Good Reduction of Abelian Varieties

Jean-Pierre Serre, John Tate


Stable URL:
http://links.jstor.org/sici?sici=0003-486X%28196811%292%3A88%3A3C492%3AGROAV%3E2.0.CO%3B2-B

Your use of the JSTOR archive indicates your acceptance of JSTOR’s Terms and Conditions of Use, available at http://www.jstor.org/about/terms.html. JSTOR’s Terms and Conditions of Use provides, in part, that unless you have obtained prior permission, you may not download an entire issue of a journal or multiple copies of articles, and you may use content in the JSTOR archive only for your personal, non-commercial use.

Each copy of any part of a JSTOR transmission must contain the same copyright notice that appears on the screen or printed page of such transmission.

*The Annals of Mathematics* is published by Annals of Mathematics. Please contact the publisher for further permissions regarding the use of this work. Publisher contact information may be obtained at http://www.jstor.org/journals/annals.html.


JSTOR and the JSTOR logo are trademarks of JSTOR, and are Registered in the U.S. Patent and Trademark Office. For more information on JSTOR contact jstor-info@umich.edu.

©2002 JSTOR
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 $O_v/m_v$ of $v$ will be denoted by $k_v$, or simply by $k$. Let $K_v$ be a separable closure of $K$ and $\bar{v}$ an extension of $v$ to $K_v$. 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 $\text{Gal}(K_v/K)$ and we have a canonical isomorphism

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

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

A Galois extension $L$ of $K$ contained in $K_v$ is unramified at $v$ if and only if $L$ is fixed by $I(\bar{v})$. More generally, if $\text{Gal}(K_v/K)$ 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 $\text{Gal}(K_v/K)$. 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 $\text{Gal}(\bar{k}/k)$.

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 $\text{Spec}(O_v)(\text{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 $A \simeq A_v \times_{o_v} K$; 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 $m \in \mathbb{Z}$ is prime to the characteristic of $K$, we put

$$A_m = \text{Hom} \left( \mathbb{Z}/m\mathbb{Z}, A(K) \right).$$

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

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

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

This is a free module of rank $2 \dim(A)$ over the ring $\mathbb{Z}_l$ of $l$-adic integers; the group $\text{Gal}(K/K)$ 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 perfect1, and let $l$ be a prime number different from $\text{char}(k)$. The following properties are equivalent:

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

(b) $A_m$ is unramified at $v$ for all $m$ prime to $\text{char}(k)$.

(b') There exist infinitely many integers $m$, prime to $\text{char}(k)$, 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 $f: A \rightarrow A'$ 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 $I(\overline{v})$ acts trivially on the former, it does also on the latter.

**Corollary 3.** Let $0 \rightarrow A' \rightarrow A \rightarrow A'' \rightarrow 0$ 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 $I(\overline{v'}) \to I(\overline{v})$ of the corresponding inertia groups is surjective (for instance, $K' = \bar{K}$, 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, $T_1(A) = T_1(A')$ 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 $A_{s}$ 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 $A_s$ be the Néron minimum model of $A$ relative to $v$ (cf. [14, Ch. II]); thus, $A_s$ is a smooth group scheme of finite type over $O_v$, together with an isomorphism $A_s \times_{o_v} K \simeq A$, which represents the functor

$$Y \mapsto \text{Hom}_K(Y \times_{o_v} K, A)$$

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

Let $\tilde{A}_s = A_s \times_{o_v} k$ be the special fiber of $A_s$. 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

$$\tilde{A}_m = \text{Hom}(\mathbb{Z}/m\mathbb{Z}, \tilde{A}(k)) .$$

It is known (cf. [5], [17]) that the connected component $\tilde{A}_c$ 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 $\tilde{A}_c$ in $\tilde{A}$. The $\mathbb{Z}/m\mathbb{Z}$-module $\tilde{A}_m$ is an extension of a group of order dividing $c$ by a free $\mathbb{Z}/m\mathbb{Z}$-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 \( \tilde{A}_m^0 \) in \( \tilde{A}_m \) divides \( c = (\tilde{A} : \tilde{A}_m) \). On the other hand, the fact that \( H(\kappa) \) is \( m \)-divisible shows that the sequence

\[
0 \longrightarrow H_m \longrightarrow \tilde{A}_m^0 \longrightarrow B_m \longrightarrow 0
\]

is exact. Since \( H_m \) and \( B_m \) are free \( \mathbb{Z}/m\mathbb{Z} \)-modules of rank \( \dim(S) \) and \( 2 \dim(B) \) respectively, \( \tilde{A}_m^0 \) 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 \( I = I(\overline{v}) \).

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

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

\[
\text{Hom}(\mathbb{Z}/m\mathbb{Z}, A(L)) = \text{Hom}_I(\mathbb{Z}/m\mathbb{Z}, A(K,I)) = A^I_m.
\]

On the other hand, let \( O_L \) be the ring of \( \overline{v} \)-integers of \( L \); its residue field is \( \kappa \).

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 \( O_L \rightarrow \kappa \) defines a homomorphism

\[
r: A(L) = A_v(O_L) \longrightarrow \tilde{A}(\kappa).
\]

Since \( O_L \) is henselian, and \( A_v \) is smooth, \( r \) is surjective. Moreover, since \( m \) is prime to \( \text{char}(k) \), 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

\[
\text{Hom}(\mathbb{Z}/m\mathbb{Z}, A(L)) = A_m^I \longrightarrow \text{Hom}(\mathbb{Z}/m\mathbb{Z}, \tilde{A}(\kappa)) = \tilde{A}_m;
\]

this isomorphism commutes with the action of \( D(\overline{v}) \) 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 \( \text{char}(k) \), such that \( A_m = A_m^I \). Taking \( m > c = (\tilde{A} : \tilde{A}_m) \), and applying Lemmas 1 and 2 we see that

\[
\dim(S) + 2 \dim(B) \geq 2 \dim(A),
\]

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

We may assume $O_s$ is complete, since geometrical connectedness (of $X$) ascends and properness (of $X_s$) descends, cf. [9, IV, Prop. 2.7.1]. By [9, III, Cor. 5.5.2], there exist open disjoint subschemes $Z$ and $Z'$ of $X_s$, with $X_s = Z \cup Z'$, $Z$ proper and $\tilde{X} \subset Z$. Since $X$ is connected, this implies $Z' = \emptyset$, hence $X_s = Z$ is proper over $O_s$. 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

$$\rho_i: \text{Gal}(K_s/K) \longrightarrow \text{Aut}(T_i)$$

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

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

(ii) When this is the case, the restriction of $\rho_i$ to $I(\overline{v})$ is independent of $l$ in the following sense: its kernel is the same for all $l$, and its character has values in $\mathbb{Z}$ 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 $\text{Gal}(K_s/K)$ is now equal to its inertia subgroup $I(\overline{v})$. Let $\overline{K}$ be an algebraic closure of $K$, and $K'$ a finite subextension of $\overline{K}$; let $G_{K'} = \text{Gal}(\overline{K}/K') = \text{Gal}(K_s/K_s \cap K')$ 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 $\rho_i$; hence this kernel is independent of $l$. Choose now a finite Galois extension $K'/K$ having this property, and let $A'_1$ be the Néron model of $A'$; it is an abelian scheme
over the ring \( O'_t \) of integral elements of \( K' \). The Galois group \( G = \text{Gal}(K'/K) \) 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 \( A'_t \); the map

\[
A'_t \longrightarrow \text{Spec} (O'_t)
\]

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 \( \text{Gal}(K/K) \) in \( \text{Aut}(T_l) \) 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 \( \text{Aut}(T_l) \) 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 \( \text{Aut}(T_l) \) intersects the pro-\( l \)-group \( 1 + l \cdot \text{End}(T_l) \) only in the neutral element, so the image of \( P \) maps injectively into the finite group \( \text{Aut}(T_l/lT_l) \) and is finite. Hence the image of \( I \) in \( \text{Aut}(T_l) \) is finite.

**Corollary 2.** Suppose \( A \) has potential good reduction at \( v \). Let \( m \) be an integer \( \geq 3 \) and prime to \( p = \text{char}(k) \); let \( K(A_m) \) be the smallest subextension of \( K \), 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 \( l \geq 3 \) and \( l' = 4 \) if \( l = 2 \). The kernel of \( \text{Aut}(T_l) \rightarrow \text{Aut}(T_l/l'T_l) = \text{Aut}(A_{l'}) \) 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 \( \rho_l \) 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 $K(A_w)/K$ 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

$$\text{Card} \left( \text{Aut} \left( A_l \right) \right) = l^{d(2d-1)} \prod_{n=1}^{n=2d} (l^n - 1)$$

is divisible by $p$, and consequently the exponent of $l$ mod $p$ is $\leq 2d$. Taking $l$ to be a primitive root mod $p$ (by Dirichlet's theorem) we conclude that $p - 1 \leq 2d$; 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 sub-extension $L/K$ of $\bar{K}/K$ over which $A$ acquires good reduction; it is a Galois extension, equal to $K(A_w)$ for all $m \geq 3$ prime to char $(k)$; the Galois group $\text{Gal} (K_s/L)$ is equal to $\text{Ker} (\rho_l)$ for all $l \neq \text{char} (k)$.

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

**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 $p \leq 2d + 1$ 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 $\text{Gal} (\bar{k}/k)$. Let $\sigma$ be an element of $D(\bar{v})$ whose image in $\text{Gal} (\bar{k}/k)$ 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 $\rho_l(\sigma) \in \text{Aut} (T_l(A))$, when $l \neq \text{char} (k)$. We may assume, as above, that the Galois group $G = \text{Gal} (K_s/K)$ is equal to the decomposition group $D(\bar{v})$. Let $\Gamma_\sigma$ denote the closure of the subgroup of $G$ generated by $\sigma$; the projection map $G \rightarrow \text{Gal} (\bar{k}/k)$ defines an isomorphism of $\Gamma_\sigma$ onto $\text{Gal} (\bar{k}/k)$; in particular, $G$ is the semi-direct product of $\Gamma_\sigma$ and $I(\bar{v})$. Let now $H$ be the kernel of the restriction of $\rho_l$ 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 \( H \cdot \Gamma_\sigma = \text{Gal}(K'/K') \) acts on \( T_l(A') \) via its quotient \( \text{Gal}(\overline{k}/k) \). Since the image of \( \sigma \) in the latter group is \( F_\sigma \), we then see that the action of \( \sigma \) 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 \( (N\sigma)^{1/2} \), where \( N\sigma = \text{Card}(k) \).

Moreover:

**Corollary.** Let \( s \) be an element of \( D(\overline{\sigma}) \) whose image in \( \text{Gal}(\overline{k}/k) \) is an integral power \( \text{F}_\sigma^*, n \in \mathbb{Z} \), of the Frobenius element \( F_\sigma \). The characteristic polynomial of \( \rho_l(s) \) has rational coefficients independent of \( l \). The absolute values of its roots are equal to \( (N\sigma)^{1/2} \).

When \( n = 0 \), one has \( s \in I(\overline{\sigma}) \) 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 \( O_\sigma \) 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 \( \text{char}(k) \). The Galois module \( A_l \) is a finite dimensional vector space over the field \( \mathbb{Z}/l\mathbb{Z} \). 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 \( \delta_l \) is independent of \( l \) and it has been conjectured that the same is true in higher dimension as well\(^8\). 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 \( K_\sigma \), 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 \( G = \text{Gal}(L/K) \), and let \( a_\sigma \) (resp. \( b_\sigma \)) denote the Artin character (resp. the Swan character) of \( G \) (cf. Ogg, loc. cit., § 1). Let \( \varphi_A \) be the character of the repre-

---

\(^8\) 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 \( \text{char}(k) \neq 2 \).
sentation of $G$ in $T_1(A)$; by Theorem 2, $\varphi_\lambda$ takes values in $\mathbb{Z}$ and is independent of $l$. If $f$ and $g$ are functions on $G$, define their scalar product $\langle f, g \rangle$ as usual by

$$\langle f, g \rangle = \frac{1}{n} \sum_{s \in G} f(s^{-1})g(s),$$

where $n = \text{Card}(G) = [L: K]$.

**Theorem 4.** Assume $A$ has potential good reduction. Then

$$\delta_i = \langle b_\varphi, \varphi_\lambda \rangle.$$

In particular, $\delta_i$ is independent of $l$.

Let $P_i$ be a $\mathbb{Z}_l[G]$-projective module whose character is $b_\varphi$, so that

$$\delta_i = \dim_{\mathbb{Z}/l\mathbb{Z}} \text{Hom}_G(P_i, A_i),$$

(cf. Ogg, loc. cit.). Since $A_i = T_i/lT_i$ and $P_i$ is projective, we have

$$\text{Hom}_G(P_i, A_i) \cong \mathbb{Z}/l\mathbb{Z} \otimes \text{Hom}_G(P_i, T_i),$$

hence

$$\delta_i = \text{rank}_{\mathbb{Z}_l} \text{Hom}_G(P_i, T_i) = \dim_{\mathbb{Q}_l} \text{Hom}_G(\mathbb{Q}_l \otimes P_i, \mathbb{Q}_l \otimes T_i)$$

$$= \langle b_\varphi, \varphi_\lambda \rangle,$$

q.e.d.

**Corollary.** Let $\varepsilon$ be the codimension of the invariants of $\text{Gal}(\overline{K}/K)$ in $\mathbb{Q}_l \otimes T_i$. Then

$$\varepsilon + \delta_i = \langle a_\varphi, \varphi_\lambda \rangle.$$

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

$$\varepsilon = \langle r_\varphi - 1, \varphi_\lambda \rangle$$

and

$$\varepsilon + \delta_i = \langle b_\varphi + r_\varphi - 1, \varphi_\lambda \rangle.$$

The corollary follows now from the fact that $a_\varphi = b_\varphi + r_\varphi - 1$ (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 $\varepsilon + \delta_i$ 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 $\varepsilon$ if and only if the Galois module $A_i$ is tame (i.e., if and only if $A$ acquires good reduction over a Galois extension of $K$ of degree prime to $p = \text{char}(k)$), 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 $\delta_i$ is independent of $l$ (cf. footnote 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 \( \operatorname{End}_K(A) \), or \( \operatorname{End}(A) \), the ring of \( K \)-endomorphisms of \( A \); if \( K' \) is an extension of \( K \), we write \( \operatorname{End}_{K'}(A) \) instead of \( \operatorname{End}_K(A \times_K K') \). Let \( d = \dim(A) \), let \( F \) be an algebraic number field of degree \( 2d \), and let

\[ i: F \longrightarrow \mathbb{Q} \otimes \operatorname{End}_K(A) \]

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 \( \text{cm}\)-type" in the sense of Shimura-Taniyama [18, § 5], except that the \( \text{cm}\)-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 \( R = F \cap \operatorname{End}_K(A) \); this is an "order" of \( F \), i.e., a subring of \( F \) which is free of rank \( 2d \) over \( \mathbb{Z} \); 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 \( F \cap \operatorname{End}_{K'}(A) \). Since \( F/R \) is a torsion group, this follows from a general fact on abelian varieties, namely that \( \operatorname{End}_{K'}(A)/\operatorname{End}_K(A) \) is torsion-free. Indeed, if \( \varphi \in \operatorname{End}_{K'}(A) \) and \( m \varphi \in \operatorname{End}_K(A) \) for some integer \( m \geq 1 \), then \( m \varphi \) vanishes on the kernel \( A_m \) of multiplication by \( m \) in \( A \), viewed as a finite subgroup scheme of \( A \). Since \( A/A_m \cong A \), this implies the existence of \( \varphi_0 \in \operatorname{End}_K(A) \) such that \( m \varphi = m \varphi_0 \).
Hence \( \varphi = \varphi_0 \) and \( \varphi \) belongs to the ring \( \operatorname{End}_K(A) \).

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

\[ T_i = T_i(A) \quad \text{and} \quad V_i = V_i(A) = \mathbb{Q}_l \otimes_{\mathbb{Z}_l} T_i. \]

As usual, we identify \( T_i \) with a sublattice of \( V_i \) via the map \( t \mapsto 1 \otimes t \).

The ring \( R \) operates on \( T_i \) and, by linearity, this makes \( T_i \) an \( R_i \)-module and \( V_i \) an \( F_i \)-module, where \( R_i = \mathbb{Z}_l \otimes R \) and \( F_i = \mathbb{Q}_l \otimes R = \mathbb{Q}_l \otimes F \).

**Theorem 5.** (i) The \( F_i \)-module \( V_i \) is free of rank 1.

(ii) An element of \( F_i \) carries \( T_i \) into itself if and only if it belongs to \( R_i \).

These facts are well known. We recall a proof:

Since the map \( \mathbb{Q}_l \otimes \operatorname{End}(A) \longrightarrow \operatorname{End}(V_i) \) is injective (Weil [21, p. 139]), the semi-simple \( \mathbb{Q}_l \)-algebra \( F_i \) acts faithfully on \( V_i \). Since \( V_i \) and \( F_i \) have the same dimension \( 2d \) over \( \mathbb{Q}_l \), it follows that \( V_i \) is free of rank 1 over \( F_i \).

\[ ^4 \text{An alternate proof can be given, using Galois theory together with the fact that every endomorphism of } A \times_K K \text{ comes from one of } A \times_K K_s \text{ (for this, consider the graph of the endomorphism, and use [12, p. 26, Th. 5]).} \]
On the other hand, let $\varphi$ be an element of $F_i$ such that $\varphi T_i \subset T_i$. There exists an integer $N \geq 0$ such that $l^N \varphi \in R_i$, and an element $\psi \in R$ such that $\psi \equiv l^N \varphi \pmod{l^N R_i}$. Since $l^N \varphi T_i \subset l^N T_i$, we have $\psi T_i \subset l^N T_i$, i.e., $\psi$ vanishes on the kernel of multiplication by $l^N$ in $A$. This implies that $\psi = l^N \varphi_0$, with $\varphi_0 \in \text{End}_k(A) \cap F = R$. But then $\varphi \equiv \varphi_0 \pmod{R_i}$ hence $\varphi \in R_i$, as was to be shown.

From now on, we view $R_i$, $F_i$ and $\text{End}(T_i)$ as subrings of $\text{End}(V_i)$.

**Corollary 1.** The commutant of $R$ in $\text{End}(V_i)$, resp. $\text{End}(T_i)$, resp. $\mathbb{Q} \otimes \text{End}_k(A)$, resp. $\text{End}_k(A)$ is $F_i$, resp. $R_i$, resp. $F$, resp. $R$.

The assertion relative to $\text{End}(V_i)$ follows from part (i) of Theorem 5, since any element of $\text{End}(V_i)$ which commutes with $R$ also commutes with the ring $F_i = \mathbb{Q}_i \otimes R$. The assertion relative to $\text{End}(T_i)$ follows from part (ii) of Theorem 5, i.e., from the fact that $R_i$ is equal to $F_i \cap \text{End}(T_i)$. Since the map

$$\mathbb{Q}_i \otimes \text{End}_k(A) \longrightarrow \text{End}(V_i)$$

is injective (Weil, *loc. cit.*), the dimension over $\mathbb{Q}$ of the commutant of $R$ in $\mathbb{Q} \otimes \text{End}_k(A)$ is at most $[F_i: \mathbb{Q}_i] = [F: \mathbb{Q}]$; hence that commutant is $F$. The last assertion follows from the previous one and the definition of $R$ as $F \cap \text{End}_k(A)$.

Now consider the representation

$$\rho_i : \text{Gal}(K_i/K) \longrightarrow \text{Aut}(T_i)$$

defined by the Galois module $T_i$. If $s \in \text{Gal}(K_i/K)$, it is clear that $\rho_i(s)$ commutes with the elements of $R$, and, by Corollary 1, this means that $\rho_i(s)$ is contained in $R_i$. Hence:

**Corollary 2.** The representation $\rho_i$ attached to $T_i$ is a homomorphism of $\text{Gal}(K_i/K)$ into the group $U_i(R)$ of invertible elements of $R_i = \mathbb{Z}_i \otimes R$. In particular, $\text{Im}(\rho_i)$ is a commutative group.

**Remark.** It is not true in general that $T_i$ is a free $R_i$-module. However, this is the case if $R_i$ 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 $R_i$ is a "Gorenstein ring", for example, if $\text{dim}(A) = 1$.

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 $\mu$ 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 $I(\overline{v})$ under the homomorphism $\rho_i: \text{Gal} (K_v/K) \to U_l(R)$ (cf. Corollary 2 of Theorem 5) is contained in the subgroup $\mu \cap R[p_v^{-1}]$ of $\mu$; the homomorphism

$$\varphi_v: I(\overline{v}) \rightarrow \mu$$

obtained in this way is independent of $l$.

(c) Let $n_v$ be the smallest integer $n \geq 0$ such that $\varphi_v$ is trivial on the $n^{\text{th}}$ ramification group $I(\overline{v})^{(n)}$ 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 $\text{Im} (\rho_i)$ 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 $\overline{v}$ 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 $V_i(A)$ with $V_i(A')$ and $V_i(\tilde{A}')$, we know (cf. proof of Theorem 2) that $I(\overline{v})$ acts on $V_i(\tilde{A}')$ through a group of $k'$-automorphisms of $\tilde{A}'$. Let $\Phi_v$ 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

$$\tilde{i}_v: R \rightarrow \text{End}_{k'}(\tilde{A}')$$

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

$$\tilde{i}: F \rightarrow \mathbb{Q} \otimes \text{End}_{k'}(\tilde{A}')$$

Thus $(\tilde{A}', \tilde{i})$ is an abelian variety with complex multiplication by $F$; since the elements of $\Phi_v$ 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 $\Phi_v$ is finite, $\Phi_v \subset \mu$. The fact that $\Phi_v$ is contained in the subgroup $\mu \cap R[p_v^{-1}]$ of $\mu$ results simply from the fact that $\Phi_v$ acts on $V_i$ through $R_l = \mathbb{Z}_l \otimes R$ for all $l \neq p_v$. This finishes the proof of (b).
For (c), notice first that $\Phi_v$ can be identified with a quotient of the inertia group $I(\overline{v})$. The filtration of $I(\overline{v})$ by its ramification subgroups (in the upper numbering) defines a filtration $\Phi_v^{(n)}$ of $\Phi_v$ whose "jumps" are integers (cf. Artin-Tate [1, Ch. 11, § 4, Th. 11]). The integer $n_v$ defined in (c) is the smallest integer $n \geq 0$ such that $\Phi_v^{(n)} = \{1\}$. Now, let $\text{Tr}$ denote the character of the natural representation of $\Phi_v$ in $V_i$; by what has been said in § 3, the exponent of the conductor of $A$ at $v$ is equal to $\langle a_v, \text{Tr} \rangle$, where $a_v$ denotes the Artin character of $\Phi_v$, considered as a Galois group. But we have

$$\text{Tr}(\omega) = \text{Tr}_{F/\mathbb{Q}}(\omega) \quad \text{for } \omega \in \Phi_v$$

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

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

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

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

This follows from Theorem 1 and the definition of $\varphi_v$.

**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 $V_i(A)$, except 0, is invariant by $\Phi_v$ (or, what is the same, by the inertia group $I(\overline{v})$). Let $\overline{A}$ 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 $\overline{A}$ is unipotent; with the notations of § 3, this means that $\varepsilon = 2d$, and hence $\delta_i = 2d(n_v - 1)$.

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

$$\varphi_v : I(\overline{v}) \rightarrow \mu$$

with a homomorphism $U_*(K) \rightarrow \mu$, where $U_*(K)$ 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 $v(x - 1) \geq n_v$.

**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 \( \varphi_v : U_\nu(K) \to \mu \), with image \( \Phi_v \). Let \( m = m_\nu \) be the least common multiple of the orders of the groups \( \Phi_v \) for \( v \in S \), and let \( \mu_m \) (resp. \( \mu_{2m} \)) be the group of \( m \)th (resp. of \( 2m \)th) roots of unity in an algebraic closure of \( F \). Then \( \Phi_v \subset \mu_m \subset \mu \) for each \( v \in S \), and \( \mu_m \) is the smallest subgroup of \( \mu \) containing the \( \Phi_v \) for \( v \in S \).

Let \( C_K \) be the group of idèle classes of \( K \). Since the character \( \varphi_v \) of \( U_\nu(K) \) can be extended to a character of \( K_v^* \simeq \mathbb{Z} \times U_\nu(K) \), it follows from the theorem of Grunwald-Hasse-Wang (cf. [1, Ch. 10]) that there exists a continuous homomorphism \( \varphi : C_K \to \mu_m \) such that \( \varphi \circ i_v = \varphi_v \) for each \( v \in S \), where \( i_v : U_\nu(K) \to C_K \) is the canonical injection. If there exists such a \( \varphi \) with values in \( \mu_m \) (instead of merely in \( \mu_{2m} \)), 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 \( m = 2^m m_0 \), with \( m_0 \) odd, the extension of \( K_v \) obtained adjoining the \( 2^m \)th roots of unity is not cyclic, and such that \( 2^m \) divides the order of \( \Phi_v \). In particular, \( S \) is ordinary if \( K \) is a function field, or if \( m \equiv 0 \pmod{4} \), 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 \( S_\Delta \) be the set of valuations \( v \) of \( K \) where \( A \) does not have good reduction (i.e., such that at \( \Phi_v \neq \{1\} \)), and let \( m \) be the least common multiple of the orders of the \( \Phi_v \) for \( v \in S_\Delta \). There exists a cyclic extension \( K' \) of \( K \) of degree \( m \) or \( 2m \) over which \( A \) acquires good reduction everywhere; if \( S_\Delta \) is ordinary for \( A \) (see above), there exists such a \( K' \) of degree \( m \).

Let \( \varphi : C_K \to \mu_{2m} \) be a continuous homomorphism of minimal order such that \( \varphi \circ i_v = \varphi_v \) for each \( v \in S_\Delta \). Let \( K' \) be the abelian extension of \( K \) corresponding, by class field theory, to the kernel of \( \varphi \). The extension \( K'/K \) is cyclic; its degree is \( m \) if \( S_\Delta \) is ordinary, \( 2m \) if \( S_\Delta \) 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 \( v \in S_\Delta \); if \( v' \) divides \( v \in S_\Delta \), 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 \( S_\Delta \) 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 \( \text{Ker}(\varphi_v) \supset \text{Ker}(\varphi \circ i_v) \), that is, that \( \varphi_v \) 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 ([17]—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 \(\Phi_v\) for \(v \in S\). Suppose \(S\) satisfies the following condition:

(a) Either \(\mu_{\mathfrak{m}^m} \subset R\) or \(S\) is ordinary and \(\mu_{\mathfrak{m}} \subset R\).

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. \(B \times_{\kappa} K_v\) is isomorphic to \(A \times_{\kappa} K_v\) (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 \(\alpha: C_{\kappa} \to \mu \cap R\) such that, for each \(v \in S\), its local component \(\alpha_v = \alpha \circ i_v\) coincides on \(U_s(K)\) with the reciprocal of \(\varphi_v: U_s(K) \to \mu\). Choose such an \(\alpha\); one has

\[
\alpha_v(u)\varphi_v(u) = 1 \quad \text{for } v \in S, \ u \in U_s(K).
\]

Since \(\mu \cap R\) is a subgroup of the group of automorphisms of \(A\), one can view \(\alpha\) as a 1-cocycle of the group \(\text{Gal} (K_s/K)\) with values in \(\text{Aut}_{\kappa_s}(A)\). Let \(B = A_\alpha\) be the abelian variety over \(K\) obtained by twisting \(A\) by the cocycle \(\alpha\) (cf. [4, loc. cit.]). One sees immediately that the Galois module \(V_s(A)\) can be identified with the module \(V_s(A)_\alpha\) obtained by twisting \(V_s(A)\) by \(\alpha\). 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 \(\theta\) of \(A\) invariant by the finite group \(\mu \cap R\) (this is always possible), then we can furnish \(B = A_\alpha\) with a polarization \(\theta_B\) and a homomorphism

\[
i_B: F \to \mathbb{Q} \otimes \text{End}_{\kappa}(B),
\]

in such a way that \((B, i_B, \theta_B)\) is a \(K\)-form of \((A, i, \theta)\). 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 \(R = \text{End}_{\kappa_s}(A)\), 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 $\mu \subseteq R$, 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 $R = \text{End}_K(A)$. The action of $R$ on the tangent space to $A$ at the origin gives an embedding $F \rightarrow K$, by which we identify $F$ with a subfield of $K$. Note that $\mu$ 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: $F = \mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$, i.e., $\mu = \mu_4$ or $\mu_6$ and $F = \mathbb{Q}(\mu)$; moreover, the conductor of the order $R = \text{End}_K(A)$ is a prime power $p^\nu$, $\nu \geq 1$.

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 $N_{K_v/F_v}(U_v(K)) \subseteq U_p(R)$, where $w$ is the valuation of $F$ induced by $v$, and where $U_p(R)$ is the group of invertible elements of $R_p = \mathbb{Z}_p \otimes R$, viewed as a subgroup of $\prod_{p \neq p} U_w(F)$.

(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 $F = \mathbb{Q}(\mu)$. Let $z$ be a generator of $\mu$, and let $R_1 = \mathbb{Z} + \mathbb{Z}z$ be the ring of integers of $F$. For each integer $f \geq 1$, the order of $F$ with conductor $f$ is
$R(f) = \mathbb{Z} + fR_1 = \mathbb{Z} + \mathbb{Z}fz$, \\
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 $S$ satis-

fies (a) except possibly if the conductor $f$ of $R$ is a prime power $p^\nu, \nu \geq 1$. This \\
proves part (1) of Theorem 9.

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

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

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 $I_K \to C_K \to \text{Gal}(K^{ab}/K)$, \\
let us interpret the representation $\rho$, discussed in Corollary 2 of Theorem 5 \\
as a homomorphism \\

$$\rho_i : I_K \longrightarrow U_i(R) \subset F_i^*.$$ 

By the theory of complex multiplication (see § 7 below), there is a continuous 

homomorphism $\varepsilon : I_K \to F^*$ such that $\varepsilon | K^* = N_{K/F}$, and such that, for each 

prime number $l$, we have 

$$\rho_i(a) = \varepsilon(a)N_{K_{l/F_i}}(a_l^{-1}), \quad a \in I_K,$$

where $a_i$ denotes the component of the idèle $a$ in the group 

$$K_{l,*} = \left(\mathbb{Q}_l \otimes K\right)^* = \prod_{p_v = l} K_{v,*}.$$ 

Let $v$ be a valuation of $K$ with $p_v = p$. Taking $l \neq p$, the above formula 

shows that the restriction of $\varepsilon$ to $U_v(K)$ is $\varphi_v$. Taking $l = p$, and $u \in U_v(K)$, 

we have 

$$\rho_p(u) = \varepsilon(u)N_{K_{p/F_v}}(u^{-1});$$

since $\rho_p(u) \in U_p(R)$ and $\varepsilon(u) = \varphi_v(u)$, this shows that $\varphi_v(u)$ belongs to 

$N_{K_{p/F_v}}(u) \cdot U_p(R)$. But $U_p(R)$ intersects the image of $\mu$ in $F_p^*$ only at 1 and 

$-1$; it follows that $\varphi_v(U_v(K)) \subset \{\pm 1\}$ if and only if $N_{K_{p/F_v}}(U_v(K)) \subset U_p(R)$. 

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: 

$$X = C^* \times \prod_i U_i(R) = C^* \times \prod_{p \neq p} U_{p}(F) \times U_p(R).$$

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

field theory,
\[ N_{\mathbb{K}_w/F_w}(U_v(K)) = U_w(F) \cap XF^* . \]

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
\[
\frac{U_w(F \cap XF^*)}{U_w(F) \cap XF^* \cap U_p(R)} = \frac{U_w(F \cap XF^*)}{U_w(F) \cap XF^* \cap X} \cong \frac{(U_w(F) \cap XF^*)X}{X} \\
= \frac{(F^* \cap UXU_w(F))X}{X} = \frac{\mu X}{X} \cong \frac{\mu}{\mu z} = \frac{\mu}{\mu} .
\]

The only non-obvious step in this chain is the equality
\[ F^* \cap UXU_w(F) = \mu . \]

It holds because \( UXU_w(F) \) 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 \( U_p(Z) \) 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:

\[ j \in J(v) \iff v(j) \geq 0, v(j) \equiv 0 \pmod{3} \text{ and } v(j - 2^{63}) \equiv 0 \pmod{2}, \]

with the convention that \( \infty \equiv 0 \pmod{2} \) and \( \pmod{3} \), in case \( j = 0 \) or \( j = 2^{63} \). 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 explicitly 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 \( v(j) = 0 = v(j - 2^{63}) \), as the equation

\[ y^2 + xy = x^3 - \frac{\gamma^2 3^2}{j - 2^{63}} x - \frac{1}{j - 2^{63}} \]

shows. On the other hand, if \( p_v = 2 \) and \( v(j) > 0 \), then
\[ j \in J(v) \quad \overset{v(j) \geq 9,}{\text{if } v(2) = 1} \quad \overset{v(j) \leq 12,}{\text{if } v(2) > 1}, \]

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

\[ j \in J(v) \quad \overset{v(j - 2^{a}3^{b}) \geq 6.}{\text{}} \]

**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, and finally the property of \( j \) which implies the bad reduction at a place \( v \) of \( K = F(j) \) dividing \( f \):

<table>
<thead>
<tr>
<th>( F )</th>
<th>( f )</th>
<th>( j )</th>
<th>page</th>
<th>bad property</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \mathbb{Q} (\mu_6) )</td>
<td>2</td>
<td>( 2^{4}3^{3}5^{3} )</td>
<td>474</td>
<td>( v(j) = 4 \equiv 0 \pmod{3} )</td>
</tr>
<tr>
<td>( \mathbb{Q} (\mu_6) )</td>
<td>3</td>
<td>( -3 \cdot 2^{15}5^{3} )</td>
<td>462</td>
<td>( v(j) = 2 \equiv 0 \pmod{3} )</td>
</tr>
<tr>
<td>( \mathbb{Q} (\mu_4) )</td>
<td>2</td>
<td>( 2^{3}3^{3}11^{3} )</td>
<td>477</td>
<td>( 0 &lt; v(j) = 6 &lt; 12 )</td>
</tr>
<tr>
<td>( \mathbb{Q} (\mu_4) )</td>
<td>3</td>
<td>( 2^{4}(x^9 - 4)x^{-8} )</td>
<td>479</td>
<td>( v(j - 2^{a}3^{b}) = 3 \equiv 0 \pmod{2} )</td>
</tr>
<tr>
<td>( \mathbb{Q} (\mu_4) )</td>
<td>3</td>
<td>( 2^{6}(4x^{24} - 1)x^{-24} )</td>
<td>479</td>
<td>( v(j - 2^{a}3^{b}) = 1 \equiv 0 \pmod{2} )</td>
</tr>
</tbody>
</table>

In the first three examples, one has \( K = F \). In the fourth,

\[ K = \mathbb{Q} (\sqrt{-1}, \sqrt{3}) \quad \text{and} \quad x = 1 \pm \sqrt{3}. \]

In the fifth, \( K = \mathbb{Q} (\sqrt{-1}, \sqrt{5}) \) 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 \( \mathbb{Q} \)) 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 \( R \otimes K = F \otimes_{\mathbb{Q}} K \); in other words, \( t \) is an \( (F, K) \)-bimodule over \( \mathbb{Q} \). Let \( d' \) be the dimension of \( t \) as an \( F \)-vector space. Then \( [K: \mathbb{Q}] = 2d' \), because

\[ d[K: \mathbb{Q}] = \dim_{\mathbb{Q}}(t) = [F: \mathbb{Q}]d' = 2dd'. \]

For each commutative \( \mathbb{Q} \)-algebra \( \Lambda \), the tensor product \( t \otimes_{\mathbb{Q}} \Lambda \) is an

---

5 Weber usually gives, instead of \( j \), some modular function of higher level. For instance, if \( F = \mathbb{Q}(\mu_6) \) and the conductor is 2, one has \( R = \mathbb{Z} + \mathbb{Z} \sqrt{-3}, j = j(\sqrt{-3}) \) and one finds in Weber, p. 474, \( f(\sqrt{-3}) = \frac{3}{2} \), where \( f \) is such that \( j_0 = f(\omega^{24} - 16)f(\omega)^6 \); hence \( j(\sqrt{-3}) = 2^{4}3^{3}5^{3} \).
(\(F \otimes_{\mathbb{Q}} \Lambda, K \otimes_{\mathbb{Q}} \Lambda\))-bimodule over \(\Lambda\). If \(u \in K \otimes_{\mathbb{Q}} \Lambda\), we denote by \(\text{det}_t(u)\) the determinant of the corresponding endomorphism of \(t \otimes_{\mathbb{Q}} \Lambda\) (viewed as a free module of rank \(d'\) over \(F \otimes_{\mathbb{Q}} \Lambda\); if \(u\) is invertible in \(K \otimes_{\mathbb{Q}} \Lambda\), so is \(\text{det}_t(u)\) in \(F \otimes_{\mathbb{Q}} \Lambda\). Hence the map \(\text{det}_t\) gives a homomorphism

\[
\psi_\Lambda: (K \otimes_{\mathbb{Q}} \Lambda)^* \longrightarrow (F \otimes_{\mathbb{Q}} \Lambda)^*
\]

which is functorial in \(\Lambda\). In the language of algebraic groups, this means that \(\psi\) is a morphism \(T_\Lambda \rightarrow T_F\), where \(T_\Lambda\) and \(T_F\) are the tori corresponding to \(K\) and \(F\), i.e., the affine algebraic groups over \(\mathbb{Q}\) which represent the functors

\[
\Lambda \longmapsto (K \otimes_{\mathbb{Q}} \Lambda)^* \quad \text{and} \quad \Lambda \longmapsto (F \otimes_{\mathbb{Q}} \Lambda)^*,
\]

respectively. When \(\Lambda\) is \(\mathbb{Q}\) (resp. \(\mathbb{Q}_t\), resp. \(\mathbb{R}\)) we write \(\psi_0\) (resp. \(\psi_1\), resp. \(\psi_\infty\)) instead of \(\psi_\Lambda\). These are homomorphisms

\[
\begin{align*}
&\psi_0: K^* \longrightarrow F^*, \\
&\psi_1: K_1^* \longrightarrow F_1^*, \quad \text{where } K_1 = \mathbb{Q}_t \otimes K \text{ and } F_1 = \mathbb{Q}_t \otimes F, \\
&\psi_\infty: K_\infty^* \longrightarrow F_\infty^*, \quad \text{where } K_\infty = \mathbb{R} \otimes K \text{ and } F_\infty = \mathbb{R} \otimes F.
\end{align*}
\]

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

\[
\bar{\iota}: F \longrightarrow \mathbb{Q} \otimes \text{End}(A) \longrightarrow \mathbb{Q} \otimes \text{End}(\bar{A}_v).
\]

Since \(\bar{\pi}_v\) commutes with every \(k_v\)-endomorphism of \(\bar{A}_v\), Corollary 1 of Theorem 5 shows that \(\bar{\pi}_v \in \text{Im}(\bar{\iota})\). Thus there is a unique element \(\pi_v \in F\) such that \(\bar{\iota}(\pi_v) = \bar{\pi}_v\); we call \(\pi_v\) 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 \(\varepsilon\) to \(K^*\) is the map \(\psi_0: K^* \rightarrow F^*\) defined above.

(b) The homomorphism \(\varepsilon\) 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
\[ (*) \quad \varepsilon(a) = \prod_{v \in S} \pi_v^{s(a_v)} \quad \text{for } a \in I_K^S. \]

(The last condition means that, for \( v \in S \), the image under \( \varepsilon \) of any uniformizing element at \( v \) is the Frobenius element \( \pi_v \) 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 \( \varepsilon : I_K \to F_l^* \) be a homomorphism. Then it is clear that \( \varepsilon \) 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 \( \varepsilon \) satisfying all three conditions, and shows also that the existence of such an \( \varepsilon \) for the set \( S \) in question is equivalent to the existence of an \( N \) as above such that

\[ \prod_{v \in S} \pi_v^{s(a)} = \psi_v(\alpha) \quad \text{for all } \alpha \in K^* \cap N. \]

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 \( f_m \), and for \( N \) the group of idèles \( \equiv 1 \) (mod \( f_m \)). Hence the theorem.

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

\[ \rho_l : I_K \to F_l^* \]

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 \( \rho_l \) is unramified at \( v \) (i.e., \( \rho_l \) is trivial on \( U_v(K) \)) and takes the value \( \pi_v \) at each uniformizing element of \( K_v^* \).

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

\[ (***) \quad \rho_l(a) = \varepsilon(a)\psi_l(a_l^{-1}) \quad \text{for all } a \in I_K, \]

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

(ii) For every valuation \( v \) of \( K \), the restriction of \( \varepsilon \) to \( U_v(K) \) is the homomorphism \( \varphi_v \) of § 5 (cf. Remark 3 after Theorem 6).

Let \( S \) be a set of places satisfying condition (c) of Theorem 10, and let \( I_{K,1}^S \) 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, \( \rho_l \) coincides with \( \varepsilon \) on \( I_{K,1}^S \), and since \( a_1 = 1 \) for \( a \in I_{K,1}^S \), it follows that \((***)\) holds for \( a \in I_{K,1}^S \). For \( \alpha \in K^* \) we have \( \varepsilon(\alpha) = \psi_0(\alpha) = \psi_l(\alpha) \); hence \((***)\) holds for the dense subgroup \( K^* I_{K,1}^S \).
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 $a_i = 1$ for $a \in K^*_v$, and $(**)$ shows that $\varepsilon$ coincides with $\rho_i$ on $K^*_v$. Hence, on $U_v(K)$, $\varepsilon$ coincides with $\varphi_v$, the restriction of $\rho_i$ (cf. Theorem 6).

**Corollary 1.** The abelian variety $A$ has good reduction at $v$ if and only if $\varepsilon$ 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 $\rho_i$ and $1/\psi_i$ coincide on an open subgroup of $U_i(K) = \prod_{p_v = l} U_v(K)$; they coincide on all of $U_i(K)$ 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 $\rho_i$ and $1/\psi_i$ coincide on all of $U_i(K)$ if and only if $A$ has good reduction at $v$.)

Indeed, if $x \in U_i(K)$, one has $\rho_i(x) = 1/\psi_i(x)$ if and only if $\varepsilon(x) = 1$.

**Remark.** Conversely, if for one prime $l$ one knows$^6$ that $\rho_i$ and $1/\psi_i$ coincide on some open subgroup of $U_i(K)$, then one recovers Theorem 10 immediately by defining $\varepsilon$ by the formula

$$\varepsilon(a) = \rho_i(a)\psi_i(a)$$

for $a \in I_K$.

(A priori, this $\varepsilon$ has values in $F_i^*$, 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

$$\rho_{\infty}: I_K \longrightarrow F^*_\infty = (R \otimes F)^*$$

by putting $\rho_{\infty}(a) = \varepsilon(a)\psi_{\infty}(a_{\infty})$, where $a_{\infty}$ 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 $\varepsilon$ on the group $I_K^\infty$ of idèles whose infinite component is 1.

Let $\sigma: F \rightarrow C$ be a homomorphism. The composition

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

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

$^6$ Indeed, this can also be proved by focal 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 \( \chi_\sigma \) to \( U_\sigma(K) \) is \( \sigma \circ \varphi_\sigma \), and, since \( \sigma \) is injective, it follows that the exponent at \( v \) of the conductor of \( \chi_\sigma \) is equal to the number \( n_v \) of Theorem 6. Hence:

**Theorem 12.** The conductor of the abelian variety \( A \) is the \( 2d^{th} \) power of the conductor of \( \chi_\sigma \); in particular, the support of the conductor of \( \chi_\sigma \) 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 \( \text{char} \ (k) \), and let \( i \) be a positive integer. Denote by \( H^i_l \) the \( i^{th} \) \( l \)-adic cohomology vector space of \( X_\sigma = X \times_k K_\sigma \), for the étale topology (cf. [2]). Assume that \( \text{char} \ (K) = 0 \) or that \( X \) is proper over \( K \), so that \( H^i_l \) is finite dimensional over \( Q_l \) (loc. cit.). The group \( \text{Gal} \ (K_s/K) \) acts on \( H^i_l \). This defines a continuous homomorphism

\[ \rho_\sigma : \text{Gal} \ (K_s/K) \longrightarrow \text{Aut} \ (H^i_l). \]

Let \( \text{Tr} (\rho_\sigma) \) be the character of this representation.

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

If so, there is an open subgroup \( H \) of \( I(\overline{v}) \) such that \( \rho_\sigma(s) \) is unipotent for all \( s \in H \) (this has been proved by Grothendieck in a special case, see below). Moreover, \( \text{Tr} (\rho_\sigma) \) then defines a character of a finite quotient of \( I(\overline{v}) \); 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 \( D(\overline{v}) \) whose image in \( \text{Gal} \ (\overline{k}/k) \) is an integral power \( F^* \) of the Frobenius element \( F_\sigma \).

**Problem 2.** Is it true that the characteristic polynomial of \( \rho_\sigma(s) \) has rational coefficients independent of \( l \)? If so, is it true that the roots \( z_\sigma \) of this polynomial have absolute value \( q^{-n_\sigma i/2} \), where \( 0 \leq i_\sigma \leq 2i \)?

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 \( H^i_l \) 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 \( \rho: D(\bar{v}) \rightarrow \text{GL}(n, \mathbb{Q}_l) \) 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 \( x \in \text{Im}(\rho) \) has coefficients in \( \mathbb{Z}_l \) and is congruent to 1 mod \( l^r \). This implies in particular that \( \text{Im}(\rho) \) 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 \( K \); we have

\[
\text{Gal}(K_s/K_{nr}) = I(\bar{v}) \quad \text{and} \quad \text{Gal}(K_{nr}/K) = \text{Gal}(k_s/k).
\]

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

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

\[
T_i(\mu) \simeq \text{Gal}(K_i/K_{nr})
\]

is compatible with the action of \( \text{Gal}(k_s/k) \), acting in the natural way on \( T_i(\mu) \) and acting on \( \text{Gal}(K_i/K_{nr}) \) by inner automorphisms of the extension \( \text{Gal}(K_i/K) \). Let \( \chi: \text{Gal}(k_s/k) \rightarrow \mathbb{Z}_l^* \) be the character giving the action of \( \text{Gal}(k_s/k) \) on \( T_i(\mu) \). If \( s \) belongs to the pro-\( l \)-group \( \text{Gal}(K_i/K_{nr}) \), the compatibility mentioned above shows that \( s \) and \( s^{\chi(\mu)} \) are conjugate in \( \text{Gal}(K_i/K) \) for
every \( t \in \text{Gal}(k_s/k) \). 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 \( t \in \text{Gal}(k_s/k) \). If \( a_i(X) \) is the \( i \)th symmetric function of the characteristic roots of \( X \), this shows that
\[
a_i(X) = a_i(\chi(t)X) = \chi(t)^i a_i(X).
\]
But the condition \((C_i)\) means that the image of \( \chi \) is an infinite subgroup of \( \mathbb{Z}_l^* \). 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 \( \rho(s) = 1 \mod l^2 \), we have
\[
\rho(s) = \exp \left( \log \rho(s) \right) = \exp(X),
\]
hence \( \rho(s) \) is unipotent, q.e.d.

Collège de France,
Harvard University

Bibliography


(Received March 18, 1968)