RIBET'S CONVERSE TO HERBRAND'S THEOREM

AYAN NATH

Abstract. In this article, we present an overview of Ribet's proof of the converse to Herbrand's theorem. While Erickson's work [Eri08] provides an excellent exposition on the topic, our focus is on elucidating the scheme-theoretic details found in Ribet's paper [Rib76, §4], particularly his use of finite flat group schemes towards the end of the proof, a facet not covered in Erickson's essay.

1 Introduction

Fix an odd prime number p. Let A be the ideal class group of $\mathbb{Q}(\mu_p)$ where μ_p is the group of all pth roots of unity as usual. Denote $C = A \otimes_{\mathbb{Z}} \mathbb{F}_p$, an $\mathbb{F}_p$-vector space. If $C \neq 0$ then p is called **irregular**. Define the nth Bernoulli number B_n by the exponential generating function

$$\frac{T}{e^T - 1} = \sum_{n \in \mathbb{N}} B_n \frac{T^n}{n!}.$$

1.1. Kummer's criterion. — *p is irregular if and only if $p \mid B_2 B_4 \cdots B_{p-3}$.*

The $\mathbb{F}_p$-vector space C carries an action of the cyclotomic Galois group $\Delta = \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ for which there is an isomorphism $\chi\colon \Delta \to \mathbb{F}_p^\times$ given by the mod p cyclotomic character. Thus, there is a Δ-module decomposition

$$C = \bigoplus_{0 \leqslant i \leqslant p-2} C(\chi^i),$$

where $C(\chi^i)$ is the part of C on which $\sigma \in \Delta$ acts as multiplication by $\chi^i(\sigma)$. Herbrand's theorem states that if $C(\chi^{1-k}) \neq 0$ for some even integer $k \in [2, p-3]$ then $p \mid B_k$. The main result of [Rib76] is the following–

1.2. Theorem (Ribet). — *Let k be an even integer in $[2, p-3]$. Then $p \mid B_k$ if and only if $C(\chi^{1-k}) \neq 0$.*

By class field theory, the above theorem is implied by–

1.3. Theorem. — *Let $k \in [2, p-3]$ be an even integer, and suppose that $p \mid B_k$. There exists a Galois extension $E/\mathbb{Q}$ containing $\mathbb{Q}(\mu_p)$ such that*

(a) The extension $E/\mathbb{Q}(\mu_p)$ is unramified.
(b) $\mathrm{Gal}(E/\mathbb{Q}(\mu_p))$ is a nonzero abelian group killed by p.
(c) If $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$ and $\tau \in \mathrm{Gal}(E/\mathbb{Q}(\mu_p))$ then $\sigma\tau\sigma^{-1} = \chi(\sigma)^{1-k}\tau$.

Indeed, let $E/\mathbb{Q}(\mu_p)$ be as in Theorem 1.3. Let $\mathscr{C}$ be the idéle class group of $\mathbb{Q}(\mu_p)$ and $\theta\colon \mathscr{C} \to \mathrm{Gal}(E/\mathbb{Q}(\mu_p))$ be the (Δ-equivariant) reciprocity map. Then θ factors through a surjection $C = \mathscr{C} \otimes_{\mathbb{Z}} \mathbb{F}_p \twoheadrightarrow \mathrm{Gal}(E/\mathbb{Q}(\mu_p))$. Therefore, we have Δ-equivariant surjections $C(\chi^i) \twoheadrightarrow \mathrm{Gal}(E/\mathbb{Q}(\mu_p))(\chi^i)$. When $i = 1-k$, we see that the latter group is nonzero from part (c), and consequently $C(\chi^{1-k})$ is nonzero. The above theorem is in turn implied by the following–

Date: 9th September, 2023.

Affiliation: BSc 3rd year, Chennai Mathematical Institute.

1.4. Theorem. — *Let $k \in [2, p-3]$ be an even integer, and suppose that $p \mid B_k$. There exists a finite field $\mathbb{F}/\mathbb{F}_p$ and a Galois representation $\overline{\rho}\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F})$ with the following properties–*

(a) $\overline{\rho}$ *is unramfied at all primes $\ell \neq p$.*
(b) The representation $\overline{\rho}$ is reducible in such a way that $\overline{\rho}$ is isomorphic to a representation of the form $\begin{bmatrix} 1 & b \\ 0 & \chi^{k-1} \end{bmatrix}$ *where $b\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}$.*
(c) $\mathrm{Im}\,\overline{\rho}$ *has order divisible by p. That is, $\overline{\rho}$ is not diagonalizable.*
(d) Let D be a decomposition group for p in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Then the image of D has order prime to p. That is, $\overline{\rho}|_D$ is diagonalizable.

We first show that Theorem 1.4 implies Theorem 1.3 with $\mathbb{Q}(\mu_p)$ replaced by $\mathbb{Q}(\mu_p^{1-k})$. Indeed, the claim is that the fixed subfield of $\mathrm{Ker}\,\overline{\rho}$, say E, the Galois number field cut out by $\overline{\rho}$, satisfies the conditions of Theorem 1.3. Then $\overline{\rho}$ induces an injection $\mathrm{Gal}(E/\mathbb{Q}) \hookrightarrow \mathrm{GL}_2(\mathbb{F})$. It is clear that there is a tower $E/\mathbb{Q}(\mu_p^{1-k})/\mathbb{Q}$ since $\mathbb{Q}(\mu_p^{1-k})$ is precisely the fixed subfield of $\mathrm{Ker}\,\chi^{k-1}$. Further, $\mathrm{Gal}(E/\mathbb{Q}(\mu_p^{1-k}))$ is an abelian p-group, for the image of $\mathrm{Gal}(E/\mathbb{Q}(\mu_p^{1-k}))$ consists of upper unipotent matrices. Since $\overline{\rho}$ is not diagonalizable, it follows that $E \neq \mathbb{Q}(\mu_p^{1-k})$. It is clear that $E/\mathbb{Q}(\mu_p^{1-k})$ is unramified away from p. It remains to prove that $E/\mathbb{Q}(\mu_p^{1-k})$ is unramified at the unique prime $\mathfrak{p}$ of $\mathbb{Q}(\mu_p^{1-k})$ above p. The inertia group of $\mathfrak{p}$ in $\mathrm{Gal}(E/\mathbb{Q}(\mu_p^{1-k}))$ has order prime to p because $\mathrm{Im}(\overline{\rho}|_D)$ has order prime to p, so $E/\mathbb{Q}(\mu_p^{1-k})$ is at worst tamely ramified. However, $E/\mathbb{Q}(\mu_p^{1-k})$ is a p-extension, hence it must be everywhere unramified. Part (c) of Theorem 1.3 is just a consequence of the matrix identity

$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}^{-1} = \begin{bmatrix} 1 & ad^{-1}x \\ 0 & 1 \end{bmatrix}.$$

Finally, we can just replace E by $E(\mu_p)$ to get the result in the desired form.

1.5. *Alternative explanation bypassing the construction of E.* It is easily checked that b is a 1-cocycle in $Z^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathbb{F}(\chi^{1-k}))$, and hence gives a cohomology class in $\mathrm{H}^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathbb{F}(\chi^{1-k}))$. In fact, b is nonzero due to (c). The inflation-restriction sequence gives

$$0 \to \mathrm{H}^1(\Delta, \mathbb{F}(\chi^{1-k})) \to \mathrm{H}^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathbb{F}(\chi^{1-k})) \to \mathrm{H}^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_p)), \mathbb{F}(\chi^{1-k}))^{\Delta}.$$

Note that $\mathrm{H}^1(\Delta, \mathbb{F}(\chi^{1-k})) = 0$ since $|\Delta|$ is prime to p. As $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_p))$ acts trivially on $\mathbb{F}(\chi^{1-k})$, b gives rise to a nonzero Δ-equivariant homomorphism $h\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_p)) \to \mathbb{F}(\chi^{1-k})$. We have $\overline{\rho}|_{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_p))} = \begin{bmatrix} 1 & h \\ 0 & 1 \end{bmatrix}$, and that $h|_{D \cap \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_p))} = 0$ from (d). Therefore, h is unramified and factors through the class group A by class field theory. Since $\mathbb{F}$ has characteristic p, it further factors through $C = A \otimes_{\mathbb{Z}} \mathbb{F}_p$ and gives a nonzero map $C \to \mathbb{F}(\chi^{1-k})$. Due to Δ-equivariance, this factors through $C(\chi^{1-k})$ and thus implies $C(\chi^{1-k}) \neq 0$.

2 Reductions of p-adic representations

Let K be a finite extension of $\mathbb{Q}_p$ with integer ring $\mathcal{O}_K$, uniformizer π, and residue field $\mathbb{F}$. Let V be a two-dimensional K-vector space. A lattice Λ is a free $\mathcal{O}$-submodule of V such that $\Lambda \otimes_{\mathcal{O}} K = V$.

2.1. Lemma. — *Let F be a nonarchimedian local field, G a profinite group, and $\rho\colon G \to \mathrm{GL}_d(F)$ a continuous representation. Then ρ stabilizes some lattice. In other words, ρ can be conjugated to a representation with values in $\mathrm{GL}_d(\mathcal{O}_F)$.*

Proof. Choose a basis and consider the standard lattice $L = \mathcal{O}_F^{\oplus d}$. The stabilizer of L is precisely $\mathrm{GL}_d(\mathcal{O}_F)$, which is open in $\mathrm{GL}_d(F)$. Set $H = \rho^{-1}(\mathrm{GL}_d(\mathcal{O}_F))$, an open subgroup. Then G/H is finite and G stabilizes $\sum_{g \in G/H} gL$. □

Let $\rho\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(V)$ be a Galois representation. For a stable lattice T, we have the associated **reduction**, $\overline{\rho}\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(T/\pi T)$. It is a consequence of Brauer-Nesbitt theorem that the semisimplification of the reduction doesn't depend on the choice of T. When $\overline{\rho}$ is reducible, their semisimplification is described by two Galois character φ_1, φ_2 which depend only on ρ.

2.2. Ribet's lemma. — *Suppose that the K-representation ρ is simple but that its reductions are reducible. Let φ_1 and φ_2 be the associated Galois characters. Then G leaves stable some lattice $\Lambda \subset V$ for which the associated reduction is of the form* $\begin{bmatrix} \varphi_1 & \star \\ 0 & \varphi_2 \end{bmatrix}$ *but not semisimple.*

Proof. See [Rib76, §2.1] or [Eri08, §5.2]. □

3 A congruence between a cusp form and an Eisenstein series

Let ε be a nontrivial character with $\varepsilon(-1) = 1$. We consider modular forms on $\Gamma_1(p)$. Consider

$$\begin{aligned} G_{2,\varepsilon} &= L(-1,\varepsilon)/2 + \sum_{n \geqslant 1} \sum_{d \mid n} \varepsilon(d) d q^n, \\ G_{1,\varepsilon} &= L(0,\varepsilon)/2 + \sum_{n \geqslant 1} \sum_{d \mid n} \varepsilon(d) q^n, \\ s_{2,\varepsilon} &= \sum_{n \geqslant 1} \sum_{d \mid n} \varepsilon(n/d) d q^n. \end{aligned}$$

The first two are Eisenstein series of weights 2 and 1 respectively, and $s_{2,\varepsilon}$ is the unique semicusp[1] eigenform which is not a cusp form. All these are eigenforms away from p and have Nebentypus ε. For any prime $\mathfrak{p}$ of $\mathbb{Q}(\mu_{p-1})$ lying above p there is a Teichmüller lift $\omega\colon \mathbb{F}_p^\times \to \mu_{p-1}$. It satisfies $\omega(d) \equiv d \pmod{\mathfrak{p}}$ for each $d \in \mathbb{F}_p^\times$.

3.1. Lemma. — *Let $k \in [2, p-3]$ be even. Then $G_{2,\omega^{k-2}}$ and $G_{1,\omega^{k-1}}$ have $\mathfrak{p}$-integral Fourier expansions in $\mathbb{Q}(\mu_{p-1})$ which are congruent modulo $\mathfrak{p}$ to E_k.*

Sketch. This is easy to see for the nonconstant terms. For the constant coefficient, one easily gets the result by apply known congruences about Bernoulli numbers. Omitted. □

3.2. Lemma. — *Let $k \in [2, p-3]$ be even. Then there exists a modular form g of weight 2 and type ω^{k-2} whose Fourier coefficients are $\mathfrak{p}$-integral and the constant term is* 1.

Sketch. We use Lemma 3.1. If $p \nmid B_k$ then take $G_{2,\omega^{k-2}}$. Otherwise, consider the products $G_{1,\omega^{n-1}} G_{1,\omega^{m-1}}$ for even $m, n \in [2, p-3]$ such that $n + m \equiv k \pmod{p-1}$. If none of these work then p divides at least $(p-1)/4$ many of $B_2, B_4, \ldots, B_{p-3}$. It turns out that this implies that the p-adic valuation of the negative part h_p^- of the class number of $\mathbb{Q}(\mu_p)$ is at least $(p-1)/4$. This is a contradiction due to size reasons. □

[1] A semicusp form is a modular form whose constant coefficient is 0.

3.3. Proposition. — *Suppose $p \mid B_k$. There exists a normalized cuspidal newform $f = \sum_{n\geqslant 1} a_n q^n$ of weight 2, level p, and Nebentypus ω^{k-2}, and a prime $\mathfrak{p}$, lying above p, of the number field K_f generated by the coefficients a_n such that for each prime $\ell \neq p$, the coefficient a_ℓ is $\mathfrak{p}$-integral and $a_\ell \equiv 1+\ell^{k-1} \equiv 1+\omega^{k-2}(\ell)\ell \pmod{\mathfrak{p}}$.*

Sketch. Consider $f = G_{2,\omega^{k-2}} - cg$ where c is the constant coefficient of $G_{2,\omega^{k-2}}$. Then $f \equiv G_{2,\omega^{k-2}} \equiv E_k \pmod{\mathfrak{p}}$. So f is a mod $\mathfrak{p}$ eigenform away from p with eigenvalue $1+\omega^{k-2}(\ell)\ell$ for the Hecke operator T_ℓ, $\ell \neq p$. The *Deligne-Serre lifting lemma* produces a semi cusp form (of level p), which we again denote by f, satisfying the conditions in the statement of the result. However, we want a cusp form. We know that $s_{2,\omega^{k-2}}$ has eigenvalue $\omega^{k-2}(\ell)+\ell$. Thus, $f \neq s_{2,\omega^{k-2}}$ as ω^{k-2} is nontrivial, and f must be cuspidal. Normalize f. I claim that f must be a newform, and hence an eigenvalue for all Hecke operators. Indeed, if f were old, it must come from a modular form on $\mathrm{SL}_2(\mathbb{Z})$ since we are working at a prime level. This is not possible because there are no nonzero weight 2 forms on $\mathrm{SL}_2(\mathbb{Z})$. □

4 The Galois representation

We retain notations of Proposition 3.3. In addition, let $\mathcal{O}$ be the integer ring of K_f, $K_{f,\mathfrak{p}}$ the completion of K_f at $\mathfrak{p}$, $\mathcal{O}_\mathfrak{p}$ the integer ring of $K_{f,\mathfrak{p}}$, and $\mathbb{F}$ the residue field at $\mathfrak{p}$, and $\chi\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{Z}_p^\times \hookrightarrow K_{f,\mathfrak{p}}^\times$ be the p-adic cyclotomic character. Let A be the abelian variety attached to f. It is a quotient of the modular Jacobian variety. Define $V_f = T_p(A) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ where $T_p(A)$ is the p-adic Tate module of A. It is also dual to the p-adic étale cohomology group $H^1_{\text{ét}}(A, \mathbb{Q}_p)$. Finally, let $V_{f,\mathfrak{p}} = V_f \otimes_{K_f \otimes \mathbb{Q}_p} K_{f,\mathfrak{p}}$ and $\rho_{f,\mathfrak{p}}\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(V_{f,\mathfrak{p}})$ be the p-adic Galois representation attached to f at $\mathfrak{p}$. We show that it has a reduction satisfying the conditions of Theorem 1.4.

4.1. Proposition. — *The representation $\rho_{f,\mathfrak{p}}$ is irreducible.*

Proof. See [Rib76, §4.1] or [Eri08, §5.5]. □

4.2. Proposition. — *There exists a Galois stable $\mathcal{O}_\mathfrak{p}$-lattice $\Lambda \subset V_{f,\mathfrak{p}}$ for which the action of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *on $\Lambda/\pi\Lambda$ can be described in terms of matrices as* $\begin{bmatrix} 1 & \star \\ 0 & \chi^{k-1} \end{bmatrix}$ *and is furthermore not semisimple.*

Sketch. By Ribet's lemma 2.2, it suffices to find a Galois stable lattice whose reduction is reducible and whose semisimplication is $1 \oplus \chi^{k-1}$. In fact, we may choose any stable lattice (such lattice exists because a finite dimensional p-adic representation of a compact group always stabilizes a lattice). We know that $\mathrm{Trace}(\mathrm{Frob}_\ell) = a_\ell$ and $\det(\mathrm{Frob}_\ell) = \ell\varepsilon(\ell)$ for $\ell \neq p$ by the Eichler-Shimura relations. By Proposition 3.3, these numbers are congruent to $\ell^{k-1}+1$ and ℓ^{k-1} modulo $\mathfrak{p}$, respectively. Since Frobenius elements topologically generate the absolute Galois group the trace and determinant must be $1+\chi^{k-1}$ and χ^{k-1} respectively. By the Brauer-Nesbitt theorem, we are done. □

Fix such a lattice Λ and set $M = \Lambda/\pi\Lambda$. This will be our $\overline{\rho}$ of Theorem 1.4. From Proposition 4.2, it is clear that parts (b) and (c) are satisfied. Part (a) is a consequence of the fact that A acquires good reduction away from p. What remains is to check that the image under $\overline{\rho}$ of a decomposition group, say D', of p in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ has order prime to p. Note that $\mathbb{Q}(\mu_p)/\mathbb{Q}$ is totally ramified at p. Denote $\mathbb{Q}(\mu_p)^+ := \mathbb{Q}(\mu_p) \cap \mathbb{R} = \mathbb{Q}(\cos 2\pi/p)$. It is a theorem of Deligne-Rapoport [DR72] that A acquires good reduction everywhere over $\mathbb{Q}(\mu_p)^+$. Since p is prime to $[\mathbb{Q}(\mu_p)^+ : \mathbb{Q}]$, it suffices to show that the iamge of $D := D' \cap \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_p)^+)$ under $\overline{\rho}$ is of order prime to p. We note that D is a decomposition group in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_p)^+)$ of the unique prime of $\mathbb{Q}(\mu_p)^+$ lying above p. Denote by E the completion of $\mathbb{Q}(\mu_p)^+$ at

p. One can identify D with the local Galois group $\mathrm{Gal}(\overline{E}/E)$. In what follows, all structure morphisms of schemes are finite type.

4.3. Definition. Let R be a Dedekind domain with fraction field K and A an abelian variety over K. Then a **Néron model** $\mathcal{A}$ is a smooth commutative group over R whose generic fiber is A which is universal in the following sense: if X_R is smooth over R then any K-morphism $X_R \times_R K \to A_K$ can be extended to a unique R-morphism $X_R \to \mathcal{A}$.

The universal property tells us that if a Néron model exists then it is unique up to unique isomorphism. Néron models of abelian varieties always exist, see [CS86, §VIII].

4.4. Definition. Let R be a Dedekind domain with fraction field K. Let G be a commutative group scheme over R. Then $G(K^{\mathrm{sep}})$ is naturally a $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-module, called the **Galois module attached to** G.

4.5. Proposition. — *The $\mathrm{Gal}(\overline{E}/E)$-module M is the Galois module attached to a finite flat commutative group scheme killed by p over the integer ring $\mathcal{O}_E$ of E.*

Proof. Let A be the abelian variety attached to f which induces $\rho_{f,\mathfrak{p}}$. There is an inclusion $K_f \hookrightarrow \mathrm{End}_{\mathbb{Q}} A \otimes_{\mathbb{Z}} \mathbb{Q}$ given by the Hecke action on A. Change A by a $\mathbb{Q}$-isogeny so that $\mathcal{O}_{K_f} \subseteq \mathrm{End}_{\mathbb{Q}} A$. Indeed, we have

$$\mathrm{Hom}_{\mathbb{Q}}(A,B) \otimes_{\mathbb{Z}} \mathbb{Q} \cong \operatorname{colim}_{\substack{A' \to A \\ \text{isogeny}}} \mathrm{Hom}_{\mathbb{Q}}(A',B)$$

for any abelian $\mathbb{Q}$-varieties A, B. This is actually a general fact about localization of categories [Stacks, Tag 05Q5]. Then M is isomorphic to $A[\mathfrak{p}] = \{a \in A \colon ha = 0 \text{ for all } h \in \mathfrak{p}\}$, the "kernel of $\mathfrak{p}$", as a Galois module. To see this, recall that the p-adic Tate module $T_p(A)$ is an $\mathcal{O}_{K_f} \otimes_{\mathbb{Z}} \mathbb{Z}_p$-module in a Galois-compatible fashion. Since $\mathcal{O}_{K_f} \otimes_{\mathbb{Z}} \mathbb{Z}_p = \prod_{\mathfrak{p}|p} \mathcal{O}_{K_f,\mathfrak{p}}$, it follows that there is a Galois-equivariant decomposition

$$T_p(A) = \bigoplus_{\mathfrak{p}|p} T_{\mathfrak{p}}(A),$$

where $T_{\mathfrak{p}}(A) := T_p(A) \otimes_{\mathcal{O}_{K_f} \otimes_{\mathbb{Z}} \mathbb{Z}_p} \mathcal{O}_{K_f,\mathfrak{p}}$ is an $\mathcal{O}_{K_f,\mathfrak{p}}$-module. Here, $T_{\mathfrak{p}}(A) \otimes K_{f,\mathfrak{p}}$ is in fact $V_{f,\mathfrak{p}}$. In particular, the lattice Λ of Proposition 4.2 is essentially a "conjugate" of $T_{\mathfrak{p}}(A)$ in $V_{f,\mathfrak{p}}$. Lastly, we obtain that $T_{\mathfrak{p}}(A) = \lim_n A[\mathfrak{p}^n]$ from

$$T_p(A) = \lim_n A[p^n] = \lim_n A\left[\prod_{\mathfrak{p}|p} \mathfrak{p}^{v_{\mathfrak{p}}(p)n}\right] = \bigoplus_{\mathfrak{p}|p} \lim_n A[\mathfrak{p}^{v_{\mathfrak{p}}(p)n}] = \bigoplus_{\mathfrak{p}|p} \lim_n A[\mathfrak{p}^n]$$

and applying $(-) \otimes_{\mathcal{O}_{K_f} \otimes_{\mathbb{Z}} \mathbb{Z}_p} \mathcal{O}_{K_f,\mathfrak{p}}$ to both sides. Of course, here we are using that $A[fg] = A[f] \oplus A[g]$ for $f, g \in \mathrm{End}_{\mathbb{Q}} A$ such that $(f,g) = (1)$. Since $\mathfrak{p} \mid p$, M is a submodule, say M', of the p-torsion subgroup $A[p]$. We know that there is a Néron model $\mathcal{A}$ for A over $\mathcal{O}_E$ by Deligne-Rapoport's result [DR72]. Therefore, M' is the Galois module attached to the scheme-theoretic p-torsion $\mathcal{A}[p]$, which is a finite flat commutative group scheme over $\mathcal{O}_E$ simply because isogenies are finite flat. Define $\mathcal{M}$ to be the scheme-theoretic closure of M in $\mathcal{A}[p]$. Then $\mathcal{M}$ is a finite flat commutative group scheme, killed by p, over $\mathcal{O}_E$ with attached Galois module M (c.f. Lemma 4.6). Indeed, $M = (\mathcal{M} \times_{\mathcal{O}_E} E)(\overline{E})$ holds because M is just a finite set of closed points as a subset of A. □

4.6. Lemma. — *Let R be a DVR with fraction field K. Let X be an R-scheme and Y_K be a closed subscheme of $X_K = X \times_R K$. Then the scheme-theoretic closure of Y_K in X, say Y, is flat over R.*

Proof. Without any loss of generality, assume $X = \operatorname{Spec} A$. Suppose X_K is cut out by the ideal I in $A \otimes_R K$. Then the closure is cut out by $I \cap A$ in A. If $A/I \cap A$ has R-torsion, say $ra \in I \cap A$ for some $r \in R \setminus \{0\}$ and $a \in A \setminus (I \cap A)$, then $a \otimes 1 \in I$, which implies $a \in I \cap A$. We are now done because flatness is same as torsion-free for PIDs. □

4.7. *Remark.* Using the notations of the above lemma, if X is an R-group scheme and Y_K is a closed subgroup of X_K then Y, the scheme-theoretic closure of Y_K in X, is a closed R-subgroup of X. This is easily checked affine-locally by rewriting things in terms of Hopf algebras.

4.8. Definition. A commutative group scheme G over a base S is said to be an **$\mathbb{F}$-module scheme** if there is an injection $\mathbb{F} \hookrightarrow \operatorname{End}_S G$. This is same as saying $\operatorname{Mor}_S(-,G)$ is a functor valued in $\mathbb{F}$-vector spaces.

The $\mathcal{M}$ obtained in the proof of Proposition 4.5 is an $\mathbb{F}$-module scheme where $\mathbb{F}$ is the residue field of $\mathcal{O}_E$. Indeed, it follows from the universal property of Néron models that $\mathcal{O}_E \hookrightarrow \operatorname{End}_{\mathcal{O}_E} \mathcal{A}$. The $\mathbb{F}$-action is then induced from $\mathbb{F} \hookrightarrow \operatorname{End}_{\mathcal{O}_E} \mathcal{A}[p]$. Of course, $\mathfrak{p}$-torsion points remain $\mathfrak{p}$-torsion under the action of an endomorphism. Thus, there is an action of $\mathbb{F}$ on $\mathcal{M}$ by $\mathcal{O}_E$-automorphisms. Let us summarise what we have obtained so far–

(a) $\mathcal{M}$ is a finite flat $\mathbb{F}$-module scheme over $\mathcal{O}_E$ with the attached Galois module $M = \mathcal{M}(\overline{\mathbb{Q}}_p)$ of dimension 2 as an $\mathbb{F}$-vector space.
(b) D acts trivially on a 1-dimensional subspace X of M and via the character χ^{k-1} on the quotient $Y = M/X$.

4.9. Theorem. — *The image of D in* $\operatorname{Aut} M$ *has order prime to p.*

We will need the following two results in the proof of Theorem 4.9:

4.10. Theorem (Raynaud [Ray74]). — *Suppose $E/\mathbb{Q}_p$ is an extension of local fields with ramification index less than $p-1$. Let G be a finite flat commutative group scheme over E which is killed by a power of p. Then there is at most one finite flat extension of G to $\mathcal{O}_E$.*

Proof. See [Ray74, Theorem 3.3.3], [CSS97, Chapter 5, §4], [Sno], or [Ed92, §5]. □

4.11. Lemma. — *Let $E/\mathbb{Q}_p$ be a finite extension of local fields and X a finite étale scheme over $\mathcal{O}_E$. Then the* $\operatorname{Gal}(\overline{E}/E)$*-action on $X(\overline{\mathbb{Q}}_p)$ is unramified.*

Proof. Indeed, the $\operatorname{Gal}(\overline{E}/E)$-action on $X(\overline{\mathbb{Q}}_p)$ factors through a finite quotient of $\pi_1^{\text{ét}}(\operatorname{Spec} \mathcal{O}_E) = \operatorname{Gal}(E^{\text{unr}}/E)$ by the very definition of the étale fundamental group. □

4.12. *Proof of Theorem 4.9.* Let $\mathcal{X}$ be the scheme-theoretic closure of X in $\mathcal{M}$. Then X is the Galois module attached to $\mathcal{X}$. By Theorem 4.10 and Lemma 4.6, it follows that $\mathcal{X}$ is a (nonzero) constant group scheme over $\mathcal{O}_E$. In particular, $\mathcal{X}$ is a proper, nontrivial étale subgroup. Hence, $\mathcal{M}$ cannot be connected. The *connected-étale sequence* [CSS97, §V.3.7] states

$$0 \to \mathcal{M}_E^{\circ} \to \mathcal{M}_E \to \mathcal{M}_E^{\text{ét}} \to 0,$$

where $\mathcal{M}_E^{\circ}$ is the (geometrically) connected component of $\mathcal{M}_E$ containing 0 and $\mathcal{M}_E^{\text{ét}}$ the largest étale quotient. It is not hard to see that the above sequence is an exact sequence of $\mathbb{F}$-module schemes and the maps therein are defined over E. Taking $\overline{\mathbb{Q}}_p$-points, we get a sequence of D-representations

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

Now, M° cannot be all of M because $\mathcal{M}$ is not connected. Further, $M^{\circ} \neq 0$ because $M^{\text{ét}}$ is unramified as a Galois module (Lemma 4.11) but M is not. Therefore, $\dim_{\mathbb{F}} M^{\circ} = \dim_{\mathbb{F}} M^{\text{ét}} = 1$. Since $M^{\text{ét}}$ is unramified and Y isn't, the image of M° in M must be distinct from X. Hence, D stabilizes X and the image of M°. It is easily verified that any element of order p in $\operatorname{Aut} M$ leaves stable a unique line. This completes the proof. □

References

[CS86] G. Cornell and J. H. Silverman, *Arithmetic Geometry*, Springer-Verlag New York, 1986

[CSS97] G. Cornell, J. H. Silverman, and G. Stevens, *Modular forms and Fermat's Last Theorem*, Springer-Verlag, New York, 1997

[DR72] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, International Summer School on Modular Functions, Antwerp 1972

[Ed92] B. Edixhoven, *The weight in Serre's conjectures on modular forms*, Invent. Math. **109**, 563-594, 1992

[Eri08] C. Wang-Erickson, *Ribet's converse to Herbrand's theorem*, https://sites.pitt.edu/~caw203/pdfs/ribet2.pdf

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

[Rib76] K. Ribet, *A modular construction of unramified* p*-extension of* $\mathbb{Q}(\mu_p)$, Invent. Math. **34**, 151-162, 1976

[Sai09] A. Saikia. *Ribet's construction of a suitable cusp eigenform*, arXiv:0910.1408v2, 2009

[Sno] A. Snowden, *Course on Mazur's theorem*, Lecture 7: Raynaud's theorem, http://www-personal.umich.edu/~asnowden/teaching/2013/679/L07.html

[Stacks] The Stacks project authors, *The Stacks project*, https://stacks.math.columbia.edu, 2023