IJMMS 2004:52, 2795–2808
PII. S0161171204302243
http://ijmms.hindawi.com

THE FIELD OF MODULI OF QUATERNIONIC MULTIPLICATION ON ABELIAN VARIETIES

VICTOR ROTGER

Received 25 February 2003

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.

2000 Mathematics Subject Classification: 11G18, 14G35.

1. Introduction. Let $\bar{\mathbb{Q}}$ be an algebraic closure of the field $\mathbb{Q}$ of rational numbers and let $(A,\mathcal{L})/\bar{\mathbb{Q}}$ be a nonzero 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 (see [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, from Albert's classification of involuting division algebras (see [13]) and the work of Shimura [18], it is known that there are other rings that can occur as the endomorphism ring of an abelian variety. Namely, if $A/\overline{\mathbb{Q}}$ is simple, $\mathrm{End}(A)$ may be 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.

We recall that a quaternion algebra B over a totally real field F is called *totally indefinite* if $B \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathrm{M}_2(\mathbb{R}) \times \cdots \times \mathrm{M}_2(\mathbb{R})$ and *totally definite* if $B \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{H} \times \cdots \times \mathbb{H}$, where $\mathbb{H} = (-1,-1/\mathbb{R})$ 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

$$\begin{array}{ccc} A & \longrightarrow & A^\sigma \\ {\scriptstyle\beta}\downarrow & & \downarrow{\scriptstyle\beta^\sigma} \\ A & \longrightarrow & A^\sigma \end{array} \tag{1.1}$$

for any $\beta \in S$.

We remark that, as a consequence of the very basic definitions, when $S = \mathbb{Z}$, we have $k_S = k_{A,\mathscr{L}}$. But in the case that $\mathrm{End}(A) \supsetneq \mathbb{Z}$, little is known on the chain of Galois extensions $k_{\mathrm{End}(A)} \supseteq k_S \supseteq k_{A,\mathscr{L}}$.

The main aim of this paper 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 specialize our results to abelian surfaces. We use our results together with those of Mestre [12] and Jordan [11] to compare the field of moduli and field of definition of the quaternionic multiplication on an abelian surface.

In the appendix, we discuss a question on the arithmetic of quaternion algebras that naturally arises from our considerations and which is also related to the recent work by Chinburg and Friedman [3, 4].

A cryptographical application of the results in the appendix has been derived in [9] 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 will 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 $\Omega_{\mathrm{odd}}(L) = \{\xi \in R_L,\ \xi^f = 1,\ f \text{ odd}\}$ denote the set of roots of unity of odd order in L. We let $\omega_{\mathrm{odd}}(L) = |\Omega_{\mathrm{odd}}(L)|$. 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 $\mathrm{End}(A) \simeq \mathcal{O}$ and $\dim(A) = 2n$.

Proposition 2.2. [15] *Let $(A,\mathscr{L})$ 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 $B \simeq (-D, m/F)$ for some $m \in F_+^*$ supported at the prime ideals $\wp \mid D$ of F. The main result of this paper 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 $\operatorname{disc}(B)=D$ for some $D\in F_+^*$. Let $\omega_{\mathrm{odd}}=\omega_{\mathrm{odd}}(F(\sqrt{-D}))$.*

(i) *If B is not twisting, then*
  (1) *for any totally real quadratic order $S\subset\mathcal{O}$ over R_F, $k_{\mathcal{O}}=k_S$,*
  (2) $\mathrm{Gal}(k_{\mathcal{O}}/k_{R_F})$ *is an elementary abelian 2-group of rank at most ω_{odd}.*

(ii) *If B is twisting, then*
  (1) *for any totally real quadratic order $S\subset\mathcal{O}$, $\mathrm{Gal}(k_{\mathcal{O}}/k_S)$ is either trivial or of order two,*
  (2) $\mathrm{Gal}(k_{\mathcal{O}}/k_{R_F})$ *is an elementary abelian 2-group of rank at most $2\omega_{\mathrm{odd}}$.*

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 $\operatorname{disc}(B)=(D)$ for some $D\in F_+^*$. Let $\mathrm{n}:B\to F$ denote the reduced norm on B. Let $\mathcal{O}$ be a maximal order in B and fix a quaternion $\mu\in\mathcal{O}$ satisfying $\mu^2+D=0$. Its existence is guaranteed by Eichler's theory on optimal embeddings (see [1, 22]) 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 $(\mathcal{O},\mu)$, a Shimura variety $X_{\mathcal{O},\mu}/\mathbb{Q}$ that is associated to the coarse moduli problem of classifying triplets $(A,\iota,\mathcal{L})$ over $\mathbb{Q}$ can be considered, where

(i) $(A,\mathcal{L})$ is a principally polarized abelian variety,

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

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

$$W=\frac{\mathrm{N}_{B^*}(\mathcal{O})}{F^*\mathcal{O}^*}. \tag{3.1}$$

The group W is isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\overset{2r}{\dots}\times\mathbb{Z}/2\mathbb{Z}$, where $2r=\sharp\{\wp\mid\operatorname{disc}(B)\}$ is the number of ramifying prime ideals of B (cf. [16, 22]).

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 $X_{\mathcal{O},\mu}$.

The group W^1 is an elementary abelian 2-group of rank s for some $2r\le s\le n+2r-1$.

The first inequality holds because there is a natural map $W^1\twoheadrightarrow W$ which is an epimorphism of groups due to the 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 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 $\operatorname{disc}(B)=(D)$, $D\in F_+^*$.

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

$$B = F + F\mu + F\chi + F\mu\chi = \left(\frac{-D, -\mathrm{n}(\chi)}{F}\right). \tag{3.2}$$

If χ is a twist of $(\mathbb{O},\mu)$ and $S \subset \mathbb{O}$ is a subring, χ is said to be a twist of $(\mathbb{O},\mu)$ in S if $\chi \in S$.

We say that $(\mathbb{O},\mu)$ is *twisting* if it admits some twist in $\mathbb{O}$ 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 $(\mathbb{O},\mu)$. It is a twisting involution in $S \subseteq \mathbb{O}$ 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 $(\mathbb{O},\mu)$ in S and simply write V_0 for $V_0(\mathbb{O})$.

We remark that, since B is totally indefinite, no $\chi \in B_+^*$ can be a twist of $(\mathbb{O},\mu)$ because a necessary condition for $B \simeq (-D, -\mathrm{n}(\chi)/F)$ 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 $B \simeq (-D, m/F)$ for some element $m \in F_+^*$ supported at the prime ideals $\wp \mid D$ (i.e., $v_\wp(m) \neq 0$ only if $\wp \mid D$).

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

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

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

The motivation for introducing the Shimura variety $X_{\mathbb{O},\mu}$ and the above Atkin-Lehner groups in this paper is that this introduction gives a modular interpretation of the field of moduli $k_{\mathbb{O}}$ of the quaternionic multiplication on A such that $k_{\mathbb{O}} = \mathbb{Q}(P)$ is the extension over $\mathbb{Q}$ generated by the coordinates of the point $P = [A, \iota, \mathscr{L}]$ on Shimura's canonical model $X_{\mathbb{O},\mu}/\mathbb{Q}$ 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 $S = L \cap \mathbb{O}$ is an order of L over R_F which is optimally embedded in $\mathbb{O}$. 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 $P_{|S} = [A, \iota_{|S}, \mathscr{L}]$ on the Hilbert-Blumenthal variety $\mathscr{H}_S/\mathbb{Q}$ 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

$$\begin{aligned} \pi_F : X_{\mathcal{O},\mu} \xrightarrow{\pi_S} \mathcal{H}_S \longrightarrow \mathcal{H}_F, \\ P \mapsto P_{|S} \mapsto P_{|R_F}. \end{aligned} \tag{3.3}$$

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 are a birational equivalence $b_S : X_{\mathcal{O},\mu}/V_0(S) \xrightarrow{\sim} \pi_S(X_{\mathcal{O},\mu})$ and a commutative diagram

$$\begin{array}{ccc} \pi_S : X_{\mathcal{O},\mu} & \longrightarrow & \mathcal{H}_S \\ & {\scriptstyle p_S} \searrow \quad \nearrow {\scriptstyle b_S} & \\ & X_{\mathcal{O},\mu}/V_0(S) & \end{array} \tag{3.4}$$

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

(ii) there are a birational equivalence $b_F : X_{\mathcal{O},\mu}/W_0 \xrightarrow{\sim} \pi_F(X_{\mathcal{O},\mu})$ and a commutative diagram

$$\begin{array}{ccc} \pi_F : X_{\mathcal{O},\mu} & \longrightarrow & \mathcal{H}_F \\ & {\scriptstyle p_F} \searrow \quad \nearrow {\scriptstyle b_F} & \\ & X_{\mathcal{O},\mu}/W_0 & \end{array} \tag{3.5}$$

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 such that 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 nontwisting 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 nontwisting polarized order, then $k_{\mathcal{O}}=k_S$ for any totally real quadratic order $S\subset\mathcal{O}$ over R_F and $\mathrm{Gal}(k_{\mathcal{O}}/k_{R_F})$ is an elementary abelian 2-group of rank at most ω_{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 all pairs $(\mathcal{O},\mu)$. □

Lemma 3.5. *Let $(\mathcal{O},\mu)$ be a principally polarized maximal order. Then U_0 is an elementary abelian 2-group of rank ω_{odd}.*

Proof. We 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 $(\mathbb{Z}/2\mathbb{Z})^{\omega_{\mathrm{odd}}}$.

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 $\omega\in F^*\cup F^*\sqrt{-D}$. We write $\bar{H}=H/\langle\sqrt{-D}\rangle$. We then have that, if $\xi\in\Omega$, there exists at most one subgroup $\langle\omega\rangle\subseteq\bar{H}$ such that $\omega\in F(\sqrt{-D})^*$, $\omega^2\in F^*\xi$. Indeed, if $\omega_1,\omega_2\in F(\sqrt{-D})$, $\omega_i^2=\lambda_i\xi$ for some $\lambda_i\in F^*$, then $(\omega_1/\omega_2)^2\in F^*$, and hence $\omega_1/\omega_2\in F^*\cup F^*\sqrt{-D}$. 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 $\omega=\xi_f^{(f+1)/2}\in F(\sqrt{-D})^*$ generates a 2-torsion subgroup of $F(\sqrt{-D})^*/F^*\Omega$ such that $\omega^2=\xi_f$.

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

Finally, it is also impossible that there exist $\omega\in F(\sqrt{-D})$, $\omega^2=\lambda\xi$, $\xi^f=1$, $f=2^Nf_0$ with $N\geq 1$ and $f_0\geq 3$ odd. Indeed, in this case, ξ^{f_0} is a root of unity of order 2^N, hence, by the argument in the previous paragraph, $N=1$. Let $\xi'=\xi^2$ and $\omega'=\xi^{(f_0+1)/2}$ so that ξ' is a root of unity of order f_0 and $\omega'^2=\xi'$. Then $(\omega'/\omega)^2=\xi'/\lambda\xi=\xi/\lambda=(1/\lambda^2)\omega^2$. Hence $[\omega']=[\omega^2]=1\in\bar{H}$, which is a contradiction. This shows that $\bar{\bar{H}}$ is trivial, and therefore $H=\langle\sqrt{-D},\{\xi_f^{(f+1)/2}\}_{\xi_f\in\Omega_{\mathrm{odd}}}\rangle$. In order to conclude the lemma, we only need to observe that both μ and $\xi_f^{(f+1)/2}\in F(\mu)$ 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 nontwisting 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 proposition. As for the second, it follows from a result of Shimura (see [20, Theorem 0]) 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 $\operatorname{disc}(B) = (D)$, $D \in F_+^*$. Then $U_0 \subset V_0$ is a subgroup of V_0 and $V_0/U_0 \simeq U_0$. In particular, $W_0 = V_0 \simeq (\mathbb{Z}/2\mathbb{Z})^{2\omega_{\text{odd}}}$.*

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 $\mathrm{tr}(\mu(\omega\chi)) = \mu\omega\chi + \overline{\omega\chi}\bar{\mu} = \mu\omega\chi - \overline{\omega\chi}\mu = -\mathrm{tr}\omega\chi\mu \in F$, 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 $\wp \mid \operatorname{disc}(B)$. We 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 $U_0 \subset V_0$ such that 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 noncanonical 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 $D \in F_+^*$, $\operatorname{disc}(B) = (D)$, 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 $\chi_1, \ldots, \chi_{s_0} \in \mathcal{O}$ be representatives of the twists of $(\mathcal{O},\mu)$ up to multiplication by elements in F^*. Then,

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

$$k_{\mathcal{O}} = k_S, \tag{3.6}$$

(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) $k_{\mathcal{O}} = k_{S_1} \cdot \cdots \cdot k_{S_{s_0}}$ *and* $\mathrm{Gal}(k_{\mathcal{O}}/k_{R_F})$ *is an elementary abelian* 2*-group of rank at most* $2\omega_{\mathrm{odd}}$.

Proof. If $S \not\subset F(\chi_i)$ for any $i = 1,\dots,s_0$, 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 $V_0(S) \simeq \mathbb{Z}/2\mathbb{Z}$ 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 3.7 that there exist two noncommuting twists $\chi,\chi' \in \mathcal{O}$. 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 $k_{\mathcal{O}} \subseteq k_{S_1} \cdot \cdots \cdot k_{S_{s_0}}$. The converse inclusion is obvious.

Finally, we deduce that $k_{\mathcal{O}}/k_{R_F}$ is a $(2,\dots,2)$-extension of degree at most $2^{2\omega_{\mathrm{odd}}}$ 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 homogeneity does not occur in the nontwisting 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 normal to ask the following questions:

(i) whether there exists $\mu \in \mathcal{O}$, $\mu^2 + D = 0$, such that $(\mathcal{O},\mu)$ is twisting,

(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.

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 $D = p_1 \cdot \cdots \cdot p_{2r}$. 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 $B \simeq (-D,m/\mathbb{Q})$ 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 $p \nmid m$ (resp., D/m if $p \mid m$).

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

If $(\mathcal{O},\mu)$ is a nontwisting 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 Theorem 2.3.

On the other hand, if $(\mathcal{O},\mu)$ is twisting and $B = (-D, m/\mathbb{Q})$ for $m \mid D$, then $V_0 = \{1, \omega_m, \omega_{D/m}, \omega_D\} \simeq (\mathbb{Z}/2\mathbb{Z})^2$, 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 nonzero rational numbers, ω_m and $\omega_{D/m}$ are the only twists of $(\mathcal{O},\mu)$. When we specialize Theorem 2.3 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 indefinite quaternion division algebra B of reduced discriminant D.*

(i) *$k_{\mathcal{O}}/k_C$ is at most a quartic abelian extension.*

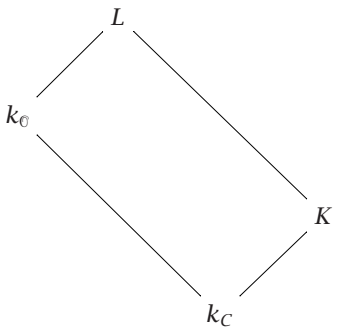
(ii) *$k_{\mathcal{O}} = k_S$ for any real quadratic order $S \not\subset \mathbb{Q}(\omega_m) \simeq \mathbb{Q}(\sqrt{m})$ or $\mathbb{Q}(\omega_{D/m}) \simeq \mathbb{Q}(\sqrt{D/m})$.*

(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 [12], 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 H_C in $\mathrm{Br}_2(k_C)$ for C to be defined over its field of moduli. If K is a number field, he showed that C admits a model over K if and only if K contains k_C and H_C lies in the kernel of the natural map $\mathrm{Br}(k_C) \to \mathrm{Br}(K)$.

If $\mathrm{Aut}(C) \supsetneq \mathbb{Z}/2\mathbb{Z}$, Cardona [2] has recently proved that C always admits a model over its field of moduli k_C.

Assume now, as in the above theorem, 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, $\mathrm{Aut}(C) \simeq \mathbb{Z}/2\mathbb{Z}$, 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, we obtain 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



(4.1)

The nature of the Galois extensions L/K was studied in [5, 6], 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 [11]. The combination of all these facts yields the following statement and recovers, in a weakened form, a result proved in [6].

Proposition 4.2. *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 be the minimal extension of K over which all endomorphisms of $J(C)$ are defined.*

Then $\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(k_{\mathcal{O}}/k_C) \simeq \{1\}, \mathbb{Z}/2\mathbb{Z}$ or $D_2 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Proof. Assume first that $k_C = K$ is a field of definition of the curve. Then $k_{\mathcal{O}} = L$ is a field of definition of all endomorphisms of $J(C)$ such that if it was not, there would be infinitely many pairwise different extensions L_α/K such that $\mathrm{End}_{L_\alpha}(J(C)) = \mathcal{O}$. This would contradict Silverberg's result that such an extension is uniquely determined (see [21]).

If, on the contrary, Mestre's obstruction H_C is nontrivial in $\mathrm{Br}_2(k_C)$, then C admits a model over any quadratic extension K/k_C that splits H_C but not over k_C itself. We then have that any field of definition L of all endomorphisms of $J(C)$ must be a quadratic extension of k_C that strictly contains it. Indeed, by [11], we know that $[L : k_C] \leq 2$. Suppose that $L = k_C$. Then, L would contain all fields of definition H of C and this is not possible.

In either case, the possibilities for $\mathrm{Gal}(L/K)$ are $\{1\}$, $\mathbb{Z}/2\mathbb{Z}$, and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ by Theorem 2.3. □

Remark 4.3. The above argument actually yields more than this: it either holds that $k_C \subsetneq K \subsetneq k_{\mathcal{O}} \subsetneq L$ is a chain of quadratic extensions or $L = k_{\mathcal{O}} \cdot K$. Moreover, the first of these possibilities only arises when $[L : K] = 4$ and for the finitely many subextensions K/k_C of $k_{\mathcal{O}}$ such that $H_C \otimes_{k_C} K$ is trivial.

Example 4.4. Let C be the smooth projective curve with hyperelliptic model

$$Y^2 = \frac{1}{48} X(9075X^4 + 3025(3 + 2\sqrt{-3})X^3 - 6875X^2 + 220(-3 + 2\sqrt{-3})X + 48). \tag{4.2}$$

Let $A = J(C)/K$ be the Jacobian variety of C over $K = \mathbb{Q}(\sqrt{-3})$.

By [10], A is an abelian surface with quaternionic multiplication by a maximal order in the quaternion algebra of discriminant 6. As it is shown explicitly in [10], 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.

In addition, it was shown in [6] that $L = \mathbb{Q}(\sqrt{-3}, \sqrt{-11})$ is the minimal field of definition of the quaternionic endomorphisms of A. By our last proposition and remark, we must have that $L = K \cdot k_{\mathcal{O}}$ with $[k_{\mathcal{O}} : k_C] = 2$. In addition, by Shimura's theorem asserting that such Shimura curves fail to have rational points over real fields, $k_{\mathcal{O}}$ must be an imaginary quadratic extension of $\mathbb{Q}$. This shows that $k_{\mathcal{O}} = \mathbb{Q}(\sqrt{-11})$ and the picture of fields of moduli and definition is completed.

Appendix.

Integral quaternion basis and distance ideals. A quaternion algebra over a field F is a central simple algebra B over F of $\operatorname{rank}_F(B) = 4$. However, there are several classical and more explicit ways to describe quaternion algebras, which we now review. Indeed, if L is a quadratic separable algebra over the field F and $m \in F^*$ is any nonzero 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 nontrivial 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 (see [22]).

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

$$B = \left(\frac{a,b}{F}\right) = F + Fi + Fj + Fij, \tag{A.1}$$

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 $B = (a, b/F) = (F(i), b)$.

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 nontrivial 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 $\operatorname{tr}(\beta) = \beta + \bar{\beta}$ and $\operatorname{n}(\beta) = \beta\bar{\beta}$.

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

Question A.1. Let B be a quaternion algebra over a global or local field F, $\operatorname{char}(F) \neq 2$, and let $\mathbb{O}$ be an order in B.

(1) If $B \simeq (a, b/F)$ for some $a, b \in R_F$, can one find integral elements $\iota, \eta \in \mathbb{O}$ 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 $\chi \in \mathbb{O}$ such that $\chi^2 = m$, $\chi\beta = \bar{\beta}\chi$ for any $\beta \in L$?

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

If $B = (a, b/F) = F + Fi + Fj + Fij$, let $\mathbb{O}_0 = R_F[i, j]$. Obviously, Question A.1(1) is answered positively whenever $\gamma^{-1}\mathbb{O}\gamma \supseteq \mathbb{O}_0$ 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 [4], it is due to Chinburg and Friedman and follows from the ideas therein. It is a consequence of Hilbert's Theorem 90. Let us agree to say that two orders $\mathbb{O}, \mathbb{O}'$ of B are of the same *type* if $\mathbb{O} = \gamma^{-1}\mathbb{O}'\gamma$ for some $\gamma \in B^*$.

Proposition A.2. *Let $B = F + Fi + Fj + Fij = (a,b/F)$ with $a,b \in R_F$. Let $\mathbb{O}_0 = R_F[i,j]$.*

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

Proof. Assume that there exist $\iota,\eta \in \mathbb{O}$ satisfying the above relations. By the Skolem-Noether theorem (see [22]), j and η are conjugated (by, say, $\alpha \in B^*$). Thus, by replacing i by $\alpha^{-1}i\alpha$ and $\mathbb{O}_0$ by $\alpha^{-1}\mathbb{O}_0\alpha$, we may assume that $j = \eta \in \mathbb{O}$. 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 Theorem 90, there exists $\omega \in F(\eta)$ such that $\iota i^{-1} = \omega\bar{\omega}^{-1}$, that is, $\iota = \omega\bar{\omega}^{-1}i$. We need to find an element $\gamma \in F(\eta)$ stated in this form with $\gamma^{-1}\omega\bar{\omega}^{-1}i\gamma = i$. Since $\gamma i = i\bar{\gamma}$, we can choose $\gamma = \omega$. □

An order $\mathbb{O}$ in B is *maximal* if it is not properly contained in any other order. It is an *Eichler order* if it is the intersection of two maximal orders. The reduced discriminant ideal of an Eichler order is $\mathrm{disc}(\mathbb{O}) = \mathrm{disc}(B)\cdot\mathcal{N}$ for some integral ideal $\mathcal{N}$ of F, the *level* of $\mathbb{O}$, coprime to $\mathrm{disc}(B)$ (see [1] and [22, page 39]). With this notation, maximal orders are Eichler orders of level 1.

Corollary A.3. *Assume that F is a local field and that $\mathbb{O}$ is an Eichler order of level $\mathcal{N}$ in $B = (a,b/F)$, $a,b \in R_F$. Then there exist $\iota,\eta \in \mathbb{O}$, $\iota^2 = a$, $\eta^2 = b$, $\iota\eta = -\eta\iota$ if and only if $\mathcal{N} \mid 4ab$.*

Proof. By [22, Section 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 $\mathbb{O}_0 = R_F[i,j]$. Since $\mathrm{disc}(\mathbb{O}_0) = 4ab$, as one can check, a necessary and sufficient condition for $\mathbb{O}$ to contain a conjugate order of $\mathbb{O}_0$ is that $\mathcal{N} \mid 4ab$. The corollary follows from Proposition A.2. □

In the global case, the approach to Question A.1(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 A.4. 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 A.5 (see [7, 8] and [22, page 89]). *The reduced norm* n *induces a bijection of sets*

$$\mathcal{T}(\mathcal{N}) \xrightarrow{\sim} \overline{\mathrm{Pic}}_{+}^{\mathcal{N}}(F). \tag{A.2}$$

The bijection is not canonical in the sense that it depends on the choice of an Eichler order $\mathbb{O}$ in B. For $\mathcal{N} = 1$, the bijection is described explicitly as follows. For any two maximal orders $\mathbb{O}$, $\mathbb{O}'$ of B over R_F, define the *distance ideal* $\rho(\mathbb{O},\mathbb{O}')$ to be the order ideal of the finite R_F-module $\mathbb{O}/\mathbb{O}\cap\mathbb{O}'$ (see [14, page 49]). Alternatively, $\rho(\mathbb{O},\mathbb{O}')$ can also be defined locally in terms of the local distances between $\mathbb{O}\otimes_{R_F} R_{F_\wp}$ and $\mathbb{O}'\otimes_{R_F} R_{F_\wp}$ in the Bruhat-Tits tree $\mathcal{T}_\wp$ for any (non-Archimedean) prime ideal $\wp$ of F that does not ramify in B (see [3]). Finally, $\rho(\mathbb{O},\mathbb{O}')$ is also the *level* of the Eichler order $\mathbb{O}\cap\mathbb{O}'$. This notion of distance proves to be suitable to classify the set of types of maximal orders of B, as the assignation $\mathbb{O}' \mapsto \rho(\mathbb{O},\mathbb{O}')$ induces the bijection claimed in Proposition A.5.

Corollary A.6. *Let $B = (a,b/F)$, $a,b \in R_F$, 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 $\mathbb{O}$ in B, there is an integral basis $\iota,\eta \in \mathbb{O}$, $\iota^2 = a$, $\eta^2 = b$, $\iota\eta = -\eta\iota$ of B.*

As for Question A.1(2), let $B = F + Fi + Fj + Fij = (a,b/F) = (L,b)$ with $a,b \in R_F$ and $L = F(\sqrt{a})$. Choose an order $\mathbb{O}$ of B. For a given $\eta \in \mathbb{O}$, $\eta^2 = a$, we ask whether there exists $\chi \in \mathbb{O}$, $\chi^2 = b$, such that $\eta\chi = -\eta\chi$. By Proposition A.2, a necessary condition is that $\mathbb{O}_0 = R_F[i,j] \subseteq \mathbb{O}$ up to conjugation by elements of B^* and, without loss of generality, we assume that this is the case. With these notations, we have the following.

Definition A.7. Let $\mathbb{O} \supseteq \mathbb{O}'$ be two orders in B. Define $(\mathbb{O}:\mathbb{O}') := \{\gamma \in B^*,\ \gamma^{-1}\mathbb{O}_0\gamma \subset \mathbb{O}\}$.

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

Proposition A.8. *Let $\mathbb{O} \supseteq \mathbb{O}_0$ be an order in B and let $\eta \in \mathbb{O}$, $\eta^2 = a$. Then there exists $\chi \in \mathbb{O}$, and $\chi^2 = b$, $\eta\chi = -\chi\eta$ if and only if $\eta = \gamma^{-1}i\gamma$ for $\gamma \in (\mathbb{O}:_{B^*}\mathbb{O}_0)$.*

Let $f = |(\mathbb{O}:\mathbb{O}_0) : \mathrm{N}_{B^*}(\mathbb{O})|$ be the index of the normalizer group $\mathrm{N}_{B^*}(\mathbb{O})$ in $(\mathbb{O}:\mathbb{O}_0)$. Let $\mathscr{C}(a)$ be the finite set of $\mathrm{N}_{B^*}(\mathbb{O})$-conjugation classes of elements $\eta \in \mathbb{O}$ such that $\eta^2 = a$. Then it follows from the above proposition that Question A.1(2) for $(\mathbb{O},\eta)$ is answered in the affirmative for elements η lying on exactly f of the conjugation classes in $\mathscr{C}(a)$. Again, the cardinality of $\mathscr{C}(a)$ can be computed explicitly in many cases in terms of class numbers by means of the theory of Eichler optimal embeddings (cf. [22]).

Acknowledgments. 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 and the referee for useful remarks. Finally, I thank J. Kramer and U. Kuehn for their warm hospitality at the Humboldt-Universität zu Berlin during the fall of 2001. This work was partially supported by DGICYT Grant BFM2003-06768-C02-02.

References

[1] M. Alsina and P. Bayer, *Quaternion Orders, Quadratic Forms, and Shimura Curves*, CRM Monograph Series, vol. 22, American Mathematical Society, Rhode Island, 2004.

[2] G. Cardona, *On the number of curves of genus 2 over a finite field*, Finite Fields Appl. **9** (2003), no. 4, 505–526.

[3] T. Chinburg and E. Friedman, *An embedding theorem for quaternion algebras*, J. London Math. Soc. (2) **60** (1999), no. 1, 33–44.

[4] ———, *Hilbert symbols, class groups and quaternion algebras*, J. Théor. Nombres Bordeaux **12** (2000), no. 2, 367–377.

[5] L. V. Dieulefait and V. Rotger, *On abelian surfaces with potential quaternionic multiplication*, to appear in Bull. Belg. Math. Soc.

[6] ———, *The arithmetic of QM-abelian surfaces through their Galois representations*, J. Algebra **281** (2004), 124–143.

[7] M. Eichler, *Bestimmung der Idealklassenzahl in gewissen normalen einfachen Algebren*, J. reine angew. Math. **176** (1937), 192–202 (German).

[8] ———, *Über die Idealklassenzahl hypercomplexer Systeme*, Math. Z. **43** (1938), 481–494 (German).

[9] S. Galbraith and V. Rotger, *Easy decision Diffie-Hellmann groups*, LMS J. Math. Comp. **7** (2004), 201–218.

[10] K. Hashimoto and N. Murabayashi, *Shimura curves as intersections of Humbert surfaces and defining equations of QM-curves of genus two*, Tohoku Math. J. (2) **47** (1995), no. 2, 271–296.

[11] B. W. Jordan, *Points on Shimura curves rational over number fields*, J. reine angew. Math. **371** (1986), 92–114.

[12] J. F. Mestre, *Construction de courbes de genre* 2 *à partir de leurs modules*, Effective Methods in Algebraic Geometry (Castiglioncello, 1990), Progr. Math., vol. 94, Birkhäuser Boston, Massachusetts, 1991, pp. 313–334.

[13] D. Mumford, *Abelian Varieties*, Tata Institute of Fundamental Research Studies in Mathematics, vol. 5, Oxford University Press, London, 1970.

[14] I. Reiner, *Maximal Orders*, Academic Press, London, 1975.

[15] V. Rotger, *Quaternions, polarization and class numbers*, J. reine angew. Math. **561** (2003), 177–197.

[16] ———, *Modular Shimura varieties and forgetful maps*, Trans. Amer. Math. Soc. **356** (2004), no. 4, 1535–1550.

[17] ———, *Shimura curves embedded in Igusa's threefold*, Modular Curves and Abelian Varieties, Progr. Math., vol. 224, Birkhäuser, Basel, 2004, pp. 263–276.

[18] G. Shimura, *On analytic families of polarized abelian varieties and automorphic functions*, Ann. of Math. (2) **78** (1963), 149–192.

[19] ———, *On the field of rationality for an abelian variety*, Nagoya Math. J. **45** (1972), 167–178.

[20] ———, *On the real points of an arithmetic quotient of a bounded symmetric domain*, Math. Ann. **215** (1975), 135–164.

[21] A. Silverberg, *Fields of definition for homomorphisms of abelian varieties*, J. Pure Appl. Algebra **77** (1992), no. 3, 253–262.

[22] M. F. Vignéras, *Arithmétique des Algèbres de Quaternions*, Lect. Notes in Math., vol. 800, Springer, Berlin, 1980.

Victor Rotger: Departament de Matemàtica Aplicada IV (EPSEVG), Universitat Politècnica de Catalunya, Av. Victor Balaguer s/n, 08800 Vilanova i la Geltrú, Spain

E-mail address: vrotger@mat.upc.es

Mathematical Problems in Engineering

Special Issue on Space Dynamics

Call for Papers

Space dynamics is a very general title that can accommodate a long list of activities. This kind of research started with the study of the motion of the stars and the planets back to the origin of astronomy, and nowadays it has a large list of topics. It is possible to make a division in two main categories: astronomy and astrodynamics. By astronomy, we can relate topics that deal with the motion of the planets, natural satellites, comets, and so forth. Many important topics of research nowadays are related to those subjects. By astrodynamics, we mean topics related to spaceflight dynamics.

It means topics where a satellite, a rocket, or any kind of man-made object is travelling in space governed by the gravitational forces of celestial bodies and/or forces generated by propulsion systems that are available in those objects. Many topics are related to orbit determination, propagation, and orbital maneuvers related to those spacecrafts. Several other topics that are related to this subject are numerical methods, nonlinear dynamics, chaos, and control.

The main objective of this Special Issue is to publish topics that are under study in one of those lines. The idea is to get the most recent researches and published them in a very short time, so we can give a step in order to help scientists and engineers that work in this field to be aware of actual research. All the published papers have to be peer reviewed, but in a fast and accurate way so that the topics are not outdated by the large speed that the information flows nowadays.

Before submission authors should carefully read over the journal's Author Guidelines, which are located at http://www.hindawi.com/journals/mpe/guidelines.html. Prospective authors should submit an electronic copy of their complete manuscript through the journal Manuscript Tracking System at http://mts.hindawi.com/ according to the following timetable:

Manuscript Due	July 1, 2009
First Round of Reviews	October 1, 2009
Publication Date	January 1, 2010

Lead Guest Editor

Antonio F. Bertachini A. Prado, Instituto Nacional de Pesquisas Espaciais (INPE), São José dos Campos, 12227-010 São Paulo, Brazil; prado@dem.inpe.br

Guest Editors

Maria Cecilia Zanardi, São Paulo State University (UNESP), Guaratinguetá, 12516-410 São Paulo, Brazil; cecilia@feg.unesp.br

Tadashi Yokoyama, Universidade Estadual Paulista (UNESP), Rio Claro, 13506-900 São Paulo, Brazil; tadashi@rc.unesp.br

Silvia Maria Giuliatti Winter, São Paulo State University (UNESP), Guaratinguetá, 12516-410 São Paulo, Brazil; silvia@feg.unesp.br