ADJOINT LIFTS AND MODULAR ENDOMORPHISM ALGEBRAS

DEBARGHA BANERJEE AND EKNATH GHATE

Abstract. We prove that the ramification of the endomorphism algebra of the Grothendieck motive attached to a non-CM cuspform of weight two or more is completely determined by the slopes of the adjoint lift of this form, when the slopes are finite. We treat all places of good and bad reduction, answering a question of Ribet about the Brauer class of the endomorphism algebra in the finite slope case.

1. Introduction

Let $f = \sum_{n=1}^{\infty} a_n q^n$ be a primitive non-CM cusp form of weight $k \geq 2$, level $N \geq 1$ and character ϵ, and let M_f be the motive attached to f. If f has weight 2, M_f is the abelian variety attached to f by Shimura [Sh71], and for weights larger than 2, M_f is the Grothendieck motive attached to f by Scholl in [Sc90]. In all cases, M_f is a pure motive of rank 2, weight $k-1$, with coefficients in the Hecke field $E = \mathbb{Q}(a_n)$ of f. Let $\mathrm{End}(M_f)$ denote the ring of endomorphisms of M_f defined over $\bar{\mathbb{Q}}$ and let

$$X_f = \mathrm{End}(M_f) \otimes_{\mathbb{Z}} \mathbb{Q}$$

be the $\mathbb{Q}$-algebra of endomorphisms of M_f. One knows that X_f is a central simple algebra over a subfield F of E, and that the class of X_f in the Brauer group $\mathrm{Br}(F)$ of F is 2-torsion. Ribet has remarked that it seems difficult to describe this class by pure thought. The goal of this paper is to give a complete description of the class of X_f in terms of the slopes of a functorial lift of f, under a finiteness hypothesis on these slopes.

That X_f is a central simple algebra over F follows from an explicit structure theorem for X_f which shows that X_f is isomorphic to a crossed product algebra. Let $\Gamma \subset \mathrm{Aut}(E)$ be the group of extra twists of f. Recall that a pair (γ, χ_γ), where $\gamma \in \Gamma \subset \mathrm{Aut}(E)$ and χ_γ is an E-valued Dirichlet character, is called an extra twist for f if $f^\gamma = f \otimes \chi_\gamma$, i.e., $a_p^\gamma = a_p \cdot \chi_\gamma(p)$, for all primes $p \nmid N$. Define the E-valued Jacobi sum 2-cocycle c on Γ by

$$c(\gamma, \delta) = \frac{G(\chi_\delta^{-\gamma}) G(\chi_\gamma^{-1})}{G(\chi_{\gamma \cdot \delta}^{-1})} \in E,$$

for γ, $\delta \in \Gamma$, where $G(\chi)$ is the usual Gauss sum attached to the character χ. Let X be the corresponding crossed product algebra defined by:

$$X = \bigoplus_{\gamma \in \Gamma} E \cdot x_\gamma, \tag{1.1}$$

where the x_γ are formal symbols satisfying the relations

$$\begin{aligned} x_\gamma \cdot x_\delta &= c(\gamma,\delta)\cdot x_{\gamma\delta}, \\ x_\gamma \cdot e &= \gamma(e)\cdot x_\gamma, \end{aligned}$$

for γ, $\delta \in \Gamma$ and $e \in E$. Clearly X is a central simple algebra over F, the fixed field of Γ in E. A fundamental result due to Momose [Mo81] and Ribet [Ri80] in weight 2, and [BG04] (see also [GGQ05]) in higher weight, says that $X_f \cong X$. Moreover $F \subset E$ is known to be the subfield generated by $a_p^2\epsilon^{-1}(p)$, for primes $p \nmid N$.

To study the Brauer class of $X = X_f$, the standard exact sequence from classfield theory

$$0 \to {}_2\mathrm{Br}(F) \to \oplus_v\, {}_2\mathrm{Br}(F_v) \to \mathbb{Z}/2 \to 0,$$

where v runs over all places of F, shows that it is enough to study the class of $X_v = X \otimes_F F_v$ in $\mathrm{Br}(F_v)$, for each place v. It is well known that ${}_2\mathrm{Br}(F_v) \cong \mathbb{Z}/2$, including if v is infinite since F is totally real, and X_v is a matrix algebra over F_v if the class of X_v is trivial, and is a matrix algebra over a quaternion division algebra over F_v if the class of X_v is non-trivial. A theorem of Momose [Mo81] says that X is totally indefinite if k is even, and totally definite if k is odd, giving complete information about the Brauer class at the infinite places v. When v is a finite place, we shall prove in this paper that the class of X_v in $\mathrm{Br}(F_v)$ is completely determined in terms of the *parity* of the slope at v of the *adjoint lift* of f (when this slope is finite).

According to Langlands principle of functoriality, given two reductive algebraic groups H and G over $\mathbb{Q}$ and a homomorphism between their L-groups $u : {}^L\mathrm{H} \to {}^L\mathrm{G}$, there should be a way to lift cuspidal automorphic representations π of $\mathrm{H}(\mathbb{A}_\mathbb{Q})$ to cuspidal automorphic representation Π of $\mathrm{G}(\mathbb{A}_\mathbb{Q})$, so that the Langlands L-functions of π and Π are related by the formula $L(s,\Pi,r) = L(s,\pi,r\circ u)$. In the case that $\mathrm{H} = \mathrm{GL}_2$ and $\mathrm{G} = \mathrm{GL}_3$, and u is the adjoint map, it is (by now) a classical theorem of Gelbart and Jacquet [GJ78] that every cuspidal automorphic form π on $\mathrm{GL}_2(\mathbb{A}_\mathbb{Q})$ has a lift $\mathrm{ad}(\pi)$, called the Gelbart-Jacquet adjoint lift, to an automorphic representation of $\mathrm{GL}_3(\mathbb{A}_\mathbb{Q})$. If the Satake parameters at an unramified prime p of π are α_p and β_p, then the Satake parameters of the adjoint lift $\mathrm{ad}(\pi)$ are $\frac{\alpha_p}{\beta_p}, 1, \frac{\beta_p}{\alpha_p}$.

Let now $\pi = \pi_f$ be the automorphic representation attached to the non-CM form f as above, and let $\mathrm{Ad}(\pi) = \mathrm{ad}(\pi) \oplus 1$ be the automorphic form on $\mathrm{GL}_4(\mathbb{A}_\mathbb{Q})$ obtained from the Gelbart-Jacquet adjoint lift by adding the trivial representation. Finally let

$$\Pi = \mathrm{Ad}(\pi)(k-1)$$

be the automorphic representation on $\mathrm{GL}_4(\mathbb{A}_\mathbb{Q})$ obtained by taking the $(k-1)$-st twist of $\mathrm{Ad}(\pi)$.

The following meta-theorem may be considered as a summary of all the results of this paper.

Theorem 1. *If v is a finite place of F, then the class of X_v in $\mathrm{Br}(F_v)$ is determined by the parity of the slope $m_v \in \mathbb{Z} \cup \{\infty\}$ of Π at v, when this slope is finite.*

Before we proceed further, we wish to remark that the theorem above is another instance of a recurring theme in the theory of the arithmetic of automorphic forms, wherein arithmetic information about an object attached to a form (in this case the endomorphism algebra) is contained in the Fourier coefficients of a suitable lift of the original form (in this case the twisted adjoint lift). The most striking example of this theme occurs in the correspondence between forms of even integral weight k and forms of half-integral weight $(k+1)/2$ as in [Sh73], [Wa81], [KZ91]. Here, twisted central critical L-values of the original form on PGL_2 occur as Fourier coefficients of the Shimura-Shintani-Waldspurger lift of this form to the metaplectic group $\widetilde{\mathrm{SL}}_2$. The meta-theorem above establishes another instance where this theme is played out.

The slope m_v of Π at a place $v \mid p$ of F in Theorem 1 is defined to be a suitably normalized v-adic valuation of the trace of Frobenius at p in the Galois representation corresponding to Π. In general, the trace depends on a choice of Frobenius, but is independent of this choice for primes of semistable reduction. Equivalently, on the automorphic side, the slope m_v may also be defined as a suitably normalized v-adic valuation of the sum of certain parameters coming from the local automorphic representation of Π at p. Though the shape of the trace of Frobenius, or the shape of the specific parameters, vary in different cases, they can be made completely precise. As a result we obtain various explicit versions of the above meta-theorem which we state now.

For instance, suppose that $v \mid p$ with $p \nmid N$, so that π_p is an unramified representation. Then the slope m_v of Π at v is the (normalized) v-adic valuation of the sum of the Satake parameters of Π_p. Since $\mathrm{Ad}(\pi)$ has Satake parameters $\frac{\alpha_p}{\beta_p}, 1, \frac{\beta_p}{\alpha_p}, 1$, we have

$$\begin{aligned} m_v &:= [F_v : \mathbb{Q}_p] \cdot v\left((\frac{\alpha_p}{\beta_p} + 1 + \frac{\beta_p}{\alpha_p} + 1) \cdot p^{k-1} \right) = [F_v : \mathbb{Q}_p] \cdot v\left(\frac{(\alpha_p + \beta_p)^2}{\alpha_p \beta_p} \cdot p^{k-1} \right) \\ &= [F_v : \mathbb{Q}_p] \cdot v(a_p^2 \epsilon^{-1}(p)) \in \mathbb{Z} \cup \{\infty\}, \end{aligned}$$

where v is normalized so that $v(p) = 1$. We remark that F may be considered as the Hecke field of the adjoint lift Π, since it is generated by the quantities $a_p^2 \epsilon^{-1}(p)$, for $p \nmid N$. Moreover, the slope m_v of Π at v is an integer because of the local degree term $[F_v : \mathbb{Q}_p]$ (unless of course $a_p = 0$, in which case m_v is infinite). We prove (cf. Theorem 10):

Theorem 2 (Spherical case)**.** *Assume* $\gcd(p, N) = 1$. *Let v be a place of F lying over p. Assume $a_p \neq 0$. Then X_v is a matrix algebra over F_v if and only if* $m_v = [F_v : \mathbb{Q}_p] \cdot v(a_p^2 \epsilon(p)^{-1}) \in \mathbb{Z}$ *is even.*

The case $k = 2$ and $m_v = 0$ (good, ordinary reduction) is due to Ribet [Ri81]. The general case for odd primes, and for $p = 2$ when $F = \mathbb{Q}$, was proved in [BG04] and [GGQ05, Thm. 2.2], under a mild hypothesis. Here we include the case $p = 2$ for all F, and remove this hypothesis. The proof we give in this paper is much simpler, and was motivated by the recent proof of an analogous theorem for weight one forms [BG11] (this is also where the idea of using the adjoint lift in higher weight germinated).

However, the main point of this article is to treat completely the primes of bad reduction, i.e., the primes $v \mid p$ of F with $p \mid N$. Let $N_p \geq 1$ be the exponent of the exact power of p dividing N. Let C denote the conductor of ϵ and let $C_p \geq 0$ be the exponent of the exact power of p dividing C. Note $N_p \geq C_p$. Since $p \mid N$, we no longer have the Satake parameters of π_p at our disposal. However, we can replace these numbers by the corresponding eigenvalues of ℓ-adic Frobenius in the ℓ-adic Weil-Deligne representation corresponding to π_p, for $\ell \neq p$, or equivalently by [Sa97], with the eigenvalues of crystalline

Frobenius on the filtered (φ, N)-module attached to π_p as in [GM09], and can still compute the slope of Π at v.

For example, in the case that $N_p = 1$ and $C_p = 0$, it is well known that π_p is an unramified twist of the Steinberg representation. In this case, the eigenvalues of ℓ-adic Frobenius are nothing but $\alpha_p = a_p$ and $\beta_p = pa_p$, up to multiplication by the same constant. We thus have:

$$\begin{aligned} m_v &:= [F_v : \mathbb{Q}_p] \cdot v\left(\frac{(\alpha_p+\beta_p)^2}{\alpha_p\beta_p} \cdot p^{k-1}\right) \\ &= [F_v : \mathbb{Q}_p] \cdot (k-2) \in \mathbb{Z}. \end{aligned}$$

In Theorem 15 we prove:

Theorem 3 (Steinberg case)**.** *Suppose $v \mid p$ with $N_p = 1$ and $C_p = 0$. Then X_v is a matrix algebra over F_v if and only if $m_v = [F_v : \mathbb{Q}_p] \cdot (k-2) \in \mathbb{Z}$ is even.*

The proof of Theorem 3 uses the structure of the ℓ-adic Galois representation attached to f at p, for $\ell \neq p$, due to Langlands. The case $k = 2$ is due to Ribet [Ri81], who in fact showed that the algebra X is trivial in the Brauer group of F, using the fact that the corresponding residual abelian variety has toric reduction. Ribet's result was extended to forms of even weight k in [BG04, Thm. 1.0.6]. In this paper examples were also given of forms of odd weight for which the endomorphism algebra is ramified at Steinberg primes. The above theorem gives a complete criterion for the ramification of X at Steinberg primes in all weights k.

We now turn to the very interesting case when $N_p = C_p \geq 1$ and π_p is in the ramified principal series. The behaviour of the local Brauer class in this case is mysterious, but has now become possible to treat using the adjoint lift. The eigenvalues of ℓ-adic or crystalline Frobenius are not well-defined in this case since the Weil-Deligne parameter corresponding to π_p is ramified. However, one more or less canonical choice is $\alpha_p = a_p$ and $\beta_p = \bar{a}_p\epsilon'(p)$, where we decompose $\epsilon = \epsilon' \cdot \epsilon_p$ into its prime-to-p conductor and p-power conductor parts. We then have:

$$\begin{aligned} m_v &:= [F_v : \mathbb{Q}_p] \cdot v\left(\frac{(\alpha_p+\beta_p)^2}{\alpha_p\beta_p} \cdot p^{k-1}\right) \\ &= [F_v : \mathbb{Q}_p] \cdot v(a_p^2\epsilon'(p)^{-1} + 2p^{(k-1)} + \bar{a}_p^2\epsilon'(p)) \in \mathbb{Z} \cup \{\infty\}. \end{aligned}$$

It can be checked that the three term expression in the last line above is indeed an element of F. It is clearly fixed by complex conjugation; it is in fact fixed by all elements of Γ (cf. Lemma 16). Note again that $m_v \in \mathbb{Z}$ (unless it is infinite). In view of the two previous theorems, one might conjecture:

(??) If $m_v < \infty$, then X_v is a matrix algebra over F_v if and only if m_v is even.

We prove that (??) is essentially true. In particular, when the slopes of α_p and β_p are unequal, or equivalently, when $m_v < [F_v : \mathbb{Q}_p] \cdot (k-1)$, we prove (in Theorem 22, for odd primes p, and in Theorem 27, for $p = 2$) that:

Theorem 4 (Ramified principal series unequal slope case)**.** *Assume that $v \mid p$ and $N_p = C_p \geq 1$. Suppose $m_v < [F_v : \mathbb{Q}_p] \cdot (k-1)$. Then X_v is a matrix algebra over F_v if and only if*

$$m_v = [F_v : \mathbb{Q}_p] \cdot v\left(\frac{a_p^2}{\epsilon'(p)} + 2p^{(k-1)} + \frac{\bar{a}_p^2}{\bar{\epsilon}'(p)}\right) \in \mathbb{Z}$$

is even.

We remark that while a partial result in the 'if' direction was proved in [GGQ05, Thm. 5.1], Theorem 4 gives complete information about the ramification of X_v in the unequal slope case.

When the slopes of α_p and β_p are the same, or equivalently, $m_v \geq [F_v : \mathbb{Q}_p] \cdot (k-1)$, the guess (??) is, somewhat surprisingly, false, even when $m_v < \infty$. Counterexamples are given in Examples 5-7 at the end of the paper. This is related to the fact that the eigenvalues of ℓ-adic Frobenius are not well-defined. To salvage the situation, we introduce two new quantities $m_v^{\pm}$, which may be thought of as replacements of m_v. Let e_v and f_v be the ramification index and residue degree of $v \mid p$, let G_v be the decomposition group of F at v, and set

$$m_v^{\pm} = e_v \cdot v((a_p^2 \epsilon'(p)^{-1})^{f_v} \pm 2p^{(k-1)f_v} + (\bar{a}_p^2 \epsilon'(p))^{f_v}) \in \mathbb{Z} \cup \{\infty\},$$

where v is normalized so the $v(p) = 1$. Again the three term expression lies in F, so $m_v^{\pm}$ are well-defined, and at least one of $m_v^{\pm}$ is finite. Then we prove (see Theorems 28, 30 and 32 for precise statements):

Theorem 5 (Ramified principal series equal slope case)**.** *Assume that $v \mid p$ and $N_p = C_p \geq 1$. Suppose $m_v \geq [F_v : \mathbb{Q}_p] \cdot (k-1)$.*

(1) *If p is odd and the tame part of ϵ_p is not quadratic on G_v, then X_v is a matrix algebra over F_v if and only if one of*

$$m_v^{\pm} = e_v \cdot v\left(\left(\frac{a_p^2}{\epsilon'(p)}\right)^{f_v} \pm 2p^{(k-1)f_v} + \left(\frac{\bar{a}_p^2}{\bar{\epsilon}'(p)}\right)^{f_v}\right) \in \mathbb{Z}$$

is even.

(2) *If $p = 2$ and ϵ_2 is not quadratic on G_v, there exists an integer n_v mod 2 depending only on ϵ_2 such that X_v is a matrix algebra over F_v if and only if one of*

$$m_v^{\pm} + n_v \in \mathbb{Z}$$

is even.

(3) *Finally, if p is odd and the tame part of ϵ_p is quadratic on G_v, or if $p = 2$ and ϵ_2 is quadratic on G_v, then there is an integer n_v mod 2 defined in terms of a Hilbert symbol $(t, d)_v$, with t depending only on ϵ_p and d on an explicit Fourier coefficient of f, such that X_v is a matrix algebra over F_v if and only if a particular choice of*

$$m_v^{\pm} + n_v \in \mathbb{Z}$$

is even.

In parts (1) and (2), $m_v^{\pm}$ have the same parity if both are finite (and if -1 lies in the image of ϵ_p). Also, the theorem reduces to the previous theorem when the slopes are unequal. Indeed the quantities $m_v^{\pm} = m_v$ coincide in the unequal slope case, since $e_v f_v = [F_v : \mathbb{Q}_p]$, and it turns out that $n_v = 0$ as well. Thus we may think of n_v as an error term to the truth of (??) in the equal slope case.

The above results give a complete answer to Ribet's question on the Brauer class of $X_f = X$ in the cases of finite slope. These results cover all forms f of square-free level, and more generally all forms f for which M_f has either semistable or crystabelian (crystalline over an abelian extension of $\mathbb{Q}$) reduction. The remaining finite places of bad reduction occur when $N_p > C_p$. In such cases $a_p = 0$ and even the slope of f is not finite. We hope to return to the infinite slope cases in subsequent work (for a weak result, see Proposition 33).

In closing, we note that although Theorems 2 through 5 are proved separately, there is the tantalizing possibility that there is a more uniform, conceptual proof of these results along the following lines. The Tate conjecture for the motive M_f says that the natural map $X_f \otimes \mathbb{Q}_\ell \to \mathrm{End}(M_\ell)^H$ is an isomorphism, for any prime ℓ, and for a sufficiently deep finite index subgroup H of the full Galois group $G_{\mathbb{Q}}$ (cf. [Ri80] and [GGQ05]). Here M_ℓ is the ℓ-adic realization of M_f. Now $G_{\mathbb{Q}}$ acts via the adjoint (conjugation) action on M_ℓ, so clearly the local algebra $X \otimes \mathbb{Q}_\ell$ and certain fixed points in the adjoint representation of M_ℓ are related. Moreover, Pink [Pi98] has shown that a compact subgroup of GL_n over a local field is essentially determined by its $\mathfrak{sl}_n$-adjoint representation. It would be interesting to see if these remarks can be made into a direct proof of Theorem 1.

2. Functoriality and the Adjoint Lift

We start by recalling a few more details about the adjoint lift mentioned above.

2.1. **Functoriality.** Let H and G be reductive algebraic groups defined over $\mathbb{Q}$, and let ${}^L\mathrm{H} = {}^L\mathrm{H}^0 \rtimes G_{\mathbb{Q}}$ and ${}^L\mathrm{G} = {}^L\mathrm{G}^0 \rtimes G_{\mathbb{Q}}$ be the corresponding L-groups. Let $u : {}^L\mathrm{H} \to {}^L\mathrm{G}$ be an L-homomorphism (this map is identity on the second factor). According to Langlands' principle of functoriality there should be a way to lift automorphic forms on $\mathrm{H}(\mathbb{A}_{\mathbb{Q}})$ to those on $\mathrm{G}(\mathbb{A}_{\mathbb{Q}})$, using the map u.

The lifting is in fact done locally. Let $G_p \subset G_{\mathbb{Q}}$ be the decomposition subgroup at the prime p. The corresponding local L-groups are ${}^L\mathrm{H}_p = {}^L\mathrm{H}^0 \rtimes G_p \subset {}^L\mathrm{H}$ and ${}^L\mathrm{G}_p = {}^L\mathrm{G}^0 \rtimes G_p \subset {}^L\mathrm{G}$. Let $u_p : {}^L\mathrm{H}_p \to {}^L\mathrm{G}_p$ be the local L-homomorphism obtained by restricting u on the second factor to G_p. We now define the local lift with respect to the local L-homomorphism u_p. Let π_p be an irreducible admissible representation of $\mathrm{H}(\mathbb{Q}_p)$, with parameter an admissible homomorphism $\phi_p : W_p' \to {}^L\mathrm{H}_p$, where W_p' is the Weil-Deligne group at p. The composition $\phi_p' = u_p \circ \phi_p$ is an admissible (if G is quasi-split) homomorphism of W_p' to ${}^L\mathrm{G}_p$. Then ϕ' (conjecturally) parametrises a local L-packet and the elements of this L-packet are the local functorial lifts Π_p of π_p.

Let now $\pi = \otimes' \pi_p$ be an irreducible automorphic representation of $\mathrm{H}(\mathbb{A}_{\mathbb{Q}})$. An automorphic representation $\Pi = \otimes' \Pi_p$ of $\mathrm{G}(\mathbb{A}_{\mathbb{Q}})$ is a weak functorial lift of π with respect to u, if for all but finitely many places p, Π_p is a local functorial lift of π_p with respect to u_p. Similarly, we call Π a strong functorial lift of π, if Π_p is a local functorial lift of π_p, for all places p. By definition, if Π is a weak lift of π then for all representations $r : {}^L\mathrm{G} \to \mathrm{GL}_n(\mathbb{C})$, we have the identity of partial Langlands L-functions

$$L_S(s, \pi, r \circ u) = L_S(s, \Pi, r),$$

where S is a finite set of places where we do not know how to locally lift π_p. Note $S = \emptyset$ if Π is a strong functorial lift of π.

2.2. **Adjoint lift.** Now suppose that $\mathrm{H} = \mathrm{GL}_2$ and $\mathrm{G} = \mathrm{GL}_3$ are defined over $\mathbb{Q}$. By definition, the connected parts of the corresponding L-groups are ${}^L\mathrm{H}^0 = \mathrm{GL}_2(\mathbb{C})$ and ${}^L\mathrm{G}^0 = \mathrm{GL}_3(\mathbb{C})$. The adjoint action of $\mathrm{GL}_2(\mathbb{C})$ on the Lie algebra of $\mathrm{SL}_2(\mathbb{C})$, namely the trace zero matrices of $\mathrm{M}_{2\times 2}(\mathbb{C})$, induces L-homomorphisms u, and u_p, for each prime p. On diagonal elements (of the first factor) the map u_p is easily checked to be given by

$$\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \mapsto \begin{pmatrix} \frac{\alpha}{\beta} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \frac{\beta}{\alpha} \end{pmatrix}.$$

By a classical theorem of Gelbart and Jacquet [GJ78], every automorphic representation of H has a strong lift to G. If $\pi = \pi_f$ is the automorphic representation of $\mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}})$ corresponding to $f \in S_k(N, \epsilon)$, let $\mathrm{ad}(\pi)$ denote the automorphic lift to $\mathrm{G}(\mathbb{A}_{\mathbb{Q}})$. The image of arithmetic Frobenius Frob_p at p under ϕ_p is of the form

$$\left(\begin{pmatrix} \alpha_p & 0 \\ 0 & \beta_p \end{pmatrix}, \mathrm{Frob}_p\right).$$

If $p \nmid N$ is an unramified prime, α_p and β_p are the Satake parameters of π_p. Then by definition of u_p it is clear that the image of Frob_p under ϕ'_p is a diagonal matrix with entries $\frac{\alpha_p}{\beta_p}, 1, \frac{\beta_p}{\alpha_p}$ (on the first factor, and just Frob_p on the second factor).

It is more convenient to work with $\Pi = (\mathrm{ad}(\pi) \oplus 1)(k-1)$, the $(k-1)$-th twist of the automorphic representation on $\mathrm{GL}_4(\mathbb{A}_{\mathbb{Q}})$ obtained by adding the trivial representation to $\mathrm{ad}(\pi)$. We define the slope m_v of Π at $v \mid p$ to be

$$m_v := [F_v \cdot \mathbb{Q}_p] \cdot v(t_p),$$

where v is normalized so that $v(p) = 1$ and $t_p \in F$ is defined to be the sum of the four parameters of Π_p, namely

$$t_p = \left(\frac{\alpha_p}{\beta_p} + 1 + \frac{\beta_p}{\alpha_p} + 1\right) \cdot p^{k-1} = \frac{(\alpha_p + \beta_p)^2}{\alpha_p \beta_p} \cdot p^{k-1}.$$

We note that t_p can be computed easily in various cases. When $p \nmid N$ an easy check shows

$$t_p = \frac{a_p^2}{\epsilon(p)}.$$

When $p \mid N$ and $N_p = 1$ and $C_p = 0$, it is known that $\alpha_p = a_p$ and $\beta_p = pa_p$ (up to multiplication by a constant), and so

$$t_p = p^{k-2}(p+1)^2.$$

Finally, if $N_p = C_p$, then a natural choice is $\alpha_p = a_p$ and $\beta_p = \bar{a}_p \epsilon'(p)$ (again up to multiplication by a constant), so

$$t_p = \frac{{a_p}^2}{\epsilon'(p)} + 2p^{k-1} + \frac{\bar{a}_p^2}{\bar{\epsilon}'(p)},$$

noting $|a_p|^2 = p^{k-1}$. In fact the Weil Deligne parameter in this case is ramified at p, so there are other choices for α_p and β_p and hence for t_p. This causes some complications in the statements and the proofs of results in this case.

2.3. **Galois representations.** All the above formulas can be computed on the Galois side as well. Let $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(E_\lambda)$ be an ℓ-adic Galois representation attached by Deligne to f, for a prime $\lambda \mid \ell$ of E with $\ell \neq p$. Let $\lambda(x)$ be the unramified character which takes arithmetic Frobenius Frob_p to $x \in E_\lambda$.

Theorem 6 (Langlands)**.** *The local behaviour of $\rho_f|_{G_p}$ at a decomposition group G_p at p is as follows.*

- *If $p \nmid N$, let α_p and β_p be roots of the polynomial $x^2 - a_p x + \epsilon(p)p^{k-1}$. Then*
$$\rho_f|_{G_p} \sim \begin{pmatrix} \lambda(\beta_p) & 0 \\ 0 & \lambda(\alpha_p) \end{pmatrix}.$$
- *If $N_p = 1$ and $C_p = 0$, let $\alpha_p = a_p$ and $\beta_p = pa_p$. Then*
$$\rho_f|_{G_p} \sim \begin{pmatrix} \lambda(\beta_p) & * \\ 0 & \lambda(\alpha_p) \end{pmatrix}.$$
- *If $N_p = C_p \geq 1$, let $\alpha_p = a_p$ and $\beta_p = \bar{a}_p \epsilon'(p)$. Then*
$$\rho_f|_{G_p} \sim \begin{pmatrix} \lambda(\beta_p) \cdot \epsilon_p & 0 \\ 0 & \lambda(\alpha_p) \end{pmatrix}.$$
- *If $N_p \geq 2 > C_p$ and $p > 2$, and π_p is supercuspidal, then $\rho_f|_{G_p} \sim \mathrm{Ind}_{G_K}^{G_p} \chi$, for a quadratic extension K of $\mathbb{Q}_p$, and a character χ of G_K.*

Let $\pi = \pi_f$ be the automorphic representation corresponding to f. Then ρ_π, the Galois representation attached to π, differs a bit from ρ_f (e.g., the Satake parameters differ from the roots of the polynomial $x^2 - a_p x + \epsilon(p)p^{k-1}$ by a factor of $p^{(k-1)/2}$, and similarly the L-functions satisfy $L(s, f) = L(s - \frac{k-1}{2}, \pi, 1)$. However the resulting adjoint Galois representation obtained by making $G_{\mathbb{Q}}$ act by conjugation on $\mathrm{M}_{2\times 2}(E_\lambda)$ is the same, and we let

$$\rho_{\mathrm{Ad}(\pi)} : G_{\mathbb{Q}} \to \mathrm{GL}_4(E_\lambda)$$

be defined by $\rho_{\mathrm{Ad}(\pi)}(g)(X) = \rho_\pi(g) X \rho_\pi(g)^{-1}$, for all $X \in \mathrm{M}_{2\times 2}(E_\lambda)$ and $g \in G_{\mathbb{Q}}$. Finally, let

$$\rho_\Pi = \rho_{\mathrm{Ad}(\pi)} \otimes \chi_\ell^{k-1}$$

be the representation obtained by taking the $(k-1)$-fold twist of the adjoint representation by the ℓ-adic cyclotomic character.

Corollary 7. *We have*

- *If $p \nmid N$, then* $\mathrm{trace}(\rho_\Pi(\mathrm{Frob}_p)) = a_p^2/\epsilon(p)$.

- *If* $N_p = 1$ *and* $C_p = 0$, *then* $\mathrm{trace}(\rho_\Pi(\mathrm{Frob}_p)) = p^{k-2}(p+1)^2$.
- *If* $N_p = C_p \geq 1$, *then in many cases there exists an arithmetic Frobenius* Frob_p *such that* $\mathrm{trace}(\rho_\Pi(\mathrm{Frob}_p)) = a_p^2/\epsilon'(p) + 2p^{k-1} + \bar{a}_p^2/\bar{\epsilon}'(p)$.

Proof. If

$$\rho_\pi(\mathrm{Frob}_p) \sim \begin{pmatrix} \alpha_p & 0 \\ 0 & \beta_p \end{pmatrix},$$

then

$$\rho_{\mathrm{Ad}(\pi)}(\mathrm{Frob}_p) \sim \begin{pmatrix} \frac{\alpha_p}{\beta_p} & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{\beta_p}{\alpha_p} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

and $\chi_\ell(\mathrm{Frob}_p)^{k-1} = p^{k-1}$. Taking the trace of $\rho_\Pi(\mathrm{Frob}_p)$ gives the corollary. □

3. The Brauer class of X

3.1. **Definition of α.** Recall that for $\gamma \in \Gamma$, there is a unique E-valued Dirichlet character χ_γ such that $f^\gamma = f \otimes \chi_\gamma$, and hence $\rho_{f^\gamma} \sim \rho_f \otimes \chi_\gamma$. For γ, $\delta \in \Gamma$, the identity

$$\chi_{\gamma\delta} = \chi_\gamma \chi_\delta^\gamma$$

shows that $\gamma \mapsto \chi_\gamma$ is a 1-cocycle. Specialising to $g \in G_\mathbb{Q}$, we see that $\gamma \mapsto \chi_\gamma(g)$ is an E-valued 1-cocycle as well. By Hilbert's theorem 90, $\mathrm{H}^1(\Gamma, E^*)$ is trivial, so there is an element $\alpha(g) \in E^*$ such that

$$\alpha(g)^{\gamma - 1} = \chi_\gamma(g), \tag{3.1}$$

for all $\gamma \in \Gamma$ (cf. [Ri85]). Clearly, $\alpha(g)$ is completely determined up to multiplication by elements of F^*. Varying $g \in G_\mathbb{Q}$, we obtain a well defined map

$$\tilde{\alpha} : G_\mathbb{Q} \to E^*/F^*.$$

Since each χ_γ is a character, $\tilde{\alpha}$ is a homomorphism.

We can and do lift $\tilde{\alpha}$ to a map $\alpha : G_\mathbb{Q} \to E^*$. The following result summarizes some well-known properties of these maps. The proofs given in [Ri75, Thm. 1.1], [Ri04, Thm. 5.5] for $k = 2$ (see also [Ri85], [BG11, Lem. 9]) easily extend to higher weight.

Proposition 8 (Ribet)**.** *We have:*

(1) $\tilde{\alpha} : G_\mathbb{Q} \to E^*/F^*$ *is unramified at all primes* p *of semistable reduction.*
(2) $\alpha^2(g) \equiv \epsilon(g)$ *mod* F^*, *for all* $g \in G_\mathbb{Q}$.
(3) $\alpha(\mathrm{Frob}_p) \equiv a_p$ *mod* F^*, *for primes* $p \nmid N$, *if* $a_p \neq 0$.
(4) $\alpha(g) \equiv$ *trace* $(\rho_f(g))$ *mod* F^*, *for* $g \in G_\mathbb{Q}$, *if trace* $(\rho_f(g)) \neq 0$.

3.2. **The 2-cocycle c_α.** By [Ri81, Prop. 1], whose proof holds for weights $k \geq 2$ as well, the class of X in $\mathrm{Br}(F) = \mathrm{H}^2(G_F, \bar{\mathbb{Q}}^*)$ is given by the 2-cocycle $(g,h) \mapsto \chi_g(h)$, for g, $h \in G_F$, where $\chi_g := \chi_\gamma$ for γ the image of g in Γ. By the definition of α, this 2-cocycle is the same as the 2-cocycle given by $(g,h) \mapsto \frac{\alpha(h)^g}{\alpha(h)}$, which differs from the 2-cocycle

$$c_\alpha(g,h) = \frac{\alpha(g)\alpha(h)}{\alpha(gh)} \tag{3.2}$$

by a coboundary. Hence, the class of X is given by the 2-cocycle $c_\alpha(g,h)$ above.

Observe that the class of c_α is independent of the lift α of $\tilde{\alpha}$. Suppose α' is another lift of $\tilde{\alpha}$. Then $\alpha'(g) = \alpha(g)f(g)$, for some map $f : G_F \to F^*$. Then c_α and $c_{\alpha'}$ differ by the map $(g,h) \mapsto \frac{f(g)f(h)}{f(gh)}$, which is clearly a 2-coboundary.

We also note that the class of c_α (hence X) is 2-torsion in the Brauer group of F, since $c_\alpha^2(g,h) = \frac{d(g)d(h)}{d(gh)}$ is a 2-coboundary, where $d(g) := \alpha^2(g)/\epsilon(g) \in F^*$, by part (2) of Proposition 8.

3.3. **Invariant map.** To study the Brauer class of X, it suffices to study the Brauer class of $X_v := X \otimes_F F_v$ in $\mathrm{Br}(F_v)$, for each place v of F. It is well known that if v is finite then

$$\mathrm{inv}_v : \mathrm{Br}(F_v) \simeq \mathbb{Q}/\mathbb{Z}$$

via the invariant map inv_v at v. Since the class of X is 2-torsion in the Brauer group of F, we have that $\mathrm{inv}_v(X_v) \in \frac{1}{2}\mathbb{Z}/\mathbb{Z}$. Identifying this group with $\mathbb{Z}/2$, we see that X_v is a matrix algebra over F_v if $\mathrm{inv}_v(X_v) = 0 \bmod 2$, and is a matrix algebra over a quaternion division algebra over F_v if $\mathrm{inv}_v(X_v) = 1 \bmod 2$.

To aid in the computation of $\mathrm{inv}_v(X_v)$, for finite places v, it is useful to recall the explicit definition of the invariant map, which we do now. Let I_v be the inertia subgroup of G_F at the prime v. Let $\mathrm{Gal}(F_v^{\mathrm{nr}}/F_v)$ be the Galois group of F_v^{nr}, the maximal unramified extension of F_v, over F_v. The inflation map

$$\mathrm{Inf} : \mathrm{H}^2(\mathrm{Gal}(F_v^{\mathrm{nr}}/F_v), F_v^{\mathrm{nr}}) \to \mathrm{Br}(F_v)$$

is well-known to be an isomorphism. Now, the surjective valuation $v : F^* \to \mathbb{Z}$ can be extended uniquely to $(F_v^{\mathrm{nr}})^*$ which we continue to call v. This gives rise to a map

$$v : \mathrm{H}^2(\mathrm{Gal}(F_v^{\mathrm{nr}}/F_v), F_v^{\mathrm{nr}}) \to \mathrm{H}^2(\mathrm{Gal}(F_v^{\mathrm{nr}}/F_v), \mathbb{Z})$$

which we again denote by v. Also, the short exact sequence of abelian groups

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

gives rise to a long exact sequence of cohomology groups, with boundary map

$$\delta : \mathrm{H}^1(\mathrm{Gal}(F_v^{\mathrm{nr}}/F_v), \mathbb{Q}/\mathbb{Z}) \to \mathrm{H}^2(\mathrm{Gal}(F_v^{\mathrm{nr}}/F_v), \mathbb{Z})$$

which is an isomorphism since $\mathrm{H}^i(\mathrm{Gal}(F_v^{\mathrm{nr}}/F_v), \mathbb{Q}) = 0$ for $i = 1$, 2. We recall the definition of δ. If $\chi : \mathrm{Gal}(F_v^{\mathrm{nr}}/F_v) \to \mathbb{Q}/\mathbb{Z}$ is a homomorphism, and $\tilde{\chi}$ is a lift of χ to $\mathbb{Q}$, then $\delta(\chi)$ is the $\mathbb{Z}$-valued 2-cocycle on $\mathrm{Gal}(F_v^{\mathrm{nr}}/F_v)$ given by

$$(g,h) \mapsto \frac{\tilde{\chi}(g)\tilde{\chi}(h)}{\tilde{\chi}(gh)}.$$

Finally, there is a map, say Ev (for evaluation)

$$\mathrm{Ev} : \mathrm{H}^1(\mathrm{Gal}(F_v^{\mathrm{nr}}/F_v), \mathbb{Q}/\mathbb{Z}) \to \mathbb{Q}/\mathbb{Z}$$

obtained by evaluating a homomorphism at the arithmetic Frobenius at v. Then, by definition, the invariant map at v is given by

$$\mathrm{inv}_v = \mathrm{Ev} \circ \delta^{-1} \circ v \cdot \mathrm{Inf}^{-1} : \mathrm{Br}(F_v) \to \mathbb{Q}/\mathbb{Z}.$$

3.4. **Local 2-cocycle.** Now let $K : G_v \to \bar{F}_v^*$ be any map. Then

$$c_K(g,h) = \frac{K(g)K(h)}{K(gh)}$$

defines a local 2-cocycle on G_v, if $c_K(g,h) \in F_v$, for all g, $h \in G_v$. We call it the local 2-cocycle defined by the function K. The following general lemma regarding the Brauer class of this local 2-cocycle will be very useful in computations.

Lemma 9. *Let $K : G_v \to \bar{F}_v^*$ be a map and let $t : G_v \to \bar{F}_v^*$ be an unramified homomorphism such that*

(1) *$K(i) \in F_v^*$, for all $i \in I_v$,*
(2) *$K(g)^2/t(g) \in F_v^*$, for all $g \in G_v$.*

Then, for any arithmetic Frobenius Frob_v *at v, we have*

$$\mathrm{inv}_v(c_K) = \frac{1}{2} \cdot v\left(\frac{K(\mathrm{Frob}_v)^2}{t(\mathrm{Frob}_v)}\right) \in \frac{1}{2}\mathbb{Z}/\mathbb{Z},$$

where $v : F_v^* \to \mathbb{Z}$ is the surjective valuation.

Proof. We will calculate $\mathrm{inv}_v(c_K)$, step by step, using the definition of inv_v just recalled.

Replacing the induced homomorphism $K : G_v \to \bar{F}_v^*/F_v^*$ with another lift $K : G_v \to \bar{F}_v^*$ which we again call K does not change the cohomology class of c_K. By property (1) we may choose a lift K such that for $g \in G_v$, $K(gi) = K(g)$, for all $i \in I_v$. Denote the image of g under the projection map $G_v \to G_v/I_v = \hat{\mathbb{Z}}$ by $\bar{g}$. Define $c_{\bar{K}} : \hat{\mathbb{Z}} \times \hat{\mathbb{Z}} \to F_v^*$ by $c_{\bar{K}}(\bar{g},\bar{h}) = c_K(g,h)$. Then $c_{\bar{K}}$ is clearly a well-defined 2-cocycle on $\hat{\mathbb{Z}}$ whose image under the inflation map is c_K.

Now, by definition, $v(c_{\bar{K}})$ is the 2-cocycle defined by

$$(g,h) \mapsto v\left(\frac{K(g)K(h)}{K(gh)}\right) \in \mathbb{Z},$$

for g, $h \in G_v$.

By property (2), $d(g) = K^2(g)/t(g) \in F_v^*$, for $g \in G_v$. The 2-cocycle above is the same as the 2-cocycle induced by

$$(g,h) \mapsto \frac{1}{2} \cdot v\left(\frac{d(g)d(h)}{d(gh)}\right) \in \mathbb{Z}.$$

Consider now the map $\chi : \mathrm{Gal}(F_v^{\mathrm{nr}}/F_v) \to \mathbb{Q}/\mathbb{Z}$ defined by

$$\chi(g) = \frac{1}{2} \cdot v(d(g)) \bmod \mathbb{Z}.$$

Under the boundary map δ the 1-cocycle χ maps to the 2-cocycle above, so $(\delta^{-1} \circ v \circ \mathrm{Inf}^{-1})(c_K))$ is just χ. Hence

$$\mathrm{inv}_v(c_K) = (\mathrm{Ev} \circ \delta^{-1} \circ v \circ \mathrm{Inf}^{-1})(c_K) = \chi(\mathrm{Frob}_v) = \frac{1}{2} \cdot v\left(\frac{K(\mathrm{Frob}_v)^2}{t(\mathrm{Frob}_v)}\right) \bmod \mathbb{Z}.$$

□

4. Good primes

Theorem 10. *Assume* $\gcd(p, N) = 1$ *and assume* $a_p \neq 0$*. Let* v *be a place of* F *lying over* p*. Then* X_v *is a matrix algebra over* F_v*, if and only if the slope*

$$m_v = [F_v : \mathbb{Q}_p] \cdot v(a_p^2/\epsilon(p)) \in \mathbb{Z}$$

is even, where v *is normalized such that* $v(p) = 1$*.*

Proof. This follows immediately from the lemma above taking $K = \alpha$ and $t = \epsilon$. Indeed, we have $\mathrm{inv}_v(c_\alpha) = \frac{1}{2}v(\alpha^2(\mathrm{Frob}_v)/\epsilon(\mathrm{Frob}_v)) \bmod \mathbb{Z}$, and $\alpha(\mathrm{Frob}_v) \equiv a_p^{f_v} \bmod F^*$, by part (3) of Proposition 8. □

For the cases where $a_p = 0$ we have the following criterion (which is not in terms of a slope). Let $p^\dagger \nmid N$ be a prime such that $p^\dagger \equiv p \bmod N$ and $a_{p^\dagger} \neq 0$. Let

$$m_v^\dagger := [F_v : \mathbb{Q}_{p^\dagger}] \cdot v(a_{p^\dagger}^2/\epsilon(p^\dagger)) \in \mathbb{Z},$$

where v is normalized so that $v(p) = 1$.

Theorem 11. *Let* $\gcd(p, N) = 1$ *and suppose* $a_p = 0$*. Let* v *be a place of* F *lying over* p*. Then* X_v *is a matrix algebra over* F_v *if and only if* $m_v^\dagger \in \mathbb{Z}$ *is even.*

Proof. The proof is similar to that of the previous theorem, with minor changes. Note that $p^\dagger \equiv p \bmod N$ implies $\chi_\gamma(p) = \chi_\gamma(p^\dagger)$, for all $\gamma \in \Gamma$. So, if Frob_p and $\mathrm{Frob}_{p^\dagger}$ denote the Frobenii at the prime p and $p^\dagger$, then by (3.1), we have $\alpha(\mathrm{Frob}_p) \equiv \alpha(\mathrm{Frob}_{p^\dagger}) \equiv a_{p^\dagger} \bmod F^*$. Hence

$$\mathrm{inv}_v(c_\alpha) = \frac{1}{2}v\left(\frac{\alpha^2(\mathrm{Frob}_v)}{\epsilon(\mathrm{Frob}_v)}\right) = \frac{1}{2} \cdot f_v \cdot v\left(\frac{\alpha^2(\mathrm{Frob}_p)}{\epsilon(p)}\right) = \frac{1}{2} \cdot f_v \cdot v\left(\frac{a_{p^\dagger}^2}{\epsilon(p^\dagger)}\right) \bmod \mathbb{Z}.$$

□

5. Steinberg primes

Let now turn to the cases where $p \mid N$. In this section we assume that $N_p = 1$ and $C_p = 0$. Thus $N = Mp$, where M is a positive integer with $(M, p) = 1$, and ϵ is a character mod M.

Lemma 12. *If* (γ, χ_γ) *is an extra twist for* f*, then the conductor of* χ_γ *divides* M*.*

Proof. A general result due to Atkin-Li [AL78, Thm. 3.1] allows one to calculate the exact level of the newform attached to a twisted form $f \otimes \chi$. We recall this now. Let $f \in S_k(N, \epsilon)$ be a newform of weight $k \geq 2$, and nebentypus ϵ. In the notation of *loc. cit.*, let $q \mid N$ be a prime and let Q be the q-primary factor of N. So $N = QM$, with $(M, q) = 1$. Let the conductor of ϵ_Q, the q-part of ϵ, be q^α, for $\alpha \geq 0$. Let χ be a character of conductor q^β, with $\beta \geq 1$. Set

$$Q' = \mathrm{Max}\{Q, q^{\alpha+\beta}, q^{2\beta}\}.$$

According to the theorem, the level of the newform attached to $f \otimes \chi_\gamma$ is $Q'M$, provided that

- max $\{q^{\alpha+\beta}, q^{2\beta}\} \leq Q$, if $Q' = Q$, or
- Conductor of $\epsilon_Q \chi =$ max $\{q^\alpha, q^\beta\}$, if $Q' > Q$.

In our case, taking $Q = q = p$, we have $\epsilon_Q = \epsilon_p = 1$. We let χ be the p-part of χ_γ. Suppose towards a contradiction that χ_γ has level divisible by p. Then $\alpha = 0$ and $\beta = 1$. Then $Q' = p^2 > Q = p$ and the Q-part of the conductor of $\epsilon_Q \chi_\gamma = \chi_\gamma$ is p. So the second condition above is satisfied and we get the p-part of the level of the newform attached to $f \otimes \chi_\gamma$ is p^2. On the other hand, $f \otimes \chi_\gamma = f^\gamma$ has the same level as f namely Mp, which is not divisible by p^2, a contradiction. Thus the p-part of the conductor of χ_γ must be trivial, as desired. □

Recall that $a_\ell^\gamma = a_\ell \cdot \chi_\gamma(\ell)$ for all primes $\ell \nmid N$. We show that this also holds for $p || N$.

Lemma 13. *$a_p^\gamma = \chi_\gamma(p) \cdot a_p$, for all $\gamma \in \Gamma$.*

Proof. We use the precise form of the local Galois representation at p from Langlands' theorem (Theorem 6, see also [Hi00, Thm. 3.26]). We have

$$\rho_f|_{G_p} \sim \begin{pmatrix} \lambda(pa_p) & * \\ 0 & \lambda(a_p) \end{pmatrix},$$

where $\lambda(x) : G_p \longrightarrow \mathbb{Z}_l^*$ is the unramified character taking arithmetic Frobenius to x. Note that both characters make sense since both pa_p and a_p are ℓ-adic units. By the previous lemma, the conductor of χ_γ, for $\gamma \in \Gamma$, is prime to p and so $\chi_\gamma(p)$ makes sense, and is an ℓ-adic unit, and locally we have $\chi_\gamma|_{G_p} = \lambda(\chi_\gamma(p))$. Applying Langlands' theorem for f^γ, we get

$$\rho_{f^\gamma}|_{G_p} \sim \begin{pmatrix} \lambda(pa_p^\gamma) & * \\ 0 & \lambda(a_p^\gamma) \end{pmatrix}.$$

Since $f^\gamma = f \otimes \chi_\gamma$, implies $\rho_{f^\gamma} \sim \rho_f \otimes \chi_\gamma$, we have locally that

$$\begin{pmatrix} \lambda(pa_p^\gamma) & * \\ 0 & \lambda(a_p^\gamma) \end{pmatrix} \sim \begin{pmatrix} \lambda(pa_p)\lambda(\chi_\gamma(p)) & * \\ 0 & \lambda(a_p)\lambda(\chi_\gamma(p)) \end{pmatrix}.$$

An important part of Langlands' theorem (not mentioned explicitly above) is that $* \neq 0$, since the inertia group I_p acts unipotently with infinite image. Thus comparing like diagonal entries, we see that $a_p^\gamma = \chi_\gamma(p) \cdot a_p$. □

Recall that the map $\tilde{\alpha} : G_{\mathbb{Q}} \to E^*/F^*$ is unramified at primes of semistable reduction, and $\alpha(\mathrm{Frob}_p) \equiv a_p \bmod F^*$ at primes of good reduction (cf. Proposition 8). We now observe that this last formula continues to hold for primes of semistable reduction.

Proposition 14. *Suppose p is a prime such that $N_p = 1$ and $C_p = 0$. Then $\alpha(\mathrm{Frob}_p) \equiv a_p \bmod F^*$.*

Proof. Since, for $\gamma \in \Gamma$, the conductor of χ_γ is prime to p, we have $\chi_\gamma(i) = 1$, for $i \in I_p$. By (3.1), we deduce $\alpha(i) \in F^*$, for all $i \in I_p$. Thus we recover the fact that $\tilde{\alpha}$ is unramified at the Steinberg primes for any $k \geq 2$. In any case, it makes sense to speak of $\alpha(\mathrm{Frob}_p) \bmod F^*$. By Lemma 13, we have $a_p^{\gamma-1} = \chi_\gamma(p)$, for $\gamma \in \Gamma$. By (3.1), $\alpha(\mathrm{Frob}_p)^{\gamma-1} = \chi_\gamma(p)$. Since these identities hold for all $\gamma \in \Gamma$, we deduce that $\alpha(\mathrm{Frob}_p) \equiv a_p \bmod F^*$. $\square$

Theorem 15. *Let $N_p = 1$ and $C_p = 0$ and let $v \mid p$ be a prime of F. Then X_v is a matrix algebra if and only if $[F_v : \mathbb{Q}_p] \cdot (k-2)$ is even.*

Proof. Applying Lemma 9 to $K = \alpha$ and $t = \epsilon$, we get $\mathrm{inv}_v(c_\alpha) = \frac{1}{2} v(\frac{\alpha^2(\mathrm{Frob}_v)}{\epsilon(\mathrm{Frob}_v)}) \bmod \mathbb{Z}$. By the previous proposition, $\alpha(\mathrm{Frob}_v) = a_p^{f_v} \bmod F^*$. Thus $\mathrm{inv}_v(c_\alpha) = \frac{1}{2} \cdot f_v \cdot v(\frac{a_p^2}{\epsilon(p)})$. By Theorem 4.6.17 [Mi89], $\frac{a_p^2}{\epsilon_M(p)} = p^{k-2}$. Also we may replace the valuation v by $e_v \cdot v$, where the second v is normalized such that $v(p) = 1$. We obtain that $\mathrm{inv}_v(c_\alpha) = [F_v : \mathbb{Q}_p] \cdot (k-2) \bmod 2$, as desired. $\square$

6. Ramified principal series primes

We now assume that $N_p = C_p \geq 1$. Let v be a place of F lying above p. Let e_v and f_v be the ramification degree and inertia degree of v over p. Recall that in this case π_p is in the ramified principal series.

Recall that $\epsilon = \epsilon' \cdot \epsilon_p$ is a decomposition of the nebentypus ϵ into its prime-to-p part and p part. We use repeatedly a fundamental theorem of Langlands (Theorem 6), which states that the local Galois representation at the prime p is given by

$$\rho_f|_{G_p} \sim \begin{pmatrix} \lambda(\bar{a}_p \epsilon'(p)) \cdot \epsilon_p & 0 \\ 0 & \lambda(a_p) \end{pmatrix}.$$

where $\lambda(x)$ is the usual local unramified character.

Lemma 16. *Let $\mu = \frac{a_p^2}{\epsilon'(p)}$ and $\nu = \bar{\mu} = \frac{\bar{a}_p^2}{\bar{\epsilon}'(p)}$. Then $\mu^f + \nu^f \in F$, for all integers $f \geq 1$.*

Proof. Let (γ, χ_γ) be an extra twist for the form f. Thus we have $\rho_{f^\gamma} \sim \rho_f \otimes \chi_\gamma$. Hence, by Langlands' theorem, locally on G_p we have

$$\begin{pmatrix} \lambda(\bar{a}_p^\gamma \epsilon'(p)^\gamma) \cdot \epsilon_p^\gamma & 0 \\ 0 & \lambda(a_p^\gamma) \end{pmatrix} \sim \begin{pmatrix} \lambda(\bar{a}_p \epsilon'(p)) \cdot \epsilon_p \cdot \chi_\gamma & 0 \\ 0 & \lambda(a_p) \cdot \chi_\gamma \end{pmatrix}.$$

One of the two characters on the left is unramified and the other one is ramified. Thus the same must be true on the right hand side. Moreover, the unramified characters on both sides must be equal and the ramified characters must also be equal.

We decompose χ_γ into its prime-to-p and p parts, namely $\chi_\gamma = \chi'_\gamma \cdot \chi_{\gamma,p}$. First, assume that χ_γ is unramified at p. Then, $\chi_\gamma = \chi'_\gamma = \lambda(\chi_\gamma(p))$, and comparing unramified characters, we get $a_p^\gamma = \chi_\gamma(p)a_p$. Using the fact that $\chi_\gamma^2 = \epsilon^{\gamma-1}$, we have $\chi_\gamma^2(p) = \epsilon'(p)^{\gamma-1}$. Thus $(\mu^f)^\gamma = \mu^f$ and $(\nu^f)^\gamma = \nu^f$, since Γ is abelian, so complex conjugation commutes with γ. Hence, γ fixes $\mu^f + \nu^f$.

Now assume that χ_γ is ramified at p. Comparing ramified characters, we get, on I_p, that $\chi_{\gamma,p} = \epsilon_p^\gamma$ and $\epsilon_p\chi_{\gamma,p} = 1$. Thus $\bar\epsilon_p = \epsilon_p^\gamma = \chi_{\gamma,p}$. Now, comparing unramified characters, we get $a_p^\gamma = \bar a_p \cdot \epsilon'(p) \cdot \chi'_\gamma(p)$. Again, since $(\chi'_\gamma)^2 = (\epsilon')^{\gamma-1}$, we deduce that

$$\frac{(a_p^2)^\gamma}{\epsilon'(p)^\gamma} = \frac{\bar a_p^2}{\bar\epsilon'(p)}.$$

In other words, $\mu^\gamma = \nu$, and hence $(\mu^f)^\gamma = \nu^f$, for all integers $f \geq 1$. Applying complex conjugation we see that similarly $(\nu^f)^\gamma = \mu^f$. Hence again γ fixes $\mu^f + \nu^f$.

In both cases $\gamma \in \Gamma = \mathrm{Gal}(E/F)$ is arbitrary, so $\mu^f + \nu^f$ must belong to F, for all integers $f \geq 1$. □

For later use we state the following generalization of Lemma 16 which can be proved in a similar manner, or directly by noting that $\alpha^2 \equiv \epsilon \bmod F^*$.

Lemma 17. *Let* Frob_v *be an arithmetic Frobenius at* v*, and let* $\zeta = \epsilon_p(\mathrm{Frob}_v)$*. Then* $\mu^{f_v} \cdot 1/\zeta + \nu^{f_v} \cdot \zeta \in F$*.*

6.1. **Unequal slope.** In this section, we assume that

$$v\left(\frac{a_p^2}{\epsilon'(p)} + 2p^{(k-1)} + \frac{\bar a_p^2}{\bar\epsilon'(p)}\right) < k-1.$$

Here v is the valuation such that $v(p) = 1$.

By an elementary calculation it can be shown that the above assumption is equivalent to the assertion that for all place w of E lying over v, we have $w(a_p) \neq w(\bar a_p)$. Let O_v be the ring of integers of F_v. Let P_v be the prime ideal of O_v and let π_v be a prime element of O_v. Let $U_v^{(n)} = 1 + P_v^n$, for $n \geq 1$.

Lemma 18. *μ and ν belong to F_v.*

Proof. By Lemma 16, $\mu + \nu$ belongs to F. Consider the quantity

$$\frac{(\mu-\nu)^2}{(\mu+\nu)^2} = 1 - 4\frac{\mu \cdot \nu}{(\mu+\nu)^2}.$$

Now $\mu\nu = p^{2(k-1)}$. Since the slopes of μ and ν are not the same, the expression on the right hand side belongs to $U_v^{(1)} = 1 + \pi_v O_v$, for p odd, and it belongs to $U_v^{(3e_v)} = 1 + \pi_v^{3e_v} O_v$, for $p = 2$. It therefore has a square root in $U_v^{(1)} = 1 + \pi_v O_v$, in both cases. Hence, $\frac{\mu-\nu}{\mu+\nu}$ belongs to F_v. Since we have already proved that $\mu + \nu$ belongs to F, we see $\mu - \nu$ belongs to F_v. Hence, individually, both μ and ν belong to F_v. □

6.1.1. *The case of odd primes.* We now assume that p is an odd prime. We say that ϵ_p is tame if the order of ϵ_p divides $p-1$.

Lemma 19. *If ϵ_p is tame, then for any arithmetic Frobenius* Frob_v *at v,*

$$\frac{(a_p^{f_v} + \epsilon_p(\mathrm{Frob}_v)(\bar{a}_p\epsilon'(p))^{f_v})^2}{a_p^{2f_v} + (\bar{a}_p\epsilon'(p))^{2f_v}} \in F_v^{*2}$$

is a square.

Proof. We may rewrite this expression as

$$\frac{\mu^{f_v} + \epsilon_p^2(\mathrm{Frob}_v)\nu^{f_v}}{\mu^{f_v} + \nu^{f_v}} \cdot \left(1 + 2\epsilon_p(\mathrm{Frob}_v) \cdot \frac{p^{(k-1)f_v}}{\mu^{f_v} + \epsilon_p^2(\mathrm{Frob}_v)\nu^{f_v}}\right),$$

where μ and ν are as above. By the previous lemma, μ and ν belong to F_v. Since ϵ_p is tame, the image of ϵ_p belongs to $\mathbb{Q}_p$, and hence to F_v. Thus all terms in the display above are in F_v. Now, since p is odd, and the slopes are unequal, the second term (in parentheses) is in $U_v^{(1)}$, hence a square. If $w(a_p) > w(\bar{a}_p)$, the first term is of the form $\epsilon_p^2(\mathrm{Frob}_v)$ times an element of $U_v^{(1)}$, and if $w(a_p) < w(\bar{a}_p)$, then the first term is in $U_v^{(1)}$, so in both cases, the first term is also a square. □

Lemma 20. *If ϵ_p is tame and* Frob_v *is an arithmetic Frobenius at v, then*

$$\alpha^2(\mathrm{Frob}_v) \equiv a_p^{2f_v} + (\bar{a}_p\epsilon'(p))^{2f_v} \bmod F_v^{*2}.$$

Proof. If the trace of $\rho_f(g)$ is non-zero, for $g \in G_{\mathbb{Q}}$, then (cf. part (4) of Proposition 8)

$$\alpha^2(g) \equiv (\mathrm{trace}\ \rho_f(g))^2 \bmod F^{*2}.$$

Since $w(a_p) \neq w(\bar{a}_p)$, the trace of $\rho_f(\mathrm{Frob}_v)$ is non-zero. Using Langlands' theorem to compute the trace we obtain

$$\alpha^2(\mathrm{Frob}_v) \equiv (a_p^{f_v} + \epsilon_p(\mathrm{Frob}_v)(\bar{a}_p\epsilon'(p))^{f_v})^2 \bmod F^{*2}.$$

The lemma now follows from the previous lemma. □

Lemma 21. *If ϵ_p is tame, then $\alpha(i)$ belongs to F_v^*, for $i \in I_v$.*

Proof. If $i \in I_v$, and σ_v is an arithmetic Frobenius at v, then $\sigma_v' = \sigma_v i$ is also an arithmetic Frobenius at v. By the lemma above, $\alpha(\sigma_v) \equiv \pm\alpha(\sigma_v') \bmod F_v^*$. Since

$$c_\alpha(\sigma, i) = \frac{\alpha(\sigma_v)\alpha(i)}{\alpha(\sigma_v')} \in F^*,$$

we see that $\alpha(i)$ belongs to F_v^*. □

Theorem 22. *Let p be an odd prime such that $p \mid N$ and $N_p = C_p$. Let v be a place of F lying above p. Let w be an extension of v to a place of E. If $w(a_p) \neq w(\bar{a}_p)$, then X_v is a matrix algebra if and only if*

$$m_v = [F_v : \mathbb{Q}_p] \cdot v\left(\mu + 2p^{k-1} + \nu\right) \in \mathbb{Z}$$

is even, where v is normalized so that $v(p) = 1$.

Proof. Let L be the extension of F_v cut out by the wild part of ϵ_p. So ϵ_p, thought of as a character of G_L, is tame. Note that L/F_v is a totally ramified extension of odd (p-power) degree. By Lemma 21, $\tilde{\alpha} : G_L \to \bar{F}_v^*/F_v^*$ is an unramified character. On G_L, we have $\alpha^2 \equiv \epsilon' \bmod F_v^*$, since this is true with ϵ' replaced with ϵ, and on G_L we have $\epsilon' \equiv \epsilon \bmod F_v^*$, since $\epsilon_p(G_L) \subset \mathbb{Q}_p^* \subset F_v^*$, since $\epsilon_p|_{G_L}$ is tame. We calculate $\mathrm{inv}_L(\mathrm{res}_{F_v/L} c_\alpha)$ using Lemma 9 applied to $K = \alpha|_{G_L}$ and $t = \epsilon'|_{G_L}$. Let u be the prime of L lying over v and let Frob_u be an arithmetic Frobenius at u. We obtain

$$\mathrm{inv}_L(\mathrm{res}_{F_v/L} c_\alpha) = \frac{1}{2} \cdot u\left(\frac{\alpha^2(\mathrm{Frob}_u)}{\epsilon'(\mathrm{Frob}_u)}\right) \bmod \mathbb{Z} \in {}_2\mathrm{Br}(L).$$

Since f_v is also the residue degree of $u \mid p$, by Lemma 20 we obtain

$$\alpha^2(\mathrm{Frob}_u) \equiv a_p^{2f_v} + (\bar{a}_p \epsilon'(p))^{2f_v} \bmod F_v^{*2}.$$

Hence

$$\frac{\alpha^2}{\epsilon'}(\mathrm{Frob}_u) \equiv \mu^{f_v} + \nu^{f_v} \bmod F_v^{*2}.$$

Now $[L : F_v] \cdot \mathrm{inv}_v c_\alpha = \mathrm{inv}_L(\mathrm{res}_{F_v/L} c_\alpha)$, and for $x \in F_v$, $u(x) = [L : F_v] \cdot v(x)$, where both u and v are the surjective valuations onto $\mathbb{Z}$. But $[L : F_v]$ is a power of p, so is odd, and so in both cases can be ignored. We obtain

$$\mathrm{inv}_v c_\alpha = \frac{1}{2} \cdot v\left(\frac{\alpha^2}{\epsilon'}(\mathrm{Frob}_u)\right) = \frac{1}{2} \cdot v(\mu^{f_v} + \nu^{f_v}) = \frac{1}{2} \cdot v(\mu^{f_v} + \nu^{f_v} + 2p^{(k-1)f_v}) \bmod \mathbb{Z}.$$

Since the last three terms lie in F and have distinct valuations, replacing v with the valuation v satisfying $v(p) = 1$, we obtain the theorem. ☐

6.1.2. *The case of $p = 2$.* We now assume that $p = 2$, so that $N_2 = C_2 \geq 2$. We continue to assume that $w(a_2) \neq w(\bar{a}_2)$.

Lemma 23. *There exists an arithmetic Frobenius* Frob_v *such that* $\epsilon_p(\mathrm{Frob}_v) = 1$.

Proof. Let σ_v be an arithmetic Frobenius at v. Then $\epsilon_p(\sigma_v) = \zeta_{2^n}$, a 2^n-th root of unity, for $n \geq 0$. If $n = 0$, we are done. Otherwise, since $\epsilon_p(G_v) = \epsilon_p(I_v)$, there exists $i \in I_v$ such that $\epsilon_p(\sigma_v^{2^n - 1}) = \epsilon_p(i)$. Hence $\epsilon_p^{2n}(\sigma_v) = 1 = \epsilon_p(\sigma_v) \cdot \epsilon_p(i) = \epsilon_p(\tilde{\sigma}_v)$, where $\tilde{\sigma}_v = \sigma_v i$ is another arithmetic Frobenius at v. ☐

Lemma 24. *If* Frob_v *is an arithmetic Frobenius at v, then* $\epsilon_p(\mathrm{Frob}_v)$ *belongs to* F_v^*.

Proof. Let $\sigma_v = \mathrm{Frob}_v$. Assume $\epsilon_p(\sigma_v)$ is a primitive 2^m-th root of unity, for $m \geq 0$. Let $r \geq 1$ be such that F_v contains a primitive 2^r-th root of unity, but not a 2^{r+1}-th root of unity. It is enough to prove $m \leq r$.

Assume, towards a contradiction, that $m \geq r + 1$. Then $\epsilon_p^{2^{m-r-1}}(\sigma_v)$ is a 2^{r+1}-th root of unity. Using the fact that $\epsilon_p(G_v) = \epsilon_p(I_v)$, we can find $i \in I_v$ such that $\epsilon_p^{2^{m-r-1}}(\sigma_v) = \epsilon_p(\sigma_v \cdot i)$ (see proof of previous lemma). For example, if $m = r + 1$, we can take $i = 1$. Now $\sigma_v' = \sigma_v i$ is another arithmetic Frobenius at v. Using Langlands' theorem to compute the (non-zero) trace of $\rho_f(\sigma_v')$ we obtain

$$\alpha(\sigma_v') \equiv a_p^{f_v} + \epsilon_p(\sigma_v')(\bar{a}_p \epsilon'(p))^{f_v} \bmod F^*.$$

Since $\alpha^2 \equiv \epsilon \bmod F^*$, we deduce that

$$\frac{\mu^{f_v} + \epsilon_p^2(\sigma_v')\nu^{f_v}}{\epsilon_p(\sigma_v')} \in F^*.$$

By lemma 18, μ^{f_v} and ν^{f_v} belong to F_v. Also, $\epsilon_p^2(\sigma_v')$ is a primitive 2^r-th root of unity, so belongs to F_v. We conclude that the primitive 2^{r+1}-th root of unity $\epsilon_p(\sigma_v') = \epsilon_p^{2^{m-r-1}}(\sigma_v)$ belongs to F_v, a contradiction. □

Lemma 25. *If $i \in I_v$, then $\alpha(i)$ belongs to F_v^*.*

Proof. If $\epsilon_p(G_v) = \pm 1$, then by Langlands' theorem

$$\alpha(\mathrm{Frob}_v) \equiv a_p^{f_v} \pm (\bar{a}_p\epsilon'(p))^{f_v} \bmod F^*.$$

Let i be an arbitrary element of I_v and let σ_v and $\sigma_v' = \sigma_v i$ be two arithmetic Frobenii at v. The above congruence for α (and a calculation similar to that in Lemma 18 and Lemma 20 in the case of unequal sign) guarantees that $\alpha(\sigma_v) \equiv \alpha(\sigma_v') \bmod F_v^*$. Since $\alpha(\sigma_v)\alpha(i)/\alpha(\sigma_v') \in F^*$, so $\alpha(i) \in F_v$.

Let us assume now that $\epsilon_p(G_v) \neq \pm 1$. We first show that if $\epsilon_p(i) \neq -1$, then $\alpha(i) \in F_v$. We first choose an arithmetic Frobenius σ_v such that $\epsilon_p(\sigma_v) = 1$, by Lemma 23. Then $\epsilon_p(i) = \epsilon_p(\sigma_v)\cdot\epsilon_p(i) = \epsilon_p(\sigma_v')$, for $\sigma_v' = \sigma_v i$. Hence $\epsilon_p(i) \in F_v$, by Lemma 24. By Langlands' theorem, we know $\alpha(i) \equiv 1 + \epsilon_p(i) \bmod F^*$. Hence, $\alpha(i)$ belongs to F_v^*. If $\epsilon_p(i) = -1$, we choose $j \in I_v$ such that $\epsilon_p(j) \neq \pm 1$, using the fact that $\epsilon_p(G_v) = \epsilon_p(I_v)$. Since $\epsilon_p(j)$ and $\epsilon_p(ij) \neq -1$, the previous argument shows that $\alpha(j)$ and $\alpha(ij)$ belongs to F_v. Since $\alpha(i)\alpha(j)/\alpha(ij) \in F^*$, we see that $\alpha(i) \in F_v^*$. □

Lemma 26. *Let Frob_v be an arithmetic Frobenius at v. Then*

$$\alpha^2(\mathrm{Frob}_v) \equiv a_p^{2f_v} + (\bar{a}_p\epsilon'(p))^{2f_v} + 2p^{(k-1)f_v}\epsilon'(p)^{f_v} \ \mathit{mod}\ F_v^{*2}.$$

Proof. Let σ_v be a Frobenius as in Lemma 23, and let $\tilde{\sigma}_v$ be any arithmetic Frobenius at v. Then σ_v and $\tilde{\sigma}_v$ will differ by an element of I_v. By Lemma 25,

$$\alpha(\tilde{\sigma}_v) \equiv \alpha(\sigma_v) \bmod F_v^*.$$

Since $\epsilon_p(\sigma_v) = 1$, we get by Langlands' theorem

$$\alpha^2(\sigma_v) \equiv a_p^{2f_v} + (\bar{a}_p\epsilon'(p))^{2f_v} + 2p^{(k-1)f_v}\epsilon'(p)^{f_v} \bmod F^{*2}.$$

Hence,

$$\alpha^2(\tilde{\sigma}_v) \equiv a_p^{2f_v} + (\bar{a}_p\epsilon'(p))^{2f_v} + 2p^{(k-1)f_v}\epsilon'(p)^{f_v} \bmod F_v^{*2}.$$

□

Theorem 27. *Let $p = 2$ and assume $N_2 = C_2 \geq 1$. Let $v \mid 2$ be a place of F. Assume that $w(a_2) \neq w(\bar{a}_2)$. Then X_v is a matrix algebra over F_v if and only if*

$$m_v = [F_v : \mathbb{Q}_2] \cdot v(\mu + 2p^{k-1} + \nu) \in \mathbb{Z}$$

is even, where v is normalized such that $v(p) = 1$.

Proof. By Lemma 25, the map $\alpha : G_v \longrightarrow \bar{F}_v^*/F_v^*$ is unramified. Applying Lemma 9 with $K = \alpha|_{G_v}$ and $t = \epsilon'|_{G_v}$, we have

$$\mathrm{inv}_v c_\alpha = \frac{1}{2} \cdot v\left(\frac{\alpha^2}{\epsilon'}(\mathrm{Frob}_v)\right) = \frac{1}{2} \cdot v(\mu^{f_v} + 2p^{(k-1)f_v} + \nu^{f_v}) \bmod \mathbb{Z},$$

where the last equality follows from Lemma 26. The theorem now follows replacing v by the valuation v normalized such that $v(p) = 1$. □

6.2. **Equal slope.** In this section, we assume that

$$v\left(\frac{a_p^2}{\epsilon'(p)} + 2p^{(k-1)} + \frac{\bar{a}_p^2}{\bar{\epsilon}'(p)}\right) \geq k-1,$$

where $v(p) = 1$. So $w(a_p) = w(\bar{a}_p)$, for all place w of E lying above v. In this case it is possible for $m_v = \infty$. To avoid this we introduce a new quantity m_v^ζ, for any root of unity ζ in the image of ϵ_p, defined by

$$m_v^\zeta := e_v \cdot v\left(\mu^{f_v} \cdot 1/\zeta + 2p^{(k-1)f_v} + \nu^{f_v} \cdot \zeta\right) \in \mathbb{Z} \cup \{\infty\},$$

where v is normalized such that $v(p) = 1$. By Lemma 17, the three term expression above is in F, so the above expression is well-defined. Moreover, for some ζ, the three term expression above is non-zero and $m_v^\zeta \in \mathbb{Z}$ is finite. When $\zeta \in F_v^*$, e.g., if ζ is the value of the tame part of ϵ_p, then we may rewrite

$$m_v^\zeta = e_v \cdot v\left(\mu^{f_v} + 2\zeta p^{(k-1)f_v} + \zeta^2 \nu^{f_v}\right) \in \mathbb{Z} \cup \{\infty\}.$$

Note that in the unequal slope case $m_v^\zeta = m_v$, if $\zeta \in F_v^*$, so the quantities m_v^ζ may be considered as generalizations of m_v in the equal slope case. In particular taking $\zeta = \pm 1$ we have

$$m_v^\pm = e_v \cdot v\left(\mu^{f_v} \pm 2p^{(k-1)f_v} + \nu^{f_v}\right) \in \mathbb{Z} \cup \{\infty\}.$$

We remark that m_v^+ is finite if and only if $a_p^{f_v} + (\bar{a}_p \epsilon'(p))^{f_v} \neq 0$, and m_v^- is finite if and only if $a_p^{f_v} - (\bar{a}_p \epsilon'(p))^{f_v} \neq 0$, so that one of the two quantities $m_v^\pm$ is always finite.

6.2.1. *The case of odd primes.* We now assume that p is odd and work under a condition on the tame part of ϵ_p.

Theorem 28. *Let p be an odd prime with $N_p = C_p \geq 1$ and $v \mid p$ be a place of F. Assume that the tame part of ϵ_p on G_v is not quadratic. Let ζ be in the image of the tame part of ϵ_p on G_v. Then the parity of*

$$m_v^\zeta = e_v \cdot v\left(\mu^{f_v} + 2\zeta p^{(k-1)f_v} + \zeta^2 \nu^{f_v}\right) \in \mathbb{Z} \cup \{\infty\}$$

is independent of ζ when it is finite, and then X_v is a matrix algebra over F_v if and only if $m_v^\zeta \in \mathbb{Z}$ is even.

Thus, if -1 lies in the image of the tame part of ϵ_p on G_v, and

- if $a_p^{f_v} + (\bar{a}_p \epsilon'(p))^{f_v} \neq 0$, then X_v is a matrix algebra over F_v if and only if $m_v^+ \in \mathbb{Z}$ is even,
- if $a_p^{f_v} - (\bar{a}_p \epsilon'(p))^{f_v} \neq 0$, then X_v is a matrix algebra over F_v if and only $m_v^- \in \mathbb{Z}$ is even,

noting that one of $m_v^{\pm}$ is always finite, and both have the same parity if both are finite. If -1 does not lie in the image of the tame part of ϵ_p on G_v (e.g., if the tame part of ϵ_p is trivial on G_v) and if $m_v^+ < \infty$, then X_v is a matrix algebra over F_v if and only if $m_v^+ \in \mathbb{Z}$ is even.

Proof. The proof goes along the lines of the proof of Theorem 22, with a few modifications. We base change to L so that $\epsilon_p|_{G_L}$ is tame, compute the invariant there, and then descend back to F_v.

We first show that $\tilde{\alpha} : G_L \to \bar{F}_v^*/F_v^*$ is unramified. If the trace of $\rho_f(g)$ is non-zero, then $\alpha(g) \equiv$ trace $\rho_f(g)$ mod F^*, for $g \in G_L$ (cf. part (4) of Proposition 8). If the tame part of ϵ_p is trivial on G_v, then by Langlands' theorem $\alpha(i) \equiv 1 + \epsilon_p(i) = 2 \bmod F^*$, for all $i \in I_L$. So we may assume that the tame part of ϵ_p is non-trivial on G_v. If $\epsilon_p(i) \neq -1$, for $i \in I_L$, then $\alpha(i)$ belongs to F_v^*. Indeed by Langlands' theorem again, $\alpha(i) \equiv 1 + \epsilon_p(i) \bmod F^*$, and since ϵ_p is tame on G_L, $\epsilon_p(i) \in \mathbb{Q}_p^* \subset F_v^*$. If $\epsilon_p(i) = -1$, for $i \in I_L$, we choose $j \in I_L$ such that $\epsilon_p(j) \neq \pm 1$. Such a choice is possible since by assumption the tame part of ϵ_p is not quadratic. The above argument shows that $\alpha(j)$ and $\alpha(ij)$ belong to F_v^*, and since $\alpha(i)\alpha(j)/\alpha(ij) \in F^*$, $\alpha(i) \in F_v^*$ as well.

Write u for the prime of L lying over v and Frob_u be an arithmetic Frobenius at u. We calculate $\mathrm{inv}_L(\mathrm{res}_{F_v/L} c_\alpha)$ using Lemma 9 applied to $K = \alpha|_{G_L}$ and $t = \epsilon'|_{G_L}$, and get

$$\mathrm{inv}_L(\mathrm{res}_{F_v/L} c_\alpha) = \frac{1}{2} \cdot u \left(\frac{\alpha^2}{\epsilon'}(\mathrm{Frob}_u) \right) \mod \mathbb{Z}.$$

Since $[L : F_v]$ is odd (a power of p) we may descend to F_v as before to get

$$\mathrm{inv}_v c_\alpha = \frac{1}{2} \cdot v \left(\frac{\alpha^2}{\epsilon'}(\mathrm{Frob}_u) \right) \mod \mathbb{Z}.$$

Let $\zeta = \epsilon_p(\mathrm{Frob}_u) \in \mathbb{Q}_p^* \subset F_v^*$. Then the usual argument using Langlands' theorem shows that

$$\frac{\alpha^2}{\epsilon'}(\mathrm{Frob}_u) \equiv \mu^{f_v} + 2\zeta p^{(k-1)f_v} + \zeta^2 \nu^{f_v} \mod F_v^{*2}$$

and replacing v with the valuation v such that $v(p) = 1$ we obtain the theorem. We note that the parity of m_v^{ζ} is independent of ζ since $\tilde{\alpha}$ is unramified on G_L. $\square$

6.2.2. *The case of* $p = 2$. We now show that if $p = 2$ and ϵ_2 is not quadratic on G_v, then the ramification of X_v is also determined by $m_v^{\pm}$, up to an error term n_v which depends purely on the nebentypus ϵ_2, which we define now.

If ϵ_2 is trivial on G_v, set $n_v = 0$. If ϵ_2 has order 2^r on G_v, for $r > 1$, let $F_v(\sqrt{t})/F_v$, for $t \in F_v^*$ be the quadratic extension of F_v cut out by the quadratic character $\epsilon_2^{2^{r-1}}$ on G_v. Let ζ_{2^r} be a primitive 2^r-th root of unity and define

$$z = \frac{(1 + \zeta_{2^r})^2}{\zeta_{2^r}} \in F^*$$

noting that $z \in F^*$ by Langlands' theorem. Define n_v mod 2 by

$$(-1)^{n_v} = \epsilon_v(-1) \cdot (t, z)_v,$$

where ϵ_v is the restriction of ϵ_2 to G_v and $(t, z)_v$ is the Hilbert symbol of t and z at v.

Lemma 29. *Assume ϵ_2 has order 2^r on G_v, for $r > 1$. Let h be the function on G_v defined by*

$$h(g) = \begin{cases} \frac{1+\epsilon_2(g)}{\sqrt{\epsilon_2(g)}} & \text{if } \epsilon_2(g) \neq -1 \\ 1 & \text{if } \epsilon_2(g) = -1, \end{cases}$$

and let c_h be the corresponding F-valued 2-cocycle on G_v. Then the class of c_h in ${}_2\mathrm{Br}(F_v)$ is given by the symbol $(t, z)_v$.

Proof. We first claim that if $-1 \neq \zeta = \epsilon_2(g)$ is not a primitive 2^r-th root of unity, then $\frac{1+\zeta}{\sqrt{\zeta}} \in F^*$. Indeed, choose $g \in G_v$ such that $\epsilon_2(g) = \zeta_{2^r}$, where ζ_{2^r} is a primitive 2^r-th root of unity. We may assume $g \in I_v$, and applying Langlands' theorem we obtain that $\frac{(1+\epsilon_2(g))^2}{\epsilon_2(g)} \in F^*$, and hence that $\frac{1+\zeta_{2^{r-1}}}{\sqrt{\zeta_{2^{r-1}}}} \in F^*$, where $\zeta_{2^{r-1}} = \epsilon_2(g^2)$ is a primitive 2^{r-1}-th root of unity. Now set $h = g^2 \in I_v$. Set $d = \frac{\alpha^2}{\epsilon_2}$ on I_v. Then by Langlands' theorem $d(h) \in F^{*2}$. Since $d : I_v \to F^*/F^{*2}$ is a homomorphism we see that $d(h^a) \in F^{*2}$, for all integers a. Hence by Langlands' theorem again we deduce that $\frac{(1+\zeta_{2^{r-1}}^a)^2}{\zeta_{2^{r-1}}^a} \in F^{*2}$, if it is non-zero. Hence $\frac{1+\zeta_{2^{r-1}}^a}{\sqrt{\zeta_{2^{r-1}}^a}} \in F^*$, for all integers a, if it is non-zero, proving the claim. We now claim that if $\epsilon_2(g^b)$ with b odd is any primitive 2^r-th root of unity then $h(g^b) \equiv h(g) \bmod F^*$. Indeed by the discussion above $h(g^{b-1}) \in F^*$ since $b-1$ is even.

The two claims above show that the 2-cocycle c_h is cohomologous to the 2-cocycle c_l where

$$l(g) = \begin{cases} 1 & \text{if } \epsilon_2^{2^{r-1}}(g) = 1, \\ \frac{1+\zeta_{2^r}}{\sqrt{\zeta_{2^r}}} & \text{if } \epsilon_2^{2^{r-1}}(g) = -1. \end{cases}$$

Let σ be the non-trivial element of the Galois group $\mathrm{Gal}(F_v(\sqrt{t})/F_v)$. Let $z = \left(\frac{1+\zeta_{2^r}}{\sqrt{\zeta_{2^r}}}\right)^2 \in F^*$. Then the class of c_l is completely determined by the table

	1	σ
1	1	1
σ	1	z

which is precisely the symbol $(t, z)_v$. $\square$

Theorem 30. *Let $p = 2$ and assume that ϵ_2 is not quadratic on G_v. If ϵ_2 is trivial on G_v and $m_v^+ < \infty$, then X_v is a matrix algebra if and only if $m_v^+ \in \mathbb{Z}$ is even. If ϵ_2 on G_v has order 4 or more and if*

- *$a_p^{f_v} + (\bar{a}_p \epsilon'(p))^{f_v} \neq 0$, then X_v is a matrix algebra if and only if $m_v^+ + n_v \in \mathbb{Z}$ is even,*
- *$a_p^{f_v} - (\bar{a}_p \epsilon'(p))^{f_v} \neq 0$, then X_v is a matrix algebra if and only if $m_v^- + n_v \in \mathbb{Z}$ is even,*

noting that if both $a_p^{f_v} \pm (\bar{a}_p \epsilon'(p))^{f_v} \neq 0$, then $m_v^\pm$ have the same parity.

Proof. If ϵ_2 is trivial on G_v, then by Langlands' theorem, $\alpha(i) \equiv 2 \bmod F^*$, for all $i \in I_v$. Lemma 9 applies directly to prove the first statement. So we may assume that ϵ_2 is not of order 1 or order 2 on G_v. Hence there exists $i \in I_v$, such that $\epsilon_2(i) = \sqrt{-1}$. If $\epsilon_2(j) = -1$, for $j \in I_v$, then a short computation using the fact that $c_\alpha(i, j) \in F^*$ shows that $\alpha(j) \equiv \sqrt{-1} \bmod F^*$.

We define a function $f : G_v \to E^*$ by

$$f(g) = \begin{cases} 1 + \epsilon_2(g) & \text{if } \epsilon_2(g) \neq -1, \\ \sqrt{-1} & \text{if } \epsilon_2(g) = -1. \end{cases}$$

Now define $K : G_v \to E^*$ by $K(g) = \frac{\alpha(g)}{f(g)}$, for $g \in G_v$. Then the cocycle c_α can be decomposed as $c_\alpha = c_K c_f$, where c_K and c_f are the cocycles corresponding to K and f respectively. That these are indeed cocycles follows from the fact that they are F-valued, which can be proved using $\epsilon_2(G_v) = \epsilon_2(I_v)$ and Langlands' theorem.

We first calculate $\mathrm{inv}_v c_K$. By choice of f, $K(i)$ belongs to F^*, for all $i \in I_v$. Since $\epsilon_2(G_v) = \epsilon_2(I_v)$ a computation using Langlands' theorem shows that $\frac{K^2(g)}{\epsilon'(g)} \in F^*$, for all $g \in G_v$. Let σ_v be the Frobenius at the prime v. By Lemma 9 applied to K as above and $t = \epsilon'$ we have

$$\mathrm{inv}_v c_K = \frac{1}{2} \cdot v\left(\frac{K^2}{\epsilon'}(\sigma_v)\right) \bmod \mathbb{Z}.$$

Assume $a_2^{f_v} \neq -(\bar{a}_2\epsilon'(2))^{f_v}$, then we choose σ_v in such a way that $\epsilon_2(\sigma_v) = 1$. Then $\alpha(\sigma_v) \equiv (a_2^{f_v} + (\bar{a}_2\epsilon'(2))^{f_v}) \bmod F^*$, so that $\frac{K^2}{\epsilon'}(\sigma_v) \equiv \mu^{f_v} + \nu^{f_v} + 2p^{(k-1)f_v} \bmod F^{*2}$. Finally, the valuation considered in the statement of the theorem is normalized so that $v(2) = 1$, and differs from the valuation used in the proof by e_v. Noting $e_v f_v = [F_v : \mathbb{Q}_2]$, we obtain

$$\mathrm{inv}_v c_K = \frac{1}{2} \cdot m_v^+ \bmod \mathbb{Z}.$$

If $a_2^{f_v} = -(\bar{a}_2\epsilon'(2))^{f_v}$, then we choose σ_v in such a way that $\epsilon_2(\sigma_v) = -1$. Then $\alpha(\sigma_v) \equiv (a_2^{f_v} - (\bar{a}_2\epsilon'(2))^{f_v}) \bmod F^*$, so that $\frac{K^2}{\epsilon'}(\sigma_v) \equiv \mu^{f_v} + \nu^{f_v} - 2p^{(k-1)f_v} \bmod F^{*2}$. We obtain

$$\mathrm{inv}_v c_K = \frac{1}{2} \cdot m_v^- \bmod \mathbb{Z}.$$

We also remark that since $K^2/\epsilon' : G_v \to F^*/F^{*2}$ is an unramified homomorphism, $\mathrm{inv}_v c_K$ does not depend on the choice of arithmetic Frobenius at v, and in particular $m_v^{\pm}$ have the same parity if both are simultaneously finite.

Now we calculate $\mathrm{inv}_v(c_f)$. Let c_ϵ be the cocycle

$$c_\epsilon(g, h) = \frac{\sqrt{\epsilon(g)}\sqrt{\epsilon(h)}}{\sqrt{\epsilon(gh)}},$$

for g, $h \in G_{\mathbb{Q}}$. We have $\mathrm{inv}_v c_f = \mathrm{inv}_v c_h + \mathrm{inv}_v c_\epsilon$, where h is the function defined in the previous lemma. The theorem now follows from the previous lemma and the fact that $\mathrm{inv}_v c_\epsilon$ is trivial if and only if $\epsilon_v(-1) = 1$ [Qu98]. $\square$

Corollary 31. *Assume that $p = 2$ and ϵ_2 is not quadratic on G_v. Assume also that $F = \mathbb{Q}$. Then:*

(1) *If $\epsilon_2(-1) = 1$, then X_v is a matrix algebra over F_v if and only if one of $m_v^{\pm} \in \mathbb{Z}$ is even.*
(2) *If $\epsilon_2(-1) = -1$, then X_v is a matrix algebra over F_v if and only if one of $m_v^{\pm} \in \mathbb{Z}$ is odd.*

Proof. We show that the symbol $(t, z)_v$ vanishes when $F = \mathbb{Q}$, so that $n_v = 0 \bmod 2$ if and only if $\epsilon_2(-1) = 1$. Note that $\mathbb{Q}$ has three quadratic extensions of absolute discriminant a power of 2, namely

$\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-2})$, but only the middle one is cut out by the quadratic character $\epsilon_2^{2^{r-1}}$, since it is a even character of level 8. It follows that $t = 2 \in \mathbb{Q}_2$ and $(t, z)_v = (t, N_{F_v/\mathbb{Q}_2}(z))_2$.

To compute the norm, we assume F is general. Now $N_{\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}}(\zeta_{2^r}) = 1$ and $N_{\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}}(1 + \zeta_{2^r}) = 2$ for all $r > 1$, since the minimal polynomial of $1 + \zeta_{2^r}$ is $(x - 1)^{2^{r-1}} + 1 = 0$. Since the local norm is the same as the global norm, we have $N_{\mathbb{Q}_2(\zeta_{2^r})/\mathbb{Q}_2}(z) = 4$. We have $\mathbb{Q}_2 \subset \mathbb{Q}(z)_v \subset \mathbb{Q}_2(\zeta_{2^r})$. Noting that the second index is 2, by the transitivity of the norm in towers we have $N_{\mathbb{Q}(z)_v/\mathbb{Q}_2}(z)^2 = 4$, and we obtain $N_{\mathbb{Q}(z)_v/\mathbb{Q}_2}(z) = \pm 2$. Since $z \in F$, by the transitivity of the norm again, we obtain $N_{F_v/\mathbb{Q}_2}(z) = (\pm 2)^d$ where $d = [F_v : \mathbb{Q}(z)_v]$.

Thus $(t, z)_v = (t, N_{F_v/\mathbb{Q}_2}(z))_2 = (2, \pm 2)_2^d = 1$, since $(2, \pm 2)_2 = 1$, as one can check directly. □

The corollary predicts that when $p = 2$ and $F = \mathbb{Q}$, there is a switch in the parity of $m_v^{\pm}$ in determining the triviality of the class of X_v, when ϵ_2 moves from even to odd characters. For a numerical example of this interesting phenomenon, see Example 3 at the end of the paper.

6.2.3. *Remaining quadratic cases.* If the tame part of ϵ_p is quadratic on G_v for an odd prime p or if $p = 2$ and ϵ_2 is quadratic on G_v we again show that X_v is determined completely by $m_v^{\pm}$ up to an extra Hilbert symbol. The following results are quite general and hold for the unequal slope case also. In the case of unequal slope the extra symbol is trivial.

We need some notation.

Assume that the quadratic extension cut out by the tame part of ϵ_p if p is odd, or by ϵ_p if $p = 2$, is $F_v(\sqrt{t})$, for some $t \in F_v^*$.

Define
$$a = \frac{\mu^{f_v} + \nu^{f_v} + 2p^{(k-1)f_v}}{\mu^{f_v} + \nu^{f_v} - 2p^{(k-1)f_v}} \in F^* \cup \{0, \infty\}.$$
Note $a \in F^*$ if and only if $a_p^{f_v} \neq \pm(\bar{a}_p \epsilon'(p))^{f_v}$. In this case define the integer n_v mod 2 by $(-1)^{n_v} = (t, a)_v$. Let $p^\dagger \nmid N$ be an auxiliary prime such that $a_{p^\dagger} \neq 0$ and such that, for all $\gamma \in \Gamma$,
$$\chi_\gamma(p^\dagger) = \begin{cases} \text{-1} & \text{if } \chi_\gamma \text{ is ramified at } p, \\ 1 & \text{if } \chi_\gamma \text{ is unramified at } p. \end{cases}$$
We can always choose $p^\dagger$ as above, since f is a non-CM form. Since ϵ^{-1} is an extra twist, we have $\epsilon(p^\dagger) = -1$. Let
$$b = a_{p^\dagger}^2 = -\frac{a_{p^\dagger}^2}{\epsilon(p^\dagger)} \in F^*.$$
If $a_p^{f_v} = (\bar{a}_p \epsilon'(p))^{f_v}$, define an integer n_v mod 2 by $(-1)^{n_v} = (t, b)_v$, and if $a_p^{f_v} = -(\bar{a}_p \epsilon'(p))^{f_v}$, define n_v by $(-1)^{n_v} = (t, b)_v \cdot (-1)^{(e_v v(b))}$.

Theorem 32. *Assume that the tame part of ϵ_p is quadratic for an odd prime p, or $p = 2$ and ϵ_2 is quadratic.*

(1) *Assume that $a \in F^*$. Then, X_v is a matrix algebra over F_v if and only if*
$$m_v^+ + n_v$$
is even.

(2) *If* $a_p^{f_v} = (\bar{a}_p\epsilon'(p))^{f_v}$, *then* X_v *is a matrix algebra over* F_v *if and only if*

$$m_v^+ + n_v$$

is even.

(3) *If* $a_p^{f_v} = -(\bar{a}_p\epsilon'(p))^{f_v}$, *then* X_v *is a matrix algebra over* F_v *if and only if*

$$m_v^- + n_v$$

is even.

Proof. If $\epsilon_p(i) = -1$, for $i \in I_v$, then $\alpha^2(i) \in F^*$. We claim that the image of $\alpha(i)^2$ in F_v^*/F_v^{*2} is constant, i.e., there exists $d \in F_v^*$ such that $\alpha^2(i) \equiv d \bmod F_v^{*2}$. Indeed, a priori $\alpha(i) = \sqrt{t(i)}d(i)$, for some $t(i)$, $d(i) \in F_v^*$. If $j \in I_v$ with $\epsilon_p(j) = -1$, then by Langlands' theorem, since $\epsilon_p(ij) = 1$, $\alpha(ij) \in F^*$. Since $c_\alpha(i,j) \in F^*$, we get $\sqrt{t(i)} \equiv \sqrt{t(j)} \bmod F_v^*$, as desired. Thus $\sqrt{t(i)} \equiv \sqrt{d} \bmod F_v^*$ for all $i \in I_v$ such that $\epsilon_p(i) = -1$. We compute d and show that the ramification of X_v is controlled by $m_v^\pm$, and an extra Hilbert symbol involving d. In case (1) we show we can take $d = a$, whereas in case (2) and (3) we show take $d = b$.

For p odd, we do a base change as in Theorem 22 and assume without loss of generality that ϵ_p is tame (and quadratic).

Assume we are in case (1), so that $a \in F^*$. Let σ_v be an arithmetic Frobenius at v, such that $\epsilon_p(\sigma_v) = 1$. Let $i \in I_v$ be such that $\epsilon_p(i) = -1$. By Langlands' theorem,

$$\frac{\alpha(\sigma_v)}{\alpha(\sigma_v i)} \equiv \sqrt{a} \bmod F^*.$$

Since $c_\alpha(\sigma_v, i) \in F^*$, and a belongs to F^*, we have $\alpha(i) \equiv \sqrt{a} \bmod F^*$. We define a function f on G_v by

$$f(g) = \begin{cases} 1 & \text{if } \epsilon_p(g) = 1, \\ \sqrt{a} & \text{if } \epsilon_p(g) = -1. \end{cases}$$

Let $K(g) = \frac{\alpha(g)}{f(g)}$ on G_v. Then the cocycle c_α can be decomposed as $c_\alpha = c_K c_f$. Clearly $K(i)$ belongs to F_v^*, for all $i \in I_v$. Using Lemma 9 applied to K and $t = \epsilon'$, we have $\mathrm{inv}_v c_K = \frac{1}{2} \cdot v\left(\frac{K^2}{\epsilon'}(\sigma_v)\right) = \frac{1}{2} \cdot m_v^+ \bmod \mathbb{Z}$. To compute $\mathrm{inv}_v c_f$, let σ be the nontrivial element of $\mathrm{Gal}(F_v(\sqrt{t})/F_v)$. Then the cocycle table of the cocycle c_f is given by

	1	σ
1	1	1
σ	1	a

which gives the symbol $(t,a)_v$. This proves (1).

We now turn to parts (2) and (3). We wish to find $d \in F^*$, such that $\alpha(i) \equiv \sqrt{d} \bmod F_v^*$, if $\epsilon_p(i) = -1$. We cannot take $d = a$ in parts (2) and (3) since $a = 0$ or ∞. So we argue a bit differently.

Let $i \in I_v$ with $\epsilon_p(i) = -1$. We claim that $\alpha(i) \equiv a_{p^\dagger} \bmod F^*$. By (3.1) and the proof of Theorem 16, if χ_γ is unramified at p, then $\alpha(i)^\gamma = \alpha(i)$. Similarly, if χ_γ is ramified at p, then $\alpha(i)^\gamma = \chi_\gamma(i)\alpha(i) =$

$\epsilon_p(i)\alpha(i) = -\alpha(i)$. Thus, if $\mathrm{Frob}_{p^\dagger}$ is an arithmetic Frobenius at the prime $p^\dagger$, then $\alpha(i) \equiv \alpha(\mathrm{Frob}_{p^\dagger}) \equiv a_{p^\dagger} \bmod F^*$, as claimed. Define f on G_v by

$$f(g) = \begin{cases} 1 & \text{if } \epsilon_p(g) = 1, \\ a_{p^\dagger} & \text{if } \epsilon_p(g) = -1. \end{cases}$$

Let $K(g) = \frac{\alpha(g)}{f(g)}$ on G_v. Then the cocycle c_α can be decomposed as, $c_\alpha = c_K c_f$. We now proceed as in the proof of part (1). If $a_p^{f_v} + (\bar{a}_p\epsilon'(p))^{f_v} \neq 0$, the cocycle c_K has invariant $\mathrm{inv}_v c_K = \frac{1}{2} \cdot m_v^+ \bmod \mathbb{Z}$. If $a_p^{f_v} - (\bar{a}_p\epsilon'(p))^{f_v} \neq 0$, then we get an extra term on evaluating α at an arithmetic Frobenius Frob_v for which $\epsilon_p(\mathrm{Frob}_v) = -1$, and get $\mathrm{inv}_v(c_K) = \frac{1}{2} \cdot (m_v^- - e_v \cdot v(b))$. It remains to calculate $\mathrm{inv}_v c_f$. Let σ be the nontrivial element of the Galois group of the quadratic field cut out by ϵ_p. The table for the cocycle c_f is given by

	1	σ
1	1	1
σ	1	b

which is clearly the symbol $(t, b)_v$. This proves (2) and (3). □

The above theorem shows that the ramification of X at the place v is determined by $m_v^\pm$ and one extra Hilbert symbol. We can calculate those symbols using the formulas of page 211-212 of [Se80], except if $p = 2$ and $F_v \neq \mathbb{Q}_2$, in which case we can use the formulas stated, e.g., in [Sn81] and [FV93].

7. Supercuspidal primes

We assume in this section that p is an odd prime, $N_p \geq 2$ and $N_p > C_p$, and prove a weak result on the ramification of X_v. Since $a_p = 0$, results of the kind proved so far, relating the ramification to the valuations of expressions involving the Fourier coefficients at p, are no longer possible.

Note that when the local Galois representation is a twist of cases already treated above we can often predict the ramification since the Brauer class of the endomorphism algebra is invariant under twist. Thus we may assume that the local Galois representation is supercuspidal, and is induced by a character χ of an index two subgroup G_K of the local Galois group $G_p = G_{\mathbb{Q}_p}$, i.e.,

$$\rho_f|_{G_p} \sim \mathrm{Ind}_{G_K}^{G_p} \chi.$$

We manage to sometimes predict the ramification of X_v in terms of this character. Let σ be the nontrivial automorphism of $K/\mathbb{Q}_p$. We define an extension L of F_v and for an arithmetic Frobenius Frob_u of L set

$$m_v := e_v \cdot v\left(\frac{(\chi(\mathrm{Frob}_u) + \chi^\sigma(\mathrm{Frob}_u))^2}{\epsilon'(p)^{f_v}}\right) \in \mathbb{Z} \cup \{\infty\},$$

where v is normalized such that $v(p) = 1$. Note $m_v < \infty$, if $\chi(\mathrm{Frob}_u) + \chi^\sigma(\mathrm{Frob}_u) \neq 0$.

Proposition 33. *Assume F_v contains K. If m_v is finite, then X_v is a matrix algebra over F_v if and only if m_v is even.*

Proof. Since F_v contains K, we have

$$\rho_f|_{I_v} \sim \begin{pmatrix} \chi & 0 \\ 0 & \chi^\sigma \end{pmatrix}.$$

So if $i \in I_v$ and $\chi(i) \neq -\chi^\sigma(i)$, then by part (4) of Proposition 8

$$\alpha(i) \equiv (\chi(i) + \chi^\sigma(i)) \bmod F^*.$$

If $K = \mathbb{Q}_{p^2}$ is unramified, then we may write $\chi|_{I_K} = \omega_2^j \chi_1 \chi_2$, where, following the notation of [GM09, §3.3], ω_2 is the fundamental character of level two and χ_i, for $i = 1, 2$, are characters of p-power order. On the other hand if $K/\mathbb{Q}_p$ is ramified then, in the notation of [GM09, §3.4], we may write $\chi|_{I_K} = \omega^j \chi_1 \chi_2$, where ω is the Teichmüller character and again the χ_i have p-power order. Choose an extension L of odd degree over F_v such that ϵ_p is tame and χ_i, for $i = 1, 2$, are trivial, when restricted to I_L. In the unramified case, $\omega_2^\sigma = \omega_2^p$, and we get $\alpha(i) \equiv \omega_2^j(i) + \omega_2^{pj}(i) \bmod F^*$, for $i \in I_L$ such that the expression on the right is non-zero. Since ω_2 takes value in the (p^2-1)-th roots of unity and F_v contains $\mathbb{Q}_{p^2}$, we see that $\alpha(i) \in F_v^*$, for $i \in I_L$, under the non-vanishing assumption. Since, $\tilde{\alpha}$ is a homomorphism, we can show $\alpha(i)$ belongs to F_v^* even if the expression on the right vanishes, by the usual argument. In the ramified case, $\omega = \omega^\sigma$, and we have $\alpha(i) \equiv (\omega^j(i) + \omega^{\sigma j}(i)) = 2\omega^j(i) \bmod F^*$, for $i \in I_L$. Since ω takes values in the $(p-1)$-th roots of unity, we again deduce that $\alpha(i) \in F_v^*$, for $i \in I_L$.

Let u be the prime of L lying over v. By Lemma 9 applied to $K = \alpha$ and $t = \epsilon'$, both restricted to G_L, we have

$$\mathrm{inv}_L(\mathrm{res}_{F_v|L} c_\alpha) = \frac{1}{2} \cdot u\left(\frac{\alpha^2}{\epsilon'}(\mathrm{Frob}_u)\right) \bmod \mathbb{Z}.$$

Here as usual since ϵ_p is tame when restricted to L, $\epsilon_p(g) \in \mathbb{Q}_p^*$, and since $\frac{\alpha^2}{\epsilon}(g) \in F^*$, we get $\frac{\alpha^2}{\epsilon'}(g) \in F_v^*$, for all $g \in G_L$. If $[L : F_v] = p^t$, then $\mathrm{inv}_L(\mathrm{res}_{F_v|L} c_\alpha) = p^t \cdot \mathrm{inv}_v c_\alpha$, so X_v is a matrix algebra over F_v if and only if $e_{L/F_v} \cdot v(\frac{\alpha^2}{\epsilon'}(\mathrm{Frob}_u))$ is even, where $e_{L/F_v} = p^t$ is the degree of the totally ramified extension L/F_v and v is the surjective valuation of F_v^* onto $\mathbb{Z}$. If we choose the valuation v such that $v(p) = 1$, then X_v is a matrix algebra if and only if $e_v \cdot v(\frac{\alpha^2}{\epsilon'}(\mathrm{Frob}_u))$ is even. Since, the inertia degree of L/F_v is also f_v, we get the desired result. $\square$

8. Numerical Examples

We end this paper with some examples. For forms of quadratic nenbetypus, the examples were generated by the program `Endohecke` due to Brown and Ghate, which was made by suitably modifying the C++ program `Hecke` created by W. Stein. The notation for the nebentypus is the one used in these programs (and not that used in [GGQ05]). For forms of non-quadratic nebentypus, we used tables of Quer [Qu05]. The first example is a Steinberg case, the next two are unequal slope ramified principal series (RPS) cases, whereas the remaining examples are equal slope RPS cases.

(1) Let $f \in S_5(15, [2, 1])$ be the unique primitive form. It is Steinberg at the prime 5 since $N_5 = 1$ and $C_5 = 0$. F is a cubic extension of $\mathbb{Q}$. Now, 5 decomposes into two distinct primes v_1, v_2 in F with ramification index and inertia degree $(1, 1)$ and $(2, 1)$ respectively. It turns out that X_{v_1} is ramified but X_{v_2} is not ramified, as predicted by Theorem 15.

(2) Let $f \in S_3(35, [2,2])$ be the unique primitive form of orbit size 4. $F = \mathbb{Q}$ and X is ramified at the RPS prime 5. Also $v_5(\mu+\nu) = v_5(\mu+\nu+10) = 1$, corroborating Theorem 22.
(3) Let $f \in S_2(88, [2,2,2])$ be the unique primitive form of orbit size 4. Then $F = \mathbb{Q}(\sqrt{2})$ and X is ramified at the unique prime v of F lying above the RPS prime 2. One checks $\mu+\nu = -\sqrt{2}$ so $v(\mu+\nu) = v(\mu+\nu+4) = 1/2$, hence $m_v = [F_v : \mathbb{Q}_2] \cdot 1/2 = 1$ is odd, supporting Theorem 27.
(4) Let $f \in S_2(35, [4,2])$ be the unique primitive form of orbit size 4. Then $F = \mathbb{Q}$ and X is ramified at the RPS prime 5 (and also at the good prime 2). One checks $\mu = -\nu = -5i$, so $v_5(\mu+\nu+10) = 1$, hence $m_v^+ = 1$ is odd, supporting Theorem 28.
(5) Let $f \in S_2(112, [2,4,2])$ be the primitive form of orbit size 4 with $a_2 = 1+i$. Then $F = \mathbb{Q}$ and $p = 2$ is an RPS prime, since ϵ_2 has level 16, with 'tame' part of order 2, and 'wild' part of order 4. Now $\mu = -\nu = 2i$, so $v(\mu+\nu \pm 2p) = v(\pm 4) = 2$ is even, yet X is ramified at 2 (X is also ramified at 3). This interesting 'switch in parity' is predicted by part (2) of Corollary 31. We thank E. González-Jiménez for finding this example.
(6) Let $f \in S_2(363, [2,2])$ be the unique eigenform of orbit size 4. Then $F = \mathbb{Q}$ and X is ramified at the RPS prime 3. Yet $m_v = m_v^+ = v_3(\mu+\nu+6) = 2$ is even. This is an equal slope case, so we use Theorem 32. We compute that $a = -3$ and $t = -3$. Since $(-3,-3)_3 = -1$, we have $n_v = 1$ mod 2. Thus part (1) of Theorem 32 holds, and explains the switch in parity.
(7) Let $f \in S_3(91, [2,2])$ be the eigenform of orbit size 4. Then $F = \mathbb{Q}$ and X is not ramified at the RPS prime 7. Now $a_7 = \pm 7i = \bar{a}_7\epsilon'(7)$, so we cannot use part (1) of Theorem 32, since $\mu = \nu = 49$ and $a = \infty$. We use part (2) instead. We take $p^\dagger = 3$ and see $b = a_3^2 = -26$. Also $t = -7$ and $m_v^+ = 2$ is even. We have $(-26,-7)_7 = 1$, so $n_v = 0$. This corroborates part (2) of Theorem 32.

Acknowledgements: D.B. was partly supported by ARC grant DP0773301. He thanks the second author for constant encouragement during the course of his Ph. D. at TIFR. E.G. was partly supported by the Indo-French (CEFIPRA-IFCPAR) project 3701-2. Part of this work was done at the Institut Henri Poincaré during the "Galois trimester" in 2010. Finally, the authors thank Ken Ribet for his interest and his support.

References

[AL78] A. Atkin and W. Li. Twists of newforms and pseudo-eigenvalues of W-operators. *Invent. Math.*, 48(3):221–243, 1978.

[BG11] D. Banerjee and E. Ghate. Crossed product algebras attached to weight one forms. *Math. Res. Lett.*, 18(1):141–150, 2011.

[BG04] A. Brown and E. Ghate. Endomorphism algebras of motives attached to elliptic modular forms. *Ann. Inst. Fourier (Grenoble)*, 53(6):1615–1676, 2003.

[FV93] I. Fesenko and S. Vostokov. Local Fields and Their Extensions. A constructive approach. *Translations of Mathematical Monographs, 121. American Mathematical Society*, 1993.

[GJ78] S. Gelbart and H. Jacquet. A relation between automorphic representations of GL(2) and GL(3). *Ann. Sci. École Norm. Sup. (4)*, 11(4):471–542, 1978.

[GGQ05] E. Ghate, E. González-Jiménez and J. Quer. On the Brauer class of modular endomorphism algebras. *Int. Math. Res. Not.*, 12:701–723, 2005.

[GM09] E. Ghate and A. Mézard. Filtered modules with coefficients. *Trans. Amer. Math. Soc.*, 361(5):2243–2261, 2009.

[Hi00] H. Hida. Modular forms and Galois cohomology. *Cambridge Studies in Advanced Mathematics, 69. Cambridge University Press*, 2000.

[KZ91] W. Kohnen and D. Zagier. Values of L-series of modular forms at the center of the critical strip. *Invent. Math.*, 64(2):175–198, 1981.

[Mi89] T. Miyake. Modular forms. *Springer Verlag, Berlin*, 1989.

[Mo81] F. Momose. On the l-adic representations attached to modular forms. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 28(1):89–109, 1981.

[Pi98] R. Pink. Compact subgroups of linear algebraic groups. *J. Algebra*, 206(2):438–504, 1998.

[Qu98] J. Quer. La classe de Brauer de l'algèbre d'endomorphismes d'une variété abélienne modulaire. *C. R. Acad. Sci. Paris*, 327(3): 227–230, 1998.

[Qu05] J. Quer. Tables of modular endomorphism algebras $X_f = \mathrm{End}(M_f)$ of motives M_f attached to non-CM newforms. 255 pages, 2005.

[Ri75] K. Ribet. Endomorphisms of semi-stable abelian varieties over number fields. *Ann. Math. (2)*, 101:555–562, 1975.

[Ri80] K. Ribet. Twists of modular forms and endomorphisms of abelian varieties. *Math. Ann.*, 253(1):43–62, 1980.

[Ri81] K. Ribet. Endomorphism algebras of abelian varieties attached to newforms of weight 2. *Progr. Math.*, 12, Birkhäuser, Boston, Mass., 263–276, 1981.

[Ri85] K. Ribet. On ℓ-adic representations attached to modular forms. II. *Glasgow Math. J.*, 27:185–194, 1985.

[Ri04] K. Ribet. Abelian varieties over $\mathbb{Q}$ and modular forms. *Modular curves and abelian varieties*, Prog. Math. 224, Birkhaüser, 241–261, 2004.

[Sa97] T. Saito. Modular forms and p-adic Hodge theory. *Invent. Math*, 129(3):607–620, 1997.

[Sh71] G. Shimura. Introduction to the arithmetic theory of automorphic functions. *Princeton University Press, Princeton*, 1971.

[Sh73] G. Shimura. On modular forms of half integral weight. *Ann. of Math. (2)*, 97:440–481, 1973.

[Sc90] A. Scholl. Motives for modular forms. *Invent. Math.*, 100(2):419–430, 1990.

[Sn81] S. Sen. On explicit reciprocity laws. II. *J. Reine Angew. Math.*, 323:68–87, 1981.

[Se80] J-P. Serre. Local fields. *Graduate Texts in Mathematics, 67. Springer Verlag*, 1980.

[Wa81] J-L. Waldspurger. Sur les coefficients de Fourier des formes modulaires de poids demi-entier. *J. Math. Pures Appl.*, 9(4):375–484, 1981.

Mathematical Sciences Institute, Australian National University, Canberra, ACT 0200

E-mail address: `debargha.banerjee@anu.edu.au`

School of Mathematics, TIFR, Homi Bhabha Road, Mumbai 400005

E-mail address: `eghate@math.tifr.res.in`