J. Inst. Math. Jussieu (2014) **13**(3), 517–559
doi:10.1017/S1474748013000182

DETERMINANTS OF SUBQUOTIENTS OF GALOIS REPRESENTATIONS ASSOCIATED WITH ABELIAN VARIETIES

ERIC LARSON AND DMITRY VAINTROB

[1] *Department of Mathematics Faculty of Arts and Sciences, Harvard University, One Oxford Street, Cambridge, MA, 02138, USA* (elarson3@gmail.com)

[2] *Department of Mathematics, Massachusetts Institute of Technology, Headquarters Office, Building 2, Room 236, 77 Massachusetts Avenue, Cambridge, MA 02139-4307, USA*

(Received 23 December 2012; revised 22 May 2013; accepted 23 May 2013; first published online 18 July 2013)

Abstract Given an abelian variety A of dimension g over a number field K, and a prime ℓ, the ℓ^n-torsion points of A give rise to a representation $\rho_{A,\ell^n} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_{2g}(\mathbb{Z}/\ell^n\mathbb{Z})$. In particular, we get a mod-ℓ *representation* $\rho_{A,\ell} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_{2g}(\mathbb{F}_\ell)$ and an ℓ*-adic representation* $\rho_{A,\ell^\infty} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_{2g}(\mathbb{Z}_\ell)$. In this paper, we describe the possible determinants of subquotients of these two representations. These two lists turn out to be remarkably similar.

Applying our results in dimension $g = 1$, we recover a generalized version of a theorem of Momose on isogeny characters of elliptic curves over number fields, and obtain, conditionally on the Generalized Riemann Hypothesis, a generalization of Mazur's bound on rational isogenies of prime degree to number fields.

Keywords: abelian varieties; Galois representations

2010 *Mathematics subject classification:* Primary 11G05
Secondary 14K02; 11G15; 14K15

1. Introduction

Let A be a g-dimensional abelian variety over a number field K. The ℓ*-adic Tate module*

$$A[\ell^\infty] := \varprojlim_n A[\ell^n]$$

is the limit of ℓ-power torsion points over $\overline{K}$. It is a $\mathbb{Z}_\ell$-lattice with action by the Galois group $G_K := \mathrm{Gal}(\overline{K}/K)$, and is one of the fundamental examples of a Galois representation.

We study in this paper one-dimensional Galois characters arising from these representations. Namely, we consider determinants of subquotients of $A[\ell^\infty]$ with scalars extended from $\mathbb{Z}_\ell$ to either ℓ-adic fields or finite fields $\mathbb{F}_{\ell^n}$. Any such determinant character with values in a field k appears after extending scalars all the way to $\overline{k}$. Hence studying these determinant characters with scalars extended to $\overline{\mathbb{Q}}_\ell$ gives all such characters with values in an ℓ-adic field, and extending scalars to $\overline{\mathbb{F}}_\ell$ gives all such characters with values in $\mathbb{F}_{\ell^n}$.

If V is a representation of a group G over a field k, we say that $\psi : G \to \bar{k}$ is an *associated character* of degree d of V if there is a d-dimensional subquotient W of $V \otimes_k \bar{k}$ such that $\psi = \det_{\bar{k}} W$. We call our principal objects of study — the associated characters of $A[\ell^\infty] \otimes \mathbb{Q}_\ell$ and $A[\ell^\infty] \otimes \mathbb{F}_\ell = A[\ell]$ — the *ℓ-adic* and *mod-ℓ* associated characters of A respectively.

The study of such associated characters goes back to Serre's foundational work on the Open Image Theorem, which states that for an elliptic curve E without complex multiplication (CM), the action of G_K on the adèlic Tate module $H_1(E, \widehat{\mathbb{Z}}) = \prod_\ell E[\ell^\infty]$ is open (i.e. has finite index) in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. This is proved in two principal steps. First, in [16], Serre shows that the ℓ-adic image $\rho_{E,\ell^\infty} : G_K \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ has finite index for all ℓ. Second, in [17], Serre shows that for sufficiently large primes, the mod-ℓ image $\rho_{E,\ell} : G_K \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ is surjective. In each case, the proof proceeds by reducing the problem to the study of the ℓ-adic and mod-ℓ associated characters of E respectively (i.e. studying the Galois action on the one-dimensional subquotients).

A major conjecture, which is still open, is whether the index of the image of G_K in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ is bounded *uniformly* in E. The first step in this direction, for $K = \mathbb{Q}$, is Mazur's seminal theorem on isogenies [9]. This theorem is equivalent to the statement that, for an elliptic curve E over $\mathbb{Q}$ and for a prime $\ell > 163$, the ℓ-torsion module $E[\ell]$ is irreducible (equivalently, no isogenies $E \to E'$ defined over $\mathbb{Q}$ have kernel of order ℓ). An essential step of Mazur's proof is analyzing the possible associated characters (up to torsion of small degree) of subquotients of $E[\ell]$, and ultimately showing that for $\ell > 163$ the list of possible associated characters is empty.

Momose in [13] gives an exhaustion (i.e. a list containing all possibilities, perhaps with excess) for the mod-ℓ associated characters of elliptic curves over number fields K attached to subquotients of $E[\ell]$, for ℓ sufficiently large depending on K. When K is quadratic, $K \neq \mathbb{Q}[\sqrt{D}]$ for $D \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$, the list of possible associated characters is empty. In particular, any elliptic curve E over such a quadratic field K has irreducible torsion module $E[\ell]$ (equivalently, admits no ℓ-isogenies) as long as $\ell > C_K$ for some constant C_K that depends only on K.

The main theorem of our paper gives an analogous exhaustion for abelian varieties of dimension g over K. Applied to elliptic curves, it gives slightly stronger versions of the above results of Momose (see Theorem 1 and Corollary 2 below). While it is hopeless to try to classify all proper subquotients of $A[\ell]$ for $g > 1$, achieving a complete characterization of their determinants is more feasible — and this is the task that we study in this paper.

Our paper consists of two main parts. First we give an essentially complete classification of ℓ-adic associated characters of abelian varieties. This analysis is relatively simple, but requires a number of technical results including Faltings' Theorem [4] and the theory of Shimura varieties of PEL type [3]. It also uses the local characterization of determinants of subquotients of the p-adic Tate module, proved by Brian Conrad in Appendix using p-adic Hodge theory. Second, we given an exhaustion, for ℓ greater than some constant depending only on K and g, of mod-ℓ associated characters. This part is significantly more involved but uses less machinery: we use a

https://doi.org/10.1017/S1474748013000182 Published online by Cambridge University Press

result of Raynaud to control the action of the inertia groups at primes dividing ℓ, and use the Weil conjectures (and Grothendieck's generalization in [6] for primes of bad reduction) to control the behavior of Frobenius elements at primes not dividing ℓ. These pieces of information are then combined to produce a list of explicit expressions for the mod-ℓ associated characters in terms of class field theory.

An abelian variety with a mod-ℓ associated character does not necessarily have an ℓ-adic associated character; therefore, *a priori*, there could be many more possibilities for mod-ℓ associated characters than for ℓ-adic associated characters. Remarkably, this is not the case: *our list of possible mod-ℓ characters is closely related to the list of ℓ-adic associated characters that can occur.*

The relationship between ℓ-adic and mod-ℓ associated characters is particularly sharp in dimension $g = 1$ (elliptic curves), especially under GRH. This case was first studied by Fumiyuki Momose [13], who proved the following theorem for the case where ψ is an isogeny character (i.e. results from a Borel image). More generally, we prove:

Theorem 1 (Theorem 6.4). *Let K be a number field. Then, there exists a finite set S_K of prime numbers depending only on K such that, for a prime $\ell \notin S_K$, and an elliptic curve E over K for which $E[\ell] \otimes \overline{\mathbb{F}}_\ell$ is reducible with degree 1 associated character ψ, one of the following holds.*

(1) *There exists a CM elliptic curve E', defined over K and whose CM field is contained in K, with an ℓ-adic degree 1 associated character whose mod- ℓ reduction ψ' satisfies*

$$\psi^{12} = (\psi')^{12} \tag{1}$$

(2) *The Generalized Riemann Hypothesis fails for $K[\sqrt{-\ell}]$, and*

$$\psi^{12} = \mathrm{cyc}_\ell^6, \tag{2}$$

where cyc_ℓ is the cyclotomic character. (Moreover, in this case we must have $\ell \equiv 3$ mod 4 and the representation $\rho_{E,\ell}$ is already reducible over $\mathbb{F}_\ell$.)

Remark 1.1. The proof of Theorem 1 implies that E' depends only on E (not on ℓ); moreover, $\psi' \otimes \psi^{-1}$ is ramified only at primes of bad additive reduction for E or at primes dividing the discriminant Δ_K of K. The proof also shows that the set S_K is effectively computable; in Theorem 7.9, we give an explicit bound on the value of $\prod_{\ell \in S_K} \ell$.

Theorem 1 implies the following result. (This is also a straightforward consequence of the results of [10] and [13], but does not appear to be written anywhere in the literature.)

Corollary 2 (Corollary 6.5). *Under GRH, the degrees of prime degree isogenies of elliptic curves over K are bounded uniformly if and only if K does not contain the Hilbert class field of an imaginary quadratic field (i.e. if and only if there are no elliptic curves with CM defined over K).*

https://doi.org/10.1017/S1474748013000182 Published online by Cambridge University Press

Theorem 1 follows from the more general Theorem 3, which gives an analogous statement for arbitrary abelian varieties. To formulate it, we need to first describe the ℓ-adic associated characters of abelian varieties.

Using a theorem of Faltings [4], we will see that any ℓ-adic associated character arises from an F-eigenspace in the Tate module of an abelian variety B with (generalized) *complex multiplication* by F (i.e. with an action by an order in F, where F is a CM field or $F = \mathbb{Q}$). Note that we do *not* assume that $\deg F = 2 \cdot \dim B$ (as is the case in the classical theory of complex multiplication); if this is the case, we call it *full* CM. We will see that such associated characters can be explicitly determined (up to twists) by the *CM type* of B, i.e. the isomorphism class of the K–F bimodule $\Phi = \mathrm{Lie}(B)$; which is automatically *balanced*, i.e. satisfies $\Phi \oplus \overline{\Phi} \simeq F^n \otimes_{\mathbb{Q}} K$ for some integer n (see Lemma 3.11).

Specifically, given a balanced CM type (F, Φ), we define a field $K_{F,\Phi}$ and Galois character $\psi_{F,\Phi} : G_{K_{F,\Phi}} \to \overline{\mathbb{Q}}_\ell^\times / \mu_F$ (where μ_F is the group of roots of unity in F), which are uniquely determined by the following properties, as shown in Theorems 3.6 and 3.10. (Technically, the character $\psi_{F,\Phi}$ depends on a choice of embedding $\sigma : F \hookrightarrow \overline{\mathbb{Q}}_\ell$ as well, but we will usually suppress this and assume that we have chosen an appropriate embedding.)

(1) If an abelian variety B over K has CM of type (F, Φ) which is defined over K, then $K_{F,\Phi}$ is contained in the ground field K.

(2) In the above case, the associated characters of the F-eigenspaces of $B[\ell^\infty] \otimes \mathbb{Q}_\ell$ define characters $\psi_{B,\sigma} : G_K \to \overline{\mathbb{Q}}_\ell^\times$ (indexed by embeddings $\sigma : F \hookrightarrow \overline{\mathbb{Q}}_\ell$), and

$$\psi_{F,\Phi}|_{G_K} \equiv \psi_{B,\sigma} \bmod \mu_F.$$

(3) The field $K_{F,\Phi}$ is the *separating field* (i.e. minimal field of definition of the geometrically irreducible components) of the Shimura (coarse moduli) variety for some nonempty collection of polarized abelian varieties with CM type (F, Φ).

Roughly speaking, our main result is that there exists an effectively computable finite set $S_{K,g}$ such that for $\ell \notin S_{K,g}$ and ψ a mod-ℓ associated character of a g-dimensional abelian variety, ψ^a is equal (mod ℓ) to a character $\psi_{F,\Phi}^b$ arising from a CM type (F, Φ) with separating field $K_{F,\Phi}$ contained in K, for some exponents $a > 0$ and $b \geqslant 0$. The exponents a and b, and the dimension $\dim_K \Phi$ of abelian varieties of CM type (F, Φ) are both bounded by a constant depending only on g (i.e. independent of the abelian variety and the ground field K), and satisfy some additional restrictions. To improve our bound on $\dim_K \Phi$, we note that if ψ_0 is an associated character of A, then $\mathrm{cyc}_\ell^d \otimes \psi_0^{-1}$ is also an associated character of A, due to the Galois-invariance of the Weil pairing. Thus, to describe all associated characters of A, it suffices to consider one character in each pair $\{\psi_0, \mathrm{cyc}_\ell^d \otimes \psi_0^{-1}\}$. Now we state the main theorem of our paper. (Recall that a representation of an algebra is said to be *primitive* if it is not induced from a representation of some subalgebra.)

Theorem 3 (Theorem 5.16). *Let K be a number field, and g and d be positive integers. Then, there exists a finite set $S_{K,g}$ of prime numbers depending only on K and g, and*

https://doi.org/10.1017/S1474748013000182 Published online by Cambridge University Press

a constant $0 < c(g) < 12^{4g^2}$ *depending only on* g *such that, for a prime* $\ell \notin S_{K,g}$, *and a* g*-dimensional abelian variety* A *with a mod-*ℓ *associated character* ψ_0 *of degree* d, *we have*

$$\psi^{e \cdot w} \equiv \psi_{F,\Phi}^{w} (\mathrm{mod}\ \ell),$$

where ψ *is either* ψ_0 *or* $\mathrm{cyc}_\ell^d \otimes \psi_0^{-1}$, *and* $w = \frac{\mathrm{lcm}(N, c(g))}{\gcd(e, c(g))}$. *Here,* F *is either* $\mathbb{Q}$ *or a CM field, and* $\Phi : F \to \mathrm{End}(K^m)$ *is a primitive balanced representation such that* $K \supset K_{F,\Phi}$. *The quantities* a, e, *and* N *are integers with* e *and* N *positive, which satisfy* $m = \frac{1}{2} \cdot a \cdot e \cdot [F : \mathbb{Q}]$. *Moreover,* $0 \leqslant a \leqslant d$, *and both* $\varphi(N)$ *and* $e \cdot [F : \mathbb{Q}]$ *are at most* $\binom{2g}{d}$.

Remark 1.2. The proof of Theorem 3 implies that the set $S_{K,g}$ is effectively computable; in Theorem 7.9, we give an explicit bound on the value of $\prod_{\ell \in S_{K,g}} \ell$.

We think of Φ as giving the isomorphism class of the K–F bimodule $\mathrm{Lie}(B)$, for any abelian variety B with CM type (F, Φ). The above bounds imply that $m = \dim B \leqslant \frac{d}{2} \cdot \binom{2g}{d}$. In particular, if $d = 1$, then $m = \dim B \leqslant g = \dim A$.

In many important special cases — including abelian surfaces and threefolds, as well as when K has a real embedding — the above theorem is equivalent to simpler statements whose analogy with Theorem 6.4 is more transparent; this will be discussed in § 5.4.

Applying Theorem 3 to the Albanese variety of any smooth proper scheme X of finite type over K, we obtain (for ℓ sufficiently large) nontrivial restrictions for the G_K-action on the étale cohomology $H^1(X, \mathbb{F}_\ell) \simeq H^1(\mathrm{Alb}(X), \mathbb{F}_\ell)$. We believe that it may be possible to study associated characters of higher étale cohomology groups $H^r(X, \mathbb{F}_\ell)$ using our methods. Indeed, in several cases — e.g. when X has everywhere good reduction — our techniques give analogous results for $H^r(X, \mathbb{F}_\ell)$. However, in the general case there are some difficulties that occur due to the lack of a good theory of semistable reduction (see Remark 5.1).

Our proof of Theorem 3 is similar in spirit to the method used by Serre in [17] to classify elliptic curves with non-surjective mod-ℓ Galois action. Higher-dimensional abelian varieties introduce additional issues: while there are only finitely many elliptic curves (over $\overline{\mathbb{Q}}$) with a given endomorphism ring larger than $\mathbb{Z}$, there are positive-dimensional moduli of such abelian varieties. This forces the theory of associated characters to become more complicated, once these Shimura varieties enter into the picture. Moreover, obtaining uniform bounds requires a more delicate analysis than Serre's [17], in particular because we cannot assume that A is everywhere semistable by extending the ground field (since the field extension we would have to make depends on A).

Notational conventions. Throughout the paper, we normalize the Artin map to carry uniformizers to *arithmetic* Frobenius elements, i.e. the map $\alpha \mapsto \alpha^q$. We write n_K, r_K, R_K, h_K, and Δ_K for the degree, rank of the unit group, regulator, class number, and discriminant of K respectively.

https://doi.org/10.1017/S1474748013000182 Published online by Cambridge University Press

2. Algebraic characters

A multiplicative map of number fields of algebraic origin — for example the norm map $\mathrm{Nm} : K^\times \to \mathbb{Q}^\times$ — can be interpreted as the induced map on $\mathbb{Q}$-points of a map of commutative algebraic groups over $\mathbb{Q}$. Such maps — which we call *algebraic characters* — will appear as determinants of representations induced by CM (§ 3.1) and as Galois characters (Definition 2.25). The main technical result of this section, Lemma 2.26, gives a way of defining global *Galois* characters from algebraic characters between global fields, an idea originally due to Serre (in [16]) but approached here from the slightly different vantage point of CM fields and groups of Weil numbers.

2.1. Definitions and first properties of algebraic characters

We will be interested in algebraic characters between pairs of number fields and pairs of p-adic fields, but we first give some general definitions over any infinite base field Q. Let K and L be algebraic extensions of Q; assume that K/Q is finite and L is equipped with a fixed embedding $L \hookrightarrow \overline{Q}$. Write T_K and T_L for the algebraic tori $\mathrm{Res}^K_Q \mathbb{G}_{m,K}$ and $\mathrm{Res}^L_Q \mathbb{G}_{m,L}$, viewed as algebraic groups over Q.

Definition 2.1. An *algebraic character* is a multiplicative map $\theta : K^\times \to L^\times$ induced given by the map on Q-points induced by a morphism of algebraic groups $T_K \to T_L$.

Definition 2.2. We write Γ_K for the set of embeddings $K \hookrightarrow \overline{Q}$.

Proposition 2.3. *The (discrete) abelian group of multiplicative maps* $\mathrm{Hom}(T_K, T_L)$ *is the group of invariants* $\mathbb{Z}[\Gamma_K]^{G_L}$*, with induced map on* Q*-points*

$$\sum_{\sigma \in \Gamma_K} a_\sigma \sigma : x \mapsto \prod (x^\sigma)^{a_\sigma} \quad \text{for } x \in T_K(Q) = K^\times.$$

Proof. See [16], § 1.1 of chapter 2. □

Corollary 2.4. *If* L *contains the Galois closure* $K^{\mathrm{gal}} \subset \overline{Q}$ *of* K*, then*

$$\mathrm{Hom}(T_K, T_L) = \mathbb{Z}[\Gamma_K].$$

Remark 2.5. One may simply take Proposition 2.3 as the definition of algebraic characters.

Definition 2.6. For $S = \sum S(\sigma) \cdot \sigma \in \mathbb{Z}[\Gamma_K]^{G_L}$, we define the algebraic character θ^S via

$$\theta^S(x) = \prod \sigma(x)^{S(\sigma)}.$$

Definition 2.7. We say that an algebraic character $\theta : T_K \to T_L$ is *positive* if it extends from T_K to $\mathrm{Res}^K_Q \mathbb{A}^1_K$, or equivalently if $\theta = \theta^S$ for $S = \sum S(\sigma) \cdot \sigma$ with all $S(\sigma)$ nonnegative (so a positive character could have some $S(\sigma)$ equal to zero). Similarly, we say that θ is *negative* if $\theta \circ (x \mapsto x^{-1})$ is positive.

https://doi.org/10.1017/S1474748013000182 Published online by Cambridge University Press

Definition 2.8. We define the *degree* of an algebraic character θ^S to be $\max_{\sigma\in\Gamma_K}|S(\sigma)|$.

Now we give the dictionary between characters and representations. Let V be a $K\otimes_Q L$ bimodule which is finite-dimensional as an L-module. Viewing V as an L-vector space with an action of the (algebraic) group $K^\times$, we define $\det_L V : K^\times \to L^\times$ via the L-determinant of the K-action, i.e.

$$a \mapsto \det_L\big((x \mapsto a\cdot x) : V \to V\big).$$

Proposition 2.9. *For a positive algebraic character $\theta : K^\times \to L^\times$, there is a unique (up to isomorphism) $K\otimes_Q L$-bimodule V, finite-dimensional as an L-module, with* $\det_L V = \theta$.

Proof. Suppose at first that $L = \overline{Q}$. Let the a_σ be as in Proposition 2.3, and write $\overline{Q}[\sigma]$ for the one-dimensional $\overline{Q}$-vector space with K-action given by σ composed with the $\overline{Q}$-action. Then in this case, the desired bimodule $V = \bigoplus_{\sigma\in\Gamma_K}\overline{Q}[\sigma]^{\oplus a_\sigma}$.

For the general case, we invoke the primitive element theorem to write $K = Q[\alpha]$; note that such a bimodule V is the same as an L-vector space equipped with the endomorphism $A(x) = \alpha\cdot x$. By the above case, we can choose A uniquely up to conjugacy after we base-change to $\overline{Q}$; moreover, by the explicit description $V = \bigoplus_{\sigma\in\Gamma_K}\overline{Q}[\sigma]^{\oplus a_\sigma}$, this conjugacy class is G_L-invariant. The Jordan normal form of this conjugacy class is thus unique over $\overline{Q}$ and G_L-invariant; hence it uniquely defines a conjugacy class in $\mathrm{GL}_n(L)$ (where $n = \sum_{\sigma\in\Gamma_K} a_\sigma$). □

Now suppose that $\mathcal{O}\subset Q$ is an integrally closed subring. Since embeddings of fields preserve rings of integers, Proposition 2.3 implies that any algebraic character $\theta : K^\times \to L^\times$ sends $\mathcal{O}_K^\times \subset K^\times$ to $\mathcal{O}_L^\times \subset L^\times$.

Definition 2.10. For an ideal $I\subset\mathcal{O}_L$ and algebraic character $\theta : K^\times \to L^\times$, we define

$$\theta \bmod I : \mathcal{O}_K^\times \to (\mathcal{O}_L/I)^\times$$

to be the composition of $\mathcal{O}_L^\times \to (\mathcal{O}_L/I)^\times$ with θ. We call a character of the above form a *reduction of an algebraic character*.

We will be particularly interested in the case where $Q = \mathbb{Q}_p$ and $I = m_L$ is the maximal ideal of $\mathcal{O}_L$, giving a map $\theta \bmod m_L : \mathcal{O}_K^\times \to k_L^\times$.

2.2. ℓ-adic characters induced from global characters

Let K be a number field, $L = \overline{\mathbb{Q}}$, and ℓ be a prime; fix an embedding $\iota : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$.

Proposition 2.11. *There is a (unique) bijective correspondence*

$$(\theta \mapsto \theta_\ell) : \mathrm{Hom}\left(T_K, T_{\overline{\mathbb{Q}}}\right) \xrightarrow{\sim} \mathrm{Hom}\left(\prod_{v|\ell} T_{K_v}, T_{\overline{\mathbb{Q}}_\ell}\right),$$

https://doi.org/10.1017/S1474748013000182 Published online by Cambridge University Press

such that the maps on points $K^\times \to \overline{\mathbb{Q}}^\times$ *and* $\prod K_v^\times \to \overline{\mathbb{Q}}_\ell^\times$ *fit into the commutative diagram*

$$\begin{array}{ccc} K^\times & \xrightarrow{\theta} & \overline{\mathbb{Q}} \\ \downarrow & & \downarrow \iota \\ \prod_{v|\ell} K_v & \xrightarrow[\theta_\ell]{} & \overline{\mathbb{Q}}_\ell \end{array}$$

Definition 2.12. We will call this bijective correspondence *localization* of characters.

Proof. Note that if θ_ℓ exists, it is unique, since $K^\times \subset \prod_{v|\ell} K_v$ is dense. If $\theta = \sigma$ is a single embedding, then by the decomposition theorem for ideals under of finite extensions, the composition $\iota \circ \sigma$ can be uniquely written as $K \subset K_v \xrightarrow{\sigma_\ell} \overline{\mathbb{Q}}_\ell$, where $\sigma_\ell \in \Gamma_{K_v}$. Having constructed σ_ℓ for $\sigma \in \Gamma_K$ fitting into the above diagram, we define θ_ℓ for arbitrary θ multiplicatively. This is an isomorphism $\mathrm{Hom}(T_K, T_{\overline{\mathbb{Q}}}) \xrightarrow{\sim} \mathrm{Hom}\big(\prod_{v|p} T_{K_v}, T_{\overline{\mathbb{Q}}_\ell}\big)$ as it induces a bijection between generators of two free groups. □

2.3. Galois characters induced from algebraic characters

Localizing an algebraic character $\theta : K^\times \to L^\times$ of global fields, one can define a number of characters on the group of idèles (e.g., by considering the induced map on adelic points $T_K(\mathbb{A}) \to T_L(\mathbb{A})$), which will in some cases descend to Galois characters. Here we give such a construction in a rather specific case, which will be of interest in the rest of the paper.

Definition 2.13. We say $\theta : K^\times \to L^\times$ is *balanced* if $\theta \cdot (\sigma \circ \theta)$ is a power of $\mathrm{Nm}_{\mathbb{Q}}^K$ for *any* complex conjugation $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$. Otherwise, we say θ is *unbalanced*. Similarly, a K-L bimodule V is balanced (resp. unbalanced) if $\det_L V$ is balanced (resp. unbalanced).

Remark 2.14. If $\theta = \theta^{\sum a_\tau \tau}$ and $\theta \cdot (\sigma \circ \theta) = (\mathrm{Nm}_{\mathbb{Q}}^K)^{m_\sigma}$, then $m_\sigma = a_\tau + a_{\sigma(\tau)}$ for all τ. Thus, $m_\sigma = \frac{2}{|\Gamma_K|} \sum a_\tau$; in particular for θ balanced, m_σ is independent of σ.

The next two lemmas, to play a central role in the following sections, show that if θ_ℓ extends to a *global* Galois character with certain ramification conditions then θ is balanced.

Lemma 2.15. *The character* θ^S *is balanced if and only if* $\theta^S(u)$ *is a root of unity for any unit* $u \in \mathcal{O}_K^\times$.

Proof. Order the σ_i with $\sigma_1, \sigma_2, \ldots, \sigma_{r_1}$ the real embeddings, and σ_{r_1+i} the complex conjugate of $\sigma_{r_1+r_2+i}$. Let $\mu : \mathcal{O}_K^\times \to \mathbb{R}^{r_K+1}$ be the multiplicative Minkowski embedding:

$$\mu : x \mapsto \big(\log|\sigma_1(x)|, \log|\sigma_2(x)|, \ldots, \log|\sigma_{r_1}(x)|, 2\log|\sigma_{r_1+1}(x)|, \ldots, 2\log|\sigma_{r_1+r_2}(x)|\big).$$

Dirichlet's Unit Theorem states that the kernel of μ is roots of unity and the image of μ is a lattice $\Lambda \subset \mathbb{R}^{r_K+1}{}_0$, the subspace of vectors in $\mathbb{R}^{r_K+1}$ whose sum of coordinates

https://doi.org/10.1017/S1474748013000182 Published online by Cambridge University Press

is zero. For any $S \in \mathbb{Z}[\Gamma_K]$,

$$\left(x \mapsto \log|\theta^S(x)|\right) = f^S \circ \mu$$

factors as the composition of μ with the linear function $f^S : \mathbb{R}^{r_K+1} \to \mathbb{R}$ given by

$$f^S(x_1, \ldots, x_{r_1+r_2}) = \sum_{i=1}^{r_1} S(\sigma_i) \cdot x_i + \sum_{i=r_1+1}^{r_1+r_2} \frac{S(\sigma_i) + S(\sigma_{r_2+i})}{2} \cdot x_i.$$

Since $\theta^S(u)$ is a root of unity for any unit $u \in \mathcal{O}_K^\times$, it follows that f^S vanishes on units; as f^S is linear, f^S vanishes on the hyperplane spanned by the units. Hence it must be a multiple of the defining equation of the hyperplane, $\sum_{i=1}^{r_1+r_2} x_i$.

The converse follows from the fact that if $|\theta(u)| = 1$ under any complex embedding, then $\theta(u)$ is a root of unity. □

Lemma 2.16. *If the localization θ_ℓ^S coincides on an open subgroup $U \subset \prod_{v|\ell} \mathcal{O}_{K_v}^\times$ with the composition*

$$\prod_{v|\ell} \mathcal{O}_{K_v}^\times \longrightarrow \mathbb{I}_K \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K) \xrightarrow{\psi} \bar{\mathbb{Q}}_\ell^\times$$

for a Galois character (not to be confused with the algebraic characters that we have been discussing) $\psi : \mathrm{Gal}(K^{ab}/K) \to \overline{\mathbb{Q}}_\ell^\times$ which is ramified at only finitely many primes and has finite ramification index at primes not lying over ℓ, then θ^S is balanced.

Proof. Let $(\mathcal{O}_K^\times)_\ell$ be the image of the unit group under the embedding $\mathcal{O}_K^\times \hookrightarrow \prod_{v|\ell} \mathcal{O}_{K_v}^\times$, and let $U_\ell \subset \mathbb{I}_K$ be the subgroup $(\mathcal{O}_K^\times)_\ell \times \prod_{v\nmid\ell} \mathcal{O}_{K_v}^\times$. Then the image of U_ℓ in $\mathbb{I}_K/K^\times$ coincides with the image of $\prod_{v\nmid\ell} \mathcal{O}_{K_v}^\times$ (since any element of $u_\ell \in (\mathcal{O}_K^\times)_\ell$ coming from an element $u \in \mathcal{O}_K^\times$ is equivalent modulo $\mathcal{O}_K^\times \subset K^\times$ to $u^{-1}u_\ell \in \prod_{v\nmid\ell} \mathcal{O}_{K_v}^\times$). But $\prod_{v\nmid\ell} \mathcal{O}_{K_v}^\times$ has (by the finite ramification outside of ℓ assumption) finite image under ψ. On the other hand, $\psi(U_\ell)$ contains a subgroup of finite index of the image $\theta^S(\mathcal{O}_K^\times)$. Hence, $\theta^S(\mathcal{O}_K^\times)$ is finite, so θ^S is balanced by Lemma 2.15. □

Next we prove a converse — that if the character *is* balanced then we can in fact extend it to a global Galois character with appropriately mild ramification behavior.

Definition 2.17. The *group of Weil elements* $W_L \subset L^\times$ is the group of elements $w \in L^\times$ satisfying $w \cdot \sigma(w) \in \mathbb{Q}^\times$ for *any* complex conjugation $\sigma \in \mathrm{Gal}(K^{\mathrm{gal}}/\mathbb{Q})$.

Example 2.18. For L a quadratic field, every element of $L^\times$ is a Weil element.

Remark 2.19. If $w \cdot \sigma(w) = N_\sigma \in \mathbb{Q}^\times$, then

$$\left(\mathrm{Nm}_{\mathbb{Q}}^{K^{\mathrm{gal}}} w\right)^2 = \mathrm{Nm}_{\mathbb{Q}}^{K^{\mathrm{gal}}} w \cdot \mathrm{Nm}_{\mathbb{Q}}^{K^{\mathrm{gal}}} \sigma(w) = \mathrm{Nm}_{\mathbb{Q}}^{K^{\mathrm{gal}}} (w \cdot \sigma(w)) = \mathrm{Nm}_{\mathbb{Q}}^{K^{\mathrm{gal}}} N_\sigma = N_\sigma^{[K^{\mathrm{gal}}:\mathbb{Q}]}.$$

In particular, for w a Weil element, N_σ is independent of σ (using that $N_\sigma \in \mathbb{Q}_{>0}$).

Definition 2.20. We say that F is a *CM field* if *any* complex conjugation restricts to the same nontrivial element of $\mathrm{Gal}(F^{\mathrm{gal}}/\mathbb{Q})$. Equivalently, F is a CM field if F is a quadratic totally imaginary extension of a totally real subfield.

https://doi.org/10.1017/S1474748013000182 Published online by Cambridge University Press

A balanced character $K^\times \to L^\times$ factors through an embedding $F \subset L$, where F is either a CM field or $F = \mathbb{Q}$. Indeed, for any complex conjugation σ, we have $\theta \cdot (\sigma \circ \theta) = (\mathrm{Nm}_{\mathbb{Q}}^K)^m$ for m independent of σ (see Remark 2.14); hence, $\sigma \circ \theta$ is independent of σ. In particular, every complex conjugation has the same restriction to the field generated by the image of θ. When this restriction of complex conjugation is nontrivial, then F is a CM field. When it is trivial, then $\theta^2 = \theta \cdot (\sigma \circ \theta) = (\mathrm{Nm}_{\mathbb{Q}}^K)^m$, which is only possible if m is even and $\theta = (\mathrm{Nm}_{\mathbb{Q}}^K)^{m/2}$ (since θ is an algebraic character); but in this case θ factors through $\mathbb{Q} \subset L$.

We will from now on take F to be a CM field (or $\mathbb{Q}$) and $\theta : K^\times \to F^\times$ to be an algebraic character.

Definition 2.21. The *Weil class group* $\mathrm{Cl}^W(F) = I_F/W_F$ is the group of fractional ideals modulo the group of Weil elements of F. (Note that it is in general an infinite group.)

As θ is a map of algebraic groups, it induces a map from the idèles of K to the idèles of L. Since θ is balanced, the image (viewed as a map $K^\times \to F^\times$) of θ lies in the group of Weil elements of F. (Indeed, for any $x \in K^\times$, we have $\theta(x) \cdot \sigma(\theta(x)) = (\mathrm{Nm}_{\mathbb{Q}}^K x)^m \in \mathbb{Q}^\times$.)

Definition 2.22. We define $C\theta : \mathrm{Cl}(K) \to \mathrm{Cl}^W(F)$ to be the map induced by θ.

Definition 2.23. Write $\mathbb{I}_K^\theta$ for the group of idèles of K whose ideal class is in the kernel of $C\theta$, and K_θ for the abelian extension of K corresponding to the subgroup $\mathbb{I}_K^\theta \subset \mathbb{I}_K$.

Definition 2.24. We write N_0 for the number of roots of unity in F, and $\mu_F = \mu_{N_0}$ for the group of roots of unity in F.

A Weil element which is a unit has norm 1 under any complex embedding, and hence is a root of unity. Therefore, θ induces a map $I\theta$ from $\mathbb{I}_K^\theta$ to W_F/μ_F. Now, we fix an embedding $F \hookrightarrow \overline{\mathbb{Q}}_\ell$.

Definition 2.25. For a character $\theta : K^\times \to F^\times \subset \overline{\mathbb{Q}}^\times$, we define $\psi_\theta : \mathbb{I}_K^\theta \to \overline{\mathbb{Q}}_\ell/\mu_F$ via $\psi_\theta := I\theta \cdot \theta_\ell^{-1}$. For a K–F bimodule Φ, we define $\psi_{F,\Phi} := \psi_\theta$ where $\theta = \det_K \Phi : K^\times \to \overline{\mathbb{Q}}^\times$.

Lemma 2.26. *The character ψ_θ is trivial on principal idèles and has image in $\mathcal{O}_{\overline{\mathbb{Q}}_\ell}^\times/\mu_F$.*

Proof. To show $\psi_\theta(x) = 1$ for $x \in K^\times$, note that we have an equality of principal ideals $(I\theta(x)) = (\theta(x))$, both of which are generated by a Weil number. For $\psi_\theta(\mathbb{I}_K^\theta) \subset \mathcal{O}_{\overline{\mathbb{Q}}_\ell}^\times/\mu_F$, note that $I\theta(\pi_v)$ and $\theta_\ell(\pi_v)$ have the same norm for $\pi_v \in K_v$ a uniformizer. □

Extending to infinite places by the trivial map, this lets us define a Galois character (on $\mathrm{Gal}(\overline{K}/K_\theta)$) given any CM field F and balanced character $\theta : K^\times \to F^\times$.

Remark 2.27. This character is uniquely determined by taking any uniformizer π_w, for $w \nmid \ell$ and $[w] \in \ker C\theta$, to a Weil number generating the ideal $I\theta(w)$ (up to roots of unity).

https://doi.org/10.1017/S1474748013000182 Published online by Cambridge University Press

3. Abelian varieties with complex multiplication

3.1. Galois characters associated with CM abelian varieties

Let B be an abelian variety over a field K, with an injection $\iota : E \hookrightarrow \mathrm{End}_K(B) \otimes \mathbb{Q}$. The p-adic Tate module is a finite-dimensional $(E \otimes \mathbb{Q}_p)$-module, so we can take the determinant over $(E \otimes \mathbb{Q}_p)$ of the G_K-action. (Writing $E \otimes \mathbb{Q}_p = \prod_{v|p} E_v$, this is the product of the E_v-linear determinants.) This gives a map $\mathrm{Gal}(\overline{K}/K) \to (E \otimes \mathbb{Q}_p)^\times$. This determinant encodes the associated characters of the eigenspaces for the E-action, via:

Definition 3.1. Define the character $\psi_{B,\sigma} : \mathrm{Gal}(\overline{K}/K) \to \overline{\mathbb{Q}}_p^\times$ by

$$\psi_{B,\sigma} := (\sigma \otimes \mathrm{id}) \circ \det_{E \otimes \overline{\mathbb{Q}}_p} B[p^\infty] \otimes \overline{\mathbb{Q}}_p.$$

We now show that the study of ℓ-adic associated characters of abelian varieties B over a *number field* K reduces to studying the characters $\psi_{B,\sigma}$. Let V and W be subspaces of $B[\ell^\infty] \otimes \overline{\mathbb{Q}}_\ell$; write V^0 and W^0 for $V \cap B[\ell^\infty] \otimes \overline{\mathbb{Z}}_\ell$ and $W \cap B[\ell^\infty] \otimes \overline{\mathbb{Z}}_\ell$ respectively. We define the distance function $d(V, W) = \ell^{-n(V,W)}$, where

$$n(V, W) = \max \left\{ m : V^0 + \ell^m B[\ell^\infty] \otimes \overline{\mathbb{Z}}_\ell = W^0 + \ell^m B[\ell^\infty] \otimes \overline{\mathbb{Z}}_\ell \right\}.$$

Lemma 3.2. *Let B be an abelian variety over a number field K, and V be an irreducible G_K-equivariant subspace (or, in this case equivalently, subquotient) of $B[\ell^\infty] \otimes \overline{\mathbb{Q}}_\ell$. Then for any $\epsilon > 0$, there is an $\alpha \in \mathrm{End}(B)$ and an eigenspace W for the action of α on $B[\ell^\infty] \otimes \overline{\mathbb{Q}}_\ell$, such that $d(V, W) \leqslant \epsilon$.*

Proof. Let $V = \sigma_0 V, \sigma_1 V, \ldots, \sigma_m V$ be the conjugates of V under the $\mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$-action. By a theorem of Faltings (Theorem 3 of [4]), the G_K-representation $B[\ell^\infty] \otimes \overline{\mathbb{Q}}_\ell$ is semisimple. Thus, $B[\ell^\infty] \otimes \overline{\mathbb{Q}}_\ell = \sigma_0 V \oplus \cdots \oplus \sigma_m V \oplus V'$ for some subrepresentation V'. Let H be the subgroup of $G_{\mathbb{Q}_\ell}$ of elements which take V to itself, and $\mathcal{K} \subset \overline{\mathbb{Q}}_\ell$ be the fixed subfield of H. As $\mathcal{K}/\mathbb{Q}_\ell$ is finite, there is a primitive element $\alpha \in \mathcal{K}$ over $\mathbb{Q}_\ell$. The endomorphism

$$\alpha_0 = \sigma_0(\alpha) \cdot \mathrm{id}_{\sigma_0 V} \oplus \cdots \oplus \sigma_m(\alpha) \cdot \mathrm{id}_{\sigma_m V} \oplus 0_{V'} : B[\ell^\infty] \otimes \overline{\mathbb{Q}}_\ell \to B[\ell^\infty] \otimes \overline{\mathbb{Q}}_\ell,$$

is $\mathrm{Gal}(\mathcal{K}/\mathbb{Q}_\ell)$-invariant, and so restricts to an endomorphism $\alpha_0 : B[\ell^\infty] \otimes \mathbb{Q}_\ell \to B[\ell^\infty] \otimes \mathbb{Q}_\ell$ that is G_K-invariant. Another theorem of Faltings (Theorem 4 of [4]) gives that

$$\mathrm{End}(B) \otimes \mathbb{Q}_\ell \cong \mathrm{End}_{G_K}(B[\ell^\infty] \otimes \mathbb{Q}_\ell).$$

In particular, there is $\alpha \in \mathrm{End}B \otimes \mathbb{Q}$ approximating α_0 to arbitrary ℓ-adic precision, so V is arbitrarily close to a single eigenspace of the action of α on $B[\ell^\infty] \otimes \overline{\mathbb{Q}}_\ell$. □

Now suppose B is simple (we can study the general case by decomposing B up to isogeny into a product of simple abelian varieties). We take $E = \mathbb{Q}(\alpha)$, so $\det_W = \psi_{B,\sigma}$. In the next two sections, we will see that up to multiplication by roots of unity in E, the character $\psi_{B,\sigma}$ is determined by the field E plus some *finite* combinatorial data. In particular (up to multiplication by bounded roots of unity), there are only finitely many

https://doi.org/10.1017/S1474748013000182 Published online by Cambridge University Press

characters giving the Galois action $\det_W$ in the above lemma; it follows by taking a sufficiently good approximation W that one of these finitely many characters gives the action on $\det_V$.

3.2. Local case

Suppose that $K = \mathcal{K}$ is a p-adic field. By local class field theory, we have a natural map $\mathrm{rec} : \mathcal{K}^\times \to \mathrm{Gal}(\mathcal{K}^{\mathrm{ab}}/\mathcal{K})$. The following theorem, due to Conrad, describes the $(E \otimes \mathbb{Q}_p)$-determinant of the Galois action in terms of the action of E on the Lie algebra $\mathrm{Lie}(B)$.

Theorem (Conrad, Appendix). *Let B be an abelian variety defined over a local field $\mathcal{K}$ of residue characteristic p, which admits an injection $\iota : E \hookrightarrow \mathrm{End}_{\mathcal{K}}(B) \otimes \mathbb{Q}$. Then, there is an open subgroup $U \subset \mathcal{O}_{\mathcal{K}}^\times$ on which the following diagram commutes:*

$$\begin{array}{ccc} U \subset \mathcal{K}^\times & \xrightarrow{\mathrm{rec}} & \mathrm{Gal}(\mathcal{K}^{\mathrm{ab}}/\mathcal{K}) \\ {\scriptstyle u \mapsto (x \mapsto u^{-1}\cdot x)}\downarrow & & \downarrow{\scriptstyle \det_{E\otimes\mathbb{Q}_p} \circ \rho_{B,p^\infty}} \\ \mathrm{Aut}_{E\otimes\mathbb{Q}_p}(\mathrm{Lie}(B)) & \xrightarrow[\det_{E\otimes\mathbb{Q}_p}]{} & (E \otimes \mathbb{Q}_p)^\times \end{array}$$

Remark 3.3. For B semistable, we can take $U = \mathcal{O}_{\mathcal{K}}^\times$ (see Appendix). By Lemma 4.6, this implies that we can take U to have index dividing the constant $c(g)$ defined in § 4.2.

3.3. Global case

Let B be a simple abelian variety over a number field K. Recall from § 3.1 that any ℓ-adic associated character of B is a product of characters of the form $\psi_{B,\sigma}$ for embeddings $\sigma : E \hookrightarrow \mathrm{End}_{\mathcal{K}}(B) \otimes \mathbb{Q}$, which by Conrad's Theorem above equals $(\det_E \mathrm{Lie}(B))_\ell$ when restricted to an open subgroup of $\prod_{v|\ell} \mathcal{O}_v^\times \subset \mathrm{Gal}(\overline{K}/K)^{ab}$. Define $F \subset E$ to be the composite of all CM subfields of E (so F is either a CM field or $F = \mathbb{Q}$).

Lemma 3.4. *The E-representation $\mathrm{Lie}(B)$ is induced from some F-representation Φ, i.e. $\mathrm{Lie}(B) \simeq \Phi \otimes_F E$. Moreover, $\det_E \mathrm{Lie}(B) = \det_F \Phi$.*

Proof. By Lemma 2.16, $\det_E \mathrm{Lie}(B)$ is balanced, and hence has image contained in a CM field (or $\mathbb{Q}$). Equivalently by Proposition 2.9, the E-module $\mathrm{Lie}(B)$ is induced from an F-module, i.e. $\mathrm{Lie}(B) \simeq \Phi \otimes_F E$ for some F–K bimodule Φ. It follows that $\det_E \mathrm{Lie}(B) = \det_F \Phi$. □

Definition 3.5. Let F be a CM field (or $F = \mathbb{Q}$), and Φ be an F-representation. We say that a polarized abelian variety B is an (F, Φ)-*abelian variety* if it has endomorphisms by a number field $E \supset F$, making $\mathrm{Lie}(B) \simeq \Phi \otimes_F E$ as an E–K bimodule. We call (F, Φ) the *CM type* of B.

The following theorem therefore classifies associated characters of simple abelian varieties.

https://doi.org/10.1017/S1474748013000182 Published online by Cambridge University Press

Theorem 3.6. *Let B be an (F, Φ) abelian variety and $\theta = \det_F \Phi$. Then in the notation of Definitions 2.23 and 2.25, we have $K = K_\theta$ and $\psi_{B,\sigma} \equiv \psi_\theta$ mod μ_F.*

Before proving the theorem, we give a convenient alternative formulation.

Definition 3.7. We write $K_{F,\Phi} = K_{\theta_0}$ and $\psi_{F,\Phi} = \psi_{\theta_0}$, where $F' \subset K$ is the minimal field such that $\theta : K^\times \to F^\times$ factors as the composition of $\mathrm{Nm}_{F'}^K$ with $\theta_0 : F'^\times \to F^\times$.

Remark 3.8. We have $K_\theta = K \cdot K_{F,\Phi}$, and $\psi_\theta = \psi_{\theta_0} \circ \mathrm{Nm}_{F'}^K$. Both the field $K_{F,\Phi}$ and the character $\psi_{F,\Phi}$ are *geometric* invariants of B; i.e. they are unchanged under base extensions.

Unwinding the definition, the first part of Theorem 3.6 is equivalent to $K \supset K_{F,\Phi}$.

Proof of Theorem 3.6. First we show that $\psi_{B,\sigma} \equiv \psi_\theta \bmod \mu_F$ on $\mathrm{Gal}(\overline{K}/K_\theta)$. Let

$$\epsilon := \psi_{B,\sigma}/\psi_\theta : \mathrm{Gal}(\overline{K}/K_\theta) \to \overline{\mathbb{Q}}_\ell/\mu_F.$$

The two characters $\psi_{B,\sigma}$ and ψ_θ coincide on an open subgroup of any inertia subgroup $\mathcal{O}_{K_v}^\times \subset \mathbb{I}_K$ for $v|\ell$ and have finite ramification degree outside of ℓ, so ϵ is finite-order.

Claim. For any prime v of good reduction for B, there is an embedding $E \subset \overline{\mathbb{Q}}_\ell$ such that $\psi_{B,\sigma}(\pi_v) \in E \subset \overline{\mathbb{Q}}_\ell$. Furthermore, if $F \neq \mathbb{Q}$, then $\psi_{B,\sigma}(\pi_v) \in F^\times$.

Proof. We have $\psi_{B,\sigma}(\pi_v) \in E \subset \overline{\mathbb{Q}}_\ell$ by paragraph 11.10 of [19]. If $F \neq \mathbb{Q}$, then F contains all totally real and CM subfields of E; as $\psi_{B,\sigma}$ is a Weil number, $\psi_{B,\sigma} \in F$. □

By definition, ψ_θ takes values in $F^\times/\mu_F$, so ϵ takes Frobenius elements to elements of $\mu_E/\mu_F = \{1\}$. Hence, by the Chebotarev Density Theorem, ϵ is trivial.

It remains to prove that $K = K_\theta$. Although this follows from Theorem 3.10 of the next section, we give an alternative proof here. For $F = \mathbb{Q}$, this is immediate; thus, we assume $F \neq \mathbb{Q}$. Now suppose v is a prime ideal of K of good reduction for B. Since $\pi_v^{h_K} \in \mathrm{Gal}(\overline{K}/K_\theta)$, we have $\psi_{B,\sigma}(\pi_v^{h_K}) \equiv \psi_\theta(\pi_v^{h_K}) \bmod \mu_F$. By the above claim, $\psi_{B,\sigma}(\pi_v) \in F$, so $(\psi_{B,\sigma}(\pi_v))^{h_K} = (\psi_\theta(\pi_v))^{h_K}$ as ideals of F. As the group of ideals of F is torsion-free, $(\psi_{B,\sigma}(\pi_v)) = (\psi_\theta(\pi_v))$. Hence, $\theta(v)$ is generated by $\psi_{B,\sigma}(\pi_v)$, which is a Weil element of F. By the Chebotarev Density Theorem, $C\theta : \mathrm{Cl}(K) \to \mathrm{Cl}^W(F)$ is trivial, i.e. $K = K_\theta$. □

3.4. Shimura varieties and the field $K_{F,\Phi}$

We have seen in the previous section that if there is an (F, Φ)-abelian variety B defined (and with its CM defined) over a number field K, then K contains a certain field $K_{F,\Phi}$ associated with the CM type (F, Φ). One can ask whether the converse holds, namely:

Question 1. *Does there exist an abelian variety with CM by (F, Φ) over $K_{F,\Phi}$?*

As far as we know, this question is open, although we suspect that it is false in general. Here we give a statement (Theorem 3.10 below) which is the best we can do short of answering Question 1.

While no result from this section will be used in the rest of the paper, this section gives important context for the main theorem. In the case of elliptic curves, the results

https://doi.org/10.1017/S1474748013000182 Published online by Cambridge University Press

of this section reduce to the well-known fact that there is an elliptic curve with CM by an imaginary quadratic field F defined over its Hilbert class field H_F; in particular, the requirement in Corollary 2 that K does not contain any H_F is necessary. Here we establish an analogous (but slightly weaker) result in higher dimensions.

Suppose X is a reduced scheme of finite type over a field $K \subset \mathbb{C}$ and $B \to X$ is a (flat) family of polarized abelian varieties over X.

Definition 3.9. The family $B \to X$ is a *strong* (F, Φ)*-family of abelian varieties* if there is a map of rings $\iota : \mathcal{O}_F \hookrightarrow \mathrm{End}(B/X)$ making every $\mathbb{C}$-fiber of $B \to X$ an (F, Φ)-abelian variety with $E = F$ and $\theta \circ \iota(\overline{\alpha}) = \iota(\alpha)^* \circ \theta$, where $\theta : B \to B^\vee$ is the polarization.

We might hope to weaken Question 1 by replacing $\mathrm{Spec} K_{F,\Phi}$ with a geometrically irreducible K-scheme X of finite type. In other words at least morally, for any field K, there should be a strong (F, Φ)-family of abelian varieties $B \to X$ over a geometrically irreducible K-scheme of finite type if and only if $K \supset K_{F,\Phi}$. The main result of this section is that this holds in the category of (Deligne–Mumford) stacks; or in classical language:

Theorem 3.10. *Let (F, Φ) be a CM type, with Φ balanced. Then there exists a coarse moduli space of strong (F, Φ)-abelian varieties, which is defined over K provided that Φ is defined over K. Moreover, the separating field of this moduli space (i.e. the minimal field over which any irreducible component is geometrically irreducible) is $K_{F,\Phi}$.*

The rest of this section is devoted to a proof of this theorem.

Lemma 3.11. *There exists an (F, Φ)-abelian variety over $\mathbb{C}$ if and only if $\Phi \oplus \overline{\Phi} \simeq F^b \otimes_{\mathbb{Q}} K$ for some integer b (i.e. if and only if Φ is balanced).*

Proof. Suppose there was an (F, Φ)-abelian variety B over $\mathbb{C}$; write $B(\mathbb{C}) = \mathbb{C}^g/\Lambda$. Note that $\Lambda \otimes_{\mathbb{Z}} \mathbb{Q}$ is an F-vector space, and so isomorphic to F^b for some b. As representations of F:

$$\Phi \oplus \overline{\Phi} \simeq \mathrm{Lie}(B) \oplus \mathrm{Lie}(B^\vee) \simeq \Lambda \otimes_{\mathbb{Z}} \mathbb{C} \simeq (\Lambda \otimes_{\mathbb{Z}} \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{C} \simeq F^b \otimes_{\mathbb{Q}} \mathbb{C}.$$

Conversely, as $\Phi \oplus \overline{\Phi} \simeq F^b \otimes_{\mathbb{Q}} \mathbb{C}$ and all irreducible complex representations of F are one-dimensional,

$$\Phi = \bigoplus_{i=1}^{b} \Phi_i \quad \text{where } \Phi_i \oplus \overline{\Phi_i} \simeq F \otimes_{\mathbb{Q}} \mathbb{C}.$$

By the theory of complex multiplication [12], there exist complex abelian varieties B_i with CM by $\mathcal{O}_F$ of CM type Φ_i. Then $B = \prod_{i=1}^{b} B_i$ is an (F, Φ)-abelian variety. □

The (coarse) moduli space of strong (F, Φ)-abelian varieties has infinitely many connected components, which we can remedy by keeping track of both the skew form $\langle \cdot, \cdot \rangle$ on the adelic Tate module $H_1(B, \widehat{\mathbb{Z}}) = \prod_\ell B[\ell^\infty]$ induced by the polarization, and the action $\alpha : \mathcal{O}_F \to \mathrm{End}(H_1(B, \widehat{\mathbb{Z}}))$, which must satisfy

$$\langle \alpha(a) \cdot x, y \rangle = \langle x, \alpha(\overline{a}) \cdot y \rangle \quad \text{for all } a \in \mathcal{O}_F. \tag{3}$$

https://doi.org/10.1017/S1474748013000182 Published online by Cambridge University Press

As symplectic F-representations, $H_1(B, \widehat{\mathbb{Z}}) \simeq H_1(B, \mathbb{Z}) \otimes \widehat{\mathbb{Z}}$ and $\Phi \oplus \overline{\Phi} \simeq H_1(B, \mathbb{Z}) \otimes \mathbb{C}$, where $H_1(B, \mathbb{Z})$ is the singular homology of B with integral coefficients.

Definition 3.12. A *CM datum* is a quintuple $D = (F, \Phi, \langle \cdot, \cdot \rangle, \alpha, \Lambda)$ where (F, Φ) is a CM type with Φ of dimension g over $\mathbb{C}$, Λ is a $2g$-dimensional $\widehat{\mathbb{Z}}$-lattice, $\langle \cdot, \cdot \rangle$ is a skew-symmetric integral form on Λ, and $\alpha : \mathcal{O}_F \to \mathrm{End}(\Lambda)$ is an action of $\mathcal{O}_F$ on Λ, satisfying formula (3). We additionally require that Λ is compatible with Φ: i.e., for some (not necessarily unique) $\mathbb{Z}$-lattice Λ_0, we have $\Lambda_0 \otimes \widehat{\mathbb{Z}} \simeq \Lambda$ and $\Lambda_0 \otimes \mathbb{C} \simeq \Phi \oplus \overline{\Phi}$ as symplectic $\mathcal{O}_F$-modules.

A polarized abelian variety B is said to have CM datum D if there is an isomorphism $H_1(B, \widehat{\mathbb{Z}}) \cong \Lambda$ with $\mathcal{O}_F$-action and polarization form induced by α and $\langle \cdot, \cdot \rangle$ respectively. (More generally, for X a reduced scheme over K, a strong (F, Φ)-family $B \to X$ of abelian varieties has CM datum D if the $\mathcal{O}_F$-action induces CM datum D on each $\mathbb{C}$-fiber.)

Let (F, Φ) be a CM type defined over K. From now on suppose that the moduli space of strong (F, Φ)-abelian varieties is nonempty; equivalently (by Lemma 3.11), suppose that $\Phi \oplus \overline{\Phi} \simeq F^b \otimes_{\mathbb{Q}} K$ for some b. Note that this moduli space is the disjoint union over CM data D of the moduli space of strong (F, Φ)-abelian varieties with CM datum D. To prove Theorem 3.10 we identify this latter moduli space with a Shimura variety (defined below).

Definition 3.13. If G is an algebraic group over k, and K is an extension of k, we define

$$G_{/K} = G \times_{\mathrm{Spec} k} \mathrm{Spec} K.$$

Definition 3.14. We write $\mathbb{S} = \mathrm{Res}^{\mathbb{C}}_{\mathbb{R}} \mathbb{G}_{m,\mathbb{C}}$.

Definition 3.15. Let G be an algebraic group over the rationals, $h : \mathbb{S} \to G_{/\mathbb{R}}$ be a map of real algebraic groups, and $G_{\mathcal{O}} \subset G(\mathbb{A}^f)$ be a compact subgroup. Writing K_∞ for the stabilizer of h in $G(\mathbb{R})$, we define the *Shimura variety* to be the double coset space

$$\mathrm{Sh}_{G_{\mathcal{O}}}(G, h) := K_\infty \times G_{\mathcal{O}} \setminus G(\mathbb{A}) / G(\mathbb{Q}).$$

We now describe how a CM datum $D = (F, \Phi, \langle \cdot, \cdot \rangle, \alpha, \Lambda)$ gives rise to a Shimura variety. Let Λ_0 a $\mathbb{Z}$-lattice with $\Lambda_0 \otimes \widehat{\mathbb{Z}} \cong \Lambda$ and $\Lambda_0 \otimes \mathbb{C} \simeq \Phi \oplus \overline{\Phi}$ as symplectic $\mathcal{O}_F$-modules. While Λ_0 is noncanonical, $V = \Lambda_0 \otimes \mathbb{Q}$ (which we think of as a vector space over F) is uniquely determined by D by the Hasse–Minkowski principle for quadratic forms.

Definition 3.16. Define $\mathrm{GSp}(V)$ to be the group of F-linear maps $V \to V$ preserving $\langle \cdot, \cdot \rangle$ up to a (rational) scalar, thought of as an algebraic group over $\mathbb{Q}$.

Take $G = \mathrm{GSp}(V)$, and let $G_{\mathcal{O}} \simeq G(\mathcal{O}_{\mathbb{A}^f}) \subset G(\mathbb{A}^f)$ be the stabilizer of $\Lambda \otimes_{\mathbb{Z}} \mathcal{O}_{\mathbb{A}^f}$. Let $h : \mathbb{S} \to G_{\mathbb{R}}$ be the unique map of real algebraic groups inducing multiplication by z^{-1} on Φ and by $\bar{z}^{-1}$ on $\overline{\Phi}$ for an isomorphism $V \otimes_{\mathbb{Q}} \mathbb{C} \simeq \Phi \oplus \overline{\Phi}$ as F–$\mathbb{C}$ bimodules.

Theorem (Shimura; see Deligne [3], Paragraph 4.12). *The coarse moduli space of strong (F, Φ)-abelian varieties with CM datum D is the above Shimura variety.*

https://doi.org/10.1017/S1474748013000182 Published online by Cambridge University Press

We now recall some theorems of Shimura which describe when the irreducible components of $\mathrm{Sh}_{G_{\mathcal{O}}}(G,h)$ are geometrically irreducible. Note that $\mathrm{Hom}(\mathbb{S}_{/\mathbb{C}}, \mathbb{G}_{m,\mathbb{C}})$ has for a basis the characters z and $\bar{z}$ such that the compositions $\mathbb{C}^\times \simeq \mathbb{S}(\mathbb{R}) \hookrightarrow \mathbb{S}(\mathbb{C}) \to \mathbb{G}_{m,\mathbb{C}} \simeq \mathbb{C}^\times$ are the identity and complex conjugation respectively. Write $r : \mathbb{G}_{m,\mathbb{C}} \to \mathbb{S}_{/\mathbb{C}}$ for the unique map such that $z \circ r$ is the identity and $\bar{z} \circ r$ is trivial.

Theorem (Shimura; see Deligne [3], Paragraphs 3.6, 3.7, 3.9 and 3.14). *Suppose that the commutator subgroup $G' = [G,G]$ of G is simply connected. Then $\mathrm{Sh}_{G_{\mathcal{O}}}(G,h)$ is defined over K if and only if the conjugacy class of*

$$h \circ r : \mathbb{G}_{m,\mathbb{C}} \to \mathbb{S}_{\mathbb{C}} \to G_{\mathbb{C}}$$

is defined over K. Moreover, writing $T = G^{\mathrm{ab}} = G/G'$, and $\nu : G \to T$ for the projection map, the irreducible components of $\mathrm{Sh}_{G_{\mathcal{O}}}(G,h)$ are geometrically irreducible if and only if

$$\lambda((\mathrm{Res}^K_{\mathbb{Q}} \mathbb{G}_{m,K})(\mathbb{A})) \subset \nu(G_{\mathcal{O}}) \cdot T(\mathbb{Q}) \cdot \nu(K_\infty),$$

where $\lambda : \mathrm{Res}^K_{\mathbb{Q}} \mathbb{G}_{m,K} \to T$ is defined by

$$\lambda(a) = \mathrm{Nm}^K_{\mathbb{Q}} \circ \mathrm{Res}^K_{\mathbb{Q}}(\nu \circ h \circ r)(a^{-1}).$$

We use these results to prove Theorem 3.10.

Proof of Theorem 3.10. By the above discussion, we need to show that the $\mathrm{Sh}_{G_{\mathcal{O}}}(G,h)$ are defined over K provided that Φ is defined over K; and that in this case, every irreducible component of $\mathrm{Sh}_{G_{\mathcal{O}}}(G,h)$ is geometrically irreducible if and only if $f = \det_F \Phi$ induces the zero map $\mathrm{Cl}(K) \to \mathrm{Cl}^W(F)$. Note that G' is simply connected, since it is isomorphic to a special unitary group over F. Thus, we can invoke the theorems of Shimura above.

That $\mathrm{Sh}_{G_{\mathcal{O}}}(G,h)$ is defined over K is clear: because Φ is defined over K, the conjugacy class of $r \circ h$ is defined over K.

To see that every irreducible component of $\mathrm{Sh}_{G_{\mathcal{O}}}(G,h)$ is geometrically irreducible if and only if $f : \mathrm{Cl}(K) \to \mathrm{Cl}^W(F)$ is zero, we notice that

$$T = \left\{ (x,y) \in \left(\mathrm{Res}^F_{\mathbb{Q}} \mathbb{G}_{m,F}\right) \times \mathbb{G}_{m,\mathbb{Q}} : x \cdot \bar{x} = y^b \right\}$$

and the abelianization map $\nu : G \to T$ is $g \mapsto (\det g, a)$, where a is the unique element of $\mathbb{Q}$ for which $\langle gx, gy \rangle = a \cdot \langle x, y \rangle$. Under this identification, the map λ is

$$\lambda(a) = \left(\det_F \big((x \mapsto a \cdot x) : \Phi \to \Phi \big), \mathrm{Nm}^K_{\mathbb{Q}} a \right).$$

Thus, the irreducible components of $\mathrm{Sh}_{G_{\mathcal{O}}}(G,h)$ are geometrically irreducible if and only if for all $a \in K^\times(\mathbb{A})$, we have $\lambda(a) \subset \nu(G_{\mathcal{O}}) \cdot T(\mathbb{Q}) \cdot \nu(K_\infty)$.

As $\nu(G_{\mathcal{O}}) = T(\mathcal{O}_{\mathbb{A}^f})$ and $\nu(K^\infty)$ contains the connected component of $T(\mathbb{R})$, this is equivalent to the assertion that for all $a \in K^\times(\mathbb{A})$, we can find $x \in F^\times$ such that $(f(a)) = (x)$ and $x \cdot \bar{x} \in (\mathbb{Q}^\times)^b$. Since $(f(a) \cdot \overline{f(a)}) = (g(a))^b$ and $x \cdot \bar{x} > 0$, this is equivalent to $x \cdot \bar{x} \in \mathbb{Q}^\times$. But this is just the assertion that $f : \mathrm{Cl}(K) \to \mathrm{Cl}^W(F)$ is the zero map. □

https://doi.org/10.1017/S1474748013000182 Published online by Cambridge University Press

As a corollary of Theorem 3.10, we can re-prove a well-known fact about the field of definition of abelian varieties with full CM (see for example [12]).

Corollary 3.17. *If* $\dim_K \Phi = \frac{[F:\mathbb{Q}]}{2}$, *then there is an* (F, Φ)*-abelian variety* B *over* $K_{F,\Phi}$.

Proof. The Shimura varieties $\mathrm{Sh}_{G_\mathcal{O}}(G, h)$ are zero-dimensional; hence any geometrically irreducible component over $K_{F,\Phi}$ corresponds to a single (strong) (F, Φ)-abelian variety whose field of moduli is $K_{F,\Phi}$, which can be defined over its field of moduli by [11]. □

Corollary 3.18. *The intersection of all number fields* K *over which one can define an* (F, Φ)*-abelian variety is* $K_{F,\Phi}$.

Proof. This follows from Theorem 3.10 by a theorem of Rizov [15]. □

4. Associated characters of $A[\ell]$: local properties

In this section, we give some local properties of an associated character ψ of $A[\ell]$, most importantly Lemmas 4.3 and 4.10, and Corollary 4.7.

4.1. Action of Frobenius elements

Lemma 4.1 (Grothendieck). *Let* $v \in \Sigma_K \setminus \Sigma_\ell$ *be any prime not dividing* ℓ. *Then for any choice of Frobenius element* $\pi = \pi_v \in G_K$ *extending* $frob_v$, *the characteristic polynomial* P_π *of* π *acting on* $A[\ell^\infty]$ *has the following properties.*

(1) *The coefficients of* P_π *are integers, independent of* ℓ.
(2) *Every root of* P_π *has magnitude independent from the choice of complex embedding; the magnitude is* 1 *or* $\sqrt{\mathrm{Nm}v}$ *or* $\mathrm{Nm}v$.
(3) *The roots of* P_π *come in pairs which multiply to* $\mathrm{Nm}v$.

Proof. Properties 1 and 2 are Theorem 4.3(b) and Corollary 4.4 in [6] respectively; property 3 follows from the Galois-invariance of the Weil pairing. □

For the remainder of the paper, fix a prime ideal $\mathfrak{l} \subset \mathcal{O}_{\overline{\mathbb{Q}}}$ lying over ℓ.

Definition 4.2. For any prime v of K, choose a Frobenius element π over v and let

$$\psi_\mathbb{C}(v) \in \overline{\mathbb{Q}}$$

be a product of some choice of d distinct roots of P_π such that $\psi(\pi) \equiv \psi_\mathbb{C}(v) \bmod \mathfrak{l}$. (There may be several choices for $\psi_\mathbb{C}(v)$, but always at least one by the above lemma.)

Lemma 4.3. *For any prime ideal* $v \nmid \ell$, *there are only finitely many possible values of* $\psi_\mathbb{C}(v)$, *all of which are algebraic of degree at most* $\binom{2g}{d}$. *Moreover, there is some integer* a *with* $0 \leqslant a \leqslant 2d$ *such that under any complex embedding,*

$$|\psi_\mathbb{C}(v)| = \sqrt{|\mathrm{Nm}_\mathbb{Q}^K(v)|}^a.$$

https://doi.org/10.1017/S1474748013000182 Published online by Cambridge University Press

Proof. This is a direct consequence of Lemma 4.1. (To see that $\psi_{\mathbb{C}}(v)$ is algebraic of degree at most $\binom{2g}{d}$, note that any conjugate of $\psi_{\mathbb{C}}(v)$ in $\overline{\mathbb{Q}}$ is a product of d roots of the Frobenius polynomial $P_\pi \in \mathbb{Z}[x]$, and in particular there are at most $\binom{2g}{d}$ of them.) □

4.2. Semistable reduction

It is well-known that any abelian variety A becomes semistable after a finite extension of the ground field. In order to analyze the local action of $\rho_{A,\ell}$ in § 4.3, we need to make some more precise statements which let us control the ramification in a careful way.

Definition 4.4. For a set S of prime numbers, let $c_S(g)$ be the positive integer which, for all primes p, is exactly divisible by the biggest power p^a of p such that $\mathrm{Sp}_{2g}(\mathbb{F}_q)$ has an element of order p^a for all primes $q \in S \setminus \{p\}$. We define the constant $c(g) = c_P(g)$, where P is the set of all prime numbers.

Remark 4.5. For an alternative definition of $c(g)$, see Theorem 7.2.

Lemma 4.6. *For every prime v of K, there exists a finite and Galois extension L/K over which A acquires semistable reduction at primes of L lying over v, and the exponent of the inertia subgroup at v of* $\mathrm{Gal}(L/K)$ *divides $c(g)$.*

Proof. Write p_v for the residue characteristic of v. For any odd prime $p \neq p_v$, write $L^{(p)}$ for the field obtained by adjoining the p-torsion points of A to K. By Proposition 4.7 of [6], A acquires semistable reduction over each $L^{(p)}$.

Select some finite set $S = \{p_1, p_2, \ldots, p_k\}$ of primes, all distinct from p_v and coprime to the degree of some fixed polarization of A, such that $c_S(g) = c(g)$. As p_i does not divide the degree of some polarization, we get a Weil (symplectic) pairing on $A[p_i]$; therefore, the inertia subgroup at v in $\mathrm{Gal}(L^{(p_i)}/K)$ is contained in $\mathrm{Sp}_{2g}(\mathbb{F}_{p_i})$.

Write $F = L^{(p_1)} \cdot L^{(p_2)} \cdots L^{(p_k)}$ for the composite field, and $I \subset \mathrm{Gal}(F/K)$ for the inertia subgroup at v. Define $L \subset F$ to be the fixed field of the subgroup generated by the kernels of the restriction maps on I, i.e.

$$L = \text{fixed field of } \left(\left\langle \ker \left(I \to \mathrm{Gal}\left(L^{(p_i)}/K \right) \right) : i = 1, 2, \ldots k \right\rangle \subset \mathrm{Gal}(F/K) \right).$$

An element of $\mathrm{Gal}(L/K)$ is the image of an element of $\mathrm{Gal}(L^{(p_i)}/K)$ for any i, so its order divides $c(g)$.

To see that A acquires semistable reduction over L, fix some prime $q \notin \{p_v, p_1, p_2, \ldots, p_k\}$. By § 4.1 of [6], the subset $I' \subset I$ of elements acting unipotently on $A[q^\infty]$ form a normal subgroup. Proposition 3.5 of [6] implies that the kernel $\ker\left(I \to \mathrm{Gal}(L^{(p_i)}/K)\right)$ acts unipotently on $A[q^\infty]$ for all i; hence the kernel belongs to I'. Thus, the subgroup spanned by the kernels belongs to I', and therefore acts unipotently on $A[q^\infty]$. Applying Proposition 3.5 of [6] again, A acquires semistable reduction at v over L. □

https://doi.org/10.1017/S1474748013000182 Published online by Cambridge University Press

Corollary 4.7. *The character $\psi^{c(g)}$ is unramified at all $v \nmid \ell$.*

Proof. By Proposition 3.5 of [6], $\rho_{A,\ell,L}$ is unramified at v if v is semistable for A over L. Now $g^{c(g)} \in G_L \subset G_K$ for any $g \in G_K$; hence the corollary. □

Lemma 4.8. *Let $v|\ell$, and suppose $\ell \nmid c(g)$. Then, for any abelian variety A, there exists an extension L_w/K_v over which A acquires semistable reduction and such that $[L_w : K_v]|c(g)$.*

Proof. Write L^0 for the field L given by Lemma 4.6, and let w_0 be an extension of v to L^0. Since $\ell \nmid c(g)$, it follows that $L^0_{w_0}/K_v$ is tamely ramified. In particular, its inertia subgroup is cyclic. Thus, the order e of its inertia subgroup divides $c(g)$.

Write $I_v \subset G_v = \mathrm{Gal}(\overline{K_v}/K_v)$ for the inertia subgroup and $G_{\mathrm{res}} = \mathrm{Gal}(\overline{k_v}/k_v)$ for the Galois group of the residue field. Fix a choice of splitting $G_{\mathrm{res}} \to G_v$ making G_v into a semidirect product of I_v and G_{res}. If H_0 is the normal subgroup corresponding to $L^0_{w_0}$ then $H_0 \cap I_v$ is normal in G_v, and we can take for L_w the field corresponding to the (not necessarily normal) subgroup $H_0 \cap I_v \times G_{\mathrm{res}}$. □

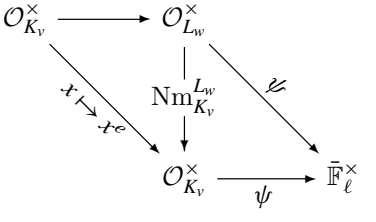
4.3. Action of inertia groups

Lemma 4.9. *If A has semistable reduction at $v|\ell$, then $\psi|_{I_v}$ is the reduction of a negative algebraic character of degree at most d times the ramification index of v.*

Proof. As explained in [6], § 2.2.3, we have a canonically defined subrepresentation $A[\ell]^{\mathrm{f}} \subset A[\ell]$ which comes from a finite flat commutative group scheme over $\mathrm{Spec}\mathcal{O}_{K_v}$. Thus, when restricted to the inertia subgroup, the associated character ψ decomposes as a product of at most d associated characters of $A[\ell]^{\mathrm{f}}$ and of the quotient $A[\ell]/A[\ell]^{\mathrm{f}}$. For the associated characters of $A[\ell]^{\mathrm{f}}$, we are done by Corollary 3.4.4 of [14]. On the other hand, Proposition 5.6 of [6] implies that the action of the Galois group on $A[\ell]/A[\ell]^{\mathrm{f}}$ is unramified at v, i.e., each associated character of the restriction to the inertia subgroup is trivial. □

Lemma 4.10. *Let $v|\ell$, and suppose $\ell \nmid \Delta_K \cdot c(g)$. Then, for any abelian variety A, the restriction $\psi^{c(g)}|_{I_v}$ is the reduction of a negative algebraic character of degree at most $d \cdot c(g)$.*

Proof. Let L_w be the field given by Lemma 4.8; write $e = [L_w : K_v]$. By functoriality of class field theory, the following diagram commutes:



https://doi.org/10.1017/S1474748013000182 Published online by Cambridge University Press

Since $\ell \nmid \Delta_K$, the ramification index of w is at most e. Therefore,

$$\psi(u)^{c(g)} = \psi(u^e)^{c(g)/e} = \psi\left(\mathrm{Nm}_{K_v}^{L_w} u\right)^{c(g)/e}$$

is the reduction of a negative algebraic character of degree at most $d \cdot c(g)$ by Lemma 4.9. □

5. Associated characters of $A[\ell]$: global analysis

In this section, we will patch the local information from the previous section together into global information in order to deduce the main theorem.

Remark 5.1. In fact, we will prove the main theorem using only Lemmas 4.3 and 4.10, and Corollary 4.7 from the previous section (as well as the fact that $c(g)$ is even). In particular, the conclusion of the main theorem holds more generally for any Galois character satisfying these three results. (When we make the main theorem effective in § 7, we will for concreteness use the more explicit Lemma 4.1 as well.)

5.1. The character θ^S

For the remainder of the paper, we will assume $\ell \nmid c(g) \cdot \Delta_K$. Taken together, the data of ψ at all inertia groups let us reconstruct $\psi^{c(g)}$ on the subgroup of G_K fixing the Hilbert class field. Namely let $U \subset \mathbb{I}$ be the group of units.

Lemma 5.2. *There is a positive algebraic character θ^F of degree at most $d \cdot c(g)$ such that the restriction $\psi^{c(g)}|_U \equiv (\theta_\ell^F)^{-1}$ mod $\mathfrak{l}$.*

Proof. This is an immediate consequence of Lemma 4.10 and the fact that $\psi^{c(g)}$ is unramified at $v \nmid \ell$ (by Corollary 4.7). (We do not need to worry about infinite places since $c(g)$ is even.) □

Definition 5.3. We say that a pair (S, e) where $e | c(g)$ and $S \in \mathbb{Z}[\Gamma_K]$ is of degree $d \cdot e$ *corresponds* to an associated character ψ if for all $x \in K^\times$ relatively prime to ℓ,

$$\psi(x_{\widehat{\ell}})^{c(g)} \equiv \theta^S(x)^{c(g)/e} \bmod \mathfrak{l}.$$

If e is coprime to S as an element of $\mathbb{Z}[\Gamma_K]$, we say that (S, e) is *reduced*.

Lemma 5.4. *Every associated character corresponds to a reduced pair (S, e). When A is semistable at all primes lying over ℓ, we can take $e = 1$.*

Proof. Let $F \in \mathbb{Z}[\Gamma_K]$ be the index from Lemma 5.2. Let f be the greatest common divisor of $c(g)$ and F, and write $e = c(g)/f$. By Lemma 4.9, $e = 1$ when A is semistable at all primes over ℓ. We define

$$S = \frac{F}{f} \in \mathbb{Z}[\Gamma_K].$$

Since $\psi(x_{\widehat{\ell}}) \cdot \psi(x_\ell) = 1$ for $x \in K^\times$, and $\theta^F(x) = (\theta^S(x))^{c(g)/e}$, we are done by Lemma 5.2. □

https://doi.org/10.1017/S1474748013000182 Published online by Cambridge University Press

5.2. Analysis of the character θ^S

Definition 5.5. We adopt the notation 'ℓ sufficiently large' to mean 'ℓ larger than a constant depending only on K and g'.

For the rest of this section, we fix K and one of the $(d \cdot c(g) + 1)^{n_K}$ possible reduced pairs (S, e), and we assume that (S, e) corresponds to an associated character of an abelian variety. Here we give ineffective bounds; we will make these arguments effective in § 7.

Lemma 5.6. *For ℓ sufficiently large, θ^S is balanced.*

Proof. Otherwise, by Lemma 2.15 there is a unit u for which $\theta^S(u)$ is not a root of unity. But then

$$\theta^S(u)^{c(g)/e} \equiv \psi(u_{\widehat{\ell}})^{c(g)} \equiv 1 \bmod \mathfrak{l},$$

which is a contradiction for ℓ sufficiently large, as ℓ divides the norm of their difference. □

Definition 5.7. We define h'_K to be the exponent of the class group $\mathrm{Cl}(K)$.

Lemma 5.8. *Let v be a prime ideal, and write $v^{h'_K} = (x)$. For ℓ sufficiently large relative to v,*

$$\psi_{\mathbb{C}}(v)^{c(g) \cdot h'_K} = \theta^S(x)^{c(g)/e}.$$

Proof. If ℓ is sufficiently large relative to v, then v does not lie over ℓ. Thus, for any choice of Frobenius element π_v at v, Lemma 5.4 implies

$$\psi\left(\pi_v^{h'_K}\right)^{c(g)} \equiv \theta^S(x)^{c(g)/e} \bmod \mathfrak{l}. \tag{4}$$

By Lemma 4.3, there are only finitely many possibilities for the left-hand side as A ranges over all abelian varieties of dimension g. Since ℓ divides the norm of their difference, the desired equality must hold for ℓ sufficiently large relative to v. □

Lemma 5.9. *For ℓ sufficiently large, there is a fixed integer a with $0 \leqslant a \leqslant 2d$ such that if σ and τ are complex conjugate embeddings, for any choice of embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$, then*

$$S(\sigma) + S(\tau) = ae.$$

Proof. By Lemma 5.6, there is an a' with $S(\sigma) + S(\tau) = a'$ for any complex conjugate embeddings σ and τ. It thus suffices to show that $a' = a \cdot e$ for an integer a with $0 \leqslant a \leqslant 2d$.

Let v be a prime ideal of K, and write $v^{h'_K} = (x)$. From Lemma 4.3, there exists some integer a with $0 \leqslant a \leqslant 2d$ such that under any complex embedding,

$$|\psi_{\mathbb{C}}(v)| = \sqrt{|\mathrm{Nm}_{\mathbb{Q}}^K(v)|}^a.$$

https://doi.org/10.1017/S1474748013000182 Published online by Cambridge University Press

On the other hand, under any complex embedding,

$$|\theta^S(x)| = \sqrt{|\mathrm{Nm}_{\mathbb{Q}}^K(x)|}^{a'} = \sqrt{|\mathrm{Nm}_{\mathbb{Q}}^K(v)|}^{a' \cdot h'_K}.$$

By Lemma 5.8,

$$\psi_{\mathbb{C}}(v)^{c(g) \cdot h'_K} = \theta^S(x)^{c(g)/e} \Rightarrow \psi_{\mathbb{C}}(v)^{e \cdot c(g) \cdot h'_K} = \theta^S(x)^{c(g)}.$$

Combining these,

$$\sqrt{|\mathrm{Nm}_{\mathbb{Q}}^K(v)|}^{a \cdot e \cdot c(g) \cdot h'_K} = |\psi_{\mathbb{C}}(v)|^{e \cdot c(g) \cdot h'_K} = |\theta^S(x)|^{c(g)} = \sqrt{|\mathrm{Nm}_{\mathbb{Q}}^K(v)|}^{a' \cdot c(g) \cdot h'_K}.$$

Hence $a' = a \cdot e$, which is what we wanted to show. □

Definition 5.10. We define $F \subset \overline{\mathbb{Q}}$ to be the smallest field containing the image of θ^S.

Lemma 5.11. *Let $v \subset \mathcal{O}_K$ be degree 1 prime, unramified in $K/\mathbb{Q}$. Then there is no factor e' of e such that $\theta^S(v)$ is an (e')th power in the group of ideals of F.*

Proof. By assumption, the set of exponents to which primes occur in the prime factorization of $\theta^S(v)$ are the same as the coefficients of S, so e is coprime to the greatest common divisor. □

Lemma 5.12. *Let ℓ be sufficiently large; suppose that $v \subset \mathcal{O}_K$ is a prime ideal of degree 1, unramified in $K/\mathbb{Q}$. Write $v^{h'_K} = (x)$. Then $\theta^S(x)^{c(g)/e}$ generates F over $\mathbb{Q}$.*

Proof. Take any $\tau \in \mathrm{Gal}(K^{\mathrm{gal}}/\mathbb{Q})$ which fixes $\theta^S(x)^{c(g)/e}$. We want to show that τ fixes the field F. Since τ fixes $\theta^S(x)^{c(g)/e}$, we have an equality of ideals of K^{gal}:

$$\left(\prod_{\sigma \in \Gamma_K} \sigma(v)^{S(\sigma)}\right)^{h'_K \cdot c(g)/e} = \left(\prod_{\sigma \in \Gamma_K} \tau\sigma(v)^{S(\sigma)}\right)^{h'_K \cdot c(g)/e}.$$

Since the group of ideals of K^{gal} is torsion-free, this implies

$$\prod_{\sigma \in \Gamma_K} \sigma(v)^{S(\sigma)} = \prod_{\sigma \in \Gamma_K} \tau\sigma(v)^{S(\sigma)} = \prod_{\sigma \in \Gamma_K} \sigma(v)^{S(\tau^{-1}\sigma)}.$$

Because v is an unramified prime of degree 1, its images under distinct embeddings into K^{gal} generate coprime ideals of K^{gal}. Hence, by the uniqueness of prime factorization for ideals of K^{gal}, we have $S(\sigma) = S(\tau^{-1}\sigma)$ for all $\sigma \in \Gamma_K$. Thus, for any $z \in K^\times$,

$$\theta^S(z) = \prod_{\sigma \in \Gamma_K} \sigma(z)^{S(\sigma)} = \prod_{\sigma \in \Gamma_K} \sigma(z)^{S(\tau^{-1}\sigma)} = \prod_{\sigma \in \Gamma_K} \tau\sigma(z)^{S(\sigma)} = \tau\theta^S(z),$$

so τ fixes the image of θ^S and hence the field F. □

The above lemma together with Lemma 4.3 implies that for ℓ sufficiently large, F has degree at most $\binom{2g}{d}$. In fact, we can prove a stronger statement.

https://doi.org/10.1017/S1474748013000182 Published online by Cambridge University Press

Lemma 5.13. *If ℓ is sufficiently large, then for any ideal class $\mathfrak{v} \in \mathrm{Cl}(K)$,*

$$\mathrm{ord}_{\mathrm{Cl}^W(F)}\left(C\theta^S(\mathfrak{v})\right) \cdot [F:\mathbb{Q}] \cdot e \leqslant \binom{2g}{d}.$$

Proof. By the Chebotarev Density Theorem, there is a prime ideal $v \subset \mathcal{O}_K$ representing the ideal class $\mathfrak{v}$ which is of degree 1 and unramified in $K/\mathbb{Q}$ (since the set of prime ideals of degree greater than 1 or ramified in $K/\mathbb{Q}$ has density zero). Write $v^{h'_K} = (x)$. By Lemma 5.8,

$$\psi_{\mathbb{C}}(v)^{c(g)\cdot h'_K} = \theta^S(x)^{c(g)/e}. \tag{5}$$

By Lemma 4.3, the field L generated by $\psi_{\mathbb{C}}(v)$ has degree at most $\binom{2g}{d}$. However, by Lemma 5.12, the right-hand side generates F; thus, $F \subset L$. Hence, we have an equality of ideals of L:

$$(\psi_{\mathbb{C}}(v))^{c(g)\cdot h'_K} = \left(\theta^S(x)^{c(g)/e}\right) = \theta^S(v)^{c(g)\cdot h'_K/e}.$$

Because the group of fractional ideals is torsion-free, $(\psi_{\mathbb{C}}(v))^e = \theta^S(v)$. Taking the norm down to F, we have an equality of ideals of F:

$$(\mathrm{Nm}_F^L \psi_{\mathbb{C}}(v))^e = (\theta^S(v))^{[L:F]}.$$

Since the left-hand side is an eth power in the group of ideals, the right-hand side must be as well; thus $e|[L:F]$ by Lemma 5.11. Because the group of ideals is torsion-free,

$$(\mathrm{Nm}_F^L \psi_{\mathbb{C}}(v)) = (\theta^S(v))^{\frac{[L:F]}{e}}.$$

The left-hand side is zero in $\mathrm{Cl}^W(F)$, so the right-hand side is too. This gives

$$\mathrm{ord}_{\mathrm{Cl}^W(F)}\left(\theta^S(v)\right) \leqslant \frac{[L:F]}{e} = \frac{[L:\mathbb{Q}]}{[F:\mathbb{Q}]\cdot e} \leqslant \frac{\binom{2g}{d}}{[F:\mathbb{Q}]\cdot e},$$

which implies the desired inequality. □

Lemma 5.14. *There exists an integer N divisible by eN_0 (recall that N_0 is the number of roots of unity in F) and satisfying $\varphi(N) \leqslant \binom{2g}{d}$ such that when restricted to $\mathrm{Gal}(\overline{K}/K_{F,\Phi})$,*

$$(\psi|_{\mathrm{Gal}(\overline{K}/K_{F,\Phi(S)})})^{e\cdot w} = \psi_{F,\Phi(S)}^w \quad \textit{where } w = \frac{1}{e}\cdot \mathrm{lcm}(N, c(g)).$$

Proof. Define

$$\chi = (\psi|_{\mathrm{Gal}(\overline{K}/K_{F,\Phi(S)})})^{e\cdot N_0} \otimes \psi_{F,\Phi(S)}^{N_0} \quad \text{and} \quad w_0 = \frac{c(g)}{\gcd(eN_0, c(g))}.$$

From Corollary 4.7, it follows that χ^{w_0} is unramified at all places not lying over ℓ. By assumption, it is trivial at all idèles of the form $x_{\widehat{\ell}}$ for $x \in K^\times$ relatively prime to ℓ. It follows that χ^{w_0} is trivial on $\mathrm{Gal}(\overline{K}/H_K)$ (by the idèlic formulation of class field theory). That is, χ^{w_0} gives a well-defined character $\chi^{w_0} : \mathrm{Gal}(H_K/K_{F,\Phi}) \to \overline{\mathbb{F}}_\ell^\times$.

https://doi.org/10.1017/S1474748013000182 Published online by Cambridge University Press

Let $\mathfrak{v}$ be an ideal class such that $\chi^{w_0}(\mathfrak{v})$ generates the image of χ^{w_0} in $\overline{\mathbb{F}}_\ell^\times$, and v be a prime ideal representing $\mathfrak{v}$ which is of degree 1, does not divide $h'_K \cdot c(g)$, and is unramified in $K/\mathbb{Q}$. By definition,

$$\chi(\pi_v) = X^{N_0} \quad \text{for } X = \frac{\psi_{\mathbb{C}}(v)^e}{g},$$

where $g \in F^\times$ is any Weil number such that $\theta^S(v) = (g)$.

Lemma 5.8 implies that $X^{h'_K \cdot c(g)} = 1$ for ℓ sufficiently large. Note that by Lemma 5.12, $F \subset \mathbb{Q}[\pi_{\mathbb{C}}(v)^e]$, so $\mathbb{Q}[X] \subset \mathbb{Q}[\psi_{\mathbb{C}}(v)^e] \cdot F \subset \mathbb{Q}[\psi_{\mathbb{C}}(v)^e]$.

By Lemma 5.11, there is no factor e' of e for which $(g) = \theta^S(v)$ is an (e')th power in the group of ideals of F. But Lemma 5.8 implies that $\psi_{\mathbb{C}}(\pi_v)^e$ equals g times an $(h'_K \cdot c(g))$th root of unity, so $\mathbb{Q}[\psi_{\mathbb{C}}(\pi_v)^e]/F$ is unramified at all primes dividing $\theta^S(v)$. Hence, there is no factor e' of e for which $(\psi_{\mathbb{C}}(v)^e) = (g)$ is an (e')th power in the group of ideals of $\mathbb{Q}[\psi_{\mathbb{C}}(v)^e]$. Consequently, $[\mathbb{Q}[\psi_{\mathbb{C}}(v)] : \mathbb{Q}[\psi_{\mathbb{C}}(v)^e]] = e$. Hence, Lemma 4.3 gives

$$[\mathbb{Q}[X] : \mathbb{Q}] \leqslant [\mathbb{Q}[\psi_{\mathbb{C}}(v)^e] : \mathbb{Q}] = \frac{1}{e} \cdot [\mathbb{Q}[\psi_{\mathbb{C}}(v)] : \mathbb{Q}] \leqslant \frac{1}{e} \cdot \binom{2g}{d}.$$

Since $\varphi(em) \leqslant e\varphi(m)$, we can take N to be e times the number of roots of unity in $\mathbb{Q}[X]$. By construction, $eN_0 | N$ and $X^{N/e} = 1$, so

$$(\psi|_{\mathrm{Gal}(\overline{K}/K_{F,\Phi(S)})})^{e \cdot w} = \psi^w_{F,\Phi(S)} \quad \text{where } w = \gcd(N/e, N_0 \cdot w_0) = \frac{1}{e} \cdot \mathrm{lcm}(N, c(g)). \qquad \square$$

Theorem 5.15. *Let K be a number field, g and d be positive integers, and ℓ is a prime number not belonging to some finite set $S_{K,g}$ depending only on K and g. Let A be a g-dimensional abelian variety defined over K, and ψ_0 an associated character of $\rho_{A,\ell}$ of degree d. Then there are a positive algebraic character θ^S and a positive integer e satisfying:*

(1) *The character θ^S is balanced, of total degree $a \cdot e$ for some $0 \leqslant a \leqslant 2d$.*
(2) *The induced map $C\theta^S : \mathrm{Cl}(K) \to \mathrm{Cl}^W(F)$ is trivial, i.e. $K \supset K_{F,\Phi(S)}$.*
(3) *There exists an integer N divisible by eN_0 and satisfying $\varphi(N) \leqslant \binom{2g}{d}$ such that*

$$\psi^{e \cdot w} = \psi^w_{F,\Phi(S)} \quad \textit{where } w = \frac{1}{e} \cdot \mathrm{lcm}(N, c(g)).$$

(4) *We have the inequality $[F : \mathbb{Q}] \cdot e \leqslant \binom{2g}{d}$.*

(Here, $\psi_{F,\Phi(S)}$ and $K_{F,\Phi(S)}$ are as in Definition 2.25.)

Proof. Write e' for the exponent of the induced map $C\theta^S : \mathrm{Cl}(K) \to \mathrm{Cl}^W(F)$. Then after replacing (S, e) with $(S \cdot e', e \cdot e')$, this follows from Lemmas 5.9, 5.13 and 5.14. $\square$

5.3. Proof of the main theorem

Theorem 5.16. *Let K be a number field, and g and d be positive integers. Then, there exists a finite set $S_{K,g}$ of prime numbers depending only on K and g, and a constant $0 < c(g) < 12^{4g^2}$ depending only on g such that, for a prime $\ell \notin S_{K,g}$, and a g-dimensional*

https://doi.org/10.1017/S1474748013000182 Published online by Cambridge University Press

abelian variety A with a mod-ℓ associated character ψ_0 of degree d, we have

$$\psi^{e\cdot w} \equiv \psi_{F,\Phi}^{w} (\mathrm{mod}\ \ell),$$

where ψ is either ψ_0 or $\mathrm{cyc}_\ell^d \otimes \psi_0^{-1}$ and $w = \frac{\mathrm{lcm}(N, c(g))}{\gcd(e, c(g))}$. Here, F is either $\mathbb{Q}$ or a CM field, and $\Phi : F \to \mathrm{End}(K^m)$ is a primitive balanced representation such that $K \supset K_{F,\Phi}$. The quantities a, e, and N are integers with e and N positive, which satisfy $m = \frac{1}{2} \cdot a \cdot e \cdot [F : \mathbb{Q}]$. Moreover, $0 \leqslant a \leqslant d$, and both $\varphi(N)$ and $e \cdot [F : \mathbb{Q}]$ are at most $\binom{2g}{d}$.

Proof. Let (S, e) corresponding to ψ be as in Theorem 5.15. Note that (S', e) corresponds to $\mathrm{cyc}_\ell^d \otimes \psi^{-1}$, where S' is defined by $S'(\sigma) = de - S(\sigma)$. One can easily check that (S', e) satisfies the conclusion of Theorem 5.15 for the character $\mathrm{cyc}_\ell^d \otimes \psi^{-1}$. Thus, by replacing ψ with $\mathrm{cyc}_\ell^d \otimes \psi^{-1}$ if necessary, we may suppose that $0 \leqslant a \leqslant d$.

Let Φ be the F-representation with $\det_F \Phi = \theta^S$ (see Theorem 3.6). By construction, $\dim \Phi = \frac{1}{2} \cdot [F : \mathbb{Q}] \cdot a \cdot e$. The conclusion of this theorem then follows from Theorem 5.15. □

Theorem 5.17. *In Theorem 5.16, if we assume in addition that A is semistable at primes lying over ℓ, then we can take $e = 1$, provided that we weaken the conclusion to be that $\psi^w = \psi_{F,\Phi}^w$ on $\mathrm{Gal}(\overline{K}/K \cdot K_{F,\Phi})$ and*

$$[F : \mathbb{Q}] \cdot (\mathrm{exponent} K \cdot K_{F,\Phi}/K) \leqslant \binom{2g}{d}.$$

Proof. We argue as in Theorem 5.16, without replacing (S, e) by $(e' \cdot S, e' \cdot e)$; instead, we replace K with the unramified abelian extension M of K defined by the kernel of $C\theta^S$. □

5.4. Some corollaries of the main theorem

Corollary 5.18. *Let K be a number field not containing any CM fields (which is in particular true when K has a real embedding), and g and d be positive integers. There exists a finite set $S_{K,g}$ of prime numbers depending only on K and g, and a constant $0 < c(g) < 12^{4g^2}$ depending only on g such that, for a prime $\ell \notin S_{K,g}$, and a g-dimensional abelian variety A with a mod-ℓ associated character ψ of degree d,*

$$\psi^{2w} = \mathrm{cyc}_\ell^{aw},$$

where a is an integer with $0 \leqslant a \leqslant 2d$, and $w = \frac{\mathrm{lcm}(c(g), N)}{2}$ for some positive $N \leqslant \binom{2g}{d}$.

Proof. Since $K \supset K_{F,\Phi}$ and $K_{F,\Phi}$ contains a CM field when F is a CM field, F cannot be a CM field. Thus, $F = \mathbb{Q}$, which gives the desired conclusion. □

Corollary 5.19. *Let K be a number field, and g and d be positive integers. Then, there exists a finite set $S_{K,g}$ of prime numbers depending only on K and g, and a constant $0 < c(g) < 12^{4g^2}$ depending only on g such that, for a prime $\ell \notin S_{K,g}$, and a g-dimensional abelian variety A with mod-ℓ associated character ψ of degree 1, one of the following holds.*

https://doi.org/10.1017/S1474748013000182 Published online by Cambridge University Press

(1) *The character* $\psi^{c(g)}$ *is trivial or equal to* $\mathrm{cyc}_\ell^{c(g)}$.

(2) *There exists an abelian unramified extension* M/K*, a (full) CM abelian variety* A' *defined over* M*, such that* K *contains the reflex field of the CM field of* A' *(which in particular implies that* A' *has CM defined over* M*), and an* ℓ*-adic associated character of degree* 1 *of* A'*, whose mod-*ℓ *reduction* ψ' *satisfies*

$$(\psi|_{\mathrm{Gal}(\overline{K}/M)})^{c(g)} = (\psi')^{c(g)} \quad \text{and} \quad (\dim A') \cdot (\text{exponent} M/K) \leqslant g.$$

Proof. Here, we use Theorem 5.17. The two cases correspond to $F = \mathbb{Q}$ and F a CM field. In the second case, we have $m = \frac{1}{2} \cdot [F : \mathbb{Q}]$, so the result follows from Corollary 3.17. □

The next two corollaries list the possible degree 1 associated characters for $g \in \{2, 3\}$. (Note that the easiest way of computing $c(g)$ is to use Theorem 7.2 of § 7 below.)

Corollary 5.20. *Let* K *be a number field. Then there exists a finite set* $S_{K,2}$ *of prime numbers depending only on* K *such that, for a prime* $\ell \notin S_{K,2}$*, and an abelian surface* A *with a mod-* ℓ *associated character* ψ *of degree* 1*, one of the following holds.*

(1) *There exists a full CM abelian surface* A' *over* K *whose CM is defined over* K*, with an* ℓ*-adic degree* 1 *associated character whose mod-* ℓ *reduction* ψ' *satisfies*

$$\psi^{120} = (\psi')^{120}.$$

(2) *There exists an abelian unramified extension* L/K *of exponent at most* 2*, a CM elliptic curve* E' *defined over* L*, such that* K *contains the CM field, and an* ℓ*-adic degree* 1 *associated character of* E' *whose mod-* ℓ *reduction* ψ' *satisfies*

$$\psi|^{120}_{\mathrm{Gal}(\overline{K}/L)} = (\psi')^{120}.$$

(3) *For some* $a \in \{0, 60, 120\}$*,*

$$\psi^{120} = \mathrm{cyc}_\ell^a.$$

Corollary 5.21. *Let* K *be a number field. Then there exists a finite set* $S_{K,3}$ *of prime numbers depending only on* K *such that, for a prime* $\ell \notin S_{K,3}$*, and an abelian threefold* A *with a mod-* ℓ *associated character* ψ *of degree* 1*, one of the following holds.*

(1) *There exists a full CM abelian surface or threefold* A' *over* K *whose CM is defined over* K*, with an* ℓ*-adic degree* 1 *associated character whose mod-* ℓ *reduction* ψ' *satisfies*

$$\psi^{2520} = (\psi')^{2520}.$$

(2) *There exists an abelian unramified extension* L/K *of exponent at most* 3*, a CM elliptic curve* E' *defined over* L*, such that* K *contains the CM field, and an* ℓ*-adic degree* 1 *associated character of* E' *whose mod-* ℓ *reduction* ψ' *satisfies*

$$\psi|^{2520}_{\mathrm{Gal}(\overline{K}/L)} = (\psi')^{2520}.$$

https://doi.org/10.1017/S1474748013000182 Published online by Cambridge University Press

(3) *There exists a CM elliptic curve E' over K, such that K contains the CM field, and an ℓ-adic degree 1 associated character of E' whose mod-ℓ reduction ψ' satisfies*

$$\psi^{2520} = (\psi' \otimes \mathrm{cyc}_\ell)^{840}.$$

(4) *For some $a \in \{0, 1260, 2520\}$,*

$$\psi^{2520} = \mathrm{cyc}_\ell^a.$$

Remark 5.22. For $g \geqslant 4$, the Shimura varieties relevant to Theorem 5.16 may have nonzero dimension even for $d = 1$, so no similar reformulation is possible.

6. The special case of elliptic curves

In this section we specialize to the case $g = 1$, i.e. where $A = E$ is an elliptic curve.

6.1. Theorem 5.16 in the case $g = 1$

Lemma 6.1. *Let K be a number field. Then, there exists a finite set S_K of prime numbers depending only on K such that, for a prime $\ell \notin S_K$, and an elliptic curve E over K for which $E[\ell] \otimes \overline{\mathbb{F}}_\ell$ is reducible with degree 1 associated character ψ, one of the following holds.*

(1) *We have $\psi^{12} \in \{1, \mathrm{cyc}_\ell^6, \mathrm{cyc}_\ell^{12}\}$.*

(2) *There exists a CM elliptic curve E', defined over K and whose CM field is contained in K, with an ℓ-adic degree 1 associated character whose mod-ℓ reduction ψ' satisfies*

$$\psi^{12} = (\psi')^{12}.$$

Proof. If $F = \mathbb{Q}$ in Theorem 5.16, case 1 holds. Otherwise, F is imaginary quadratic, and we can take $E' = \mathbb{C}/\mathcal{O}_F$, since $\psi_{F,\Phi} = \psi'$ and $K_{F,\Phi}$ is the Hilbert class field of F. □

6.2. The Effective Chebotarev Theorem

Under GRH, we have the following effective version of the Chebotarev Density Theorem, due to Lagarias and Odlyzko, with improvements due to Bach.

Theorem (Effective Chebotarev Theorem). *Let E/K be a Galois extension of number fields with $E \neq \mathbb{Q}$. Under GRH, there exists an effectively computable absolute constant c_5 such that every conjugacy class of $\mathrm{Gal}(E/K)$ is represented by a Frobenius element of a prime ideal $v \in \Sigma_K$ which is unramified in E, such that*

$$\mathrm{Nm}_{K/\mathbb{Q}}(v) \leqslant c_5(\log \Delta_E)^2.$$

Moreover, we can take v to be a prime of degree 1 and unramified in $K/\mathbb{Q}$.

Proof. See [7], the remark at the end of paper regarding the improvement to Corollary 1.2. That we can take $\mathfrak{p}$ to be of degree 1 and unramified in $K/\mathbb{Q}$ follows from Theorem 3.1 in [1]. □

https://doi.org/10.1017/S1474748013000182 Published online by Cambridge University Press

Remark 6.2. Unconditionally, a similar theorem is true, with the bound of $c_5(\log \Delta_E)^2$ replaced by $\exp(c_6 \Delta_E)$, for an effectively computable absolute constant c_6.

We will need a slight strengthening of the above theorem, to avoid issues at the prime 3.

Corollary 6.3. *Let E/K be a Galois extension of number fields with $E \neq \mathbb{Q}$, and let N be a positive (rational) integer. Then under GRH, there exists an effectively computable absolute constant c_7 such that every conjugacy class of $\mathrm{Gal}(E/K)$ is represented by a Frobenius element of a prime ideal $v \in \Sigma_K$ which is unramified in E, such that*

$$\mathrm{Nm}_{K/\mathbb{Q}}(v) \leqslant c_7 \cdot (\log \Delta_E + n_E \log N)^2.$$

Moreover, we can take v to be of degree 1, unramified in $K/\mathbb{Q}$, and not divide N.

Proof. This is proven in [18] for $K = \mathbb{Q}$. Thanks to Bach's improvement to the Effective Chebotarev Theorem (that we can take v to be unramified in $K/\mathbb{Q}$), the same argument works for arbitrary number fields. For completeness, we recall the proof below.

Clearly, we can assume that N is square-free. Define $E' = E[\sqrt{N}]$. Then every prime of E' lying over a prime divisor of N is ramified in $E'/\mathbb{Q}$.

Now, we apply the Effective Chebotarev Theorem to $\mathrm{Gal}(E'/K)$, to conclude that every conjugacy class of $\mathrm{Gal}(E'/K)$ is represented by a Frobenius element of a prime ideal $v \in \Sigma_K$ of degree 1 which is unramified in E' and in $K/\mathbb{Q}$, and thus is coprime to N, such that $\mathrm{Nm}_{\mathbb{Q}}^K(v) \leqslant c_5(\log \Delta_{E'})^2$. Since E'/E is ramified only at primes dividing $2N$, we can bound $\Delta_{E'}$ using Proposition 5 of § 1.3 of [18], and thereby conclude we can take v such that

$$\begin{aligned}\mathrm{Nm}_{\mathbb{Q}}^K(v) &\leqslant c_5(\log \Delta_{E'})^2 \\ &\leqslant c_5 \cdot (2\log \Delta_E + n_E \log 2N + n_E \log 2)^2 \\ &\leqslant c_7 \cdot (\log \Delta_E + n_E \log N)^2\end{aligned}$$

for some effectively computable absolute constant c_7. □

6.3. Proof of Theorem 6.4

Theorem 6.4. *Let K be a number field. There exists a finite set S_K of prime numbers depending only on K such that, for a prime $\ell \notin S_K$, and elliptic curve E over K for which $E[\ell] \otimes \overline{\mathbb{F}}_\ell$ is reducible with degree 1 associated character ψ, one of the following holds.*

(1) *There exists a CM elliptic curve E', defined over K and whose CM field is contained in K, with an ℓ-adic degree 1 associated character whose mod- ℓ reduction ψ' satisfies*

$$\psi^{12} = (\psi')^{12}.$$

(2) *The Generalized Riemann Hypothesis fails for $K[\sqrt{-\ell}]$, and*

$$\psi^{12} = \mathrm{cyc}_\ell^6,$$

where cyc_ℓ is the cyclotomic character. (Moreover, in this case we must have $\ell \equiv 3$ mod 4 and the representation $\rho_{E,\ell}$ is already reducible over $\mathbb{F}_\ell$.)

https://doi.org/10.1017/S1474748013000182 Published online by Cambridge University Press

Proof. Since $\rho_{E,\ell}$ is reducible and two-dimensional, its semisimplification is the direct sum of two associated characters ψ_1 and ψ_2. If $\psi_1^{12} \notin \{1, \mathrm{cyc}_\ell^6, \mathrm{cyc}_\ell^{12}\}$, then by Lemma 6.1, case 1 holds. Hence, it remains to show that case 2 holds when $\psi_1^{12} \in \{1, \mathrm{cyc}_\ell^6, \mathrm{cyc}_\ell^{12}\}$.

Case 1: $\psi_1^{12} \in \{1, \mathrm{cyc}_\ell^{12}\}$. If $\psi_1^{12} = \mathrm{cyc}_\ell^{12}$, then the Weil pairing gives

$$\psi_2^{12} = (\mathrm{cyc}_\ell \otimes \psi_1^{-1})^{12} = \mathrm{cyc}_\ell^{12} \otimes (\psi_1^{12})^{-1} = 1.$$

Thus, by interchanging indices if necessary, we can assume that ψ_1^{12} is trivial.

Then, ψ_1 defines a degree (at most) 12 extension M of K. By construction, ψ_1 is trivial on $\mathrm{Gal}(K^{\mathrm{ab}}/M)$. Thus, we have a Galois-invariant subspace $V \subset E[\ell]$ such that either V is pointwise fixed by $G_M = \mathrm{Gal}(\overline{K}/M)$, or the quotient $E[\ell]/V$ is pointwise fixed by G_M. In the first case, E has an ℓ-torsion point defined over M, and in the second case, the isogenous curve E/V has an ℓ-torsion point defined over M. Writing $n_M \leqslant 12n_K$ for the degree of M, Merel's Theorem [10] implies that

$$\ell \leqslant \left(\sqrt{3^{n_M}} + 1\right)^2 \leqslant \left(3^{6n_K} + 1\right)^2.$$

Thus, so long as we choose S_K to contain all primes at most $\left(3^{6n_K} + 1\right)^2$, we are done.

Case 2: $\psi_1^{12} = \mathrm{cyc}_\ell^6$. The Weil pairing implies

$$\psi_2^{12} = (\mathrm{cyc}_\ell \otimes \psi_1^{-1})^{12} = \mathrm{cyc}_\ell^{12} \otimes (\psi_1^{12})^{-1} = \mathrm{cyc}_\ell^{12} \otimes (\mathrm{cyc}_\ell^6)^{-1} = \mathrm{cyc}_\ell^6.$$

In other words,

$$\widetilde{\rho}_{E,\ell}^{12} = \mathrm{cyc}_\ell^6 \oplus \mathrm{cyc}_\ell^6.$$

If $\rho_{E,\ell}$ is irreducible over $\mathbb{F}_\ell$, then $\widetilde{\rho}_{E,\ell} = \rho_{E,\ell}$, so the projective image of $\rho_{E,\ell}$ in $\mathrm{PGL}_2(\mathbb{F}_\ell)$ has order at most 6. But by Lemma 18′ of [18] (which is stated for $K = \mathbb{Q}$, but the same proof works as long as ℓ is unramified in K), the projective image has an element of order at least $(\ell - 1)/4$. Hence, choosing S_K to contain all primes less than 25, it follows that $\rho_{E,\ell}$ is already reducible over $\mathbb{F}_\ell$.

In particular, cyc_ℓ^6 is the twelfth power of some character valued in $\mathbb{F}_\ell^\times$. Since we are assuming that ℓ is unramified in K, the cyclotomic character surjects onto $\mathbb{F}_\ell^\times$. Thus, every sixth power in $\mathbb{F}_\ell^\times$ is a twelfth power, so $\ell \equiv 3 \bmod 4$.

Now, suppose GRH holds for $K[\sqrt{-\ell}]$. By Corollary 6.3, there is a prime ideal v of K such that v is split in $K[\sqrt{-\ell}]$, of degree 1, does not lie over 3, and satisfies the inequality

$$\begin{aligned}\mathrm{Nm}_{\mathbb{Q}}^K(v) &\leqslant c_7 \cdot (\log \Delta_{K[\sqrt{\pm\ell}]} + n_{K[\sqrt{\pm\ell}]} \log 3)^2 \\ &= 4c_7 \cdot (2 \log \Delta_K + 2n_K \log 3 + n_K \log \ell)^2.\end{aligned}$$

We claim that $\psi_{1,\mathbb{C}}(\pi_v) + \psi_{2,\mathbb{C}}(\pi_v) = 0$, for ℓ more than a constant depending on K alone. Indeed,

$$\psi_{1,\mathbb{C}}(\pi_v) + \psi_{2,\mathbb{C}}(\pi_v) \equiv \sqrt{\mathrm{Nm}_{\mathbb{Q}}^K(v)} \cdot (\zeta + \overline{\zeta}) \bmod \mathfrak{l}$$

https://doi.org/10.1017/S1474748013000182 Published online by Cambridge University Press

for a twelfth root of unity ζ. As $v \nmid 3$, the right-hand side cannot be a nonzero rational number. Thus, if $\psi_{1,\mathbb{C}}(\pi_v)+\psi_{2,\mathbb{C}}(\pi_v) \neq 0$, we have a nontrivial divisibility condition on ℓ:

$$\ell \left| \mathrm{Nm}_{\mathbb{Q}}^{\mathbb{Q}\left[\sqrt{\mathrm{Nm}_{\mathbb{Q}}^{K}(v)}\cdot(\zeta+\overline{\zeta})\right]} \left(\sqrt{\mathrm{Nm}_{\mathbb{Q}}^{K}(v)} \cdot (\zeta + \overline{\zeta}) - (\psi_{1,\mathbb{C}}(\pi_v) + \psi_{2,\mathbb{C}}(\pi_v)) \right) . \right.$$

But under any complex embedding,

$$\left| \sqrt{\mathrm{Nm}_{\mathbb{Q}}^{K}(v)} \cdot (\zeta + \overline{\zeta}) - (\psi_{1,\mathbb{C}}(\pi_v) + \psi_{2,\mathbb{C}}(\pi_v)) \right| \leqslant \left(1 + \sqrt{\mathrm{Nm}_{\mathbb{Q}}^{K}(v)} \right)^2 .$$

Since $\mathbb{Q}\left[\sqrt{\mathrm{Nm}_{\mathbb{Q}}^{K}(v)} \cdot (\zeta + \overline{\zeta})\right]$ is a quadratic field,

$$\ell \leqslant \left(1 + \sqrt{\mathrm{Nm}_{\mathbb{Q}}^{K}(v)} \right)^4 \leqslant \left(1 + 2\sqrt{c_7} \cdot (2 \log \Delta_K + 2n_K \log 3 + n_K \log \ell)\right)^4.$$

But this is clearly impossible for all ℓ larger than a constant depending on K alone. Thus, we have $\psi_{1,\mathbb{C}}(\pi_v) + \psi_{2,\mathbb{C}}(\pi_v) = 0$. Hence,

$$(\psi_{1,\mathbb{C}}(\pi_v) - \psi_{2,\mathbb{C}}(\pi_v))^2 = (\psi_{1,\mathbb{C}}(\pi_v) + \psi_{2,\mathbb{C}}(\pi_v))^2 - 4\psi_{1,\mathbb{C}}(\pi_v)\psi_{2,\mathbb{C}}(\pi_v) = -4\mathrm{Nm}_{\mathbb{Q}}^{K} v,$$

which is a quadratic nonresidue mod ℓ, contradicting the reducibility of $\rho_{E,\ell}$. □

Corollary 6.5. *Under GRH, the degrees of prime degree isogenies of elliptic curves over K are bounded uniformly if and only if K does not contain the Hilbert class field of an imaginary quadratic field (i.e. if and only if there are no elliptic curves with CM defined over K).*

Proof. If K does not contain the Hilbert class field of an imaginary quadratic field F, then there are no CM elliptic curves which are defined over K and whose CM field is contained in K. Thus, $\rho_{E,\ell}$ is absolutely irreducible if $\ell \notin S_K$, for any elliptic curve E over K. In particular, E cannot admit an isogeny of degree ℓ.

Conversely, if K contains the Hilbert class field of an imaginary quadratic field F, then there is a CM elliptic curve defined over K, whose CM field is contained in K. But such a curve has an isogeny of degree ℓ for all primes ℓ split in F. □

7. Effective results

In this section, we prove Theorem 7.9, making Theorems 5.16 and 6.4 (as well as Corollary 6.5) effective. The method of proof does not depend essentially on GRH; we only use GRH in § 7.4 when putting everything together to get the final bound.

7.1. The quantity $c(g)$

In this section, we calculate the value of $c(g)$ (see Definition 4.4).

Lemma 7.1. *Suppose q is a prime power and $[\mathbb{Q}[\zeta_q] : \mathbb{Q}] \leqslant 2g$. Then $q | c(g)$.*

https://doi.org/10.1017/S1474748013000182 Published online by Cambridge University Press

Proof. For every prime p coprime to q, we have a symplectic form on $\mathcal{O}_{\mathbb{Q}[\zeta_q]}/(p)$ given by

$$(\alpha, \beta) \mapsto \mathrm{Tr}_{\mathbb{Q}}^{\mathbb{Q}[\zeta_q]} \left(\alpha\overline{\beta} - \beta\overline{\alpha}\right).$$

Multiplication by ζ_q thus defines an element of $\mathrm{Sp}_{[\mathbb{Q}[\zeta_q]:\mathbb{Q}]}(\mathbb{F}_p)$ of order q. Since we have an injection $\mathrm{Sp}_{[\mathbb{Q}[\zeta_q]:\mathbb{Q}]}(\mathbb{F}_p) \hookrightarrow \mathrm{Sp}_{2g}(\mathbb{F}_p)$, it follows that $q|c(g)$ by the definition of $c(g)$. □

Theorem 7.2. *We have*

$$c(g) = \prod_{\substack{\text{prime powers } p^n \\ (p-1)p^{n-1} \leqslant 2g < (p-1)p^n}} p^n.$$

In particular, $c(1) = 12$. *In general, for some effectively computable absolute constant* c_1,

$$c(g) \leqslant c_1 \cdot (7.4)^g \leqslant c_1 \cdot 8^g.$$

Proof. From the prime number theorem, we have

$$\prod_{\substack{\text{prime powers } p^n \\ (p-1)p^{n-1} \leqslant 2g < (p-1)p^n}} p^n = e^{2g(1+o(1))} \leqslant c_1 \cdot 7.4^g \leqslant c_1 \cdot 8^g$$

for an effectively computable absolute constant c_1. Thus, it suffices to verify the formula for $c(g)$. By Lemma 7.1, it is clear that $c(g)$ is divisible by the above product. Conversely, take $p^n|c(g)$; we will show that p^n divides the above product.

Case 1: p *is odd.* By Dirichlet's Theorem, there is an odd prime $q \neq p$ whose class mod p^n generates the cyclic group $(\mathbb{Z}/p^n\mathbb{Z})^\times$. Suppose there is an element $X \in \mathrm{Sp}_{2g}(\mathbb{F}_q)$ of order p^n. Applying the Frobenius automorphism of $\overline{\mathbb{F}}_q$ to X, we see that if X has an eigenvalue ω, it must also have an eigenvalue ω^q. Therefore, every primitive (p^n)th root of unity would be an eigenvalue of X, so $(p-1)p^{n-1} = |(\mathbb{Z}/p^n\mathbb{Z})^\times| \leqslant 2g$.

Case 2: $p = 2$. By Dirichlet's Theorem, we can find a prime $q \equiv 3 \bmod 2^n$. Suppose there was an element $X \in \mathrm{Sp}_{2g}(\mathbb{F}_q)$ of order 2^n. Applying the Frobenius automorphism of $\overline{\mathbb{F}}_q$ to X, we see that if X has an eigenvalue ω, it must also have an eigenvalue ω^q. Since $X \in \mathrm{Sp}_{2g}(\mathbb{F}_q)$, we see that if X has an eigenvalue ω, it must also have an eigenvalue ω^{-1}.

But it is well-known that $q \equiv 3$ and -1 generate $(\mathbb{Z}/2^n\mathbb{Z})^\times$. As X has order 2^n, it has an eigenvalue which is a primitive (2^n)th root of unity; hence, every primitive (2^n)th root of unity is an eigenvalue of X. Consequently, $2^{n-1} = |(\mathbb{Z}/2^n\mathbb{Z})^\times| \leqslant 2g$. □

7.2. Balanced characters

Here we make Lemma 5.6 effective; we also note that balanced characters have bounds on their archimedean valuations, which will be helpful for making other arguments effective.

Lemma 7.3. *When* θ^S *is balanced with* $S(\sigma) + S(\tau) = a'$, *then for any archimedean absolute value* $|\ |$ *on* K,

$$|\theta^S(x)| = \sqrt{\mathrm{Nm}_{\mathbb{Q}}^K(x)}^{a'}.$$

Proof. Clear from Definition 2.13. □

https://doi.org/10.1017/S1474748013000182 Published online by Cambridge University Press

For every unbalanced character θ^S, there is a unit u_S for which $\theta^S(u_S)$ is not a root of unity. Observe that we have a natural action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the elements $S \in \mathbb{Z}[\Gamma_K]$. If S and S' are related under this action, then $\theta^S(u)$ is Galois-conjugate to $\theta^{S'}(u)$; in particular, $\theta^S(u)$ is a root of unity if and only if $\theta^{S'}(u)$ is a root of unity. Thus, we can choose the u_S such that they depend only on the orbit of S under the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. If we do this,

$$B_{\mathrm{char}}(K, g) := \prod_{\theta^S \text{ unbalanced}} \left(1 - \theta^S(u_S)^{c(g)/e}\right)$$

is a rational integer. Moreover, by Definition 5.3, any prime ℓ for which a corresponding character θ^S is unbalanced must divide $B_{\mathrm{char}}(K, g)$.

Lemma 7.4. *There exists an effectively computable absolute constant c_8 for which we can choose the u_S such that the following inequality holds:*

$$B_{\mathrm{char}}(K, g) \leqslant c_8 \cdot \exp\left(\frac{2 \cdot R_K \cdot (r_K + 2)! \cdot (2g \cdot c(g) + 1)^{n_K+1} \cdot (\log n_K)^3}{|\log\log n_K|^3}\right).$$

Remark 7.5. The constant $B_{\mathrm{char}}(K, g)$ can be directly computed for any field K, and in many interesting cases (such as that of quadratic imaginary fields) is small.

Proof. Define the multiplicative Minkowski embedding μ and functions f^S as in the proof of Lemma 2.15. Suppose that θ^S is a unbalanced character.

Write $\Lambda_S \subset \Lambda$ for the kernel of f^S. Since θ^S is unbalanced, $\Lambda_S \subsetneq \Lambda$. By definition, f^S does not vanish on any element of the quotient lattice Λ/Λ_S. Therefore, to choose u_S such that $f^S(u_S)$ is small, it suffices to find a short lattice vector of the quotient lattice Λ/Λ_S, which we can do via Minkowski's Theorem if we first bound

$$\mathrm{vol}(\Lambda/\Lambda_S) = \frac{\mathrm{vol}(\Lambda)}{\mathrm{vol}(\Lambda_S)} = \frac{R_K\sqrt{r_K+1}}{\mathrm{vol}(\Lambda_S)}.$$

(Here, we think of Λ/Λ_S sitting inside $\mathbb{R}_0^{r_K+1}/\langle\Lambda_S\rangle$, which we give an inner product by identifying it with the orthogonal complement of Λ_S and taking the induced inner product from $\mathbb{R}_0^{r_K+1}$.) To do this, we use the following theorem of Voutier:

Theorem (Voutier [20]). *For any $u \in \mathcal{O}_K^\times$ which is not a root of unity,*

$$\log\left(\prod_{i=1}^{n_K} \max(1, |\sigma_i(u)|)\right) \geqslant \alpha \quad \textit{where } \alpha = \frac{1}{4}\left(\frac{\log\log n_K}{\log n_K}\right)^3.$$

It follows that the length of any unit in Λ under the L^1 norm (i.e. the sum of the absolute values of the coordinates) satisfies

$$\begin{aligned}\|\mu(u)\|_{L^1} &= \sum_{i=1}^{r_1} |\log|\sigma_i(u)|| + \sum_{i=r_1+1}^{r_1+r_2} 2|\log|\sigma_i(u)|| \\ &= 2 \cdot \log\left(\prod_{i=1}^{n_K} \max(1, |\sigma_i(u)|)\right) \geqslant 2\alpha.\end{aligned}$$

https://doi.org/10.1017/S1474748013000182 Published online by Cambridge University Press

(For the second equality above, we use $\sum_{i=1}^{n_K} \log|\sigma_i(u)| = 0$.) Extend Λ_S to a lattice Λ'_S of dimension $r_K + 1$ by adding more basis vectors which are mutually orthogonal, orthogonal to Λ_S, and whose length (under the euclidean metric) equals 2α. By the above theorem, the (open) unit L^1-ball of radius 2α intersects Λ'_S only at the origin, so by Minkowski's Theorem,

$$\mathrm{vol}(\Lambda'_S) \geqslant \frac{1}{2^{r_K+1}} \cdot \left(\frac{2^{r_K+1}}{(r_K+1)!} \cdot (2\alpha)^{r_K+1} \right) = \frac{(2\alpha)^{r_K+1}}{(r_K+1)!}.$$

Write c for the codimension of Λ_S in Λ. Then,

$$\mathrm{vol}(\Lambda_S) = \frac{1}{(2\alpha)^{c+1}} \cdot \mathrm{vol}(\Lambda'_S) \geqslant \frac{1}{(2\alpha)^{c+1}} \cdot \frac{(2\alpha)^{r_K+1}}{(r_K+1)!} = \frac{(2\alpha)^{r_K-c}}{(r_K+1)!}$$

which gives

$$\mathrm{vol}(\Lambda/\Lambda_S) = \frac{\mathrm{vol}(\Lambda)}{\mathrm{vol}(\Lambda_S)} \leqslant \frac{R_K \cdot \sqrt{r_K+1} \cdot (r_K+1)!}{(2\alpha)^{r_K-c}}.$$

Applying Minkowski's Theorem again, there is a vector in Λ/Λ_S whose length under the euclidean metric (we use the euclidean metric because the L^1 metric on $\mathbb{R}^{r_K+1}$ does not induce the L^1 metric on $\mathbb{R}_0^{r_K+1}/\langle\Lambda_S\rangle$) is bounded by (here, we use that the volume of the unit euclidean c-ball is greater than that of the unit L^1-ball, $2^c/c!$)

$$\begin{aligned}(\mathrm{vol}(\Lambda/\Lambda_S) \cdot c!)^{\frac{1}{c}} &\leqslant \left(\frac{R_K \cdot \sqrt{r_K+1} \cdot (r_K+1)!}{(2\alpha)^c} \cdot c! \right)^{\frac{1}{c}} \\ &= \frac{1}{2\alpha} \cdot \left(R_K \cdot \sqrt{r_K+1} \cdot (r_K+1)! \cdot c! \right)^{\frac{1}{c}}.\end{aligned}$$

The above is a decreasing function of c, since $R_K \geqslant 1/5$ by [5]. Thus,

$$\leqslant \frac{R_K \cdot \sqrt{r_K+1} \cdot (r_K+1)!}{2\alpha}.$$

Consequently, we can find some vector of Λ/Λ_S whose length under the metric induced from the L^1 metric on $\mathbb{R}^{r_K+1}$ is bounded by

$$\sqrt{r_K+1} \cdot \frac{R_K \cdot \sqrt{r_K+1} \cdot (r_K+1)!}{2\alpha} \leqslant \frac{R_K \cdot (r_K+2)!}{2\alpha}.$$

Now, observe that $|f^S(u)| \leqslant 2g \cdot c(g) \cdot \|\mu(u)\|_{L^1}$ for any S. Therefore, for any unbalanced character θ^S, we can select u_S such that $\theta^S(u_S)$ is not a root of unity, and

$$|\log|\theta^{S'}(u_S)^{c(g)/e}|| \leqslant M \quad \text{where } M := 2g \cdot c(g) \cdot \frac{R_K \cdot (r_K+2)!}{2\alpha}$$

https://doi.org/10.1017/S1474748013000182 Published online by Cambridge University Press

where S' is any subset of Γ_K. This gives

$$\begin{aligned} B_{\mathrm{char}}(K,g) &= \prod_{\substack{S\subset\Gamma_K \\ \theta^S \text{ is unbalanced}}} \left(1-\theta^S(u_S)^{c(g)/e}\right) \\ &\leqslant \prod_{\substack{S\subset\Gamma_K \\ \theta^S \text{ is unbalanced}}} \left(1+|\theta^S(u_S)^{c(g)/e}|\right) \\ &\leqslant (1+\exp(M))^{(2g\cdot c(g)+1)^{n_K}}. \end{aligned}$$

Since $\exp(M) \geqslant c_9 \cdot (2g\cdot c(g)+1)^{n_K}$ for some effectively computable absolute constant c_9, we have for some effectively computable absolute constant c_8,

$$\begin{aligned} B_{\mathrm{char}}(K,g) &\leqslant c_8 \cdot \exp(M\cdot(2g\cdot c(g)+1)^{n_K}) \\ &= c_8 \cdot \exp\left(\frac{2\cdot R_K\cdot(r_K+2)!\cdot(2g\cdot c(g)+1)^{n_K+1}\cdot(\log n_K)^3}{(\log\log n_K)^3}\right). \quad \square \end{aligned}$$

For the rest of the paper, we suppose that $\ell \nmid B_{\mathrm{char}}(K,g)$, so θ^S is a balanced character.

7.3. Bounds for Theorem 5.15

Lemma 7.6. *Let $v \subset \mathcal{O}_K$ be a prime ideal, with $\mathrm{Nm}_{\mathbb{Q}}^K v \leqslant V$. Then, as A ranges over all abelian varieties of dimension g, and d ranges over all integers between 0 and $2g$, and ℓ ranges over all rational primes coprime to x, there are at most*

$$B_{\mathrm{poss}}(K,g,V) = c_{10}\cdot(256\cdot V)^{\frac{g(g+1)}{4}}$$

possible values of $\psi_{\mathbb{C}}(v)$, for some effectively computable absolute constant c_{10}. Moreover, the magnitude of $\psi_{\mathbb{C}}(v)$ under any complex embedding is bounded by V^g.

Proof. First, we count the number of polynomials P_π satisfying Lemma 4.1, assuming that all of its roots have magnitude equal to $\sqrt{\mathrm{Nm}v}$, under any complex embedding. The first $g+1$ coefficients of P_π determine the rest, as the roots of P_π come in pairs multiplying to $\mathrm{Nm}v$. Thus, to find the total number of possible such polynomials, we can multiply together the number of possible values for the coefficient of z^{2g-i} in P_π for $0 \leqslant i \leqslant g$. Thus,

$$\begin{aligned} \prod_{0\leqslant i\leqslant g}\left(2\cdot\binom{2g}{i}\cdot\left(\sqrt{\mathrm{Nm}_{\mathbb{Q}}^K(x)}\right)^i\right) &= 2^{g+1}\cdot\left(\mathrm{Nm}_{\mathbb{Q}}^K(x)\right)^{\frac{g(g+1)}{4}}\cdot\prod_{0\leqslant i\leqslant 3}\binom{2g}{i}\cdot\prod_{4\leqslant i\leqslant g}\binom{2g}{i} \\ &\leqslant 2^{g+1}\cdot\left(\mathrm{Nm}_{\mathbb{Q}}^K(x)\right)^{\frac{g(g+1)}{4}}\cdot\prod_{0\leqslant i\leqslant 3}\binom{2g}{i}\cdot\left(2^{2g}\right)^{g-3} \\ &\leqslant \frac{c_{11}}{64^g}\cdot\left(256\cdot\mathrm{Nm}_{\mathbb{Q}}^K(x)\right)^{\frac{g(g+1)}{4}} \end{aligned}$$

for some effectively computable absolute constant c_{11}.

Any $\psi_{\mathbb{C}}(v)$ can be written as a product of distinct roots of such a polynomial, times a $c(g)$th root of unity, times a power of $\mathrm{Nm}_{\mathbb{Q}}^K v$ which is at most g. Therefore, the number

https://doi.org/10.1017/S1474748013000182 Published online by Cambridge University Press

of possible values of $\psi_{\mathbb{C}}(v)$ is at most the product of the number of possible polynomials calculated above and $2^{2g} \cdot c(g) \cdot (g+1) \leqslant c_1 \cdot 64^g$. This implies the desired statement. □

Fix a direct sum decomposition

$$\mathrm{Cl}(K) \simeq \mathbb{Z}/h'_K\mathbb{Z} \oplus H(K),$$

for a subgroup $H(K) \subset \mathrm{Cl}(K)$, and fix a generator α of $\mathbb{Z}/h'_K\mathbb{Z}$. By elementary group theory, the image of any homomorphism from $\mathrm{Cl}(K)$ to a cyclic group is generated by the image of an element in $\alpha + H(K)$. Choose prime ideals $\{v_1, v_2, \ldots, v_{h_K/h'_K}\}$ which are of degree 1, coprime to $c(g) \cdot h_K$, and represent each element of $\alpha + H(K)$; write $(v_i)^{h'_K} = (x_i)$.

To make Theorem 5.15 effective, note that if ψ is an associated character not satisfying the conclusion of Theorem 5.15, our proof shows that either θ^S is unbalanced, or there is an i such that Lemma 5.8 fails for v_i. Thus $B_{\mathrm{rat}}(K, g)$, which we define as the product of

$$\prod_{\text{balanced characters } \theta^S} \left(\prod_{i=1}^{h_K/h'_K} \prod_{\substack{\text{possible values of } \psi(\pi_{v_i}) \\ \psi(\pi_{v_i})^{c(g)\cdot h'_K} \neq \theta^S(x_i)^{c(g)/e}}} \left(\psi(\pi_{v_i})^{c(g)\cdot h'_K} - \theta^S(x_i)^{c(g)/e} \right) \right)$$

with all primes lying under one of the v_i or dividing Δ_K, is a rational integer with the property that we can take $S_{K,g}$ to consist of all primes dividing $B_{\mathrm{rat}}(K, g) \cdot B_{\mathrm{char}}(K, g)$.

Lemma 7.7. *We have*

$$B_{\mathrm{rat}}(K, g) \leqslant \left(2 \cdot V^{2g\cdot c(g)\cdot h'_K}\right)^{\sqrt{(2g\cdot c(g)+1)^{n_K}}\cdot (h_K/h'_K)\cdot B_{\mathrm{poss}}(K,g,V)} \cdot V^{h_K/h'_K} \cdot \Delta_K,$$

where V is the maximum norm of the v_i.

Proof. Under any complex embedding, Lemma 7.3 implies that

$$\begin{aligned} \left|\psi(\pi_{v_i})^{c(g)\cdot h'_K} - \theta^S(x_i)^{c(g)/e}\right| &\leqslant \left|\psi(\pi_{v_i})^{c(g)\cdot h'_K}\right| + \left|\theta^S(x_i)^{c(g)/e}\right| \\ &\leqslant 2 \cdot |\mathrm{Nm}_{\mathbb{Q}}^K v_i|^{2g\cdot c(g)\cdot h'_K} \\ &\leqslant 2 \cdot V^{2g\cdot c(g)\cdot h'_K} \end{aligned}$$

which completes the proof, using Lemma 7.6, together with the fact that there are at most $\sqrt{(2g \cdot c(g)+1)^{n_K}}$ balanced characters. (The factor of V^{h_K/h'_K} is there to account for the primes which lie under one of the v_i.) □

7.4. Proof of Theorem 7.9

In this subsection, we prove Theorem 7.9. While Theorem 5.16 is true unconditionally, assuming GRH allows us to get a significantly better bound.

Remark 7.8. Using an unconditional version of the Chebotarev Density Theorem (see Remark 6.2), one could make Theorem 7.9 unconditional by the same method. For $g = 1$,

https://doi.org/10.1017/S1474748013000182 Published online by Cambridge University Press

there is also an unconditional bound due to David; see Theorem 2 of [2]. (The logarithm of David's bound is roughly the n_Kth power of the logarithm of our conditional bound.)

Theorem 7.9. *Under GRH, there are effectively computable absolute constants c_2, c_3, and c_4 such that we can take in Theorems 6.4 and 5.16*

$$\prod_{\ell \in S_K} \ell \leqslant \exp\Big(c_2^{n_K} \cdot \Big(R_K \cdot n_K^{r_K} + h_K^2 \cdot (\log \Delta_K)^2\Big)\Big)$$

$$\prod_{\ell \in S_{K,g}} \ell \leqslant \exp\left(c_3^{n_K} \cdot \left(8^{g(n_K+1)} \cdot R_K \cdot n_K^{r_K} + 3^{g \cdot n_K} \cdot \big(c_4 \cdot g \cdot h_K \cdot n_K \cdot \log \Delta_K\big)^{\frac{g(g+1)}{2}+1}\right)\right).$$

Remark 7.10. In fact, we have proven (independently of GRH) that

$$\prod_{\ell \in S_{K,g}} \ell \leqslant B_{\mathrm{char}}(K,g) \cdot B_{\mathrm{rat}}(K,g).$$

Proof. Under GRH, Corollary 6.3 (applied to $N = c(g) \cdot h_K$) and $\log h_K \leqslant \frac{3}{2} \log \Delta_K$ (which follows from [8], Theorem 6.5) imply that we can choose the v_i such that

$$V = \max \operatorname*{Nm}_{\mathbb{Q}}^{K}(v_i) \leqslant c_7 \cdot \big(\log \Delta_{H_K} + n_{H_K} \log(c(g) \cdot h_K)\big)^2 \leqslant c_{12} \cdot g^2 \cdot h_K^2 \cdot n_K^2 \cdot (\log \Delta_K)^2$$

for some effectively computable absolute constant c_{12}.

We use the notation $f \lesssim g$ to mean that $f \leqslant C \cdot g$ for an effectively computable absolute constant C.

By Remark 7.10 above, it suffices to show that both $\log B_{\mathrm{char}}(K,g)$ and $\log B_{\mathrm{rat}}(K,g)$ are bounded by a constant times the logarithm of the right-hand side of the first inequality appearing in the statement of the theorem. First, we bound $B_{\mathrm{char}}(K,g)$, as follows:

$$\log B_{\mathrm{char}}(K,g) \lesssim \frac{R_K \cdot (r_K+2)! \cdot (2g \cdot c(g)+1)^{n_K+1} \cdot (\log n_K)^3}{|\log\log n_K|^3} \lesssim 8^{g(n_K+1)} \cdot R_K \cdot (c_3 n_K)^{r_K}$$

for some effectively computable absolute constant c_3. Next, we bound $B_{\mathrm{rat}}(K,g)$, using $\log h_K \leqslant \frac{3}{2} \log \Delta_K$:

$$\begin{aligned}\log B_{\mathrm{rat}}(K,g) &\lesssim g \cdot c(g) \cdot h_K' \cdot \sqrt{(2g \cdot c(g)+1)^{n_K}} \cdot (\log g + \log h_K + \log n_K + \log\log \Delta_K) \\ &\quad \cdot (h_K/h_K') \cdot \Big(256 \cdot c_{12} \cdot g^2 \cdot h_K^2 \cdot n_K^2 \cdot (\log \Delta_K)^2\Big)^{\frac{g(g+1)}{4}} \\ &\lesssim (c_{13} \cdot 3^g)^{n_K} \cdot \big(c_4 \cdot g \cdot h_K \cdot n_K \cdot \log \Delta_K\big)^{\frac{g(g+1)}{2}+1}\end{aligned}$$

for effectively computable absolute constants c_4 and c_{13}.

From the proof of Theorem 6.4, it suffices to show that the logarithm of the product of all primes ℓ for which

$$\ell \leqslant \Big(3^{12 n_K}+1\Big)^2 \quad \text{or} \quad \ell \leqslant \big(1 + 2\sqrt{c_7} \cdot (2\log \Delta_K + 2 n_K \log 3 + n_K \log \ell)\big)^8$$

is bounded by an absolute constant times the logarithm of the right-hand side of the second inequality appearing in the statement of the theorem. For the product of all

https://doi.org/10.1017/S1474748013000182 Published online by Cambridge University Press

primes satisfying the first of the above inequalities, this is clear from the prime number theorem.

For the second factor, note that the Brauer–Siegel Theorem (which is effective under GRH) implies that

$$c_2^{n_K} \cdot \left(R_K \cdot n_K^{r_K} + h_K^2 \cdot (\log \Delta_K)^4\right) \gtrsim h_K^2 + n_K^{n_K/2} \cdot R_K \gtrsim n_K^{n_K/3} \cdot (h_K R_K)^{2/3} \gtrsim \Delta_K^{1/4}.$$

Thus, it suffices to show that for $\ell \geqslant \sqrt[4]{\Delta_K}$ and more than an effectively computable absolute constant,

$$\ell \geqslant \left(1 + 2\sqrt{c_7} \cdot (2 \log \Delta_K + 2n_K \log 3 + n_K \log \ell)\right)^4.$$

But this is clear, since Minkowski's bound, together with the assumption that $\ell \geqslant \sqrt[4]{\Delta_K}$, implies that the right-hand side of the above inequality is at most an effectively computable absolute constant times $(\log \ell)^8$. This completes the proof. □

Acknowledgements. We would like to thank David Zureick-Brown, Bryden Cais and Ken Ono for giving us the problem that led to this paper and answering questions. We are grateful to Brian Conrad for writing Appendix. Thanks also to Brian Conrad, Jordan Ellenberg, Benedict Gross, Mark Kisin, Barry Mazur, Jean-Pierre Serre and Vadim Vologodsky for valuable comments and discussions. Finally we would like to express our admiration for Serre's paper [17] whose techniques provided the mathematical inspiration and departure point of our work.

Appendix. A determinantal comparison (by Brian Conrad)

A.1. Motivation

For a linear representation ρ of a group Γ on a finitely generated module $V = \prod V_i$ over a finite product $\prod F_i$ of fields F_i, we get a determinant $\det \rho : \Gamma \to \prod F_i^\times$ via the Γ-action on $\prod \det(V_i)$. (This is the usual $(\prod F_i)$-linear determinant when V is free as a $(\prod F_i)$-module.) The case of interest to us will be $\Gamma = G_K := \mathrm{Gal}(K_s/K)$ for a finite extension K of $\mathbb{Q}_p$ and the action of G_K on $V = \mathrm{V}_p(A)$ for an abelian variety A of dimension $g > 0$ over K.

Consider a commutative subfield $F \subseteq \mathrm{End}_K^0(A)$ (which could even be $\mathbb{Q}$, though that case will not be interesting), so for $F_p := \mathbb{Q}_p \otimes_{\mathbb{Q}} F$, there is a natural continuous F_p-linear representation $\rho_{A,p}$ of G_K on $\mathrm{V}_p(A)$. This yields a continuous determinant homomorphism $G_K^{\mathrm{ab}} \to F_p^\times$. Composing with the Artin map $r_K : K^\times \to G_K^{\mathrm{ab}}$, we get a composite map

$$\psi_A : K^\times \xrightarrow{r_K} G_K^{\mathrm{ab}} \xrightarrow{\det_{F_p} \rho_{A,p}} F_p^\times.$$

A natural question, inspired by the use of the reflex norm in the main theorem of complex multiplication, is to ask whether the restriction of ψ_A to an open subgroup of $\mathcal{O}_K^\times$ can be described in terms of the F-action on $\mathrm{Lie}(A)$. To be precise, $\mathrm{Lie}(A)$ is naturally a module over $K \otimes_{\mathbb{Q}} F = K \otimes_{\mathbb{Q}_p} F_p$, so K acts F_p-linearly on $\mathrm{Lie}(A)$ and hence we

https://doi.org/10.1017/S1474748013000182 Published online by Cambridge University Press

can take the F_p-linear determinant of (the inverse of) the $K^\times$-action on $\mathrm{Lie}(A)$:

$$\chi_A(a) = \det_{F_p}\big((x \mapsto a \cdot x) : \mathrm{Lie}(A) \to \mathrm{Lie}(A)\big).$$

It is natural to ask whether the homomorphisms $\psi_A, \chi_A : K^\times \rightrightarrows F_p^\times$ are equal on an open subgroup of $\mathcal{O}_K^\times$ when F is a totally real or CM field. The answer is affirmative without archimedean restrictions on F, and by using p-adic Hodge theory in the form due to Fontaine (see [3, 4]), which goes beyond what was used by Serre and Tate (who worked in the area before the discovery of B_{crys}), we can say a bit more:

Theorem A.1. *The two maps $K^\times \rightrightarrows F_p^\times$ coincide on an open subgroup of $\mathcal{O}_K^\times$. If A has semistable reduction then these maps agree on $\mathcal{O}_K^\times$.*

Example A.2. If A is a CM abelian variety with good reduction and F is a CM field with $[F : \mathbb{Q}] = 2g$ then this theorem recovers the inertial description of the reflex norm in the theory of complex multiplication when there is good reduction.

We will use Grothendieck's Orthogonality Theorem in the semistable case to reduce Theorem A.1 to a more general assertion about p-divisible groups over the valuation ring of a finite extension of K. The main point is to then recast this general assertion in terms of p-adic Hodge theory, since that admits a robust tensorial structure whereas p-divisible groups do not. In what follows, we will use the covariant Fontaine functors (i.e., $(B \otimes_{\mathbb{Q}_p} V)^{G_K}$ rather than $\mathrm{Hom}_{\mathbb{Q}_p[G_K]}(V, B)$).

A.2. Reformulation via p-divisible groups

To prove Theorem A.1, it is harmless to replace K with a finite extension so that A has semistable reduction. So we now assume this to be the case. Let $\mathcal{A}$ denote the semi-abelian relative identity component of the Néron model $N(A)$ over $\mathcal{O}_K$ (i.e., the open complement in $N(A)$ of the union of the non-identity components of the special fiber $N(A)_k$). The special fiber $\mathcal{A}_k$ is an extension of an abelian variety B by a torus T. We will use a filtration on $\mathrm{V}_p(A)$ arising from the filtration on $\mathcal{A}_k$ to reduce our problem to an intrinsic question about p-divisible groups over $\mathcal{O}_K$.

Now we recall Grothendieck's results on the structure of p-adic Tate modules of abelian varieties with semistable reduction over p-adic fields. (This is developed in [SGA 7, Exp. IX]; see [2, §§ 4–5] for an exposition, especially [2, Theorem 5.5].) Let $a = \dim B$ and $t = \dim T$. The 'finite parts' of the $\mathcal{A}[p^n]$ (according to the decomposition of the quasi-finite flat separated $\mathcal{O}_K$-groups $\mathcal{A}[p^n]$ via Zariski's Main Theorem) define a p-divisible group Γ over $\mathcal{O}_K$ of height $2a + t$ lifting $\mathcal{A}_k[p^\infty]$. This has generic fiber contained in $A[p^\infty]$, and it is final among p-divisible groups over $\mathcal{O}_K$ whose generic fiber is equipped with a map to $A[p^\infty]$. By Grothendieck's Orthogonality Theorem, the quotient $\mathrm{V}_p(A)/\mathrm{V}_p(\Gamma)$ is the Galois representation associated with the Cartier dual of the unique p-divisible group Γ'_{t} over $\mathcal{O}_K$ lifting the p-divisible group $T'[p^\infty]$ of the maximal torus T' in the special fiber of the Néron model of the dual abelian variety A'. Since Γ'_{t} has étale Cartier dual (as this holds for its special fiber $T'[p^\infty]$), it follows

https://doi.org/10.1017/S1474748013000182 Published online by Cambridge University Press

that $\mathrm{V}_p(A)/\mathrm{V}_p(\Gamma)$ is *unramified*. Hence, the inertial restriction of ψ_A is unaffected by replacing $\mathrm{V}_p(A)$ with $\mathrm{V}_p(\Gamma)$.

The Lie algebra of A is the generic fiber of $\mathrm{Lie}(\mathcal{A})$, and $\mathrm{Lie}(\mathcal{A})$ is naturally identified with the Lie algebra of the formal $\mathcal{O}_K$ group $\widehat{\mathcal{A}} = \mathrm{Spf}(\mathcal{O}^{\wedge}_{\mathcal{A},0})$ of $\mathcal{A}$ (completion along the identity section over $\mathcal{O}_K$). But $\widehat{\mathcal{A}}$ is the formal group over $\mathcal{O}_K$ corresponding to the connected part of the p-divisible group Γ under the Serre–Tate equivalence between connected p-divisible groups and commutative formal Lie groups on which $[p]$ is an isogeny (over any complete local noetherian ring with residue characteristic p). Hence, $\mathrm{Lie}(A) = \mathrm{Lie}(\Gamma)[1/p]$ functorially in the isogeny category over K. (Note that $\mathrm{Lie}(\Gamma)[1/p]$ is functorial with respect to K-homomorphisms in Γ, due to Tate's Isogeny Theorem for p-divisible groups over $\mathcal{O}_K$.) The F_p-action on $\mathrm{V}_p(\Gamma)$ arises from an F_p-action on Γ in the isogeny category over $\mathcal{O}_K$.

We conclude that our entire problem is intrinsic to the p-divisible group Γ over $\mathcal{O}_K$, in the sense that it involves relating the inertial action on $\det_{F_p}(\mathrm{V}_p(\Gamma))$ to the F_p-determinant of the $K^\times$-action on $\mathrm{Lie}(\Gamma)[1/p]$. In this way, our problem makes sense more generally for an arbitrary p-divisible group over $\mathcal{O}_K$ equipped with an action by F_p in the isogeny category over $\mathcal{O}_K$. Decomposing Γ (up to isogeny over $\mathcal{O}_K$) according to the idempotents of F_p, and renaming each factor field of F_p as F, thereby reduces Theorem A.1 to:

Theorem A.3. *Let K be a finite extension of $\mathbb{Q}_p$, Γ a p-divisible group over $\mathcal{O}_K$, and F a finite extension of $\mathbb{Q}_p$ equipped with an action on Γ in the isogeny category over $\mathcal{O}_K$.*

Let $\chi : K^\times \to F^\times$ be defined by the reciprocal of the F-linear determinant of the $K^\times$-action on $\mathrm{Lie}(\Gamma)[1/p]$, and let the composite map

$$\psi : K^\times \xrightarrow{r_K} G_K^{\mathrm{ab}} \longrightarrow F^\times$$

be defined by the F-linear determinant of the G_K-action on $\mathrm{V}_p(\Gamma)$. Then $\psi|_{\mathcal{O}_K^\times} = \chi|_{\mathcal{O}_K^\times}$.

A.3. Proof of Theorem A.3

In view of how χ is constructed from a $(K \otimes_{\mathbb{Q}_p} F)$-module, it arises from a homomorphism of $\mathbb{Q}_p$-tori $\mathrm{Res}^K_{\mathbb{Q}_p} \mathbb{G}_{m,K} \to \mathrm{Res}^F_{\mathbb{Q}_p} \mathbb{G}_{m,F}$. Thus, by [1, Proposition B.4(i)], $\chi|_{\mathcal{O}_K^\times}$ is the I_K-restriction of a crystalline representation $G_K^{\mathrm{ab}} \to F^\times$. Hence, if ψ and χ agree on an open subgroup of $\mathcal{O}_K^\times$ then their ratio on $\mathcal{O}_K^\times$ is the I_K-restriction of a crystalline representation that is finite on I_K. But a crystalline p-adic representation of G_K with finite image on I_K is unramified, so it would follow that χ and ψ coincide on $\mathcal{O}_K^\times$. In particular, if χ^e and ψ^e coincide on $\mathcal{O}_K^\times$ for some $e > 0$ (so χ and ψ agree on the open subgroup $(\mathcal{O}_K^\times)^e$) then we will be done.

It is harmless to replace Γ with an $\mathcal{O}_K$-isogenous p-divisible group, so we may and do assume that $\mathcal{O}_F$ acts on Γ (not just in the isogeny category). If F'/F is a finite extension then it is harmless to replace Γ with its power $\mathcal{O}_{F'} \otimes_{\mathcal{O}_F} \Gamma$ (defined in the evident manner), since at the determinant level we would be replacing χ and ψ with their $[F' : F]$th powers, which we have seen is harmless. Thus, we may and do arrange that F splits $K/\mathbb{Q}_p$.

https://doi.org/10.1017/S1474748013000182 Published online by Cambridge University Press

Let $\Gamma^\vee$ denote the dual of Γ, and consider the $\mathbb{C}_K$-linear G_K-equivariant canonical Hodge–Tate decomposition $\mathbb{C}_K \otimes_{\mathbb{Q}_p} V_p(\Gamma) \simeq (\mathbb{C}_K(1) \otimes_K t_\Gamma) \oplus (\mathbb{C}_K \otimes_K \mathrm{Hom}_K(t_{\Gamma^\vee}, K))$, where $t_\Gamma := \mathrm{Lie}(\Gamma)[1/p]$ (and similarly for $t_{\Gamma^\vee}$). For later purposes, it will be convenient to apply the follow elementary lemma to rewrite the second summand.

Lemma A.4. *Let K and F be finite separable extensions of a field k. For any finitely generated $(K \otimes_k F)$-module W, the $(K \otimes_k F)$-modules $\mathrm{Hom}_K(W, K)$ and $\mathrm{Hom}_F(W, F)$ are naturally isomorphic, where F acts K-linearly on $\mathrm{Hom}_K(W, K)$ through functoriality applied to its K-linear action on W and similarly for the F-linear K-action on $\mathrm{Hom}_F(W, F)$.*

Proof. It suffices to prove that the natural $(K \otimes_k F)$-linear map

$$\mathrm{Hom}_K(W, K) \to \mathrm{Hom}_k(W, k) \quad \text{defined via } \ell \mapsto \mathrm{Tr}_k^K \circ \ell$$

is an isomorphism, as then we can argue similarly with the roles of K and F swapped. This only involves the underlying K-vector space of W (ignoring the F-action), so we can reduce to the trivial case $W = K$. □

We now rewrite the Hodge–Tate decomposition in the form

$$\mathbb{C}_K \otimes_{\mathbb{Q}_p} V_p(\Gamma) \simeq (\mathbb{C}_K(1) \otimes_K t_\Gamma) \oplus (\mathbb{C}_K \otimes_K \mathrm{Hom}_F(t_{\Gamma^\vee}, F)), \tag{6}$$

where $\mathrm{Hom}_F(t_{\Gamma^\vee}, F)$ is a K-vector space through functoriality applied to the F-linear K-action on $t_{\Gamma^\vee}$. Since F splits $K/\mathbb{Q}_p$, any $(K \otimes_{\mathbb{Q}_p} F)$-module W (such as t_Γ and $t_{\Gamma^\vee}$) decomposes into F-subspaces

$$W = \oplus_\sigma W_\sigma$$

according to a $\mathbb{Q}_p$-embedding $\sigma : K \to F$ through which K acts. That is, for $w \in W_\sigma$ we have $(c \otimes 1)w = \sigma(c)w$ for $c \in K$. We can therefore compute the $(\mathbb{C}_K \otimes_{\mathbb{Q}_p} F)$-linear determinant on both sides of (6) by first collapsing the K-action into the F-structure by decomposing modules into isotypic subspaces according to $\mathbb{Q}_p$-embeddings $\sigma : K \to F$, then decomposing those subspaces into isotypic $\mathbb{C}_K$-subspaces according to the $\mathbb{Q}_p$-embedding $F \to \mathbb{C}_K$ through which F acts, and then finally forming the $\mathbb{C}_K$-determinant of each such subspace of the latter sort. Thus, the $(\mathbb{C}_K \otimes_{\mathbb{Q}_p} F)$-determinant of the left side of (6) is $\mathbb{C}_K \otimes_{\mathbb{Q}_p} \psi = \mathbb{C}_K \otimes_K (K \otimes_{\mathbb{Q}_p} \psi)$ and the $(\mathbb{C}_K \otimes_{\mathbb{Q}_p} F)$-determinant of the right side of (6) is

$$\bigoplus_{\sigma : K \to F} \mathbb{C}_K \otimes_{K,\sigma} \left(\det_F(t_{\Gamma,\sigma}(1)) \otimes_F \det_F(\mathrm{Hom}_F(t_{\Gamma^\vee}, F)_\sigma) \right) \tag{7}$$

as σ varies through the $\mathbb{Q}_p$-embeddings of K into F.

Let $\theta_\chi : G_K^{\mathrm{ab}} \to \mathcal{O}_F^\times$ correspond to a map extending $\chi|_{\mathcal{O}_K^\times}$ via r_K, so it suffices to prove that ψ and θ_χ coincide on an open subgroup of $\mathcal{O}_K^\times$. It is equivalent to say that the ratio of these $\mathcal{O}_F^\times$-valued Hodge–Tate characters has finite image on inertia, or in other words that their $\mathbb{C}_K$-scalar extensions (over $\mathbb{Q}_p$) are $(\mathbb{C}_K \otimes_{\mathbb{Q}_p} F)$-linearly and G_K-equivariantly isomorphic. In other words, it suffices to prove that $\mathbb{C}_K \otimes_{\mathbb{Q}_p} \theta_\chi$ is $(\mathbb{C}_K \otimes_{\mathbb{Q}_p} F)$-linearly

https://doi.org/10.1017/S1474748013000182 Published online by Cambridge University Press

and G_K-equivariantly isomorphic to (7). It is harmless to replace G_K-equivariance with H-equivariance for an open subgroup H, such as the Galois group of $\overline{K}$ over the Galois closure F' of $F/\mathbb{Q}_p$.

Our remaining task is to compute the Hodge–Tate weights of the $\mathbb{C}_K$-semilinear $G_{F'}$-representation $\mathbb{C}_K \otimes_{j,F} \theta_\chi$ for each $\mathbb{Q}_p$-embedding $j : F \to \mathbb{C}_K$. For any such j the image $j(F)$ contains K and so induces a $\mathbb{Q}_p$-embedding of K into F. Since we use covariant Fontaine functors, the Hodge–Tate weight of $\mathbb{Q}_p(n)$ is $-n$ ($B_{\mathrm{HT}}(n)$ has its G_K-invariants occurring in degree $-n$). It therefore suffices to prove that for each $\mathbb{Q}_p$-embedding $\sigma : K \to F$, the K-dimension of the σ-isotypic part of the $(K \otimes_{\mathbb{Q}_p} F)$-module $\mathrm{gr}^n(D_{\mathrm{dR}}(\theta_\chi))$ vanishes for $n \neq n_\sigma := -\dim_F t_{\Gamma,\sigma}$ and is $[F : K]$ for $n = n_\sigma$. This means precisely that the σ-isotypic part of $D_{\mathrm{dR}}(\theta_\chi)$ is one-dimensional over F with its unique nonzero gr^n occurring for $n = n_\sigma$.

Combining these assertions over all σ, our task is to prove that $D_{\mathrm{dR}}(\theta_\chi)$ free of rank 1 over $K \otimes_{\mathbb{Q}_p} F$ and the σ-isotypic part of $\mathrm{gr}^\bullet(D_{\mathrm{dR}}(\theta_\chi))$ is supported in degree $-\dim_F t_{\Gamma,\sigma}$. By [1, Proposition A.3], θ_χ is crystalline and $D_{\mathrm{crys}}(\theta_\chi)$ is invertible as a $(K_0 \otimes_{\mathbb{Q}_p} F)$-module. Extending scalars by $K_0 \to K$ yields $D_{\mathrm{dR}}(\theta_\chi)$, so the invertibility over $K \otimes_{\mathbb{Q}_p} F$ holds.

It remains to prove that the degree of the σ-isotypic F-line in $\mathrm{gr}^\bullet(D_{\mathrm{dR}}(\theta_\chi))$ is equal to $-\dim_F t_{\Gamma,\sigma}$ for each $\sigma : K \to F$. Recall that by definition, $\chi : K^\times \to F^\times$ encodes the K-action on the F-line

$$\det_F(t_\Gamma)^{-1} = \bigotimes_{\sigma : K \to F} \det_F(t_{\Gamma,\sigma})^{-1}.$$

In other words, for any $c \in K^\times$, $\chi(c) = \prod_\sigma \sigma(c)^{n_\sigma}$ as a product of $F^\times$-valued characters, i.e. $\theta_\chi = \otimes_\sigma \theta_\sigma^{\otimes n_\sigma}$ where (i) $\theta_\sigma : G_K^{\mathrm{ab}} \to \mathcal{O}_F^\times$ extends $r_K(u) \mapsto \sigma(u)$ for $u \in \mathcal{O}_K^\times$, and (ii) the tensor product is formed as one-dimensional F-linear representations. Since we are using covariant Fontaine functors, $D_{\mathrm{dR}}(\theta_\chi) \simeq \otimes_\sigma D_{\mathrm{dR}}(\theta_\sigma)^{\otimes n_\sigma}$ where the tensor product is formed over $K \otimes_{\mathbb{Q}_p} F$ and the definition of the F-linear K-action on the σ-factor is via $\sigma : K \to F$.

By Serre [5, Appendix III, A.4], the representation θ_σ^{-1} corresponds to the scalar extension along σ of a Lubin–Tate group G_π over $\mathcal{O}_K$ arising from a uniformizer π of K. The associated filtered K-vector space $D_{\mathrm{dR}}(\mathrm{V}_p(G_\pi))$ has gr^{-1} of dimension 1 and gr^0 of dimension $[K : \mathbb{Q}_p] - 1$ (since G_π is a one-dimensional p-divisible group of height $[K : \mathbb{Q}_p]$ over $\mathcal{O}_K$, and $\mathbb{C}_K \otimes D_{\mathrm{dR}} = D_{\mathrm{HT}}$).

Using the G_K-equivariant K-linear structure on $\mathrm{V}_p(G_\pi)$, view $D_{\mathrm{dR}}(\mathrm{V}_p(G_\pi))$ as a filtered $(K \otimes_{\mathbb{Q}_p} K)$-module with the left tensor factor encoding the K-linear structure on D_{dR} (arising from B_{dR}) and the right tensor factor encoding the K-action arising from $\mathrm{V}_p(G_\pi)$.

Lemma A.5. *As a $(K \otimes_{\mathbb{Q}_p} K)$-module, $D_{\mathrm{dR}}(\mathrm{V}_p(G_\pi))$ is free of rank* 1.

Proof. The comparison isomorphism $B_{\mathrm{dR}} \otimes_K D_{\mathrm{dR}}(\mathrm{V}_p(G_\pi)) \simeq B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} \mathrm{V}_p(G_\pi)$ has a target that is visibly faithful over $K \otimes_{\mathbb{Q}_p} K$. Hence, $D_{\mathrm{dR}}(\mathrm{V}_p(G_\pi))$ is a faithful

https://doi.org/10.1017/S1474748013000182 Published online by Cambridge University Press

$(K\otimes_{\mathbb{Q}_p}K)$-module, so for K-dimension reasons (for the left tensor structure) it is free of rank 1. □

Using the K-structure for the right tensor factor, $D_{\mathrm{dR}}(\theta_\sigma^{-1}) = D_{\mathrm{dR}}(\mathrm{V}_p(G_\pi))\otimes_{K,\sigma}F$. Thus, by the lemma, $D_{\mathrm{dR}}(\theta_\sigma)$ is an invertible $(K\otimes_{\mathbb{Q}_p}F)$-module equipped with a linear filtration whose associated graded module is supported in degrees 1 and 0 with the term in degree 1 equal to the σ-isotypic F-line and the term in degree 0 equal to the span of the isotypic F-lines for the other $\mathbb{Q}_p$-embeddings of K into F. In particular, the $(K\otimes_{\mathbb{Q}_p}F)$-linear structure canonically splits the filtration (via the decomposition into isotypic F-lines for the K-action), so we may and do view $D_{\mathrm{dR}}(\theta_\sigma)$ as a graded $(K\otimes_{\mathbb{Q}_p}F)$-module (equipped with the associated tautologous filtration). Hence, $D_{\mathrm{dR}}(\theta_\sigma)^{\otimes n_\sigma}$ is an invertible $(K\otimes_{\mathbb{Q}_p}F)$-line equipped with a linear grading such that the σ-isotypic F-line is in degree n_σ and whose other isotypic F-lines are in degree 0 (since the factor rings of $K\otimes_{\mathbb{Q}_p}F$ are pairwise orthogonal).

Finally, the $(K\otimes_{\mathbb{Q}_p}F)$-linear tensor product over all σ gives that $D_{\mathrm{dR}}(\theta_\chi)$ is an invertible $(K\otimes_{\mathbb{Q}_p}F)$-module equipped with a linear grading such that its σ-isotypic F-line is the tensor product of the σ-isotypic F-line in $D_{\mathrm{dR}}(\theta_\sigma)^{\otimes n_\sigma}$ (which occurs in degree n_σ) and the σ-isotypic F-lines in the $D_{\mathrm{dR}}(\theta_\tau)^{\otimes n_\tau}$ for $\tau\neq\sigma$ (which all occur in degree 0). To summarize, for every σ the σ-isotypic F-line in $\mathrm{gr}^\bullet(D_{\mathrm{dR}}(\theta_\chi))$ occurs in degree $n_\sigma = -\dim_F t_{\Gamma,\sigma}$, as desired.

References

1. B. Conrad, Lifting global representations with local properties, 2010 preprint available at the webpage http://math.stanford.edu/∼conrad/papers/locchar.pdf.
2. B. Conrad, Semistable reduction for abelian varieties, Seminar Lecture Notes available at the webpage http://math.stanford.edu/∼akshay/ntslearn.html.
3. J.-M. Fontaine, Le corps des périodes p-adiques, *Périodes p-adiques*, *Astérisque* **223** (1994), 59–111.
4. J.-M. Fontaine, Représentations p-adiques semi-stables, *Périodes p-adiques*, *Astérisque* **223** (1994), 113–184.
5. J.-P. Serre, *Abelian ℓ-adic representations and elliptic curves*, 2nd ed. (A.K. Peters, 1998).

References

1. E. Bach and J. Sorenson, Explicit bounds for primes in residue classes, *Math. Comp.* **65**(216) (1996), 1717–1735.
2. A. David, Caractère d'isogénie et critères d'irréductibilité, Preprint available online at http://arxiv.org/abs/1103.3892.
3. P. Deligne, Travaux de Shimura, in *Séminaire Bourbaki, 23ème année (1970/71), Exp. No. 389*, Lecture Notes in Math., Volume 244, pp. 123–165 (Springer, Berlin, 1971).
4. G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, *Invent. Math.* **73**(3) (1983), 349–366.
5. E. Friedman, Analytic formulas for the regulator of a number field, *Invent. Math.* **98**(3) (1989), 599–622.
6. A. Grothendieck, Modèles de Néron et monodromie. In *Séminaire de Géométrie Algébrique, Volume 7, Exposé 9.*

https://doi.org/10.1017/S1474748013000182 Published online by Cambridge University Press

7. J. C. Lagarias and A. M. Odlyzko, Effective versions of the Chebotarev density theorem, in *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pp. 409–464 (Academic Press, London, 1977).
8. H. W. Lenstra Jr., Algorithms in algebraic number theory, *Bull. Amer. Math. Soc. (N.S.)* **26**(2) (1992), 211–244.
9. B. Mazur, Rational isogenies of prime degree (with an appendix by D. Goldfeld), *Invent. Math.* **44**(2) (1978), 129–162.
10. L. Merel, Bornes pour la torsion des courbes elliptiques sur les corps de nombres, *Invent. Math.* **124**(1–3) (1996), 437–449.
11. J. S. Milne, Abelian varieties defined over their fields of moduli. I, *Bull. Lond. Math. Soc.* **4** (1972), 370–372.
12. J. S. Milne, Complex multiplication (v0.00), 2006. Available at www.jmilne.org/math/.
13. F. Momose, Isogenies of prime degree over number fields, *Compositio Math.* **97**(3) (1995), 329–348.
14. M. Raynaud, Schémas en groupes de type $(p, \dots, p)$, *Bull. Soc. Math. France* **102** (1974), 241–280.
15. J. Rizov, Fields of definition of rational points on varieties. 2005. Available at http://arxiv.org/abs/math/0505364.
16. J.-P. Serre, *Abelian l-adic representations and elliptic curves*, McGill University Lecture Notes Written with the Collaboration of Willem Kuyk and John Labute (W. A. Benjamin, Inc., New York, Amsterdam, 1968).
17. J.-P. Serre, Propriétés Galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15**(4) (1972), 259–331.
18. J.-P. Serre, Quelques applications du théorème de densité de Chebotarev, *Publ. Math. Inst. Hautes Études Sci.*(54) (1981), 323–401.
19. G. Shimura, Algebraic number fields and symplectic discontinuous groups, *Ann. of Math. (2)* **86** (1967), 503–592.
20. P. Voutier, An effective lower bound for the height of algebraic numbers, *Acta Arith.* **74**(1) (1996), 81–95.