

Available online at www.sciencedirect.com

SCIENCE @ DIRECT®

Journal of Algebra 281 (2004) 124–143

JOURNAL OF
Algebrawww.elsevier.com/locate/jalgebra

The arithmetic of QM-abelian surfaces through their Galois representations [☆]

Luis V. Dieulefait ^a, Victor Rotger ^{b,*}^a Centre de Recerca Matemàtica, Apartat 50, E-08193 Bellaterra, Spain^b Escola Universitària Politècnica de Vilanova i la Geltrú, Av. Víctor Balaguer s/n,
E-08800 Vilanova i la Geltrú, Spain

Received 4 April 2003

Available online 2 September 2004

Communicated by Michel Broué

Abstract

This note provides an insight to the diophantine properties of abelian surfaces with quaternionic multiplication over number fields. We study the fields of definition of the endomorphisms on these abelian varieties and the images of the Galois representations on their Tate modules. We illustrate our results with an explicit example.

© 2004 Elsevier Inc. All rights reserved.

Keywords: Abelian varieties; Galois representations; Quaternions

1. Abelian surfaces with quaternionic multiplication

Fix $\overline{\mathbb{Q}}$ an algebraic closure of the field \mathbb{Q} of rational numbers and let $K \subset \overline{\mathbb{Q}}$ be a number field. Let A be an abelian surface defined over K . Due to Albert's classification of

[☆] Supported by European Research Networks at the Université de Paris 13 and the Institut de Mathématiques de Jussieu and by a MECD postdoctoral grant at the Centre de Recerca Matemàtica from Ministerio de Educación y Cultura. Partially supported by DGICYT Grant BFM2003-06768-C02-02.

* Corresponding author.

E-mail addresses: ldieulefait@crm.es (L.V. Dieulefait), vrotger@mat.upc.es (V. Rotger).

involving division algebras (cf. [11]), there is a limited number of possible structures for the algebra of endomorphisms $\text{End}_{\overline{\mathbb{Q}}}(A) \otimes \mathbb{Q}$ of A .

We focus our attention on the quaternionic case. While the existing literature concerning the theme mainly restrict to abelian surfaces with multiplication by a maximal order in a division quaternion algebra, in this note we consider quaternionic multiplication in a wider sense: we shall assume that $\text{End}_{\overline{\mathbb{Q}}}(A) \otimes \mathbb{Q}$ is an arbitrary indefinite quaternion algebra B over \mathbb{Q} , including the split case $B = M_2(\mathbb{Q})$, which is recurrently encountered in the modular setting. This allows the abelian surface to be isogenous to the product of two isogenous elliptic curves without CM.

Moreover, we will let $\mathcal{O} = \text{End}_{\overline{\mathbb{Q}}}(A)$ be an arbitrary order in B , although our main results restrict to so called hereditary orders. We need to be careful on the exact order $\text{End}_{\overline{\mathbb{Q}}}(A) \subset B$ of endomorphisms of A since we are interested on properties of A that heavily depend on its isomorphism class and badly behave up to isogeny.

Let then $B = \left(\frac{a,b}{\mathbb{Q}}\right) = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij$, $ij = -ji$, $i^2 = a$, $j^2 = b$ with $a, b \in \mathbb{Q}^*$, be a quaternion algebra and let $\text{tr} : B \rightarrow \mathbb{Q}$ and $\text{n} : B \rightarrow \mathbb{Q}$, denote the reduced trace and norm, respectively. The algebra B is said to be indefinite if the archimedean place of \mathbb{Q} is unramified: $B \otimes \mathbb{R} \simeq M_2(\mathbb{R})$. Equivalently, B is indefinite if either $a > 0$ or $b > 0$.

An order \mathcal{O} in B is a subring of rank 4 over \mathbb{Z} . It is called a *maximal* order if \mathcal{O} is not properly contained in any other and it is an *Eichler* order if $\mathcal{O} = \mathcal{O}_1 \cap \mathcal{O}_2$ is the intersection of two maximal orders $\mathcal{O}_1, \mathcal{O}_2$ in B . An order \mathcal{O} is *hereditary* if all its one-sided modules are projective.

The (reduced) discriminant of an order is $\text{disc}(\mathcal{O}) = |\det(\text{tr}(\beta_i \bar{\beta}_j))|^{1/2}$ for any \mathbb{Z} -basis $\{\beta_1, \beta_2, \beta_3, \beta_4\}$ of \mathcal{O} . The discriminant of a maximal order is square-free and, since only depends on B , it is simply denoted $\text{disc}(B)$. We have that $p \mid \text{disc}(B)$ if and only if $B_p = B \otimes \mathbb{Q}_p$ is a division algebra over \mathbb{Q}_p . If \mathcal{O} is an Eichler order, then $\text{disc}(\mathcal{O}) = \text{disc}(B) \cdot N$ for some $N > 0$ coprime to $\text{disc}(B)$; N is called the level of \mathcal{O} . Hereditary orders are exactly the orders in B of square-free discriminant. It can be shown that an order $\mathcal{O} \subset B$ is hereditary if and only if it is an Eichler order of square-free level.

Under the indefiniteness assumption, all one-sided ideals of an hereditary order are principal. Moreover, two hereditary orders $\mathcal{O}, \mathcal{O}'$ in B are isomorphic if and only if $\text{disc}(\mathcal{O}) = \text{disc}(\mathcal{O}')$. We refer the reader to [1,9,14,26] for more details on quaternion algebras and orders.

Definition 1.1. Let \mathcal{O} be an order in an indefinite quaternion algebra B over \mathbb{Q} . An abelian surface has quaternionic multiplication by \mathcal{O} if there is an isomorphism $\iota : \mathcal{O} \xrightarrow{\sim} \text{End}_{\overline{\mathbb{Q}}}(A)$. A field of definition for the pair (A, ι) is an extension L/K such that $\iota : \mathcal{O} \xrightarrow{\sim} \text{End}_L(A)$.

It is one of the aims of this paper to study

- (1) The field extension L/K given by the field of definition L of the quaternionic multiplication on an abelian surface A/K .
- (2) The filtration of intermediate endomorphism algebras $\text{End}_E(A) \otimes \mathbb{Q} \subseteq B$ for $K \subseteq E \subseteq L$.

The first question was studied in greater generality by Silverberg in [25] and Ribet in [16]. When particularized to our situation we obtain the first interesting result on this direction.

Proposition 1.2 [16,25]. *Let A/K be an abelian variety over a number field K and let $\mathcal{O} \subseteq \text{End}_{\overline{\mathbb{Q}}}(A)$ be a subring of endomorphisms of A . Then there is a unique minimal extension L/K such that $\mathcal{O} \subseteq \text{End}_L(A)$.*

The extension L/K is normal and non-ramified at the prime ideals of K of good or semistable reduction of A .

With respect to Proposition 1.2, let us remark that, if $\text{End}_{\overline{\mathbb{Q}}}(A)$ is an order in a division quaternion algebra, then A/K has potential good reduction and therefore no places of K of bad reduction of A are semistable. This is a consequence of Grothendieck's potential good reduction theorem.

Further, Silverberg gave an upper bound for the degree $[L : K]$ in terms of certain combinatorial numbers. In the particular case of abelian surfaces with quaternionic multiplication, [25, Proposition 4.3] predicts that $[L : K] \leq 48$. As our results will show, these bounds are not sharp (see Proposition 2.1 for arbitrary orders \mathcal{O} and Theorem 3.4 for hereditary orders).

Concerning the second question, the non-trivial sub-algebras of B over \mathbb{Q} are the quadratic fields $\mathbb{Q}(\sqrt{d})$ for $d \in \mathbb{Z}$ such that any prime number $p \mid D$ does not split in $\mathbb{Q}(\sqrt{d})$. Although there are infinitely many choices of them, main Theorem 3.4 shows that, under the assumption on \mathcal{O} to be hereditary, there are very restrictive conditions for $\mathbb{Q}(\sqrt{d})$ to be realized as the algebra of endomorphisms of A over K .

Below, for any positive integer N , we write $M_0(N) = \left\{ \begin{pmatrix} a & b \\ cN & d \end{pmatrix} : a, b, c, d \in \mathbb{Z} \right\}$ for the matrix Eichler order of level N . When particularized to the Jacobian variety of a curve C/K of genus 2, Theorem 3.4 asserts the following.

Theorem 1.3. *Let C/K be a curve of genus 2 defined over a number field K and let $J(C)$ be its Jacobian variety.*

- (I) (Simple case) *Assume that $J(C)$ is absolutely simple and that $\text{End}_{\overline{\mathbb{Q}}}(J(C)) = \mathcal{O}$ is an hereditary order of discriminant $D = \text{disc}(\mathcal{O})$ in a quaternion algebra B . Let L/K be the minimal extension of K over which all endomorphisms of $J(C)$ are defined. Then*
- (1) *L/K is an abelian extension with $G = \text{Gal}(L/K) \simeq (1), C_2$ or $D_2 = C_2 \times C_2$, where C_2 denotes the cyclic group of order two.*
 - (2) *If $B \not\cong \left(\frac{-D, m}{\mathbb{Q}} \right)$ for any $m \mid D$, then L/K is at most a quadratic extension of K . In this case, $\text{End}_K(A) \simeq \mathbb{Q}(\sqrt{-D})$.*
 - (3) *If $B = \left(\frac{-D, m}{\mathbb{Q}} \right)$ for some $m \mid D$, then $\text{End}_K(A)$ is isomorphic to either \mathcal{O} , an order in $\mathbb{Q}(\sqrt{-D})$, $\mathbb{Q}(\sqrt{m})$, or $\mathbb{Q}(\sqrt{D/m})$, or \mathbb{Z} . In each case, we respectively have $\text{Gal}(L/K) \simeq (1), C_2$ and D_2 .*
- (II) (Split case) *Assume that there is an isomorphism $\psi_{/\overline{\mathbb{Q}}} : J(C) \xrightarrow{\sim} E_1 \times E_2$ of $J(C)$ onto the product of two isogenous elliptic curves E_1, E_2 without CM over $\overline{\mathbb{Q}}$. Let $\varphi :$*

$E_1 \rightarrow E_2$ be an isogeny of minimal degree between them and assume that $N = \deg(\varphi)$ is square-free. Let $L = \mathbb{Q}(\varphi, \psi)$ be the compositum of the minimal fields of definition of φ and ψ . Then, there are the following possibilities for $G = \text{Gal}(L/K)$ and $\text{End}_K(A)$:

- (1) G is trivial and $\text{End}_K(A) = M_0(N)$.
- (2) $G = C_2$ and $\text{End}_K^0(A) = \mathbb{Q}(\sqrt{-N})$, $\mathbb{Q} \times \mathbb{Q}$ or $\mathbb{Q}(\sqrt{m})$ for $m > 1$, $m \mid N$, such that $M_2(\mathbb{Q}) = (\frac{-N, m}{\mathbb{Q}})$.
- (3) $G = C_4$ and $\text{End}_K^0(A) = \mathbb{Q}(\sqrt{-1})$.
- (4) $G = D_2$ or D_4 and $\text{End}_K^0(A) = \mathbb{Q}$.

A third aspect that we will regard concerning the arithmetic of abelian surfaces with QM stems from the following result obtained independently by M. Jacobson and M. Ohta.

Theorem 1.4 [8,12]. *Let A/K be an abelian surface with quaternionic multiplication by a maximal order \mathcal{O} in a division quaternion algebra over an extension L of K . Let $\{\sigma_\ell\}$ be the compatible family of Galois representations given by the action of $\text{Gal}(\overline{\mathbb{Q}}/K)$ on the Tate modules $T_\ell(A)$ of A and let $H = \text{Gal}(\overline{\mathbb{Q}}/L)$. Then $\sigma_\ell|_H = \rho_\ell \oplus \rho_\ell$ with*

$$\rho_\ell : H \rightarrow \text{Aut}_{\mathcal{O}}(T_\ell(A)) \simeq \mathcal{O}_\ell^*$$

and ρ_ℓ is surjective for almost every prime.

We will obtain an explicit description of the action of the absolute Galois group $G_K = \text{Gal}(\overline{\mathbb{Q}}/K)$ on the Tate modules of abelian surfaces A with quaternionic multiplication. This allows us to characterize the three possibilities for $\text{Gal}(L/K)$ described in Theorem 1.3(I), and we show how to effectively determine the field extension L/K . Moreover, we explain how to explicitly bound the finite set of *exceptional primes*, those where the surjectivity conclusion in Jacobson–Ohta’s theorem fails, and illustrate it in a concrete example with $\text{Gal}(L/K) = C_2$. For all non-exceptional primes, we also describe the image of the Galois representation σ_ℓ in $GL_4(\mathbb{Z}_\ell)$.

The paper is organized as follows. We devote next two sections to study the action of G_K on the ring of endomorphisms $\text{End}_{\overline{\mathbb{Q}}}(A)$ and the Néron–Severi $\text{NS}(A_{\overline{\mathbb{Q}}})$ group of A , respectively. The combination of the description of both Galois representations eventually yields the proof of our main Theorem 3.4 and, as an immediate consequence, proves Theorem 1.3.

In Section 4 we study the action of Galois on the Tate modules in the case that L/K is a quadratic extension. Under this assumption, we show that the Galois representations behave as in the case of a modular form with (a single) inner twist (cf. [17]). Following the results of Ribet, we provide sufficient conditions on a prime ℓ for the image of Galois $\rho_\ell(G_L)$ to be as large as possible.

In Section 5, we consider a concrete example of a Jacobian surface of a curve $C/\mathbb{Q}(\sqrt{-3})$ of genus 2 with maximal quaternionic multiplication borrowed from [7]. Firstly, we describe the image of the inertia subgroup at ℓ for the residual mod ℓ Galois representations and then, we give a result (Lemma 5.2) to distinguish the cases $\text{Gal}(L/K) = C_2$ and $\text{Gal}(L/K) = D_2$ of Theorem 1.3(I). By these means, we show that,

in our example, L/K is a quadratic extension and explicitly determine the field L . Then, we proceed to the determination, by successive elimination of some special cases, of the images of Galois, following the ideas of [17]. The main difference with the techniques used in [17] (described algorithmically in [6]) is that we are dealing with representations of the Galois group of a number field $K \neq \mathbb{Q}$.

2. The action of $\text{Gal}(\overline{\mathbb{Q}}/K)$ on the endomorphism ring

In this section we use Chinburg–Friedman’s recent classification of the finite subgroups of maximal arithmetic Kleinian groups [3] to describe the field of definition of the quaternionic multiplication on an (unpolarized) abelian surface.

Let A/K be an abelian surface over a number field K with quaternionic multiplication by an order \mathcal{O} in an indefinite quaternion algebra B over \mathbb{Q} .

The absolute Galois group $G_K = \text{Gal}(\overline{\mathbb{Q}}/K)$ of K acts in a natural way on the full ring of endomorphisms $\text{End}_{\overline{\mathbb{Q}}}(A) = \mathcal{O}$ of A that we already identify with \mathcal{O} and induces a Galois representation

$$\gamma : G_K \longrightarrow \text{Aut}(\mathcal{O}).$$

The Skolem–Noether theorem [26] asserts that all automorphisms of a quaternion algebra are inner. Therefore $\text{Aut}(B) \simeq B^*/\mathbb{Q}^*$ and the group of automorphisms of \mathcal{O} is $N_{B^*}(\mathcal{O})/\mathbb{Q}^*$ where $N_{B^*}(\mathcal{O}) = \{\gamma \in B^*, \gamma^{-1}\mathcal{O}\gamma\}$ is the normalizer group of \mathcal{O} . For $\tau \in G_K$ we will denote $[\gamma_\tau] : B \rightarrow B$ the automorphism of B such that $\beta^\tau = \gamma_\tau^{-1}\beta\gamma_\tau$ for any $\beta \in \text{End}_{\overline{\mathbb{Q}}}(A) = \mathcal{O}$.

If we let L/K be the minimal (and hence normal by Proposition 1.2) field extension of K such that $\text{End}_{\overline{\mathbb{Q}}}(A) = \text{End}_L(A) = \mathcal{O}$, we obtain an exact sequence of groups

$$1 \rightarrow G_L \rightarrow G_K \rightarrow N_{B^*}(\mathcal{O})/\mathbb{Q}^*$$

and thus a monomorphism $\text{Gal}(L/K) \hookrightarrow N_{B^*}(\mathcal{O})/\mathbb{Q}^*$.

Proposition 2.1. *Let A/K be an abelian surface with quaternionic multiplication by an order \mathcal{O} , $D = \text{disc}(\mathcal{O})$, and let L/K be the minimal extension of K over which all endomorphisms of A are defined. Then L/K is either cyclic or dihedral with $\text{Gal}(L/K) \simeq C_n$ or D_n , $n = 1, 2, 3, 4$, or 6 .*

- (1) If $\text{Gal}(L/K) \simeq D_2$, then $B = \left(\frac{d,m}{\mathbb{Q}}\right)$ for some $d, m \in \mathbb{Z}$, $d, m \mid D$.
- (2) If $\text{Gal}(L/K) \simeq C_3$, then any ramified prime $p \mid D$, $p \neq 2, 3$, satisfies $p \equiv -1 \pmod{3}$; if $\text{Gal}(L/K) \simeq D_3$, then in addition $B = \left(\frac{-3,m}{\mathbb{Q}}\right)$ with $m \mid D$.
- (3) If $\text{Gal}(L/K) \simeq C_4$, then $2 \mid D$ and any odd ramified prime $p \mid D$ satisfies $p \equiv -1 \pmod{4}$; if $\text{Gal}(L/K) \simeq D_4$, then in addition $B = \left(\frac{-1,m}{\mathbb{Q}}\right)$ with $m \mid D$.
- (4) If $\text{Gal}(L/K) \simeq C_6$, then $3 \mid D$ and any $p \mid D$, $p \neq 2, 3$, satisfies $p \equiv -1 \pmod{3}$; if $\text{Gal}(L/K) \simeq D_6$, then in addition $B = \left(\frac{-3,m}{\mathbb{Q}}\right)$ with $m \mid D$.

Proof. As we already observed, $\text{Gal}(L/K)$ is a finite subgroup of $N_{B^*}(\mathcal{O})/\mathbb{Q}^*$. Let us firstly note that, if $\gamma \in B^*$ normalizes the order \mathcal{O} , then $n(\gamma) \in \mathbb{Q}^*$ has odd p -adic valuation at any non-ramified prime number $p \nmid D$. This holds because $N_{GL_2(\mathbb{Q}_p)}(M_2(\mathbb{Z}_p)) = \mathbb{Q}_p^* GL_2(\mathbb{Z}_p)$.

In [3, §2], Chinburg and Friedman proved that the only possible finite subgroups of B^*/\mathbb{Q}^* are the cyclic groups C_n , the dihedral groups D_n and S_4 , A_4 , and A_5 .

By [3, Lemma 2.8], a necessary condition for B^*/\mathbb{Q}^* to contain either S_4 , A_4 , or A_5 is that $B = \begin{pmatrix} -1 & -1 \\ & 1 \end{pmatrix}$ and this can not be the case because B is indefinite.

Lemma 2.1 in [3] yields that B^*/\mathbb{Q}^* contains a cyclic group of order $n > 2$ if and only if there exists $\zeta_n \in B^*$ satisfying $\zeta_n^n = 1$, $\zeta_n^{n/d} \neq 1$ for any proper divisor d of n . In this case, any subgroup $C_n \subseteq B^*/\mathbb{Q}^*$ is conjugated to $\langle [1 + \zeta_n] \rangle$. In our case, $\zeta_n \in B^*$ generates a quadratic field extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ and this is only possible for $n = 3, 4$, and 6 . In addition, since $n(1 + \zeta_n) = 1, 2$, and 3 respectively, the condition $1 + \zeta_n \in N_{B^*}(\mathcal{O})$ implies that $2 \mid D$ for $n = 4$ and $3 \mid D$ for $n = 6$.

It follows from [3, Lemma 2.2] that the conjugacy classes of subgroups of $N_{B^*}(\mathcal{O})/\mathbb{Q}^*$ of order two are in bijection with the set of divisors $m \mid D$ of D , $m \neq 1$, such that p does not split in $\mathbb{Q}(\sqrt{m})$ for any prime $p \mid D$, together with $m = 1$ if $B \simeq M_2(\mathbb{Q})$. This set is always non-trivial because at least $\pm D$ satisfy these conditions.

Finally, Chinburg and Friedman proved that B^*/\mathbb{Q}^* contains a dihedral subgroup D_n , $n \geq 2$, if and only if it contains a cyclic group C_n [3, Lemma 2.3]. If $n = 2$, any subgroup of B^*/\mathbb{Q}^* isomorphic to $D_2 = C_2 \times C_2$ is of the form $\langle [x], [y] \rangle \subset B^*/\mathbb{Q}^*$ with $x, y \in B^*$, $x^2 = d$, $y^2 = m$, $xy = -yx$ for some $d, m \in \mathbb{Q}^*$. It follows that $N_{B^*}(\mathcal{O})/\mathbb{Q}^*$ contains a dihedral group D_2 if and only if $B = \begin{pmatrix} d & m \\ & 1 \end{pmatrix}$ for some $d, m \in \mathbb{Z}$, $d, m \mid D$. Similarly, if $n = 3, 4$, or 6 , $N_{B^*}(\mathcal{O})/\mathbb{Q}^*$ contains a dihedral subgroup D_n if and only if $B = \begin{pmatrix} d & m \\ & 1 \end{pmatrix}$ with $d = -1$ if $n = 4$, $d = -3$ if $n = 3$ or 6 and $m \in \mathbb{Z}$, $m \mid D$. In this case $D_n = \langle [1 + \zeta_n], [y] \rangle \subset B^*/\mathbb{Q}^*$ for some $y \in B^*$, $y^2 = m$. \square

3. The action of $\text{Gal}(\overline{\mathbb{Q}}/K)$ on the Néron–Severi group

Let A be an abelian variety defined over a number field K . For any field extension L/K , we let $A_L = A \times_K L$ denote the same abelian variety A with the base extended to $\text{Spec } L$. Let $\text{Div}(A)$ denote the group of Weil divisors of A and let $\text{Pic}(A)$ denote the group of invertible sheaves on A over K .

Let $\text{Pic}^0(A_{\overline{\mathbb{Q}}})$ denote the subgroup of $\text{Pic}(A_{\overline{\mathbb{Q}}})$ of invertible sheaves algebraically equivalent to 0 and let $\text{Pic}^0(A) = \text{Pic}(A) \cap \text{Pic}^0(A_{\overline{\mathbb{Q}}})$. The Néron–Severi group $\text{NS}(A)$ of A is $\text{NS}(A) = \text{Pic}(A)/\text{Pic}^0(A)$. The algebraic class of an invertible sheaf \mathcal{L} lies in $H^0(\text{NS}(A_{\overline{\mathbb{Q}}})) = H^0(\text{Gal}(\overline{\mathbb{Q}}/K), \text{NS}(A_{\overline{\mathbb{Q}}}))$ if and only if all its Galois conjugates \mathcal{L}^τ , $\tau \in \text{Gal}(\overline{\mathbb{Q}}/K)$, are algebraically equivalent to \mathcal{L} . We define the Picard number of A_K to be $\rho(A_K) = \text{rank}_{\mathbb{Z}} H^0(\text{NS}(A_{\overline{\mathbb{Q}}}))$; it is a finite number due to Néron’s basis theorem.

Let now \mathcal{O} be an hereditary order in a quaternion algebra B over \mathbb{Q} . Assume that A is an abelian surface defined over a number field K together with an isomorphism of rings $\iota: \mathcal{O} \xrightarrow{\sim} \text{End}_{\overline{\mathbb{Q}}}(A)$. The underlying complex torus $A_{\mathbb{C}} = V/\Lambda$ is the quotient of a complex vector space V of dimension 2 by a lattice Λ of rank 4 over \mathbb{Z} . Upon fixing an isomorphism

$B \otimes \mathbb{R} \xrightarrow{\sim} M_2(\mathbb{R})$ there is an action of $\mathcal{O} \subset B \subset M_2(\mathbb{R})$ on the lattice Λ that makes it a left \mathcal{O} -module. Since all left ideals of \mathcal{O} are principal and from the work of Shimura [23], it is well-known that there exists $\tau \in \mathcal{H} = \{a + bi \in \mathbb{C}, b > 0\}$ such that $\Lambda = \mathcal{O} \begin{pmatrix} \tau \\ 1 \end{pmatrix}$.

In [20], the absolute Néron–Severi group $\text{NS}(A_{\mathbb{C}}) \simeq \text{NS}(A_{\mathbb{Q}})$ was largely studied under the assumption on \mathcal{O} to be hereditary: it was seen that the first Chern class allows us to regard $\text{NS}(A_{\mathbb{C}})$ as a sub-lattice of the 3-dimensional vector space $B_0 = \{\mu \in B: \text{tr}(\mu) = 0\}$ of pure quaternions of B in a way that fundamental properties of line bundles \mathcal{L} on A such as the degree $\text{deg}(\mathcal{L})$ [20, Proposition 3.1], the behaviour under pull-backs by endomorphisms [20, Theorem 2.2] and the index $i(\mathcal{L})$ and the ampleness [20, Theorem 5.1] can be interpreted in terms of the arithmetic of B . We summarize it in the following theorem.

Theorem 3.1 [20]. *Let $A/\overline{\mathbb{Q}}$ be an abelian surface with $\text{End}_{\overline{\mathbb{Q}}}(A) \stackrel{\sim}{=} \mathcal{O}$ an hereditary order of discriminant D in a quaternion algebra. Then there is an isomorphism of additive groups*

$$c_1 : \text{NS}(A_{\overline{\mathbb{Q}}}) \rightarrow \mathcal{O}_0^{\sharp}, \quad \mathcal{L} \mapsto c_1(\mathcal{L})$$

such that

- (1) $\text{deg}(\mathcal{L}) = D \cdot n(c_1(\mathcal{L}))$.
- (2) For any endomorphism $\alpha \in \mathcal{O} = \text{End}_{\overline{\mathbb{Q}}}(A)$, $c_1(\alpha^*(\mathcal{L})) = \bar{\alpha} c_1(\mathcal{L}) \alpha$.
- (3) A line bundle $\mathcal{L} \in \text{NS}(A_{\overline{\mathbb{Q}}})$ is a polarization if and only if $n(c_1(\mathcal{L})) > 0$ and $\det(v_{\mathcal{L}}) > 0$ where $v_{\mathcal{L}} \in GL_2(\mathbb{R})$ is (any) matrix such that $v_{\mathcal{L}}^{-1} c_1(\mathcal{L}) v_{\mathcal{L}} \in \mathbb{Q}^* \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

Here, $\mathcal{O}^{\sharp} = \{\beta \in B: \text{tr}(\mathcal{O}\beta) \subseteq \mathbb{Z}\}$ denotes the codifferent ideal of \mathcal{O} in B . By \mathcal{O}_0^{\sharp} we mean the subgroup $\mathcal{O}^{\sharp} \cap B_0$ of pure quaternions of \mathcal{O}^{\sharp} . For our purposes in this note, we only need to know that it is a lattice in B_0 and in particular $\rho(A_{\overline{\mathbb{Q}}}) = 3$.

Let us also remark that, by Eichler’s theory on optimal embeddings (cf., e.g., [1,26]), there always exists $\mu \in \mathcal{O}$ such that $\mu^2 + D = 0$ and, as a corollary of Theorem 3.1, $A_{\overline{\mathbb{Q}}}$ is always principally polarizable. We refer the reader to [20] for more details.

We consider now the action of the Galois group $G_K = \text{Gal}(\overline{\mathbb{Q}}/K)$ on $\text{NS}(A_{\overline{\mathbb{Q}}})$ given by $\mathcal{L}(\mathcal{D})^{\tau} = \mathcal{L}(\mathcal{D}^{\tau})$ for any line bundle \mathcal{L} on A represented by a Weil divisor \mathcal{D} and $\tau \in G_K$. From Theorem 3.1, any automorphism of $\text{NS}(A_{\overline{\mathbb{Q}}})$ can be regarded as a linear automorphism of B_0 . Moreover, since the Galois action preserves the degree of line bundles and the first Chern class is a monomorphism of quadratic modules $c_1 : (\text{NS}(A_{\overline{\mathbb{Q}}}), \text{deg}) \hookrightarrow (B_0, D \cdot n)$, we obtain a Galois representation

$$\eta : G_K \longrightarrow \text{Aut}(\text{NS}(A_{\overline{\mathbb{Q}}}), \text{deg}) \subset \text{Aut}(B_0, D \cdot n), \quad \tau \mapsto \eta_{\tau}.$$

We have that

- (1) For any $\alpha \in \mathcal{O} = \text{End}_{\overline{\mathbb{Q}}}(A)$, $(\alpha^*(\mathcal{L})^{\tau}) = (\alpha^{\tau})^*(\mathcal{L}^{\tau})$.
- (2) The index $i(\mathcal{L})$ only depends on the G_K -orbit of \mathcal{L} , that is, $i(\mathcal{L}^{\tau}) = i(\mathcal{L})$, for any $\tau \in G_K$. In particular \mathcal{L}^{τ} is a polarization if and only if \mathcal{L} is.

The following relates the Galois actions on $\text{End}_{\overline{\mathbb{Q}}}(A)$ and on the Néron–Severi group of A/K by means of a reciprocity law.

Theorem 3.2. *Let A/K be an abelian surface with QM by an hereditary order \mathcal{O} of discriminant D in a quaternion algebra B .*

Let $\gamma : G_K \rightarrow \text{Aut}(\text{End}_{\overline{\mathbb{Q}}}(A))$, $\tau \mapsto [\gamma_\tau] : \mathcal{O} \rightarrow \mathcal{O}$, $\beta \mapsto \gamma_\tau^{-1}\beta\gamma_\tau$, be the action of $\text{Gal}(\overline{\mathbb{Q}}/K)$ on the ring of endomorphisms of A . Define $\varepsilon_\tau = \text{sign}(n(\gamma_\tau)) = \pm 1$. Then

$$c_1(\mathcal{L}^\tau) = \varepsilon_\tau \cdot \gamma_\tau^{-1}c_1(\mathcal{L})\gamma_\tau$$

for any line bundle $\mathcal{L} \in \text{NS}_{\overline{\mathbb{Q}}}(A)$ and any $\tau \in G_K$.

Proof. Fix $\tau \in G_K$. We firstly claim that $\eta_\tau : B_0 \rightarrow B_0$ is given by $\mu \mapsto \tilde{\varepsilon}\tilde{\gamma}^{-1}\mu\tilde{\gamma}$ for some $\tilde{\varepsilon} = \pm 1$, $\tilde{\gamma} \in B^*$. Indeed, any linear endomorphism of B_0 extends uniquely to an endomorphism of B and $\text{End}(B) \simeq B \otimes B$ with $\tilde{\gamma}_1 \otimes \tilde{\gamma}_2 : B \rightarrow B$, $\beta \mapsto \tilde{\gamma}_1\beta\tilde{\gamma}_2$. We must have in addition that $\text{tr}(\tilde{\gamma}_1\mu\tilde{\gamma}_2) = \text{tr}(\tilde{\gamma}_2\tilde{\gamma}_1\mu) = 0$ for any $\mu \in B_0$. This automatically implies that $\tilde{\gamma}_2\tilde{\gamma}_1 \in \mathbb{Q}$.

Since the action of G_K on $\text{NS}_{\overline{\mathbb{Q}}}(A)$ conserves the degree of line bundles, we deduce from Theorem 3.1 that $n(\eta_\tau(\mu)) = n(\tilde{\gamma}_1\mu\tilde{\gamma}_2) = n(\tilde{\gamma}_1)n(\mu)n(\tilde{\gamma}_2) = n(\mu)$ for any $\mu \in B_0$. Hence $n(\tilde{\gamma}_2) = n(\tilde{\gamma}_1)^{-1}$ and thus $\tilde{\gamma} := \tilde{\gamma}_2 = \tilde{\varepsilon}\tilde{\gamma}_1^{-1}$ for some $\tilde{\varepsilon} = \pm 1$. This proves the claim.

We now show that $\tilde{\gamma} = \gamma_\tau \in B^*/\mathbb{Q}^*$ and $\tilde{\varepsilon} = \varepsilon_\tau$. We know that $(\alpha^*(\mathcal{L})^\tau) = (\alpha^\tau)^*(\mathcal{L}^\tau)$ for any $\alpha \in \mathcal{O}$. Taking Theorem 3.1 into account this implies that $\eta_\tau(\tilde{\alpha}\mu\alpha) = [\gamma_\tau](\alpha)\eta_\tau(\mu)[\gamma_\tau](\alpha)$ and thus $\tilde{\varepsilon}\tilde{\gamma}^{-1}(\tilde{\alpha}\mu\alpha)\tilde{\gamma} = \tilde{\varepsilon}(\gamma_\tau^{-1}\alpha\gamma_\tau)\tilde{\gamma}^{-1}\mu\tilde{\gamma}(\gamma_\tau^{-1}\alpha\gamma_\tau)$ for any $\alpha \in B$, $\mu \in B_0$. Choosing $\alpha = \mu$ and bearing in mind that $\gamma_\tau^{-1} = \tilde{\gamma}_\tau n(\gamma_\tau)^{-1}$, this says that $\tilde{\gamma}^{-1}\mu\tilde{\gamma} = \gamma_\tau^{-1}\mu^{-1}\gamma_\tau\tilde{\gamma}^{-1}\mu\tilde{\gamma}\gamma_\tau^{-1}\mu\gamma_\tau$ and thus $\mu(\omega\mu\omega^{-1}) = (\omega\mu\omega^{-1})\mu$, where we write $\omega = \gamma_\tau\tilde{\gamma}^{-1}$. The centralizer of $\mathbb{Q}(\mu)$ in B is $\mathbb{Q}(\mu)$ itself and therefore $(\omega\mu\omega^{-1}) \in \mathbb{Q}(\mu)$. But $\text{tr}(\mu) = \text{tr}(\omega\mu\omega^{-1}) = 0$, $n(\mu) = n(\omega\mu\omega^{-1})$ and this implies that $\mu = \pm\omega\mu\omega^{-1}$. Since this must hold for any $\mu \in B_0$, it follows that $\omega \in \mathbb{Q}^*$ and thus $\tilde{\gamma} = \gamma_\tau \in B^*/\mathbb{Q}^*$ as we wished.

We then already have that $\eta_\tau : B_0 \rightarrow B_0$ is given by $\mu \mapsto \tilde{\varepsilon}\gamma_\tau^{-1}\mu\gamma_\tau$ for some $\tilde{\varepsilon} = \pm 1$. If $\mu = c_1(\mathcal{L})$ for a polarization \mathcal{L} on A , this means that $c_1(\mathcal{L}^\tau) = \tilde{\varepsilon}\gamma_\tau^{-1}\mu\gamma_\tau$. Since \mathcal{L}^τ is still an ample line bundle we have, according to Theorem 3.1(3), that $\tilde{\varepsilon} = \text{sign}(n(\gamma_\tau))$. \square

We can now prove the following result that yields Theorem 1.3 in the introduction as an immediate corollary. Let us before say a word about the Néron–Severi group and the cone of polarizations on an abelian variety A/K .

Firstly, we remark that A_K is always attached with a polarization and thus the Picard number $\rho(A_K)$ never vanishes. Namely, if $A \xrightarrow{i} \mathbb{P}_K^N$ is an embedding of A into a projective space over K , then $i^*(\mathcal{O}(1)) \in \text{NS}(A_K)$. However, any polarization constructed by these means is very ample and hence can not be principal. This should be taken into account together with the fact that any abelian surface with hereditary quaternionic multiplication admits a principal polarization over $\overline{\mathbb{Q}}$ (cf. [20, Corollary 6.3]).

By [11], or also Theorem 3.1, we thus have that $1 \leq \rho(A_K) \leq 3$. Both three cases are possible and each possibility has a direct translation in terms of the algebra of endomorphisms: $\rho(A_K) = 1$ if and only if $\text{End}_K^0(A) := \text{End}_K(A) \otimes \mathbb{Q}$ is \mathbb{Q} or an imaginary quadratic field, $\rho(A_K) = 2$ if and only if $\text{End}_K^0(A)$ is a real quadratic field and $\rho(A_K) = 3$ if and only if $\text{End}_K^0(A) = \text{End}_{\overline{\mathbb{Q}}}(A) = B$.

The following definition was introduced in [21] and [22].

Definition 3.3. Let \mathcal{O} be an order in a quaternion algebra B over \mathbb{Q} and let $D = \text{disc}(\mathcal{O})$. We say that \mathcal{O} admits a *twist of degree* $\delta \geq 1$ if there exists $m \in \mathbb{Z}$, $m \mid D$, such that

$$B = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij = \left(\frac{-D\delta, m}{\mathbb{Q}} \right)$$

with $i, j \in \mathcal{O}$, $i^2 = -D\delta$, $j^2 = m$ and $ij = -ji$. In this case we say that the twist is of *norm* m . If $\delta = 1$, we say that \mathcal{O} admits a *principal twist*.

Remark. For a given order \mathcal{O} in an indefinite quaternion algebra, let $\mathcal{N}_\delta = \{m_1, \dots, m_t\}$, $0 < m_i \mid D$, denote the (possibly empty) set of norms of the twists of degree δ on \mathcal{O} . It is easy to show that \mathcal{N}_1 is either empty or $\mathcal{N}_1 = \{m, D/m\}$ for some $m \mid D$. In other cases, \mathcal{N}_δ can be larger. Indeed, if $\delta = D$ for instance, then \mathcal{N}_D is either empty or equal to the set of sums of two squares $m = m_1^2 + m_2^2$ that divide D . We finally note that a quaternion order \mathcal{O} can very well admit twists of several different degrees.

Remark. In practice, the computation of a finite number of Hilbert symbols suffices to decide whether a given indefinite order is twisting of certain degree δ . Let us just quote that a necessary and sufficient condition for B to contain a maximal order \mathcal{O} admitting a twist of degree δ and norm m is that $m > 0$, $m \mid D = \text{disc}(\mathcal{O}) = \text{disc}(B)$ and that for any odd prime $p \mid D$: $m \notin \mathbb{F}_p^{*2}$ if $p \nmid m$ ($D/m \notin \mathbb{F}_p^{*2}$ if $p \mid m$, respectively).

Examples of quaternion algebras with principally twisting maximal orders are $B = \left(\frac{-6, 2}{\mathbb{Q}} \right)$ and $B = \left(\frac{-10, 2}{\mathbb{Q}} \right)$ of discriminant $D = 6$ and $D = 10$, respectively.

Theorem 3.4. Let A/K be an abelian surface defined over a number field K with quaternionic multiplication by an hereditary order \mathcal{O} of discriminant D in a quaternion algebra B and let L/K be the minimal extension of K such that $\text{End}_L(A) \simeq \mathcal{O}$. Fix a polarization $\mathcal{L}_0 \in H^0(\text{Gal}(\overline{\mathbb{Q}}, K), \text{NS}(A_{\overline{\mathbb{Q}}}))$ and let $\delta = \text{deg}(\mathcal{L}_0)$ be its degree.

- (A) (1) If δ is not equal to D neither to $3D$ up to squares, then $\text{Gal}(L/K) \simeq \{1\}$, C_2 or $D_2 = C_2 \times C_2$.
 (2) If $\delta = Dk^2$ for some $k \in \mathbb{Z}$, then $\text{Gal}(L/K) \simeq C_n$ or D_n with $n = 1, 2$, or 4 .
 (3) If $\delta = \frac{Dk^2}{3}$ for some $k \in \mathbb{Z}$, then $\text{Gal}(L/K) \simeq C_n$ or D_n for $n = 1, 2, 3$, or 6 .
 (B) In any of the cases above, if \mathcal{O} does not admit any twist of degree δ , then $\text{Gal}(L/K)$ is necessarily cyclic.
 (C) (1) If $\text{Gal}(L/K) \simeq C_2$, then $\text{End}_K^0(A) \simeq \mathbb{Q}(\sqrt{-D\delta})$ or $\mathbb{Q}(\sqrt{m_i})$ for $0 < m_i \in \mathcal{N}_\delta$ a norm of a twist of degree δ on \mathcal{O} .

- (2) If $G = C_3$ or C_6 , then $\text{End}_K^0(A) \simeq \mathbb{Q}(\sqrt{-3})$.
- (3) If $G = C_4$, then $\text{End}_K^0(A) \simeq \mathbb{Q}(\sqrt{-1})$.
- (4) If $G = D_n$, then $\text{End}_K(A) \simeq \mathbb{Q}$.

Proof. Recall that, according to Proposition 2.1, $\text{Gal}(L/K) \simeq C_n$ or D_n with $n = 1, 2, 3, 4$, or 6 . Let $\mathcal{L}_0 \in H^0(\text{Gal}(\overline{\mathbb{Q}}, K), \text{NS}(A_{\overline{\mathbb{Q}}}))$ be a polarization on A and let $\mu = c_1(\mathcal{L}_0) \in \mathcal{O}_0$. It satisfies that $\mu^2 + D\delta = 0$ by Theorem 3.1(1). Fix $\tau \in \text{Gal}(L/K)$ and let $\gamma_\tau \in B^*$ the quaternion associated to τ in Section 2. Suitably scaling it, we can (and we do) choose a representative in $N_{B^*}(\mathcal{O})/\mathbb{Q}^*$ such that $\gamma_\tau \in \mathcal{O}$ and $n(\gamma_\tau)$ is a square-free integer. Then, since γ_τ must normalize \mathcal{O} , we know that $n(\gamma_\tau) \mid D$.

Since the algebraic class of \mathcal{L}_0 is $\text{Gal}(\overline{\mathbb{Q}}/K)$ -invariant, it follows from Theorem 3.2 that $\mu = c_1(\mathcal{L}_0) = c_1(\mathcal{L}_0^\tau) = \varepsilon_\tau \gamma_\tau^{-1} \mu \gamma_\tau$.

If $\varepsilon_\tau = -1$, then the above expression implies that $\mu \gamma_\tau = -\gamma_\tau \mu$. Since $\text{tr}(\mu \gamma_\tau) = \mu \gamma_\tau - \bar{\gamma}_\tau \mu = -\text{tr}(\gamma_\tau) \mu \in \mathbb{Q}^*$, we deduce that $\text{tr}(\gamma_\tau) = 0$. This means that $\gamma_\tau^2 = m$ for some $m \mid D$ and $B = \mathbb{Q} + \mathbb{Q}\mu + \mathbb{Q}\gamma_\tau + \mathbb{Q}\mu\gamma_\tau = (\frac{-D\delta, m}{\mathbb{Q}})$. The indefiniteness of B forces m to be positive. We obtain that in this case $\langle [\gamma_\tau] \rangle \simeq C_2$.

On the other hand, if $\varepsilon_\tau = 1$, then $\gamma_\tau \in \mathbb{Q}(\mu) \simeq \mathbb{Q}(\sqrt{-D\delta}) = \mathbb{Q}(\sqrt{-D\delta})$, where we let $\underline{D\delta}$ denote the square-free part of $D\delta$. In this case, and bearing in mind that γ_τ must generate a finite subgroup of B^*/\mathbb{Q}^* , we deduce that either

- $\gamma_\tau = \pm \sqrt{\underline{D\delta}/D\delta} \cdot \mu$ and hence $\underline{D\delta} \mid D$ and $\langle [\gamma_\tau] \rangle \simeq C_2$,
- $\gamma_\tau = 1 + \zeta_n$ for some n th-primitive root of unity $\zeta_n \in B^*$, $n = 3$ or 6 , and hence $\underline{D\delta} = 3$ and $\langle [\gamma_\tau] \rangle \simeq C_n$ or
- $\gamma_\tau = 1 + \zeta_4$ for some 4th-primitive root of unity $\zeta_4 \in B^*$ and hence $\underline{D\delta} = 1$ and $\langle [\gamma_\tau] \rangle \simeq C_4$.

We conclude that a necessary condition for $\text{Gal}(L/K)$ to contain a cyclic subgroup of order $n \geq 3$ is $\underline{D\delta} = 1$ or 3 which amounts to say that $\text{deg}(\mathcal{L}_0) = \delta$ is D or $3D$ up to squares, respectively. Also, if $\text{deg}(\mathcal{L}_0) = Dk^2$, then necessarily $\text{Gal}(L/K) \simeq C_n$ or D_n with $n = 1, 2$, or 4 and an analogous statement holds if $\text{deg}(\mathcal{L}_0) = 3D$ up to squares. Further, if $B \not\subseteq (\frac{-D\delta, m}{\mathbb{Q}})$ for any $0 < m \mid D$, then it follows from the discussion above that $\varepsilon_\tau = 1$ for any $\tau \in \text{Gal}(L/K)$ and, as a consequence, $\text{Gal}(L/K) \subset \mathbb{Q}(\mu)^*/\mathbb{Q}^*$. Since the only finite subgroups of $\mathbb{Q}(\mu)^*/\mathbb{Q}^*$ are cyclic, the proof of parts (A) and (B) is completed.

As for part (C), assume first that $\text{Gal}(L/K) = \langle [\gamma_\tau] \rangle \simeq C_2$. Then $\gamma_\tau \in B^*$ satisfies $\gamma_\tau^2 = -n(\gamma_\tau) \in \mathbb{Q}^*$ and we already saw that the only possibilities are, up to squares, $n(\gamma_\tau) = D\delta$ or $m \in \mathcal{N}_\delta$. In any of these cases, $\text{End}_K^0(A) = \{\beta \in \text{End}_L(A) : \beta^\tau = \beta\} = \{\beta \in \text{End}_L(A) : \beta\gamma_\tau = \gamma_\tau\beta\} = \mathbb{Q}(\gamma_\tau)$ and this implies our first assertion of part (C). Similarly, if $\text{Gal}(L/K) = \langle 1 + \zeta_n \rangle \simeq C_n$ with $n = 3, 4$, or 6 then $\text{End}_K^0(A) = \mathbb{Q}(1 + \zeta_n) \simeq \mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$ depending on the cases. Finally, if $\text{Gal}(L/K) = \langle \gamma_\tau, \gamma_{\tau'} \rangle \simeq D_n$ with $\langle \gamma_\tau \rangle \simeq C_n$ and $\langle \gamma_{\tau'} \rangle \simeq C_2$, then $\text{End}_K^0(A) = \{\beta \in \mathbb{Q}(\gamma_\tau) : \beta^\tau = \beta\} = \mathbb{Q}$. Here, the last equality holds because it is not possible that γ_τ and $\gamma_{\tau'}$ commute. \square

The following lemma may be useful in many situations in order to apply Theorem 3.4. It easily follows from Proposition 3.1.

Lemma 3.5. *Let $A/\overline{\mathbb{Q}}$ be an abelian surface with $\text{End}(A)$ a maximal order in a quaternion algebra of discriminant D . If there exist prime numbers $p, q \mid D$ such that p splits in $\mathbb{Q}(\sqrt{-1})$ and q splits in $\mathbb{Q}(\sqrt{-3})$, then no polarizations on A have degree Dk^2 or $3Dk^2$ for any $k \in \mathbb{Z}$.*

4. The action of $\text{Gal}(\overline{\mathbb{Q}}/K)$ on Tate modules

Let A be an abelian surface defined over a number field K such that $\text{End}_{\overline{\mathbb{Q}}}(A) \simeq \mathcal{O}$ is an order in an indefinite quaternion algebra B over \mathbb{Q} . Let L/K be the minimal field of definition of the endomorphisms of A . In this section we consider the compatible family of Galois representations $\{\sigma_\ell\}$ given by the action of $G = \text{Gal}(\overline{\mathbb{Q}}/K)$ on the Tate modules $T_\ell(A)$ of A . Throughout, we restrict ourselves to primes $\ell \nmid D \cdot N$, where $D = \text{disc}(\mathcal{O})$ and N is the product of the places of bad reduction of A . We refer the reader to [10] for an accurate study of the Galois representations arising from ramified primes $\ell \mid \text{disc}(B) \mid D$.

Our aim is two-fold: we wish to make an effective approach to Jacobson–Ohta’s Theorem 1.4 and to our main result Theorem 3.4. Bearing this idea in mind, we assume that L/K is a quadratic extension, in contraposition to the other possibilities permitted by Theorem 3.4. Then, we know that $\text{End}_K(A)$ is an order in a quadratic field $\mathbb{Q}(\sqrt{d})$. Assume further for simplicity that $\mathbb{Q}(\sqrt{d})$ is real, and let \mathcal{R} be its ring of integers. The imaginary quadratic case is described along the same lines but for certain differences (cf. Section 5.2).

In this setting, it is well known that the four dimensional Galois representations σ_ℓ are reducible over $\mathbb{Q}(\sqrt{d})$, that is,

$$\sigma_\ell = \rho_\lambda \oplus \rho_\lambda^\gamma,$$

where $\lambda \mid \ell$ is a prime in $\mathbb{Q}(\sqrt{d})$ over ℓ and $\text{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) = \langle \gamma \rangle$. Moreover, $\det(\rho_\lambda) = \chi$ is the ℓ -adic cyclotomic character (cf. [18]).

The representations ρ_λ have their images contained in the groups

$$\mathcal{U}_\lambda = \{M \in GL_2(\mathcal{R}_\lambda) : \det M \in \mathbb{Z}_\ell^*\}.$$

If we consider the subgroup $H = \text{Gal}(\overline{\mathbb{Q}}/L)$ of index two of G , we know by Theorem 1.4 that $\rho_\lambda|_H : H \rightarrow \text{Aut}_{\mathcal{O}}(T_\ell(A)) \simeq \mathcal{O}_\ell^* \simeq GL_2(\mathbb{Z}_\ell)$ is surjective for almost every prime ℓ . This imposes a strong restriction on the image of ρ_λ : in general, it can not be the full group \mathcal{U}_λ but a subgroup $\mathcal{V}_\lambda := \text{Image}(\rho_\lambda)$ that contains the image of H as a normal subgroup of index at most 2.

For a prime λ , let us call $H_\ell := \text{Image}(\rho_\lambda|_H)$. We know that it always holds that $H_\ell \subseteq \mathcal{O}_\ell^*$ and we say that ℓ is an *exceptional* prime if the inclusion fails to be an equality.

By applying Faltings’ proof of Tate’s conjecture as in [18, Proposition 3.5] (together with Chebotarev density theorem) the condition on $\text{End}_K(A) \subseteq \mathcal{R}$ to be a real quadratic order implies that there are infinitely many Frobenius elements with $\text{tr}(\rho_\lambda(\text{Frob } \wp)) \in \mathcal{R} \setminus \mathbb{Z}$. In turn, this implies that $\mathcal{V}_\lambda \not\subseteq \mathcal{O}_\ell^*$ and that H_ℓ is a normal subgroup of \mathcal{V}_λ of index two for almost every prime λ such that $(\frac{d}{\ell}) = -1$. If, on the other hand, $(\frac{d}{\ell}) = 1$, then $\mathcal{R}_\lambda = \mathbb{Z}_\ell$

and thus $\mathcal{V}_\lambda \subseteq \mathcal{O}_\ell^*$. In particular, by applying Theorem 1.4, it holds that $\mathcal{O}_\ell^* \subseteq \mathcal{V}_\lambda \subseteq \mathcal{U}_\lambda$ and $[\mathcal{V}_\lambda : \mathcal{O}_\ell^*] = 2$ if $\binom{d}{\ell} = -1$ and $\mathcal{O}_\ell^* = \mathcal{V}_\lambda$ if $\binom{d}{\ell} = 1$, for almost every prime λ .

Let us restrict for a while to inert primes: those such that $\binom{d}{\ell} = -1$. For them, we have that $\mathcal{V}_\lambda \subseteq \mathcal{U}_\lambda$ and there is the following exact sequence:

$$0 \rightarrow H_\ell \rightarrow \mathcal{V}_\lambda \rightarrow \{\pm 1\} \rightarrow 0. \quad (4.1)$$

Moreover, it is easy to see that $H_\ell = \mathcal{V}_\lambda \cap \mathcal{O}_\ell^*$. By considering the quotient $\mathcal{V}_\lambda/H_\ell \simeq \text{Gal}(L/K)$, using the information on the ramification of ρ_λ and varying the prime ℓ , we conclude that L/K is unramified outside N in agreement with Proposition 1.2. From (4.1), it follows that the quadratic character ψ corresponding to $\text{Gal}(L/K)$ determines whether or not the image $\rho_\lambda(\text{Frob } \wp)$ belongs to H_ℓ , i.e., $\rho_\lambda(\text{Frob } \wp) \in H_\ell \Leftrightarrow \psi(\wp) = 1$. Equivalently,

$$\rho_\lambda(\text{Frob } \wp) \in \mathcal{O}_\ell^* \iff \psi(\wp) = 1. \quad (4.2)$$

Let \wp be a prime such that $\psi(\wp) = -1$, so that $\rho_\lambda(\text{Frob } \wp) \in \mathcal{V}_\lambda \setminus H_\ell$. Since $[\mathcal{V}_\lambda : H_\ell] = 2$, we have that

$$\rho_\lambda^2(\text{Frob } \wp) \in H_\ell \subseteq \mathcal{O}_\ell^*. \quad (4.3)$$

Let us denote $a_\wp := \text{tr}(\rho_\lambda(\text{Frob } \wp))$. We know that the determinant of ρ_λ is the ℓ -adic cyclotomic character χ and we hence obtain that $\text{tr}(\rho_\lambda^2(\text{Frob } \wp)) = a_\wp^2 - 2p$. Thus, (4.3) implies that

$$a_\wp^2 \in \mathbb{Z}_\ell. \quad (4.4)$$

Observe that (4.4) is automatic for the remaining primes: those that split in $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$. Therefore, we have $\mathbb{Q}(\{a_\wp\}) = \mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\{a_\wp^2\}) = \mathbb{Q}$. From this and the fact that the character ψ governs the behaviour of ρ_λ for every ℓ inert in $\mathbb{Q}(\sqrt{d})$ (see (4.2)), it is an easy exercise to show that, for every $\wp \nmid D \cdot N$:

$$a_\wp^\gamma = \psi(\wp) a_\wp. \quad (4.5)$$

In fact, if the determinant is defined over \mathbb{Q} , Serre proved that compatible families of Galois representations verifying this property of having *inner twists* are characterized by the strict inclusion of $\mathbb{Q}(\{a_\wp^2\})$ in $\mathbb{Q}(\{a_\wp\})$.

For an arbitrary rational prime ℓ , observe that $a_\wp = u_\wp \sqrt{d}$, $u_\wp \in \mathbb{Z}$ if $\psi(\wp) = -1$. Let us fix such an element with the further restriction $a_\wp \neq 0$ and let p be the rational prime such that $\wp \mid p$. To ease the notation, we denote $M_\wp = \begin{pmatrix} a_\wp & 0 \\ 0 & 1/a_\wp \end{pmatrix}$.

Using (4.5) and imitating the proof of the theorem of Papier (see [17, Section 4] or [4, p. 398]) with the restriction that $\ell \nmid pN(a_\wp)$, we deduce that $\mathcal{V}_\lambda = \langle GL_2(\mathbb{Z}_\ell), M_\wp \rangle$ for those non-exceptional primes ℓ . In particular, this holds for almost every prime ℓ . In conclusion, we have shown that for every prime ℓ verifying

$$\ell \nmid D \cdot N \cdot p \cdot N(a_\wp), \quad (4.6)$$

the maximal possible image of ρ_λ is $\tilde{\mathcal{O}}_\ell^* := \langle GL_2(\mathbb{Z}_\ell), M_\wp \rangle \subseteq GL_2(\mathcal{R}_\lambda)$ and that the image is in fact maximal for almost every λ . We thus wonder: *How can the finite set of rational primes ℓ such that $\mathcal{V}_\lambda \subsetneq \tilde{\mathcal{O}}_\ell^*$ be bounded?*

In addition to restriction (4.6), the main point is that we need to impose the following condition on the residual mod λ representations $\bar{\rho}_\lambda$ (obtained from ρ_λ by composing with the naive reduction): $\bar{\rho}_\lambda|_H$ must be irreducible and the order of the image $\text{Image}(\bar{\rho}_\lambda|_H)$ must be a multiple of ℓ .

As explained in [17], for $\ell > 2 \geq [\mathcal{V}_\lambda : H_\ell]$, if one checks that $\bar{\rho}_\lambda$ is irreducible and that the order of its image is a multiple of ℓ , then $\bar{\rho}_\lambda|_H$ will also verify both these conditions. The main result on the determination of images for 2-dimensional Galois representations in [17] (see also [15] and [4]) then implies that $H_\ell = GL_2(\mathbb{Z}_\ell)$ and $\mathcal{V}_\lambda = \tilde{\mathcal{O}}_\ell^*$ for every prime λ , $\lambda \nmid \ell$ such that

- ℓ verifies (4.6);
- $\bar{\rho}_\lambda$ is irreducible with image of order multiple of ℓ ;
- $\ell \geq 5$ and $\det : H_\ell \rightarrow \mathbb{Z}_\ell^*$ is surjective;
- there exists a prime \mathfrak{R} in K with $a_{\mathfrak{R}} \in \mathbb{Z}$ and $\ell \nmid a_{\mathfrak{R}}$, $\mathfrak{R} \nmid \ell$.

Since $\det(\rho_\lambda|_H) = \chi|_H$, $\det|_{H_\ell}$ is surjective whenever ℓ does not ramify in L/\mathbb{Q} . As L/K is unramified outside N , it is enough to impose that $\ell \nmid N$, $\ell \nmid \text{disc}(K)$.

Theorem 4.1. *Let \wp, \mathfrak{R} be primes in K such that $\mathbb{Q}(a_\wp) = \mathbb{Q}(\sqrt{d})$ and $a_{\mathfrak{R}} \in \mathbb{Z}$. Let $\ell \geq 5$ be a rational prime such that $\ell \neq p$, $\ell \nmid N(a_\wp)$, $\ell \nmid N \cdot D$, $\ell \nmid \text{disc}(K)$, $\ell \nmid a_{\mathfrak{R}}$, $\mathfrak{R} \nmid \ell$ and let $\lambda \mid \ell$ in $\mathbb{Q}(\sqrt{d})$ be such that $\bar{\rho}_\lambda$ is irreducible and $\ell \mid |\text{Image}(\bar{\rho}_\lambda)|$. Then,*

$$\text{Image}(\rho_\lambda) = \langle GL_2(\mathbb{Z}_\ell), M_\wp \rangle.$$

The condition $\ell \mid |\text{Image}(\bar{\rho}_\lambda)|$ can be dealt with by elimination. Using the classification of maximal subgroups of PGL_2 over a finite field (of characteristic ℓ) due to L.E. Dickson, we know that any irreducible subgroup either has order multiple of ℓ or its projective image falls in one of the following cases: cyclic, dihedral or *small exceptional* (isomorphic to A_4 , S_4 , or A_5). Thus, the above theorem asserts that, in order to explicitly bound the set of exceptional primes in a concrete example, it only remains to bound the set of primes such that $\bar{\rho}_\lambda$ (modulo its centre) is either reducible, cyclic, dihedral or small exceptional. This will be accomplished in the following section.

Another key ingredient in the determination of the image of ρ_λ is the description of the restriction of $\bar{\rho}_\lambda$ to the inertia subgroup at ℓ : the determinant of ρ_λ being the cyclotomic character, we know a priori that both ρ_λ and its residual counterpart $\bar{\rho}_\lambda$ necessarily ramify at ℓ . Thanks to the results of Raynaud (cf. [13]), we know that one of the following must hold:

$$\bar{\rho}_\lambda|_{I_\ell} \simeq \begin{pmatrix} 1 & * \\ 0 & \chi \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} \psi_2 & 0 \\ 0 & \psi_2^\ell \end{pmatrix}, \quad (4.7)$$

where χ denotes the mod ℓ fundamental character and ψ_2 a fundamental character of level 2.

5. A concrete example of GL_2 -type

5.1. Fields of definition and endomorphism algebras

In this section we illustrate our results with an explicit example. We refer to [5] to further examples of Jacobians with quaternionic multiplication with different behaviours.

Let C be the smooth projective model of the genus 2 hyperelliptic curve

$$Y^2 = \frac{1}{48}X(9075X^4 + 3025(3 + 2\sqrt{-3})X^3 - 6875X^2 + 220(-3 + 2\sqrt{-3})X + 48).$$

By [7], the ring of endomorphisms of the Jacobian variety of C over $\overline{\mathbb{Q}}$ is a maximal order in the quaternion algebra of discriminant $D = 10$ over \mathbb{Q} . In this section we prove the following theorem.

Theorem 5.1. *Let $J(C)/K$ be the Jacobian variety of C over $K = \mathbb{Q}(\sqrt{-3})$. Then, $L = \mathbb{Q}(\sqrt{-3}, \sqrt{-11})$ is the minimal field of definition of the quaternionic endomorphisms of $J(C)$ and*

$$\text{End}_K(J(C)) \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}(\sqrt{5}).$$

Moreover, as it is shown in [7], there is an isomorphism of curves $C \xrightarrow{\cong} C^\tau$ between C and the Galois conjugated curve C^τ , where τ denotes the non trivial involution of K over \mathbb{Q} . Since the isomorphism lifts to an isomorphism $J(C) \simeq J(C)^\tau$ of abelian varieties, the generalized Shimura–Taniyama–Weil conjecture predicts that $J(C)$ should be modular (cf. [18]).

According to Theorem 1.3, in order to prove that L/K is a quadratic extension, it suffices to exclude the cases $L = K$ and $\text{Gal}(L/K) = D_2$.

From the model we have of C we see that its set of primes of bad reduction is contained in $\{2, 3, 5, 7, 11\}$. Thus, we take $N = 2 \cdot \check{3} \cdot 5 \cdot 7 \cdot 11$, where $\check{3} = \sqrt{-3}$ ramifies in K/\mathbb{Q} . Let us consider the Galois representations σ_ℓ acting on the Tate modules of $A = J(C)$. In [7], the characteristic polynomials $\text{Pol}_\wp(x)$ of the matrices $\sigma_\ell(\text{Frob } \wp)$ for the first primes $\wp \nmid N$ of K of residue class degree 1 were computed and factorized as follows:

$$\text{Pol}_\wp(x) = (x^2 - a_\wp x + p)(x^2 - b_\wp x + p). \tag{5.1}$$

The computed values of a_\wp, b_\wp satisfy the following: they are either both rational integers or both integers in $\mathbb{Q}(\sqrt{5})$; while $a_\wp = b_\wp$ in the first case, they are conjugated to each other in the second. In particular, this implies that the case $L = K$ is impossible, since else we would have $\mathbb{Q}(\{a_\wp\}) = \mathbb{Q}$.

Suppose then that $[L : K] = 4$. This would imply that the representations σ_ℓ would be absolutely irreducible. Indeed, this is a consequence of Faltings’ proof of Tate’s conjecture since by Theorem 1.3 we know that in this case $\text{End}_K(A) = \mathbb{Z}$.

Now, since $\text{Gal}(L/K) = D_2$, we know that there are three intermediate fields $K \subsetneq E_1, E_2, E_3 \subsetneq L$ satisfying $E_1 \cdot E_2 = E_2 \cdot E_3 = E_3 \cdot E_1 = L$. For each of them, we know that $\text{End}_{E_i}(A)$ is an order \mathcal{R}_i in a quadratic field W_i .

We wish to apply the results of the previous section to the extensions L/E_i and we first need to explain how these results generalize to the case of a nonreal field W_i . The only changes concern the determinant of the two-dimensional irreducible components ρ_λ^i and $\rho_\lambda^{i\gamma_i}$ of the representations of $\text{Gal}(\overline{\mathbb{Q}}/E_i)$: by the Riemann hypothesis, it easily follows that in the standard factorization (5.1) of the characteristic polynomials it must hold that $a_\wp, b_\wp \in \mathbb{R}$. Thus, if W_i is not real, we have that $\text{tr}(\rho_\lambda^i(\text{Frob } \wp)) = a_\wp \in W_i \setminus \mathbb{Q} \Rightarrow a_\wp \notin \mathbb{R}$ for almost every prime \wp in E_i inert in L/E_i and hence $\det(\rho_\lambda^i(\text{Frob } \wp)) \neq p$. This and the description of $\rho_\lambda^i|_{I_\ell}$ forces the determinant of ρ_λ^i to be equal to $\phi_i \cdot \chi$ for some non-trivial finite order character ϕ_i unramified outside N . Finally, since the determinant is χ when restricted to the subgroup G_L of index two of G_K , we conclude that ϕ_i is precisely the quadratic character corresponding to $\text{Gal}(L/E_i)$. Formula (4.5) is thus verified (with the obvious change of notation: ψ becomes ϕ_i).

Let us call $T_i = \text{Gal}(\overline{\mathbb{Q}}/E_i)$, $i = 1, 2, 3$. We conclude that σ_ℓ is absolutely irreducible and we know that it contains the reducible groups $\sigma_\ell|_{T_i} = \rho_\lambda^i \oplus \rho_\lambda^{i\gamma_i}$ as normal subgroups of index two, where $\langle \gamma_i \rangle = \text{Gal}(W_i/\mathbb{Q})$.

We also know that the extensions E_i/K only ramify at the primes in N so there are finitely many options for them and thus also for L . Let $H = \text{Gal}(\overline{\mathbb{Q}}/L)$. We know that $\sigma_\ell|_H = (\rho_\lambda^i \oplus \rho_\lambda^{i\gamma_i})|_H = \rho_\ell \oplus \rho_\ell$ for $i = 1, 2$, and 3 and ρ_ℓ with values in $GL(2, \mathbb{Z}_\ell)$ for almost every ℓ . Let \wp be a prime in K . If \wp is totally decomposed in L/K , then $\text{Frob } \wp \in H$ and $\text{tr}(\sigma_\ell(\text{Frob } \wp)) = 2 \cdot \text{tr}(\rho_\ell(\text{Frob } \wp)) = 2a_\wp$ with $a_\wp \in \mathbb{Z}$.

On the other hand, let \wp be a prime in K not totally decomposed in L/K . Despite this fact, there exists $i \in \{1, 2, 3\}$ such that \wp decomposes in E_i/K , but is inert in L/E_i . Then $\text{Frob } \wp \in T_i \setminus H$ and by applying formula (4.5), we obtain that

$$\begin{aligned} \text{tr}(\sigma_\ell(\text{Frob } \wp)) &= \text{tr}(\rho_\lambda^i(\text{Frob } \wp)) + \text{tr}(\rho_\lambda^{i\gamma_i}(\text{Frob } \wp)) = a_\wp + a_\wp^{\gamma_i} \\ &= a_\wp + \phi_i(\text{Frob } \wp)a_\wp = 0. \end{aligned}$$

Lemma 5.2. *Let A/K be an abelian surface with quaternionic multiplication and let L/K be the minimal field of definition of the endomorphisms of A . Let N be the product of the primes of bad reduction of A over K . Then, if $\text{Gal}(L/K) = D_2$, there exist two different quadratic extensions E_1 and E_2 of K , both unramified outside N , such that*

- L is the compositum of E_1 and E_2 .
- For every prime $\wp \nmid N$ of K totally decomposed in L/K , the characteristic polynomial of $\sigma_\ell(\text{Frob } \wp)$, when factorized as in (5.1), verifies $a_\wp = b_\wp \in \mathbb{Z}$.

On the other hand, if \wp does not totally decompose in L/K , then

$$\text{tr}(\sigma_\ell(\text{Frob } \wp)) = 0.$$

There is a finite number of possibilities for E_1 and E_2 : in the example considered, these two fields must be two (different) extensions of $K = \mathbb{Q}(\sqrt{-3})$ unramified outside $N = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$. Computations show that, for any choice of such a pair of quadratic extensions,

there is a prime \wp of K not totally decomposed in the compositum field contradicting the trace 0 condition of the lemma above.

We recall that, in order to simplify computations, we only computed the characteristic polynomials for primes \wp of K that have residue class degree 1. We have performed these computations for all such \wp with residue characteristic $p \leq 193$. Therefore, in virtue of Lemma 5.2, we conclude that L/K is not a quartic extension in our example. Having eliminated two of the three cases of Theorem 1.3(I), we conclude that the Jacobian variety $J(C)$ of Hashimoto–Murabayashi’s curve C has quaternionic multiplication over a quadratic extension L of $K = \mathbb{Q}(\sqrt{-3})$ and that $\text{End}_K(J(C))$ is the real quadratic field $\mathbb{Q}(\sqrt{5})$.

The quadratic extension L/K is unramified outside $N = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$ and formula (4.5) tells us that a non zero trace a_\wp is in \mathbb{Z} if and only if the prime \wp decomposes in L/K . Thus, considering all possible quadratic extensions of K unramified outside N and applying formula (4.5) to the traces computed, we see that the only extension that matches is $L = \mathbb{Q}(\sqrt{-3}, \sqrt{-11})$.

5.2. Explicit determination of the images of the Galois representations

We now wish to compute the finite set of (possibly) exceptional primes of the Galois representations on the Tate modules of the Jacobian variety of Hashimoto–Murabayashi’s curve C . By Theorem 5.1, we are placed under the assumptions of Theorem 4.1 in Section 4.

The hard part of the task is determining the primes such that the residual representation fails to be irreducible or does not have a multiple of ℓ order. These primes must fall in one of the following cases:

- (1) $\bar{\rho}_\lambda$ reducible,
- (2) $\mathbb{P}(\bar{\rho}_\lambda)$ cyclic,
- (3) $\mathbb{P}(\bar{\rho}_\lambda)$ dihedral,
- (4) $\mathbb{P}(\bar{\rho}_\lambda)$ small exceptional.

5.2.1. Reducible primes

We begin with the determination of those primes falling in cases (1) and (2), i.e., primes such that $\bar{\rho}_\lambda$ is reducible over \mathbb{F}_λ . We will call them *reducible primes*. Applying Raynaud’s result, we see that if $\lambda \nmid N$ is a reducible prime, we are in one of the two following situations:

$$\begin{aligned} \text{(a)} \quad \bar{\rho}_\lambda &\simeq \begin{pmatrix} \epsilon & * \\ 0 & \epsilon^{-1}\chi \end{pmatrix}, \\ \text{(b)} \quad \bar{\rho}_\lambda &\simeq \begin{pmatrix} \epsilon\psi_2 & * \\ 0 & \epsilon^{-1}\psi_2^\ell \end{pmatrix}, \end{aligned}$$

where ϵ is, in both cases, a character unramified outside N , χ is the mod ℓ cyclotomic character and ψ_2 a fundamental character of level 2.

In order to control the character ϵ we can use the bound for conductors of abelian varieties given in [2]. Since A is an abelian surface defined over $\mathbb{Q}(\sqrt{-3})$, we obtain that $\text{cond}(A) \mid 2^{20} \cdot 3^{16} \cdot 5^9 \cdot 7^4 \cdot 11^4$. This is a bound for the conductor of $\rho_\lambda \oplus \rho_\lambda^\gamma$ and thus we can assume that, for any prime λ in $\mathbb{Q}(\sqrt{-3})$ it holds that $\text{cond}(\rho_\lambda) \mid 2^{10} \cdot 3^8 \cdot 5^5 \cdot 7^2 \cdot 11^2$. If λ is a reducible prime as in case (a) or (b) above, the character ϵ must therefore verify: $\text{cond}(\epsilon) \mid 2^5 \cdot 3^4 \cdot 5^2 \cdot 7 \cdot 11$. Let us first treat

Case (a). Equating traces, we obtain

$$(a_\wp \bmod \lambda) = \epsilon(\text{Frob } \wp) + \epsilon^{-1}(\text{Frob } \wp)p$$

as elements in $\overline{\mathbb{F}}_\lambda$, for every $\wp \nmid \ell N$. Let $K := \mathbb{Q}(\sqrt{-3})$ and \mathcal{R} its ring of integers. We will apply class field theory over K to compute the reducible primes. We shall use repeatedly the fact that K has class number 1 and that the only units in K are the sixth roots of unity.

Observe that the image of ϵ is contained in $\overline{\mathbb{F}}_\lambda^*$, so this character of the Galois group G of K corresponds to a cyclic extension of K unramified outside N with conductor dividing $c := 2^5 \cdot 3^4 \cdot 5^2 \cdot 7 \cdot 11$. If we call

$$P(c) = \{ \wp : \text{there exists } \pi \in \mathcal{R} \text{ with } \wp = (\pi) \text{ and } \pi \equiv 1 \pmod{c} \}$$

and let F denote the ray class field of K of conductor c , then F is characterized by the fact that F/K is abelian and the set $P(c)$ is exactly the set of prime ideals of K that decompose totally in F . The cyclic extension F' of K corresponding to ϵ is of course contained in F . Thus, given a prime $\mathfrak{B} = (t)$ in K verifying $t^f \equiv 1 \pmod{c}$, we have $(\mathfrak{B}^f, F/K) = (\mathfrak{B}, F/K)^f = 1 \in \text{Gal}(F/K)$ and from $K \subseteq F' \subseteq F$ we obtain: $\epsilon(\text{Frob } \mathfrak{B})^f = 1$. From this and the assumption that the characteristic polynomial of $\bar{\rho}_\lambda(\text{Frob } \mathfrak{B})$ admits $\epsilon(\text{Frob } \mathfrak{B})$ as a root, we obtain the equation for the resultant:

$$\text{Res}_q := \text{Res}(x^2 - a_\mathfrak{B}x + q, x^f - 1) \equiv 0 \pmod{\lambda}$$

for $\mathfrak{B} \nmid \ell N$, q the rational prime below \mathfrak{B} and $\mathfrak{B} = (t)$ for some t with $t^f \equiv 1 \pmod{c}$.

In the example, we apply this equation with $q = 31, 43$, and 61 , $\mathfrak{B} \mid q$ generated by $t = 2 + 3\sqrt{-3}, 4 + 3\sqrt{-3}$, and $7 + 2\sqrt{-3}$ (respectively) having all them order mod c equal to $f = 240$. The values of the traces are $a_\mathfrak{B} = -4, 4\sqrt{5}$, and $4\sqrt{5}$ (respectively). Having computed Res_q for these three values of q , we see that for every prime λ in $\mathbb{Q}(\sqrt{5})$ with $\lambda \mid \ell > 11$ one of them verify $\lambda \nmid \text{Res}_q$, $\ell \neq q$. Thus we conclude that $\bar{\rho}_\lambda$ is not reducible as in case (a) for any $\ell > 11$.

Case (b). The analysis made in case (a) tells us how to control character ϵ , now it remains to say a few words about the “fundamental character” ψ_2 : in fact, we are abusing notation since we are denoting ψ_2 a character of G_K unramified outside ℓ whose restriction to I_ℓ agrees with a level 2 fundamental character. We can identify these two characters because K has class number 1. Let $\mathfrak{B} = (t)$ be a prime in K , then we know that $\psi_2(\text{Frob } \mathfrak{B}) \equiv \zeta t' \pmod{\lambda}$ where ζ is a unit in K ($\zeta^6 = 1$) and $t' = t$ or t^α , α the order two element in $\text{Gal}(K/\mathbb{Q})$. Observe that for case (b) to hold it should be ℓ inert in K/\mathbb{Q} ,

and so $t^\alpha \equiv t^\ell \pmod{\lambda}$. Take as in the previous discussion of case (a) a prime $\mathfrak{B} = (t)$ of K with $t^f \equiv 1 \pmod{c}$. Increase f if necessary so that $6 \mid f$. Then, using the assumption that both $\epsilon(\text{Frob } \mathfrak{B})\psi_2(\text{Frob } \mathfrak{B})$ and $\epsilon^{-1}(\text{Frob } \mathfrak{B})\psi_2^\ell(\text{Frob } \mathfrak{B})$ are roots of the characteristic polynomial of $\bar{\rho}_\lambda(\text{Frob } \mathfrak{B})$, we conclude that the following equation is satisfied:

$$\text{Res}(x^2 - a_\mathfrak{B}x + q, x^f - t^f) \equiv 0 \pmod{\lambda}$$

for $\mathfrak{B} \nmid \ell N$, q the rational prime below \mathfrak{B} and $\mathfrak{B} = (t)$ for some t with $t^f \equiv 1 \pmod{c}$, $6 \mid f$. We apply this equation in the example with $q = 43, 61$ and 193 . For $q = 193$ we take $\mathfrak{B} \mid q$ generated by $t = 1 + 8\sqrt{-3}$, this generator has order mod c equal to $f = 120$ and the corresponding trace is $a_\mathfrak{B} = 6\sqrt{5}$. From these computations it follows that if $\lambda \mid \ell > 11$ and $\ell \neq 89$ the residual representation $\bar{\rho}_\lambda$ does not fall in case (b).

It only remains to say a word about $\ell = 89$. In order to prove that this is not reducible prime, we use the following fact: let $H = \text{Gal}(\bar{\mathbb{Q}}/L)$ be the absolute Galois group of the field L of definition of the quaternionic endomorphisms. We know that, for any $\lambda \nmid N \cdot D$, the image of the restriction $\bar{\rho}_\lambda|_H$ lies in $GL_2(\mathbb{F}_\ell)$. Combined with the assumption in case (b), this shows that (the semisimplification of) $\bar{\rho}_\lambda|_H$ is contained in a non-split Cartan subgroup of $GL_2(\mathbb{F}_\ell)$ ($\mathbb{P}(\bar{\rho}_\lambda|_H)$ is cyclic). Thus, the image of $\bar{\rho}_\lambda|_H$ can contain no matrix whose characteristic polynomial is reducible over \mathbb{F}_ℓ with two different mod ℓ eigenvalues. We have computed a few characteristic polynomials for primes \wp such that $\text{Frob } \wp \in H$ (recall that we have shown that this is the case if $a_\wp \in \mathbb{Z}$, $a_\wp \neq 0$) and we found that, for $p = 157$, the corresponding characteristic polynomial is $x^2 + 4x + 157$ and that it reduces mod 89 with two different eigenvalues. This shows that 89 is not a reducible prime as in case (b).

5.2.2. Dihedral and small exceptional primes

The determination of dihedral primes is carried out by using the technique applied in [6, 19, 24] via the description of the restriction to I_ℓ provided by Raynaud’s theorem.

If $\mathbb{P}(\bar{\rho}_\lambda)$ is dihedral, then there exists a Cartan subgroup C such that the image \bar{V}_λ of $\bar{\rho}_\lambda$ is contained in the normalizer \mathcal{N} of C but not in C itself. Composing $\bar{\rho}_\lambda$ with the quotient $\mathcal{N}/C \simeq C_2 \simeq \{\pm 1\}$, we obtain a quadratic character ϕ of the Galois group $G = \text{Gal}(\bar{\mathbb{Q}}/K)$ corresponding to a quadratic extension E_ℓ of K unramified outside ℓN . Furthermore, the description of $\bar{\rho}_\lambda|_{I_\ell}$ for $\ell \nmid N$ shows that, if $\ell > 3$, it must be contained in C , so E_ℓ/K does not ramify at ℓ . The traces of elements in $\mathcal{N} \setminus C$ all vanish and the value $\phi(\text{Frob } \wp)$, where ϕ only ramifies at the prime divisors of N , determines whether $\bar{\rho}_\lambda(\text{Frob } \wp)$ falls in C or not. Thus, for every prime \wp in K such that \wp is inert in E_ℓ/K , we have that $\phi(\text{Frob } \wp) = -1$ and hence $a_\wp \equiv 0 \pmod{\lambda}$.

Therefore, the algorithm to compute all dihedral primes is the following:

- List all quadratic extensions E of K unramified outside $\{2, 3, 5, 7, 11\}$.
- For each of these extensions, find several primes \wp in K such that

$$\wp \text{ inert in } E/K \quad \text{and} \quad a_\wp \neq 0.$$

If $\lambda \mid \ell$ is a dihedral prime, we then should have that, for some quadratic extension E/K as above and all primes $\wp \nmid \ell$ verifying \dagger ,

$$\lambda \mid a_{\wp}.$$

We have computed the traces a_{\wp} for every prime \wp of K with residue class degree 1 and $N(\wp) \leq 193$ and applied the above algorithm to all quadratic extensions of $\mathbb{Q}(\sqrt{-3})$ unramified outside $\{2, 3, 5, 7, 11\}$ and we found no dihedral primes $\lambda \mid \ell > 11$. Finally, in order to eliminate the possibility of primes with small exceptional image, we use the trick applied in [6,19]: the description of $\mathbb{P}(\bar{\rho}_{\lambda}|_{I_{\ell}})$ shows that this group contains a cyclic subgroup of order $\ell \pm 1$. Hence, if $\ell > 5$, $\ell \nmid N$, the image of $\mathbb{P}(\bar{\rho}_{\lambda})$ can not be isomorphic to neither A_4 , S_4 nor A_5 . We have thus proved the following theorem.

Theorem 5.3. *Let C/K be a smooth projective model of the curve*

$$Y^2 = \frac{1}{48}X(9075X^4 + 3025(3 + 2\sqrt{-3})X^3 - 6875X^2 + 220(-3 + 2\sqrt{-3})X + 48)$$

over $K = \mathbb{Q}(\sqrt{-3})$ and let A/K be its Jacobian variety. Let $\{\rho_{\lambda}\}$ be the two-dimensional Galois representations on the Tate modules of A . Then, for every prime $\ell > 11$, $\lambda \mid \ell$, the residual representation $\bar{\rho}_{\lambda}$ is absolutely irreducible and the order of its image is a multiple of ℓ .

In order to apply Theorem 4.1, we just observe that, for primes \wp above 13 and 19, we have $a_{\wp} = 2\sqrt{5}$, whereas for primes \wp above 31 and 37, we have $a_{\wp} = -4, 4$, respectively.

Theorem 5.4. *For every prime $\ell > 11$, $\lambda \mid \ell$, the image of the Galois representation ρ_{λ} is the subgroup of $GL_2(\mathbb{Z}[\sqrt{5}]_{\lambda})$ generated by $GL_2(\mathbb{Z}_{\ell})$ and the diagonal matrix $\begin{pmatrix} \sqrt{5} & 0 \\ 0 & \sqrt{5}^{-1} \end{pmatrix}$. In particular, if $\ell \equiv \pm 1 \pmod{5}$, $\ell \neq 11$, the groups $GL_2(\mathbb{Z}_{\ell})$ and $GL_2(\mathbb{F}_{\ell})$ are realized as Galois groups over $\mathbb{Q}(\sqrt{-3})$ and the corresponding extension is unramified outside 2310ℓ . Furthermore, for every prime $\ell > 11$, the group $PGL_2(\mathbb{F}_{\ell})$ is realized as a Galois group over $\mathbb{Q}(\sqrt{-3})$, again through an extension unramified outside 2310ℓ .*

References

- [1] M. Alsina, P. Bayer, Quaternion Orders, Quadratic Forms, and Shimura Curves, CRM Monogr. Ser., vol. 22, ISBN 0-8218-3359-6, 2004.
- [2] A. Brumer, K. Kramer, The conductor of an abelian variety, *Compositio Math.* 92 (1994) 227–248.
- [3] T. Chinburg, E. Friedman, The finite subgroups of maximal arithmetic Kleinian groups, *Ann. Inst. Fourier Grenoble* 50 (2000) 1765–1798.
- [4] L. Dieulefait, Newforms, inner twists and the inverse Galois problem for projective linear groups, *J. Théor. Nombres Bordeaux* 13 (2001) 395–411.
- [5] L. Dieulefait, V. Rotger, On abelian surfaces with potential quaternionic multiplication, *Bull. Belg. Math. Soc.*, in press.
- [6] L. Dieulefait, N. Vila, Projective linear groups as Galois groups over \mathbb{Q} via modular representations, *J. Symbolic Comput.* 30 (2000) 799–810.

- [7] K. Hashimoto, N. Murabayashi, Shimura curves as intersections of Humbert surfaces and defining equations of QM-curves of genus two, *Tôhoku Math. J.* 47 (1995) 271–296.
- [8] M. Jacobson, Variétés abéliennes de dimension deux ayant pour algèbre de quaternions indéfinie, *Uspekhi Mat. Nauk* 29 (1974) 185–186 (in Russian).
- [9] S. Johansson, A description of quaternion algebras, preprint.
- [10] B.W. Jordan, Points on Shimura curves rational over number fields, *J. Reine Angew. Math.* 371 (1986) 92–114.
- [11] D. Mumford, *Abelian Varieties*, Tata Inst. Fund. Res. Stud. Math., Oxford Univ. Press, 1970.
- [12] M. Ohta, On ℓ -adic representations of Galois groups obtained from certain two dimensional abelian varieties, *J. Fac. Sci. Univ. Tokyo* 21 (1974) 299–308.
- [13] M. Raynaud, Schémas en groupes de type (p, \dots, p) , *Bull. Soc. Math. France* 102 (1974) 241–280.
- [14] I. Reiner, *Maximal Orders*, Academic Press, London, 1975.
- [15] K.A. Ribet, On ℓ -adic representations attached to modular forms, *Invent. Math.* 28 (1975) 245–275.
- [16] K.A. Ribet, Endomorphisms of semi-stable abelian varieties over number fields, *Ann. of Math.* 101 (1975) 555–562.
- [17] K.A. Ribet, On ℓ -adic representations attached to modular forms II, *Glasgow Math. J.* 27 (1985) 185–194.
- [18] K.A. Ribet, Abelian varieties over \mathbb{Q} and modular forms, in: J. Cremona, J.-C. Lario, J. Quer, K. Ribet (Eds.), *Modular Curves and Abelian Varieties*, in: *Progr. Math.*, vol. 224, Birkhäuser, 2004, pp. 241–261.
- [19] K.A. Ribet, Images of semistable Galois representations, *Pacific J. Math.* 181 (1997).
- [20] V. Rotger, Quaternions, polarizations and class numbers, *J. Reine Angew. Math.* 561 (2003) 177–197.
- [21] V. Rotger, Modular Shimura varieties and forgetful maps, *Trans. Amer. Math. Soc.* 356 (2004) 1535–1550.
- [22] V. Rotger, On the field of moduli of quaternionic multiplication on abelian varieties, *Internat. J. Math. Math. Sci.*, in press.
- [23] G. Shimura, Construction of class fields and zeta functions of algebraic curves, *Ann. of Math.* 85 (1967) 58–159.
- [24] J.-P. Serre, Propriétés galoisiennes des points d’ordre fini des courbes elliptiques, *Invent. Math.* 15 (1972) 259–331.
- [25] A. Silverberg, Fields of definition for homomorphisms of abelian varieties, *J. Pure Appl. Algebra* 77 (1992) 253–262.
- [26] M.F. Vignéras, *Arithmétique des algèbres de quaternions*, *Lecture Notes in Math.*, vol. 800, Springer-Verlag, New York, 1980.