whenever $i < s$.

Note that the base case may be unsolvable only if $(s-r)/(l-1)$ is a negative integer and $H_{(ls-r)/(l-1)} \neq 0$; or if $(a/b) \in (\mathbf{k}^\times)^{l-1}$ so that the map $\alpha \mapsto \alpha - (b/a)\alpha^l$ is not surjective. In the latter case, fix any η not in the image of the map $\alpha \mapsto \alpha - (b/a)\alpha^l$.

As an example of the usefulness of this description, we can employ it show the following proposition:

Proposition 7.3. *Suppose $H = u^sT - (b/a)u^rT^l$ has a solution and $\deg H < s$. Then $H = 0$.*

Proof. If the base case is not vacuous, then either $(ls-r)/(l-1) \geqslant s$ and so $H_{(ls-r)/(l-1)} = 0$ by assumption, or else $r > s$ and the assumption that the equation can be solved forces $H_{(ls-r)/(l-1)} = 0$; in any case the base case may be solved by taking $T_{(s-r)/(l-1)} = 0$. We claim that in our inductive procedure, all T_i will be determined to be 0: indeed, if $i \geqslant s$, then $T_{i-s} = H_i + (b/a)T^l_{(1-r)/l} = 0$ by induction, while if $i < s$ then perforce $T_{i-s} = 0$. Thus if the system of Equations (7.2) can be solved, then $T = 0$ is a solution, and so $H = 0$. □

In a similar vein, we can show the following.

Proposition 7.4. *Let H be as before.*

i) *If the base case for H is vacuous, can be solved, or cannot be solved but if $r > s$ then there exists a unique H' such that $H' = u^sT - (b/a)u^rT^l$ can be solved and such that $\deg(H - H') < s$.*
ii) *If the base case cannot be solved and $s \geqslant r$, then there exists a unique H' such that the only non-zero term of $H - H'$ of degree at least s is of the form $N\eta u^{(ls-r)/(l-1)}$ for $N \in \mathbb{F}_l$.*

Proof. For item i, uniqueness is evident by Proposition 7.3. Existence when the base case is vacuous or can be solved follows from the inductive procedure for H, simply defining $H'_i = -(b/a)T^l_{(i-r)/l}$ whenever $i < s$. If $r > s$ and the base case cannot be solved, first set $H'_{(ls-r)/(l-1)} = 0$, and proceed as before. For item ii, if $s > r$ and the base case cannot be solved, then since the $N\eta$ are coset representatives for $\{\alpha - (b/a)\alpha^l\}$ in $\mathbf{k}$ there is a unique $H'_{(ls-r)/(l-1)} \in \{\alpha - (b/a)\alpha^l\}$ such that $H_{(ls-r)/(l-1)} - H'_{(ls-r)/(l-1)} = N\eta$ for some n, and then we proceed to construct H' via the inductive procedure as in item i. □

Finally we return to the situation under consideration, namely that all monomial terms of h with degree $k < s + e_K$ must have $k \equiv r + k_2 - k_1 \pmod{e}$ and coefficient in $\mathbf{l}$. Notice that if $i - s < e_K$, then $i < s + e_K$ and $(i-r)/l < e_K$. Moreover, since $k_2 - k_1 \equiv s - r + l^{-1}(k_2 - k_1) \pmod{e}$, we find that $i - s \equiv l^{-1}(k_2 - k_1) \pmod{e}$ if and only if $(i-r)/l \equiv l^{-1}(k_2 - k_1) \pmod{e}$ if and only if $i \equiv k_2 - k_1 + r \pmod{e}$.

We use our procedure to attempt to solve the equation $h = u^st - (b/a)u^rt^l$. Suppose first that the base case is vacuous, or cannot be solved but $r > s$. Using the above observations, and by induction, the coefficient t_{i-s} for $i - s < e_K$ can become non-zero only if $i \equiv s + l^{-1}(k_2 - k_1) \pmod{e}$; and in that case induction and the formula for t_{i-s} in terms of H_i and $t_{(i-r)/l}$ shows that $t_{i-s} \in \mathbf{l}$. It follows from the method of item i of Proposition 7.4 that when we construct h' and t such that $h' = u^st - (b/a)u^rt^l$ and $\deg(h - h') < s$, the resulting t satisfies our condition that every non-zero term of degree k smaller than e_K has $k \equiv l^{-1}(k_2 - k_1)$ and coefficient in $\mathbf{l}$. Moreover, also by construction, the terms of h' of degree less than $s + e_K$ have coefficients in $\mathbf{l}$, and so all the coefficients of $h - h'$ lie in $\mathbf{l}$.

Next, consider the situation where $s \geqslant r$, and the base case is non-vacuous, so $s \equiv r \pmod{l-1}$. If $(ls-r)/(l-1) \not\equiv r + k_2 - k_1 \pmod{e}$, then $h_{(ls-r)/(l-1)} = 0$ and so taking $t_{(s-r)/(l-1)} = 0$ the conclusions of the previous paragraph hold. Suppose, then, that $(ls-r)/(l-1) \equiv r+k_2-k_1 \pmod{e}$, or in other words that $(s-r)/(l-1) \equiv l^{-1}(k_2-k_1) \pmod{e}$. It is not difficult to see that this congruence is equivalent to $c-d \equiv V((r-s)/(l-1)) \pmod{(l-1,e)}$. If a/b is not an $(l-1)$st power in $\mathbf{l}^\times$, then the base case can solved with $t_{(s-r)/(l-1)} \in \mathbf{l}$, and again the conclusions of the previous paragraph hold. (Note that the congruence $(s-r)/(l-1) \equiv l^{-1}(k_2-k_1) \pmod{e}$ ensures that the possibly non-zero coefficient $t_{(s-r)/(l-1)}$ lies in suitable degree.)

We are finally left with the case when $s \geqslant r$, $s \equiv r \pmod{l-1}$, a/b is an $(l-1)$st power in $\mathbf{l}^\times$, and $c-d \equiv V((r-s)/(l-1)) \pmod{(l-1,e)}$. Note that this is exactly the case when there is a non-trivial map $\mathcal{M}_U(r,a,c) \to \mathcal{M}_U(s,b,d)$. Let η be any fixed element of $\mathbf{l}$ not in the image of $\alpha \mapsto \alpha-(b/a)\alpha^l$. Following the method of item ii of Proposition 7.4 and using the same arguments as in the previous paragraphs, we construct t such that the non-zero terms of t of degree $k<e_K$ have $k \equiv l^{-1}(k_2-k_1)$ and coefficient in $\mathbf{l}$, and such that $h-(u^s t-(b/a)t^l)$ has coefficients in $\mathbf{l}$ and all terms of degree less than s, save possibly for a term of the form $N\eta u^{(ls-r)/(l-1)}$. Putting this all together, we obtain the following theorem.

Theorem 7.5. *Put $k_1 = e'd - Uls'$ and $k_2 = e'c - Ulr'$.*

i) *Suppose that there is no map $\mathcal{M}_U(r,a,c) \to \mathcal{M}_U(s,b,d)$. Then every extension of $\mathcal{M}_U(r,a,c)$ by $\mathcal{M}_U(s,b,d)$ with descent data is isomorphic to exactly one of the form*

$$\mathcal{M} = \langle \mathbf{e}, \mathbf{e}' \rangle, \quad \mathcal{M}_1 = \langle u^s\mathbf{e}, u^r\mathbf{e}' + h\mathbf{e} \rangle,$$
$$\phi_1(u^s\mathbf{e}) = b\mathbf{e}, \quad \phi_1(u^r\mathbf{e}' + h\mathbf{e}) = a\mathbf{e}',$$
$$[g](\mathbf{e}) = \left(\frac{g\pi}{\pi}\right)^{k_1}\mathbf{e}, \quad [g](\mathbf{e}') = \left(\frac{g\pi}{\pi}\right)^{k_2}\mathbf{e}',$$

where $h \in u^{\max(0,r+s-e_K)}\mathbf{l}[u]/u^{e_K l}$ has degree less than s and all non-zero terms of degree congruent to $r+k_2-k_1 \pmod{e}$. In particular, the $\mathbb{F}_l$-dimension of this space of extensions is at most $[L:\mathbb{Q}_l]$.

ii) *If there is a map $\mathcal{M}_U(r,a,c) \to \mathcal{M}_U(s,b,d)$, let η be any fixed element of $\mathbf{l}$ not in the image of $\alpha \mapsto \alpha-(b/a)\alpha^l$ on $\mathbf{l}$. Then the same conclusion holds as in item i, except that h may also have a term of the form $N\eta u^{(ls-r)/(l-1)}$ for $N \in \mathbb{F}_l$. In particular, the $\mathbb{F}_l$-dimension of this space of extensions is at most $[L:\mathbb{Q}_l]+1$.*

To see the dimension claims, note in item i that at most $e_K/e = e_L$ different terms in h can be non-zero. Since each coefficient lies in $\mathbf{l}$, the dimension over $\mathbb{F}_l$ is at most $e_L f_L = [L:\mathbb{Q}_l]$. The claim in item ii follows identically.

We remark that this result is intuitive: the number of extensions grows as s gets larger and r gets smaller, in other words as the group scheme corresponding to $\mathcal{M}_U(s,b,d)$ gets 'more étale' and that corresponding to $\mathcal{M}_U(r,a,c)$ gets 'more multiplicative'. This is sensible as there are plenty of extensions of étale group schemes by multiplicative ones, and none in the other direction.

7.1 Start of the proof of Theorem 2.10

We return once again to the case where K/L is the extension $H'/\mathbb{Q}_l$. Since we are only interested in two-dimensional residual representations of $G_{\mathbb{Q}_l}$ with a trivial centralizer, we are safely in the situation where there is no map $\mathcal{M}(r,a,c) \to \mathcal{M}(s,b,d)$, for otherwise the two diagonal characters would be equal; that is, since $V=0$, we are assuming $(a,c) \neq (b,d)$. In this case, item i of Theorem 7.5 tells us that the space of extensions with descent data of $\mathcal{M}(r,a,c)$ by $\mathcal{M}(s,b,d)$ is at most one-dimensional, and in fact non-split extensions exist exactly whenever there is a solution to the congruence

$$n \equiv (l+1)(c-d) + ls' - r'$$

https://doi.org/10.1112/S0010437X03000289 Published online by Cambridge University Press

with

$$\max(0, r+s-(l^2-1)) \leqslant n < s.$$

Then write $h = h_n u^n$, and denote the resulting extension $\mathcal{M}(r,a,c;s,b,d;n,h_n)$.

Since we have assumed that $\overline{\rho}$ has a trivial centralizer, we may henceforth restrict ourselves to the non-split situation above; in particular $s \neq 0$ and $r \neq l^2-1$, so that an n satisfying the given inequality and congruence can exist. Moreover, we will always take $h_n = 1$: if $h_n \neq 1$, the resulting group scheme with descent data is isomorphic to the group scheme with descent data having identical parameters save $h_n = 1$ – they are simply non-isomorphic as extension classes, which will be of no concern. Therefore, we will need to consider only Breuil modules with descent data of the form $\mathcal{M}(r,a,c;s,b,d;n,1)$.

We now turn to the question of which of the group schemes with descent data corresponding to these Breuil modules with descent data satisfy relations (2.3)–(2.5) on their Dieudonné modules: namely, that $[\zeta]+[\zeta]^l$ acts as $\zeta^{-m}+\zeta^{-lm}$, that $[\zeta]^{l+1}$ acts as $\zeta^{-(l+1)m}$, and that $F+TV = F+abV$ acts as 0. It is easy to see, using the compatibility between Dieudonné theory and Breuil theory as described in § 3, that the Dieudonné module of the closed fibre of $\mathcal{M}(r,a,c;s,b,d;n,1)$ has a basis $\mathbf{v}, \mathbf{w}$ on which $[\zeta]$ acts in the following manner:

$$[\zeta](\mathbf{v}) = \zeta^{(l+1)c-lr'}\mathbf{v} \quad \text{and} \quad [\zeta](\mathbf{w}) = \zeta^{(l+1)d-ls'}\mathbf{w},$$

and so

$$[\zeta]^l(\mathbf{v}) = \zeta^{(l+1)c-r'}\mathbf{v} \quad \text{and} \quad [\zeta]^l(\mathbf{w}) = \zeta^{(l+1)d-s'}\mathbf{w}.$$

It follows that if $[\zeta]$ satisfies the desired relations, then either

$$\zeta^{(l+1)c-lr'} = \zeta^{-m} \quad \text{and} \quad \zeta^{(l+1)c-r'} = \zeta^{-lm}$$

or

$$\zeta^{(l+1)c-lr'} = \zeta^{-lm} \quad \text{and} \quad \zeta^{(l+1)c-r'} = \zeta^{-m},$$

and a similar relationship holds between d, s', and m. Recalling that $m = i+(l+1)j$, the first possibility yields the congruences

$$(l+1)c - lr' \equiv -m \pmod{l^2-1} \quad \text{and} \quad (l+1)c - r' \equiv -lm \pmod{l^2-1}.$$

Solving for r' we obtain $r' \equiv -i \pmod{l+1}$. Since $1 \leqslant i \leqslant l$ and $0 \leqslant r' \leqslant l+1$, we conclude that $r' = l+1-i$. This allows us to solve $c \equiv 1-i-j \pmod{l-1}$ (which completely determines c since it is an element of $\mathbb{Z}/(l-1)\mathbb{Z}$). Applying a similar analysis to the second of the possible sets of relations among c, r', and m, we find that between the two cases

$$(r',c) = (i,-j) \quad \text{or} \quad (l+1-i, 1-i-j).$$

By an identical calculation

$$(s',d) = (i,-j) \quad \text{or} \quad (l+1-i, 1-i-j).$$

However, if $r' = s'$ and $c = d$, we would require

$$n \equiv (l+1)(c-d) + ls' - r' \equiv (l-1)s' = s \pmod{l^2-1}.$$

Since we require $0 \leqslant n < s$ and since $s < l^2-1$ (as $i \neq l+1$), this situation is impossible. We have therefore proved that the only possibilities for Breuil modules with descent data attached to integral models with descent data for $\overline{\rho}$ which satisfy our Dieudonné module relations are those of the form

$$\mathcal{M}((l-1)(l+1-i), a, 1-i-j; (l-1)i, b, -j; 0, 1)$$

and

$$\mathcal{M}((l-1)i, a, -j; (l-1)(l+1-i), b, 1-i-j; 0, 1).$$

https://doi.org/10.1112/S0010437X03000289 Published online by Cambridge University Press

By Theorem 6.3 (and recalling the contravariance of the Breuil module functor) the descended $G_{\mathbb{Q}_l}$-representations $\overline{\rho}$ corresponding to these Breuil modules with descent data are exactly of the form $\overline{\rho} = \left(\begin{smallmatrix} \omega^{i+j}\chi_a & * \\ 0 & \omega^{1+j}\chi_b \end{smallmatrix}\right)$ and $\overline{\rho} = \left(\begin{smallmatrix} \omega^{1+j}\chi_a & * \\ 0 & \omega^{i+j}\chi_b \end{smallmatrix}\right)$. Note that unless $i = 1$ or $i = l$, each different possibility for $\overline{\rho}$ yields at most one Breuil module with descent data in our list. When $i = 1$ and $i = l$, it is still possible that $\mathcal{M}(l(l-1), a, -j; (l-1), b, -j; 0, 1)$ and $\mathcal{M}((l-1), a, -j; l(l-1), b, -j; 0, 1)$ are both integral models with descent data for the same $\overline{\rho}$; however, we will see in § 8 that the former arises from a residual representation of $G_{\mathbb{Q}_l}$ which is either split or non-split but has non-trivial centralizer, and since we have assumed that $\overline{\rho}$ has trivial centralizer this group scheme with descent data cannot arise from our $\overline{\rho}$. Therefore it is again the case that our $\overline{\rho}$ gives rise to at most one integral model with descent data. We will also prove in § 8 that if $\overline{\rho} = \left(\begin{smallmatrix} \omega^{i+j}\chi_a & * \\ 0 & \omega^{1+j}\chi_b \end{smallmatrix}\right)$ gives rise to one of the integral models with descent data in the above list and if $i = 2$, then $*$ is peu ramifié. Similarly if $\overline{\rho} = \left(\begin{smallmatrix} \omega^{1+j}\chi_a & * \\ 0 & \omega^{i+j}\chi_b \end{smallmatrix}\right)$ and if $i = l-1$, then $*$ is peu ramifié. Once done, all of these results together will have completed the proof of the following proposition.

Proposition 7.6. *If $\tau = \tilde{\omega}_2^m \oplus \tilde{\omega}_2^{lm}$ and $\overline{\rho} : G_{\mathbb{Q}_l} \to \mathrm{GL}_2(\mathbb{F}_l)$ has centralizer $\mathbb{F}_l$ and is reducible, and if $R(\overline{\rho}, 2, \tau) \neq 0$, then $\overline{\rho}|_{I_l}$ does indeed have one of the forms specified in Theorem 1.1. Furthermore $\overline{\rho}$ gives rise to exactly one finite flat group scheme over $\mathcal{O}_{H'}$ with descent data for $\mathbb{Q}_l$ satisfying the necessary relations on the Dieudonné module of its closed fibre.*

Remark 7.7. The relationship $F + TV = F + abV = 0$ is indeed satisfied on the Dieudonné modules of the closed fibres of the above group schemes. One may check that on our basis $\mathbf{v}$,$\mathbf{w}$, F and V act via the matrices

$$\begin{pmatrix} -b & 0 \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1/a & 0 \\ 0 & 0 \end{pmatrix},$$

respectively.

8. Maps between rank-two Breuil modules with descent data

8.1 Generalities

Our strategy for proving that certain pairs of rank-two Breuil modules with descent data arise from the same representation is to find maps between these rank-two modules.

Definition 8.1. Let $\mathcal{M}$ be the Breuil module corresponding to a group scheme $\mathcal{G}$ over $\mathcal{O}_K$. Then, by Raynaud [Ray74], $\mathcal{G}$ is mapped to by a maximal integral model $\mathcal{G}_+$ and maps to a minimal integral module $\mathcal{G}_-$. The maximal and minimal Breuil module of $\mathcal{M}$ are defined to be, respectively, the Breuil modules corresponding to $\mathcal{G}_+$ and $\mathcal{G}_-$.

By Lemma 4.1.4 of [BCDT01], if two extensions with descent data of rank-one Breuil modules for $\mathcal{O}_K$ with descent data from K to L arise from the same representation of G_L, they both map to a maximal Breuil module with descent data for this representation, and are also mapped to by a minimal Breuil module with descent data, where the maps are generic fibre isomorphisms. A scheme-theoretic closure argument as in Lemma 4.1.3 of [BCDT01] shows that in this situation, the maximal and minimal Breuil module with descent data are again extensions of rank-one Breuil modules with descent data.

As an initial example, note that as a corollary of Lemma 6.1 and Theorem 6.3, if $\chi_U(r, a, c) = \chi_U(r', a', c')$ then there is a non-zero map either from $\mathcal{M}_U(r, a, c)$ to $\mathcal{M}_U(r', a', c')$ or *vice versa*, depending on whether $r \leqslant r'$ or $r' \leqslant r$. For instance, when $l - 1 \mid e$, so that $U = 1$ and $V = 0$, this implies that the maximal and minimal Breuil modules with descent data of $\mathcal{M}(r, a, c)$ are $\mathcal{M}(e_K, a, c)$ and $\mathcal{M}(0, a, c)$, respectively. It follows easily that if $\mathcal{M}$ is an extension with descent data

https://doi.org/10.1112/S0010437X03000289 Published online by Cambridge University Press

of $\mathcal{M}(r,a,c)$ by $\mathcal{M}(s,b,d)$, where $\chi(r,a,c) \neq \chi(s,b,d)$, then the descended G_L-representation of $\mathcal{M}$ is split if and only if there is a non-zero map $\mathcal{M}(0,a,c) \to \mathcal{M}$, and that in this case the maximal and minimal Breuil modules with descent data are $\mathcal{M}(e_K,a,c) \oplus \mathcal{M}(e_K,b,d)$ and $\mathcal{M}(0,a,c) \oplus \mathcal{M}(0,b,d)$, respectively. In a similar vein we have the following proposition.

Proposition 8.2. *Suppose that we have a diagram*

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{G}_1' \arrow[r] & \mathcal{G}_1 \arrow[r] \arrow[d] & \mathcal{G}_1'' \arrow[r] & 0 \\
0 \arrow[r] & \mathcal{G}_2' \arrow[r] & \mathcal{G}_2 \arrow[r] & \mathcal{G}_2'' \arrow[r] & 0
\end{tikzcd}$$

where for $i = 1, 2$, $\mathcal{G}_i'$ and $\mathcal{G}_i''$ are finite flat group schemes over $\mathcal{O}_K$ of order l with descent data from K to L whose generic fibres descend to non-isomorphic irreducible G_L-representations, and where $\mathcal{G}_i$ is an extension with compatible generic fibre descent data. Suppose furthermore that the map $\mathcal{G}_1 \to \mathcal{G}_2$ induces a generic fibre isomorphism of group schemes with descent data, and that the descended generic fibre representation of G_L is not semisimple. Then there are maps $\mathcal{G}_1' \to \mathcal{G}_2'$ and $\mathcal{G}_1'' \to \mathcal{G}_2''$ which are isomorphisms on the generic fibre.

Proof. By the semisimplicity assumption, the irreducible G_L-representations corresponding to $\mathcal{G}_1'$ and $\mathcal{G}_2''$ are different. Therefore the composite map

$$\mathcal{G}_1' \to \mathcal{G}_1 \to \mathcal{G}_2 \to \mathcal{G}_2''$$

is the zero map and so factors through $\mathcal{G}_2'$. Let $\check{\mathcal{G}}$ denote the Cartier dual of $\mathcal{G}$. Dualizing our diagram, we obtain a non-zero map $\check{\mathcal{G}}_2'' \to \check{\mathcal{G}}_1''$, and dualizing again gives a non-zero map $\mathcal{G}_1'' \to \mathcal{G}_2''$. □

Finally, we will need to make use of the following result.

Proposition 8.3. *Let $\mathcal{G} \to \mathcal{G}'$ be a map of finite flat group schemes over $\mathcal{O}_K$ of equal order, both killed by l. If the kernel of the corresponding map $\mathcal{M}' \to \mathcal{M}$ of Breuil modules does not contain a free $\mathbf{k}[u]/u^{el}$-submodule, then $\mathcal{G} \to \mathcal{G}'$ is an isomorphism on generic fibres.*

Proof. Assume $f : \mathcal{G} \to \mathcal{G}'$ does not induce an isomorphism on generic fibres. Then the image of $f_{/K}$ in $G'_{/K}$ is not all of $G'_{/K}$, and taking the scheme-theoretic closure of this image yields an exact sequence of group schemes

$$0 \longrightarrow \mathcal{H} \longrightarrow \mathcal{G}' \xrightarrow{g} \mathcal{H}' \longrightarrow 0$$

with $\mathcal{H}' \neq 0$ and $g \circ f = 0$. If $\mathcal{N}'$ is the Breuil module corresponding to $\mathcal{H}'$, then $\mathcal{N}' \hookrightarrow \ker(\mathcal{M}' \to \mathcal{M})$, since short-exact sequences of group schemes yield short-exact sequences of Breuil modules. □

Note that, if the map $\mathcal{G} \to \mathcal{G}'$ in Proposition 8.3 is in fact a map of group schemes with descent data, then the isomorphism in the conclusion is also an isomorphism of group schemes with descent data.

8.2 Application to the proof of Proposition 7.6

Return once again to the situation where the extension K/L is $H'/\mathbb{Q}_l$, and suppose henceforth that $(a,c) \neq (b,d)$, so that our representations have different diagonal characters. We begin with the following proposition.

Proposition 8.4. *When $(a,c) \neq (b,d)$, the descended representation of*

$$\mathcal{M}(r,a,c;s,b,d;n,1)$$

is split if and only if $r > s$ and $c = d$.

https://doi.org/10.1112/S0010437X03000289 Published online by Cambridge University Press

Proof. By the discussion in § 8.1, we must determine when there exists a non-zero map

$$\Psi : \mathcal{M}(0,a,c) \to \mathcal{M}(r,a,c;s,b,d;n,1).$$

Let $\mathbf{f}$ denote the standard basis vector of $\mathcal{M}(0,a,c)$. Assume that Ψ exists. Then $\Psi(\mathbf{f}) = V\mathbf{e}+W\mathbf{e}'$, and since $(a,c) \neq (b,d)$ it follows that $W \neq 0$.

From the fact that Ψ commutes with generic fibre descent data, it follows that all non-zero terms of V are in degrees congruent to $(l+1)(c-d)+ls' \pmod{l^2-1}$ and have coefficients in $\mathbb{F}_l$; and that all non-zero terms of W are in degrees congruent to $lr' \pmod{l^2-1}$ with coefficient in $\mathbb{F}_l$. From the fact that Ψ commutes with ϕ_1, it follows that all non-zero terms of V and W are in degrees divisible by l. By the Chinese remainder theorem, $V = vu^{\alpha}$ and $W = wu^{\beta}$ are monomials with $v,w \in \mathbb{F}_l$, and from the given conditions it follows with one exception that $\alpha = l((l+1)\{c-d\}+s')$ and $\beta = lr'$, where for $x \in \mathbb{Z}/(l-1)\mathbb{Z}$, $\{x\}$ is the unique representative of x lying between 0 and $l-2$. The exception is that $\alpha = 0$ when $s' = l+1$ and $\{c-d\} = l-2$, as in this case $l((l+1)\{c-d\}+s') = l(l^2-1)$.

Since $V\mathbf{e}+W\mathbf{e}' \in \mathcal{M}_1(r,a,c;s,b,d;n,1)$, it follows that

$$\beta \geqslant r, \quad \alpha \geqslant s, \quad \beta - r + n \geqslant s, \tag{8.5}$$

and

$$V\mathbf{e}+W\mathbf{e}' = (vu^{\alpha-s} - wu^{\beta-r+n-s})u^s\mathbf{e} + wu^{\beta-r}(u^r\mathbf{e}'+u^n\mathbf{e}).$$

Note that the inequalities (8.5) rule out the possibility $s' = l+1$ and $\alpha = 0$, and so we indeed have $\alpha = l((l+1)\{c-d\}+s')$. The condition that Ψ commutes with ϕ_1 is then equivalent to

$$bvu^{l(\alpha-s)} - bwu^{l(\beta-r+n-s)} = avu^{\alpha}.$$

Now $\beta - r + n - s = r' + n - s < r'$, so $l(\beta-r+n-s) < l(l^2-1)$ and the term $bwu^{l(\beta-r+n-s)}$ is non-zero. It follows that v is non-zero, and since a sum of three monomials can equal zero only if each non-zero term in the sum has the same degree, we see that $\alpha = l(\beta-r+n-s)$. This yields $n = (l+1)\{c-d\}+ls'-r'$, and since $n < s$ this forces $c = d$ and $r' > s'$.

Finally, under the assumptions $c = d$ and $r' > s'$, one can check that

$$\mathbf{f} \mapsto vu^{ls'}\mathbf{e} + \left(1-\frac{a}{b}\right)vu^{lr'}\mathbf{e}'$$

is a map of the desired sort, and so these conditions are sufficient as well as necessary. □

Note that, as claimed in § 7.1, this shows that descended $G_{\mathbb{Q}_l}$-representation corresponding to the Breuil module $\mathcal{M}(l(l-1),a,-j;(l-1),b,-j;0,1)$ is split.

Observe that the preceeding proposition may be reinterpreted as follows. The quantity $(l+1)\{c-d\}+ls'-r'$ lies between 0 and $2(l^2-1)$, and so $n = (l+1)\{c-d\}+ls'-r'-N(l^2-1)$ for some $N \in \{0,1,2\}$. The equality $n = (l+1)\{c-d\}+ls'-r'$ occurs precisely when $\{c-d\} = 0$ and $r > s$, and this is exactly the case when the descended $G_{\mathbb{Q}_l}$-representation is split. Note that $(l+1)\{c-d\}+ls'-r' = 2(l^2-1)$ only when $\{c-d\} = l-2$, $s = l^2-1$, and $r = 0$, and the rest of the time we must have $n = (l+1)\{c-d\}+ls'-r'-(l^2-1)$. We can now prove the following proposition.

Proposition 8.6. *Suppose that*

$$\mathcal{M}(r,a,c;s,b,d;n,1) \quad \text{and} \quad \mathcal{M}(r_1,a_1,c_1;s_1,b_1,d_1;n_1,1)$$

have non-split descended $G_{\mathbb{Q}_l}$-representation. Then there is a map

$$\mathcal{M}(r,a,c;s,b,d;n,1) \to \mathcal{M}(r_1,a_1,c_1;s_1,b_1,d_1;n_1,1)$$

which is an isomorphism on generic fibres if and only if $(a,c) = (a_1,c_1)$, $(b,d) = (b_1,d_1)$, $r \leqslant r_1$, and $s \leqslant s_1$.

https://doi.org/10.1112/S0010437X03000289 Published online by Cambridge University Press

Proof. The conditions in the proposition are necessary by Proposition 8.2 and Lemma 6.1. To see that the conditions are sufficient, we will exhibit the desired maps

$$\mathcal{M}(r, a, c; s, b, d; n, 1) \to \mathcal{M}(r_1, a, c; s_1, b, d; n_1, 1)$$

whenever $r \leqslant r_1$ and $s \leqslant s_1$. Let $\mathbf{e}, \mathbf{e}'$ and $\mathbf{f}, \mathbf{f}'$ denote our standard bases for the left-hand and right-hand Breuil modules with descent data above, respectively. Most of the time, we have

$$n - (ls' - r') = n_1 - (ls'_1 - r'_1) = (l+1)\{c-d\} - (l^2 - 1)$$

and in these cases one can check that the maps given by

$$\begin{aligned} \mathbf{e} &\mapsto vu^{l(s'_1 - s')}\mathbf{f} \\ \mathbf{e}' &\mapsto vu^{l(r'_1 - r')}\mathbf{f}' \end{aligned}$$

are indeed maps of Breuil modules with descent data. The equality $n - (ls' - r') = n_1 - (ls'_1 - r'_1)$ is crucial to the verification that the map preserves the filtration and commutes with ϕ_1. Similarly, we have maps

$$\mathcal{M}(0, a, d-1; s, b, d; ls' - (l+1), 1) \to \mathcal{M}(0, a, d-1; l^2 - 1, b, d; 0, 1)$$

given by

$$\begin{aligned} \mathbf{e} &\mapsto vu^{l(l+1-s')}\mathbf{f} \\ \mathbf{e}' &\mapsto a^{-1}bv\mathbf{f} + a^{-1}bv\mathbf{f}' \end{aligned}$$

and maps

$$\mathcal{M}(0, a, d-1; l^2 - 1, b, d; 0, 1) \to \mathcal{M}(r_1, a, d-1; l^2 - 1, b, d; l^2 - 1 - r'_1, 1)$$

given by

$$\begin{aligned} \mathbf{e} &\mapsto v\mathbf{f} \\ \mathbf{e}' &\mapsto -v\mathbf{f} + b^{-1}avu^{lr'_1}\mathbf{f}'. \end{aligned}$$

This exhibits the desired maps in the remaining cases, when one or the other Breuil modules with descent data has $\{c-d\} = l-2$, $s = l^2 - 1$, and $r = 0$.

To see that these maps all induce isomorphisms on the generic fibre, we note that this follows from the following general criterion. If we have a map of such Breuil modules sending

$$\begin{aligned} \mathbf{e} &\mapsto vu^{\alpha}\mathbf{f} \\ \mathbf{e}' &\mapsto yu^{\beta}\mathbf{f} + zu^{\gamma}\mathbf{f}' \end{aligned}$$

with $v, z \in \mathbb{F}_l^{\times}$, then any element of the kernel of our homomorphism is annihilated by $u^{\max(\gamma, \alpha+\gamma-\beta)}$. If $\alpha + \gamma - \beta < l(l^2 - 1)$, this shows that the kernel does not contain any free $\mathbb{F}_{l^2}[u]/u^{l(l^2-1)}$-submodules, and so by Proposition 8.3 the map induces an isomorphism on generic fibres. □

The analogous result is true for maps between Breuil modules with descent data in which the descended $G_{\mathbb{Q}_l}$-representation is split.

8.3 Lattices of rank-two Breuil modules

Consider the non-split Breuil module with descent data $\mathcal{M} = \mathcal{M}(r, a, c; s, b, d; n, 1)$. Implicit in the existence of this Breuil module with descent data is that n satisfies the inequalities $\max(0, r + s - (l^2 - 1)) \leqslant n < s$ as well as the congruence $n \equiv (l+1)(c-d) + ls' - r' \pmod{l^2 - 1}$. By our earlier comparisons of n and $(l+1)\{c-d\} + ls' - r'$, we see that $n - (ls' - r') = -k(l+1)$ for an integer k between 0 and l. Indeed, if $c = d$ then $k = 0$ or $l - 1$, the former if and only if $r > s$; if $c = d - 1$,

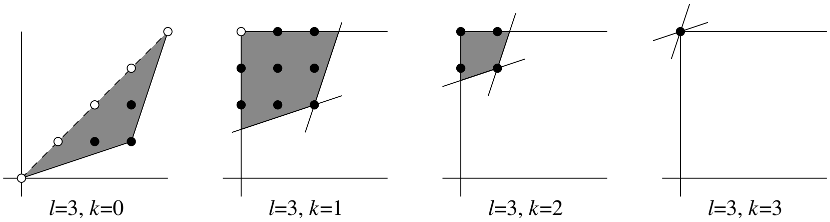

Figure 1. The regions of Proposition 8.7 when $l = 3$.

then $k = 1$ or l, the latter if and only if $s = l^2 - 1$ and $r = 0$; and otherwise k is the unique integer between 2 and $l - 2$ which represents $d - c$. In fact, we can show the following proposition.

Proposition 8.7. *(See Figure 1.) For fixed $k \in \{0, \dots, l\}$, the pairs (r', s') for which $n = (ls' - r') - k(l + 1)$ satisfies the inequalities $\max(0, r + s - (l^2 - 1)) \leqslant n < s$ are precisely the pairs satisfying $0 \leqslant r' \leqslant l - k$ and $k + 1 \leqslant s' \leqslant l + 1$ with the exceptions that for $k = 0$ we require $r' > s'$, and for $k = 1$ the pair $(0, l + 1)$ is excluded.*

Proof. We shall prove that for fixed $k > 0$ the desired pairs (r', s') are the lattice points inside the convex quadrilateral bounded by the inequalities

$$r' \geqslant 0, \quad s' \leqslant l + 1, \quad ls' - r' \geqslant (l + 1)k, \quad s' - lr' + (l^2 - 1) \geqslant (l + 1)k,$$

and, if $k = 1$, the region excludes the extremal point $(0, l + 1)$. For $k = 0$, we shall similarly prove that the pairs (r', s') for which $n = (ls' - r') - k(l + 1)$ are precisely the lattice points inside the triangle bounded by the inequalities

$$r' > s', \quad ls' - r' \geqslant (l + 1)k, \quad s' - lr' + (l^2 - 1) \geqslant (l + 1)k.$$

It is easy to see that the lattice points inside these regions are exactly those described in the statement of the proposition.

At the outset, we know that we must satisfy the following inequalities:

$$0 \leqslant s' \leqslant l + 1, \quad 0 \leqslant r' \leqslant l + 1, \quad 0 \leqslant n < s, \quad r + s - (l^2 - 1) \leqslant n.$$

From $n = (ls' - r') - k(l + 1) < s$ we get $-k(l + 1) < r' - s'$. This is no condition if $k \geqslant 2$, but if $k = 1$ we exclude $(0, l + 1)$ and if $k = 0$ we need $r' > s'$. The condition $n \geqslant 0$ translates into $ls' - r' \geqslant (l + 1)k$, and the condition $n \geqslant r + s - (l^2 - 1)$ translates into $s - lr' + (l^2 - 1) \geqslant (l + 1)k$. Therefore, the conditions in the proposition are necessary. We need to show that they are sufficient.

If $k = 0$, the inequalities $ls' \geqslant r' > s'$ imply $s > 0$, so $r > 0$, while the inequalities $r' + (l^2 - 1) > s' + (l^2 - 1) \geqslant lr'$ imply $r' < l + 1$, so $s' < l + 1$.

If $k > 0$, the inequalities $r' \geqslant 0$ and $ls' - r' \geqslant (l + 1)k > 0$ imply $s > 0$, while the inequalities $s' \leqslant l + 1$ and $s' - lr' + (l^2 - 1) \geqslant (l + 1)k > 0$ imply $r' < l + 1$. □

Corollary 8.8. *For all choices of r, s, and n such that*

$$\mathcal{M}(r, a, d - 1; s, b, d; n, 1)$$

is a Breuil module with descent data whose descended $G_{\mathbb{Q}_l}$-representation is non-split, that representation is peu ramifié.

Proof. This is the $k = 1, l$ case in Proposition 8.7. The above discussion, combined with the maps constructed in Proposition 8.6, show that the module $\mathcal{M}(r, a, d - 1; s, b, d; n, 1)$ has minimal Breuil module with descent data $\mathcal{M}(0, a, d - 1; 2(l - 1), b, d; l - 1, 1)$, and so for fixed a, b, d these

https://doi.org/10.1112/S0010437X03000289 Published online by Cambridge University Press

Breuil modules with descent data all correspond to integral models with descent data having the same descended representation. To see that this representation is peu ramifié, we note (see, e.g., [Edi92, § 8]) that peu ramifié representations of $G_{\mathbb{Q}_l}$ have integral $\mathbb{Z}_l$-models. Therefore, since we have constructed all possible integral models with descent data, at least one of the above Breuil modules with descent data corresponds to an integral model with descent data for a peu ramifié representation. Consequently, they all do. □

This completes the proof of Proposition 7.6. We summarize these results as follows.

Theorem 8.9. *Fix $a, b \in \mathbb{F}_l^\times$ and $c, d \in \mathbb{Z}/(l-1)\mathbb{Z}$, and let ρ be a representation*

$$\begin{pmatrix} \chi_a \omega^{1-c} & * \\ 0 & \chi_b \omega^{1-d} \end{pmatrix}$$

of $G_{\mathbb{Q}_l}$ with $* \neq 0$ and $(a,c) \neq (b,d)$. If $d - c \equiv 1 \pmod{l-1}$, suppose $*$ is peu ramifié. Let k be the integer between 1 and $l-1$ congruent to $d-c \pmod{l-1}$. Then the Breuil modules with descent data corresponding to the integral models with descent data for ρ over $\mathcal{O}_{H'}$ are the Breuil modules with descent data $\mathcal{M}(r,a,c;s,b,d;n,1)$ with $0 \leqslant r' \leqslant l-k$ and $k+1 \leqslant s' \leqslant l+1$. The lattice of these Breuil modules with descent data is a square with $l-k+1$ points on each side, and maps from $\mathcal{M}(r,a,c;s,b,d;n,1)$ to $\mathcal{M}(r',a,c;s',b,d;n',1)$ respecting generic fibre descent data exist whenever $r' \geqslant r$ and $s' \geqslant s$. In particular, there are $(l-k+1)^2$ such integral models with descent data, and the maximal and minimal integral models for this representation correspond to the Breuil modules with descent data

$$\mathcal{M}((l-k)(l-1), a, c; (l+1)(l-1), b, d; l^2 - kl, 1)$$

and

$$\mathcal{M}(0, a, c; (k+1)(l-1), b, d; l-k, 1).$$

If $*$ were très ramifié, then ρ would have no such integral models with descent data.

Proof. Our analysis in § 8.2 shows that the descended $G_{\mathbb{Q}_l}$-representations of these Breuil modules with descent data are indeed non-split. The rest of the claims follow from Propositions 8.6 and 8.7 and Corollary 8.8. □

9. Rank-four calculations

Recall that our list of non-split rank-two Breuil modules with descent data satisfying Dieudonné module conditions (2.3)–(2.5) was

$$\mathcal{M}((l-1)(l+1-i), a, 1-i-j; (l-1)i, b, -j; 0, 1)$$

and

$$\mathcal{M}((l-1)i, a, -j; (l-1)(l+1-i), b, 1-i-j; 0, 1).$$

Notice that the change of variables $i \mapsto l+1-i$ and $j \mapsto i+j-1$ interchanges the two collections of Breuil modules with descent data above, so it suffices to consider the latter; moreover, we need consider only those Breuil modules with descent data whose descended $G_{\mathbb{Q}_l}$-representation is non-split and has trivial centralizer. So, to prove Theorem 2.10 we are reduced to showing, for each

$$\mathcal{M} = \mathcal{M}((l-1)i, a, -j; (l-1)(l+1-i), b, 1-i-j; 0, 1) \tag{9.1}$$

with $i = 1, \dots, l-1$ and $j \in \mathbb{Z}/(l-1)\mathbb{Z}$, and $a \neq b$ if $i = 1$, that the space of extensions of $\mathcal{M}$ by $\mathcal{M}$ with descent data still satisfying the desired Dieudonné module relations is at most one-dimensional. We now begin this computation. For clarity we will continue to write r' for i and s'

https://doi.org/10.1112/S0010437X03000289 Published online by Cambridge University Press

for $l+1-i$, since that is what we are used to. Note that $r'+s'=l+1$, $ls'-r'=(l-i)(l+1)$, and $lr'-s'=(l+1)(i-1)$.

Let $(\mathcal{N},\mathcal{N}_1,\phi_1)$ be an arbitrary extension of $\mathcal{M}$ by $\mathcal{M}$ with descent data. We will let $\mathbf{e},\mathbf{e}'$ denote the standard basis for the submodule $\mathcal{M}$ of $\mathcal{N}$, while $\mathbf{f},\mathbf{f}'$ will denote lifts of the standard basis for the quotient $\mathcal{M}$ of $\mathcal{N}$. Then $\mathcal{N}=\langle\mathbf{e},\mathbf{e}',\mathbf{f},\mathbf{f}'\rangle$, and *a priori* $\mathcal{N}_1$ has the form

$$\mathcal{N}_1=\langle u^s\mathbf{e},u^r\mathbf{e}'+\mathbf{e},u^s\mathbf{f}+A\mathbf{e}+B\mathbf{e}',u^r\mathbf{f}'+\mathbf{f}+C\mathbf{e}+D\mathbf{e}'\rangle.$$

Our study of these $(\mathcal{N},\mathcal{N}_1,\phi_1)$ will proceed in the following steps.

i) Show that we may take $A=B=C=D=0$ in the above form for $\mathcal{N}_1$.

ii) Find the most general change of $\mathbf{f},\mathbf{f}'$ preserving this form for $\mathcal{N}_1$.

iii) Simplify $\phi_1(u^s\mathbf{f})$ as much as possible using these changes of variable.

iv) Simplify $\phi_1(u^s\mathbf{f})$ the rest of the way by studying possible descent data.

v) Repeat for $\phi_1(u^r\mathbf{f}'+\mathbf{f})$.

Step i: we wish to see that $\mathbf{f},\mathbf{f}'$ may be chosen appropriately so that $A=B=C=D=0$. To begin, replace $u^s\mathbf{f}+A\mathbf{e}+B\mathbf{e}'$ with $u^s\mathbf{f}+A\mathbf{e}+B\mathbf{e}'-A(u^r\mathbf{e}'+\mathbf{e})$ in our basis for $\mathcal{N}_1$, so that we may take $A=0$. Similarly we can take $C=0$. Now note that since $u^{l^2-1}\mathbf{f}\in u^{l^2-1}\mathcal{N}\subset\mathcal{N}_1$ and $u^r(u^s\mathbf{f}+B\mathbf{e}')\in\mathcal{N}_1$, we obtain $u^rB\mathbf{e}'\in\mathcal{N}_1$. This implies $u^s\mid B$. Writing $B=u^sB'$, we may take $\tilde{\mathbf{f}}=\mathbf{f}+B'\mathbf{e}'$, and then $\mathcal{N}_1$ has the basis $\langle u^s\mathbf{e},u^r\mathbf{e}'+\mathbf{e},u^s\tilde{\mathbf{f}},u^r\mathbf{f}'+\tilde{\mathbf{f}}+D\mathbf{e}'\rangle$ for some D. Finally, we wish to alter $\mathbf{f}'$ to eliminate D. By the same considerations as before, we can see $u^sD\mathbf{e}'\in\mathcal{N}_1$, and so $u^r\mid D$. Putting $D=u^rD'$ we can take $\tilde{\mathbf{f}}'=\mathbf{f}'+D'\mathbf{e}'$, and we conclude that we may suppose

$$\mathcal{N}_1=\langle u^s\mathbf{e},u^r\mathbf{e}'+\mathbf{e},u^s\mathbf{f},u^r\mathbf{f}'+\mathbf{f}\rangle.$$

Step ii: the next thing we want to do is determine the ways we can still alter $\mathbf{f}$, $\mathbf{f}'$ to $\tilde{\mathbf{f}}$, $\tilde{\mathbf{f}}'$ while preserving this form for $\mathcal{N}_1$, i.e. keeping $u^s\tilde{\mathbf{f}}$, $u^r\tilde{\mathbf{f}}'+\tilde{\mathbf{f}}\in\mathcal{N}_1$. To this end, suppose

$$\mathbf{f}\mapsto\tilde{\mathbf{f}}=\mathbf{f}+A\mathbf{e}+B'\mathbf{e}',\quad \mathbf{f}'\mapsto\tilde{\mathbf{f}}'=\mathbf{f}'+C\mathbf{e}+D'\mathbf{e}'.$$

Then

$$u^s\tilde{\mathbf{f}}=u^s\mathbf{f}+Au^s\mathbf{e}+B'u^s\mathbf{e}',$$

and this is in $\mathcal{N}_1$ provided u^r divides B'. Write $B'=u^rB$. Now

$$u^r\tilde{\mathbf{f}}'+\tilde{\mathbf{f}}=(u^r\mathbf{f}'+\mathbf{f})+(A+u^rC-B-D')\mathbf{e}+(B+D')(u^r\mathbf{e}'+\mathbf{e}).$$

Thus C may be arbitrary so long as we select D' such that u^s divides $A+u^rC-B-D'$. Writing $A+u^rC-B-D'=u^sD$ we may evidently make D arbitrary and put $D'=A+u^rC-B-u^sD$. So our most general change of variables is

$$\tilde{\mathbf{f}}=\mathbf{f}+A\mathbf{e}+u^rB\mathbf{e}',\quad \tilde{\mathbf{f}}'=\mathbf{f}'+C\mathbf{e}+(A-B+u^rC+u^sD)\mathbf{e}' \tag{9.2}$$

with A,B,C,D arbitrary.

Step iii: we now turn to the question of ϕ_1. We suppose

$$\phi_1(u^s\mathbf{e})=b\mathbf{e},\quad \phi_1(u^r\mathbf{e}'+\mathbf{e})=a\mathbf{e}',$$

$$\phi_1(u^s\mathbf{f})=b\mathbf{f}+V\mathbf{e}+W\mathbf{e}',\quad \phi_1(u^r\mathbf{f}'+\mathbf{f})=a\mathbf{f}'+Y\mathbf{e}+Z\mathbf{e}'.$$

Using the change-of-variables (9.2), we wish to simplify V, W, Y, Z. To begin with, we try $\tilde{\mathbf{f}}=\mathbf{f}+A\mathbf{e}+u^rB\mathbf{e}'$ (with a commensurate choice of $\tilde{\mathbf{f}}'$, which for now will be irrelevant). Then one computes that $\phi_1(u^{(l-1)s'}\tilde{\mathbf{f}})$ is equal to

$$b\tilde{\mathbf{f}}+(V-bA+b(A-B)^l)\mathbf{e}+(W+u^r(aB^lu^{(ls-r)}-bB))\mathbf{e}'.$$

https://doi.org/10.1112/S0010437X03000289 Published online by Cambridge University Press

Since B may be arbitrary and $ls - r > 0$ we may make $(aB^l u^{(ls-r)} - bB)$ arbitrary, and we may use this choice to eliminate all terms in W of degree at least r. Thus we may assume $\deg(W) < r$. Making this change completely determines $u^r B$, so we may now make this change and assume henceforth that $B = 0$ and $\deg(W) < r$. Then V is altered to $V + b(A^l - A)$ by our choice of A, which we can use to eliminate every term of V except the constant term. We can therefore suppose that V is a constant v, that W is a polynomial of degree less than r, and that the only still-allowable change of $\mathbf{f}$ is $\mathbf{f} \mapsto \mathbf{f} + \alpha\mathbf{e}$, with α a constant, moving $V \mapsto V + b(\alpha^l - \alpha)$. Note for later reference that if we take $C = D = 0$, then this change of variables also takes

$$Z \mapsto Z + a(\alpha^l - \alpha). \tag{9.3}$$

Consider the additive map from $\mathbb{F}_{l^2} \to \mathbb{F}_{l^2}$ sending x to $x^l - x$. The kernel is exactly $\mathbb{F}_l$, while if $x^l - x \in \mathbb{F}_l$ then $(x^l - x)^l = x^l - x$; since $x^{l^2} = x$ and $l \neq 2$ we find $x^l = x$. So our map induces an isomorphism $\mathbb{F}_{l^2}/\mathbb{F}_l \to \mathbb{F}_{l^2}/\mathbb{F}_l$. Thus we may select α above so that $V \in \mathbb{F}_l$, and then V is completely fixed, while $\mathbf{f} \mapsto \mathbf{f} + \alpha\mathbf{e}$ with $\alpha \in \mathbb{F}_l$ is the only possible change of $\mathbf{f}$.

Summary (so far): we have now shown that our $(\mathcal{N}, \mathcal{N}_1, \phi_1)$ without descent data may be taken to have the following simplified form:

$$\begin{gathered}
\mathcal{N} = \langle \mathbf{e}, \mathbf{e}', \mathbf{f}, \mathbf{f}' \rangle, \quad \mathcal{N}_1 = \langle u^s\mathbf{e}, u^r\mathbf{e}' + \mathbf{e}, u^s\mathbf{f}, u^r\mathbf{f}' + \mathbf{f} \rangle, \\
\phi_1(u^s\mathbf{e}) = b\mathbf{e}, \quad \phi_1(u^r\mathbf{e}' + \mathbf{e}) = a\mathbf{e}', \\
\phi_1(u^s\mathbf{f}) = b\mathbf{f} + v\mathbf{e} + W\mathbf{e}', \quad \phi_1(u^r\mathbf{f}' + \mathbf{f}) = a\mathbf{f}' + Y\mathbf{e} + Z\mathbf{e}',
\end{gathered}$$

with $v \in \mathbb{F}_l$ and $\deg(W) < r$. Moreover, the changes of variable preserving this form are those of Equation (9.2) with $A = \alpha \in \mathbb{F}_l$ and $B = 0$.

Step iv: to reduce further, we now wish to see the ways in which these extensions of Breuil modules admit generic fibre descent data. Suppose

$$[g]\mathbf{f} = \left(\frac{g\pi}{\pi}\right)^{(l+1)d-ls'} \mathbf{f} + A_g\mathbf{e} + B_g\mathbf{e}'.$$

Then

$$[g](u^s\mathbf{f}) = \left(\frac{g\pi}{\pi}u\right)^s \left(\left(\frac{g\pi}{\pi}\right)^{(l+1)d-ls'} \mathbf{f} + A_g\mathbf{e} + B_g\mathbf{e}'\right) \in \mathcal{N}_1,$$

which requires $u^r \mid B_g$, say $B_g = u^r B'_g$. We see that $\phi_1([g](u^s\mathbf{f}))$ is equal to

$$\left(\frac{g\pi}{\pi}\right)^{(l+1)d-ls'} (b\mathbf{f} + v\mathbf{e} + W\mathbf{e}') + \left(\frac{g\pi}{\pi}\right)^{ls} u^{sl}(B'_g)^l a\mathbf{e}' + g\left(\frac{g\pi}{\pi}\right)^{sl} (A_g - B'_g)^l\mathbf{e},$$

whereas $[g](\phi_1(u^s\mathbf{f}))$ is

$$\left(\frac{g\pi}{\pi}\right)^{(l+1)d-ls'} b\mathbf{f} + \left(v\left(\frac{g\pi}{\pi}\right)^{(l+1)d-ls'} + bA_g\right)\mathbf{e} + \left({}^gW\left(\frac{g\pi}{\pi}\right)^{(l+1)c-lr'} + bB_g\right)\mathbf{e}'$$

using ${}^gv = v$ since $v \in \mathbb{F}_l$. Matching coefficients we get

$$A_g = \left(\frac{g\pi}{\pi}\right)^{sl} (A_g - B'_g)^l \tag{9.4}$$

and

$${}^gW\left(\frac{g\pi}{\pi}\right)^{(l+1)c-lr'} + bB_g = w\left(\frac{g\pi}{\pi}\right)^{(l+1)d-ls'} + a\left(\frac{g\pi}{\pi}\right)^{sl} u^{sl}(B'_g)^l. \tag{9.5}$$

Since W is of degree less than r whereas B_g and u^{sl} are divisible by u^r, Equation (9.5) implies

$${}^gW\left(\frac{g\pi}{\pi}\right)^{(l+1)c-lr'} = W\left(\frac{g\pi}{\pi}\right)^{(l+1)d-ls'} \tag{9.6}$$

https://doi.org/10.1112/S0010437X03000289 Published online by Cambridge University Press

and

$$bB_g = a\left(\frac{g\pi}{\pi}\right)^{sl} u^{sl}(B'_g)^l. \tag{9.7}$$

All of the rank-two Breuil modules under consideration here have $n = 0$, so $(l+1)d - ls' \equiv (l+1)c - r' \pmod{l^2-1}$, and using this in Equation (9.6) we obtain ${}^gW = (g\pi/\pi)^r W$ for all g. Since $\deg W < r$, this is only possible if $W = 0$. In Equation (9.7), if the left-hand side has lowest non-zero term of degree k, then for the right-hand side the lowest term has degree $sl + l(k-r)$. Equating these degrees gives $k = r + (r' - ls') < r$, contradicting our divisibility condition on B_g. Thus $B_g = 0$. Taking $B'_g = 0$ in Equation (9.4), we finally obtain

$$A_g = \left(\frac{g\pi}{\pi}\right)^{sl} A_g^l,$$

which implies that A_g is a constant. Indeed $A_g(g\pi/\pi)^{-(l+1)d+ls'} \in \mathbb{F}_l$, and one checks from this and from the relation $[h][g] = [hg]$ that the map $g \mapsto (g\pi/\pi)^{-(l+1)d+ls'}A_g$ is a homomorphism from $G = \mathrm{Gal}(H'/\mathbb{Q}_l)$ to $\mathbb{F}_l$, which must be the zero map. We have thus shown $A_g = B_g = 0$ and $W = 0$.

Step v: next we consider the more difficult problem of simplifying Y, Z, and $[g]\mathbf{f}'$ by altering $\mathbf{f}'$. Taking $A = B = 0$ in Equation (9.2), we select

$$\tilde{\mathbf{f}}' = \mathbf{f}' + C\mathbf{e} + (u^rC + u^sD)\mathbf{e}'.$$

Then one computes that $\phi_1(u^r\tilde{\mathbf{f}}' + \mathbf{f})$ is equal to

$$a\tilde{\mathbf{f}}' + (Y - aC - bD^l)\mathbf{e} + (Z - a(u^rC + u^sD) + a(u^rC + u^sD)^l)\mathbf{e}'.$$

Whatever D is, we will certainly want to take $aC = Y - bD^l$ to eliminate Y (which completely determines C in terms of D). We may therefore assume $Y = 0$ and $aC = -bD^l$, and then our map alters

$$Z \mapsto Z - (bu^rD^l - au^sD)^l + (bu^rD^l - au^sD). \tag{9.8}$$

Noting this, we now turn to the consideration of generic fibre descent data. Suppose for each g that

$$[g]\mathbf{f}' = \left(\frac{g\pi}{\pi}\right)^{(l+1)c-lr'}\mathbf{f}' + E_g\mathbf{e} + F_g\mathbf{e}'.$$

We then have

$$[g](u^r\mathbf{f}' + \mathbf{f}) = \left(\frac{g\pi}{\pi}\right)^{(l+1)c-r'}(u^r\mathbf{f}' + \mathbf{f}) + \left(\frac{g\pi}{\pi}\right)^r(E_gu^r - F_g)\mathbf{e} + \left(\frac{g\pi}{\pi}\right)^r F_g(u^r\mathbf{e}' + \mathbf{e})$$

so $u^s \mid (g\pi/\pi)^r(E_gu^r - F_g) = u^s\Delta_g$ and

$$\phi_1[g](u^r\mathbf{f}' + \mathbf{f}) = \left(\frac{g\pi}{\pi}\right)^{(l+1)c-lr'}(a\mathbf{f}' + Z\mathbf{e}') + \Delta_g^l b\mathbf{e} + a\left(\frac{g\pi}{\pi}\right)^{lr}F_g^l\mathbf{e}'.$$

Matching coefficients with

$$[g]\phi_1(u^r\mathbf{f}' + \mathbf{f}) = \left(\frac{g\pi}{\pi}\right)^{(l+1)c-lr'}a\mathbf{f}' + aE_g\mathbf{e} + aF_g\mathbf{e}' + {}^gZ\left(\frac{g\pi}{\pi}\right)^{(l+1)c-lr'}\mathbf{e}'$$

gives $aE_g = b\Delta_g^l$ and

$$aF_g + {}^gZ\left(\frac{g\pi}{\pi}\right)^{(l+1)c-lr'} = a\left(\frac{g\pi}{\pi}\right)^{lr}F_g^l + Z\left(\frac{g\pi}{\pi}\right)^{(l+1)c-lr'}. \tag{9.9}$$

With these equations in hand we compute from $[hg] = [h][g]$ that the map $g \mapsto (g\pi/\pi)^{-(l+1)c+lr'}E_g$ is a cocycle in the group cohomology $H^1(G, \mathbb{F}_{l^2}[u]/u^{l(l^2-1)})$ where G acts on $\mathbb{F}_{l^2}[u]/u^{l(l^2-1)}$ via $gf = (g\pi/\pi)^r\ {}^gf$. Similarly $g \mapsto (g\pi/\pi)^{-(l+1)c+lr'}F_g$ is a cocycle in $H^1(G, \mathbb{F}_{l^2}[u]/u^{l(l^2-1)})$ for the action $gf = {}^gf$. We know from the proof of Lemma 4.1 that both

https://doi.org/10.1112/S0010437X03000289 Published online by Cambridge University Press

these cohomological groups are trivial, and therefore we obtain elements $P, Q \in \mathbb{F}_{l^2}[u]/u^{l(l^2-1)}$ such that

$$\left(\frac{g\pi}{\pi}\right)^{-(l+1)c+lr'} E_g = \left(\frac{g\pi}{\pi}\right)^r {}^gQ - Q$$

and

$$\left(\frac{g\pi}{\pi}\right)^{-(l+1)c+lr'} F_g = {}^gP - P.$$

Setting $R = u^rQ - P$, we see

$$E_gu^r - F_g = \left(\frac{g\pi}{\pi}\right)^{(l+1)c-lr'} ({}^gR - R).$$

Recalling that $u^s\Delta_g = (g\pi/\pi)^r(E_gu^r - F_g)$, so that

$$\Delta_g = \left(\frac{g\pi}{\pi}\right)^{(l+1)c-r'} \frac{{}^gR - R}{u^s}$$

we find that R must have no terms of degree less than s, except possibly for a constant term in $\mathbb{F}_l$. We write $R = r_0 + r_su^s + \cdots = r_0 + u^sR_0$. Then the equation $aE_g = b\Delta_g^l$ gives

$$\left(\frac{{}^gR - R}{u^s}\right)^l = \frac{a}{b}\left(\left(\frac{g\pi}{\pi}\right)^r {}^gQ - Q\right).$$

Writing $Q = q_0 + q_1u + \cdots$, we examine the above equation term-by-term. Using the fact that $r \equiv ls \pmod{l^2-1}$, the left-hand side has terms of the form $({}^gr_{i+s}^l(g\pi/\pi)^{il+r} - r_{i+s}^l)u^{il}$ while the right-hand side has terms of the form $(a/b)({}^gq_j(g\pi/\pi)^{r+j} - q_j)u^j$. Thus $q_j = 0$ unless j is divisible by l, or unless $j \equiv s \pmod{l^2-1}$ and $q_j \in \mathbb{F}_l$. If $j = il$ and is not congruent to $s \pmod{l^2-1}$ then the map $x \mapsto {}^gx(g\pi/\pi)^{r+il} - x$ is injective and we can match $q_{il} = (b/a)r_{i+s}^l$. From this analysis, we conclude that $Q = (b/a)R_0^l + Q'$, where the terms of Q' have degree congruent to $s \pmod{l^2-1}$ and coefficients in $\mathbb{F}_l$. Therefore $P = u^rQ - R = \frac{b}{a}u^rR_0^l - u^sR_0 + P'$, where P' has terms of degree divisible by l^2-1 and coefficients in $\mathbb{F}_l$. Combining Equation (9.9) with

$$F_g = \left(\frac{g\pi}{\pi}\right)^{(l+1)c-lr'} ({}^gP - P)$$

we get

$${}^g(aP - aP^l + Z) = aP - aP^l + Z$$

and so all terms of $aP - aP^l + Z$ are of degree divisible by l^2-1 with coefficients in $\mathbb{F}_l$. Putting all this together, we find that

$$Z = (bu^rR_0(u)^l - au^sR_0(u))^l - (bu^rR_0(u)^l - au^sR_0(u)) + Z',$$

where Z' has terms of degree divisible by l^2-1 and coefficients in $\mathbb{F}_l$. Therefore *taking $D = R_0$ in our change-of-variables (9.2) for $\mathbf{f}'$ transforms Z into Z'*, a polynomial with all terms of degree divisible by l^2-1 and coefficients in $\mathbb{F}_l$.

We still wish to reduce Z further, which is easier now that we can assume that Z has no terms of low degree except a constant term in $\mathbb{F}_l$. If we alter Z via some choice of D, we suppose that $D = \sum_i d_iu^i$ has no terms of degree less than $s' - r'$. Then the lowest non-zero term of

$$\frac{b}{a}u^{lr}D^{l^2} - \left(\frac{b}{a}u^r + u^{ls}\right)D^l + u^sD$$

has degree $ls' - r'$, and specifically the lowest term is

$$\left(-\frac{b}{a}d_{s'-r'}^l + d_{s'-r'}\right)u^{ls'-r'}.$$

https://doi.org/10.1112/S0010437X03000289 Published online by Cambridge University Press

The equation $x = -(b/a)d_{s'-r'}^l + d_{s'-r'}$ may be solved for

$$d_{s'-r'} = \left(1 - \frac{b^2}{a^2}\right)^{-1}\left(x + \frac{b}{a}x^l\right)$$

except possibly if $a = \pm b$ and $x \neq 0$. Note also that, if $x \in \mathbb{F}_l$, there is a solution for $d_{s'-r'}$ except possibly if $a = b$.

The terms of degree $i > ls' - r'$ in our transformation of Z are

$$u^s(d_{i-s}u^{i-s}) - u^{ls}(d_{(i-ls)/l}u^{(i-ls)/l})^l - \frac{b}{a}u^r(d_{(i-r)/l}u^{(i-r)/l})^l + \frac{b}{a}u^{lr}(d_{(i-lr)/l^2}u^{(i-lr)/l^2})^{l^2}.$$

Since $i - s > (i - ls)/l$, $(i - r)/l$, $(i - lr)/l^2$ for $i > ls' - r'$ we see that taking $d_{i-s} = 0$ for i up to $ls' - r'$ and solving the resulting *linear* equations for d_{i-s} for $i > ls' - r'$, we may alter Z to remove all terms of degree greater than $ls' - r'$ (without introducing a term of degree $ls' - r'$ if there was not one to begin with). Therefore unless $ls' - r' = l^2 - 1$, i.e. unless $r' = 1$, $s' = l$, we may certainly take Z to be a constant. In case $r' = 1$, $s' = l$, note that the case $a = b$ is excluded automatically from our list of rank-two Breuil modules with descent data (9.1), and so again the term of degree $ls' - r' = l^2 - 1$ can be removed by this argument. Therefore in any case we can suppose Z is a constant $z \in \mathbb{F}_l$.

In case $a = \pm b$ and $s' \geqslant r'$, let η be a choice of $(a/b)^{1/(l-1)}$. We note, for future reference, that for any $d \in \mathbb{F}_l$ by the above argument there is a change-of-$\mathbf{f}'$ leaving Z fixed, given by $D = \eta\, du^{s'-r'} +$ (higher terms) and the corresponding C.

Now observe that because we have reduced Z to a simple form, we get $F_g = a(g\pi/\pi)^{lr}F_g^l$, and since u divides F_g we get $F_g = 0$. Then our equation for E_g becomes

$$aE_g = b\left(\frac{(g\pi/\pi)^r u^r E_g}{u^s}\right)^l$$

and so if E_g is non-zero then: E_g is a monomial of degree $u^{l(s'-r')}$, but also $s' \geqslant r'$ and a/b is an $(l-1)$st power in $\mathbb{F}_{l^2}^{\times}$, i.e. $a = \pm b$.

So automatically $E_g = 0$ unless $s' \geqslant r'$ and $a = \pm b$, which is exactly the situation in which there was a change-of-$\mathbf{f}'$ leaving Z fixed. In this case write $(g\pi/\pi)^{-(l+1)c+lr'}E_g = e_g u^{l(s'-r')}$, so that $e_{hg} = e_h + (h\pi/\pi)^{ls'-r'}\,{}^h e_g$. If $s' = l, r' = 1$ then $g \mapsto e_g$ is a homomorphism $G \to \mathbb{F}_{l^2}$, so is zero. Otherwise, by the usual cohomological argument $e_g = (g\pi/\pi)^{ls'-r'}\,{}^g e - e$ for some $e \in \mathbb{F}_{l^2}$. Then selecting any g for which $(g\pi/\pi)^{ls'-r'} \in \mathbb{F}_l$ is not 1, we see that $e = \eta d \in \eta\mathbb{F}_l$, where η was our previously-chosen $(l-1)$st root of a/b. Finally, we make the change-of-$\mathbf{f}'$ which fixes Z and has $D = \eta\, du^{s'-r'} +$ (higher terms). The corresponding $C = -a^{-1}bD^l = -\eta\, du^{l(s'-r')} +$ (higher terms). Then $\tilde{\mathbf{f}}' = \mathbf{f}' + C\mathbf{e} + (\mathbf{e}'$ term), and we compute that $[g]\tilde{\mathbf{f}}'$ is equal to

$$\left(\frac{g\pi}{\pi}\right)^{(l+1)c-lr'}\tilde{\mathbf{f}}' + E_g\mathbf{e} + \left({}^gC\left(\frac{g\pi}{\pi}\right)^{(l+1)c-r'} - C\left(\frac{g\pi}{\pi}\right)^{(l+1)c-lr'}\right)\mathbf{e} + (\mathbf{e}' \text{ term}).$$

So we have transformed E_g into

$$E_g - \left({}^g\eta\, d\left(\frac{g\pi}{\pi}\right)^{l(s'-r')}\left(\frac{g\pi}{\pi}\right)^{(l+1)c-r'} - \eta\, d\left(\frac{g\pi}{\pi}\right)^{(l+1)c-lr'}\right)u^{l(s'-r')} + (\text{higher terms}),$$

and therefore this transformation leaves E_g with no term of degree $u^{l(s'-r')}$. However, notice that since Z is unchanged by this transformation we still obtain $F_g = 0$, and now our new E_g, having no terms of degree $u^{l(s'-r')}$, is also 0.

To summarize, we have proved the following theorem.

Theorem 9.10. *For the $\mathcal{M}$ under consideration, any $\mathcal{N} \in \operatorname{Ext}^1(\mathcal{M}, \mathcal{M})$ in the category of Breuil modules with descent data from H' to $\mathbb{Q}_l$ has the form*

$$\mathcal{N} = \langle \mathbf{e}, \mathbf{e}', \mathbf{f}, \mathbf{f}' \rangle$$

with

$$\mathcal{N}_1 = \langle u^s\mathbf{e}, u^r\mathbf{e}' + \mathbf{e}, u^s\mathbf{f}, u^r\mathbf{f}' + \mathbf{f} \rangle$$

and

$$\phi_1(u^s\mathbf{e}) = b\mathbf{e}, \quad \phi_1(u^r\mathbf{e}' + \mathbf{e}) = a\mathbf{e}',$$
$$\phi_1(u^s\mathbf{f}) = b\mathbf{f} + v\mathbf{e}, \quad \phi_1(u^r\mathbf{f}' + \mathbf{f}) = a\mathbf{f}' + z\mathbf{e}',$$

with v, $z \in \mathbb{F}_l$, and generic fibre descent data satisfying

$$[g](\mathbf{e}) = \left(\frac{g\pi}{\pi}\right)^{(l+1)d-ls'} \mathbf{e}, \quad [g](\mathbf{f}) = \left(\frac{g\pi}{\pi}\right)^{(l+1)d-ls'} \mathbf{f},$$
$$[g](\mathbf{e}') = \left(\frac{g\pi}{\pi}\right)^{(l+1)c-lr'} \mathbf{e}', \quad [g](\mathbf{f}') = \left(\frac{g\pi}{\pi}\right)^{(l+1)c-lr'} \mathbf{f}'.$$

Therefore this Ext^1 *is two-dimensional over $\mathbb{F}_l$.*

To confirm that the dimension is exactly (rather than at most) two, we have seen that any change of variables preserving the above form for $(\mathcal{N}, \mathcal{N}_1, \phi_1)$ must, in the notation of Equation (9.2), have $A \in \mathbb{F}_l$, $B = 0$, and $aC = -bD^l$ for suitable values of D. Yet the effect of such a change of variables is to alter $v \mapsto v + b(A^l - A)$ and

$$z \mapsto z + a(A^l - A) - (bu^rD^l - au^sD)^l + (bu^rD^l - au^sD)$$

by Equations (9.3) and (9.8). Since $A^l = A$ and $r, s > 0$, we note that this change of variables cannot alter the constant terms of v, z. Hence if a change of variables preserves the desired form for $(\mathcal{N}, \mathcal{N}_1, \phi_1)$ it does not alter v, z.

9.1 Dieudonné module relations

It remains to determine which of these extensions with descent data satisfies relations (2.3)–(2.5) on their Dieudonné module. We check from the compatibility between Breuil theory and Dieudonné theory described in § 3 that each of the above extensions of Breuil modules with descent data yields a Dieudonné module with basis $\mathbf{v}, \mathbf{w}, \mathbf{v}', \mathbf{w}'$ on which F and V act through the matrices

$$F = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -b & 0 & 0 & 0 \\ -v & -b & 0 & 0 \end{pmatrix} \quad \text{and} \quad V = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1/a & 0 & 0 & 0 \\ -z/a^2 & 1/a & 0 & 0 \end{pmatrix}.$$

(Note that these matrices only describe the actions of F, V on this particular basis: the actions of F, V are extended to the full Dieudonné module *semilinearly*.)

To see this, we will have $\mathbf{v}, \mathbf{w}, \mathbf{v}', \mathbf{w}'$ correspond respectively to the images of $\mathbf{e}, \mathbf{f}, \mathbf{e}', \mathbf{f}'$ in $\mathcal{N}/u\mathcal{N}$. Observe that $\phi(\mathbf{e}) = \phi_1(u^{l^2-1}\mathbf{e}) = u^r b\,\mathbf{e}$ which maps to 0 in $\mathcal{N}/u\mathcal{N}$, and similarly $\phi(\mathbf{f}) = 0$ in $\mathcal{N}/u\mathcal{N}$. This gives the first two rows of the matrix for F. Next, $\phi(\mathbf{e}') = \phi_1(u^{l^2-1}\mathbf{e}') = \phi_1(u^s(u^r\mathbf{e}'+\mathbf{e}) - u^s\mathbf{e}) = -b\,\mathbf{e}$ in $\mathcal{N}/u\mathcal{N}$, while similarly $\phi(\mathbf{f}')$ in $\mathcal{N}/u\mathcal{N}$ is $-\phi_1(u^s\mathbf{f}) = -b\mathbf{e} - v\mathbf{f}$.

To obtain the matrix for V, we note that $\phi_1^{-1}(\mathbf{e}) = b^{-1}u^s\mathbf{e}$ is 0 in $\mathcal{N}/u\mathcal{N}$, and similarly for $\phi_1^{-1}(\mathbf{f})$. Alternatively, $\phi_1^{-1}(\mathbf{e}') = a^{-1}(u^r\mathbf{e}' + \mathbf{e})$, which is $a^{-1}\mathbf{e}$ in $\mathcal{N}/u\mathcal{N}$, and

$$\phi_1^{-1}(\mathbf{f}') = a^{-1}(u^r\mathbf{f}' + \mathbf{f}) - \frac{z}{a^2}(u^r\mathbf{e}' + \mathbf{e}),$$

which indeed is $a^{-1}\mathbf{f} - (z/a^2)\mathbf{e}$ in $\mathcal{N}/u\mathcal{N}$.

We know that in this case $T = \mathrm{Teich}(\det(\overline{\rho}))(s)$ reduces in $\mathbb{F}_l$ to ab, and so $F + TV = 0$ precisely when $-v - (b/a)z = 0$. The space of extensions of Breuil modules with descent data satisfying the necessary Dieudonné module relations is one-dimensional. This completes the proof of Theorem 1.1.

Acknowledgements

This article is a somewhat improved version of the author's doctoral dissertation. The author is deeply indebted to his thesis supervisor, Richard Taylor. At every step of the way, Taylor's mathematical instruction and meticulous advice have been of inestimable value.

Throughout the author's graduate study, Brian Conrad has been a tireless resource, unfailingly willing to provide a detailed answer to any question. Several conversations with Fred Diamond and Christophe Breuil were of great help at key moments.

References

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

BM02 C. Breuil and A. Mézard, *Multiplicités modulaires et représentations de* $\mathrm{GL}_2(\mathbf{Z}_p)$ *et de* $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ *en* $l = p$, with an appendix by Guy Henniart, Duke Math. J. **115** (2002), 205–310.

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

Bru95 A. Brumer, *The rank of* $J_0(N)$, *Columbia University number theory seminar, New York, 1992*, Astérisque **228** (1995), 41–68.

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

Con B. Conrad, *Wild ramification and deformation rings*, Münster Preprint (1999).

Con99 B. Conrad, *Ramified deformation problems*, Duke Math. J. **97** (1999), 439–514.

Edi92 B. Edixhoven, *The weight in Serre's conjectures on modular forms*, Invent. Math. **109**(3) (1992), 563–594.

FM95 J.-M. Fontaine and B. Mazur, *Geometric Galois representations*, in *Elliptic curves, modular forms, and Fermat's last theorem*, eds J. Coates and S.-T. Yau (International Press, 1995), 41–78.

Fon94 J.-M. Fontaine, *Representations p-adiques semis-tables*, Astérisque **223** (1994), 113–184.

GJG03 E. González-Jiménez and J. González, *Modular curves of genus* 2, Math. Comp. **72** (2003), 397–418.

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

Ram93 R. Ramakrishna, *On a variant of Mazur's deformation functor*, Compositio Math. **87**(3) (1993), 269–286.

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

Ser87 J-P. Serre, *Sur les représentations modulaires de degré 2 de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. **54** (1987), 179–230.

Tat67 J. Tate, *p-divisible groups*, in *Proc. conf. on local fields*, Driebergen, 1966) (Springer, Berlin, 1967), 158–183.

Tay02 R. Taylor, *Remarks on a conjecture of Fontaine and Mazur*, J. Inst. Math. Jussieu **1** (2002), 1–19.

TW95 R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. Math. **142** (1995), 553–572.

Wil95 A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. Math. **142** (1995), 443–551.

David Savitt dsavitt@math.mcgill.ca
Department of Mathematics, McGill University, 805 Sherbrooke W., Montréal, Québec, Canada
H3A 2K6

https://doi.org/10.1112/S0010437X03000289 Published online by Cambridge University Press