MÉMOIRES DE LA S. M. F.

K. A. RIBET

Division fields of abelian varieties with complex multiplication

Mémoires de la S. M. F. 2e série, tome 2 (1980), p. 75-94

<http://www.numdam.org/item?id=MSMF_1980_2_2__75_0>

SOCIÉTÉ MATHÉMATIQUE DE FRANCE
2e série, Mémoire n° 2, 1980, p. 75-94

DIVISION FIELDS OF ABELIAN VARIETIES WITH COMPLEX MULTIPLICATION

by

K. A. RIBET

1. Let A be an abelian variety over a number field k. Suppose that A has complex multiplication over k in the sense that $(\mathrm{End}_k A) \otimes \mathbb{Q}$ contains a commutative semisimple algebra E over $\mathbb{Q}$ of rank 2.dim A. For $N \geq 1$, let d(N) be the degree over k of the field $k(A_N)$ obtained by adjoining to k the kernel A_N of multiplication by N on A. Let $\alpha(N)$ be the number of (distinct) prime factors of N. The main purpose of this paper is to prove the following result :

THEOREM (1.1) : *There exist positive constants* C_1, C_2 *and an integer* $\nu \geq 0$ *(depending on A, k, and E) such that we have*

$$C_1^{\alpha(N)} \leq \frac{d(N)}{N^{\nu}} \leq C_2^{\alpha(N)}$$

for all $N \geq 1$.

We prove (1.1) by writing the ℓ-adic representations of A in the form given them by Serre-Tate [15] (using the theory of Shimura-Taniyama [17] and Weil [18]) and then exploiting some elementary facts about the "mod ℓ^n" points

of tori over $\mathbb{Q}$. The possibility of doing this was suggested by a letter from Serre to Masser [13] concerning the special case where A is a product of several elliptic curves*; to prove (1.1) we have followed Serre's arguments. It should be noted that a variant of (1.1) was proved by T. Kubota [4], who considered integers N of the form ℓ^n, ℓ being a fixed prime. Also, in this volume, Masser [6] has treated prime numbers N, for abelian varieties of dimension 2.

In our proof of (1.1), the integer ν arises as the dimension of a certain torus which is familiar in other contexts. Namely, it is the Hodge group of A (see [1] and §§ 3,4 of [14]), and so its dimension bounds the transcendence degree of the field generated by the periods of differentials on A [1]. For us, the torus is given as the image of a certain explicit map between tori; therefore, via the dictionary between tori and their character groups, computing ν comes down to computing the rank of a certain matrix. In § 3 of this paper, we write down explicitly the matrix that intervenes, and this enables us to give the lower bound $2 + \mathrm{Log}_2 d$ for ν in the case where A is absolutely simple, d denoting the dimension of A. There is also a trivial upper bound for ν, namely the sum of 1 and the dimension of A. When ν attains this upper bound, we say (following Kubota) that A is "non-degenerate." For A absolutely simple, it follows from our lower bound that A is always non-degenerate for d = 1,2,3. We give several examples (due, variously, to Shimura, Serre, and Lenstra) of absolutely simple A which do not have this property. The smallest example has d = 4 and ν = 4; this is given by the CM type constructed by Mumford and described in [9].

For the reader who was present at the Conference, it might be pointed out that this article bears no relation to the author's talk, for which one can consult [10]. The material concerning the calculation of ν is based on a manuscript written in 1977-78 after correspondence with Masser and discussions with Serre and Lenstra. It later formed the basis for a talk by the author at the Rennes conference on algebraic geometry in June, 1978.

* For the convenience of the reader, the text of this letter (and a sequel) has been included as an appendix to this paper.

2. Let T be a torus over $\mathbb{Q}_\ell$, and let

$$X(T) = \mathrm{Hom}_{\overline{\mathbb{Q}}_\ell}(T, \mathbb{G}_m)$$

be the character group of T. Using an idea of Ono [7, § 2], we define subgroups $T(1+\ell^n\mathbb{Z}_\ell)$ $(n \geq 0)$ of $T(\mathbb{Q}_\ell)$ by the rule

$$T(1+\ell^n\mathbb{Z}_\ell) = \{ t \in T(\mathbb{Q}_\ell) \mid \chi(t) \equiv 1 \bmod \ell^n \text{ for all } \chi \in X(T)\} .$$

We have $\chi(t) \in \bar{\mathbb{Q}}_\ell^*$, and the condition $\chi(t) \equiv 1 \bmod \ell^n$ means that $\mathrm{ord}_\ell(\chi(t)-1)$ is at least n. Thus $T(\mathbb{Z}_\ell)$ is the maximal compact subgroup of $T(\mathbb{Q}_\ell)$, and the various $T(1+\ell^n\mathbb{Z}_\ell)$ define a filtration of $T(\mathbb{Z}_\ell)$ by open subgroups. We further define

$$T(\mathbb{Z}/\ell^n\mathbb{Z}) = T(\mathbb{Z}_\ell)/T(1+\ell^n\mathbb{Z}_\ell) \qquad (n \geq 0).$$

Example (2.1) : Let $E = E_1 \times \ldots \times E_m$ be a product of finite extensions of $\mathbb{Q}_\ell$, and let T be the torus obtained by viewing E^* as an algebraic group over $\mathbb{Q}_\ell$. Then we have

$$T(\mathbb{Z}_\ell) = R^* ,$$

where R is the integer ring of E, namely the product of the integer rings of the E_i. Further, for $n \geq 1$ we have

$$T(1+\ell^n\mathbb{Z}_\ell) = \{r \in R^* \mid r \in 1+\ell^n R\} ,$$

and

$$T(\mathbb{Z}/\ell^n\mathbb{Z}) = (R/\ell^n R)^* .$$

It is easy to check that the cardinality of $T(\mathbb{Z}/\ell^n\mathbb{Z})$ is given by the formula

$$\ell^{n\nu} \cdot \prod_{i=1}^{m} \frac{q_i - 1}{q_i} ,$$

where ν is the dimension of the torus T (i.e. the sum of the degrees of the E_i over $\mathbb{Q}_\ell$) and q_i is the order of the residue field of R_i, for $i = 1,\ldots,m$. (Cf. [12], Ch.IV,§ 2, Prop. 6.) A special case occurs when E is given by $F \otimes \mathbb{Q}_\ell$, where F is a finite extension of $\mathbb{Q}$, or a product of such extensions. Then we have $T = T_{F/\mathbb{Q}_\ell}$, where T_F is the torus over $\mathbb{Q}$ defined by F^*.

Remark (2.2) : If T has "good reduction" (i.e. T is split over a finite unramified extension of $\mathbb{Q}_\ell$), then there is a commutative smooth group scheme $T_{/\mathbb{Z}_\ell}$ whose general fibre is the torus T. One may show that $T(\mathbb{Z}/\ell^n\mathbb{Z})$ coincides with the group of $\mathbb{Z}/\ell^n\mathbb{Z}$-valued points of $T_{/\mathbb{Z}_\ell}$, for $n \geq 1$. The special case $n = 1$ is particularly easy to treat because it then suffices to identify $T(\mathbb{Z}/\ell\mathbb{Z})$ with the group of rational points of the reduction $T_{/\mathbb{F}_\ell}$ of T (i.e. of $T_{/\mathbb{Z}_\ell}$)mod ℓ. For this see Prop. 2.3.1 of [7], where $T_{/\mathbb{F}_\ell}$ is defined directly by declaring its character group to be X(T), viewed as a $\mathrm{Gal}(\bar{\mathbb{F}}_\ell/\mathbb{F}_\ell)$-module (which we may do since it is an unramified $\mathrm{Gal}(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$-module by hypothesis).

We now consider a map $\lambda : T \to T'$ between $\mathbb{Q}_\ell$-tori. For $n \geq 0$, it is clear that λ induces maps

$$T(1 + \ell^n\mathbb{Z}_\ell) \longrightarrow T'(1 + \ell^n\mathbb{Z}_\ell)$$

$$T(\mathbb{Z}/\ell^n\mathbb{Z}) \longrightarrow T'(\mathbb{Z}/\ell^n\mathbb{Z})$$

We denote the second map by λ_n.

Theorem (2.3) : If λ is surjective, then the order of the cokernel of λ_n is bounded independently of n. If λ is an isogeny, then both the kernel and the cokernel of λ_n have bounded order.

Proof : When λ is surjective, the map

$$\alpha : T(\mathbb{Z}_\ell) \to T'(\mathbb{Z}_\ell)$$

induced by λ has an open image, as one may see by viewing the two groups as ℓ-adic Lie groups, since the surjectivity of λ just means that the map on Lie algebras induced by α is surjective. (See Bourbaki, Groupes et Algèbres de Lie, Ch. III, Prop. 28 of § 3, n° 8 and Th. 2 of § 7, n°1.) Since $T'(\mathbb{Z}_\ell)$ is compact, the cokernel of α is finite. Since the cokernel of λ_n is a quotient of this cokernel for each n, we get the first statement of the theorem.

Now assume that λ is an isogeny. Then the kernel of α is finite, and the assertion to be proved reduces, via the snake lemma, to the assertion that the cokernel of the restriction

$$\alpha_n : T(1 + \ell^n\mathbb{Z}_\ell) \to T'(1 + \ell^n\mathbb{Z}_\ell)$$

of α to $T(1 + \ell^n\mathbb{Z}_\ell)$ has order which is bounded independently of n. For this, we consider the "transpose" isogeny $\lambda^\wedge$ and define $\alpha_n^\wedge$ for $n \geq 0$ as the map for $\lambda^\wedge$ analogous to α_n. Then $\alpha_n \circ \alpha_n^\wedge$ is just multiplication by the degree of λ on $T'(1 + \ell^n\mathbb{Z}_\ell)$. It is clear for n sufficiently large that $T'(1 + \ell^n\mathbb{Z}_\ell)$ is isomorphic to the group $\mathbb{Z}_\ell^\nu$ where $\nu = \dim T = \dim T'$ is independent of n. Hence the cokernel of $\alpha_n \circ \alpha_n^\wedge$, and therefore that of α_n, has bounded order.

We now consider once again a surjection $\lambda : T \to T'$ over $\mathbb{Q}_\ell$, and write λ^* for the corresponding inclusion

$$X(T') \hookrightarrow X(T)$$

of character groups. Let X" be the subgroup of X(T) given by

$$X'' = \{\chi \in X(T) \mid n\chi \in \lambda^*(X(T')) \text{ for some } n \geq 1\}.$$

Then $(X'' : X(T'))$ is finite, and $X(T)/(X'')$ is torsion free. If we let T'' be the $\mathbb{Q}_\ell$-torus corresponding to X'', then the inclusion

$$X(T') \subseteq X''$$

corresponds to an isogeny

$$\nu : T'' \to T'$$

and the inclusion $X(T'') \hookrightarrow X(T)$ corresponds to a map

$$\mu : T \to T''$$

whose kernel is connected (i.e. is a torus). We have

$$\lambda = \nu \circ \mu.$$

Theorem (2.4) : Suppose that $X(T)$ is an unramified $\mathrm{Gal}(\bar{\mathbb{Q}}_\ell / \mathbb{Q}_\ell)$-module, so that the tori T, T', T'' have good reduction. Suppose also that ℓ is prime to the degree N of the isogeny ν. Then, with the notation as in (2.3), the order of the cokernel of λ_n is bounded by N. If, furthermore, λ is an isogeny (so that $\lambda = \nu$), then the kernel of λ_n again has order bounded by N.

Proof : It is known that the map $T(\mathbb{Z}_\ell) \longrightarrow T''(\mathbb{Z}_\ell)$ induced by μ is surjective because of the good reduction hypothesis ([8], § 4.2). It will therefore be enough to prove the statements when λ is an isogeny, which we now suppose to be the case. Under our hypotheses, the map

$$\alpha_1 : T(1 + \ell\mathbb{Z}_\ell) \to T'(1 + \ell\mathbb{Z}_\ell)$$

induced by λ is known to be an isomorphism [7, Prop. 2.2.2] . It follows formally from this that the maps

$$\alpha_n : T(1 + \ell^n \mathbb{Z}_\ell) \to T'(1 + \ell^n \mathbb{Z}_\ell)$$

are isomorphisms for all $n \geq 1$. [Given $t' \in T'(1 + \ell^n \mathbb{Z}_\ell)$, suppose that $t' = \lambda(t)$ for $t \in T(1 + \ell\mathbb{Z}_\ell)$. It is clear that we have

$$\chi(t) \equiv 1 \bmod \ell$$

$$\chi(t)^N \equiv 1 \bmod \ell^n$$

for all $\chi \in X(T)$; from this it follows that we have $\chi(t) \equiv 1 \bmod \ell^n$ for all χ , giving $t \in T(1 + \ell^n \mathbb{Z}_\ell)$.]

We find that the cokernel and kernel of λ_n are independent of n, for $n \geq 1$. Taking $n = 1$, we see that λ_1 is the map on $\mathbf{F}_\ell$ - points induced by the reduction $\lambda_{/\mathbf{F}_\ell} : T_{/\mathbf{F}_\ell} \to T'_{/\mathbf{F}_\ell}$ of λ . Thus the kernel of λ_1 is the group of $\mathbf{F}_\ell$ - rational points of the kernel of λ , so its order is in particular a divisor of N. On the other hand, it is well known that the kernel and cokernel of λ , have equal orders, because of Lang's Theorem ([5]; cf. [11] Ch.VI, n°6, Prop.5) and the triviality of the Herbrand quotient of a finite module. (Equivalently, the isogenous tori $T_{/\mathbf{F}_\ell}$ and $T'_{/\mathbf{F}_\ell}$ have the same number of rational points.) This completes the proof.

We next consider the situation where we are given tori over $\mathbb{Q}$. If $T_{/\mathbb{Q}}$ is a torus, we define $T(\mathbb{Z}/\ell^n\mathbb{Z})$ to be $T_{/\mathbb{Q}_\ell}(\mathbb{Z}/\ell^n\mathbb{Z})$ for each prime ℓ and all $n \geq 1$. Given a map $\lambda : T \to T'$ between two tori, we now write $\lambda_{\ell,n}$ for the induced maps $T(\mathbb{Z}/\ell^n\mathbb{Z}) \to T'(\mathbb{Z}/\ell^n\mathbb{Z})$.

Theorem (2.5) : Given a torus T over $\mathbb{Q}$, there are constants C, C' > 0 such that we have

$$C \leq \ell^{-n\nu} \operatorname{Card}(T(\mathbb{Z}/\ell^n\mathbb{Z})) \leq C'$$

for all $n \geq 1$ and all primes ℓ , where ν is the dimension of T.

Theorem (2.6) : Let $\lambda : T \to T'$ be a surjective map between $\mathbb{Q}$-tori. Then the order of coker $\lambda_{\ell,n}$ is bounded independently of ℓ and n. If moreover λ is an

isogeny, the order of the ker $\lambda_{\ell,n}$ is similarly bounded.

Proofs : The second theorem is an obvious consequence of (2.3), (2.4). To prove (2.5), we will use (2.6) and a general philosophy due to Ono. First, we observe that (2.5) is visibly correct in the special case where $T = T_E$ is the torus attached to a finite extension E of $\mathbb{Q}$, cf. (2.1). Next we notice, by Brauer's theorem on induced characters, that there are finite extensions $K_1,\ldots,K_n$; $L_1,\ldots,L_m$ of $\mathbb{Q}$ and an integer $r > 0$ such that the two tori

$$\begin{cases} T^r \times (T_{K_1} \times \ldots \times T_{K_n}) \\ T_{L_1} \times \ldots \times T_{L_m} \end{cases}$$

are isogenous. (See [7], Th. 1.5.1.) Since (2.5) holds for the second of the two, it holds for the first by (2.6). It thus holds for T^r (using again the case $T = T_E$) and thus for T.

Corollary (2.7) : Let $\lambda : T \to T'$ be a homomorphism of $\mathbb{Q}$-tori. There exist constants C, C' > 0 such that we have

$$C \leq \frac{\mathrm{Card}(\mathrm{Im}(\lambda_{\ell,n}))}{\ell^{n\nu}} \leq C'$$

for all ℓ and n, where ν is the dimension of the image of λ.

Proof : Without loss of generality, we may suppose λ surjective. Then it is clear that our result follows from (2.5) and (2.6).

3. We now wish to deduce (1.1) from the above corollary. Before beginning to do so, we make some preliminary simplifications. It is clear that to prove (1.1) for a given A/k, we may replace k by a finite extension of k and A by an abelian variety which is isogenous to it. We thus introduce the hypothesis that A has everywhere good reduction, as we have a right to do by a well known theorem of Serre-Tate ([15], Th. 7). Secondly, after replacing A by a variety isogenous to it, we may suppose that $\mathrm{End}_k A$ contains the "integer ring" of E. Namely, if we write E as a product $E_1 \times \ldots \times E_t$ of fields, we suppose that $\mathrm{End}_k A$ contains the product $\mathcal{O}$ of the integer rings $\mathcal{O}_i$ of the E_i. In particular, this assumption enables us to write A as a product

$$A = A_1 \times \ldots \times A_i$$

where A_i has complex multiplication by $\mathcal{O}_i$. (It is clear that $[E_i : \mathbb{Q}] = 2 \dim A_i$ for each i because the first member is known to be a divisor of the second [17, Prop.2, p.39] and because of the assumption $[E : \mathbb{Q}] = 2 \dim A$.)

It is well known (see ch. II, §.5.1 of [17]) that each A_i is isogenous over $\bar{k}$ to a power of an (absolutely) simple abelian variety B_i of CM type. In proving (1.1), we may replace each A_i by the corresponding B_i (making a finite extension of k at the same time). This enables us to assume that each of the A_i occuring above is in fact <u>absolutely simple</u>. This means that each of the fields E_i is a CM field and that the "CM type" attached to each A_i is simple in a sense which will be presently recalled . This assumption, and the previous ones will be in force for the remainder of this paper. To summarize, we assume :

i) that A has everywhere good reduction over k ;

ii) that A is given as a product $A_1 \times \ldots \times A_i$ of absolutely simple abelian varieties, with each A_i having complex multiplication by the integer ring of a CM field E_i.

Proving (1.1) under these assumptions will give a proof in general.

In order to discuss the individual factors with a minimum of notation, we now temporarily suppose

iii) that $t = 1$,

i.e. that A is already absolutely simple. This assumption will be in force for the remainder of this paragraph.

To discuss the "CM-type" attached to A, and the "dual" (or reflex) CM type derived from A, we embed k and E into the complex field $\mathbb{C}$. Let L be the Galois closure of E in $\mathbb{C}$, and let

$$G = \mathrm{Gal}(L/\mathbb{Q}), \quad H = \mathrm{Gal}(L/E).$$

We introduce the convention that G acts on E on the right. Thus for example, we may view the set $\mathrm{Hom}(E,\mathbb{C})$ of embeddings of E into $\mathbb{C}$ as the coset space $H\backslash G$. We write c for the complex conjugation of $\mathbb{C}$, or any of its restrictions.

As in [17], the data $(A/k,E)$ define a CM-type $S \subseteq \mathrm{Hom}(E,\mathbb{C})$. This is a subset of $H\backslash G$ such that $H\backslash G$ is the disjoint union of S and Sc. Put

$$\tilde{S} = \{g \in G \mid Hg \in S\}.$$

The absolute simplicity of A translates into the equality ([17], Prop. 26)

$$H = \{g \in G \mid g\tilde{S} = \tilde{S}\}.$$

We say that the CM type (E,S) is simple. We symetrically introduce

$$H' = \{g \in G \mid \check{S}g = \check{S}\}$$

$$= \{g \in G \mid g\tilde{R} = \tilde{R}\},$$

where $\tilde{R}$ is the set $\tilde{S}^{-1}$ of inverses of elements of $\check{S}$. Let K be the fixed field of H', and let $R \subset \mathrm{Hom}(K,\mathbb{C})$ be the image of $\tilde{R}$ in $H'\backslash G$.

Then (K,R) is again a simple CM type, that dual to (E,S). Because (E,S) is simple, it is its own double dual (i.e. the dual of (K,R)), and it is known that k contains K. (See [17] , Props. 28 and 30.)

We may view G as acting (on the right) on the set of CM types for E, and H' is then the stabilizer of the CM type (E,S). Since the number of CM types for E is 2^d where $d = [E : \mathbb{Q}]/2$ is the dimension of A, we clearly have

$$[K : \mathbb{Q}] = (G : H') \leq 2^d. \tag{3.1}$$

If we put $d' = [K : \mathbb{Q}]/2$, then by (3.1) and the symmetry we have

$$1 + \mathrm{Log}_2 d \leq d' \leq 2^{d-1} . \tag{3.2}$$

It is known that for each $d \geq 1$, we may find a CM type (E,S) with this d such that $d' = 2^{d-1}$. (For a more precise statement, see ([16], 1.10).)

Associated to the pair of CM types (E,S), (K,R) is a homomorphism

$$\phi : T_K \to T_E ,$$

which is most easily described by giving the corresponding homomorphism ϕ^* of character groups of these tori. For F a finite extension of $\mathbb{Q}$, we write X_F for the character group of the torus T_F; this is the right Gal $(\bar{\mathbb{Q}}/\mathbb{Q})$-module consisting of integral linear combinations $\Sigma\, n_\sigma [\sigma]$ with $\sigma \in \mathrm{Hom}(F,\mathbb{C})$. (We take $\bar{\mathbb{Q}}$ to be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$.) This applies especially when F = K or E, in which case for $g \in G$ we write [g] for the embedding of F into $\mathbb{C}$ induced by g.

We define $\phi^*: X_E \to X_K$ by the formula

$$[g] \mapsto \sum_{r \in R} [rg] .$$

This makes sense because replacing g by hg ($h \in H$) has the effect of permuting the various terms $[rg]$. The map ϕ^* is visibly $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-equivariant. (Cf. [17], Prop. 29.)

Following T. Kubota [4], we refer to the dimension of the image of $\phi : T_K \to T_E$ as a rank, the rank of the CM type (E,S). This integer may be expressed as the rank of the $\mathbb{Z}$-submodule $\phi^*(X_E)$ of X_K; using the natural bases for X_K and X_E, we then see the rank as the rank of the matrix

$$(i(\tau,\sigma))_{\substack{\sigma \in H\backslash G \\ \tau \in H'\backslash G}}$$

defined by

$$i(\tau,\sigma) = \begin{cases} 1 & \text{if } \tau\sigma^{-1} \in \tilde{R} \\ 0 & \text{if not.} \end{cases}$$

(For $\tau, \sigma \in G$, and for $h \in H$, $h' \in H'$, we have $\tau\sigma^{-1} \in \tilde{R}$ if and only if $(h'\tau)(h\sigma)^{-1} \in \tilde{R}$.) It is obvious that if we exchange the roles of (E,S) and (K,R), we replace $(i(\tau,\sigma))$ by its transpose. Hence we find

Proposition (3.3) : The rank of a CM type (E,S) is equal to the rank of its dual.

It is easy to see that the rank of (E,S) satisfies the inequality

$$\mathrm{rank}(E,S) \leq d+1 .$$

For example, we have $\mathrm{Im}\,\phi \subset T$, where T is the $(d+1)$-dimensional torus such that

$$T(A) = \{x \in T_E(A) = (E \otimes_{\mathbb{Q}} A)^* \mid xx^c \in A^*\}$$

for $\mathbb{Q}$-algebras A. By the symmetry (i.e. by (3.3)), we have

$$\mathrm{rank}(E,S) \leq \min(d+1, d'+1). \tag{3.4}$$

These facts were all pointed out by Kubota [4], who calls a CM type non-degenerate if its rank is equal to $d+1$.

It is amusing to note that there is a lower bound for the rank :

$$\max(2+\mathrm{Log}_2 d,\ 2+\mathrm{Log}_2 d') \leqslant \mathrm{rank}(E,S). \tag{3.5}$$

To prove (3.5), it suffices by the symmetry to prove that rank (E,S) is at least $2+\mathrm{Log}_2 d = \mathrm{Log}_2(4d)$. We note that the image of ϕ^* contains the vectors

$$\begin{cases} \sum_r [rg] & g \in H\backslash G \\ \sum_r ([r]+[rg]) & g \in H\backslash G\ , \end{cases}$$

which we easily check to have pairwise distinct images in $X_K/2X_K$. [The only tricky point is to check that no vector in the first group is congruent mod 2 to a vector in the second. Write all vectors in the form $\sum_{g \in H'\backslash G} n_g[g]$. For vectors in the first group, we have $n_g + n_{gc} = 1$ for all g; for those in the second, we have $n_g + n_{gc} = 2$ for all g.] It follows (as Lenstra pointed out) that the image of ϕ^* generates an $\mathbf{F}_2$-subspace of $X_K/2X_K$ of dimension at least $\mathrm{Log}_2 4d$. This implies in particular the assertion about the rank.

Corollary (3.6) : Suppose that we have $d' = 2^{d-1}$. Then (E,S) is non-degenerate : we have $\mathrm{rank}(E,S) = d+1$.

Proof : We have under the hypothesis, by (3.5) and (3.4),

$$d+1 = 2+\mathrm{Log}_2 d' \leqslant \mathrm{rank}(E,S) \leqslant d+1.$$

Examples (3.7) : If $d = 1,2,3$, then the inequalities

$$2+\mathrm{Log}_2 d \leqslant \mathrm{rank}(E,S) \leqslant d+1$$

show that (E,S) is always non-degenerate. If $d = 4$, then we find

$$4 \leq \text{rank}(E,S) \leq 5 ,$$

and both possibilities may occur. Indeed, if d' = 8, then the rank is 5 by (3.6) ; we may specify examples with d' = 8 as remarked after (3.2). Similarly, if d' = 3 (note that $4 = 2^{3-1}$), we have rank(E,S) = 4 by (3.6), which we apply after switching the roles of (E,S) and its dual. (Incidentally, the CM type constructed by Mumford and described in Pohlmann [9] in connection with Hodge classes on abelian varieties gives a specific example where d = 4 but d' = 3.) A case-by-case analysis once performed by the author showed that rank(E,S) is 5 in all cases where d = 4 and d' $\geq$ 4. The tedious proof of this fact has been mislaid.

Before moving to the special case where E is an abelian extension of $\mathbb{Q}$,we mention an alternate interpretation of ϕ , or rather of the composite of ϕ and the norm map $N_{k/K} : T_k \to T_K$. We let $t_{A/k}$ be the tangent space to A/k at the origin, so that $t_{A/k}$ is a k-vector space of rank d on which E acts. It is alternately an E- vector space on which k acts. For $\alpha \in k^*$ we let $\psi(\alpha) \in E^*$ be the determinant of the E-linear map "multiplication by α" on $t_{A/k}$. The map $\psi : k^* \to E^*$ is obviously induced by an algebraic map $T_k \to T_E$, which we again denote by ψ , (cf. [15], p.511).

Proposition (3.8) : The map ψ is the composition of the norm map $N_{k/K} : T_k \to T_K$ and the map $\phi : T_K \to T_E$.

This is well known, and is used implicitly in [15], § 7. For a proof, see [16], § 1.3.

Corollary (3.9) : The rank of (E,S) is equal to the dimension of the image of ψ.

Proof : The map $N_{k/K}$ is surjective .

In addition to assumptions (i),(ii), (iii) introduced above, we suppose now and for the remainder of this §, that E is an abelian extension of $\mathbb{Q}$. Then L = K = E, and G = Gal(E/$\mathbb{Q}$). We may view ϕ^* as an endomorphism of $X_E = X_K$.

We calculate the effect of ϕ^* on the basis vectors $v_\chi = \sum_{g \in G} \chi(g)[g]$ of $X_E \otimes \mathbb{C}$, where χ runs over the set of $\mathbb{C}^*$-valued characters of the abelian group G. We find

$$\phi^*(v_\chi) = \left(\sum_{s \in S} \chi(s) \right) v_\chi$$

for each χ. This gives

Proposition (3.10) (cf. [4], lemma 2) : The rank of (E,S) is the number of characters χ for which the sum

$$\chi(S) = \sum_{s \in S} \chi(s)$$

is non zero.

Note that when χ is an even character (i.e. $\chi(c) = +1$), we have $\chi(S) \neq 0$ if and only if χ is non trivial. The rank is thus one plus the number of odd characters χ for which $\chi(S)$ is non zero.

We close this paragraph with some examples.

(3.11) Let $p \geq 5$ be a prime, and let E be the field $\mathbb{Q}(\mu_p)$ of p^{th} roots of unity. We identify G with $(\mathbb{Z}/p\mathbb{Z})^*$ in the usual way. For $g \in G$, write $\langle g \rangle$ for the integer between 1 and $p-1$ which represents g mod p. Let a be an integer satisfying $1 \leq a \leq p-2$. The set

$$S = \{g \in G \mid \langle g \rangle + \langle ag \rangle < p\}$$

is readily seen to be a CM type for E. It is simple if and only if a is of order $\neq 3$ in $(\mathbb{Z}/p\mathbb{Z})^*$, which we suppose to be the case. (See, e.g., [3], Th. 2.) For χ odd, one finds

$$\chi(S) = L(0, \chi)(1 + \chi^{-1}(a) - \chi^{-1}(1+a)),$$

by a computation generalizing that of [4] , lemma 3. Thus (E,S) is "degenerate" if and only if there is an odd character χ satisfying the unlikely equality

$$\chi(1+a) = \chi(1) + \chi(a) .$$

Thus S is non-degenerate, for example, if a = 1. Greenberg [2] found that S is degenerate for p = 67 and a = 10, 19, 47, 56, 60. For sufficiently large primes $p \equiv 7 \pmod{12}$, Lenstra and Stark noticed that there is always an a for which S is degenerate (loc. cit.).

(3.12) Let E be the field of 32^{nd} roots of unity. As usual, we identify G with $(\mathbb{Z}/32\,\mathbb{Z})^*$. Let S be the subset {1, 7, 13, 15, 21, 23, 27, 29} of G. Then S is a "simple" CM type, and $\chi(S)$ vanishes when χ is the character

$$x \longmapsto \begin{cases} -1 & \text{if } x \equiv 3 \pmod 4 \\ +1 & \text{if } x \equiv 1 \pmod 4 \end{cases} .$$

Thus S is degenerate . (This example was found by Lenstra.) Similarly, if we take S' = {1, 7, 9, 11, 13, 15, 27, 29} , then S' is again a simple CM type such that $\chi(S') = 0$ for both odd characters χ' of order 2.

(3.13) Take E this time to be the field of 19^{th} roots of unity, so that G is $(\mathbb{Z}/19\,\mathbb{Z})^*$. Let S = {1,3,4,5,6,7,8,10,17} . Then S is a simple CM type such that $\chi(S) = 0$ for both (odd) characters χ of order 6. (This example was provided by Serre in response to a question of Masser.)

(3.14) Let p,q,r be distinct odd primes, and let G be the cyclic group $\mathbb{Z}/2pqr\,\mathbb{Z}$. Let E be a Galois extension of $\mathbb{Q}$ with $\mathrm{Gal}(E/\mathbb{Q}) \simeq G$. Let S be the subset of G consisting of those elements having order 1, pq r, 2p, 2q, 2r, 2pq, 2pr, or 2qr. It is evident that (E,S) is a CM type, and it is simple because S contains the identity element of G but no non-trivial subgroup of G. A calculation shows that, for χ odd, we have $\chi(S) = 0$ if and only if χ has order 2pqr. Hence we have

$$\operatorname{rank}(E,S) = 1 + pqr - (p-1)(q-1)(r-1).$$

This example, recently constructed by Lenstra, shows that the rank may be quite small relative to $[E : \mathbb{Q}]$, even in the case where the CM field E is abelian.

4. We now return to the situation outlined at the beginning of § 3, where the abelian variety A/k satisfies conditions (i) and (ii), but we no longer assume that E is a single field. We wish to prove (1.1) for A.

For $N \geq 1$, let A_N be the $\mathrm{Gal}(\bar{k}/k)$-module of N-division points on A, and let G_N be the image of the representation

$$\rho_N : \mathrm{Gal}(\bar{k}/k) \to \mathrm{Aut}\, A_N$$

giving the action of $\mathrm{Gal}(\bar{k}/k)$ on A_N. Thus G_N is the Galois group over k of the division field $k(A_N)$, and the order of G_N is the degree $d(N)$ of this field. Since A has everywhere good reduction over k, $k(A_N)/k$ is ramified only at primes of k dividing N. Thus, if N and M are relatively prime, $k(A_N) \cap k(A_M)$ is contained in the Hilbert class field of k. After replacing k by its Hilbert class field, we thus find that the function

$$N \longmapsto d(N)$$

is "multiplicative" in the usual arithmetic sense. Thus to prove (1.1) it suffices to obtain for each prime ℓ and each integer $n \geq 1$ an inequality

$$(4.1) \qquad c \leq \frac{d(\ell^n)}{\ell^{n\nu}} \leq c'$$

in which C and C' are constants depending on A, k, E, and where $\nu \geq 0$ is an integer.

We recall now the decomposition $A = A_1 \times \ldots \times A_t$. For each i, let $\psi_i : T_k \longrightarrow T_{E_i}$ be the map ψ of (3.8) made with the abelian variety A of § 3 taken to be A_i. Let

$$\psi : T_k \to T_E = T_{E_1} \times \ldots \times T_{E_t}$$

be the product of the ψ_i. We will prove that (4.1) holds with ν equal to the dimension of the image of ψ. Thus if A is simple (i.e. t = 1), then ν is the rank of the CM type attached to A, in the sense of § 3.

For a prime ℓ, let ρ_{ℓ^∞} be the ℓ-adic representation of $\mathrm{Gal}(\bar{k}/k)$ attached to A, i.e. the projective limit of the ρ_{ℓ^n} $(n \geq 1)$. A priori, ρ_{ℓ^∞} takes values in the group of automorphisms of the Tate module $\varprojlim A_{\ell^n}$ of A, but it is well known that the values of ρ_{ℓ^∞} lie in the subgroup $(\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell)^*$ of $\mathrm{Aut}(\varprojlim A_{\ell^n})$, cf. [15, § 4, Cor. 2]. Hence ρ_{ℓ^∞} is abelian and may be viewed as a map

$$I_k \longrightarrow (\mathcal{O} \otimes \mathbb{Z}_\ell)^*,$$

where I_k is the group of idèles of k. For (4.1), no harm is done in replacing I_k by the product $\prod_v U_v$ of the groups of units at the non-archimedean completions of k, since this product has finite index in the abelianized Galois group of k. (In fact, this replacement is the replacement of k by its Hilbert class field which we discussed above.) Now ρ_{ℓ^∞} kills the group U_v if v is not of residue characteristic ℓ. Hence, we will view ρ_{ℓ^∞} as a map

$$\prod_{v|\ell} U_v \longrightarrow (\mathcal{O} \otimes \mathbb{Z}_\ell)^*$$

i.e., as a map

$$T_k(\mathbb{Z}_\ell) \to T_E(\mathbb{Z}_\ell),$$

cf. (2.1).

Let $\lambda : T_k \to T_E$ be the "inverse" of ψ, i.e., the map $x \mapsto \psi(x^{-1})$. Then ρ_{ℓ^∞} is just the map on $\mathbb{Z}_\ell$-points induced by λ, in view of Theorem 11 of [15] and its corollaries. Now ρ_{ℓ^n} for $n \geq 1$ is the composition of the map

ρ_{ℓ^∞} with the reduction map $(\mathcal{O} \otimes \mathbb{Z}_\ell)^* \to (\mathcal{O}/\ell^n\mathcal{O})^*$, i.e., $T_E(\mathbb{Z}_\ell) \to T_E(\mathbb{Z}/\ell^n\mathbb{Z})$.

We have an evident commutative diagram

$$\begin{array}{ccc} T_k(\mathbb{Z}_\ell) & \longrightarrow & T_E(\mathbb{Z}_\ell) \\ \downarrow & & \downarrow \\ T_k(\mathbb{Z}/\ell\mathbb{Z}) & \longrightarrow & T_E(\mathbb{Z}/\ell\mathbb{Z}) \end{array}$$

in which the two vertical maps are reduction maps, the top horizontal map is ρ_{ℓ^∞} and the lower horizontal map is the map denoted $\lambda_{\ell,n}$ toward the end of § 1. Hence G_{ℓ^n} is just the image of $\lambda_{\ell,n}$ (for $n \geq 1$), and $d(\ell^n)$ is the order of $\mathrm{Im}(\lambda_{\ell,n})$. Thus (1.1) is a special case of (2.7). Finally, again by (2.7), the integer ν of (1.1) is the dimension of the image of λ, or in other words the dimension of the image of ψ. This establishes (4.1) and the claim concerning the value of ν.

BIBLIOGRAPHY

[1] Deligne, P., Cycles de Hodge absolus et périodes des intégrales des variétés abéliennes, rédigé par J. L. Brylinski. This volume.

[2] Greenberg, R., On the Jacobian variety of some algebraic curves. Preprint, 1978.

[3] Koblitz, N. and Rohrlich, N., Simple factors in the Jacobian of a Fermat curve. Canadian J. Math. 30, 1183-1205 (1978).

[4] Kubota, T., On the field extension by complex multiplication. Trans. AMS 118, n° 6, 113-122 (1965).

[5] Lang, S., Algebraic groups over finite fields. Am. J. Math 78, 555-563 (1956).

[6] Masser, D. W., On quasi-periods of abelian functions with complex multiplication. This volume.

[7] Ono, T., Arithmetic of algebraic tori. Ann. of Math. 74, 101-139 (1961).

[8] Ono, T. , On the Tamagawa number of algebraic tori. Ann. of Math. 78 , 47-73 (1963).

[9] Pohlmann, H., Algebraic cycles on abelian varieties of complex multiplication type. Ann. of Math. 88, 161-180 (1968).

[10] Ribet, K. A. , Kummer theory on extensions of abelian varieties by tori. Duke Math. J. 46, 745-761 (1979).

[11] Serre, J. P. , Groupes Algébriques et Corps de Classes. Hermann, Paris, 1959.

[12] Serre, J. P. , Corps Locaux. Deuxième édition revue et corrigée. Hermann, Paris, 1968.

[13] Serre, J. P. , Letter to D. Masser, November, 1975.

[14] Serre, J. P. , Représentations ℓ-adiques. In Algebraic Number Theory (Int. Symp., Kyoto, 1976), Japan Society for the Promotion of Science, Tokyo, 1977.

[15] Serre, J. P. and Tate, J. , Good reduction of abelian varieties. Ann. of Math. 88, 492-517 (1968).

[16] Shimura, G. , Arithmetic quotients of bounded symmetric domains. Ann. of Math. 91, 144-222 (1970).

[17] Shimura, G. and Taniyama, Y. , Complex Multiplication of Abelian Varieties and its Applications to Number Theory. Publ. Math. Soc. Japan n°6, Tokyo, 1961.

[18] Weil, A. , On a certain type of characters of the idèle-class group of an algebraic number-field. Proc. International Symp. on Algebraic Number Theory, Tokyo-Nikko, 1-7 (1955) = Collected Papers [1955c].

Ecole Polytechnique
Centre de Mathématiques
91128 Palaiseau Cedex (France)