Contemporary Mathematics
Volume **174**, 1994

Fields of definition of abelian varieties with real multiplication

KENNETH A. RIBET

1. Introduction

Let K be a field, and let $\overline{K}$ be a separable closure of K. Let C be an elliptic curve over $\overline{K}$. For each g in the Galois group $G := \mathrm{Gal}(\overline{K}/K)$, let ${}^gC$ be the elliptic curve obtained by conjugating C by g. One says that C is an elliptic K-curve if all the elliptic curves ${}^gC$ are $\overline{K}$-isogenous to C.

Recall that a subfield L of $\overline{K}$ is said to be a $(2, \ldots, 2)$-extension of K if L is a compositum of a finite number of quadratic extensions of K in $\overline{K}$. The extension L/K is then Galois, and $\mathrm{Gal}(L/K)$ is an elementary abelian 2-group. Recently, N. Elkies proved:

(1.1) THEOREM (Elkies, [**2**]). *Let C be an elliptic K-curve over $\overline{K}$ with no complex multiplication. Then C is $\overline{K}$-isogenous to an elliptic curve defined over a $(2, \ldots, 2)$-extension of K.*

In this article, we present an approach to (1.1) which seems different from that of Elkies. At the same time, we generalize (1.1) to include higher-dimensional analogues of elliptic K-curves with no complex multiplication. These are abelian varieties A over $\overline{K}$ whose endomorphism algebras are totally real fields of dimension $\dim(A)$.

For lack of a better term, we borrow the phrase "Hilbert-Blumenthal abelian varieties" to refer to abelian varieties whose endomorphism algebras are totally real fields of maximal dimension. Our use of this expression is a bit unusual.

1991 AMS Subject Classification: 11F11, 11G10 (primary); 14K10, 14K15. This manuscript is in final form. It was written primarily during the program on L-functions at the Isaac Newton Institute for Mathematical Sciences. It is a pleasure to thank the INIMS for its hospitality. The author wishes to thank N. Elkies as well as W. Raskind and J.-L. Colliot-Thélène for helpful e-mail correspondence. This work was partially supported by NSF Grants DMS 88-06815 and DMS 93-06898.

Indeed, in standard parlance, a Hilbert-Blumenthal abelian variety relative to a totally real number field F is an abelian variety A over $\overline{K}$ which is furnished with an action of the ring of integers $\mathcal{O}$ of F. One requires that the Lie algebra $\mathrm{Lie}(A/\overline{K})$ be free of rank one over $\mathcal{O} \otimes \overline{K}$, which acts on $\mathrm{Lie}(A/\overline{K})$ by functoriality; in particular, this requirement forces the dimension of A and the degree of F to be equal. In this article, we insist that $\mathrm{End}(A) \otimes \mathbf{Q}$ be equal to (and not bigger than) a totally real field of dimension $\dim(A)$. On the other hand, we do not require the full ring of integers of this field to act on A.

Suppose that A is a Hilbert-Blumenthal abelian variety in our sense, and let F be the totally real number field $\mathrm{End}(A) \otimes \mathbf{Q}$. We say that A is a K-Hilbert-Blumenthal abelian variety (or "K-HBAV") if ${}^gA$ is F-equivariantly isogenous to A for all $g \in G$. The equivariance refers to the evident isomorphism $\varphi \mapsto {}^g\varphi$ between the endomorphism algebras of A and of ${}^gA$: we demand that there be for each $g \in \mathrm{Gal}(\overline{K}/K)$ an isogeny $\mu_g \colon {}^gA \to A$ which satisfies $\varphi{\circ}\mu_g = {}^g\varphi{\circ}\mu_g$ for all $\varphi \in F$.

(1.2) THEOREM. *Suppose that A is a K-HBAV. Then A is F-equivariantly isogenous to a Hilbert-Blumenthal abelian variety over a finite* $(2, \ldots, 2)$ *extension of K.*

One motivation for proving Theorem 1.2 is the study of Jacobians of modular curves. Indeed, let f be a weight-two newform on the group $\Gamma_1(N)$, and let X_f be the abelian variety associated to f by Shimura's construction [**7**, Th. 7.14]. Thus X_f is a $\mathbf{Q}$-simple factor of the abelian variety $J_1(N)$. If f is a cusp form with complex multiplication, then X_f becomes isogenous to a power of a CM elliptic curve over $\overline{\mathbf{Q}}$. In the opposite case, Propositions 2.1–2.2 below show that the $\overline{\mathbf{Q}}$-simple factors of X_f are then either $\mathbf{Q}$-HBAVs or quaterionic analogues of $\mathbf{Q}$-HBAVs. (It should be possible to prove a version of Theorem 1.2 in the quaternionic case as well.) The absolute decomposition of X_f is controlled by coincidences between the Galois conjugates of f and twists of f by Dirichlet characters (see [**4**]). From the point of view of [**4**], one sees that this absolute decomposition is achieved over the abelian extension of $\mathbf{Q}$ cut out by the set of Dirichlet characters which intervene. This extension is a $(2, \ldots, 2)$-extension of $\mathbf{Q}$ if f has trivial Nebentypus character, but not in general. Nevertheless, Theorem 1.2 tells us that the absolute "building blocks" of X_f are defined over a $(2, \ldots, 2)$-extension of $\mathbf{Q}$ in all cases.

We turn now to a discussion of the proof of Theorem 1.2 and some associated results. First of all, let us indicate how Theorem 1.2 follows immediately from a series of results in §3. As we will see, if A is a K-HBAV, then A defines a class γ in the cohomology group $\mathrm{H}^2(G, F^*)$ made from locally constant cocycles $G \times G \longrightarrow F^*$ and the trivial action of G on F^*. Proposition 3.1 shows that the class γ represents the obstruction to finding a Hilbert-Blumenthal abelian variety over K which is isogenous over $\overline{K}$ to the given one. Therefore, to prove (1.2) is to show that γ becomes trivial under the cohomological restriction map corresponding to a base extension $K \rightsquigarrow K'$, where K' is a $(2,\dots,2)$-extension of K.

Now, by Proposition 3.2, γ lies in the subgroup $\mathrm{H}^2(G,F^*)[2]$ of $\mathrm{H}^2(G,F^*)$ consisting of classes of order at most two. On the other hand, Theorem 3.3 asserts that each element of $\mathrm{H}^2(G,F^*)[2]$ becomes trivial under the restriction map corresponding to a base extension $K \rightsquigarrow K'$ of the desired type. This completes our discussion of (1.2).

Secondly, we wish to highlight a technical point that arises in applying Theorem 3.3 to γ. Namely, let P be the quotient $F^*/\{\pm 1\}$ so that we have an exact sequence of abelian groups

$$0 \to \{\pm 1\} \to F^* \to P \to 0.$$

This sequence is *split*, since the abelian group P is free (Lemma 3.5). Consequently, $\mathrm{H}^2(G,F^*)[2]$ is a split extension of $\mathrm{H}^2(G,P)[2]$ by $\mathrm{H}^2(G,\{\pm 1\})$. As will be seen in §3, there is an elementary isomorphism $\mathrm{Hom}(G,P/P^2) \xrightarrow{\sim} \mathrm{H}^2(G,P)[2]$. Hence we have a split exact sequence

$$0 \to \mathrm{H}^2(G,\{\pm 1\}) \to \mathrm{H}^2(G,F^*)[2] \to \mathrm{Hom}(G,P/P^2) \to 0.$$

Call $\overline{\gamma}$ the image of γ in $\mathrm{Hom}(G,P/P^2)$. Then $\overline{\gamma}$ cuts out a $(2,\dots,2)$-extension of K. This is the extension K_P of K in $\overline{K}$ such that $\mathrm{Gal}(\overline{K}/K_P)$ is the kernel of $\overline{\gamma}$. Certainly, any extension of K in $\overline{K}$ which trivializes γ must contain K_P.

In the case of elliptic curves (i.e., the case $F = \mathbf{Q}$), Elkies shows that γ is trivialized by the field K_P. This point, although admittedly technical, seems very striking to us. The present article may be viewed as an attempt to find a generalization of this phenomenon to the Hilbert-Blumenthal case.

Such a generalization is presented in §4, where we introduce the presumably superfluous requirement that K has characteristic zero. (This hypothesis does not intervene in [**2**].) We show (in Corollary 4.5 below) that γ is trivialized by K_P whenever $[F\colon \mathbf{Q}]$ is odd, and more generally whenever there is an embedding $F \hookrightarrow \overline{K}$ for which the degree $[FK\colon K]$ is odd. It would be interesting to determine whether this hypothesis is necessary.

In the case where $[F\colon \mathbf{Q}]$ is odd, F^* is canonically a product $P \times \{\pm 1\}$. Indeed, P may be identified with the *subgroup* of F^* consisting of elements with positive norm to $\mathbf{Q}^*$. Hence we have canonically

$$\mathrm{H}^2(G,F^*)[2] = \mathrm{H}^2(G,\{\pm 1\}) \times \mathrm{Hom}(G,P/P^2).$$

This suggests a study of the image $\gamma_\pm$ of γ in the first factor $\mathrm{H}^2(G,\{\pm 1\})$. One may be tempted to think that $\gamma_\pm$ is trivial, which would certainly explain the vanishing of γ over K_P. Although $\gamma_\pm$ is trivial for the $\mathbf{Q}$-elliptic curves constructed by Shimura in [**8**], there seem to be examples where $\gamma_\pm$ can be non-trivial. One such example was communicated to the author by E. Pyle of Berkeley, California; here, $K = \mathbf{Q}$ and A is a $\mathbf{Q}$-elliptic curve.

2. K-Hilbert-Blumenthal abelian varieties

Let K, $\overline{K}$ and G be as above, and let F be a totally real number field.

We consider pairs (A, ι), where A is an abelian variety of dimension $[F\colon \mathbf{Q}]$ over $\overline{K}$, and where ι is an isomorphism $F \xrightarrow{\sim} \mathbf{Q} \otimes \operatorname{End}(A)$; such a pair will be called a Hilbert-Blumenthal abelian variety. As mentioned above, it would be more standard to allow ι to be an *injection* $F \hookrightarrow \mathbf{Q} \otimes \operatorname{End}(A)$; however, the more restrictive definition seems to be convenient in what follows. It should be stressed that our Hilbert-Blumenthal abelian varieties are, in particular, non-CM abelian varieties.

Abusing notation, we will generally write A for the pair (A, ι). Moreover, we will frequently view A as an object in the category of abelian varieties *up to isogeny* over $\overline{K}$. In this category, isogenies of abelian varieties become isomorphisms, and the endomorphism algebra usually denoted $\mathbf{Q} \otimes \operatorname{End}(A)$ can be written more simply as $\operatorname{End}(A)$.

Suppose that g is an element of G. Then ${}^gA$ admits a natural multiplication ${}^g\iota$ by F, so that ${}^gA$ is again a Hilbert-Blumenthal abelian variety. As mentioned in §1, we say that A is a K-HBAV if there is an F-equivariant isomorphism $\mu_g\colon {}^gA \xrightarrow{\sim} A$ of abelian varieties up to isogeny for each $g \in G$. Notice that a K-HBAV of dimension one is an elliptic K-curve with no complex multiplication.

To motivate the study of K-HBAVs, we record some facts concerning $\overline{\mathbf{Q}}$-simple factors of abelian varieties over $\mathbf{Q}$ with many endomorphisms. We begin with some terminology: an abelian variety A over $\overline{\mathbf{Q}}$ is said to be a "fake" Hilbert-Blumenthal abelian variety if its endomorphism algebra is a quaternion division algebra over a totally real field F and if $\dim(A) = 2 \cdot [F\colon \mathbf{Q}]$. Also, an abelian variety C over $\mathbf{Q}$ is said to be of $\mathbf{GL}_2$-type if $\mathbf{Q} \otimes \operatorname{End}_{\mathbf{Q}}(C)$ is a number field of degree $\dim(C)$. One knows that the $\mathbf{Q}$-simple factors of the Jacobian of a modular curve $X_1(N)$ are of $\mathbf{GL}_2$-type. Moreover, it is reasonable to conjecture that *all* abelian varieties of $\mathbf{GL}_2$-type over $\mathbf{Q}$ are $\mathbf{Q}$-simple factors of the Jacobian of some $X_1(N)$, cf. [**5**, 4.4]. (Such a conjecture may be viewed as a higher-dimensional analogue of the conjecture of Taniyama and Shimura to the effect that all elliptic curves over $\mathbf{Q}$ are modular.)

(2.1) Proposition. *Suppose that C is an abelian variety over $\mathbf{Q}$ of $\mathbf{GL}_2$-type. Then $C_{/\overline{\mathbf{Q}}}$ is "isotypical": it is isogenous to a product $A \times \cdots \times A$, where A is a simple abelian variety over $\overline{\mathbf{Q}}$. Further, A must be one of the following: (i) an elliptic curve with complex multiplication; (ii) a Hilbert-Blumenthal abelian variety (for some totally real field F); (iii) a "fake" Hilbert-Blumenthal abelian variety.*

Proof. Proposition 2.1 is implicit in the discussion of §5 of [**5**] (which is based principally on results of G. Shimura). For completeness, we shall deduce the proposition from some results included in [**5**].

First of all, if $C_{/\overline{\mathbf{Q}}}$ contains any non-zero abelian subvariety with complex multiplication, then a result of Shimura (Proposition 1.5 of [**8**]) implies that $C_{/\overline{\mathbf{Q}}}$ is a power of an elliptic curve with complex multiplication; thus, we are in case (i). Assume instead that $C_{/\overline{\mathbf{Q}}}$ has no non-zero abelian subvariety with complex multiplication. The number field $E := \mathbf{Q} \otimes \mathrm{End}_{\mathbf{Q}}(C)$ is then its own commutant in $\mathcal{X}$, the algebra of all endomorphisms of C over $\overline{\mathbf{Q}}$. This implies that the center of $\mathcal{X}$ is contained in E: it is therefore a subfield F of E. One shows that F is in fact a *totally real* number field [**5**, 5.4]. Since the center of $\mathcal{X}$ is a single field (as opposed to a product of several fields), C is isotypical, as we claimed. In fact, if we write $\mathcal{X}$ as $\mathrm{M}(n, D)$, where D is a division algebra with center F, then $C_{/\overline{\mathbf{Q}}}$ is isogenous to the nth power of a simple abelian variety A over $\overline{\mathbf{Q}}$ whose endomorphism algebra is D.

Let t be such that t^2 is the rank of D over F. Then a short calculation, based on the fact that E is a maximal commutative semisimple subalgebra of $\mathrm{M}(n, D)$, establishes the formula $\dim(A) = t \cdot [F\colon \mathbf{Q}]$. An argument exploiting the action of D on $\mathrm{H}^1(A(\mathbf{C}), \mathbf{Q})$ shows that t is at most 2. (See the proof of Proposition 5.2 of [**5**] for these facts.) If $t = 1$, we are in case (ii), while if $t = 2$ we are in case (iii). ■

(2.2) PROPOSITION. *Suppose that C is an abelian variety over $\mathbf{Q}$ of $\mathbf{GL}_2$-type. Let A be a simple $\mathbf{Q}$-quotient of C whose endomorphism algebra is a totally real field. Then A is a $\mathbf{Q}$-HBAV.*

PROOF. From what we have seen, the abelian variety $C_{/\overline{\mathbf{Q}}}$ is isogenous to a product $A \times \cdots \times A$ (with, say, n factors), and we are in case (ii). Using the analysis of [**5**], §5 again, we see that the center of the endomorphism algebra $\mathcal{X}$ of $C_{/\overline{\mathbf{Q}}}$ is a subalgebra of the algebra of $\mathbf{Q}$-endomorphisms of C. If this center is F, then $\mathcal{X}$ is isomorphic to $\mathrm{M}(n, F)$, and the endomorphism algebra of A is F. After fixing an isomorphism $\mathcal{X} \approx \mathrm{M}(n, F)$, we may view A as the image of the matrix whose upper left-hand corner entry is 1 and whose other entries are 0. In this model, there is an obvious F-equivariant isogeny $\lambda\colon C_{\overline{\mathbf{Q}}} \to A^n$, given by the n different matrices with a single 1 in the first column and 0's elsewhere.

Let g be an element of G and take $d \in F$. Then we have a commutative diagram

$$\begin{array}{ccccccc} A^n & \stackrel{\lambda}{\leftarrow} & C & = & {}^gC & \stackrel{{}^g\lambda}{\rightarrow} & {}^gA^n \\ \downarrow d & & \downarrow d & & \downarrow {}^gd & & \downarrow {}^gd \\ A^n & \stackrel{\lambda}{\leftarrow} & C & = & {}^gC & \stackrel{{}^g\lambda}{\rightarrow} & {}^gA^n \end{array}$$

in which the central square expresses the fact that d is defined over $\mathbf{Q}$. Contracting it, we get a diagram

$$\begin{array}{ccc} A^n & \stackrel{\sim}{\rightarrow} & {}^gA^n \\ \downarrow d & & \downarrow {}^gd \\ A^n & \stackrel{\sim}{\rightarrow} & {}^gA^n \end{array}$$

in which the isomorphism $A^n \xrightarrow{\sim} {}^gA^n$ is ${}^g\lambda\circ\lambda^{-1}$.

For each pair of integers (i,j) with $1 \le i,j \le n$, we get a map $A \to {}^gA$ by composing the following maps: the inclusion $A \hookrightarrow A^n$ which uses the ith coordinate, the isomorphism $A^n \approx {}^gA^n$, and the projection ${}^gA^n \to {}^gA$ which uses the jth coordinate. For some pair (i,j), this map is non-zero, hence an isogeny. (Recall that A is simple.) Let κ be this isogeny. Then we have

$$\begin{array}{ccc} A & \xrightarrow{\kappa} & {}^gA \\ \downarrow d & & \downarrow {}^gd \\ A & \xrightarrow{\kappa} & {}^gA \end{array}$$

as desired. ■

3. The class γ

Let A be a K-HBAV. For each g, let μ_g be an F-equivariant isomorphism up to isogeny ${}^gA \to A$. We can, and do, assume that the collection (μ_g) has been constructed from a model A_o of A over a finite extension L of K in such a way that μ_g and $\mu_{g'}$ are the same map ${}^gA \to A$ whenever g and g' coincide on L. Thus the association $g \mapsto \mu_g$ is in an obvious sense locally constant. For each pair $\sigma,\tau \in G$, we note that $\mu_\sigma\circ{}^\sigma\mu_\tau\circ\mu_{\sigma\tau}^{-1}$ is an automorphism of A up to isogeny, and consequently of the form $\iota(c(\sigma,\tau))$ with $c(\sigma,\tau) \in F^*$. The map $(\sigma,\tau) \mapsto c(\sigma,\tau)$ is a continuous two-cocycle on G with values in F^*, with F^* being regarded as a trivial G-module. The image γ of c in $\mathrm{H}^2(G,F^*)$ is independent of the choices of the μ_σ.

The following proposition is a mild generalization of [**5**, Th. 8.2].

(3.1) Proposition. *Let E be an extension of K in $\overline{K}$; let $H = \mathrm{Gal}(\overline{K}/E)$ be the corresponding closed subgroup of G. Then the Hilbert-Blumenthal abelian variety A is F-equivariantly isogenous to a Hilbert-Blumenthal abelian variety over E if and only if the class γ lies in the kernel of the restriction map $\mathrm{H}^2(G,F^*) \to \mathrm{H}^2(H,F^*)$.*

Proof. It suffices to prove the proposition in the case $E = K$, in which case the assertion to be proved is that $\gamma = 1$ if and only if A is (F-equivariantly) isogenous to a Hilbert-Blumenthal abelian variety over K.

Suppose first that there is a Hilbert-Blumenthal abelian variety B over K, together with an isomorphism $\lambda\colon A \xrightarrow{\sim} B_{/\overline{K}}$ of Hilbert-Blumenthal abelian varieties up to isogeny over $\overline{K}$. For each $g \in G$, we obtain an isomorphism ${}^g\lambda\colon {}^gA \xrightarrow{\sim} B$. After setting $\mu_g := \lambda^{-1}\circ{}^g\lambda$, we find that c is identically 1, so that γ is trivial.

Conversely, suppose that $\gamma = 1$. Let L and A_o be as above; to simplify notation, we shall write A for A_o. After replacing L by a finite extension of L, we can, and do, assume that the μ_σ are defined over L. Further, the hypothesis that $\gamma = 1$ means that there is a locally constant function $\alpha\colon G \to F^*$ so that

$c(\sigma, \tau) = \alpha(\sigma)\alpha(\tau)/\alpha(\sigma\tau)$; we enlarge L, if necessary so that α is defined modulo $\mathrm{Gal}(\overline{K}/L)$, and so that L is a Galois extension of K. We then replace μ_g by $(1/\alpha(g)) \cdot \mu_g$ for each $g \in G$. The new μ's satisfy $\mu_{\sigma\tau} = \mu_\sigma {}^\sigma\mu_\tau$, and μ_g depends only on the image of g in the finite group $\Delta = \mathrm{Gal}(L/K)$. Finally, μ_g may be viewed as an F-equivariant isomorphism up to isogeny ${}^gA \xrightarrow{\sim} A$ which is defined over L.

Let R be the abelian variety $\mathrm{Res}_{L/K} A$, where "Res" denotes Weil's "Restriction of scalars" functor. In other words, R represents the functor $C \mapsto \mathrm{Hom}(C_{/L}, A)$ from the category of abelian varieties up to isogeny over K to the category of $\mathbf{Q}$-vector spaces. Thus R is an abelian variety over K which is furnished with a structural homomorphism (up to isogeny) $\lambda : R_{/L} \to A$. Given C over K and a homomorphism (of abelian varieties up to isogeny) $\varphi\colon C_{/L} \to A$, there is a unique homomorphism $\theta\colon C \to R$ over K such that $\lambda\circ\theta = \varphi$.

One constructs R by considering the product $\prod_{g\in\mathrm{Gal}(L/K)} {}^gA$ and using obvious patching data to descend this product to K. In particular, R has dimension $[L\colon K] \cdot \dim(A)$. From this point of view, the map $\lambda\colon R_{/L} \to A$ is the projection of $\prod_{g\in\mathrm{Gal}(L/K)} {}^gA$ onto its factor A. Alternatively, given R with its structural map λ, and an element g of $\mathrm{Gal}(L/K)$, we can view ${}^g\lambda$ as a map $R_{/L} \to {}^gA$. One shows that the map $R_{/L} \to \prod_{g\in\mathrm{Gal}(L/K)} {}^gA$ induced by the family of ${}^g\lambda$ is an isomorphism.

By functoriality, F acts on R over K. Thus we have $F \subseteq \mathcal{X}$, where $\mathcal{X} = \mathrm{End}_K(R)$. Further, the universal property satisfied by R makes it easy to compute $\mathrm{End}_K(R)$ as a $\mathbf{Q}$-vector space. Indeed, we have

$$\mathrm{End}_K(R) = \mathrm{Hom}_K(R, R) = \mathrm{Hom}_L(R_{/L}, A) = \bigoplus_g \mathrm{Hom}_L({}^gA, A) = \bigoplus_g F \cdot \mu_g.$$

Let $[g]$ be the element of $\mathrm{End}_K(R)$ which corresponds to μ_g in the gth factor of the direct sum. Then $[g]$ is the unique element in $\mathrm{End}_K(R)$ such that $\lambda\circ[g] = \mu_g\circ{}^g\lambda$. The unicity implies that each $[g]$ commutes with the action of F on R. A short computation, based on the unicity and the formula $\mu_{\sigma\tau} = \mu_\sigma {}^\sigma\mu_\tau$, shows that $[\sigma][\tau] = [\sigma\tau]$ for $\sigma, \tau \in \Delta$. Also, the $[g]$ commute with F. Hence $\mathcal{X}$ is in the end the group algebra $F[\Delta]$.

The field F is a direct summand of the algebra $\mathcal{X} = F[\Delta]$ via the inclusion $a \in F \mapsto a \cdot [1]$ and the augmentation map $[g] \mapsto 1$. Let B be the subvariety of R corresponding to the direct summand F of $\mathcal{X}$. Then B is an abelian variety over K with an induced action of F. We claim that B is a Hilbert-Blumenthal abelian variety over K, i.e., that $\dim(B) = \dim(A)$, and that in fact A and B are isomorphic Hilbert-Blumenthal abelian varieties up to isogeny over L. To see this, we remark that $R_{/L}$ is isogenous to a product of copies of A (since the ${}^gA$ are each isogenous to A), so that $B_{/L}$ is certainly isogenous to a product of some number of copies of A. To determine the dimension of B, we remark that

$$F = \mathrm{End}_K(B) = \mathrm{Hom}_K(B, R) = \mathrm{Hom}_L(B_{/L}, A).$$

Since F is the endomorphism algebra of A, $B_{/L}$ is isogenous to A. ■

Suppose now that A is a K-HBAV over $\overline{K}$. Fix a polarization $\theta_A\colon A \to A^\vee$ of A as an abelian variety. The associated Rosati involution of the endomorphism algebra of A may be viewed as a positive involution of the totally real field F and therefore is forced to be the identity.

Let B again be a Hilbert-Blumenthal abelian variety over $\overline{K}$, and fix a polarization θ_B of B. Then for each F-equivariant map $\mu\colon B \to A$, we define the "degree" $\deg(\mu)$ by the formula

$$\deg(\mu) = \mu \circ \theta_B^{-1} \circ \mu^\vee \circ \theta_A,$$

so that $\deg(\mu)$ is an element of the endomorphism algebra of A. Identifying this algebra with F, we consider that $\deg(\mu)$ is an element of F. If $\overline{K}$ is a subfield of $\mathbf{C}$, then θ_A and θ_B identify $\bigwedge_F^2 \mathrm{H}_1(A(\mathbf{C}), \mathbf{Q})$ and $\bigwedge_F^2 \mathrm{H}_1(B(\mathbf{C}), \mathbf{Q})$ with F. The number $\deg(\mu)$ is the element of F describing the map $\bigwedge_F^2 \mathrm{H}_1(B(\mathbf{C}), \mathbf{Q}) \to \bigwedge_F^2 \mathrm{H}_1(A(\mathbf{C}), \mathbf{Q})$ induced by μ.

If $\mu\colon A \to A$ is given by an element c of F, then $\deg(\mu) = c^2$. Also, it is easy to check that deg is multiplicative in the following sense. Suppose that (C, θ_C) is a third polarized Hilbert-Blumenthal abelian variety, and that $\lambda\colon C \to B$ is F-equivariant. Then $\deg(\mu \circ \lambda) = \deg(\mu)\deg(\lambda)$, provided of course that the "degrees" are computed with respect to a fixed set of polarizations.

(3.2) Proposition. *Let A be a K-HBAV over $\overline{K}$. Then the order of the associated cohomology class $\gamma \in \mathrm{H}^2(G, F^*)$ is at most two.*

Proof. Fix a polarization $\theta\colon A \to A^\vee$ of A and for each $g \in G$ let ${}^g\theta$ denote the associated polarization of ${}^gA$. Choose a family (μ_g) as above, and let c be the F^*-valued two-cocycle on G defined by this family. For each g, let

$$d_g := \mu_g \circ {}^g\theta^{-1} \circ \mu_g^\vee \circ \theta$$

be the degree of μ_g, calculated with respect to the polarizations θ and ${}^g\theta$. This element of F is canonical in the following sense: if we replace θ by another polarization θ' of A, then d_g will remain unchanged provided that we replace ${}^g\theta$ by ${}^g\theta'$.

By construction,

$$c(\sigma, \tau) = \mu_\sigma \circ {}^\sigma\mu_\tau \circ \mu_{\sigma\tau}^{-1}$$

for $\sigma, \tau \in G$. On taking degrees, we find the formula

$$c(\sigma, \tau)^2 = \frac{d_\sigma d_\tau}{d_{\sigma\tau}}$$

which expresses the square of c as a coboundary. ■

(3.3) Theorem. *Let γ be an element of order dividing two in $\mathrm{H}^2(G, F^*)$. Then there is an open normal subgroup H of G such that G/H is an elementary abelian two-group and such that the image of γ in $\mathrm{H}^2(H, F^*)$ is trivial. In other words, γ becomes trivial after K is replaced by a finite $(2, \dots, 2)$-extension of K.*

Proof. Let $P = F^*/\{\pm 1\}$, so that there is a tautological exact sequence

$$0 \to \{\pm 1\} \to F^* \to P \to 0. \tag{3.4}$$

In the case where $[F\colon \mathbf{Q}]$ is odd, there is a natural splitting of this exact sequence: we may view P as the *subgroup* of F^* consisting of elements with positive norm to $\mathbf{Q}^*$. In the general case, (3.4) is still split, but apparently in no natural way. This follows directly from:

(3.5) Lemma. *The group P is a free abelian group, of countable rank.*

To prove the lemma, we consider the map $\phi\colon a \mapsto (a)$ which takes an element a of P to the fractional ideal of F generated by a lift of a to F^*. The image of ϕ is a subgroup (of finite index) of the group of all fractional ideals of F; this latter group is the free abelian group on the set of non-Archimedean places of F. Hence the image of ϕ is a free abelian group, so that P is abstractly isomorphic to the direct sum of the image of ϕ and the kernel of ϕ. On the other hand, $\ker(\phi)$ is the group $U/\{\pm 1\}$, where U is the group of units of F. According to Dirichlet's theorem, $\ker(\phi)$ is a free abelian group of rank $n-1$, where $n = [F\colon \mathbf{Q}]$. It follows that P is the direct sum of two free abelian groups, one finitely generated and one countably generated. This proves the lemma.

Returning to the proof of (3.3), we fix a splitting of (3.4). We shall assume that this is the indicated natural splitting if $[F\colon \mathbf{Q}]$ is odd. The splitting fixes an isomorphism of abelian groups $F^* \approx \{\pm 1\} \times P$. This isomorphism induces in turn a decomposition

$$\mathrm{H}^2(G, F^*)[2] \approx \mathrm{H}^2(G, \{\pm 1\}) \times \mathrm{H}^2(G, P)[2],$$

where the notation "[2]" indicates the kernel of multiplication by 2. The element γ of $\mathrm{H}^2(G, F^*)$ is then the product of its two projections $\gamma_\pm \in \mathrm{H}^2(G, \{\pm 1\})$ and $\overline{\gamma} \in \mathrm{H}^2(G, P)[2]$. The factor $\overline{\gamma}$ is independent of the chosen splitting of (3.4): it is the image of γ under the map on cohomology induced by the quotient map $F^* \to P$. On the other hand, the "sign" component $\gamma_\pm$ of γ depends on the splitting. We thus consider that $\gamma_\pm$ is defined intrinsically only in the case where $[F\colon \mathbf{Q}]$ is odd.

To prove (3.3), we must show that both $\gamma_\pm$ and $\overline{\gamma}$ become trivial when K is replaced by a $(2, \dots, 2)$-extension of K.

To treat $\overline{\gamma}$, we consider the exact sequence

$$1 \to P \xrightarrow{x \mapsto x^2} P \to P/P^2 \to 1;$$

note that P is torsion free. The associated long exact cohomology sequence then gives an isomorphism

$$\mathrm{Hom}(G, P/P^2) \xrightarrow{\sim} \mathrm{H}^2(G, P)[2].$$

Suppose that $\overline{\gamma}$ corresponds to the homomorphism $\varphi\colon G \to P/P^2$. Then $\ker(\varphi)$ is a subgroup of G which corresponds to a $(2, \dots, 2)$-extension K_P of K. It is clear that $\overline{\gamma}$ becomes trivial over this extension.

It remains to split $\gamma_\pm$. It is known that $\mathrm{H}^2(G, \{\pm 1\}) = 0$ if K has characteristic 2, cf. [**6**, p. II-5]. Assume, then, that the characteristic of K is different from 2. The group $\mathrm{H}^2(G, \{\pm 1\})$ may then be identified with $\mathrm{Br}(K)[2]$, where $\mathrm{Br}(K)$ is the Brauer group of K. A theorem of S. A. Merkur'ev [**3**] states that $\mathrm{Br}(K)[2]$ is generated by the classes of quaternion algebras over K. Since each quaternion algebra over K is split by a quadratic extension of K, it follows that $\gamma_\pm$ is split by a $(2, \dots, 2)$-extension of K, as required. ∎

4. The odd-dimensional situation

In this section, we assume that K has characteristic 0. (An assumption concerning the parity of $[F\colon \mathbf{Q}]$ will be made later.)

We begin with some preliminary comments concerning the class γ defined by a K-HBAV. First, we note that the tensor product $F \otimes_{\mathbf{Q}} K$ decomposes as some direct sum of fields $\oplus_{\omega\in\Omega} K_\omega$, where the K_ω are finite extensions of K. The index set Ω is the set $\mathrm{Hom}(F, \overline{K})$ of field embeddings $F \hookrightarrow \overline{K}$, modulo the action of G on $\mathrm{Hom}(F, \overline{K})$.

Next, suppose that L is a finite extension of K, and consider $M := L \otimes_K \overline{K}$ as a G-module, with G acting trivially on the first factor. Choose an embedding σ of L into $\overline{K}$, and let $H = \mathrm{Gal}(\overline{K}/\sigma(L))$. Then $L \otimes_K \overline{K}$ is the induced representation $\mathrm{Ind}_H^G \overline{K}$. Indeed, M may be written as the group of functions $f\colon \Sigma \to \overline{K}$, where Σ is the set of embeddings $L \hookrightarrow \overline{K}$. In this optic, G acts via $(g \cdot f)(\tau) = g(f(g^{-1}\tau))$ for $g \in G$ and $\tau \in \Sigma$. It is clear that $M = \oplus_{\tau\in\Sigma} M_\tau$, where M_τ consists of those functions which vanish outside of τ. Further, the subgroups M_τ of M are permuted transitively by G, since G acts transitively on Σ. The formula $M = \mathrm{Ind}_H^G \overline{K}$ then follows by a well known criterion (see, e.g., [**1**, Ch. III, 5.4]).

Finally, we consider $F \otimes_{\mathbf{Q}} \overline{K}$ as a G-module, with G acting trivially on the first factor and in the natural way on the second. Then

$$F \otimes_{\mathbf{Q}} \overline{K} = (F \otimes_{\mathbf{Q}} K) \otimes_K \overline{K} = \bigoplus_{\omega} (K_\omega \otimes_K \overline{K}).$$

Therefore,

$$F \otimes_{\mathbf{Q}} \overline{K} = \bigoplus_{\omega} \mathrm{Ind}_{H_\omega}^G \overline{K}.$$

In this latter formula, we have chosen for each ω a K-embedding $K_\omega \hookrightarrow \overline{K}$ and have put $H_\omega := \mathrm{Gal}(\overline{K}/K_\omega)$.

In a similar vein, one proves

$$(F \otimes_{\mathbf{Q}} \overline{K})^* = \bigoplus_{\omega} \operatorname{Ind}_{H_\omega}^G \overline{K}^*.$$

Shapiro's lemma [**1**, Ch. III, 6.2] provides an identification

$$\mathrm{H}^i(G, \operatorname{Ind}_{H_\omega}^G \overline{K}^*) = \mathrm{H}^i(H_\omega, \overline{K}^*)$$

for each $i \geq 0$. (The induced module $\operatorname{Ind}_{H_\omega}^G \overline{K}^*$ may be regarded as a co-induced module because the index of H_ω in G is finite.) Thus

$$\mathrm{H}^i(G, (F \otimes_{\mathbf{Q}} \overline{K})^*) = \bigoplus_{\omega} \mathrm{H}^i(H_\omega, \overline{K}^*)$$

for each i. Consequently,

$$\mathrm{H}^1(G, F \otimes_{\mathbf{Q}} \overline{K})^*) = 0$$

by Hilbert's Theorem 90. Similarly,

$$\mathrm{H}^2(G, (F \otimes_{\mathbf{Q}} \overline{K})^*) = \bigoplus_{\omega} \mathrm{Br}(K_\omega) \tag{4.1}$$

because $\mathrm{H}^2(H_\omega, \overline{K}^*)$ is the Brauer group of K_ω.

Now consider the exact sequence of G-modules

$$0 \to F^* \to (F \otimes \overline{K})^* \to (F \otimes \overline{K})^*/F^* \to 0, \tag{4.2}$$

where G acts in the usual way on $\overline{K}$ and the indicated tensor products are taken over $\mathbf{Q}$. Exploiting the vanishing of $\mathrm{H}^1(G, (F \otimes \overline{K})^*)$, we obtain

$$0 \to \mathrm{H}^1(G, (F \otimes \overline{K})^*/F^*) \xrightarrow{\delta} \mathrm{H}^2(G, F^*) \to \mathrm{H}^2(G, (F \otimes \overline{K})^*) \to \cdots .$$

Here, δ is the indicated connecting homomorphism in the long cohomology sequence arising from (4.2).

(4.3) Lemma. *Let A be a K-HBAV. Then the element γ of $\mathrm{H}^2(G, F^*)$ defined by A lies in the image of δ. Equivalently, the image of γ in $\mathrm{H}^2(G, (F \otimes \overline{K})^*)$ is zero.*

Proof. We must exhibit an element β of $\mathrm{H}^1(G, (F \otimes \overline{K})^*/F^*)$ such that $\gamma = \delta(\beta)$. Let $V = \mathrm{Lie}(A/\overline{K})$. For each $g \in G$, the map $\mu_g \colon {}^gA \to A$ induces a $(F \otimes \overline{K})$-linear homomorphism $\mathrm{Lie}({}^gA/\overline{K}) \to \mathrm{Lie}(A/\overline{K})$, or equivalently an F-linear homomorphism $\lambda_g \colon V \to V$ which is g-linear in the sense that it satisfies $\lambda(a \cdot v) = g(a)\lambda(v)$ for $a \in \overline{K}$ and $v \in V$. Now it is well known, and easy to verify, that the Lie algebra $\mathrm{Lie}(A/\overline{K})$ is free of rank one over $F \otimes \overline{K}$. Let v be a basis of V, considered as a free rank-one $F \otimes \overline{K}$-module. Then one has $\lambda_g(v) = a_g \cdot v$ for some element a_g in $(F \otimes \overline{K})^*$. The relations among the μ_g provide the formula $c(\sigma, \tau)a_{\sigma\tau} = a_\sigma {}^\sigma a_\tau$ for $\sigma, \tau \in G$. It follows that the function $G \to (F \otimes \overline{K})^*/F^*$ induced by $g \mapsto a_g$ is a 1-cocycle, and that the corresponding class β in $\mathrm{H}^1(G, (F \otimes \overline{K})^*)$ maps to γ under δ. ∎

(4.4) Proposition. *Suppose that γ is the element of $\mathrm{H}^2(G, F^*)$ arising from a K-HBAV and that $\overline{\gamma} = 0$. Then $\gamma = 0$ provided that no element of order two in the Brauer group of K is split by all extensions of K of the form K_ω.*

Proof. In view of the hypothesis $\overline{\gamma} = 0$, we have $\gamma = \gamma_\pm \in \mathrm{H}^2(G, \{\pm 1\})$. According to (4.3), γ lies in the kernel of the map

$$j \colon \mathrm{H}^2(G, \{\pm 1\}) \to \mathrm{H}^2(G, (F \otimes \overline{K})^*)$$

induced by the inclusion of $\{\pm 1\}$ in $(F \otimes \overline{K})^*$. This map may be viewed as the natural map

$$\mathrm{Br}(K)[2] \to \bigoplus_\omega \mathrm{Br}(K_\omega),$$

which is injective by hypothesis. Thus γ is indeed 0. ∎

(4.5) Corollary. *Suppose that $\gamma \in H^2(G, F^*)$ arises from a K-HBAV. Suppose that $[F\colon \mathbf{Q}]$ is odd. Then the class γ becomes zero after K is replaced by the extension K_P of K defined by $\overline{\gamma}$. In particular, if $\overline{\gamma} = 0$, then $\gamma = 0$.*

Proof. The two assertions of the corollary are equivalent, since $\overline{\gamma}$ becomes trivial after K is replaced by K_P. Because of (4.4), to prove the second assertion it is enough to prove that the map j which occurs in the proof of (4.4) is injective whenever $[F\colon \mathbf{Q}]$ is odd.

However, $[F\colon \mathbf{Q}] = \sum_\omega [K_\omega\colon K]$. Thus, if $[F\colon \mathbf{Q}]$ is odd, then there is at least one index ω for which $[K_\omega\colon K]$ is odd. Further, if $[K_\omega\colon K]$ is odd, then it is evident that the map $\mathrm{Br}(K)[2] \to \mathrm{Br}(K_\omega)$ is injective since there is a corestriction map $\mathrm{cor}\colon \mathrm{Br}(K_\omega) \to \mathrm{Br}(K)$ whose composition with the natural map $\mathrm{Br}(K) \to \mathrm{Br}(K_\omega)$ is multiplication by $[K_\omega\colon K]$. ∎

References

1. K. S. Brown, *Cohomology of groups*, Graduate Texts in Math., vol. 87, Springer-Verlag, New York, Heidelberg and Berlin, 1982.
2. N. Elkies, *Remarks on elliptic K-curves*, Preprint, 1993.
3. A. S. Merkur'ev, *On the norm residue symbol of degree 2*, Dokl. Akad. Nauk. SSSR **261** (1981), 542–547; Soviet Math. Dokl. **24** (1981), 546–551.
4. K. A. Ribet, *Twists of modular forms and endomorphisms of abelian varieties*, Math. Ann. **253** (1980), 43–62.
5. ———, *Abelian varieties over* **Q** *and modular forms*, 1992 Proceedings of KAIST Mathematics Workshop, Korea Advanced Institute of Science and Technology, Taejon, 1992, pp. 53–79.
6. J-P. Serre, *Cohomologie galoisienne*, Lecture Notes in Math., vol. 5, 4e édition, Springer-Verlag, Berlin and New York, 1973.
7. G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton University Press, Princeton, 1971.
8. ———, *Class fields over real quadratic fields and Hecke operators*, Ann. of Math. **95** (1972), 131–190.

UC Mathematics Department, Berkeley, CA 94720 USA

E-mail address: ribet@math.berkeley.edu