[1]

THE FIELD OF MODULI OF QUATERNIONIC MULTIPLICATION ON ABELIAN VARIETIES

VICTOR ROTGER

Abstract. We consider principally polarized abelian varieties with quaternionic multiplication over number fields and we study the field of moduli of their endomorphisms in relation to the set of rational points on suitable Shimura varieties.

Published in *Intern. J. Math. M. Sc.* **52** (2004), 2795-2808.

1. Introduction

Let $\bar{\mathbb{Q}}$ be a fixed algebraic closure of the field $\mathbb{Q}$ of rational numbers and let $(A,\mathcal{L})/\bar{\mathbb{Q}}$ be a polarized abelian variety. The field of moduli of $(A,\mathcal{L})/\bar{\mathbb{Q}}$ is the minimal number field $k_{A,\mathcal{L}} \subset \overline{\mathbb{Q}}$ such that $(A,\mathcal{L})$ is isomorphic (over $\overline{\mathbb{Q}}$) to its Galois conjugate $(A^\sigma,\mathcal{L}^\sigma)$, for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/k_{A,\mathcal{L}})$.

The field of moduli $k_{A,\mathcal{L}}$ is an essential arithmetic invariant of the $\overline{\mathbb{Q}}$-isomorphism class of $(A,\mathcal{L})$. It is contained in all possible fields of definition of $(A,\mathcal{L})$ and, unless $(A,\mathcal{L})$ admits a rational model over $k_{A,\mathcal{L}}$ itself, there is not a unique minimal field of definition for $(A,\mathcal{L})$. In this regard, we have the following theorem of Shimura.

Theorem 1.1 ([19])**.** *A generic principally polarized abelian variety of odd dimension admits a model over its field of moduli. For a generic principally polarized abelian variety of even dimension, the field of moduli is not a field of definition.*

Let $\mathrm{End}(A) = \mathrm{End}_{\overline{\mathbb{Q}}}(A)$ denote the ring of endomorphisms of A. It is well known that $\mathrm{End}(A) = \mathbb{Z}$ for a generic polarized abelian variety $(A,\mathcal{L})$. However, due to Albert's classification of involuting division algebras ([13]) and the work of Shimura ([18], there are other rings that can occur as the endomorphism ring of an abelian variety. Namely, if $A/\overline{\mathbb{Q}}$ is simple, $\mathrm{End}(A)$ is an order in either a totally real number field F of degree $[F:\mathbb{Q}] \mid \dim(A)$, a totally indefinite quaternion algebra B over a totally real number field F of degree $2[F:\mathbb{Q}] \mid \dim(A)$, a totally definite quaternion algebra B over a totally real number field F of degree $2[F:\mathbb{Q}] \mid \dim(A)$ or a division algebra over a CM-field.

[1]Partially supported by a grant FPI from the Ministerio de Ciencia y Tecnología and by BFM2000-0627.

1991 *Mathematics Subject Classification.* 11G18, 14G35.

Key words and phrases. Field of moduli, field of definition, abelian variety, Shimura variety, quaternion algebra.

Let us recall that a quaternion algebra B over a totally real field F is called totally indefinite if $B \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathrm{M}_2(\mathbb{R}) \oplus ... \oplus \mathrm{M}_2(\mathbb{R})$ and totally definite if $B \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{H} \oplus ... \oplus \mathbb{H}$, where $\mathbb{H} = (\frac{-1,-1}{\mathbb{R}})$ denotes the skew-field of real Hamilton quaternions.

Definition 1.2. Let $(A, \mathcal{L})/\overline{\mathbb{Q}}$ be a polarized abelian variety and let $S \subseteq \mathrm{End}(A)$ be a subring of $\mathrm{End}(A)$. The field of moduli of S is the minimal number field $k_S \supseteq k_{A,\mathcal{L}}$ such that, for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/k_S)$, there is an isomorphism $\varphi_\sigma/\overline{\mathbb{Q}} : A \to A^\sigma$, $\varphi_\sigma^*(\mathcal{L}^\sigma) = \mathcal{L}$, of polarized abelian varieties that induces commutative diagrams

$$\begin{array}{ccc} A & \longrightarrow & A^\sigma \\ \beta \downarrow & & \downarrow \beta^\sigma \\ A & \longrightarrow & A^\sigma \end{array}$$

for any $\beta \in S$.

We remark that, as a consequence of the very basic definitions, the field of moduli of the multiplication-by-n endomorphisms on A is exactly $k_{\mathbb{Z}} = k_{A,\mathcal{L}}$. But in the case that $\mathrm{End}(A) \supsetneq \mathbb{Z}$, little is known on the chain of Galois extensions $k_{\mathrm{End}(A)} \supseteq k_S \supseteq k_{A,\mathcal{L}}$.

The main aim of this article is to study the field of moduli of totally indefinite quaternionic multiplication on an abelian variety. In relation to Shimura's Theorem 1.1, we remark that the dimension of an abelian variety whose endomorphism ring contains a quaternion order is always even.

We state our main result in the next section. As we will show in Section 3, it is a consequence of the results obtained in [16], [17] on certain modular forgetful morphisms between certain Shimura varieties, Hilbert modular varieties and the moduli spaces of principally polarized abelian varieties.

In Section 4, we particularize our results to abelian surfaces. We use our results together with those of Mestre [11] and Jordan [10] to compare the field of moduli and field of definition of the quaternionic multiplication on an abelian surface.

In an appendix to this paper, we discuss a question on the arithmetic of quaternion algebras that naturally arises from our considerations and which is also related to recent work by Chinburg and Friedman [2], [3].

A cryptographical application of the results in the appendix has been derived in [8] by Galbraith and the author.

2. Main result

Let F be a totally real number field F of degree $[F : \mathbb{Q}] = n$ and let R_F denote its ring of integers. We shall let F_+^* denote the subgroup of totally positive elements of F^*. For any finite field extension L/F, let R_L denote the ring of integers of L and let $\Omega_{odd}(L) = \{\xi \in R_L, \xi^f = 1, f \text{ odd }\}$ denote the set of primitive roots of unity of odd order in L. We let $\omega_{odd}(L) = |\Omega(L)|$.

Let B be a totally indefinite quaternion algebra over F and let $\mathcal{O}$ be a maximal order in B.

Definition 2.1. An abelian variety A/k over an algebraically closed field k has quaternionic multiplication by $\mathcal{O}$ if $\mathrm{End}(A) \simeq \mathcal{O}_B$ and $\dim(A) = 2n$.

Proposition 2.2. [15] *Let $(A, \mathcal{L})$ be a principally polarized abelian variety with quaternionic multiplication by $\mathcal{O}$ over $\overline{\mathbb{Q}}$. Then the discriminant ideal* $\mathrm{disc}(B)$ *of B is principal and generated by a totally positive element $D \in F_+^*$.*

As in [16], [17] we say that a quaternion algebra B over F of totally positive principal discriminant $\mathrm{disc}(B) \in F_+^*$ is *twisting* if $B \simeq (\frac{-D,m}{F})$ for some $m \in F_+^*$ supported at the prime ideals $\wp \mid D$ of F. Let C_2 denote the cyclic group of two elements. The main result of this article is the following.

Theorem 2.3. *Let $(A, \mathcal{L})$ be a principally polarized abelian variety with quaternionic multiplication by $\mathcal{O}$ over $\overline{\mathbb{Q}}$ and let* $\mathrm{disc}(B) = D$ *for some $D \in F_+^*$. Let $\omega = \omega(F(\sqrt{-D})$.*

(i) *If B is not twisting, then*
- *For any totally real quadratic order $S \subset \mathcal{O}$ over R_F, $k_{\mathcal{O}} = k_S$.*
- $\mathrm{Gal}(k_{\mathcal{O}}/k_{R_F}) \subseteq C_2^{\omega_{odd}}$.

(ii) *If B is twisting, then*
- *For any totally real quadratic order $S \subset \mathcal{O}$,* $\mathrm{Gal}(k_{\mathcal{O}}/k_S) \subseteq C_2$.
- $\mathrm{Gal}(k_{\mathcal{O}}/k_{R_F}) \subseteq C_2^{2\omega_{odd}}$.

As we state more precisely in Section 3, Theorem 2.3 admits several refinements.

3. Proof of Theorem 2.3: Shimura varieties and forgetful maps

Let B be a totally indefinite quaternion division algebra over a totally real number field F and assume that $\mathrm{disc}(B) = (D)$ for some $D \in F_+^*$. Let $\mathcal{O}$ be a maximal order in B and fix an arbitrary quaternion $\mu \in \mathcal{O}$ satisfying $\mu^2 + D = 0$. Its existence is guaranteed by Eichler's theory on optimal embeddings ([21]) and it generates a CM-field $F(\mu) \simeq F(\sqrt{-D})$ over F embedded in B. We will refer to the pair $(\mathcal{O}, \mu)$ as a *principally polarized order*.

Attached to $(\mathcal{O}, \mu)$, we can consider a Shimura variety $X_{\mathcal{O},\mu}/\mathbb{Q}$ that solves the coarse moduli problem of classifying triplets $(A, \iota, \mathcal{L})$ over $\mathbb{Q}$ where:

(i) $(A, \mathcal{L})$ is a principally polarized abelian variety and
(ii) $\iota : \mathcal{O} \hookrightarrow \mathrm{End}(A)$ is a monomorphism of rings satisfying that $\iota(\beta)^* = \iota(\mu^{-1}\bar{\beta}\mu)$ for all $\beta \in \mathcal{O}$ and where * denotes the Rosati involution with respect to $\mathcal{L}$.

Attached to the maximal order $\mathcal{O}$ there is also the *Atkin-Lehner group*

$$W = \mathrm{N}_{B^*}(\mathcal{O})/F^*\mathcal{O}^*.$$

Let C_2 denote the cyclic group of two elements. The group W is isomorphic to $C_2 \times \overset{2r}{\cdots} \times C_2$, where $2r = \sharp\{\wp \mid \mathrm{disc}(B)\}$ is the number of ramifying prime ideals of B (cf. [21], [16]).

Let B_+^* be the group of invertible quaternions of totally positive reduced norm. The *positive Atkin-Lehner group* is $W^1 = \mathrm{N}_{B_+^*}(\mathcal{O})/F^*\mathcal{O}^1$, where $\mathcal{O}^1 = \{\gamma \in \mathcal{O}, \mathrm{n}(\gamma) = 1\}$ denotes the group of units of $\mathcal{O}$ of reduced norm 1.

As it was shown in [16], the group W^1 is a subgroup of the automorphism group $\mathrm{Aut}_{\mathbb{Q}}(X_{\mathcal{O},\mu})$ of the Shimura variety $X_{\mathcal{O},\mu}$.

We have

$$W^1 \simeq C_2^s \text{ for } 2r \leq s \leq n + 2r - 1.$$

The first inequality holds because there is a natural map $W^1 \twoheadrightarrow W$ which is an epimorphism of groups due to indefiniteness of B and the norm theorem for maximal orders (see [16]). The second inequality is a consequence of Dirichlet's unit theorem and it is actually an equality if the narrow class number of F is $h_+(F) = 1$, as is the case of $F = \mathbb{Q}$.

We now introduce the notion of *twists* of a polarized order $(\mathcal{O}, \mu)$.

Definition 3.1. Let $(\mathcal{O}, \mu)$ be a principally polarized maximal order in a totally indefinite quaternion algebra B of discriminant $\mathrm{disc}(B) = (D)$, $D \in F_+^*$.

A twist of $(\mathcal{O}, \mu)$ is an element $\chi \in \mathcal{O} \cap \mathrm{N}_{B^*}(\mathcal{O})$ such that $\chi^2 + \mathrm{n}(\chi) = 0, \mu\chi = -\chi\mu$ and therefore

$$B = F + F\mu + F\chi + F\mu\chi = (\frac{-D, -\mathrm{n}(\chi)}{F}).$$

For any subring $S \subset \mathcal{O}$, we say that χ is a twist of $(\mathcal{O}, \mu)$ in S if $\chi \in S$.

We say that $(\mathcal{O}, \mu)$ is *twisting* if it admits some twist in $\mathcal{O}$ and that a quaternion algebra B is twisting if it contains a twisting polarized maximal order. This agrees with our terminology in the preceding section.

Definition 3.2. A twisting involution $\omega \in W^1$ is an Atkin-Lehner involution such that $[\omega] = [\chi] \in W$ is represented by a twist χ of $(\mathcal{O}, \mu)$. It is a twisting involution in $S \subseteq \mathcal{O}$ if it can be represented by a twist $\chi \in S$.

Let $V_0(S)$ denote the subgroup of W^1 generated by the twisting involutions of $(\mathcal{O}, \mu)$ in S; we will simply write V_0 for $V_0(\mathcal{O})$.

Let us remark that, since B is totally indefinite, no $\chi \in B_+^*$ can be a twist of $(\mathcal{O}, \mu)$ because a necessary condition for $B \simeq (\frac{-D,-\mathrm{n}(\chi)}{F})$ is that $\mathrm{n}(\chi)$ be totally negative. In fact, twisting involutions $\omega \in W^1$ are always represented by twists $\chi \in B_-^*$ of totally negative reduced norm.

Note also that a necessary and sufficient condition for B to be twisting is that $B \simeq (\frac{-D,m}{F})$ for some element $m \in F_+^*$ supported at the prime ideals $\wp \mid D$ (that is, $v_\wp(m) \neq 0$ only if $\wp \mid D$).

For a polarized order $(\mathcal{O},\mu)$, let $R_\mu = F(\mu)\cap\mathcal{O}$ be the order in the CM-field $F(\mu)\simeq F(\sqrt{-D})$ that optimally embeds in $\mathcal{O}$. Note that, since $\mu\in\mathcal{O}$, $R_\mu\supseteq R_F[\sqrt{-D}]$. We let $\Omega=\Omega(R_\mu)=\{\xi\in R_\mu,\xi^f=1,f\geq 1\}$ denote the finite group of roots of unity in R_μ and $\Omega_{odd}=\{\xi\in R_\mu,\xi^f=1,f \text{ odd }\}$ the subgroup of primitive roots of unity of odd order. Their respective cardinalities will be denoted by $\omega=\omega(R_\mu)$ and $\omega_{odd}=\omega_{odd}(R_\mu)$.

Definition 3.3. The *stable group* $W_0=U_0\cdot V_0$ associated to $(\mathcal{O},\mu)$ is the subgroup of W^1 generated by $U_0=\mathrm{N}_{F(\mu)^*}(\mathcal{O})/F^*\cdot\Omega$ and the group of twisting involutions V_0.

Note that U_0 is indeed a subgroup of W^1 because $\Omega=F(\mu)\cap\mathcal{O}^1$.

The motivation for introducing the Shimura variety $X_{\mathcal{O},\mu}$ and the above Atkin-Lehner groups in this note is that it gives a modular interpretation of the field of moduli $k_\mathcal{O}$ of the quaternionic multiplication on A: $k_\mathcal{O}=\mathbb{Q}(P)$ is the extension over $\mathbb{Q}$ generated by the coordinates of the point $P=[A,\iota,\mathcal{L}]$ on Shimura's canonical model $X_{\mathcal{O},\mu}/\mathbb{Q}$ that represents the $\overline{\mathbb{Q}}$-isomorphism class of the triplet.

A similar construction holds for the totally real subalgebras of B. Indeed, let $L\subset B$ be a totally real quadratic extension of F embedded in B. Then $S=L\cap\mathcal{O}$ is an order of L over R_F which is optimally embedded in $\mathcal{O}$. Identifying S with a subring of the ring of endomorphisms of A, we again have that the field of moduli k_S is the extension $\mathbb{Q}(P_{|S})$ of $\mathbb{Q}$ generated by the coordinates of the point $P_{|S}=[A,\iota_{|S},\mathcal{L}]$ on the Hilbert-Blumenthal variety $\mathcal{H}_S/\mathbb{Q}$ that solves the coarse moduli problem of classifying abelian varieties of dimension $2n$ with multiplication by S.

Along the same lines, the field of moduli k_{R_F} of the central endomorphisms of A is the extension $\mathbb{Q}(P_{|R_F})$ of $\mathbb{Q}$ generated by the coordinates of the point $P_{|R_F}=[A,\iota_{|R_F},\mathcal{L}]$ on the Hilbert-Blumenthal variety $\mathcal{H}_F/\mathbb{Q}$ which solves the coarse moduli problem of classifying abelian varieties of dimension $2n$ with multiplication by R_F.

The tool for studying the Galois extensions $k_\mathcal{O}/k_S/k_{R_F}$ is provided by the forgetful modular maps

$$\begin{array}{rccccc}\pi_F: & X_{\mathcal{O},\mu} & \xrightarrow{\pi_S} & \mathcal{H}_S & \longrightarrow & \mathcal{H}_F\\ & P & \mapsto & P_{|S} & \mapsto & P_{|R_F}.\end{array}$$

It was shown in [16] that the morphisms π_F and π_S have finite fibres. Furthermore, it was proved in [16] that:

(i) There is a birational equivalence $b_S: X_{\mathcal{O},\mu}/V_0(S)\xrightarrow{\sim}\pi_{S,\varphi}(X_{\mathcal{O},\mu})$ and a commutative diagram

$$\begin{array}{rccc}\pi_S: & X_{\mathcal{O},\mu} & \longrightarrow & \mathcal{H}_S,\\ & {\scriptstyle\pi_S}\searrow & & \nearrow{\scriptstyle b_S}\\ & & X_{\mathcal{O},\mu}/V_0(S) & \end{array}$$

where $p_S: X_{\mathcal{O},\mu}\to X_{\mathcal{O},\mu}/V_0(S)$ is the natural projection.

(ii) There is a birational equivalence $b_S : X_{\mathcal{O},\mu}/V_0(S) \xrightarrow{\sim} \pi_{S,\varphi}(X_{\mathcal{O},\mu})$ and a commutative diagram

$$\begin{array}{ccccc} \pi_F : & X_{\mathcal{O},\mu} & & \longrightarrow & \mathcal{H}_F, \\ & & \overset{\pi_F}{\searrow} & & \overset{b_F}{\nearrow} \\ & & & X_{\mathcal{O},\mu}/W_0 & \end{array}$$

where $p_F : X_{\mathcal{O},\mu} \to X_{\mathcal{O},\mu}/W_0$ is the natural projection.

We say that a closed point $[A, \iota, \mathcal{L}]$ in $X_{\mathcal{O},\mu}$ or in any quotient of it is a *Heegner point* if $\mathrm{End}(A) \supsetneq \iota(\mathcal{O})$. It was also shown in [16] that the morphisms b_F and b_S are biregular on $X_{\mathcal{O},\mu}/W_0$ and $X_{\mathcal{O},\mu}/V_0(S)$, respectively, outside a finite set of Heegner points.

It follows from these facts that the Galois group $G = \mathrm{Gal}(k_{\mathcal{O}}/k_{R_F})$ of the extension of fields of moduli $k_{\mathcal{O}}/k_{R_F}$ is naturally embedded in W_0: any $\sigma \in G$ acts on a principally polarized abelian variety with quaternionic multiplication $(A, \iota : \mathcal{O} \xrightarrow{\simeq} \mathrm{End}_{\overline{\mathbb{Q}}}(A), \mathcal{L})$ by leaving the $\overline{\mathbb{Q}}$-isomorphism class of $\pi_F(A, \iota, \mathcal{L}) = (A, \iota_{|R_F} : R_F \hookrightarrow \mathrm{End}_{\overline{\mathbb{Q}}}(A), \mathcal{L})$ invariant.

Similarly, $\mathrm{Gal}(k_{\mathcal{O}}/k_S)$ embeds in $V_0(S)$ for any totally real order S embedded in $\mathcal{O}$. In what follows, we will describe the structure of the groups W_0 and $V_0(S)$ attached to a polarized order $(\mathcal{O}, \mu)$. This will automatically yield Theorem 2.3. In fact, in Propositions 3.4 and 3.8, we will be able to conclude a rather more precise statement than the one given in Section 2.

The next proposition shows that the situation is simplified considerably in the non-twisting case.

Proposition 3.4. *Let $(A, \mathcal{L})$ be a principally polarized abelian variety over $\overline{\mathbb{Q}}$ with quaternionic multiplication by $\mathcal{O}$. Let $\iota : \mathcal{O} \simeq \mathrm{End}(A)$ be any fixed isomorphism and let $\mu \in \mathcal{O}$ be such that $\mu^2 + D = 0$ for some $D \in F_+^*$, $\mathrm{disc}(B) = (D)$, and $\iota(\beta)^* = \iota(\mu^{-1}\bar{\beta}\mu)$ for all $\beta \in \mathcal{O}$.*

If $(\mathcal{O}, \mu)$ is a non twisting polarized order, then $k_{\mathcal{O}} = k_S$ for any totally real quadratic order $S \subset \mathcal{O}$ over R_F and

$$\mathrm{Gal}(k_{\mathcal{O}}/k_{R_F}) \subseteq C_2^{\omega_{odd}}.$$

Proof. It is clear from definition 3.2 that the groups of twisting involutions $V_0(S)$ are trivial for any subring S of $\mathcal{O}$. Since $\mathrm{Gal}(k_{\mathcal{O}}/k_S) \subseteq V_0(S)$, this yields the first part of the proposition. As for the second, since $\mathrm{Gal}(k_{\mathcal{O}}/k_{R_F}) \subseteq W_0$, we have that the Galois group $\mathrm{Gal}(k_{\mathcal{O}}/k_{R_F})$ is contained in $U_0 \subseteq W^1$, which is a 2-torsion abelian finite group. Our claim now follows from the following lemma, which holds true for arbitrary pairs $(\mathcal{O}, \mu)$. □

Lemma 3.5. *Let $(\mathcal{O}, \mu)$ be a principally polarized maximal order. Then $U_0 \simeq C_2^{\omega_{odd}}$.*

Proof. Let us identify $F(\mu)$ and $F(\sqrt{-D})$ through any fixed isomorphism. As U_0 naturally embeds in $F(\sqrt{-D})^*/F^*\Omega$, we first show that the maximal 2-torsion subgroup H of $F(\sqrt{-D})^*/F^*\Omega$ is isomorphic to $C_2^{\omega_{odd}}$.

If $\omega \in F(\sqrt{-D})^*$ generates a subgroup of $F(\sqrt{-D})^*/F^*\Omega$ of order 2, then $\omega^2 = \lambda\xi$ for some root of unity $\xi \in \Omega$ and $\lambda \in F^*$. In particular, note that if $\omega \in F(\sqrt{-D})^*$, then $\omega^2 \in F^*$ if and only if $\omega \in F^* \cup F^*\sqrt{-D}$. Let us write $\bar{H} = H/\langle\sqrt{-D}\rangle$.

We then have that, if $\xi \in \Omega$, there exists at most a single subgroup $\langle\omega\rangle \subseteq \bar{H}$ such that $\omega \in F(\sqrt{-D})^*$, $\omega^2 \in F^*\xi$. Indeed, if ω_1, $\omega_2 \in F(\sqrt{-D})$, $\omega_i^2 = \lambda_i\xi$ for some $\lambda_i \in F^*$ then $\frac{\omega_1}{\omega_2}^2 \in F^*$ and hence $\frac{\omega_1}{\omega_2} \in F^* \cup F^*\sqrt{-D}$. This shows that $[\omega_1] = [\omega_2] \in \bar{H}$.

Observe further that, if $\xi_f \in \Omega$ is a root of unity of odd order $f \geq 3$, then $\omega = \xi_f^{\frac{f+1}{2}} \in F(\sqrt{-D})^*$ generates a 2-torsion subgroup of $F(\sqrt{-D})^*/F^*\Omega$ such that $\omega^2 = \xi_f$.

It thus suffices to show that $\bar{\bar{H}} = H/\langle\sqrt{-D}, \{\xi_f^{\frac{f+1}{2}}\}_{f\geq 3 \text{ odd}}\rangle$ is trivial. Let $\omega \in F(\sqrt{-D})^*$, $\omega^2 = \lambda\xi$, ξ a root of unity of primitive order $f \geq 1$. If f is 2 or odd we already know that the class $[\omega] \in \bar{\bar{H}}$ is trivial. Further, it can exist no $\xi \in F(\sqrt{-D})$ of order $f = 2^N$, $N \geq 2$, because otherwise $\xi^{2^{N-1}}$ would be a square root of -1 and we would have that $F(\sqrt{-D}) = F(\sqrt{-1})$. This is a contradiction since $DR_F = \wp_1 \cdot \ldots \cdot \wp_{2r}$, $r > 0$.

Finally, it is also impossible that there should exist $\omega \in F(\sqrt{-D})$, $\omega^2 = \lambda\xi$, $\xi^f = 1$, $f = 2^N f_0$ with $N \geq 1$ and $f_0 \geq 3$ odd. Indeed, since in this case $\xi' = \xi^{2^N} \in F(\sqrt{-D})$ is a primitive root of unity of order f_0, $\omega' = \xi^{\frac{f_0+1}{2}}$ satisfies $\omega'^2 = \xi'$. Then we would have $\frac{\omega'}{\omega}^2 = (\xi^{2^{N-1}})\xi$ and this would mean that $[\frac{\omega'}{\omega}] = [\omega] \in \bar{H}$, which is again a contradiction. This shows that $\bar{\bar{H}}$ is trivial and therefore $H = \langle\sqrt{-D}, \{\xi_f^{\frac{f+1}{2}}\}_{\xi_f \in \Omega_{odd}}\rangle$. In order to conclude the lemma, we only need to observe that both μ and $\xi_f^{\frac{f+1}{2}} \in F(\mu)$ normalize the maximal order $\mathcal{O}$ for any odd f, because their respective reduced norms divide the discriminant D. □

Corollary 3.6. *Let $(\mathcal{O}, \mu)$ be a non-twisting polarized order and assume that $F(\sqrt{-D})$ is a CM-field with no purely imaginary roots of unity. Then, for any real quadratic order S over R_F, $k_\mathcal{O}/k_{R_F} = k_S/k_{R_F}$ is at most a quadratic extension.*

If, in addition, k_{R_F} admits a real embedding, then $k_\mathcal{O}$ is a totally imaginary quadratic extension of k_{R_F}.

Proof. The first part follows directly from the above. As for the second, it follows from a theorem of Shimura [18] which asserts that the Shimura varieties $X_{\mathcal{O},\mu}$ fail to have real points and hence the fields $k_\mathcal{O}$ are purely imaginary. □

However, if on the other hand $(\mathcal{O}, \mu)$ is twisting, the situation is more subtle and less homogenous as we now show.

Lemma 3.7. *Let $(\mathcal{O},\mu)$ be a* twisting *order in a totally indefinite quaternion algebra B over F of discriminant* $\mathrm{disc}(B)=(D)$, *$D\in F_+^*$. Then $U_0\subset V_0$ is a subgroup of V_0 and $V_0/U_0\simeq U_0$. In particular, $W_0=V_0\simeq C_2^{2\omega_{odd}}$.*

Proof. Let $\omega\in U_0$ be represented by an element $\omega\in \mathrm{N}_{F(\mu)^*}(\mathcal{O})\cap\mathcal{O}$ and let $\nu\in V_0$ be a twisting involution. We know that the class of ν in $\mathrm{N}_{B^*}(\mathcal{O})/F^*\mathcal{O}^*$ is represented by a twist $\chi\in \mathrm{N}_{B^*}(\mathcal{O})\cap\mathcal{O}$ that satisfies $\chi^2+\mathrm{n}(\chi)=0$ and $\mu\chi=-\chi\mu$. Then we claim that $\omega\nu\in V_0$ is again a twisting involution of $(\mathcal{O},\mu)$. Indeed, first $\omega\chi\in \mathrm{N}_{B^*}(\mathcal{O})\cap\mathcal{O}$, because both ω and χ do. Second, since $\omega\in F(\mu)$, $\mu(\omega\chi)=\mu\omega\chi=\omega\mu\chi=-\omega\chi\mu=-(\omega\chi)\mu$ and finally, we have $\mathrm{tr}(\mu(\omega\chi))=\mu\omega\chi+\bar\omega\bar\chi\bar\mu=\mu\omega\chi-\bar\omega\bar\chi\mu=-\mathrm{tr}\omega\chi\mu\in F$ and thus $\mathrm{tr}(\omega\chi)=0$.

This produces a natural action of U_0 on the set of twisting involutions of $(\mathcal{O},\mu)$ which is free simply because B is a division algebra. In order to show that it is transitive, let χ_1, χ_2 be two twists. Then $\omega=\chi_1\chi_2^{-1}\in F(\mu)$ because $\mu\omega=\mu\chi_1\chi_2^{-1}=-\chi_1\mu\chi_2^{-1}=\chi_1\chi_2^{-1}\mu=\omega\mu$ and $F(\mu)$ is its own commutator subalgebra of B; further $\omega\in \mathrm{N}_{B^*}(\mathcal{O})$ because its reduced norm is supported at the ramifying prime ideals $\wp\mid\mathrm{disc}(B)$. Let us remark that, in the same way, $\chi_1\chi_2\in \mathrm{N}_{F(\mu)^*}(\mathcal{O})$.

We are now in a position to prove the lemma. Let $\nu\in V_0$ be a fixed twisting involution. Then $U_0\subset V_0$: for any $\omega\in U_0$ we have already shown that $\omega\nu$ is again a twisting involution and hence $(\omega\nu)\nu=\omega\in V_0$ because V_0 is a 2-torsion abelian group. In addition, the above discussion shows that any element of V_0 either belongs to U_0 or is a twisting involution and that there is a non-canonical isomorphism $V_0/U_0\simeq U_0$. □

Observe that in the twisting case, by the above lemma, U_0 acts freely and transitively on the set of twisting involutions of W^1 with respect to $(\mathcal{O},\mu)$.

Proposition 3.8. *Let $(A,\mathcal{L})$ be a principally polarized abelian variety over $\overline{\mathbb{Q}}$ with quaternionic multiplication by $\mathcal{O}$. Let $\iota:\mathcal{O}\simeq\mathrm{End}(A)$ be any fixed isomorphism and let $\mu\in\mathcal{O}$ be such that $\mu^2+D=0$ for some $D\in F_+^*$,* $\mathrm{disc}(B)=(D)$, *and $\iota(\beta)^*=\iota(\mu^{-1}\bar\beta\mu)$ for all $\beta\in\mathcal{O}$.*

If $(\mathcal{O},\mu)$ is a twisting polarized order, let χ_1, ..., $\chi_{s_0}\in\mathcal{O}$ be representatives of the twists of $(\mathcal{O},\mu)$ up to multiplication by elements in F^*. Then,

(i) *For any real quadratic order S, $S\not\subset F(\chi_i)$, $1\le i\le s_0$,*

$$k_{\mathcal{O}}=k_S$$

(ii) *For any real quadratic order $S\subset F(\chi_i)\cap\mathcal{O}$, $1\le i\le s_0$, $k_{\mathcal{O}}/k_{S_i}$ is (at most) a quadratic extension.*

(iii) $k_{\mathcal{O}}=k_{S_1}\cdot\ldots\cdot k_{S_{s_0}}$ *and* $\mathrm{Gal}(k_{\mathcal{O}}/k_{R_F})\subseteq C_2^{2\omega_{odd}}$.

Proof. If $S\not\subset F(\chi_i)$ for any $i=1,...,s_0$, then $V_0(S)$ is trivial and hence, since $\mathrm{Gal}(k_{\mathcal{O}}/k_S)\subseteq V_0(S)$, $\mathrm{Gal}(k_{\mathcal{O}}/k_S)$ is also trivial. If, on the other hand, $S\subseteq F(\chi_i)\cap\mathcal{O}$, then $V_0(S)\simeq C_2$ is generated by the twisting involution associated to χ_i. Again, we deduce that in this case $k_{\mathcal{O}}/k_S$ is at most a quadratic extension.

With regard to the last statement, note that $U_0 \supseteq \langle [\mu] \rangle$ is at least of order 2. Thus, if $(\mathcal{O}, \mu)$ is a twisting polarized order, it follows from Lemma 3.4 that there exist two non-commuting twists χ, $\chi' \in \mathcal{O}$. Then $R_F[\chi, \chi']$ is a suborder of $\mathcal{O}$ and, since they both generate B over $\mathbb{Q}$, the fields of moduli $k_{\mathcal{O}}$ and $k_{R_F[\chi,\chi']}$ are the same. This shows that $k_{\mathcal{O}} \subseteq k_{S_1} \cdot ... \cdot k_{S_{s_0}}$. The converse inclusion is obvious.

Finally, we deduce that $k_{\mathcal{O}}/k_{R_F}$ is a $(2, ..., 2)$-extension of degree at most $2^{2\omega_{odd}}$ from Lemma 3.7. □

Remark 3.9. In the twisting case, the field of moduli of quaternionic multiplication is already generated by the field of moduli of any maximal real commutative multiplication but for finitely many exceptional cases. This homogeny does not occur in the non-twisting case.

In view of corollaries 3.4 and 3.8, the shape of the fields of moduli of the endomorphisms of the polarized abelian variety $(A, \mathcal{L})$ differs considerably depending on whether it gives rise to a twisting polarized order $(\mathcal{O}, \mu)$ or not.

For a maximal order $\mathcal{O}$ in a totally indefinite quaternion algebra B of principal reduced discriminant $D \in F_+^*$, it is then obvious to ask the questions whether

(i) There exists $\mu \in \mathcal{O}$, $\mu^2 + D = 0$ such that $(\mathcal{O}, \mu)$ is twisting and,
(ii) If $(\mathcal{O}, \mu)$ is twisting, what is its twisting group V_0.

Both questions are particular instances of the ones considered in the appendix at the end of the article.

4. Fields of moduli versus fields of definition

In dimension 2, the results of the previous sections are particularly neat and can be made more complete. Let $C/\overline{\mathbb{Q}}$ be a smooth irreducible curve of genus 2 and let $(J(C), \Theta_C)$ denote its principally polarized Jacobian variety. Assume that $\mathrm{End}_{\overline{\mathbb{Q}}}(J(C)) = \mathcal{O}$ is a maximal order in an (indefinite) quaternion algebra B over $\mathbb{Q}$ of reduced discriminant $D = p_1 \cdot ... \cdot p_{2r}$. Recall that $\mathcal{O}$ is unique up to conjugation or, equivalently by the Skolem-Noether Theorem, up to isomorphism.

Attached to $(J(C), \Theta_C)$ is the polarized order $(\mathcal{O}, \mu)$, where $\mu = c_1(\Theta_C) \in \mathcal{O}$ is a pure quaternion of reduced norm D. As we have seen, a necessary condition for $(\mathcal{O}, \mu)$ to be twisting is that $B \simeq (\frac{-D,m}{\mathbb{Q}})$ for some $m \mid D$. The isomorphism occurs if and only if for any odd ramified prime $p \mid D$, m is not a square mod p if $p \nmid m$ (respectively D/m if $p \mid m$).

In the rational case, the Atkin-Lehner and the positive Atkin-Lehner groups coincide and $W = W^1 = \{\omega_d; d \mid D\} \simeq C_2^{2r}$ is generated by elements $\omega_d \in \mathcal{O}$, $\mathrm{n}(\omega_d) = d \mid D$. Moreover, $U_0 = \langle \omega_D \rangle \simeq C_2$.

If $(\mathcal{O}, \mu)$ is a non twisting polarized order, then the field of moduli of quaternionic multiplication $k_{\mathcal{O}}$ is at most a quadratic extension over the field of moduli k_C of the curve C by Proposition 3.4. Moreover, $k_{\mathcal{O}} = k_S$ for any real quadratic order $S \subset \mathcal{O}$.

On the other hand, if $(\mathcal{O},\mu)$ is twisting and $B=(\frac{-D,m}{\mathbb{Q}})$ for $m \mid D$, then $V_0=\{1,\omega_m,\omega_{D/m},\omega_D\}\simeq C_2^2$, where we can choose representatives ω_m, $\omega_{D/m}$ in $\mathcal{O}$ such that $\mu\omega_m=-\omega_m\mu$ and $\mu\omega_{D/m}=-\omega_{D/m}\mu$. Note that, up to multiplication by non zero rational numbers, ω_m and $\omega_{D/m}$ are the only twists of $(\mathcal{O},\mu)$. When we particularize Proposition 3.8 to the case of Jacobian varieties of curves of genus 2, we obtain the following

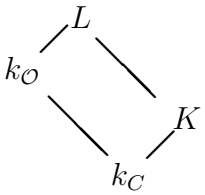
Theorem 4.1. *Let $C/\overline{\mathbb{Q}}$ be a smooth irreducible curve of genus 2 such that $\mathrm{End}_{\overline{\mathbb{Q}}}(J(C))=\mathcal{O}$ is a maximal order in a rational quaternion division algebra B of reduced discriminant D. Assume that the polarized order $(\mathcal{O},\mu)$ attached to $(J(C),\Theta_C)$ is twisting and let $m \mid D$ be such that $B\simeq(\frac{-D,m}{\mathbb{Q}})$. Then*

(i) *$k_{\mathcal{O}}/k_C$ is at most a quartic abelian extension.*
(ii) *$k_{\mathcal{O}}=k_S$ for any real quadratic order $S\not\subset\mathbb{Q}(\omega_m)\simeq\mathbb{Q}(\sqrt{m})$ or $\mathbb{Q}(\omega_{D/m})\simeq\mathbb{Q}(\sqrt{D/m})$.*
(iii) *$k_{\mathbb{Z}[\omega_m]}$ and $k_{\mathbb{Z}[\omega_{D/m}]}$ are at most quadratic extensions of k_C and these are such that $k_{\mathcal{O}}=k_{\mathbb{Z}[\omega_m]}\cdot k_{\mathbb{Z}[\omega_{D/m}]}$.*

In [11], Mestre studied the relation between the field of moduli $k_C=k_{J(C),\Theta_C}$ of a curve of genus 2 and its possible fields of definition, under the sole hypothesis that the hyperelliptic involution is the only automorphism on the curve. Mestre constructed an obstruction in $\mathrm{Br}_2(k_C)$ for C to be defined over its field of moduli. On identifying this obstruction with a quaternion algebra H_C over k_C, he showed that C admits a model over a number field K, $k_C\subseteq K$, if and only if $H_C\otimes K\simeq \mathrm{M}_2(K)$.

If $\mathrm{Aut}(C)\supsetneq C_2$, Cardona [1] has recently proved that C always admits a model over its field of moduli k_C.

Assume now, as in the theorem above, that $\mathrm{End}_{\overline{\mathbb{Q}}}(J(C))\simeq\mathcal{O}$ is a maximal order in a quaternion division algebra B over $\mathbb{Q}$. Let K be a field of definition of C; note that, since $\mathrm{End}_{\overline{\mathbb{Q}}}(J(C))\otimes\mathbb{Q}=B$ is division, $\mathrm{Aut}(C)\simeq C_2$ and therefore k_C does not need to be a possible field of definition of the curve. Having made the choice of a model C/K, there is a minimal (Galois) field extension L/K of K such that $\mathrm{End}_L(J(C))\simeq\mathcal{O}$. This gives rise to a diagram of Galois extensions



The nature of the Galois extensions L/K was studied in [4] and [5], while the relation between the field of moduli $k_{\mathcal{O}}$ and the possible fields of definition L of the quaternionic multiplication was investigated by Jordan in [10]. In the next

proposition we recall some of these facts, and we prove that L is the compositum of K and the field of moduli $k_{\mathcal{O}}$.

Proposition 4.2. [1]

Let C/K be a smooth curve of genus 2 over a number field K and assume that $\mathrm{End}_{\overline{\mathbb{Q}}}(J(C))$ is a maximal quaternionic order $\mathcal{O}$. Let L/K the minimal extension of K over which all endomorphisms of $J(C)$ are defined. Then

(i) $\mathrm{Gal}(L/K) \simeq \{1\}$, C_2 *or* $D_2 = C_2 \times C_2$.
(ii) $B \otimes_{\mathbb{Q}} L \simeq \mathrm{M}_2(L)$ *and* $L = k_{\mathcal{O}} \cdot K$.

Proof. Statement (i) was proved in [4]. As for (ii), let M be any number field. Jordan proved in [10] that the pair $(J(C), \mathrm{End}(J(C)))$ admits a model over M if and only if M contains $k_{\mathcal{O}}$ and M splits B. Since A is defined over K and all its endomorphisms are defined over L, we obtain that $L \supseteq k_{\mathcal{O}} \cdot K$ and $B \otimes_{\mathbb{Q}} L \simeq \mathrm{M}_2(L)$.

Let us now show that $L = k_{\mathcal{O}} \cdot K$. By (i), $\mathrm{Gal}(L/k_{\mathcal{O}} \cdot K) \subseteq \mathrm{Gal}(L/K) \subseteq D_2$. Assume on the contrary that $L \supsetneq k_{\mathcal{O}} \cdot K$; we will encounter a contradiction. Let $\sigma \in \mathrm{Gal}(L/k_{\mathcal{O}} \cdot K)$, $\sigma \neq 1$, be such that $\sigma^2 = 1$. Since A is defined over K, and according to the definition of $k_{\mathcal{O}}$, there exists an automorphism ϕ of the polarized abelian variety $(A, \mathcal{L})$ such that $\alpha^\sigma \cdot \phi = \phi \cdot \alpha$ for any $\alpha \in \mathcal{O} = \mathrm{End}_L(A)$. Let L^σ denote the fixed field of L by σ. By [4], Theorem 1.3, $\mathrm{End}_{L^\sigma}(A) \otimes \mathbb{Q} \simeq \mathbb{Q}(\sqrt{m})$ for $m = -D$ or a positive divisor $m \mid D$, $m \neq 1$. More precisely, as it is explained in Section 2 of [4], $\mathrm{End}_{L^\sigma}(A) \otimes \mathbb{Q} = \mathbb{Q}(\gamma)$ for some $\gamma \in B^*$, $\gamma^2 = m$, such that $\alpha^\sigma = \gamma^{-1}\alpha\gamma$ for all $\alpha \in \mathcal{O}$.

Hence, $\alpha^\sigma \cdot \phi = \phi \cdot \alpha \Leftrightarrow \gamma^{-1}\alpha\gamma \cdot \phi = \phi \cdot \alpha$. For $\alpha = \gamma$ we obtain that $\gamma\phi = \phi\gamma$ and hence $\phi \in \mathbb{Q}(\gamma) \simeq \mathbb{Q}(\sqrt{m})$.

By the Skolem-Noether theorem, there exists $\alpha \in \mathcal{O}$ such that $\alpha\gamma = -\gamma\alpha$. For such an element α, we obtain from the above equality that $\phi\gamma = -\gamma\phi$. Since we also know that $\phi \in \mathbb{Q}(\gamma)$, it follows that $\phi \in \mathbb{Q} \cdot \gamma$. This enters in contradiction with the fact that ϕ is an automorphism. □

Example 4.3. Let C be the smooth projective curve of hyperelliptic model

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

Let $A = J(C)/K$ be the Jacobian variety of C over $K = \mathbb{Q}(\sqrt{-3})$. By [9], A is an abelian surface with quaternionic multiplication by a maximal order in the quaternion algebra of discriminant 10^2. As it is explicitly shown in [9], there is an isomorphism between C and the conjugated curve C^τ over $\mathbb{Q}$. Hence, the field of moduli $k_C = \mathbb{Q}$ is the field of rational numbers. By applying the algorithm proposed

[1] Erratum: In the official published version, the statement of Proposition 4.2 and its proof are incorrect. I heartily thank Hakan Granath for pointing out to me the mistakes. In the present version of the article, I have restated Proposition 4.2 and provided a new proof for it.

[2] In the published version, there is a misprint: I wrongly claimed the discriminant to be 6.

by Mestre in [11], we also obtain that the obstruction H_C for C to admit a model over $\mathbb{Q}$ is not trivial. Hence $K = \mathbb{Q}(\sqrt{-3})$ is a minimal field of definition for C, though C also admits a model over any other quadratic field K' that splits H_C.

In addition, it was shown in [4] that $L = \mathbb{Q}(\sqrt{-3}, \sqrt{-11})/K$ is the minimal field of definition of the quaternionic endomorphisms of A. By a result of Shimura, Shimura curves fail to have rational points over real fields. Hence, $k_{\mathcal{O}}$ must be a subfield of L that does not admit a real embedding. By Proposition 4.2, $L = k_{\mathcal{O}}(\sqrt{-3})$ and thus $k_{\mathcal{O}}$ is either $\mathbb{Q}(\sqrt{-11})$ or L itself. It would be interesting to determine which of these two fields is $k_{\mathcal{O}}$.[3]

5. Appendix: Integral quaternion basis and distance ideals

A quaternion algebra over a field F is a central simple algebra B over F of $\mathrm{rank}_F(B) = 4$. However, there are several classical and more explicit ways to describe them which we now review. Indeed, if L is a quadratic separable algebra over the field F and $m \in F^*$ is any non zero element, then the algebra $B = L + Le$ with $e^2 = m$ and $e\beta = \beta^\sigma e$ for any $\beta \in L$, where σ denotes the non-trivial involution on L, is a quaternion algebra over F. The classical notation for it is $B = (L, m)$. Conversely, any quaternion algebra over F is of this form ([21]).

In addition, if $\mathrm{char}(F) \neq 2$, then

$$B = \left(\frac{a, b}{F}\right) = F + Fi + Fj + Fij,$$

with $ij = -ji$ and $i^2 = a \in F$, $j^2 = b \in F$ for any two elements a, $b \in F^*$ is again a quaternion algebra over F and again any quaternion algebra admits such a description. Note that the constructions are related since $B = (\frac{a,b}{F}) = (F(i), b)$.

On a quaternion algebra B there is a canonical anti-involution $\beta \mapsto \bar{\beta}$ which is characterized by the fact that, when restricted to any embedded quadratic subalgebra $L \subset B$ over F, it coincides with the non-trivial F-automorphism of L. Thus, if $B = (L, m)$, then $\bar{\beta} = \overline{\beta_1 + \beta_2 e} = {\beta_1}^\sigma - {\beta_2}^\sigma e$. The reduced trace and norm on B are defined by $\mathrm{tr}(\beta) = \beta + \bar{\beta}$ and $\mathrm{n}(\beta) = \beta\bar{\beta}$.

Assume that F is either a global or a local field of $\mathrm{char}(F) \neq 2$ and let it be the field of fractions of a Dedekind domain R_F. An order $\mathcal{O}$ in a quaternion algebra B is an R_F-finitely generated subring such that $\mathcal{O} \cdot F = B$. Elements $\beta \in \mathcal{O}$ are roots of the monic polynomial $x^2 - \mathrm{tr}(\beta)x + \mathrm{n}(\beta)$, $\mathrm{tr}(\beta)$, $\mathrm{n}(\beta) \in R_F$. We are now able to formulate the following question.

Question: Let B be a quaternion algebra over a global or local field F, $\mathrm{char}\,(F) \neq 2$, and let $\mathcal{O}$ be an order in B.

[3] In the published version, I claimed that $k_{\mathcal{O}} = \mathbb{Q}(\sqrt{-11})$. This followed from the incorrect statement of Proposition 4.2.

(1) If $B \simeq (\frac{a,b}{F})$ for some $a, b \in R_F$, can one find integral elements ι, $\eta \in \mathcal{O}$ such that $\iota^2 = a$, $\eta^2 = b$, $\iota\eta = -\eta\iota$?
(2) If $B \simeq (L, m)$ for a quadratic separable algebra over F and $m \in R_F$, can one find $\chi \in \mathcal{O}$ such that $\chi^2 = m$, $\chi\beta = \bar{\beta}\chi$ for any $\beta \in L$?

We note that Question 2 may be considered as a refinement of Question 1. Indeed, let $\mathcal{O}$ be an order in $B = (\frac{a,b}{F})$ and fix an arbitrary element $i \in \mathcal{O}$ such that $i^2 = a$. Then, while Question 1 asks whether there exist arbitrary elements ι, $\eta \in \mathcal{O}$ such that $\iota^2 = a$, $\eta^2 = b$ and $\iota\eta = -\eta\iota$, Question 2 wonders whether such an integral basis exists with $\eta = i$.

If $B = \left(\frac{a,b}{F}\right) = F + Fi + Fj + Fij$, let $\mathcal{O}_0 = R_F[i, j]$. Obviously, Question 1 is answered positively whenever $\gamma^{-1}\mathcal{O}\gamma \supseteq \mathcal{O}_0$ for some $\gamma \in B^*$. The following proposition asserts that this is actually a necessary condition. Although it is not stated in this form in [3], it is due to Chinburg and Friedman, and follows from the ideas therein. It is a consequence of Hilbert's Satz 90. Let us agree to say that two orders $\mathcal{O}$, $\mathcal{O}'$ of B are of the same *type* if $\mathcal{O} = \gamma^{-1}\mathcal{O}'\gamma$ for some $\gamma \in B^*$.

Proposition 5.1. *Let $B = F + Fi + Fj + Fij = \left(\frac{a,b}{F}\right)$ with a, $b \in R_F$. Let $\mathcal{O}_0 = R_F[i, j]$.*

An order $\mathcal{O}$ in B contains a basis ι, $\eta \in \mathcal{O}$, $\iota^2 = a$, $\eta^2 = b$, $\iota\eta = -\eta\iota$ of B if, and only if, the type of $\mathcal{O}_0$ is contained in the type of $\mathcal{O}$.

Proof. Assume that there exist ι, $\eta \in \mathcal{O}$ satisfying the above relations. By the Skolem-Noether Theorem ([21]), j and η are conjugated (by, say, $\alpha \in B^*$). Thus, by replacing i by $\alpha^{-1}i\alpha$ and $\mathcal{O}_0$ by $\alpha^{-1}\mathcal{O}_0\alpha$, we may assume that $j = \eta \in \mathcal{O}$. We then need to show the existence of an element $\gamma \in F(j) = F(\eta)$ such that $\gamma^{-1}\iota\gamma = i$.

We have $i\eta = -\eta i$ and thus $\eta = -i^{-1}\eta i$. In addition, since $\iota\eta = -\eta\iota$, $\iota i^{-1}\eta i = \eta\iota$. Hence, $(\iota i^{-1})\eta = \eta(\iota i^{-1})$ and we deduce that $\iota i^{-1} \in F(\eta)$ is an element of norm $\mathrm{N}_{F(\eta)/F}(\iota i^{-1}) = 1$.

By Hilbert's Satz 90, there exists $\omega \in F(\eta)$ such that $\iota i^{-1} = \omega\bar{\omega}^{-1}$, that is, $\iota = \omega\bar{\omega}^{-1}i$. Stated in this form, we need to find an element $\gamma \in F(\eta)$ with $\gamma^{-1}\omega\bar{\omega}^{-1}i\gamma = i$. Since $\gamma i = i\bar{\gamma}$, we can choose $\gamma = \omega$. □

An order $\mathcal{O}$ in B is *maximal* if it is not properly contained in any other. It is an *Eichler order* if it is the intersection of two maximal orders. The reduced discriminant ideal of an Eichler order is $\mathrm{disc}(\mathcal{O}) = \mathrm{disc}(B) \cdot \mathcal{N}$ for some integral ideal $\mathcal{N}$ of F, the *level* of $\mathcal{O}$, coprime to $\mathrm{disc}(B)$ (see [21], p. 39). With this notation, maximal orders are Eichler orders of level 1.

Corollary 5.2. *Assume that F is a local field and that $\mathcal{O}$ is an Eichler order of level $\mathcal{N}$ in $B = (\frac{a,b}{F})$, a, $b \in R_F$. Then, there exist ι, $\eta \in \mathcal{O}$, $\iota^2 = a$, $\eta^2 = b$, $\iota\eta = -\eta\iota$ if and only if $\mathcal{N} \mid 4ab$.*

Proof. By [21], §2, there is only one type of Eichler orders of fixed level $\mathcal{N}$ in B. Remark that, if B is division, necessarily $\mathcal{N} = 1$. Let $\mathcal{O}_0 = R_F[i, j]$. Since $\mathrm{disc}(\mathcal{O}_0) = 4ab$, as one can check, a necessary and sufficient condition on $\mathcal{O}$ to contain a conjugate order of $\mathcal{O}_0$ is that $\mathcal{N} \mid 4ab$. The corollary follows from proposition 5.1. □

In the global case, the approach to Question 1 can be made more effective under the assumption that B satisfies the Eichler condition. Namely, suppose that some archimedean place v of F does not ramify in B, that is, $B \otimes_F F_v \simeq \mathrm{M}_2(F_v)$. Here, we let $F_v \simeq \mathbb{R}$ or $\mathbb{C}$ denote the completion of F at v.

The following theorem of Eichler describes the set $\mathcal{T}(\mathcal{N})$ of types of Eichler orders of given level $\mathcal{N}$ purely in terms of the arithmetic of F. Let $\mathrm{Pic}_+(F)$ be the narrow class group of F of fractional ideals up to principal fractional ideals (a) generated by elements $a \in F^*$ such that $a > 0$ at any real archimedean place v that ramifies in B and let $h_+(F) = |\mathrm{Pic}_+(F)|$.

Definition 5.3. The group $\overline{\mathrm{Pic}}_+^{\mathcal{N}}(F)$ is the quotient of $\mathrm{Pic}_+(F)$ by the subgroup generated by the squares of fractional ideals of F, the prime ideals $\wp$ that ramify in B and the prime ideals $\mathfrak{q}$ such that $\mathcal{N}$ has odd $\mathfrak{q}$-valuation.

The group $\overline{\mathrm{Pic}}_+^{\mathcal{N}}(F)$ is a 2-torsion finite abelian group. Therefore, if $h_+(F)$ is odd, then $\overline{\mathrm{Pic}}_+^{\mathcal{N}}(F)$ is trivial.

Proposition 5.4 ([6], [7], [21], p. 89)**.** *The reduced norm* n *induces a bijection of sets*

$$\mathcal{T}(\mathcal{N}) \xrightarrow{\sim} \overline{\mathrm{Pic}}_+^{\mathcal{N}}(F).$$

The bijection is not canonical in the sense that it depends on the choice of an arbitrary Eichler order $\mathcal{O}$ in B. For $\mathcal{N} = 1$, the bijection is explicitly described as follows. For any two maximal orders $\mathcal{O}$, $\mathcal{O}'$ of B over R_F, define the *distance ideal* $\rho(\mathcal{O}, \mathcal{O}')$ to be the order-ideal of the finite R_F-module $\mathcal{O}/\mathcal{O} \cap \mathcal{O}'$ ([14], p. 49). Alternatively, $\rho(\mathcal{O}, \mathcal{O}')$ can also be defined locally in terms of the local distances between $\mathcal{O} \otimes_{R_F} R_{F_\wp}$ and $\mathcal{O}' \otimes_{R_F} R_{F_\wp}$ in the Bruhat-Tits tree $\mathcal{T}_\wp$ for any (non-archimedean) prime ideal $\wp$ of F that does not ramify in B ([2]). Finally, $\rho(\mathcal{O}, \mathcal{O}')$ is also the *level* of the Eichler order $\mathcal{O} \cap \mathcal{O}'$. This notion of distance proves to be suitable to classify the set of types of maximal orders of B, as the assignation $\mathcal{O}' \mapsto \rho(\mathcal{O}, \mathcal{O}')$ induces the bijection claimed in proposition 5.4.

Corollary 5.5. *Let $B = \left(\frac{a,b}{F}\right)$, a, $b \in R_F$ be a quaternion algebra over a global field F. If B satisfies Eichler's condition and $h_+(F)$ is odd then, for any Eichler order $\mathcal{O}$ in B, there is an integral basis ι, $\eta \in \mathcal{O}$, $\iota^2 = a$, $\eta^2 = b$, $\iota\eta = -\eta\iota$ of B.*

As for Question 2, let $B = F + Fi + Fj + Fij = \left(\frac{a,b}{F}\right) = (L, b)$ with a, $b \in R_F$ and $L = F(\sqrt{a})$. Choose an arbitrary order $\mathcal{O}$ of B. For given $\eta \in \mathcal{O}$, $\eta^2 = a$,

we ask whether there exists $\chi \in \mathcal{O}$, $\chi^2 = b$, such that $\eta\chi = -\eta\chi$. By proposition 5.1, a necessary condition is that $\mathcal{O}_0 = R_F[i,j] \subseteq \mathcal{O}$ up to conjugation by elements of B^* and, without loss of generality, we assume that this is the case. With these notations, we have

Definition 5.6. Let $\mathcal{O} \supseteq \mathcal{O}'$ be two arbitrary orders in B. The transportator of $\mathcal{O}'$ into $\mathcal{O}$ over B^* is $(\mathcal{O} : \mathcal{O}') := \{\gamma \in B^*, \gamma^{-1}\mathcal{O}_0\gamma \subset \mathcal{O}\}$.

Note that $\mathrm{N}_{B^*}(\mathcal{O})$ is a subgroup of finite index of $(\mathcal{O} : \mathcal{O}')$.

Proposition 5.7. *Let $\mathcal{O} \supseteq \mathcal{O}_0$ be an order in B and let $\eta \in \mathcal{O}$, $\eta^2 = a$. Then, there exists $\chi \in \mathcal{O}$, $\chi^2 = b$, $\eta\chi = -\chi\eta$ if and only if $\eta = \gamma^{-1}i\gamma$ for $\gamma \in (\mathcal{O} :_{B^*} \mathcal{O}_0)$.*

Let $f = |(\mathcal{O} : \mathcal{O}_0) : \mathrm{N}_{B^*}(\mathcal{O})|$ be the index of the normalizer group $\mathrm{N}_{B^*}(\mathcal{O})$ in $(\mathcal{O} : \mathcal{O}_0)$. Let $\mathcal{E}(a)$ be the finite set of $\mathrm{N}_{B^*}(\mathcal{O})$-conjugation classes of elements $\eta \in \mathcal{O}$ such that $\eta^2 = a$. Then, it follows from the above proposition that Question 2 for $(\mathcal{O}, \eta)$ is answered in the affirmative for elements η lying on exactly f of the conjugation classes in $\mathcal{E}(a)$. Again, the cardinality of $\mathcal{E}(a)$ can be explicitly computed in many cases in terms of class numbers by means of the theory of Eichler optimal embeddings (cf. [21]).

Acknowledgements. I am indebted to P. Bayer for her assistance throughout the elaboration of this work. I also express my gratitude to E. Friedman, J. Brzezinski, H. Granath and A. Arenas for some helpful conversations. Finally, I thank J. Kramer and U. Kuehn for their warm hospitality at the Humboldt-Universität zu Berlin during the fall of 2001.

References

[1] G. Cardona, *On the number of curves of genus 2 over finite fields*, Finite Fields and Their Applications (4) **9** (2003), 505-526.
[2] T. Chinburg, E. Friedman, An embedding theorem for quaternion algebras, *J. London Math. Soc.* **(2) 60** (1999), 33-44.
[3] T. Chinburg, E. Friedman, Hilbert symbols, class groups and quaternion algebras, *J. Théor. Nombres Bordeaux* **12** (2000), 367-377.
[4] L. Dieulefait, V. Rotger, The arithmetic of QM-abelian surfaces through their Galois representations, *J. Algebra* **281** (2004), 124-143.
[5] L. Dieulefait, V. Rotger, On abelian surfaces with potential quaternionic multiplication, to appear in *Bull. Belg. Math. Soc.*
[6] M. Eichler, Bestimmung der Idealklassenzahl in gewissen normalen einfachen Algebren, *J. Reine Angew. Math.* **176** (1937), 192-202.
[7] M. Eichler, Über die Idealklassenzahl hypercomplexer Systeme, *Math. Z.* **43** (1938), 481-494.
[8] S. Galbraith, V. Rotger, Easy Decision Diffie-Hellmann groups, *London Mathematical Society J. Comput. Math.* **7** (2004), 201-218.
[9] K. Hashimoto, N. Murabayashi, Shimura curves as intersections of Humbert surfaces and defining equations of QM-curves og genus two, *Tôhoku Math. J.* **47** (1995), 271-296.
[10] B.W. Jordan, Points on Shimura curves rational over number fields, *J. Reine Angew. Math.* **371** (1986), 92-114.

[11] J. F. Mestre, Construction de courbes de genre 2 à partir de leurs modules, *Effective methods in algebraic geometry* (Castiglioncello, 1990), Progr. Math. **94**, Birkhäuser Boston, Boston, MA, (1991), 313-334.
[12] J. S. Milne, Points on Shimura varieties mod p, *Proc. Symp. Pure Math.* **33** (1979), 165-184.
[13] D. Mumford, *Abelian varieties,* Tata Institute of Fundamental Research, Bombay, Oxford University Press, 1970.
[14] I. Reiner, *Maximal orders*, Academic Press, London, 1975.
[15] V. Rotger, Quaternions, polarizations and class numbers, *J. Reine Angew. Math.* **561** (2003), 177-197.
[16] V. Rotger, Modular Shimura varieties and forgetful maps, *Trans. Amer. Math. Soc.* **356** (2004), 1535-1550.
[17] V. Rotger, Shimura curves embedded in Igusa's threefold, *Modular curves and Abelian varieties*, Progress in Mathematics **224** Birkhäuser, (2003), 263-273.
[18] G. Shimura, On analytic families of polarized abelian varieties and automorphic functions, *Ann. Math.* **78** (1963), 149-192.
[19] G. Shimura, On the field of rationality for an abelian variety, *Nagoya Math. J.* **45** (1972), 161-178.
[20] A. Silverberg, Fields of definition for homomorphisms of abelian varieties, *J. Pure and Applied Algebra* **77** (1992), 253-262.
[21] M.F. Vignéras, *Arithmétique des algèbres de quaternions*, Lect. Notes Math. **800**, 1980.

Escola Universitària Politècnica de Vilanova i la Geltrú, Av. Víctor Balaguer s/n, E-08800 Vilanova i la Geltrú, Spain
E-mail address: vrotger@mat.upc.es