On the number of connected components of real abelian varieties that admit sufficiently many complex multiplications

J. Huisman*

1 Introduction

Let X be an algebraic variety over $\mathbb{R}$, that is, X is a geometrically integral, separated scheme of finite type over $\mathbb{R}$ [3]. Its set of real points $X(\mathbb{R})$ will be given the strong topology. It is well known that the number of connected components of $X(\mathbb{R})$ is finite [1]. If X is an abelian variety over $\mathbb{R}$, i.e., a complete algebraic group over $\mathbb{R}$ (in particular, $X(\mathbb{R})$ is non-empty), then the number of connected components of $X(\mathbb{R})$ is a power of 2, and is not greater than $2^{\dim X}$ [2]. For example, if X is a 1-dimensional abelian variety over $\mathbb{R}$, i.e., X is an elliptic curve over $\mathbb{R}$, then, either $X(\mathbb{R})$ is connected or $X(\mathbb{R})$ has 2 connected components. This can also easily be deduced from the fact that an elliptic curve over $\mathbb{R}$ is isomorphic, as an algebraic curve over $\mathbb{R}$, to a cubic curve in the projective plane $\mathbb{P}^2_{\mathbb{R}}$. Moreover, continuing our example, there is an interesting relationship between the number of connected components of $X(\mathbb{R})$ and arithmetical properties of the ring of endomorphisms $\mathrm{End}(X_{\mathbb{C}})$ of $X_{\mathbb{C}} = X \otimes_{\mathbb{R}} \mathbb{C}$, if $X_{\mathbb{C}}$ has complex multiplication. (Recall that an elliptic curve E over $\mathbb{C}$ has complex multiplication if $\mathrm{rank}(\mathrm{End}(E)) = 2$.) Indeed, using standard facts on elliptic curves (see [7]) and assuming that $\mathrm{End}(X_{\mathbb{C}})$ is a maximal order, it is not hard to prove that $X(\mathbb{R})$ necessarily is connected if the discriminant of $\mathrm{End}(X_{\mathbb{C}})$ is odd, while $X(\mathbb{R})$ necessarily is nonconnected if the discriminant of $\mathrm{End}(X_{\mathbb{C}})$ is divisible by 8. In the remaining case, that is, the

* Supported by the Netherlands Organisation for Scientific Research (NWO).

discriminant of $\mathrm{End}(X_{\mathbb{C}})$ is divisible by 4 and not by 8, nothing interesting can be said. (See also Example 2.8 where we prove these statements, as a consequence of our main result.)

The aim of this paper is to study the relationship between the number of connected components of $X(\mathbb{R})$ and arithmetical properties of $\mathrm{End}(X_{\mathbb{C}})$ for higher dimensional abelian varieties X over $\mathbb{R}$. We concentrate on abelian varieties X over $\mathbb{R}$ having the following three properties.

(i) X is absolutely simple, i.e., $X_{\mathbb{C}} = X \otimes_{\mathbb{R}} \mathbb{C}$ does not contain nontrivial complex abelian subvarieties.

(ii) X admits sufficiently many complex multiplications [5], i.e., the ring of endomorphisms $\mathrm{End}(X_{\mathbb{C}})$ of $X_{\mathbb{C}}$ has rank $2 \dim X$.

(iii) $\mathrm{End}(X_{\mathbb{C}})$ is a maximal order in the field $\mathrm{End}(X_{\mathbb{C}}) \otimes \mathbb{Q}$.

We will derive a formula for the number of connected components of $X(\mathbb{R})$ in terms of the $\mathrm{End}(X_{\mathbb{C}})$-module that defines X (Theorem 2.3). As a consequence, we will prove, among other things, that, for an abelian variety X over $\mathbb{R}$ satisfying the three conditions above, $X(\mathbb{R})$ is connected if the discriminant of $\mathrm{End}(X_{\mathbb{C}})$ over $\mathrm{End}(X)$ is prime to 2 (Corollary 2.10). On the other hand, we will prove that $X(\mathbb{R})$ has $2^{\dim X}$ connected components if the ramification of $\mathrm{End}(X_{\mathbb{C}})$ over $\mathrm{End}(X)$ is as wildly as possible at every prime ideal of $\mathrm{End}(X)$ dividing 2 (Corollary 2.12). Moreover, in the remaining cases $X(\mathbb{R})$ does not necessarily have 1 or $2^{\dim X}$ connected components. More precisely, suppose there exists a prime ideal $\mathfrak{p}$ of $\mathrm{End}(X)$ dividing 2 such that $\mathrm{End}(X_{\mathbb{C}})$ is ramified over $\mathrm{End}(X)$ at $\mathfrak{p}$, but not as wildly as possible. Then, there exists a real abelian variety Y satisfying the three conditions above with $\mathrm{End}(Y_{\mathbb{C}})$ isomorphic to $\mathrm{End}(X_{\mathbb{C}})$ such that the number of connected components of $Y(\mathbb{R})$ is neither equal to 1 nor to $2^{\dim Y}$.

2 Results

Let B be a ring and A a subring of B. Let $\mathcal{A}_{\mathbb{R}}(B/A)$ denote the set of (isomorphism classes of) absolutely simple abelian varieties X over $\mathbb{R}$ which admit sufficiently many complex multiplications such that

$$\mathrm{End}(X) \cong A \text{ and } \mathrm{End}(X_{\mathbb{C}}) \cong B.$$

2.1 Fact. The set $\mathcal{A}_{\mathbb{R}}(B/A)$ is nonempty if and only if the following three conditions hold.

(i) B is a commutative domain and finitely generated as a $\mathbb{Z}$-module.

(ii) The field of fractions L of B is a totally imaginary extension of a totally real field K, in particular, the field extension L/K is of degree 2.

(iii) $A = B \cap K$.

From this fact, on which we elaborate below, it easily follows that $X \in \mathcal{A}_{\mathbb{R}}(B/A)$ if and only if X is an absolutely simple abelian variety over $\mathbb{R}$ which admits sufficiently many complex multiplications and which has $\mathrm{End}(X_{\mathbb{C}})$ isomorphic to B. For, such an isomorphism automatically induces an isomorphism between $\mathrm{End}(X)$ and A.

Suppose, the rings A and B satisfy 2.1(i), 2.1(ii) and 2.1(iii). Then, L/K is a Galois extension. We denote its Galois group by G and we denote the nontrivial

element of G by σ. Furthermore, $B(G)$ will be the *twisted group ring*, i.e., $B(G)$ is the smallest subring of the ring $\mathrm{End}_A(B)$ of A-linear endomorphisms of B, containing B as well as G.

Then, one may construct abelian varieties $X \in \mathcal{A}_{\mathbb{R}}(B/A)$ in the following way. Choose a morphism of $\mathbb{R}$-algebras

$$\Phi\colon \mathbb{C} \longrightarrow \mathbb{R} \otimes B,$$

which does not factorize through $\mathbb{R} \otimes B' \to \mathbb{R} \otimes B$, for any proper subring B' of B. Such a morphism Φ will be called a *simple complex structure* on $\mathbb{R} \otimes B$. Moreover, choose a $B(G)$-module M which is projective of rank 1 as a B-module. Then,

$$V = \mathbb{R} \otimes M = (\mathbb{R} \otimes B) \otimes_B M$$

is a complex vector space via Φ and contains $\Lambda = 1 \otimes M$ as a lattice. Furthermore, G acts on V, where the action of σ is anti-$\mathbb{C}$-linear, and Λ is G-invariant. It is then a standard fact that there exist an absolutely simple abelian variety X over $\mathbb{R}$ and a G-equivariant isomorphism of complex Lie groups

$$X(\mathbb{C}) \longrightarrow V/\Lambda.$$

Moreover, X admits sufficiently many complex multiplications and $\mathrm{End}(X_{\mathbb{C}})$ is isomorphic to B. Therefore, $X \in \mathcal{A}_{\mathbb{R}}(B/A)$. Since the isomorphism class of X is uniquely determined by Φ and M, we denote X by $X_{\mathbb{R}}(M, \Phi)$.

Conversely, if $X \in \mathcal{A}_{\mathbb{R}}(B/A)$ then there exist a simple complex structure Φ on $\mathbb{R} \otimes B$ and a $B(G)$-module M which is B-projective of rank 1, such that

$$X_{\mathbb{R}}(M, \Phi) \cong X.$$

(For more details see [4].)

For technical reasons and because of Fact 2.1, we will assume throughout the paper the following.

2.2 Assumption. *The rings A and B satisfy 2.1(i), 2.1(ii) and 2.1(iii), and moreover, B is a maximal order (hence, A is one too), or equivalently, B is a Dedekind ring (and hence, A is Dedekind also).*

We will denote the different of B over A by $\mathfrak{D}$, and the discriminant of B over A by $\mathfrak{d}$ [6]. In our situation, $\mathfrak{D}$ is the ideal of B generated by $(1 - \sigma)(B)$. Recall that the ideal $\mathfrak{d}$ of A is equal to the norm $N_{L/K}(\mathfrak{D})$ of $\mathfrak{D}$ with respect to the extension L/K. Moreover, if $\mathfrak{P}$ is a nonzero prime ideal of B then, B is ramified over A at $\mathfrak{P}$ if and only if $\mathfrak{P}$ divides $\mathfrak{D}$. Hence, if $\mathfrak{p}$ is a nonzero prime ideal of A then, B is ramified over A at $\mathfrak{p}$ if and only if $\mathfrak{p}$ divides $\mathfrak{d}$.

It will be convenient to enumerate the set S of nonzero prime ideals $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ of A that divide the discriminant $\mathfrak{d}$ of B over A, in such a way that

$$\{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\} = \{\mathfrak{p} \in S \mid \mathfrak{p} \text{ divides } (2)\}$$

and

$$\{\mathfrak{p}_1, \ldots, \mathfrak{p}_\ell\} = \{\mathfrak{p} \in S \mid \mathfrak{p} \text{ divides } (2) \text{ and } \mathrm{ord}_{\mathfrak{p}}(\mathfrak{d}) \text{ is even}\},$$

where $0 \leq \ell \leq m$ and $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{d})$ is the greatest integer i such that $\mathfrak{p}^i \mid \mathfrak{d}$. We let $\mathfrak{P}_i$ be the unique prime ideal of B lying over $\mathfrak{p}_i$. Then, $\mathfrak{P}_i^2 = B\mathfrak{p}_i$, for $i = 1, \ldots, n$.

We will need the following notion. If M is a $B(G)$-module then the cokernel of the canonical mapping of B-modules

$$B \otimes_A (M^G) \longrightarrow M,$$

where $M^G = \{m \in M \mid \forall \tau \in G: \tau m = m\}$, will be called the *ramification module* of M and will be denoted by $\mathfrak{E}(M)$. If M is projective of rank 1 as a B-module then

$$\mathfrak{E}(M) \cong \bigoplus_{i=1}^{n} B/\mathfrak{P}_i^{\varepsilon_i}, \tag{$*$}$$

for some $\varepsilon_i \in \{0, 1\}$. For, we may assume M to be a $B(G)$-module of B. Then,

$$M = \prod \mathfrak{P}^{e_{\mathfrak{P}}},$$

where the product is taken over all nonzero prime ideals of B and where all but a finite number of the integers $e_{\mathfrak{P}}$ are zero. Since $\sigma M = M$, there exists an ideal $\mathfrak{a}$ of A such that

$$M = \mathfrak{a} \cdot \prod_{i=1}^{n} \mathfrak{P}_i^{e_i},$$

where $e_i = e_{\mathfrak{P}_i}$. Then,

$$M^G = \mathfrak{a} \cdot \prod_{i=1}^{n} \mathfrak{p}_i^{d_i},$$

where $d_i = \lfloor \frac{e_i+1}{2} \rfloor$, i.e., d_i is the integral part of $\frac{e_i+1}{2}$. Hence,

$$B \otimes_A (M^G) = \mathfrak{a} \cdot \prod_{i=1}^{n} B\mathfrak{p}_i^{d_i} = \mathfrak{a} \cdot \prod_{i=1}^{n} \mathfrak{P}_i^{2d_i}.$$

This proves $(*)$, taking $\varepsilon_i = 2d_i - e_i$.

Now, if M is a $B(G)$-module which is projective of rank 1 as a B-module then, it is easy to see that, $\mathfrak{E}(M) = 0$ if and only if there exists an A-module N such that $B \otimes_A N \cong M$, as $B(G)$-modules.

Let, for any B-module of finite length M, $\chi_B(M)$ be the ideal of B determined by the following properties (see [6] for more details).

(i) χ_B is multiplicative over short exact sequences of B-modules that are of finite B-length.

(ii) $\chi_B(B/\mathfrak{b}) = \mathfrak{b}$, for any nonzero ideal $\mathfrak{b}$ of B.

In particular, if $\mathfrak{b}$ is a nonzero ideal of B then, $\#(B/\mathfrak{b}) = |N(\mathfrak{b})|$, where the right-hand side is the unique positive rational integer that generates the absolute norm, i.e., the norm with respect to $L/\mathbb{Q}$, of the ideal $\mathfrak{b}$.

Now we can state our main theorem.

2.3 Theorem. *With notation as above. Let $X \in \mathcal{A}_{\mathbb{R}}(B/A)$, i.e., X is an absolutely simple abelian variety over $\mathbb{R}$, admitting sufficiently many complex multiplications with $\mathrm{End}(X) \cong A$ and $\mathrm{End}(X_{\mathbb{C}}) \cong B$. Then, the number of connected components of $X(\mathbb{R})$ is equal to*

$$\prod_{i=1}^{m} 2^{a_i f_i} \Big/ \prod_{i=1}^{\ell} 2^{\varepsilon_i f_i}, \qquad (**)$$

where $a_i = \left\lfloor \frac{\mathrm{ord}_{\mathfrak{p}_i}(\mathfrak{d})}{2} \right\rfloor$, $f_i = [k(\mathfrak{p}_i) : \mathbb{F}_2]$ and $\varepsilon_i = \mathrm{ord}_{\mathfrak{P}_i}(\chi_B(\mathfrak{E}(M)))$, for $i = 1, \ldots \ell$, where $k(\mathfrak{p}_i)$ is the residue field $A/\mathfrak{p}_i$, and, M is a $B(G)$-module, projective of rank 1 as a B-module, such that

$$X \cong X_{\mathbb{R}}(M, \Phi),$$

for some simple complex structure Φ on $\mathbb{R} \otimes B$.

2.4 Remark. Observe that the number of connected components of $X_{\mathbb{R}}(M, \Phi)(\mathbb{R})$ does not depend on Φ.

2.5 Remark. If a_i and f_i are as in Theorem 2.3 then, for any choice of $\varepsilon_i \in \{0, 1\}$, $i = 1, \ldots, \ell$, there exists an $X \in \mathcal{A}_{\mathbb{R}}(B/A)$ such that the number of connected components of $X(\mathbb{R})$ is equal to $(**)$. For, let

$$M = \prod_{i=1}^{\ell} \mathfrak{P}_i^{\varepsilon_i}.$$

Then, M is a $B(G)$-module and projective of rank 1 as a B-module. Choose any simple complex structure Φ on $\mathbb{R} \otimes B$. Then, $X = X_{\mathbb{R}}(M, \Phi)$ is an element of $\mathcal{A}_{\mathbb{R}}(B/A)$ and, according to Theorem 2.3, $X(\mathbb{R})$ has the required number of connected components.

2.6 Remark. It is not hard to see that, if $\mathfrak{p}$ is a nonzero prime ideal of A dividing the discriminant $\mathfrak{d}$ of B over A then

$$\begin{cases} 2 \leq \mathrm{ord}_{\mathfrak{p}}(\mathfrak{d}) \leq 2\mathrm{ord}_{\mathfrak{p}}(2) + 1, & \text{if } \mathfrak{p} \mid (2), \text{ and} \\ \mathrm{ord}_{\mathfrak{p}}(2) = 1, & \text{if } \mathfrak{p} \not\mid (2). \end{cases}$$

In particular, for any $X \in \mathcal{A}_{\mathbb{R}}(B/A)$ and with notation as in Theorem 2.3,

$$0 \leq \sum_{i=1}^{m} a_i f_i - \sum_{i=1}^{\ell} \varepsilon_i f_i \leq \sum_{i=1}^{m} \mathrm{ord}_{\mathfrak{p}_i}(2) \cdot f_i = [K : \mathbb{Q}] = \dim X,$$

since $\varepsilon_i = 0$ or 1. Hence, by Theorem 2.3, the number of connected components of $X(\mathbb{R})$ is greater than or equal to 1, and less than or equal to $2^{\dim X}$. This is in accordance with the general fact mentioned in the introduction.

Let γ be the integral-valued function on the set $\mathcal{A}_{\mathbb{R}}(B/A)$ defined by letting $\gamma(X)$ be the number of connected components of the set of real points $X(\mathbb{R})$ of X. From the general fact mentioned in the introduction it follows that

$$\gamma(\mathcal{A}_{\mathbb{R}}(B/A)) \subset \{1, 2, 2^2, \ldots, 2^g\},$$

where $2g = \mathrm{rank}(B)$.

2.7 Corollary. *Let $2g = \operatorname{rank}(B)$. Suppose that the principal ideal $\mathfrak{p} = (2)$ of A is a prime ideal. Let $X \in \mathcal{A}_{\mathbb{R}}(B/A)$. Then, either,*

(i) $\operatorname{ord}_{\mathfrak{p}}(\mathfrak{d}) = 0$, *in which case* $\gamma(\mathcal{A}_{\mathbb{R}}(B/A)) = \{1\}$, *in particular* $X(\mathbb{R})$ *is connected, or,*

(ii) $\operatorname{ord}_{\mathfrak{p}}(\mathfrak{d}) = 2$, *in which case* $\gamma(\mathcal{A}_{\mathbb{R}}(B/A)) = \{1, 2^g\}$, *in particular* $X(\mathbb{R})$ *is connected or has* 2^g *connected components, or,*

(iii) $\operatorname{ord}_{\mathfrak{p}}(\mathfrak{d}) = 3$, *in which case* $\gamma(\mathcal{A}_{\mathbb{R}}(B/A)) = \{2^g\}$, *in particular* $X(\mathbb{R})$ *has* 2^g *connected components.*

Proof. Follows from Remark 2.6, Theorem 2.3 and Remark 2.5. □

2.8 Example. Let us apply Corollary 2.7 to the case of elliptic curves over $\mathbb{R}$, i.e., abelian varieties over $\mathbb{R}$ of dimension 1. Let B be the ring of integers in the quadratic imaginary extension $L = \mathbb{Q}(\sqrt{d})$ of $\mathbb{Q}$, where d is square-free, and let $A = \mathbb{Z}$. Then,

$$\mathfrak{d} = \begin{cases} (d), & \text{if } d \equiv 1 \bmod 4, \\ (4d), & \text{if } d \not\equiv 1 \bmod 4. \end{cases}$$

If E is an elliptic curve over $\mathbb{R}$ with $\operatorname{End}(E_{\mathbb{C}}) \cong B$ then

(i) $E(\mathbb{R})$ is connected if $d \equiv 1 \bmod 4$,

(ii) $E(\mathbb{R})$ has 2 connected components if $d \equiv 2 \bmod 4$, and

(iii) $E(\mathbb{R})$ is connected or has 2 connected components otherwise.

To illustrate this let us give an example in each of the three cases.

In case (i), take $d = -3$. There are exactly 2 nonisomorphic elliptic curves over $\mathbb{R}$ admitting complex multiplication with $\frac{1}{2} + \frac{1}{2}\sqrt{-3}$. Namely, the curve given by the equation $y^2 = x^3 - 1$, which corresponds to the lattice $\mathbb{Z} + \mathbb{Z}(\frac{1}{2} + \frac{1}{2}\sqrt{-3})$, and the curve given by $y^2 = x^3 + 1$, which corresponds to the lattice $\mathbb{Z} + \mathbb{Z}(\frac{1}{2} + \frac{1}{6}\sqrt{-3})$. Indeed, both curves have a connected set of real points, as can be seen from the equation as well as from the lattice.

In case (ii), take $d = -2$ as an example. There are exactly 2 nonisomorphic elliptic curves over $\mathbb{R}$ admitting complex multiplication with $\sqrt{-2}$. Namely, the curve $y^2 = x(x^2 - 4x + 2)$, which corresponds to $\mathbb{Z} + \mathbb{Z}\sqrt{-2}$, and the curve $y^2 = x(x^2 + 4x + 2)$, which corresponds to $\mathbb{Z} + \mathbb{Z}\frac{1}{2}\sqrt{-2}$. Indeed, both curves have a set of real points consisting of 2 connected components.

Finally, in case (iii), take $d = -1$. There are, again, exactly 2 nonisomorphic elliptic curves over $\mathbb{R}$ admitting complex multiplication with $\sqrt{-1}$. Namely, the curve $y^2 = x^3 - x$, which corresponds to $\mathbb{Z} + \mathbb{Z}\sqrt{-1}$, and the curve $y^2 = x^3 + x$, which corresponds to $\mathbb{Z} + \mathbb{Z}(\frac{1}{2} + \frac{1}{2}\sqrt{-1})$. While the latter curve has a connected set of real points, the former curve has a set of real points consisting of 2 connected components.

2.9 Corollary. *The following conditions are equivalent.*

(i) For any $X, Y \in \mathcal{A}_{\mathbb{R}}(B/A)$, the sets $X(\mathbb{R})$ and $Y(\mathbb{R})$ have the same number of connected components.

(ii) $\operatorname{ord}_{\mathfrak{p}}(\mathfrak{d})$ *is odd, for each prime ideal* $\mathfrak{p}$ *dividing the discriminant* $\mathfrak{d}$ *of* B *over* A.

Proof. If $\operatorname{ord}_{\mathfrak{p}}(\mathfrak{d})$ is odd for all $\mathfrak{p} \mid \mathfrak{d}$ then $\ell = 0$, by definition of ℓ. It follows from Theorem 2.3 that, for any $X, Y \in \mathcal{A}_{\mathbb{R}}(B/A)$, the sets $X(\mathbb{R})$ and $Y(\mathbb{R})$ have the same number of connected components.

On the other hand, if there exists a nonzero prime ideal $\mathfrak{p}$ dividing $\mathfrak{d}$ with $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{d})$ even then, B is wildly ramified over $\mathfrak{p}$. Hence, $\mathfrak{p} \mid (2)$. Therefore, $\ell > 0$ and, according to Remark 2.5, there exist $X, Y \in \mathcal{A}_{\mathbb{R}}(B/A)$ such that the number of connected components of $X(\mathbb{R})$ and $Y(\mathbb{R})$ are not equal. □

2.10 Corollary. *The set $X(\mathbb{R})$ of real points of X is connected, for any $X \in \mathcal{A}_{\mathbb{R}}(B/A)$, if and only if the discriminant $\mathfrak{d}$ of B over A and the principal ideal (2) are relatively prime.*

Proof. If $X(\mathbb{R})$ is connected for every $X \in \mathcal{A}_{\mathbb{R}}(B/A)$ then, according to Corollary 2.9, $\ell = 0$. Since, by Remark 2.6, $a_i \geq 1$, for $i = 1, \ldots, m$, it follows from Theorem 2.3 that $m = 0$ also. Hence, $\mathfrak{d}$ and (2) are relatively prime.

Conversely, if $\mathfrak{d}$ and (2) are relatively prime then, by Remark 2.6, $\mathrm{ord}_{\mathfrak{p}_i}(\mathfrak{d}_i) = 1$. Hence, $a_i = 0$, for $i = 1, \ldots, n$. It follows from Theorem 2.3 that $X(\mathbb{R})$ is connected, for any $X \in \mathcal{A}_{\mathbb{R}}(B/A)$. □

2.11 Example. Let k be an integer with $k > 2$. Let ξ be a primitive k-th root of unity and let $B = \mathbb{Z}[\xi]$. Then the field of fractions L of B is a CM-field. Let K be the maximal totally real subfield of L, that is,

$$K = \mathbb{Q}(\xi + \xi^{-1}),$$

and let $A = B \cap K$. Then, the rings A and B satisfy Assumption 2.2. In order to study the number of connected components of $X(\mathbb{R})$, for any $X \in \mathcal{A}_{\mathbb{R}}(B/A)$, it will be convenient to consider two cases, the case k is even and the case k is not.

Let us first do the latter case. Let F_k be the k-th cyclotomic polynomial. It is not hard to see that

$$\prod_{i \in (\mathbb{Z}/k\mathbb{Z})^\star} (1 - \xi^i) = F_k(1) = \begin{cases} p, & \text{if } k = p^a,\ p \text{ prime}, \\ 1, & \text{otherwise.} \end{cases}$$

Hence, $\mathfrak{D} = (\xi - \xi^{-1}) = (1 - \xi^2)$ is either trivial or a divisor of the principal ideal (p). Therefore, since k is odd, $\mathfrak{d} = \mathrm{N}_{L/K}(\mathfrak{D})$ and (2) are relatively prime. It follows from Corollary 2.10 that, if k is odd, the set $X(\mathbb{R})$ of real points of X is connected, for every $X \in \mathcal{A}_{\mathbb{R}}(B/A)$.

If k is even, let $2^a k' = k$, with k' odd and $a > 0$. There exists only one prime ideal $\mathfrak{p}$ of A lying over the prime ideal (2) of $\mathbb{Z}$, and $[k(\mathfrak{p}) : \mathbb{F}_2] = \varphi(k')$, where $\varphi(k')$ is the cardinality of the group $(\mathbb{Z}/k'\mathbb{Z})^\star$, in particular, $\varphi(1) = 1$. Also, there exists only one prime ideal $\mathfrak{P}$ of B lying over $\mathfrak{p}$, and $\mathfrak{P}^2 = B\mathfrak{p}$. Moreover,

$$\mathrm{ord}_{\mathfrak{p}}(\mathfrak{d}) = \mathrm{ord}_{\mathfrak{P}}(\mathfrak{D}) = 2.$$

Therefore, it follows from Theorem 2.3 that $X(\mathbb{R})$ is connected or has $2^{\varphi(k')}$ connected components.

2.12 Corollary. *Let $2g = \mathrm{rank}(B)$. Then, the set $X(\mathbb{R})$ of real points of X has 2^g connected components, for every $X \in \mathcal{A}_{\mathbb{R}}(B/A)$, if and only if $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{d}) = 2\mathrm{ord}_{\mathfrak{p}}(2) + 1$, for every nonzero prime $\mathfrak{p}$ of A that divides the principal ideal (2).*

Proof. If $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{d}) = 2\mathrm{ord}_{\mathfrak{p}}(2)+1$, for every nonzero prime ideal $\mathfrak{p}$ of A with $\mathfrak{p} \mid (2)$, then

$$\sum_{i=1}^{m} a_i f_i = \sum_{i=1}^{m} \mathrm{ord}_{\mathfrak{p}_i}(2) \cdot f_i = [K : \mathbb{Q}] = g.$$

According to Theorem 2.3, the number of connected components of $X(\mathbb{R})$, for any $X \in \mathcal{A}_{\mathbb{R}}(B/A)$, is equal to 2^g.

Conversely, if the number of connected components of $X(\mathbb{R})$ is equal to 2^g, for every $X \in \mathcal{A}_{\mathbb{R}}(B/A)$, then, $\ell = 0$, by Corollary 2.9, and

$$\sum_{i=1}^{m} a_i f_i = g = [K : \mathbb{Q}],$$

by Theorem 2.3. Since $\mathrm{ord}_{\mathfrak{p}_i}(\mathfrak{d}) \leq 2\mathrm{ord}_{\mathfrak{p}_i}(2) + 1$ (Remark 2.6), $a_i \leq \mathrm{ord}_{\mathfrak{p}_i}(2)$ and hence $a_i = \mathrm{ord}_{\mathfrak{p}_i}(2)$, for $i = 1, \ldots, m$. Since $\ell = 0$, $\mathrm{ord}_{\mathfrak{p}_i}(\mathfrak{d})$ is odd. Hence, $\mathrm{ord}_{\mathfrak{p}_i}(\mathfrak{d}) = 2\mathrm{ord}_{\mathfrak{p}_i}(2) + 1$, for $i = 1, \ldots, m$. □

For any $B(G)$-module M, let

$$\Im(M) = \{m \in M \mid m + \sigma m = 0\}.$$

Before proving Theorem 2.3 we will prove the following two lemmas.

2.13 Lemma. *Let* $a_i = \left\lfloor \frac{\mathrm{ord}_{\mathfrak{p}_i}(\mathfrak{d})}{2} \right\rfloor$. *Then,*

$$B\Im(B) = \prod_{i=\ell+1}^{n} \mathfrak{P}_i \quad \text{and} \quad \chi_A\left(\Im(B)/(1-\sigma)(B)\right) = \prod_{i=1}^{m} \mathfrak{p}_i^{a_i},$$

Proof. Since the different $\mathfrak{D}$ of B over A is equal to the ideal generated by $(1 - \sigma)(B)$, we have an exact sequence

$$0 \longrightarrow B \otimes_A \left(\Im(B)/(1-\sigma)(B)\right) \longrightarrow B/\mathfrak{D} \longrightarrow B/B\Im(B) \longrightarrow 0. \qquad (***)$$

Let us denote the B-module $B \otimes_A (\Im(B)/(1-\sigma)(B))$ by S. It follows from exactness of $(***)$ that, a nonzero prime ideal $\mathfrak{P}$ of B divides $B\Im(B)$ or $\chi_B(S)$ only if $\mathfrak{P}$ divides $\mathfrak{D}$. Hence, $\mathfrak{P} = \mathfrak{P}_i$, for some $i \in \{1, \ldots, n\}$. In particular, it follows that $\chi_B(S)$ is a square, since $B\mathfrak{p}_i = \mathfrak{P}_i^2$ and

$$\chi_B(S) = B \cdot \chi_A\left(\Im(B)/(1-\sigma)(B)\right).$$

Moreover, since $\Im(B)$ is a direct summand of B as an A-module, $B/B\Im(B)$ is, as an A-module, a nontrivial quotient of a projective A-module of rank 1. Therefore, $B\Im(B) = \chi_B(B/B\Im(B))$ is square-free. Exactness of $(***)$ implies

$$\mathfrak{D} = \chi_B(S) \cdot B\Im(B).$$

From the fact that $\chi_B(S)$ is a square and $B\Im(B)$ is square-free, it follows that

$$\chi_B(S) = \prod_{i=1}^{n} \mathfrak{P}_i^{2a_i} \quad \text{and} \quad B\Im(B) = \prod_{i=1}^{n} \mathfrak{P}_i^{e_i - 2a_i},$$

where

$$e_i = \mathrm{ord}_{\mathfrak{P}_i}(\mathfrak{D}) = \mathrm{ord}_{\mathfrak{p}_i}(\mathfrak{d}) \quad \text{and} \quad a_i = \left\lfloor \frac{e_i}{2} \right\rfloor.$$

Observe that 2 annihilates the A-module $\Im(B)/(1-\sigma)(B)$, and therefore, 2 annihilates S. This implies that $a_i = 0$, for $i = m+1, \ldots, n$. Moreover, by definition of ℓ, $e_i = 2a_i$, for $i = 1, \ldots, \ell$. The lemma follows. □

2.14 Lemma.
(i) $\Im(\mathfrak{P}_i) = \mathfrak{p}_i\Im(B)$, *for* $i = 1, \ldots, \ell$.
(ii) $\Im(\mathfrak{P}_i) = \Im(B)$, *for* $i = \ell+1, \ldots, n$.

Proof. (ii). According to Lemma 2.13,

$$B\Im(B) = \prod_{i=\ell+1}^{n} \mathfrak{P}_i = \bigcap_{i=\ell+1}^{n} \mathfrak{P}_i.$$

Hence,

$$\Im(B) = \Im\left(\bigcap_{i=\ell+1}^{n} \mathfrak{P}_i\right) = \bigcap_{i=\ell+1}^{n} \Im(\mathfrak{P}_i).$$

Since $\Im(B) \supset \Im(\mathfrak{P})$, for every prime ideal $\mathfrak{P}$ of B, it follows that $\Im(B) = \Im(\mathfrak{P}_i)$, for $i = \ell+1, \ldots, n$.
(i). Suppose $\Im(\mathfrak{P}_i) = \Im(B)$. Then, $\mathfrak{P}_i$ divides $B\Im(B)$. For, $\mathfrak{P}_i$ clearly divides $B\Im(\mathfrak{P}_i)$ and $B\Im(B) = B\Im(\mathfrak{P}_i)$. Then, Lemma 2.13 implies that $i > \ell$. Hence, $\Im(\mathfrak{P}_i) \neq \Im(B)$, for $i = 1, \ldots, \ell$. Since

$$\Im(B)/\Im(\mathfrak{P}_i) \longrightarrow B/\mathfrak{P}_i$$

is injective and $B/\mathfrak{P}_i$ is a simple A-module, $\Im(\mathfrak{P}_i) = \mathfrak{p}_i\Im(B)$, for $i = 1, \ldots, \ell$. □

Proof of Theorem 2.3. Let $X = X_{\mathbb{R}}(M, \Phi)$. By definition of X, we have an exact sequence of G-modules

$$0 \longrightarrow M \longrightarrow \mathbb{R} \otimes M \longrightarrow X(\mathbb{C}) \longrightarrow 0.$$

We get a long exact sequence of cohomology groups

$$0 \longrightarrow H^0(G, M) \longrightarrow H^0(G, \mathbb{R} \otimes M) \longrightarrow H^0(G, X(\mathbb{C})) \longrightarrow$$
$$\longrightarrow H^1(G, M) \longrightarrow H^1(G, \mathbb{R} \otimes M) \longrightarrow H^1(G, X(\mathbb{C})) \longrightarrow \cdots$$

Which gives us the exact sequence

$$0 \longrightarrow M^G \longrightarrow \mathbb{R} \otimes M^G \longrightarrow X(\mathbb{R}) \longrightarrow H^1(G, M) \longrightarrow 0,$$

since $H^1(G, \mathbb{R} \otimes M) = 0$. Therefore, the number of connected components of $X(\mathbb{R})$ is equal to the cardinality of

$$H^1(G, M) \cong \Im(M)/(1-\sigma)(M).$$

Define the $B(G)$-submodule

$$N = \prod_{i=1}^{n} \mathfrak{P}_i^{\varepsilon_i},$$

of B, where $\varepsilon_i = \mathrm{ord}_{\mathfrak{P}_i}(\chi_B(\mathfrak{E}(M)))$. If we embed M into B as a $B(G)$-submodule then we see that $\mathfrak{E}(M) \cong \mathfrak{E}(N)$, and therefore, there exists an ideal $\mathfrak{a}$ of A such that $M = \mathfrak{a}N$. This implies that

$$\Im(N)/(1-\sigma)(N) \cong \Im(M)/(1-\sigma)(M),$$

as A-modules, for, this is a triviality if $\mathfrak{a}$ were a principal ideal, to which case we can reduce by localizing. Hence the number of connected components of $X(\mathbb{R})$ is equal to $\#\Im(N)/(1-\sigma)(N)$.

Since the canonical map $A/\mathfrak{p}_i \to B/\mathfrak{P}_i$ is bijective and σ acts as the identity on A,

$$(1-\sigma)(N) = (1-\sigma)(B).$$

Therefore we have an exact sequence

$$0 \longrightarrow \Im(N)/(1-\sigma)(N) \longrightarrow \Im(B)/(1-\sigma)(B) \longrightarrow \Im(B)/\Im(N) \longrightarrow 0.$$

Using Lemma 2.13 and Lemma 2.14, we deduce

$$\chi_A\left(\Im(N)/(1-\sigma)(N)\right) = \chi_A\left(\Im(B)/(1-\sigma)(B)\right) \cdot \chi_A\left(\Im(B)/\Im(N)\right)^{-1} = \\ = \prod_{i=1}^{m} \mathfrak{p}_i^{a_i} \cdot \prod_{i=1}^{\ell} \mathfrak{p}_i^{-\varepsilon_i}.$$

Hence, by what is said above, the number of connected components of $X(\mathbb{R})$ is equal to

$$\prod_{i=1}^{m} 2^{a_i f_i} \Big/ \prod_{i=1}^{\ell} 2^{\varepsilon_i f_i},$$

which was to be proven. □

References

1. Bochnak, J., Coste, M., Roy, M.-F.: *Géométrie algébrique réelle.* Berlin Heidelberg New York: Springer 1987
2. Gross, B. H., Harris, J.: Real algebraic curves. *Ann. scient. Ec. Norm. Sup.* **14**, 157–182 (1981)
3. Hartshorne, R.: *Algebraic geometry.* Berlin Heidelberg New York: Springer 1977
4. Huisman, J.: *Real abelian varieties with complex multiplication.* Thesis, Vrije Universiteit Amsterdam, 1992
5. Oort, F.: The isogeny class of a CM-type abelian variety is defined over a finite extension of the prime field. *J. Pure Appl. Algebra* **3**, 399–408 (1973)

6. Serre, J.-P.: *Local fields*. Berlin Heidelberg New York: Springer 1979

7. Silverman, J. H.: *The arithmetic of elliptic curves*. Berlin Heidelberg New York: Springer 1986

J. Huisman, Mathematical Institute, University of Utrecht, Postbus 80010, 3508 TA Utrecht, The Netherlands. Fax: +31 30 518394. E-mail: huisman@math.ruu.nl