Good reduction of abelian varieties

By JEAN-PIERRE SERRE and JOHN TATE*

As Ogg has shown, the fact that an elliptic curve has good reduction can be seen from the unramifiedness of its points of finite order (Woods Hole, 1964; see also [15]). It is easy to extend this criterion to abelian varieties, using the powerful tool provided by Néron's minimum models, cf. § 1 and § 2 below. More precisely, we consider both good reduction over a given ground field, or over some finite extension of it (we call the latter "potential good reduction"). The second case has an application (as in Ogg [15]) to conductor questions, cf. § 3. In the rest of the paper we give applications to abelian varieties with complex multiplication. Such a variety has potential good reduction everywhere (§ 5), it has good reduction outside the support of a corresponding Grössencharakter (§ 7) and, under suitable conditions, it can be twisted so as to have good reduction at a given finite set of places (§ 5). These facts generalize results of Deuring [7] relative to the elliptic case.

1. The criterion of Néron-Ogg-Šafarevič

Let K be a field, v a discrete valuation of K, and O_v the valuation ring of v; the residue field $O_v/\mathfrak{m}_v$ of v will be denoted by k_v, or simply by k. Let K_s be a separable closure of K and $\bar{v}$ an extension of v to K_s. We denote the inertia group and decomposition group of $\bar{v}$ by $I(\bar{v})$ and $D(\bar{v})$, respectively. They are subgroups of the Galois group $\mathrm{Gal}(K_s/K)$ and we have a canonical isomorphism

$$D(\bar{v})/I(\bar{v}) \cong \mathrm{Gal}\,(\bar{k}/k)$$

where $\bar{k}$, the residue field of $\bar{v}$, is an algebraic closure of k.

A Galois extension L of K contained in K_s is unramified at v if and only if L is fixed by $I(\bar{v})$. More generally, if $\mathrm{Gal}\,(K_s/K)$ acts on a set T, one says that T is *unramified at* v if $I(\bar{v})$ acts trivially on it; this does not depend on the choice of $\bar{v}$ because the inertia groups of two such choices are conjugate in $\mathrm{Gal}\,(K_s/K)$. In other words, T is unramified at v if and only if the decomposition group $D(\bar{v})$ acts on T through its homomorphic image $\mathrm{Gal}\,(\bar{k}/k)$.

Let A be an abelian variety over K. One says that A has *good reduction* at v if there exists an abelian scheme A_v over $\mathrm{Spec}\,(O_v)$(cf. [13, Ch. 6]) such

* Work on this paper was partially supported by the National Science Foundation and the Institut des Hautes Etudes Scientifiques.

that $A \approx A_v \times_{O_v} K$; this is equivalent to saying that there exists on A a "structure of v-variety" with respect to which A has "no defect for v" in the sense of Shimura-Taniyama [18, p. 94].

If $m \in \mathbf{Z}$ is prime to the characteristic of K, we put

$$A_m = \operatorname{Hom}\left(\mathbf{Z}/m\mathbf{Z},\ A(K_s)\right) .$$

Hence A_m is the group of points of order dividing m in the group $A(K_s)$ of K_s-points of A; it is known (cf. for instance [12, Ch. VII]) that A_m is a free $\mathbf{Z}/m\mathbf{Z}$-module of rank $2\dim(A)$ on which $\operatorname{Gal}(K_s/K)$ acts continuously.

Similarly, if l is a prime number, $l \neq \operatorname{char}(K)$, we put

$$T_l(A) = \operatorname{inv}\lim A_{l^n} = \operatorname{Hom}\left(\mathbf{Q}_l/\mathbf{Z}_l,\ A(K_s)\right) .$$

This is a free module of rank $2\dim(A)$ over the ring $\mathbf{Z}_l$ of l-adic integers; the group $\operatorname{Gal}(K_s/K)$ acts continuously on $T_l(A)$.

THEOREM 1. *Let A be an abelian variety over K. Suppose that the residue field k of v is perfect*[1], *and let l be a prime number different from* char (k). *The following properties are equivalent:*

(a) *A has good reduction at v.*

(b) *A_m is unramified at v for all m prime to* char (k).

(b′) *There exist infinitely many integers m, prime to* char (k), *such that A_m is unramified at v.*

(c) *$T_l(A)$ is unramified at v.*

Before proving this theorem, we give some immediate corollaries and remarks.

COROLLARY 1. *If $T_l(A)$ is unramified at v for one l different from the residue characteristic, it is so for all such l.*

Indeed, (a) does not depend on l.

COROLLARY 2. *Let A' be an abelian variety over K and $f: A \to A'$ a surjective homomorphism. If A has good reduction at v, then so does A'. In particular, two K-isogenous abelian varieties, and especially two K-dual abelian varieties, either both have, or both have not, good reduction at v.*

Indeed, f maps $T_l(A)$ onto a subgroup of finite index of $T_l(A')$ and, if $I(\bar{v})$ acts trivially on the former, it does also on the latter.

COROLLARY 3. *Let $0 \to A' \to A \to A'' \to 0$ be an exact sequence of abelian varieties over K. Then A has good reduction at v if and only if both A' and A'' do.*

[1] We assume k perfect because Néron does (cf. [14]), but this assumption is not necessary according to results announced by Raynaud (C. R. Acad. Sci., **262** (1966), 413–416).

Indeed, A is K-isogenous to $A' \times A''$.

COROLLARY 4. *Let K' be an extension field of K and v' an extension of v to K' such that the map $I(\bar{v}') \to I(\bar{v})$ of the corresponding inertia groups is surjective* (for instance, $K' = \hat{K}$, or K' finite extension of K unramified at v'). *Let $A' = A \times_K K'$. If A' has good reduction at v', then A has good reduction at v.*

Indeed, $T_l(A) = T_l(A')$ is unramified at v if it is so at v'.

Remarks (1). Condition (c) of Theorem 1 gives a criterion[2] for good reduction which we call the "criterion of Néron-Ogg-Šafarevič". Indeed, it follows easily (see below) from Néron's theory of minimum models [14, Ch. II]; on the other hand, Ogg [15] used a closely related criterion for elliptic curves (see remark 1 in § 2), which seems also to have been known to Šafarevič.

(2) The fact that (a) implies (b), (b′) and (c) is well known (see for instance [18, p. 150, Prop. 18]). Corollary 2 is also known, and due to Koizumi-Shimura [11, Th. 4].

PROOF OF THEOREM 1. We note first that (c) is equivalent to saying that A_{l^n} is unramified at v for all n. Hence (b) $\Rightarrow$ (c) $\Rightarrow$ (b′), and it remains to prove that (a) $\Rightarrow$ (b) and (b′) $\Rightarrow$ (a).

Let A_v be the Néron minimum model of A relative to v (cf. [14, Ch. II]); thus, A_v is a smooth group scheme of finite type over O_v, together with an isomorphism $A_v \times_{O_v} K \simeq A$, which represents the functor

$$Y \longmapsto \mathrm{Hom}_K\,(Y \times_{O_v} K, A)$$

on the category of schemes Y smooth over O_v. The abelian variety A has good reduction at v if and only if A_v is *proper* over O_v, i.e., is an abelian scheme over O_v (cf. [13, *loc. cit.*]).

Let $\tilde{A}_v = A_v \times_{O_v} k$ be the special fiber of A_v. It is a commutative algebraic group over the residue field k. If m is prime to char (k), we define $\tilde{A}_m$, as above, by

$$\tilde{A}_m = \mathrm{Hom}\,(\mathbf{Z}/m\mathbf{Z}, \tilde{A}(\bar{k}))\ .$$

It is known (cf. [5], [17]) that the connected component $\tilde{A}^0$ of $\tilde{A}$ is an extension of an abelian variety B by a linear group H, and that $H = S \times U$, where S is a torus and U is unipotent.

LEMMA 1. *Let c be the index of $\tilde{A}^0$ in $\tilde{A}$. The $\mathbf{Z}/m\mathbf{Z}$-module $\tilde{A}_m$ is an extension of a group of order dividing c by a free $\mathbf{Z}/m\mathbf{Z}$-module of rank*

[2] Grothendieck, to whom one of us pointed out this criterion in 1964, has generalized it considerably: see [10, Cor. 4.2].

equal to $\dim(S) + 2\dim(B)$.

The index of $\tilde{A}^0_m$ in $\tilde{A}_m$ divides $c = (\tilde{A} : \tilde{A}_0)$. On the other hand, the fact that $H(\bar{k})$ is m-divisible shows that the sequence

$$0 \longrightarrow H_m \longrightarrow \tilde{A}^0_m \longrightarrow B_m \longrightarrow 0$$

is exact. Since H_m and B_m are free $\mathbf{Z}/m\mathbf{Z}$-modules of rank $\dim(S)$ and $2\dim(B)$ respectively, $\tilde{A}^0_m$ is free of rank $\dim(S) + 2\dim(B)$. This proves the lemma.

Let us now denote by A^I_m the set of elements of A_m invariant under the action of the inertia group $I = I(\bar{v})$.

LEMMA 2. *The reduction map defines an isomorphism of A^I_m onto $\tilde{A}_m$. This isomorphism commutes with the action of $D(\bar{v})$.*

More precisely, let L be the fixed field of the inertia group I. We have

$$\operatorname{Hom}\big(\mathbf{Z}/m\mathbf{Z}, A(L)\big) = \operatorname{Hom}_I\big(\mathbf{Z}/m\mathbf{Z}, A(K_s)\big) = A^I_m \ .$$

On the other hand, let O_L be the ring of $\bar{v}$-integers of L; its residue field is $\bar{k}$. Since O_L is a union of étale extensions of O_v, the group $A_v(O_L)$ of the O_L-points of A_v is equal to $A(L)$, by the universal property of the Néron model A_v. The reduction map $O_L \rightarrow \bar{k}$ defines a homomorphism

$$r\colon A(L) = A_v(O_L) \longrightarrow \tilde{A}(\bar{k}) \ .$$

Since O_L is henselian, and A_v is smooth, r is surjective. Moreover, since m is prime to char (k), multiplication by m is an étale endomorphism of A_v; using again the fact that O_L is henselian, this shows that the kernel of r is uniquely divisible by m. Hence r defines a homomorphism

$$\operatorname{Hom}\big(\mathbf{Z}/m\mathbf{Z}, A(L)\big) = A^I_m \longrightarrow \operatorname{Hom}\big(\mathbf{Z}/m\mathbf{Z}, \tilde{A}(\bar{k})\big) = \tilde{A}_m \ ;$$

this isomorphism commutes with the action of $D(\bar{v})$ by *transport de structure*; this proves Lemma 2.

Now, if A has good reduction at v, $\tilde{A}$ is an abelian variety and $\tilde{A}_m$ is free of rank $2\dim(\tilde{A}) = 2\dim(A)$. By Lemma 2, the same is true for A^I_m, hence $A_m = A^I_m$; this shows that (a) implies (b).

Conversely, assume that (b′) holds, i.e., that there exist arbitrarily large integers m, prime to char (k), such that $A_m = A^I_m$. Taking $m > c = (\tilde{A}: \tilde{A}^0)$, and applying Lemmas 1 and 2 we see that

$$\dim(S) + 2\dim(B) \geqq 2\dim(A) \ ,$$

and, since $\dim(A) = \dim(U) + \dim(S) + \dim(B)$, this means that $U = S = 0$, i.e., that $\tilde{A}$ is *proper* over k. To prove (a), it remains to show that A_v itself is proper over O_v. This follows from:

LEMMA 3. *Let X_v be a smooth scheme over O_v whose general fiber*

$X = X_v \times_{O_v} K$ is geometrically connected and whose special fiber $\tilde{X}$ is proper. Then X_v is proper over O_v and $\tilde{X}$ is geometrically connected.

We may assume O_v is complete, since geometrical connectedness (of X) ascends and properness (of X_v) descends, cf. [9, IV, Prop. 2.7.1]. By [9, III, Cor. 5.5.2], there exist open disjoint subschemes Z and Z' of X_v, with $X_v = Z \cup Z'$, Z proper and $\tilde{X} \subset Z$. Since X is connected, this implies $Z' = \varnothing$, hence $X_v = Z$ is proper over O_v. The fact that $\tilde{X}$ is geometrically connected then follows from Zariski's connectedness theorem (*loc. cit.*).

2. Potential good reduction

The assumptions being as in § 1 and Theorem 1, we say that A has *potential good reduction at v* if there exists a finite extension K' of K and a prolongation v' of v to K' such that $A \times_K K'$ has good reduction at v'. Another possible terminology for this property would be to say that A is *of integral modulus at v*. Indeed, if A is an elliptic curve, then A has potential good reduction at v if and only if its modular invariant j is integral at v (cf. Deuring [6, p. 225]); one can prove an analogous result in higher dimension by using, instead of the j-line, the moduli schemes for polarized abelian varieties constructed by Mumford [13].

Let l be a prime number different from the residue characteristic, and let

$$\rho_l\colon \mathrm{Gal}\,(K_s/K) \longrightarrow \mathrm{Aut}\,(T_l)$$

denote the l-adic representation corresponding to the Galois module $T_l = T_l(A)$.

THEOREM 2. (i) *The abelian variety A has potential good reduction at v if and only if the image by ρ_l of the inertia group $I(\bar{v})$ is finite.*

(ii) *When this is the case, the restriction of ρ_l to $I(\bar{v})$ is independent of l in the following sense: its kernel is the same for all l, and its character has values in $\mathbf{Z}$ independent of l.*

Assertion (i) is a trivial consequence of Theorem 1. Since (ii) is concerned only with the inertia group, we may assume that K is henselian with algebraically closed residue field (replacing it, if necessary, by the field L introduced in the proof of Theorem 1); the group $\mathrm{Gal}\,(K_s/K)$ is now equal to its inertia subgroup $I(\bar{v})$. Let $\bar{K}$ be an algebraic closure of K_s and K' a finite subextension of $\bar{K}$; let $G_{K'} = \mathrm{Gal}(\bar{K}/K') = \mathrm{Gal}(K_s/K_s \cap K'))$ be the corresponding subgroup. Theorem 1 shows that the abelian variety $A' = A \times_K K'$ has good reduction at v if and only if $G_{K'}$ is contained in the kernel of ρ_l; hence this kernel is independent of l. Choose now a finite Galois extension K'/K having this property, and let A'_v be the Néron model of A'; it is an abelian scheme over the ring O'_v of integral elements of K'. The Galois group $G = \mathrm{Gal}(K'/K)$ acts on $A' = A \times_K K'$ *via* its action on K'; the functoriality of the Néron model implies that this action extends uniquely to an action of G on the scheme A'_v; the map

$$A'_v \longrightarrow \mathrm{Spec}\,(O'_v)$$

is compatible with the action of G on both schemes. Since G acts trivially on the residue field k, it acts on the special fiber $\tilde{A}'$, which is an abelian variety over k, by k-automorphisms (i.e. by "*algebraic*" automorphisms). Hence, by a theorem of Weil ([21, n° 68] or [12, Ch. VII]), the action of G on $T_l(\tilde{A}')$ has an *integral* character, which is independent of l. Assertion (ii) follows now from the canonical isomorphisms

$$T_l(A) \approx T_l(A') \approx T_l(\tilde{A}') \ .$$

COROLLARY 1. *Suppose that the residue field k is finite of characteristic p, and that, for some $l \neq p$, the image of* $\mathrm{Gal}\,(K_s/K)$ *in* $\mathrm{Aut}\,(T_l)$ *is abelian. Then A has potential good reduction at v.*

By Corollary 4 of Theorem 1, we can assume that K is complete; local class field theory then shows that the image of the inertia group I in $\mathrm{Aut}\,(T_l)$ is a quotient of the group U_K of units of K. But U_K is the product of a finite group and a pro-p-group P. Since $l \neq p$, the image of P in $\mathrm{Aut}\,(T_l)$ intersects the pro-l-group $1 + l \cdot \mathrm{End}\,(T_l)$ only in the neutral element, so the image of P maps injectively into the finite group $\mathrm{Aut}\,(T_l/lT_l)$ and is finite. Hence the image of I in $\mathrm{Aut}\,(T_l)$ is finite.

COROLLARY 2. *Suppose A has potential good reduction at v. Let m be an integer $\geqq 3$ and prime to $p =$* $\mathrm{char}\,(k)$; *let $K(A_m)$ be the smallest subextension of K_s over which the elements of A_m are rational. Then*

(a) *The inertia group (relative to $\bar{v}$) of the extension $K(A_m)/K$ is independent of m; this extension is tamely ramified if $p > 2d + 1$, where $d =$* $\dim(A)$.

(b) *The extension $K(A_m)/K$ is unramified if and only if A has good reduction at v.*

For each prime $l \neq p$, let $l' = l$ for $l \geqq 3$ and $l' = 4$ if $l = 2$. The kernel of $\mathrm{Aut}\,(T_l) \to \mathrm{Aut}\,(T_l/l'T_l) = \mathrm{Aut}\,(A_{l'})$ has no element of finite order except 1, and therefore meets the finite group $\rho_l(I(\bar{v}))$ only in the neutral element. Since m is divisible by l' for some l, it follows that the inertia group of the Galois extension $K(A_m)/K$ is $I(\bar{v})/N$, where N is the common kernel of the restrictions of the ρ_l to $I(\bar{v})$; this proves the first part of (a). By Theorem 1, this inertia group is trivial if and only if A has good reduction at v, hence (b).

Assume now that $K(A_m)/K$ is wildly ramified, i.e., that the order of $I(\bar{v})/N$ is divisible by p. Then, for every odd prime $l \neq p$, the number

$$\mathrm{Card}\,(\mathrm{Aut}\,(A_l)) = l^{d(2d-1)} \prod_{n=1}^{n=2d} (l^n - 1)$$

is divisible by p, and consequently the exponent of $l \bmod p$ is $\leqq 2d$. Taking l to be a primitive root mod p (by Dirichlet's theorem) we conclude that $p - 1 \leqq 2d$; this proves the second part of (a).

COROLLARY 3. *Suppose O_v is henselian with algebraically closed residue field, and A has potential good reduction at v. There is a minimal subextension L/K of $\bar{K}/K$ over which A acquires good reduction; it is a Galois extension, equal to $K(A_m)$ for all $m \geqq 3$ prime to* char (k); *the Galois group* Gal (K_s/L) *is equal to* Ker (ρ_l) *for all $l \neq$* char (k).

This follows from Corollary 2 and the fact that Gal $(K_s/K) = I(\bar{v})$.

Remarks. (1) Part (b) of Corollary 2 is due to Ogg [15] in the elliptic case. In the general case, there is an alternate proof for it, independent of Theorem 1, based on the "fine" moduli schemes of polarized abelian varieties constructed by Mumford [13, Ch. 7, § 2]. Indeed, the abelian variety A, equipped with any polarization, defines a K-point of such a moduli scheme which "becomes integral" after extension of the ground field and is therefore integral to begin with.

(2) Part (a) of Corollary 2 suggests that, for abelian varieties of dimension d (hence also for curves of genus d), it is the primes $p \leqq 2d + 1$ which can play an especially nasty role. This is well known for elliptic curves ($p = 2, 3$), and the same set of bad primes seems to arise in other connections. For instance, a function field of one variable of genus d is "conservative" if the characteristic p is $> 2d + 1$ (cf. [19]).

The case of a finite residue field. We assume here that k is *finite*, and we denote by F_v the Frobenius generator of Gal $(\bar{k}/k)$. Let σ be an element of $D(\bar{v})$ whose image in Gal $(\bar{k}/k)$ is F_v, and let A be an abelian variety over K which has potential good reduction at v. We want to give some properties of $\rho_l(\sigma) \in \mathrm{Aut}\,(T_l(A))$, when $l \neq$ char (k). We may assume, as above, that the Galois group $G =$ Gal (K_s/K) is equal to the decomposition group $D(\bar{v})$. Let Γ_σ denote the closure of the subgroup of G generated by σ; the projection map $G \rightarrow$ Gal $(\bar{k}/k)$ defines an isomorphism of Γ_σ onto Gal$(\bar{k}/k)$; in particular, G is the semi-direct product of Γ_σ and $I(\bar{v})$. Let now H be the kernel of the restriction of ρ_l to $I(\bar{v})$; this is a closed invariant subgroup of G, which is open in $I(\bar{v})$(cf. Theorem 2). Hence $H \cdot \Gamma_\sigma$ is an open subgroup of G. Let K' be the subextension of K corresponding to $H \cdot \Gamma_\sigma$; the residue field of K' is k. On the other hand, $A' = A \times_K K'$ has good reduction, hence its special fiber

$\tilde{A}'$ is an abelian variety defined over k. The reduction map r: $T_l(A') \to T_l(\tilde{A}')$ is then an isomorphism (cf. Lemma 2); hence $H \cdot \Gamma_\sigma = \mathrm{Gal}(K_s/K')$ acts on $T_l(A')$ *via* its quotient $\mathrm{Gal}(\bar{k}/k)$. Since the image of σ in the latter group is F_v, we then see that the action of σ on $T_l(A') = T_l(A)$ is transformed by r into the action of the *Frobenius endomorphism* of the k-abelian variety A'. Hence, using Weil's results:

THEOREM 3. *The characteristic polynomial of $\rho_l(\sigma)$ has integral coefficients independent of l. The absolute values of its roots are equal to $(Nv)^{1/2}$, where $Nv = \mathrm{Card}\,(k)$.*

Moreover:

COROLLARY. *Let s be an element of $D(\bar{v})$ whose image in* $\mathrm{Gal}(\bar{k}/k)$ *is an integral power F_v^n, $n \in \mathbf{Z}$, of the Frobenius element F_v. The characteristic polynomial of $\rho_l(s)$ has rational coefficients independent of l. The absolute values of its roots are equal to $(Nv)^{n/2}$.*

When $n = 0$, one has $s \in I(\bar{v})$ and the assertion follows from Theorem 2. If $n \neq 0$, we may suppose that $n > 0$; replacing K by its unramified extension of degree n, we are reduced to the case $n = 1$, hence to Theorem 3.

3. Local invariants of abelian varieties with potential good reduction

We assume here that O_v is *henselian* (for instance complete) and that its residue field k is *algebraically closed*. Let A be an abelian variety over K, and l be a prime number different from char (k). The Galois module A_l is a finite dimensional vector space over the field $\mathbf{Z}/l\mathbf{Z}$. Let $\delta_l = \delta(K, A_l)$ be its "measure of wild ramification" (we follow here the notations of Ogg [15]; see also Raynaud's exposé [16]). When A is of dimension 1, Ogg (*loc. cit.*) has proved that δ_l is independent of l and it has been conjectured that the same is true in higher dimension as well[3]. We prove here that this is the case *when A has potential good reduction.*

More precisely, let L/K be a finite Galois extension of K, contained in K_s, such that $A \times_K L$ has good reduction; such an extension exists since A is supposed to have potential good reduction, cf. Corollary 3 to Theorem 2. Let $G = \mathrm{Gal}(L/K)$, and let a_G (resp. b_G) denote the Artin character (resp. the Swan character) of G (cf. Ogg, *loc. cit.*, § 1). Let φ_A be the character of the repre-

[3] Grothendieck has told us that he can prove this conjecture. His proof will be included in a forthcoming seminar (SGA 7). He also shows the existence of a finite extension L/K having the following property:

The connected component of the special fiber of the Néron model of $A \times_K L$ is an extension of an abelian variety by a torus.

Another proof of the existence of such a "semi-stable reduction" has been given by Mumford, under the assumption that char$(k) \neq 2$.

sentation of G in $T_l(A)$; by Theorem 2, φ_A takes values in $\mathbf{Z}$ and is independent of l. If f and g are functions on G, define their scalar product $\langle f, g\rangle$ as usual by

$$\langle f, g\rangle = \frac{1}{n}\sum_{s\in G} f(s^{-1})g(s)\ , \qquad \text{where } n = \operatorname{Card}(G) = [L\colon K]\ .$$

THEOREM 4. *Assume A has potential good reduction. Then*

$$\delta_l = \langle b_G, \varphi_A\rangle\ .$$

In particular, δ_l is independent of l.

Let P_l be a $\mathbf{Z}_l[G]$-projective module whose character is b_G, so that

$$\delta_l = \dim_{\mathbf{Z}/l\mathbf{Z}} \cdot \operatorname{Hom}_G(P_l, A_l)\ ,$$

(cf. Ogg, *loc. cit.*). Since $A_l = T_l/lT_l$ and P_l is projective, we have

$$\operatorname{Hom}_G(P_l, A_l) \simeq \mathbf{Z}/l\mathbf{Z} \otimes \operatorname{Hom}_G(P_l, T_l)\ ,$$

hence

$$\begin{aligned}\delta_l &= \operatorname{rank}_{\mathbf{Z}_l} \operatorname{Hom}_G(P_l, T_l) = \dim_{\mathbf{Q}_l} \operatorname{Hom}_G(\mathbf{Q}_l \otimes P_l, \mathbf{Q}_l \otimes T_l)\\ &= \langle b_G, \varphi_A\rangle\ ,\end{aligned}$$

q.e.d.

COROLLARY. *Let ε be the codimension of the invariants of* Gal $(\bar{K}/K)$ *in* $\mathbf{Q}_l \otimes T_l$. *Then*

$$\varepsilon + \delta_l = \langle a_G, \varphi_A\rangle\ .$$

Indeed, $\varepsilon = 2d - \langle 1, \varphi_A\rangle$, where $d = \dim(A)$. Hence, if r_G denotes the character of the regular representation of G, we have

$$\varepsilon = \langle r_G - 1, \varphi_A\rangle$$

and

$$\varepsilon + \delta_l = \langle b_G + r_G - 1, \varphi_A\rangle\ .$$

The corollary follows now from the fact that $a_G = b_G + r_G - 1$ (cf. [15]).

Remarks. (1) Let $\tilde{A}$ be the special fiber of the Néron model of A. Using Lemmas 1 and 2 of § 1, one can show that the connected component of $\tilde{A}$ is an extension of an abelian variety by a unipotent group U, and that $\varepsilon = 2\dim(U)$.

(2) The integer $\varepsilon + \delta_l$ is called the *exponent of the conductor* of A at v. It is 0 if and only if A has good reduction at v. It is equal to ε if and only if the Galois module A_l is tame (i.e., if and only if A acquires good reduction over a Galois extension of K of degree prime to $p = \operatorname{char}(k)$), and in particular if $p > 2d + 1$ (cf. Corollary 2 of Theorem 2). A similar definition can be given for an arbitrary abelian variety once one knows that δ_l is independent of l (cf. footnote[3] above).

4. Abelian varieties with complex multiplication (preliminaries)

As is the preceding paragraphs, A is an abelian variety over a field K. We denote by $\mathrm{End}_K(A)$, or $\mathrm{End}(A)$, the ring of K-endomorphisms of A; if K' is an extension of K, we write $\mathrm{End}_{K'}(A)$ instead of $\mathrm{End}_{K'}(A \times_K K')$. Let $d = \dim(A)$, let F be an algebraic number field of degree $2d$, and let

$$i: F \longrightarrow \mathbf{Q} \otimes \mathrm{End}_K(A)$$

be a ring homomorphism. We call the pair (A, i) an *abelian variety with complex multiplication by* F over the field K. When K is a number field, this is essentially the same thing as a "variety of CM-type" in the sense of Shimura-Taniyama [18, § 5], except that the CM-type specifies in addition the action of F on the tangent space of A at the origin.

In what follows, we usually identify F with its image under i, that is, we view i as an inclusion. Let $R = F \cap \mathrm{End}_K(A)$; this is an "order" of F, i.e., a subring of F which is free of rank $2d$ over $\mathbf{Z}$; its integral closure is the ring of integers of F. Notice that R is *invariant with respect to a ground field extension* K'/K; that is, R is equal to $F \cap \mathrm{End}_{K'}(A)$. Since F/R is a torsion group, this follows from a general fact on abelian varieties, namely that $\mathrm{End}_{K'}(A)/\mathrm{End}_K(A)$ is *torsion-free*. Indeed, if $\varphi \in \mathrm{End}_{K'}(A)$ and $m\varphi \in \mathrm{End}_K(A)$ for some integer $m \geqq 1$, then $m\varphi$ vanishes on the kernel A_m of multiplication by m in A, viewed as a finite subgroup scheme of A. Since $A/A_m \approx A$, this implies the existence of $\varphi_0 \in \mathrm{End}_K(A)$ such that $m\varphi = m\varphi_0$. Hence $\varphi = \varphi_0$ and φ belongs to the ring $\mathrm{End}_K(A)$[4].

Now let l be a prime number different from char (K). We put

$$T_l = T_l(A) \qquad \text{and} \qquad V_l = V_l(A) = \mathbf{Q}_l \otimes_{\mathbf{Z}_l} T_l\ .$$

As usual, we identify T_l with a sublattice of V_l *via* the map $t \mapsto 1 \otimes t$.

The ring R operates on T_l and, by linearity, this makes T_l an R_l-module and V_l an F_l-module, where $R_l = \mathbf{Z}_l \otimes R$ and $F_l = \mathbf{Q}_l \otimes R = \mathbf{Q}_l \otimes F$.

THEOREM 5. (i) *The F_l-module V_l is free of rank* 1.

(ii) *An element of F_l carries T_l into itself if and only if it belongs to R_l.*

These facts are well known. We recall a proof:

Since the map $\mathbf{Q}_l \otimes \mathrm{End}(A) \to \mathrm{End}(V_l)$ is injective (Weil [21, p. 139]), the semi-simple $\mathbf{Q}_l$-algebra F_l acts *faithfully* on V_l. Since V_l and F_l have the same dimension $2d$ over $\mathbf{Q}_l$, it follows that V_l is free of rank 1 over F_l.

[4] An alternate proof can be given, using Galois theory together with the fact that *every endomorphism of* $A \times_K \bar{K}$ *comes from one of* $A \times_K K_s$ (for this, consider the graph of the endomorphism, and use [12, p. 26, Th. 5]).

On the other hand, let φ be an element of F_l such that $\varphi T_l \subset T_l$. There exists an integer $N \geqq 0$ such that $l^N\varphi \in R_l$, and an element $\psi \in R$ such that $\psi \equiv l^N\varphi \pmod{l^N R_l}$. Since $l^N\varphi T_l \subset l^N T_l$, we have $\psi T_l \subset l^N T_l$, i.e., ψ vanishes on the kernel of multiplication by l^N in A. This implies that $\psi = l^N\varphi_0$, with $\varphi_0 \in \mathrm{End}_K(A) \cap F = R$. But then $\varphi \equiv \varphi_0 \pmod{R_l}$ hence $\varphi \in R_l$, as was to be shown.

From now on, we view R_l, F_l and $\mathrm{End}\,(T_l)$ as subrings of $\mathrm{End}\,(V_l)$.

COROLLARY 1. *The commutant of R in* $\mathrm{End}\,(V_l)$, *resp.* $\mathrm{End}\,(T_l)$, *resp.* $\mathbf{Q} \otimes \mathrm{End}_K(A)$, *resp.* $\mathrm{End}_K(A)$ *is F_l, resp. R_l, resp. F, resp. R.*

The assertion relative to $\mathrm{End}\,(V_l)$ follows from part (i) of Theorem 5, since any element of $\mathrm{End}\,(V_l)$ which commutes with R also commutes with the ring $F_l = \mathbf{Q}_l \otimes R$. The assertion relative to $\mathrm{End}\,(T_l)$ follows from part (ii) of Theorem 5, i.e., from the fact that R_l is equal to $F_l \cap \mathrm{End}\,(T_l)$. Since the map

$$\mathbf{Q}_l \otimes \mathrm{End}_K(A) \longrightarrow \mathrm{End}\,(V_l)$$

is injective (Weil, *loc. cit.*), the dimension over $\mathbf{Q}$ of the commutant of R in $\mathbf{Q} \otimes \mathrm{End}_K(A)$ is at most $[F_l\colon \mathbf{Q}_l] = [F\colon \mathbf{Q}]$; hence that commutant is F. The last assertion follows from the previous one and the definition of R as $F \cap \mathrm{End}_K(A)$.

Now consider the representation

$$\rho_l\colon \mathrm{Gal}\,(K_s/K) \longrightarrow \mathrm{Aut}\,(T_l)$$

defined by the Galois module T_l. If $s \in \mathrm{Gal}\,(K_s/K)$, it is clear that $\rho_l(s)$ *commutes* with the elements of R, and, by Corollary 1, this means that $\rho_l(s)$ is contained in R_l. Hence:

COROLLARY 2. *The representation ρ_l attached to T_l is a homomorphism of* $\mathrm{Gal}\,(K_s/K)$ *into the group $U_l(R)$ of invertible elements of $R_l = \mathbf{Z}_l \otimes R$. In particular,* $\mathrm{Im}\,(\rho_l)$ *is a commutative group.*

Remark. It is not true in general that T_l is a *free* R_l-module. However, this is the case if R_l is a product of discrete valuation rings (that is, if l does not divide the index of R in its integral closure), or, more generally (cf. Bass [3, Th. 6.2 and Prop. 7.2]) if R_l is a "Gorenstein ring", for example, if $\dim\,(A) = 1$.

5. Abelian varieties with complex multiplication (properties of good reduction)

We preserve the notations and hypotheses of § 4. If v is a discrete valuation of K, we denote by p_v the characteristic of the residue field k_v (cf. § 1).

Let μ denote the group of roots of unity contained in the field of complex multiplication F.

THEOREM 6. *Let v be a discrete valuation of K with finite residue field k_v. Then*:

(a) *The abelian variety A has potential good reduction at v in the sense of* § 2.

(b) *If $l \neq p_v$, the image of the inertia group $I(\bar{v})$ under the homomorphism ρ_l*: $\mathrm{Gal}(K_s/K) \to U_l(R)$ (cf. Corollary 2 of Theorem 5) *is contained in the subgroup $\mu \cap R[p_v^{-1}]$ of μ; the homomorphism*

$$\varphi_v \colon I(\bar{v}) \longrightarrow \mu$$

obtained in this way is independent of l.

(c) *Let n_v be the smallest integer $n \geqq 0$ such that φ_v is trivial on the n^{th} ramification group $I(\bar{v})^{(n)}$ in the upper numbering* (cf. Artin-Tate [1, Ch. 11, § 2]). *Then the exponent* (*at v*) *of the conductor of A* (cf. § 3) *is equal to $2dn_v$.*

Statement (a) follows from Corollary 1 to Theorem 2 since $\mathrm{Im}(\rho_l)$ is commutative (by Corollary 2 to Theorem 5).

Hence there exists a finite Galois extension K' of K such that the abelian variety $A' = A \times_K K'$ has good reduction at v', where v' is the restriction of $\bar{v}$ to K'. Let k' be the residue field of v' and $\tilde{A}'$ the reduction of A' at v' (i.e., the special fiber of the Néron model of A'). If we identify as before $V_l(A)$ with $V_l(A')$ and $V_l(\tilde{A}')$, we know (cf. proof of Theorem 2) that $I(\bar{v})$ *acts on $V_l(\tilde{A}')$ through a group of k'-automorphisms of $\tilde{A}'$*. Let Φ_v be this group; it is finite, and independent of l by construction (*loc. cit.*). On the other hand, every endomorphism of an abelian variety extends to its Néron model and to its special fiber (this is a special case of the universal property of the Néron model). Therefore R *operates on* $\tilde{A}'$, i.e. we get an embedding

$$\tilde{i}_0 \colon R \longrightarrow \mathrm{End}_{k'}(\tilde{A}') ,$$

which is obviously compatible with the action of R on $V_l(\tilde{A}') = V_l(A')$. Tensoring by $\mathbf{Q}$, this gives a homomorphism

$$\tilde{i} \colon F \longrightarrow \mathbf{Q} \otimes \mathrm{End}_{k'}(\tilde{A}') .$$

Thus $(\tilde{A}', \tilde{i})$ is an abelian variety with complex multiplication by F; since the elements of Φ_v commute with R, Corollary 1 to Theorem 5, applied to $\tilde{A}'$, shows that they belong to F. We have therefore $\Phi_v \subset F^*$, and since Φ_v is finite, $\Phi_v \subset \mu$. The fact that Φ_v is contained in the subgroup $\mu \cap R[p_v^{-1}]$ of μ results simply from the fact that Φ_v acts on V_l through $R_l = \mathbf{Z}_l \otimes R$ for all $l \neq p_v$. This finishes the proof of (b).

For (c), notice first that Φ_v can be identified with a quotient of the inertia group $I(\bar{v})$. The filtration of $I(\bar{v})$ by its ramification subgroups (in the upper numbering) defines a filtration $\Phi_v^{(x)}$ of Φ_v whose "jumps" are integers (cf. Artin-Tate [1, Ch. 11, § 4, Th. 11]). The integer n_v defined in (c) is the smallest integer $n \geqq 0$ such that $\Phi_v^{(n)} = \{1\}$. Now, let Tr denote the character of the natural representation of Φ_v in V_l; by what has been said in § 3, the exponent of the conductor of A at v is equal to $\langle a_v, \mathrm{Tr}\rangle$, where a_v denotes the Artin character of Φ_v, considered as a Galois group. But we have

$$\mathrm{Tr}(\omega) = \mathrm{Tr}_{F/\mathbf{Q}}(\omega) \qquad \text{for } \omega \in \Phi_v$$

(cf. Theorem 5). If $\sigma_1, \cdots, \sigma_{2d}$ are the different embeddings of F in $\mathbf{C}$, this can be written $\mathrm{Tr}(\omega) = \sum_{i=1}^{i=2d} \sigma_i(\omega)$, hence

$$\langle a_v, \mathrm{Tr}\rangle = \sum_{i=1}^{i=2d} \langle a_v, \sigma_i\rangle .$$

Each σ_i is a faithful representation of degree 1 of Φ_v, and this implies (cf. Artin-Tate [1, *loc. cit.*]) that $\langle a_v, \sigma_i\rangle = n_v$. Hence we have $\langle a_v, \mathrm{Tr}\rangle = 2dn_v$, q.e.d.

COROLLARY. *The abelian variety A has good reduction at v if and only if the homomorphism φ_v of Theorem* 6 *is trivial*, i.e., *if the image Φ_v of φ_v is* $\{1\}$.

This follows from Theorem 1 and the definition of φ_v.

Remarks. (1) The fact that A has potential good reduction generalizes the well known fact that the modular invariant of an elliptic curve with complex multiplication is *integral*.

(2) Suppose that $\Phi_v \neq \{1\}$, so that A has bad reduction at v. Let l be a prime number, distinct from p_v. Then no element of $V_l(A)$, except 0, is invariant by Φ_v (or, what is the same, by the inertia group $I(\bar{v})$). Let $\tilde{A}$ be the special fiber of the Néron model of A at v. Using Lemma 2 of § 1, one then sees that the connected component of $\tilde{A}$ is *unipotent*; with the notations of § 3, this means that $\varepsilon = 2d$, and hence $\delta_l = 2d(n_v - 1)$.

(3) Local class field theory allows us to identify the homomorphism

$$\varphi_v \colon I(\bar{v}) \longrightarrow \mu$$

with a homomorphism $U_v(K) \rightarrow \mu$, where $U_v(K)$ denotes the group of units of the completion K_v of K with respect to v. The integer n_v of (c) is the smallest positive integer such that $\varphi_v(x) = 1$ for $v(x-1) \geqq n_v$.

The case of global fields. From now on we assume, in addition to the preceding hypotheses, that the ground field K is a *global field*, i.e., either an algebraic number field of finite degree, or a function field of one variable over a finite field.

Let S be a finite set of valuations of K. By the remark above we have, for each $v \in S$, a homomorphism φ_v: $U_v(K) \to \mu$, with image Φ_v. Let $m = m_S$ be the least common multiple of the orders of the groups Φ_v for $v \in S$, and let μ_m (resp. μ_{2m}) be the group of m^{th} (resp. of $2m^{\text{th}}$) roots of unity in an algebraic closure of F. Then $\Phi_v \subset \mu_m \subset \mu$ for each $v \in S$, and μ_m is the smallest subgroup of μ containing the Φ_v, for $v \in S$.

Let C_K be the group of *idèle classes* of K. Since the character φ_v of $U_v(K)$ can be extended to a character of $K_v^* \simeq \mathbf{Z} \times U_v(K)$, it follows from the theorem of Grunwald-Hasse-Wang (cf. [1, Ch. 10]) that *there exists a continuous homomorphism* φ: $C_K \to \mu_{2m}$ *such that* $\varphi \circ i_v = \varphi_v$ *for each* $v \in S$, where i_v: $U_v(K) \to C_K$ is the canonical injection. If there exists such a φ with values in μ_m (instead of merely in μ_{2m}), we shall say that the set S is *ordinary* for A; otherwise, we call S *exceptional*. One knows (cf. [1, *loc. cit.*]) that, for S to be exceptional, it is necessary that K be a number field, and that S contain a valuation v such that, if $m = 2^t m_0$, with m_0 odd, the extension of K_v obtained adjoining the $2^{t\,\text{th}}$ roots of unity is not cyclic, and such that 2^t divides the order of Φ_v. In particular, S *is ordinary if* K *is a function field, or if* $m \not\equiv 0 \pmod 4$, *or if* K *contains the* m^{th} *roots of unity, or if* S *contains no* v *with* $p_v = 2$.

We are now ready to prove:

THEOREM 7. *Let* S_A *be the set of valuations* v *of* K *where* A *does not have good reduction* (i.e., *suchth at* $\Phi_v \neq \{1\}$), *and let* m *be the least common multiple of the orders of the* Φ_v *for* $v \in S_A$. *There exists a cyclic extension* K' *of* K *of degree* m *or* $2m$ *over which* A *acquires good reduction everywhere*; *if* S_A *is ordinary for* A (*see above*), *there exists such a* K' *of degree* m.

Let φ: $C_K \to \mu_{2m}$ be a continuous homomorphism of minimal order such that $\varphi \circ i_v = \varphi_v$ for each $v \in S_A$. Let K' be the abelian extension of K corresponding, by class field theory, to the kernel of φ. The extension K'/K is cyclic; its degree is m if S_A is ordinary, $2m$ if S_A is exceptional. The abelian variety $A' = A \times_K K'$ has good reduction at each valuation v' of K'. This is clear if v' does not divide any $v \in S_A$; if v' divides $v \in S_A$, it follows from the construction of K' and the translation theorem of class field theory that $\varphi_{v'} = 1$, so that A' has good reduction at v' by the corollary of Theorem 6.

Remarks. (1) Even when S_A is exceptional, one might be able to choose K' of degree m over K, because all that is needed in the above argument is that $\operatorname{Ker}(\varphi_v) \supset \operatorname{Ker}(\varphi \circ i_v)$, that is, that φ_v is a *power* of $\varphi \circ i_v$, not necessarily equal to it.

(2) On the other hand, Theorem 7 is almost "the best possible" in the following sense: if L/K is a finite extension such that $A \times_K L$ has good

reduction everywhere, then $[L: K]$ *is divisible by* m, and, *if* L/K *is abelian of degree* m, it is necessarily cyclic. We leave the proofs of these facts to the reader.

The method we have just followed can also be used to solve a problem considered by Deuring in the case of elliptic curves ([7]—see also § 6 below).

THEOREM 8. *Let* S *be an arbitrary finite set of valuations of* K, *and let* $m = m_S$ *be the least common multiple of the orders of the* Φ_v *for* $v \in S$. *Suppose* S *satisfies the following condition*:

(a) *Either* $\mu_{2m} \subset R$ *or* S *is ordinary and* $\mu_m \subset R$.

Then there exists an abelian variety B *over* K *with the following two properties*:

(1) B *has good reduction at each* $v \in S$.

(2) $B \times_K K_s$ *is isomorphic to* $A \times_K K_s$ (in other words, B is a *K-form* of A, cf. [4, p. 129]).

The condition (a) is equivalent to the existence of a continuous homomorphism α: $C_K \longrightarrow \mu \cap R$ such that, for each $v \in S$, its local component $\alpha_v = \alpha \circ i_v$ coincides on $U_v(K)$ with the reciprocal of φ_v: $U_v(K) \longrightarrow \mu$. Choose such an α; one has

$$\alpha_v(u)\varphi_v(u) = 1 \qquad \text{for } v \in S,\ u \in U_v(K)\ .$$

Since $\mu \cap R$ is a subgroup of the group of automorphisms of A, one can view α as a 1-cocycle of the group $\mathrm{Gal}\,(K_s/K)$ with values in $\mathrm{Aut}_{K_s}(A)$. Let $B = A_\alpha$ be the abelian variety over K obtained by *twisting* A by the cocycle α (cf. [4, *loc. cit.*]). One sees immediately that the Galois module $V_l(B)$ can be identified with the module $V_l(A)_\alpha$ obtained by twisting $V_l(A)$ by α. Since $\alpha_v\varphi_v = 1$ for $v \in S$, the corollary of Theorem 6 shows that B has good reduction in S, q.e.d.

Remarks. (1) If we choose a polarization θ of A invariant by the finite group $\mu \cap R$ (this is always possible), then we can furnish $B = A_\alpha$ with a polarization θ_B and a homomorphism

$$i_B\colon F \longrightarrow \mathbf{Q} \otimes \mathrm{End}_K(B)\ ,$$

in such a way that (B, i_B, θ_B) is a K-form of (A, i, θ). In particular, B is a K-form of A *as abelian variety with complex multiplication by* F, and B has *the same modular invariant* as A (i.e., the same image in the variety of moduli of polarized abelian varieties (cf. Mumford [13, Ch. 7]).

(2) The proof above shows also that condition (a) is *necessary* (as well as sufficient) for the existence of a K-form of A *as abelian variety with complex multiplication by* F having good reduction in S. In particular, when $R = \mathrm{End}_{K_s}(A)$, condition (a) is necessary and sufficient for the existence of a

K-form of A with good reduction in S.

(3) Suppose S is ordinary. Then, by Theorem 6 (b), the condition (a) is satisfied if $\mu \cap R[p_v^{-1}] = \mu \cap R$ for all $v \in S$, hence in particular if $\mu \subset R$, and especially if R is integrally closed, or if $\mu = \{\pm 1\}$.

6. Example: good reduction of elliptic curves with complex multiplication

In addition to the hypotheses of § 5, we now suppose that $\dim(A) = 1$ and that K is a number field. Then F is an imaginary quadratic field, and $R = \mathrm{End}(A)$. The action of R on the tangent space to A at the origin gives an embedding $F \to K$, by which we identify F with a subfield of K. Note that μ is contained in K, hence every finite set of valuations of K is ordinary in the sense of § 5.

In order to apply Theorem 8, we will have to consider separately the following case: $F = \mathbf{Q}(\sqrt{-1})$ *or* $\mathbf{Q}(\sqrt{-3})$, i.e., $\mu = \mu_4$ *or* μ_6 *and* $F = \mathbf{Q}(\mu)$; *moreover, the conductor of the order* $R = \mathrm{End}_K(A)$ *is a prime power* p^ν, $\nu \geqq 1$.

This case will be referred to as the *special* case.

THEOREM 9. *Let S be a finite set of valuations of K.*

(1) *Except in the special case, S satisfies condition* (a) *of Theorem* 8.

(2) *In the special case, condition* (a) *holds if and only if, for each $v \in S$ with $p_v = p$, we have $N_{K_v/F_w}(U_v(K)) \subset U_p(R)$, where w is the valuation of F induced by v, and where $U_p(R)$ is the group of invertible elements of $R_p = \mathbf{Z}_p \otimes R$, viewed as a subgroup of $\prod_{p_w = p} U_w(F)$.*

(The prime p referred to in (2) is the one which divides the conductor of R.)

Part (1) of Theorem 9, combined with Theorem 8, gives

COROLLARY 1. *Except possibly in the special case, there is a K-form of A which has good reduction in S.*

This result is due to Deuring [7, III, Satz 3] except that he did not point out the necessity of excluding the special case. That this exclusion is necessary is shown by:

COROLLARY 2. *In the special case, assume that $K = F(j_A)$, where j_A is the modular invariant of A* (cf. Deuring [6]). *Then every K-form of A has bad reduction at all places of K dividing p.*

Before deriving Corollary 2, we prove Theorem 9. If $\mu = \{\pm 1\}$, S satisfies condition (a) by the last remark of § 5. If $\mu \neq \{\pm 1\}$, one has $\mu = \mu_4$ or $\mu = \mu_6$, and $F = \mathbf{Q}(\mu)$. Let z be a generator of μ, and let $R_1 = \mathbf{Z} + \mathbf{Z}z$ be the ring of integers of F. For each integer $f \geqq 1$, the order of F with conductor f is

$$R(f) = \mathbf{Z} + fR_1 = \mathbf{Z} + \mathbf{Z}fz ,$$

and every order is of this form. Note that $\mu \cap R(f) = \{\pm 1\}$ for $f > 1$, and that, for each prime p, we have $R \cap R(f)[p^{-1}] = R(f')$, where $f = p^{\nu}f'$ with $(p, f') = 1$. Hence, applying again the last remark of § 5, we see that S satisfies (a) except possibly if the conductor f of R is a prime power p^{ν}, $\nu \geqq 1$. This proves part (1) of Theorem 9.

In the special case, we see that S satisfies (a) if and only if

$$\varphi_v\big(U_v(K)\big) \subset \{\pm 1\}$$

for each $v \in S$ such that $p_v = p$. Let I_K denote the idèle group of K, and by means of the global reciprocity law homomorphism $I_K \longrightarrow C_K \longrightarrow \mathrm{Gal}\,(K^{ab}/K)$, let us interpret the representation ρ_l discussed in Corollary 2 of Theorem 5 as a homomorphism

$$\rho_l \colon I_K \longrightarrow U_l(R) \subset F_l^* .$$

By the theory of complex multiplication (see § 7 below), there is a continuous homomorphism $\varepsilon \colon I_K \longrightarrow F^*$ such that $\varepsilon \mid K^* = N_{K/F}$, and such that, for each prime number l, we have

$$\rho_l(a) = \varepsilon(a) N_{K_l/F_l}(a_l^{-1}) , \qquad a \in I_K ,$$

where a_l denotes the component of the idèle a in the group

$$K_l^* = (\mathbf{Q}_l \otimes K)^* = \textstyle\prod_{p_v = l} K_v^* .$$

Let v be a valuation of K with $p_v = p$. Taking $l \neq p$, the above formula shows that the restriction of ε to $U_v(K)$ is φ_v. Taking $l = p$, and $u \in U_v(K)$, we have

$$\rho_p(u) = \varepsilon(u) N_{K_v/F_w}(u^{-1}) ;$$

since $\rho_p(u) \in U_p(R)$ and $\varepsilon(u) = \varphi_v(u)$, this shows that $\varphi_v(u)$ belongs to $N_{K_v/F_w}(u) \cdot U_p(R)$. But $U_p(R)$ intersects the image of μ in F_p^* only at 1 and -1; it follows that $\varphi_v(U_v(K)) \subset \{\pm 1\}$ if and only if $N_{K_v/F_w}(U_v(K)) \subset U_p(R)$. This proves Theorem 9.

We now prove Corollary 2. It is well known (cf. for instance Deuring [8, § 9], where this is expressed in the language of ideal classes) that the field $F(j_A)$ referred to in the corollary is the abelian extension of F corresponding to the group of idèle-classes XF^*/F^* where X is the following group of idèles:

$$X = \mathbf{C}^* \times \textstyle\prod_l U_l(R) = \mathbf{C}^* \times \prod_{p_w \neq p} U_w(F) \times U_p(R) .$$

Hence, if v is a valuation of K and w its restriction to F, we have, by class field theory,

$$N_{K_v/F_w}\big(U_v(K)\big) = U_w(F) \cap XF^* \ .$$

To derive the corollary, we must therefore show that, for each valuation w of F lying over p, we have

$$U_w(F) \cap XF^* \not\subset U_p(R) \ .$$

In fact, we have canonical isomorphisms

$$\begin{aligned}\frac{U_w(F) \cap XF^*}{U_w(F) \cap XF^* \cap U_p(R)} &= \frac{U_w(F) \cap XF^*}{U_w(F) \cap XF^* \cap X} \simeq \frac{\big(U_w(F) \cap XF^*\big)X}{X} \\ &= \frac{\big(F^* \cap XU_w(F)\big)X}{X} = \frac{\mu X}{X} \simeq \frac{\mu}{\mu \cap X} = \frac{\mu}{\mu_2} \ .\end{aligned}$$

The only non-obvious step in this chain is the equality

$$F^* \cap XU_w(F) = \mu \ .$$

It holds because $XU_w(F)$ is the group of idèles of F whose components at the finite places are units. This is clear in case w is the only valuation above p; when p splits into two valuations w and w', it follows from the fact that $U_p(R)$ contains $U_p(\mathbf{Z})$ which is a subgroup of $U_w(F) \times U_{w'}(F)$ whose projection on either factor is bijective.

Modular invariants. Before giving some numerical examples, we recall a few facts about the modular invariant $j = j_A$ of an elliptic curve A (with or without complex multiplication) over a field K (cf. for instance Deuring [6], [7]). Two such curves A and B (with a rational point taken as origin) are K-forms of each other if and only if $j_A = j_B$. Therefore, the existence of a K-form of A with good reduction at a discrete valuation v of K is a property of j_A, relative to v; thus it is natural to consider the set $J(v)$ of elements $j \in K$ such that there exists an A with good reduction at v with $j_A = j$. As is well known, we have the implication:

$$j \in J(v) \Rightarrow v(j) \geqq 0,\ v(j) \equiv 0 \pmod 3 \text{ and } v(j - 2^6 3^3) \equiv 0 \pmod 2,$$

with the convention that $\infty \equiv 0 \pmod 2$ and $\pmod 3$, in case $j = 0$ or $j = 2^6 3^3$. Moreover, the converse implication holds if $p_v \neq 2$ or 3. Thus, for such a v, the set $J(v)$ has a simple description. It would be of interest to describe it explicty in the remaining cases $p_v = 2$ and $p_v = 3$. Note that, for any v, the set $J(v)$ contains the elements $j \in K$ such that $v(j) = 0 = v(j - 2^6 3^3)$, as the equation

$$y^2 + xy = x^3 - \frac{2^2 3^2}{j - 2^6 3^3}\, x - \frac{1}{j - 2^6 3^3}$$

shows. On the other hand, if $p_v = 2$ and $v(j) > 0$, then

$$j \in J(v) \Longrightarrow \begin{cases} v(j) \geqq 9\,, & \text{if } v(2) = 1 \\ v(j) \geqq 12\,, & \text{if } v(2) > 1\,, \end{cases}$$

and if $p_v = 3$ and $v(j) > 0$, then

$$j \in J(v) \Longrightarrow v(j - 2^6 3^3) \geqq 6\,.$$

Numerical examples. We now return to elliptic curves with complex multiplication, and we give a few examples of the special case, in which the bad reduction predicted by Corollary 2 above can be seen from the value of j. We list the field F, the conductor f of the order R in F, the corresponding value of j, the page in Weber [20] from which this value is taken[5], and finally the property of j which implies the bad reduction at a place v of $K = F(j)$ dividing f:

F	f	j	page	bad property
$\mathbf{Q}(\mu_6)$	2	$2^4 \cdot 3^3 \cdot 5^3$	474	$v(j) = 4 \not\equiv 0 \pmod 3$
$\mathbf{Q}(\mu_6)$	3	$-3 \cdot 2^{15} \cdot 5^3$	462	$v(j) = 2 \not\equiv 0 \pmod 3$
$\mathbf{Q}(\mu_4)$	2	$2^3 \cdot 3^3 \cdot 11^3$	477	$0 < v(j) = 6 < 12$
$\mathbf{Q}(\mu_4)$	3	$2^4(x^8 - 4)^3 x^{-8}$	479	$v(j - 2^6 3^3) = 3 \not\equiv 0 \pmod 2$
$\mathbf{Q}(\mu_4)$	3	$2^6(4z^{24} - 1)^3 z^{-24}$	479	$v(j - 2^6 3^3) = 1 \not\equiv 0 \pmod 2$

In the first three examples, one has $K = F$. In the fourth,

$$K = \mathbf{Q}(\sqrt{-1}, \sqrt{3}) \text{ and } x = 1 \pm \sqrt{3}\,.$$

In the fifth, $K = \mathbf{Q}(\sqrt{-1}, \sqrt{5})$ and $z = (1 \pm \sqrt{5})/2$.

7. Complex multiplication over number fields

We now assume that K is a number field (of finite degree over $\mathbf{Q}$) and A an abelian variety with complex multiplication by F over K; the notations of § 4 and § 5 are still in force. Let $t = t_A$ denote the tangent space to A at the origin. It is a K-vector space of dimension $d = \dim(A)$. On the other hand, R acts K-linearly on t, so that t is a module over $R \otimes K = F \otimes_{\mathbf{Q}} K$; in other words, *$t$ is an (F, K)-bimodule over* $\mathbf{Q}$. Let d' be the dimension of t as an F-vector space. Then $[K\colon \mathbf{Q}] = 2d'$, because

$$d[K\colon \mathbf{Q}] = \dim_{\mathbf{Q}}(t) = [F\colon \mathbf{Q}]d' = 2dd'\,.$$

For each commutative $\mathbf{Q}$-algebra Λ, the tensor product $t \otimes_{\mathbf{Q}} \Lambda$ is an

[5] Weber usually gives, instead of j, some modular function of higher level. For instance, if $F = \mathbf{Q}(\mu_6)$ and the conductor is 2, one has $R = \mathbf{Z} + \mathbf{Z}\sqrt{-3}$, $j = j(\sqrt{-3})$ and one finds in Weber, p. 474, $f(\sqrt{-3})) = \sqrt[3]{2}$, where f is such that $j(\omega) = (f(\omega)^{24} - 16)/f(\omega)^8$; hence $j(\sqrt{-3}) = 2^4.3^3.5^3$.

$(F \otimes_{\mathbf{Q}} \Lambda, K \otimes_{\mathbf{Q}} \Lambda)$-bimodule over Λ. If $u \in K \otimes_{\mathbf{Q}} \Lambda$, we denote by $\det_t(u)$ the determinant of the corresponding endomorphism of $t \otimes_{\mathbf{Q}} \Lambda$ (viewed as a free module of rank d' over $F \otimes_{\mathbf{Q}} \Lambda$); if u is invertible in $K \otimes_{\mathbf{Q}} \Lambda$, so is $\det_t(u)$ in $F \otimes_{\mathbf{Q}} \Lambda$. Hence the map $\det_t$ gives a homomorphism

$$\psi_\Lambda: (K \otimes_{\mathbf{Q}} \Lambda)^* \longrightarrow (F \otimes_{\mathbf{Q}} \Lambda)^*$$

which is functorial in Λ. In the language of algebraic groups, this means that ψ is a morphism $T_K \to T_F$, where T_K and T_F are the tori corresponding to K and F, i.e., the affine algebraic groups over $\mathbf{Q}$ which represent the functors

$$\Lambda \longmapsto (K \otimes_{\mathbf{Q}} \Lambda)^* \qquad \text{and} \qquad \Lambda \longmapsto (F \otimes_{\mathbf{Q}} \Lambda)^* ,$$

respectively. When Λ is $\mathbf{Q}$ (resp. $\mathbf{Q}_l$, resp. $\mathbf{R}$) we write ψ_0 (resp. ψ_l, resp. ψ_∞) instead of ψ_Λ. These are homomorphisms

$$\begin{aligned} &\psi_0: K^* \longrightarrow F^* , && \\ &\psi_l: K_l^* \longrightarrow F_l^* , && \text{where } K_l = \mathbf{Q}_l \otimes K \text{ and } F_l = \mathbf{Q}_l \otimes F , \\ &\psi_\infty: K_\infty^* \longrightarrow F_\infty^* , && \text{where } K_\infty = \mathbf{R} \otimes K \text{ and } F_\infty = \mathbf{R} \otimes F . \end{aligned}$$

If v is a valuation of K at which A has good reduction, we let k_v, $\tilde{A}_v$ and $\tilde{\pi}_v$ denote respectively the residue field of v, the reduction of A at v, and the Frobenius endomorphism of $\tilde{A}_v$ relative to k_v. We have seen in the proof of Theorem 6 that the reduction map $\operatorname{End}(A) \to \operatorname{End}(\tilde{A}_v)$ defines an injection

$$\tilde{i}: F \longrightarrow \mathbf{Q} \otimes \operatorname{End}(A) \longrightarrow \mathbf{Q} \otimes \operatorname{End}(\tilde{A}_v) .$$

Since $\tilde{\pi}_v$ commutes with every k_v-endomorphism of $\tilde{A}_v$, Corollary 1 of Theorem 5 shows that $\tilde{\pi}_v \in \operatorname{Im}(\tilde{i})$. Thus there is a unique element $\pi_v \in F$ such that $\tilde{i}(\pi_v) = \tilde{\pi}_v$; we call π_v the *Frobenius element* attached to v.

Let I_K denote the idèle group of K. For each finite set S of places of K, let I_K^S denote the group of idèles $a = (a_v)$ such that $a_v = 1$ for $v \in S$.

The next two theorems are a reformulation of results of Shimura-Taniyama [18] and Weil [22]:

THEOREM 10. *There exists a unique homomorphism*

$$\varepsilon: I_K \longrightarrow F^*$$

satisfying the following three conditions:

(a) *The restriction of ε to K^* is the map ψ_0: $K^* \to F^*$ defined above.*

(b) *The homomorphism ε is continuous, in the sense that its kernel is open in I_K.*

(c) *There is a finite set S of places of K, including the infinite ones and those where A has bad reduction, such that*

$$(*) \qquad \varepsilon(a) = \prod_{v \notin S} \pi_v^{v(a_v)} \qquad \textit{for } a \in I_K^S .$$

(The last condition means that, for $v \notin S$, the image under ε of any uniformizing element at v is the Frobenius element π_v attached to v.)

Let S be any finite set of places of K containing the infinite ones and those where A has bad reduction, and let $\varepsilon: I_K \to F^*$ be a homomorphism. Then it is clear that ε satisfies conditions (b) and (c)(relative to S) if and only if $(*)$ holds not only for $a \in I_K^S$, but for all a in some open subgroup N of I_K containing I_K^S. For any such N, we have $I_K = K^*N$ by the weak approximation theorem. This shows the unicity of an ε satisfying all three conditions, and shows also that the existence of such an ε for the set S in question is equivalent to the existence of an N as above such that

$$\prod_{v \notin S} \pi_v^{v(\alpha)} = \psi_0(\alpha) \qquad \text{for all } \alpha \in K^* \cap N .$$

But, except for the notation, this last equation is formula (3) on p. 148 of Shimura-Taniyama [18] if we take for S the set of infinite places and those dividing the ideal denoted there by $\mathfrak{fm}$, and for N the group of idèles $\equiv 1 \pmod{\mathfrak{fm}}$. Hence the theorem.

The next theorem concerns the relationship between ε and the l-adic representation ρ_l given by the action of the Galois group on $V_l(A)$. By Corollary 2 of Theorem 5, ρ_l takes its values in $U_l(R) \subset F_l^*$, and factors through $\mathrm{Gal}(K^{ab}/K)$, where K^{ab} is the maximal abelian extension of K. Class field theory allows us to interpret ρ_l as a homomorphism

$$\rho_l: I_K \longrightarrow F_l^*$$

which is trivial on K^*. If v is a valuation of K at which A has good reduction, and such that $p_v \neq l$, then ρ_l is *unramified at* v (i.e., ρ_l is trivial on $U_v(K)$) and takes the value π_v at each uniformizing element of K_v^*.

THEOREM 11. (i) *For each prime number l, we have*

$$(**) \qquad \rho_l(a) = \varepsilon(a)\psi_l(a_l^{-1}) \qquad \textit{for all } a \in I_K ,$$

where a_l denotes the component of a in $K_l^* = \prod_{p_v = l} K_v^*$, and $\psi_l: K_l^* \to F_l^*$ is the map defined above.

(ii) *For every valuation v of K, the restriction of ε to $U_v(K)$ is the homomorphism φ_v of* § 5 (cf. Remark 3 after Theorem 6).

Let S be a set of places satisfying condition (c) of Theorem 10, and let $I_K^{S,l}$ be the group of idèles a whose components are 1 at the places of S and at the places dividing l. By what has been said above, ρ_l coincides with ε on $I_K^{S,l}$, and since $a_l = 1$ for $a \in I_K^{S,l}$, it follows that $(**)$ holds for $a \in I_K^{S,l}$. For $\alpha \in K^*$ we have $\varepsilon(\alpha) = \psi_0(\alpha) = \psi_l(\alpha)$; hence $(**)$ holds for the dense subgroup $K^*I_K^{S,l}$

of I_K. By continuity, (**) holds for all $a \in I_K$. This proves (i).

To prove (ii), let l be some prime number different from p_v. Then $a_l = 1$ for $a \in K_v^*$, and (**) shows that ε coincides with ρ_l on K_v^*. Hence, on $U_v(K)$, ε coincides with φ_v, the restriction of ρ_l (cf. Theorem 6).

COROLLARY 1. *The abelian variety A has good reduction at v if and only if ε is unramified at v*, i.e., $\varepsilon(U_v(K)) = \{1\}$.

This follows from the equality $\Phi_v = \varepsilon(U_v(K))$, combined with the corollary to Theorem 6.

COROLLARY 2. *For each prime number l, the homomorphisms ρ_l and $1/\psi_l$ coincide on an open subgroup of $U_l(K) = \prod_{p_v=l} U_v(K)$; they coincide on all of $U_l(K)$ for those primes l such that A has good reduction at all the places v above l.*

(More precisely, if v divides l, the maps ρ_l and $1/\psi_l$ coincide on all of $U_v(K)$ if and only if A has good reduction at v.)

Indeed, if $x \in U_l(K)$, one has $\rho_l(x) = 1/\psi_l(x)$ if and only if $\varepsilon(x) = 1$.

Remark. Conversely, if for *one* prime l one knows[6] that ρ_l and $1/\psi_l$ coincide on some open subgroup of $U_l(K)$, then one recovers Theorem 10 immediately by defining ε by the formula

$$\varepsilon(a) = \rho_l(a)\psi_l(a_l) \qquad \text{for } a \in I_K .$$

(*A priori*, this ε has values in F_l^*, rather than in F^*, but it is easy to see that it satisfies the three conditions of Theorem 10 (with S consisting of the infinite places, those dividing l, and those where A has bad reduction), and any such homomorphism has values in F^*, as the proof of Theorem 10 shows.)

In view of Theorem 11, it is natural to define a homomorphism

$$\rho_\infty \colon I_K \longrightarrow F_\infty^* = (\mathbf{R} \otimes F)^*$$

by putting $\rho_\infty(a) = \varepsilon(a)\psi_\infty(a_\infty^{-1})$, where a_∞ is the infinite component of the idèle a. This homomorphism is obviously characterized by the fact that it is continuous, trivial on K^*, and coincides with ε on the group I_K^∞ of idèles whose infinite component is 1.

Let $\sigma\colon F \longrightarrow \mathbf{C}$ be a homomorphism. The composition

$$\chi_\sigma \colon I_K \xrightarrow{\rho_\infty} (R \otimes F)^* \xrightarrow{1 \otimes \sigma} \mathbf{C}^*$$

is continuous and trivial on K^*; that is, χ_σ is a "Grössencharakter" in the broad sense (having values in $\mathbf{C}^*$ rather than in the unit circle); it is essen-

[6] Indeed, this can also be proved by local methods, which give the analogous statements for formal groups (or p-divisible groups) with formal complex multiplication. The ingredients for such a proof can be found in our Driebergen and McGill lectures (Springer, 1967-Benjamin, 1968).

tially the same as the Grössencharakter defined in [18, p. 148]. For each valuation v of K, the restriction of χ_σ to $U_v(K)$ is $\sigma \circ \varphi_v$, and, since σ is injective, it follows that *the exponent at v of the conductor of χ_σ is equal to the number n_v of Theorem* 6. Hence:

THEOREM 12. *The conductor of the abelian variety A is the $2d^{\text{th}}$ power of the conductor of χ_σ; in particular, the support of the conductor of χ_σ is the set of valuations of K where A has bad reduction.*

For elliptic curves, the second statement was proved by Deuring [7].

APPENDIX

Some problems on l-adic cohomology

Let K be a field with a discrete valuation v and residue field k (cf. § 1). Let X be an algebraic variety over K. Let l be a prime number, distinct from char (k), and let i be a positive integer. Denote by H_l^i the i^{th} l-adic cohomology vector space of $X_s = X \times_K K_s$, for the étale topology (cf. [2]). Assume that char $(K) = 0$ or that X is proper over K, so that H_l^i is finite dimensional over $\mathbf{Q}_l$ (*loc. cit.*). The group Gal (K_s/K) acts on H_l^i. This defines a continuous homomorphism

$$\rho_l \colon \mathrm{Gal}\,(K_s/K) \longrightarrow \mathrm{Aut}\,(H_l^i)\ .$$

Let Tr (ρ_l) be the character of this representation.

Problem 1. *Is it true that the restriction of* Tr (ρ_l) *to the inertia group $I(\bar{v})$ is locally constant, takes values in* $\mathbf{Z}$, *and is independent of l?*

If so, there is an open subgroup H of $I(\bar{v})$ such that $\rho_l(s)$ is unipotent for all $s \in H$ (this has been proved by Grothendieck in a special case, see below). Moreover, Tr (ρ_l) then defines a character of a finite quotient of $I(\bar{v})$; this would make possible the definition of a *conductor*, as in § 3.

Assume moreover that the residue k is *finite*, with q elements, and let s be an element of the decomposition group $D(\bar{v})$ whose image in Gal $(\bar{k}/k)$ is an integral power F_v^n of the Frobenius element F_v.

Problem 2. *Is it true that the characteristic polynomial of $\rho_l(s)$ has rational coefficients independent of l? If so, is it true that the roots z_α of this polynomial have absolute value $q^{-ni_\alpha/2}$, where $0 \leqq i_\alpha \leqq 2i$?*

These problems are suggested by various examples (for instance, abelian varieties: the case of potential good reduction has been discussed in §§ 2, 3 and the general case is similar, once one has the existence of a "semi-stable reduction" (cf. footnote[3])). One could refine them by asking for the existence of a filtration of H_l^i with suitable properties, but we do not want to go into that here.

We finish up with a result of Grothendieck, which gives, in a special but important case, a positive answer to a part of Problem 1.

PROPOSITION (Grothendieck). *Let ρ: $D(\bar{v}) \to \mathbf{GL}(n, \mathbf{Q}_l)$ be a continuous l-adic linear representation of the decomposition group $D(\bar{v})$. Assume that the residue field k of v has the following property:*

(C_l) *No finite extension of k contains all the roots of unity of order a power of l.*

Then there exists an open subgroup H of $I(\bar{v})$ such that $\rho(s)$ is unipotent for all $s \in H$.

(Note that (C_l) holds if k is finitely generated over the prime field, for instance if it is *finite*.)

PROOF. First, we may assume that K is *complete* and (after making a finite extension) that any matrix $x \in \mathrm{Im}(\rho)$ has coefficients in $\mathbf{Z}_l$ and *is congruent to* 1 mod l^2. This implies in particular that Im (ρ) is a *pro-l-group*, i.e., a projective limit of finite l-groups. We will show that $\rho(s)$ is then unipotent for all $s \in I(\bar{v})$.

Let K_{nr} be the maximal unramified extension of K contained in its separable closure K_s; we have

$$\mathrm{Gal}\,(K_s/K_{nr}) = I(\bar{v}) \qquad \text{and} \qquad \mathrm{Gal}\,(K_{nr}/K) = \mathrm{Gal}\,(k_s/k)\ .$$

Let K_l be the l-part of the maximal tamely ramified extension of K_{nr}, i.e., the extension of K_{nr} generated by the $l^{n\text{ th}}$ roots of a uniformizing element ($n = 1, 2, \cdots$). One sees easily that, if L is a finite extension of K_l, every element of L is an l^{th}-power. Hence the *order* of the group Gal (K_s/K_l), which is a "supernatural number", is prime to l. Since the order of Im(ρ) is a power of l, as remarked above, it follows that the image by ρ of Gal (K_s/K_l) is $\{1\}$, i.e., that ρ may be viewed as a homomorphism of Gal (K_l/K) into $\mathbf{GL}(n, \mathbf{Q}_l)$.

The group Gal (K_l/K) is itself an extension of Gal (k_s/k) by Gal (K_l/K_{nr}). This last group is well known to be isomorphic with $T_l(\mu) = \mathrm{inv\,lim}\, \mu_n$, where μ_n denotes the group of $l^{n\text{ th}}$ roots of unity in k_s (or in K_{nr}, it does not matter). Moreover, the isomorphism

$$T_l(\mu) \simeq \mathrm{Gal}\,(K_l/K_{nr})$$

is compatible with the action of Gal (k_s/k), acting in the natural way on $T_l(\mu)$ and acting on Gal (K_l/K_{nr}) by inner automorphisms of the extension Gal (K_l/K). Let χ: Gal (k_s/k) $\to \mathbf{Z}_l^*$ be the character giving the action of Gal (k_s/k) on $T_l(\mu)$. If s belongs to the pro-l-group Gal (K_l/K_{nr}), the compatibility mentioned above shows that *s and $s^{\chi(t)}$ are conjugate in* Gal(K_l/K) for every $t \in \mathrm{Gal}(k_s/k)$. Let $X = \log \rho(s)$ be the l-adic logarithm of $\rho(s)$; since

$$\log \rho(s)^{\chi(t)} = \chi(t) \log \rho(s) = \chi(t)X ,$$

we see that X and $\chi(t)X$ are conjugate matrices for every $t \in \mathrm{Gal}(k_s/k)$. If $a_i(X)$ is the i^{th} symmetric function of the characteristic roots of X, this shows that

$$a_i(X) = a_i\big(\chi(t)X\big) = \chi(t)^i a_i(X) .$$

But the condition (C_l) means that the image of χ is an infinite subgroup of $\mathbf{Z}_l^*$. Hence we may choose t such that $\chi(t)$ is not a root of unity, and the equation above shows that $a_i(X) = 0$ for all $i > 0$, i.e., that X is *nilpotent*. Since $\rho(s) \equiv 1 \bmod \cdot l^2$, we have

$$\rho(s) = \exp\big(\log \rho(s)\big) = \exp(X) ,$$

hence $\rho(s)$ is unipotent, q.e.d.

COLLÈGE DE FRANCE,
HARVARD UNIVERSITY

BIBLIOGRAPHY

[1] E. ARTIN and J. TATE, Class Field Theory. Benjamin, New York, 1968.

[2] M. ARTIN, A. GROTHENDIECK et J-L. VERDIER, *Cohomologie étale des schémas*, Séminaire Géom. Alg. (SGA 4), I. H. E. S., 1963/64 [see also SGA 5, 1964/65, exposé 6].

[3] H. BASS, *On the ubiquity of Gorenstein rings*. Math. Z., **82** (1963), 8-28.

[4] A. BOREL et J-P. SERRE, *Théorèmes de finitude en cohomologie galoisienne*. Comment. Math. Helv., **39** (1964), 111-164.

[5] C. CHEVALLEY, *Une démonstration d'un théorème sur les groupes algébriques*. J. Math. pures appl., **39** (1960), 307-317.

[6] M. DEURING, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*. Abh. Math. Sem. Hamburg, **14** (1941), 197-272.

[7] ———, *Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins*, II. Gött. Nach., 1955, n° 2, p. 13-42; III, *ibid.*, 1956, n° 4, p. 37-76.

[8] ———, *Die Klassenkörper der komplexen Multiplikation*. Enz. Math. Wiss., Band I-2, Heft 10, Teil II, Teubner, 1958.

[9] A. GROTHENDIECK, Eléments de Géométrie algébrique (rédigés avec la collaboration de J. DIEUDONNÉ). Publ. Math. I.H.E.S., 1960-. . .

[10] ———, *Un théorème sur les homomorphismes de schémas abéliens*. Invent. Math., **2** (1966), 59-78.

[11] S. KOIZUMI and G. SHIMADA, *On specializations of abelian varieties*. Sc. Papers Coll. Gen. Ed., Univ. Tokyo, **9** (1959), 187-211.

[12] S. LANG, Abelian varieties. Intersc. Tracts, n° 7, New York, 1957.

[13] D. MUMFORD, Geometric Invariant Theory. Erg. der Math., Bd. 34, Springer-Verlag, 1965.

[14] A. NÉRON, *Modèles minimaux des variétés abéliennes sur les corps locaux et globaux*. Publ. Math. I.H.E.S., **21**, (1964), 5-128.

[15] A. P. OGG, *Elliptic curves and wild ramification*. Amer. J. Math., **89** (1967), 1-21.

[16] M. RAYNAUD, *Caractéristique d'Euler-Poincaré d'un faisceau et cohomologie des variétés abéliennes*. Sém. BOURBAKI, 1964/65, exposé 286.

[17] M. ROSENLICHT, *Some basic theorems on algebraic groups*. Amer. J. Math., **78** (1956), 401-443.
[18] G. SHIMURA and Y. TANIYAMA, Complex multiplication of abelian varieties and its applications to number theory. Publ. Math. Soc. Japan, n° 6, Tokyo, 1961.
[19] J. TATE, *Genus change in inseparable extensions of function fields*. Proc. Amer. Math. Soc., **3** (1952), 400-406.
[20] H. WEBER, Lehrbuch der Algebra. III. 3 Aufl., Braunschweig, 1908.
[21] A. WEIL, Variétés abéliennes et courbes algébriques. Publ. Inst. Math. Univ. Strasbourg, VIII, Hermann, Paris, 1948.
[22] ———, *On a certain type of characters of the idèle-class group of an algebraic number-field*. Proc. Intern. Symp. Tokyo-Nikko, 1955, p. 1-7.

(Received March 18, 1968)