FINITENESS THEOREMS IN GEOMETRIC CLASSFIELD THEORY

by Nicholas M. KATZ [1]) and Serge LANG [1])

(with an appendix by Kenneth A. RIBET)

0. INTRODUCTION

The geometric classfield theory of the 1950's was the principal precursor of the Grothendieck theory of the fundamental group developed in the early 1960's (cf. SGA I, Exp. X, 1.10). The problem was to understand the abelian unramified coverings of a variety X, or, as we would say today, to understand $\pi_1(X)^{ab}$. When X is "over" another variety S, the functoriality of π_1^{ab} gives a natural homomorphism.

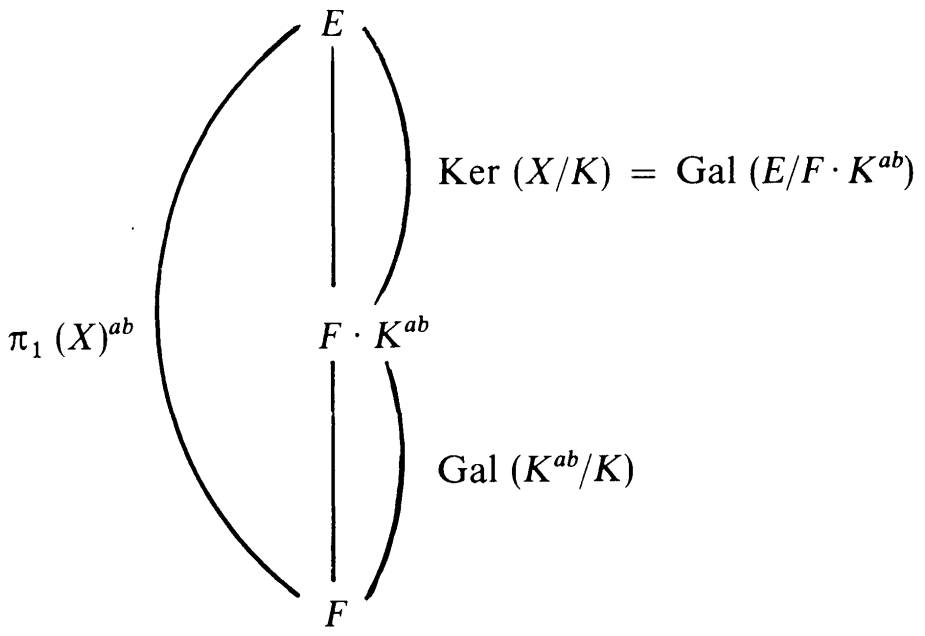
$$\pi_1(X)^{ab} \to \pi_1(S)^{ab}$$

whose kernel Ker (X/S) measures the extent to which the abelian coverings of X fail to "come from" abelian coverings of S.

In the language of the 1950's, we can make the problem "explicit" in terms of galois theory. Thus we consider the case when $S = \text{Spec}(K)$, with K a field, and X a smooth and geometrically connected variety over K. Let F denote the function field of X, and denote by E/F the compositum, inside some fixed algebraic closure of F, of all finite abelian extensions E_i/F which are unramified over X in the sense that the normalization of X in E_i is finite etale over X. Then $\pi_1(X)^{ab}$ is "just" the galois group Gal (E/F).

Each finite extension L_i/K of K gives rise to a constant-field extension $F \cdot L_i$ over F which is abelian and unramified over X, so that if we denote by K^{ab} the maximal abelian extension of K, we have a diagram of fields and galois groups

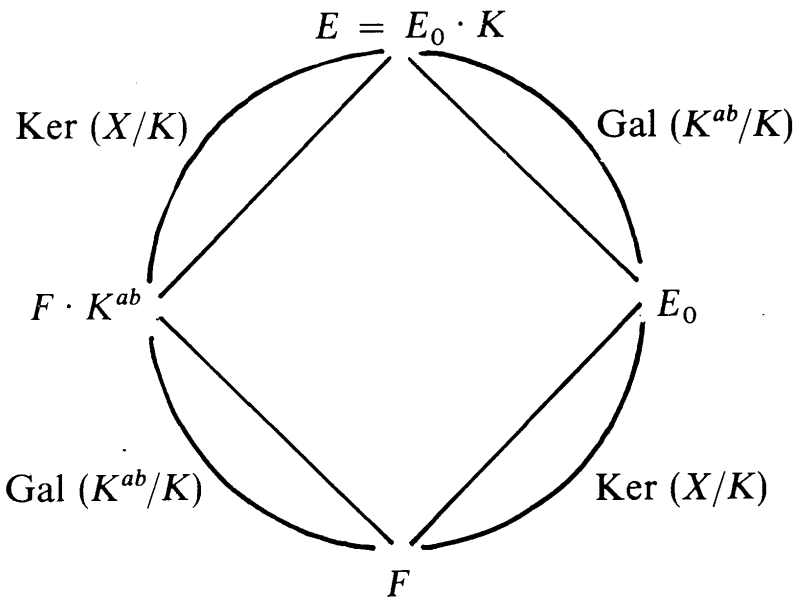
[1]) Supported by NSF grants.



and a corresponding exact sequence

$$\begin{array}{ccccccccc} 0 & \to & \mathrm{Ker}\,(X/K) & \to & \pi_1(X)^{ab} & \to & \mathrm{Gal}\,(K^{ab}/K) & \to & 0 \\ & & \| & & \| & & \| & & \\ & & \mathrm{Gal}\,(E/F\cdot K^{ab}) & & \mathrm{Gal}\,(E/F) & & \mathrm{Gal}\,(F\cdot K^{ab}/F) & & \end{array}$$

If we suppose further that X admits a K-rational point x_0, then we can "descend" the extension $E/(F \cdot K^{ab})$ to an extension E_0/F by the following device: we define E_0 to be the union of those finite abelian extensions E_i/F which are unramified over X, and such that the fibre over x_0 of the normalization X_i of X in E_i consists of deg (E_i/F) distinct K-rational points of X_i. Then E_0/F is a geometric extension, i.e. K is algebraically closed in E_0, and E is the compositum $E_0 \cdot K^{ab}$. Thus we have a diagram of fields and galois groups



and a corresponding splitting of the above exact sequence

$$\begin{array}{ccccccccc} 0 & \to & \mathrm{Ker}\,(X/K) & \to & \pi_1\,(X)^{ab} & \to & \mathrm{Gal}\,(K^{ab}/K) & \to & 0 \\ & & \| & & \| & & \| & & \\ & & \mathrm{Gal}\,(E_0/F) & & \mathrm{Gal}\,(E/F) & & \mathrm{Gal}\,(E/F_0) & & \end{array}$$

We will see that when K is a number field, i.e. a finite extension of $\mathbf{Q}$, then the group Ker (X/K) is finite, or in other words the extension $E/(F \cdot K^{ab})$ (as well as the extension E_0/F when X has a K-rational point x_0) is *finite.*

Our main result is a finiteness theorem for the kernel group Ker (X/S) for a reasonably wide class of situations X/S which are sufficiently "of absolutely finite type" (cf. Theorems 1 & 2 for precise statements). When in addition we have *a priori* control of $\pi_1\,(S)^{ab}$, [as provided by global classfield theory when S is the (spectrum of) the ring of integers in a number field], or a systematic way of ignoring $\pi_1\,(S)^{ab}$ [e.g. if X/S has a section] we get "absolute" finiteness theorems (cf. Theorems 3, 4, 5 for precise statements). Following Deligne ([2], 1.3) and Grothendieck, we also give an application of our result to the theory of l-adic representations of fundamental groups of varieties over absolutely finitely generated fields (cf. Theorem 6 for a precise statement). In fact, it was this application, already exploited so spectacularly by Deligne in the case of varieties over finite fields, which aroused [resp. rearoused] our interest in the questions discussed here. For an application of these theorems to K-theory, we refer to recent work of Spencer Bloch [1] and A. H. Parshin [12].

The idea behind our proof is to reduce first to the case of an open curve over a field, by using Mike Artin's "good neighborhoods" and an elementary but useful exact homotopy sequence (cf. Preliminaries, Lemma 2). We then reduce to the case of an abelian variety over a field by using the theory of the generalized Jacobian. A standard specialization argument then reduces us to the case of an abelian variety over a finite field. In this case, we use Weil's form ([12], thm. 36) of the Lefschetz trace formula for abelian varieties to reduce our finiteness theorem to the fact that the number of rational points on an abelian variety over a finite field is finite and non-zero!

In explicating our results in the case of an abelian variety over a number field (cf. Section II, Remark 2), we were led to the conjecture that if A is an abelian variety over a number field k, and if $k\,(\mu)$ is the extension of k obtained by adjoining to k all roots of unity, then the torsion subgroup of A in $k\,(\mu)$ is finite. We shall prove this conjecture when A has complex multiplication. In an appendix, Ribet extends this result to a proof of the conjecture in general.

II. Preliminaries

Let S be a connected, locally noetherian scheme, and s a geometric point of S (i.e., s is a point of S with values in an algebraically closed field). The fundamental group $\pi_1(S, s)$ in the sense of SGA I is a profinite group which classifies the finite etale coverings of S. Given two geometric points s_1 and s_2 each choice of "chemin" $c(s_1, s_2)$ from s_1 to s_2 determines an isomorphism

$$c(s_1, s_2): \pi_1(S, s_1) \xrightarrow{\sim} \pi_1(S, s_2)$$

and formation of this isomorphism is compatible with composition of chemins. If we fix s_1 and s_2 but vary the chemin, this isomorphism will (only) change by an inner automorphism of, say, $\pi_1(S, s_2)$.

Therefore the *abelianization* of $\pi_1(S, s)$ (in the category of profinite groups) is canonically independant of the auxiliary choice of base point; we will denote it $\pi_1(S)^{ab}$. This profinite abelian group classifies (*fppf*) torsors over S with (variable) finite abelian structure group, i.e. for any finite abelian group G we have a canonical isomorphism

$$\text{Hom}_{gp}(\pi_1(S)^{ab}, G) \xrightarrow{\sim} H^1_{et}(S, G). \tag{1.1}$$

The total space of the G-torsor T/S is connected if and only if its classifying map $\pi_1(S)^{ab} \to G$ is surjective.

Given a morphism $f: X \to S$ between connected locally noetherian schemes, a geometric point x of X and its image $s = f(x)$ in S, there is an induced homomorphism

$$\pi_1(X, x) \to \pi_1(S, s)$$

of fundamental groups. The induced homomorphism

$$\pi_1(X)^{ab} \to \pi_1(S)^{ab}$$

is independent of the choice of geometric point x; indeed for any finite abelian group G the transposed map

$$\text{Hom}(\pi_1(S)^{ab}, G) \to \text{Hom}(\pi_1(X)^{ab}, G)$$

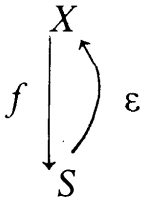
is naturally identified with the map "inverse image of G-torsors"

$$f^*: H^1_{et}(S; G) \to H^1_{et}(X; G).$$

We will denote by $\text{Ker}(X/S)$ the kernel of the map of π_1^{ab}'s. Thus we have a tautological exact sequence

(1.2) $$0 \to \mathrm{Ker}\,(X/S) \to \pi_1\,(X)^{ab} \to \pi_1\,(S)^{ab}\,.$$

When X/S has a section

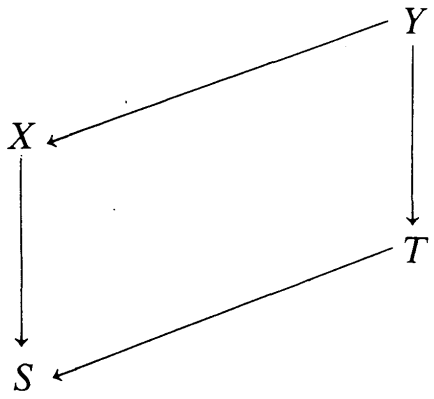


there is a simple interpretation of Ker (X/S); it classifies those torsors on X with finite abelian structure group whose inverse image via ε is trivial on S, i.e. whose restriction to the section, viewed as a subscheme of X, is completely decomposed. There is a natural product decomposition

(1.3) $$\pi_1\,(X)^{ab} \simeq \pi_1\,(S)^{ab} \times \mathrm{Ker}\,(X/S)$$

corresponding to the expression of a G-torsor on X as the "sum" of a G-torsor on X whose restriction to ε is completely decomposed and the inverse image by f of a G-torsor on S. In particular, given, a G-torsor T/X whose restriction to ε is completely decomposed, T is connected if and only if its classifying map Ker $(X/S) \to G$ is surjective. In the absence of a section, there seems to be no simple physical interpretation of Ker (X/S).

There are two elementary functorialities. it is convenient to formulate explicitly. Consider a commutative diagram of morphisms of connected, locally noetherian schemes



Proceeding down to the left, we have an exact sequence

(1.4) $$0 \to \mathrm{Ker}\,(Y/X) \to \mathrm{Ker}\,(Y/S) \to \mathrm{Ker}\,(X/S)\,.$$

Proceeding across, we have an induced map

(1.5) $$\mathrm{Ker}\,(Y/T) \to \mathrm{Ker}\,(X/S)$$

which sits in a commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Ker}\,(Y/T) & \longrightarrow & \pi_1(Y)^{ab} & \longrightarrow & \pi_1(T)^{ab} \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \mathrm{Ker}\,(X/S) & \longrightarrow & \pi_1(X)^{ab} & \longrightarrow & \pi_1(S)^{ab}. \end{array}$$

Let X be a geometrically connected noetherian scheme over a field K, (i.e. $X \otimes \overline{K}$ is connected, where $\overline{K}$ denotes an algebraic closure of K). Let $\bar{x}$ be a geometric point of $X \otimes \overline{K}$, x its image in X, and s its image in Spec $(K) = S$. The fundamental exact sequence (SGA I, IX, 6.1)

$$0 \to \pi_1(X \otimes \overline{K}, \bar{x}) \to \pi_1(X, x) \to \pi_1(S, s) \to 0 \tag{1.6}$$

yields, upon abelianization, an exact sequence

$$\pi_1(X \otimes \overline{K})^{ab} \to \pi_1(X)^{ab} \to \pi(S)^{ab} \to 0 \tag{1.7}$$

The exact sequence (1.6) allows us to define an action "modulo inner automorphism" of $\pi_1(S, s)$ on $\pi_1(X \otimes \overline{K}, \bar{x})$ (given an element $\sigma \in \pi_1(S, s)$, choose $\tilde{\sigma} \in \pi_1(X, x)$ lying over it and conjugate $\pi_1(X \otimes \overline{K}, \bar{x})$ by this $\tilde{\sigma}$). The induced action of $\pi_1(S, s)$ on $\pi_1(X \otimes \overline{K})^{ab}$ is therefore well-defined. (This same action is well-defined, and trivial, on $\pi_1(X)^{ab}$.)

Therefore the map $\pi_1(X \otimes \overline{K})^{ab} \to \pi_1(X)^{ab}$ factors through the coinvariants of the action of $\pi_1(S, s)$ on $\pi_1(X \otimes \overline{K})^{ab}$: we have an exact sequence

$$(\pi_1(X \otimes \overline{K})^{ab})_{\pi_1(S, s)} \to \pi_1(X)^{ab} \to \pi_1(S)^{ab} \to 0. \tag{1.8}$$

If we identify $\pi_1(S, s)$ for $S = \mathrm{Spec}\,(K)$ with the galois group $\mathrm{Gal}\,(\overline{K}/K)$, (which we may do canonically (only) up to an inner automorphism), then this last exact sequence may be rewritten

$$(\pi_1(X \otimes \overline{K})^{ab})_{\mathrm{Gal}\,(\bar{K}/K)} \to \pi(X)^{ab} \to \mathrm{Gal}\,(\overline{K}/K)^{ab} \to 0. \tag{1.9}$$

Consider the special case in which X has a K-rational point x_0; if we choose for $\bar{x}$ the geometric point "x_0 viewed as having values in the overfield $\overline{K}$ of K" then the morphism x_0: Spec $(K) \to X$ which "is" x_0 gives a splitting of the exact sequence (1.6)

$$0 \to \pi_1(X \otimes \overline{K}, \bar{x}) \to \pi_1(X, x) \underset{x_0}{\rightleftarrows} \pi_1(S, s) \to 0 \tag{1.10}$$

so that we have a semi-direct product decomposition

$$\pi_1(X, x) \simeq \pi_1(X \otimes \overline{K}, \bar{x}) \rtimes \mathrm{Gal}\,(\overline{K}/K). \tag{1.11}$$

"Physically", the action of Gal $(\overline{K}/K)$ on $\pi_1(X \otimes \overline{K}, \vec{x})$ is simply induced by the action of Gal $(\overline{K}/K)$ on the coefficients of the defining equations of finite etale coverings of $X \otimes \overline{K}$; this action is well defined on $\pi_1(X \otimes \overline{K}, \vec{x})$ precisely because $\vec{x}$ is a $\overline{K}$-valued point which is fixed by Gal $(\overline{K}/K)$; if $\vec{x}$ were not fixed, an element $\sigma \in$ Gal would "only" define an isomorphism

$$\pi_1(X \otimes \overline{K}, \vec{x}) \xrightarrow{\sim} \pi_1(X \otimes \overline{K}, \sigma(\vec{x})).$$

The semi-direct product decomposition (1.11) yields, upon abelianization, a product decomposition

$$\pi_1(X)^{ab} \xrightarrow{\sim} ((\pi_1(X \otimes \overline{K})^{ab})_{\mathrm{Gal}(\bar{K}/K)} \times \mathrm{Gal}(\overline{K}/K)^{ab}; \tag{1.12}$$

in other words, the existence of a K-rational point on X assures that the right exact sequence (1.9) is actually a split short exact sequence

$$0 \to ((\pi_1(X \otimes \overline{K})^{ab})_{\mathrm{Gal}(\bar{K}/K)} \to \pi_1(X)^{ab} \to \mathrm{Gal}(\overline{K}/K)^{ab} \to 0.$$

For ease of later reference, we explicitly formulate the following lemma.

LEMMA 1. *Let X be a geometrically connected noetherian scheme over a field K. Then* Ker (X/K) *is the image of* $\pi_1(X \otimes \overline{K})^{ab}$ *in* $\pi_1(X)^{ab}$. *The natural surjective homomorphism*

$$\pi_1(X \otimes \overline{K})^{ab} \to \mathrm{Ker}(X/K)$$

factors through a surjection

$$(\pi_1(X \otimes \overline{K})^{ab})_{\mathrm{Gal}(\bar{K}/K)} \twoheadrightarrow \mathrm{Ker}(X/K) \tag{1.14}$$

which is an isomorphism if X has a K-rational point. Given any algebraic extension L/K, the natural map

$$\mathrm{Ker}(X \underset{K}{\otimes} L/L) \to \mathrm{Ker}(X/K) \tag{1.15}$$

is surjective.

Proof. The only new assertion is the surjectivity of (1.15), and this follows immediately from the surjectivity of the indicated maps in the commutative diagram

$$\begin{array}{ccccc} & (\pi_1(X \otimes \overline{K})^{ab})_{\mathrm{Gal}(\bar{K}/L)} & \twoheadrightarrow & \mathrm{Ker}(X \underset{K}{\otimes} L/L) & \hookrightarrow & \pi_1(X \underset{K}{\otimes} L)^{ab} \\ \pi_1(X \otimes \overline{K})^{ab} \nearrow & \downarrow & & \downarrow & & \downarrow \\ & (\pi_1(X \otimes \overline{K})^{ab})_{\mathrm{Gal}(\bar{K}/K)} & \twoheadrightarrow & \mathrm{Ker}(X/K) & \hookrightarrow & \pi_1(X)^{ab}. \end{array}$$

Now consider a normal, connected locally noetherian scheme S with generic point η and function field K. We fix an algebraic closure $\overline{K}$ of K, and denote by $\bar{\eta}$ the corresponding geometric point of S. The fundamental group $\pi_1(S, \bar{\eta})$ is then a quotient of the Galois group $\mathrm{Gal}(\overline{K}/K)$; the functor "fibre over η"

$$\{\text{connected finite etale coverings of } S\} \to \{\text{finite separable extensions } L/K\}$$

is fully faithful, with image those finite separable extensions L/K for which the normalization of S in L is finite etale over S.

LEMMA 2. *Let S be normal, connected and locally noetherian, with generic point η and function field K. Let $f: X \to S$ be a smooth surjective morphism of finite type, whose geometric generic fibre $X_{\bar{\eta}}$ is connected. Then*

(1) *X is normal and connected.*

(2) *For any geometric point $\bar{x}$ in $X_{\bar{\eta}}$ with image x in X and s in S, the sequence*

$$\pi_1(X_{\bar{\eta}}, \bar{x}) \to \pi_1(X, x) \to \pi_1(S, s) \to 0$$

is exact.

(3) *$\mathrm{Ker}(X/S)$ is the image of $\pi_1(X_{\bar{\eta}})^{ab}$ in $\pi_1(X)^{ab}$.*

(4) *The natural map*

$$\mathrm{Ker}(X_\eta/K) \to \mathrm{Ker}(X/S)$$

is surjective.

Proof. (1) Because X is smooth over a normal scheme, it is itself normal (SGAI, Exp II, 3.1). To see that X is connected, we argue as follows. The map f, being flat (because smooth) and of finite type over a locally noetherian scheme, is *open* (SGAI, Exp IV, 6.6). Therefore any nonvoid open set $U \subset X$ meets X_η (because $f(U)$ is open and non-empty in S, so contains η). But X_η is connected (because $X_{\bar{\eta}}$ is !) and therefore the intersection of any two-non-empty open sets in X meets X_η.

(2) Because X is normal and connected, it has a generic point ξ and a function field F, and its function field F is none other than the function field of X_η (itself normal (because smooth over K) and connected). Therefore the natural map

$$\pi_1(X_{\bar{\eta}}, \bar{\xi}) \to \pi_1(X, \bar{\xi})$$

must be surjective, because it sits in the commutative diagram

$$\begin{array}{ccc} & & \pi_1(X_\eta, \bar{\xi}) \\ & \nearrow & \downarrow \\ \mathrm{Gal}(\bar{F}/F) & & \\ & \searrow & \\ & & \pi_1(X, \bar{\xi}) \end{array}$$

Comparing our putative exact sequence with its analogue for X_η/K, we have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \pi_1(X_{\bar{\eta}}, \bar{x}) & \longrightarrow & \pi_1(X_\eta, x) & \longrightarrow & \mathrm{Gal}(\bar{K}/K) & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow & & \\ & & \pi_1(X_{\bar{\eta}}, \bar{x}) & \xrightarrow{\alpha} & \pi_1(X, x) & \xrightarrow{\beta} & \pi_1(S, s) & \longrightarrow & 0 \end{array}$$

whose top row is exact. Therefore β is surjective, and $\beta \circ \alpha = 0$. To show the exactness, given the surjectivity of β, we must show (cf. SGA I, Exp V, 6.6) that any connected etale covering Y of X which admits a section over $X_{\bar{\eta}}$ is isomorphic to the inverse image of a connected etale covering of S. Given such Y, its restriction Y_η to X_η is still connected; so the existence of a section over $X_{\bar{\eta}}$ and the exactness of (1.6) imply that Y_η is the normalization of X_η in a constant-field extension $F \cdot L$, where L is a finite separable extension of K. Therefore the function field of Y is $F \cdot L$, whence Y is the normalization of X in $F \cdot L$. Let S' denote the normalization of S in L. Then S' is finite over S. We will show that S' is finite etale over S, and that Y is the inverse image over X of this covering. By (1) applied to $X \underset{S}{\times} S'/S'$, the scheme $X \underset{S}{\times} S'$ is normal and connected, and finite over X. Therefore $X \underset{S}{\times} S'$ is just the normalization of X in its function field, i.e. in $F \cdot L$. Therefore $Y = X \underset{S}{\times} S'$. It remains only to see that S'/S is finite etale. But this follows by *fpqc* descent from that fact that $Y = X \underset{S}{\times} S'$ is finite etale over X.

(3) This follows immediately from the exact sequence established in (2), by abelianization.

(4) This follows immediately from (3), and the commutativity of the diagram of maps induced by the obvious inclusions

$$\begin{array}{ccc} \pi_1(X_\eta)^{ab} & \longrightarrow & \pi_1(X_\eta)^{ab} \\ & \searrow \quad \swarrow & \\ & \pi_1(X)^{ab} & \end{array}$$

LEMMA 3. *Let X be a smooth geometrically connected variety of finite type over a field K, and let $U \subset X$ be any non-empty open set. Then the natural map*

$$\mathrm{Ker}\,(U/K) \to \mathrm{Ker}\,(X/K)$$

is surjective.

Proof. The variety $X \otimes \overline{K}$ is normal and connected, as is the non-empty open $U \otimes \overline{K}$ in it. Therefore the natural map $\pi_1(U \otimes \overline{K}) \to \pi_1(X \otimes \overline{K})$ is surjective (because both source and target are quotients of the galois group of their common function field). The result now follows from the indicated surjectivities in the commutative diagram

$$\begin{array}{ccc} \pi_1(U \otimes \overline{K})^{ab} & \twoheadrightarrow & \mathrm{Ker}\,(U/K) \\ \downarrow & & \downarrow \\ \pi_1(X \otimes \overline{K})^{ab} & \twoheadrightarrow & \mathrm{Ker}\,(X/K)\,. \end{array}$$

II. THE MAIN THEOREM

Recall that a field K is said to be absolutely finitely generated if it is a finitely generated extension of its prime field, i.e. of $\mathbf{Q}$ or of $\mathbf{F}_p$.

THEOREM 1. *Let S be a normal, connected, locally noetherian scheme, whose function field K is an absolutely finitely generated field. Let $f: X \to S$ be a smooth surjective morphism of finite type, whose geometric generic fibre is connected. Then the group $\mathrm{Ker}\,(X/S)$ is finite if K has characteristic zero, and it is the product of a finite group with a pro-p group in case K has characteristic p.*

Proof. We will first reduce to the case in which X/S is an elementary fibration in the sense of M. Artin (SGA 4, Exp XI, 3.1), i.e. the complement, in a proper and smooth *curve* C/S with geometrically connected fibres, of a divisor $D \subset C$ which is finite etale over S. By lemma 2, part (4), Ker (X/S) is a quotient of Ker (X_η/K), so we are reduced to the case $S = \text{Spec } (K)$. If L is a finite extension of K, then Ker (X/K) is a quotient of Ker $(X \otimes L/L)$ (by lemma 1), so we may further reduce to the case when X/K has a K-rational point, say x_0. Thanks to M. Artin's theory of good neighborhoods (SGA 4, Exp XI, 3.3), at the expense of once again passing to a finite extension field L of K, we can find a Zariski open neighborhood U of x_0 in $X \underset{K}{\otimes} L$ which sits atop a finite tower

$$
\begin{array}{l}
U = U_0 \\
\quad\downarrow \quad f_0 \\
\quad U_1 \\
\quad\downarrow \quad f_2 \\
\quad U_2 \\
\quad\downarrow \\
\quad\vdots \\
\quad\downarrow \\
\quad U_n = \text{Spec } (L)
\end{array}
\tag{2.1}
$$

in which each morphism f_i is an elementary fibration. By lemma 1 again, it suffices to prove the theorem for $X \otimes L/L$, and for this it suffices, by lemma 3, to prove it for a good neighborhood U/L. By the exact sequence (1.4), it suffices to prove the theorem for each step U_i/U_{i+1} individually.

This completes the reduction to the case of an elementary fibration. By lemma 2, part (4) we may further reduce to the case $S = \text{Spec } (K)$. Again passing to a finite extension L/K, which is allowable by lemma 1, we may assume that our elementary fibration $X/K\,(= (C-D)/K)$ has a K-rational point x_0 and that the divisor D of points at infinity consists of a finite set of distinct K rational points of C. We must show that the prime-to-p-part ($p = \textit{char } (K)$) of the group of Galois coinvariants

$$(\pi_1 (X \otimes \bar{K})^{ab})_{\text{Gal } (\bar{K}/K)}$$

is *finite.*

For this, we must recall the explicit description of the prime-to-p part of $\pi_1(X \otimes \overline{K})^{ab}$ as the Tate module of a generalized Jacobian. Let J denote the Jacobian $Pic^0_{C/K}$, and let J_D denote the generalized Jacobian of C/K with respect to the modulus D. Thus J_D is a smooth commutative group-scheme over K which represents the functor on $\{\text{schemes}/K\}$

(2.2)
$$W \longrightarrow \left\{ \begin{array}{l} \text{the group of } W\text{-isomorphism classes of pairs } (\mathscr{L}, \varepsilon) \text{ consisting} \\ \text{of an invertible sheaf } \mathscr{L} \text{ on } C \underset{K}{\times} W \text{ which is fibre-by-fibre of} \\ \text{degree zero, together with a trivialization } \varepsilon \text{ of the restriction} \\ \text{of } \mathscr{L} \text{ to } D \times W. \end{array} \right.$$

"Forgetting ε" defines a natural map $J_D \to J$, which makes J_D an extension of J by a $\#(D) - 1$ dimensional split torus:

(2.3)
$$0 \to (\mathbf{G}_m)^{\#(D)}/\mathbf{G}_m \to J_D \to J \to 0\,.$$

Kummer theory (cf. SGA 4, Exp. XVIII, 1.6 for a "modern" account) furnishes a canonical isomorphism between the prime-to-p part of $\pi_1(X \otimes \overline{K})^{ab}$ and the prime-to-p Tate module of J_D; for any finite abelian group G killed by an integer N prime to the characteristic p of K, it gives a canonical isomorphism

(2.4)
$$H^1_{et}(X \otimes \overline{K}, G) \xrightarrow{\sim} \mathrm{Hom}\,(J_D(\overline{K}))_N, G)$$

where $(J_D(\overline{K}))_N$ is the "abstract" subgroup of points of order N in $J_D(\overline{K})$. In terms of the prime-to-p Tate module

(2.5)
$$\begin{aligned} T_{\text{not } p}(J_D(\overline{K})) &\overset{\text{dfn}}{=} \varprojlim_{P \nmid N} (J_D(\overline{K}))_N \\ &\simeq \prod_{l \neq p} T_l(J_D(\overline{K}))\,, \end{aligned}$$

we can rewrite this

(2.6)
$$\mathrm{Hom}\,(\pi_1(X \otimes \overline{K})^{ab}, G) \xrightarrow{\sim} \mathrm{Hom}\,(T_{\text{not } p}(J_D(\overline{K}), G)\,,$$

whence finally a canonical isomorphism

(2.7)
$$\pi_1(X \otimes \overline{K})^{ab} \xrightarrow{\sim} T_{\text{not } p}(J_D(\overline{K})) \times (\text{a pro-}p\text{-}group).$$

Thus we are reduced to showing the finiteness of the group

$$(T_{\text{not } p}(J_D(\overline{K})))_{\mathrm{Gal}(\bar{K}/K)}\,.$$

The exact sequence (2.3)

$$0 \to (\mathbf{G}_m)^{\#(D)-1} \to J_D \to J \to 0$$

gives an exact sequence of $\overline{K}$-valued points

$$0 \to \mathbf{G}_m(\overline{K})^{\#(D)-1} \to J_D(\overline{K}) \to J(\overline{K}) \to 0$$

Applying the snake lemma to the endomorphism "multiplication by N" of this exact sequence, and passing to the inverse limit over N's prime to p, we get a short exact sequence of prime-to-p Tate modules

$$(2.8)\quad 0 \to T_{\text{not } p}(\mathbf{G}_m(\overline{K}))^{\#(D)-1} \to T_{\text{not } p}(J_D(\overline{K})) \to T_{\text{not } p}(J(\overline{K})) \to 0\,.$$

Because formation of Gal $(\overline{K}/K)$-coinvariants is right-exact, we are reduced to showing separately the finiteness of the groups

$$(T_{\text{not } p}(\mathbf{G}_m(\overline{K})))_{\text{Gal}(\bar{K}/K)}\,, \qquad (T_{\text{not } p}(J(\overline{K})))_{\text{Gal}(\bar{K}/K)}\,.$$

In fact, these groups are finite even if we replace $T_{\text{not } p}$ by the entire Tate module $T = T_p \times T_{\text{not } p}$.

THEOREM 1 (bis). *Let K be an absolutely finitely generated field, and A/K an abelian variety. The groups*

$$(T(\mathbf{G}_m(\overline{K}))_{\text{Gal}(\bar{K}/K)}\,, \qquad T(A(\overline{K}))_{\text{Gal}(\bar{K}/K)}$$

are finite.

Proof. We will reduce to the case when K is finite. Because K is absolutely finitely generated, it is standard that we can find an integrally closed sub-ring R of K, with fraction K, which is finitely generated as a $\mathbf{Z}$-algebra, together with an abelian scheme $\mathbf{A}$ over R whose generic fibre $\mathbf{A} \underset{R}{\otimes} K$ is A. If K has characteristic $p > 0$, we may further suppose that geometric fibres of $\mathbf{A}/R$ have constant p-rank (if $g = \dim \mathbf{A}/R$, simply localize on R until the rank of the g'th iterate of the p-linear Hasse-Witt operation on $H^1(\mathbf{A}, \mathcal{O}_A)$ is constant).

Suppose first that K has characteristic $p > 0$. Then the Gal $(\overline{K}/K)$ representations $T(G_m(\overline{K}))$ and $T(A(\overline{K}))$ are unramified over Spec (R), i.e. they are actually representations of the fundamental group $\pi_1(\text{Spec}(R), \bar{\eta})$, viewed as a quotient of Gal $(\overline{K}/K)$.

Let $\mathfrak{p}$ be a maximal ideal of R, i.e. a closed point of Spec (R), $\mathbf{F}_\mathfrak{p}$ its residue field, $\bar{\mathbf{F}}_\mathfrak{p}$ an algebraic closure of $\mathbf{F}_\mathfrak{p}$, and $\bar{\mathfrak{p}}$ the corresponding geometric point of Spec (R) (namely $R \to R/\mathfrak{p} = \mathbf{F}_\mathfrak{p} \hookrightarrow \bar{\mathbf{F}}_\mathfrak{p}$). Pick a "chemin" from $\mathfrak{p}$ to the geometric generic point $\bar{\eta}$ (which is $R \hookrightarrow K \hookrightarrow K$), i.e. letting R denote the integral closure of R in $\overline{K}$, pick a homomorphism $\overline{R} \to \bar{\mathbf{F}}_\mathfrak{p}$ which extends $\bar{\mathfrak{p}}$. Then we get isomorphisms of $\hat{\mathbf{Z}}$-modules

$$T\left(\mathbf{A}\left(\bar{\mathbf{F}}_\mathfrak{p}\right)\right) \xleftarrow[\substack{\text{chosen chemin} \\ \overline{R} \to \bar{\mathbf{F}}_\mathfrak{p}}]{\sim} T\left(\mathbf{A}\left(\overline{R}\right)\right) \xrightarrow[\overline{R} \hookrightarrow \overline{K}]{\sim} T\left(A\left(\overline{K}\right)\right)$$

which is Gal $(\bar{\mathbf{F}}_\mathfrak{p}/\mathbf{F}_\mathfrak{p})$ equivariant when we make Gal $(\bar{\mathbf{F}}_\mathfrak{p}/\mathbf{F}_\mathfrak{p})$ operate on $T\left(A\left(\overline{K}\right)\right)$ via the composite

$$\mathrm{Gal}\left(\bar{\mathbf{F}}_\mathfrak{p}/\mathbf{F}_\mathfrak{p}\right) = \pi_1\left(\mathrm{Spec}\left(\mathbf{F}_\mathfrak{p}\right); \bar{\mathfrak{p}}\right) \xrightarrow{\text{“p”}}$$

$$\pi_1\left(\mathrm{Spec}\left(R\right), \bar{\mathfrak{p}}\right) \xrightarrow[\sim]{\text{“chemin”}} \pi_1\left(\mathrm{Spec}\left(R\right), \bar{\eta}\right)$$

Passing to coinvariants now yields a diagram

$$\begin{array}{ccc}
\left(T\left(\mathbf{A}\left(\bar{\mathbf{F}}_\mathfrak{p}\right)\right)\right)_{\mathrm{Gal}\left(\bar{\mathbf{F}}_\mathfrak{p}/\mathbf{F}_\mathfrak{p}\right)} & \simeq & \left(T\left(A\left(\overline{K}\right)\right)\right)_{\mathrm{Gal}\left(\bar{\mathbf{F}}_\mathfrak{p}/\mathbf{F}_\mathfrak{p}\right)} \\
 & & \downarrow \\
 & & \left(T\left(A\left(\overline{K}\right)\right)\right)_{\pi_1\left(\mathrm{Spec}\left(R\right), \bar{\eta}\right)} \\
 & & \| \\
 & & T\left(A\left(\overline{K}\right)\right)_{\mathrm{Gal}\left(\overline{K}/K\right)},
\end{array}$$

in which the vertical arrow is trivially surjective (because Gal $(\bar{\mathbf{F}}_\mathfrak{p}/\mathbf{F}_\mathfrak{p})$ operates through its image in $\pi_1\left(\mathrm{Spec}\left(R\right), \bar{\eta}\right)$). Similarly for $\mathbf{G}_m$.

When K is of characteristic zero, and A/K has been "spread out" to an abelian scheme $\mathbf{A}/R$, we argue as follows. Fix a closed point $\mathfrak{p}$ of Spec (R). For each prime $l \neq p = \mathrm{char}\,(\mathbf{F}_\mathfrak{p})$, the l-adic Tate module $T_l\left(A\left(\overline{K}\right)\right)$ is unramified over Spec $(R\,[1/l])$ and the above specialization argument gives a surjection, for each $l \neq p$,

$$T_l\left(\mathbf{A}\left(\bar{\mathbf{F}}_\mathfrak{p}\right)\right)_{\mathrm{Gal}\left(\bar{\mathbf{F}}_\mathfrak{p}/\mathbf{F}_\mathfrak{p}\right)} \twoheadrightarrow T_l\left(A\left(\overline{K}\right)\right)_{\mathrm{Gal}\left(\overline{K}/K\right)}.$$

Therefore the prime-to-p part of the order of $(T(A(\bar{K})))_{\mathrm{Gal}(\bar{K}/K)}$ divides the order of $(T(\mathbf{A}(\bar{\mathbf{F}}_p)))_{\mathrm{Gal}(\bar{\mathbf{F}}_p/\mathbf{F}_p)}$.

Now choose a second closed point λ of Spec (R), with residue characteristic $l \neq p$. [This is possible because, K being a characteristic zero, Spec (R) necessarily dominates Spec $(\mathbf{Z})$, and hence by Chevalley's theorem all but finitely many primes occur as residue characteristics of closed points of Spec (R)]. Then the p-part (and indeed the prime to-l part) of the order of $(T(A(\bar{K})))_{\mathrm{Gal}(\bar{K}/K)}$ divides the order of $(T(\mathbf{A}(\bar{\mathbf{F}}_\lambda)))_{\mathrm{Gal}(\bar{\mathbf{F}}_\lambda/\mathbf{F}_\lambda)}$. Similarly for $\mathbf{G}_m$.

Thus we have reduced theorem 1 (bis) to the case of finite fields, where it is "classical". Explicitely, the result is

THEOREM 1 (ter). *Let k be a finite field, $q = \#k$, and A an abelian variety over k. Then we have the explicit formulas*

$$\begin{cases} \#(T(A(\bar{k})))_{\mathrm{Gal}(\bar{k}/k)} = \#A(k) \\ \#(T(\mathbf{G}_m(\bar{k})))_{\mathrm{Gal}(\bar{k}/k)} = \#\mathbf{G}_m(k) = q - 1 . \end{cases}$$

Proof. Let $F \in \mathrm{Gal}(\bar{k}/k)$ denote the arithmetic Frobenius automorphism of $\bar{k}/k$ (i.e. $F(x) = x^q$) which is a topological generator of $\mathrm{Gal}(\bar{k}/k)$. In any $\mathrm{Gal}(\bar{k}/k)$-module T, the coinvariants are simply the cokernel of $1 - F$:

$$T/(1-F)\,T \xrightarrow{\sim} (T)_{\mathrm{Gal}(\bar{k}/k)} .$$

In the case $T = T(\mathbf{G}_m(\bar{k}))$, T is a free module of rank one over $\prod_{l \neq p} \mathbf{Z}_l$ on which F operates as multiplication by q, whence the asserted result. In the case $T = T(A(\bar{k}))$, we have $T = \prod_l T_l(A(\bar{k}))$, the product extended to all primes l. Each module $T_l(A(\bar{k}))$ is a free $\mathbf{Z}_l$-module of finite rank (2 dim $\mathbf{A}$ for $l \neq p$, the "p-rank" of A for $l = p$). Because $\#A(k)$ is non-zero, it is enough to prove that, for each l, we have an equality of l-adic ordinals:

$$\mathrm{ord}_l(\#(T_l(A(\bar{k}))/(1-F)\,T_l(A(\bar{k})))) = \mathrm{ord}_l(\#A(k)) .$$

By the theory of elementary divisors, we have

$$\mathrm{ord}_l(\#(T_l/(1-F)\,T_l)) = \mathrm{ord}_l(\det(1-F \mid T_l)) .$$

Now for $l \neq p$, we have Weil's celebrated equality ([16], thm. 36)

$$\det(1 - F \mid T_l(A(\bar{k}))) = \#A(k) \qquad (l \neq p) .$$

For $l = p$, we have (cf. [13]) only the weaker, but adequate

$$\det\left(1 - F \mid T_p\left(A\left(\bar{k}\right)\right)\right) = \left(\#A\left(k\right)\right) \times (\text{a } p\text{-adic unit}) . \qquad \text{QED}$$

Remarks. (1) Given an abelian variety A over any field K, Kummer theory and duality lead to a canonical isomorphism

$$\pi_1\left(A \otimes \overline{K}\right) \xrightarrow{\sim} T\left(A\left(\overline{K}\right)\right) .$$

Because abelian varities have rational points (e.g. their origins) we have canonically

$$\mathrm{Ker}\left(A/K\right) \xrightarrow{\sim} \left(T\left(A\left(\overline{K}\right)\right)\right)_{\mathrm{Gal}\left(\overline{K}/K\right)} .$$

From this point of view, Theorem 1 (bis) is simply the abelian variety case of Theorem 1 with the added information that even the p-part is finite.

Now consider the special case when $K = k$ is a *finite* field. Then Theorem 1 (ter) gives us

$$\#\mathrm{Ker}\left(A/k\right) = \#A\left(k\right) .$$

In fact, there is a canonical isomorphism of groups

$$\mathrm{Ker}\left(A/k\right) \xrightarrow{\sim} A\left(k\right) .$$

To see this recall the interpretation of $\mathrm{Ker}\left(A/k\right)$ as the inverse limit of the galois groups of connected finite etale A-schemes $\mathbf{E}/A$ which are galois over A with abelian galois group, and completely decomposed over the origin (cf. 1.3). The Lang isogeny

$$\begin{array}{l} A \\ \downarrow \quad 1-F \\ A \end{array} \qquad (F \text{ the Frobenius endomorphism of } A/k)$$

is precisely such a covering, with structural group $A\left(k\right)$. Therefore we have a surjective homomorphism

$$\mathrm{Ker}\left(A/k\right) \twoheadrightarrow A\left(k\right)$$

which is the required isomorphism (since source and target have the same cardinality !).

(2) The $\mathbf{G}_m$ case of Theorem 1 (bis) could have been handled directly by remarking that for any field K, the cardinality (as a supernatural number) of the group of coinvariants $\left(T\left(\mathbf{G}_m\left(\overline{K}\right)\right)\right)_{\mathrm{Gal}\left(\overline{K}/K\right)}$ is equal to the number of roots of unity in the field K. But how, in fact, do we know that this number is finite for an

absolutely finitely generated field ? The proof by specialization is pretty much the simplest one ! Another approach, after "fattening" K into its finitely generated sub-ring R, is to prove the stronger assertion, in Mordell-Weil style, that the group $\mathbf{G}_m(R) = R^\times$ of units in such an absolutely finitely ring is a finitely generated abelian group.

(3) In the case of an abelian variety A over an absolutely finitely generated field K, the multiplicative upper bounds we get for $\# T(A(\overline{K}))_{\mathrm{Gal}(\overline{K}/K)}$ (essentially $\# \mathbf{A}(k)$ whenever we specialize to a finite field k, with the proviso that we must ignore the p-parts when it's a mixed-characteristic specialization) are *exactly the same bounds* usually used to control the size of the torsion subgroup of $A(K)$. There is a simple galois-theoretic interpretation of the group $(T(A(\overline{K})))_{\mathrm{Gal}(\overline{K}/K)}$, or at least its prime-to-p part, in terms of "*twisted-rational*" *torsion points*, which is perhaps worth pointing out. Thus let $A^\vee$ denote the dual abelian variety to A, p the characteristic of K, $\mathrm{Tors}_{\mathrm{not}\ p} A^\vee(\overline{K})$ the $\mathrm{Gal}(\overline{K}/K)$-module of all torsion points of order prime-to-p on $A^\vee$ and

$$(\mathrm{Tors}_{\mathrm{not}\ p} A^\vee(\overline{K}))(-1)$$

the $\mathrm{Gal}(\overline{K}/K)$-module obtained from this one by tensoring with the *inverse* of the cyclotomic character χ of $\mathrm{Gal}(\overline{K}/K)$. Alternately, we could describe this last module as the $\mathrm{Gal}(\overline{K}/K)$-module

$$\mathrm{Hom}(T(\mathbf{G}_m(\overline{K})), \mathrm{Tors}_{\mathrm{not}\ p} A^\vee(\overline{K})).$$

The e_N-pairings define a $\mathrm{Gal}(\overline{K}/K)$-equivariant pairing

$$T_{\mathrm{not}\ p}(A(\overline{K})) \times (\mathrm{Tors}_{\mathrm{not}\ p} A^\vee(\overline{K}))(-1) \to \mathbf{Q}/\mathbf{Z}.$$

which makes the compact abelian group $T_{\mathrm{not}\ p}$ and the discrete abelian group $(\mathrm{Tors}_{\mathrm{not}\ p})(-1)$ the Pontryagin duals of each other. Thus we obtain a perfect pairing

$$T_{\mathrm{not}\ p}(A(\overline{K}))_{\mathrm{Gal}(K/K)} \times ((\mathrm{Tors}_{\mathrm{not}\ p}(A^\vee(\overline{K}))(-1))^{\mathrm{Gal}(\overline{K}/K)} \to \mathbf{Q}/\mathbf{Z}.$$

The group $((\mathrm{Tors}_{\mathrm{not}\ p} A^\vee(\overline{K}))(-1))^{\mathrm{Gal}(\overline{K}/K)}$ is none other than the group $(\mathrm{Tors}_{\mathrm{not}\ p} A^\vee(\overline{K}))^\chi$ of all prime-to-p ($p = \mathrm{char}(K)$) torsion points in $A^\vee(\overline{K})$ which transform under $\mathrm{Gal}(\overline{K}/K)$ by the cyclotomic character χ. Thus we obtain

SCHOLIE. *Over any field K of characteristic zero, the Pontryagin dual of* $\mathrm{Ker}(A/K)$ *is the group* $(\mathrm{Tors}\ A^\vee(\overline{K}))^\chi$.

(4) The same reasoning as in (3) above, if carried "scheme-theoretically", leads to a concrete interpretation of the Pontryagin dual of the entire group $T(A(\overline{K}))_{\mathrm{Gal}(\bar{K}/K)}$ "in terms of" μ-type subgroupschemes" of $A^\vee$;

SCHOLIE. *Over any field K, the Pontryagin dual of the compact group $T(A(\overline{K}))_{\mathrm{Gal}(\bar{K}/K)}$ is the discrete group*

$$\varinjlim_{N} \mathrm{Hom}_{K-gp}(\mu_N, A^\vee),$$

where Hom *is taken in the category of K-groupschemes, and the transition maps are those induced by* $\mu_{NM} \xrightarrow{\text{“}M\text{”}} \mu_N$.

Still by Theorem 1 (bis), this group is *finite* for an absolutely finitely generated field K.

For any given curve X over, say, $\mathbf{Q}$, it is an interesting problem to compute the maximal μ-type subgroup of its Jacobian. For example, let p be an odd prime, and consider the modular curves $X_0(p)$ and $X_1(p)$. Then $X_1(p)$ is a ramified covering of $X_0(p)$, cyclic of degree $(p-1)/2$, which is completely split over the rational cusp at infinity. Let

$$N = \text{numerator of } (p-1)/12.$$

The unique intermediate covering of $X_0(p)$ of degree N is unramified; it is called the Shimura covering. According to Mazur [20], the corresponding μ_N inside $J_0(p)$ is the maximal μ-type subgroup of $J_0(p)$ over $\mathbf{Q}$. Therefore we have

$$\mathrm{Ker}(X_0(p)/\mathbf{Q}) \simeq \mathbf{Z}/N\,\mathbf{Z}$$

with the Shimura covering as the maximal abelian unramified geometric covering of $X_0(p)$ defined over $\mathbf{Q}$ in which the rational cusp at infinity splits completely.

On the other hand, we may extend $X_0(p)$ to a normal scheme $\mathbf{X}_0(p)$ over $\mathbf{Z}$. At the prime p, the covering $X_1(p)$ (and hence also the Shimura covering) becomes *completely* ramified over one of the two components of $\mathbf{X}_0(p) \otimes \mathbf{F}_p$. Therefore

$$\mathrm{Ker}(\mathbf{X}_0(p)/\mathbf{Z}) = 0,$$

so that Spec $(\mathbf{Z})$ being simply connected, we have

$$\pi_1(\mathbf{X}_0(p)^{ab}) = 0.$$

(5) Consider the case when K is a finitely generated extension of an algebraically closed constant field K_0, and suppose that A/K is an abelian variety over K which has *no fixed part* relative to K_0. Because K_0, and hence K, contains all roots of unity, the cyclotomic of character of Gal $(\overline{K}/K)$ is trivial. Therefore the Pontryagin dual of $T_{\text{not } p}(A(\overline{K}))_{\text{Gal}(\overline{K}/K)}$ is simply the group of K-rational torsion points of prime-to-p order on $A^\vee$. By the *Mordell-Weil theorem* in the function field case (cf. [4], V, thm. 2) the group $A(K)$ of all K-rational points on A is finitely generated so in particular its torsion subgroup is finite. Therefore the group $T_{\text{not } p}(A(\overline{K}))_{\text{Gal}(\bar{K}/K)}$ is also finite in this "geometric" case.

Whether or not the p-part $(T_p(A(\overline{K}))_{\text{Gal}(\bar{K}/K)}$ is also finite under these assumptions is unknown in general. When A/K is a non-constant elliptic curve, this finiteness can be established by considering the ramification properties of the "V-divisible group" of A near a supersingular point on the moduli scheme. However, the general case would seem to require new ideas.

(6) Theorem 1 (bis) implies the finiteness of the group $(\text{Tors } A^\vee(\overline{K}))^\chi$ when K is a finitely generated extension of $\mathbf{Q}$, e.g. a number field. Let $K(\mu)$ be the field obtained by adjoining to K all roots of unity. We clearly have the inclusion

$$(\text{Tors } A^\vee(\overline{K}))^\chi \subset \text{Tors } A^\vee(K(\mu)).$$

This leads to the conjecture:

For any abelian variety A over a number field K, the group Tors $A(K(\mu))$ *of $K(\mu)$-rational torsion points on A is finite.*

When A is an elliptic curve without complex multiplication, this is an immediate consequence of Serre's theorem that the Galois group of the torsion points is open in $\prod GL_2(\mathbf{Z}_p)$.

For an arbitrary abelian variety, Imai [Im] shows that the group of torsion points in $K(\mu_{p^\infty})$ is finite for a fixed prime p. We shall prove below that the conjecture is true when A admits complex multiplication. This was extended to a proof of the conjecture in general by Ribet, cf. the appendix.

First we need a lemma.

LEMMA. *Let k be a number field. There exists a positive integer m such that, if F is any finite extension of k ramified at only one prime number p, and contained in some cyclotomic field, then*

$$F \subset k(\mu_{p^\infty}, \mu_m).$$

Proof. There exists a finite set of primes S such that

$$\mathrm{Gal}\,(k(\mu)/k) = G_S \times \prod_{l \notin S} G_l$$

where $G_l \approx \mathbf{Z}_l^*$, and G_S contains a subgroup

$$H_S = \prod_{l \in S} H_l$$

where H_l is open in $\mathbf{Z}_l^*$. Without loss of generality, we may assume that S contains p and all primes which ramify in k. If $l \notin S$, then the inertia group at l contains G_l (embedded as a component of the product). If $l \in S$, then the inertia group at l contains a subgroup H_l' open in H_l. Consequently the subgroup of the Galois group generated by all the inertia groups at primes $l \neq p$ contains

$$\prod_{\substack{l \in S \\ l \neq p}} H_l' \times \prod_{l \notin S} G_l .$$

This proves the lemma.

Now let A be an abelian variety defined over a number field k, and with complex multiplication. Suppose that $A_{\mathrm{tor}}(k(\mu))$ is infinite, so contains points of arbitrarily high order. We consider separately the two cases when there is a point of prime order p rational over $k(\mu)$ for arbitrarily large p, or when for some fixed p, there is a point of order p^n with large n.

After extending k by a finite extension if necessary, we may assume without loss of generality that A has good reduction at every prime of k. Let $k' = k(\mu_m)$ where m is chosen as in the lemma. Let x be a point on A of order a power of the prime p. Then $k(x)$ is ramified only at p, and it follows that

$$k'(x) \subset k'(\mu_{p^\infty}) .$$

Let K be the field of complex multiplication, which we may also assume contained in k'. Furthermore, after an isogeny of A if necessary, we may assume that the ring of algebraic integers in K acts on A via an embedding

$$\iota : \mathfrak{o}_K \to \mathrm{End}\,(A) .$$

Let

$$\mathfrak{p}\mathfrak{o}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$$

be the prime ideal decomposition of p in K, and let $\mathfrak{p}_1 = \mathfrak{p}$, say.

Suppose that x has order p, and that p is large, so p is unramified in k'. By projection on the $\mathfrak{p}$-component, we may assume that x is a point of order $\mathfrak{p}$, that is $\iota(\mathfrak{p})\, x = 0$. If $r \geqq 2$, and $\mathfrak{P}'$ is a prime ideal of k' dividing one of $\mathfrak{p}_2, \ldots, \mathfrak{p}_r$, then

$\mathfrak{P}'$ is unramified in $k'(x)$. But since p is unramified in k', then $k'(\mu_{p^\infty})$ is totally ramified above every prime dividing p in k'. Therefore $r = 1$ and p remains prime in k'.

In that case, $k'(x) = k'(A_p)$ and A_p is a cyclic module over $\mathfrak{o}_K$, or also a vector space of dimension 1 over $\mathfrak{o}_K/p\mathfrak{o}_K$. Furthermore, $\mathrm{Gal}(k'(A_p)/k')$ can be identified with a subgroup of $(\mathfrak{o}_K/p\mathfrak{o}_K)^*$, which has order $\mathbf{N}\mathfrak{p} - 1$, and in particular is prime to p. By a theorem of Ribet [Ri], we have

$$|\mathrm{Gal}(k'(A_p)/k)| \gg p^2,$$

where the sign $\gg$ means that the left hand side is greater than some positive constant times the right hand side. However, the prime-to-p part of $\mathrm{Gal}(k(\mu_{p^\infty})/k)$ has order $\ll p$. This contradiction proves the theorem in the present case.

Consider finally the case when there is a point x_n of order p^n with p fixed but n arbitrarily large. Without loss of generality, we may assume that μ_p is contained in k'. We shall prove again that $r = 1$. For some prime $\mathfrak{p} = \mathfrak{p}_1$ dividing p in K, the point x_n will have a $\mathfrak{p}$-component of large p-power order, and hence without loss of generality, we may assume that all the points x_n lie in $A[\mathfrak{p}^\infty]$ (the union of all the kernels of $\iota(\mathfrak{p}^\nu)$ for $\nu \to \infty$). In particular, the degrees $[k'(x_n): k']$ contain arbitrarily large powers of p, whence the fields $k'(x_n)$ contain arbitrarily large extensions $k'(\mu_{p^\nu})$. If $r \geqq 2$ and $\mathfrak{P}'$ is any prime ideal of k' dividing some prime $\mathfrak{p}_2, \ldots, \mathfrak{p}_r$, then $\mathfrak{P}'$ is unramified in $k'(x_n)$. But the ramification indices at all primes dividing p in k' tend to infinity as n tends to infinity. Hence again $r = 1$.

Now suppose that x_n has order $\mathfrak{p}^n$, meaning that $\mathfrak{p}^n$ is the kernel of the map

$$\alpha \mapsto \iota(\alpha)\, x_n .$$

We shall prove that $k'(x_n) = k'(A[\mathfrak{p}^n])$. We have an isomorphism

$$\mathfrak{o}/\mathfrak{p}^n \approx \iota(\mathfrak{o})\, x_n .$$

On the other hand, $A[\mathfrak{p}^n]$ is cyclic module over $\mathfrak{o}/\mathfrak{p}^n$, generated by an element z, so that $x_n = \iota(\alpha) \cdot z$ for some α. Then α must be a unit in the local ring of $\mathfrak{o}$ at $\mathfrak{p}$, whence in fact

$$\iota(\mathfrak{o})\, x = A[\mathfrak{p}^n] .$$

This proves that $k'(x_n) = k'(A[\mathfrak{p}^n])$.

Using arbitrarily large n, we conclude that $k'(A[\mathfrak{p}^\infty])$ is contained in $k'(\mu_{p^\infty})$. But according to Kubota [Ku], the Galois group $\mathrm{Gal}(k'(A[\mathfrak{p}^\infty])/k')$ is a Lie group of dimension $\geqq 2$. Since the Galois group of the p-primary roots of unity is a Lie group of dimension 1, we have a contradiction, which concludes the proof.

III. A VARIANT

Let us agree to call a scheme S *accessible* if there exists an absolutely finitely generated field K for which the set $S(K)$ of K-valued points of S is non-empty. Thus for example, if K is an absolutely finitely generated field, then for *any* subring $R \subset K$, Spec (R) is accessible (by the K-valued point $R \hookrightarrow K$); also any subring R' of the power-series ring $K[[X_1, ..., ...]]$ over K in any number of variables has Spec (R') accessible

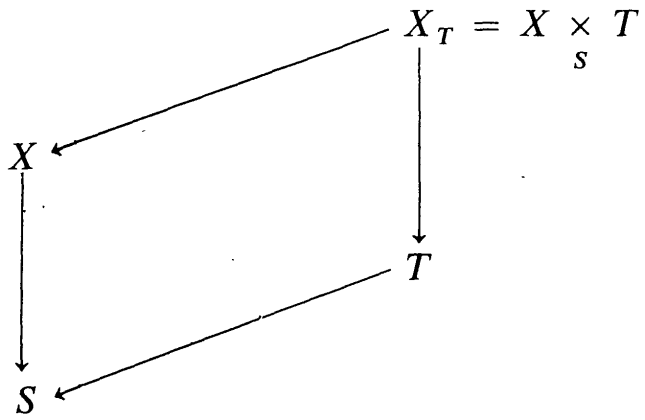
$$(\text{by } R' \hookrightarrow K[[X_1, ...]] \xrightarrow{X \to 0} K).$$

On the other hand, the spectrum of a field F is accessible if and only if F is absolutely finitely generated.

THEOREM 2. *Let S be a connected, locally noetherian scheme which is accessible. Let X/S be a proper and smooth S-scheme with geometrically connected fibres. Then the group* Ker (X/S) *is finite.*

Proof. We begin by reducing to the case when S is a finitely generated field. In view of the accessibility of S, this reduction results from the following simple lemma applied with $T = \text{Spec}(K)$.

LEMMA 4. *Let X/S be proper and smooth with geometrically connected fibres over a connected locally noetherian scheme S. Given a connected locally noetherian S-scheme T, denote by X_T/T the inverse image of X/S on T, i.e. form the cartesian diagram*



The natural map (cf. 1.5)

$$\mathrm{Ker}\,(X_T/T) \to \mathrm{Ker}\,(X/S)$$

is surjective.

Proof. Let t be a geometric point of T, s the image geometric point of S, and x a geometric point on the fibre X_s. The homotopy exact sequences (SGA I, Exp X, 1.4) for X/S and X_T/T sit in a commutative diagram

$$\begin{array}{ccccccc}
\pi_1(X_s, x) & \longrightarrow & \pi_1(X_T, x) & \longrightarrow & \pi_1(T, t) & \longrightarrow & 0 \\
\| & & \downarrow & & \downarrow & & \\
\pi_1(X_s, x) & \longrightarrow & \pi_1(X, x) & \longrightarrow & \pi_1(S, s) & \longrightarrow & 0
\end{array}$$

Passing to the abelianizations yields the commutative diagram with exact rows

$$\begin{array}{ccccccc}
\pi_1(X_s)^{ab} & \longrightarrow & \pi_1(X_T)^{ab} & \longrightarrow & \pi_1(T)^{ab} & \longrightarrow & 0 \\
\| & & \downarrow & & \downarrow & & \\
\pi_1(X_s)^{ab} & \longrightarrow & \pi_1(X)^{ab} & \longrightarrow & \pi_1(S)^{ab} & \longrightarrow & 0
\end{array}$$

whence we find

$$\pi_1(X_s)^{ab} \twoheadrightarrow \begin{array}{l} \mathrm{Ker}\,(X_T/T) = \text{image of } \pi_1(X_s)^{ab} \text{ in } \pi_1(X_T)^{ab}. \\ \downarrow \\ \mathrm{Ker}\,(X/S) = \text{image of } \pi_1(X_s)^{ab} \text{ in } \pi_1(X)^{ab}. \end{array}$$

QED

Thus we are reduced to proving the finiteness of $\mathrm{Ker}\,(X/K)$ when K is an absolutely finitely generated field, and X/K is proper, smooth, and geometrically connected. We have already proven this finiteness theorem when X/K is an abelian variety (cf. Remark (1) above). We will reduce to this case by making use of the theory of the Picard and Albanese varieties.

At the expense of replacing K by a finite extension, we may assume that X has a K-rational point x_0. The Picard scheme $Pic_{X/K}$ is then a commutative group-scheme locally of finite type over K, which represents the functor on $\{\text{Schemes}/K\}$

$$W \to \left\{ \begin{array}{l} \text{the group of } W\text{-isomorphism classes of pairs } (\mathscr{L}, \varepsilon) \text{ consisting} \\ \text{of an invertible sheaf } \mathscr{L} \text{ on } X \underset{K}{\times} W \text{ together with a} \\ \text{trivialization } \varepsilon \text{ of the restriction } \mathscr{L} \text{ to } \{x_0\} \underset{K}{\times} W \end{array} \right.$$

The subgroup-scheme $Pic^{\tau}_{X/K}$ of $Pic_{X/K}$ classifies those $(\mathscr{L}, \varepsilon)$ whose underlying $\mathscr{L}$ becomes τ-equivariant to zero when restricted to every geometric fibre of $X \times W/W$ (i.e. for each geometric point w of W, some multiple of $\mathscr{L} \mid X \times w$ is algebraically equivalent to zero). The identity component $Pic^{0}_{X/K}$ of $Pic_{X/K}$ classifies those $(\mathscr{L}, \varepsilon)$ whose $\mathscr{L}$ becomes algebraically equivalent to zero on each geometric fibre $X \times W/W$. The Picard *variety* $Pic^{0,\,\mathrm{red}}_{X/K}$ is an abelian variety over K, and it sits in an *f.p.p.f.* short exact sequence of commutative group schemes

$$0 \to Pic^{0,\,\mathrm{red}}_{X/K} \to Pic^{\tau}_{X/K} \to C \to 0 \tag{3.1}$$

in which the cokernel C is a finite flat group-scheme over K. This cokernel C should be thought of as the "scheme theoretic" torsion in the Neron-Severi group.

We denote by $\mathrm{Alb}_{X/K}$ the Albanese variety of X/K, *defined* to be the dual abelian variety to the Picard variety $Pic^{0,\,\mathrm{red}}_{X/K}$. We now recall the expression of $\pi_1 (X \otimes \overline{K})^{ab}$ in terms of the Tate module of the Albanese, and a finite "error term" involving the Cartier dual $C^{\vee}$ of C.

LEMMA 5. *Let K be a field, and X/K a proper, smooth and geometrically connected K-scheme which admits a K-rational point. Then there is a canonical short exact sequence of* $\mathrm{Gal}\,(\overline{K}/K)$*-modules*

$$0 \to C^{\vee}(\overline{K}) \to \pi_1 (X \otimes \overline{K})^{ab} \to T\left(\mathrm{Alb}_{X/K}(\overline{K})\right) \to 0\,. \tag{3.2}$$

Proof. By Kummer and Artin-Schreier theory, we have for each integer $N \geqslant 1$ a canonical isomorphism

$$\begin{aligned} &\mathrm{Hom}\left(\pi_1 (X \otimes \overline{K})^{ab}, \mathbf{Z}/N\mathbf{Z}\right) \\ &= H^1_{et}(X \otimes \overline{K}, \mathbf{Z}/N\mathbf{Z}) \xrightarrow{\sim} \mathrm{Hom}\left(\mu_N, (Pic^{\tau}_{X/K}) \otimes \overline{K}\right). \end{aligned}$$

in which the last Hom is in the sense of $\overline{K}$-group-schemes. Applying the functor $X \mapsto \mathrm{Hom}\,(\mu_N, X)$ to the short exact sequence

$$0 \to Pic^{0,\,\mathrm{red}} \to Pic^{\tau} \to C \to 0$$

gives a short exact sequence

$$\begin{aligned} 0 \to \mathrm{Hom}\left(\mu_N, (Pic^{0,\,\mathrm{red}}) \otimes \overline{K}\right) \\ \to \mathrm{Hom}\left(\mu_N, (Pic^{\tau}) \otimes \overline{K}\right) \to \mathrm{Hom}\left(\mu_N, C \otimes \overline{K}\right) \to 0 \end{aligned} \tag{3.3}$$

(the final zero because over an algebraically closed field, the group $\mathrm{Ext}^1(\mu_N, A)$ vanishes for any abelian variety A, cf. the remark at the end of this section). We now "decode" its two end terms, using Cartier-Nishi duality for the first, and Cartier duality for the last.

The first is

$$\begin{aligned}\mathrm{Hom}\left(\mu_N, (Pic^{0,\mathrm{red}}) \otimes \overline{K}\right) &= \mathrm{Hom}\left(\mu_N, (Pic^{0,\mathrm{red}})_N \otimes \overline{K}\right)\\ &\quad \wr\downarrow \quad \text{Cartier-Nishi duality}\\ &\mathrm{Hom}\left((\mathrm{Alb}_{X/N})_N \otimes \overline{K}, \mathbf{Z}/N\mathbf{Z}\right)\\ &\quad \wr\downarrow \quad \text{evaluation on } \overline{K}\text{-points}\\ &\mathrm{Hom}\left((\mathrm{Alb}_{X/K}(\overline{K}))_N, \mathbf{Z}/N\mathbf{Z}\right)\\ &\quad \wr\downarrow\\ &\mathrm{Hom}\left(T(\mathrm{Alb}_{X/K}(\overline{K})), \mathbf{Z}/N\mathbf{Z}\right).\end{aligned}$$

The last is

$$\begin{array}{ccc}\mathrm{Hom}(\mu_N, C \otimes \overline{K}) & \xrightarrow[\text{Cartier duality}]{\sim} & \mathrm{Hom}(C^\vee \otimes \overline{K}, \mathbf{Z}/N\mathbf{Z})\\ & & \Big\downarrow\Big\wr \text{ évaluation}\\ & & \mathrm{Hom}(C^\vee(\overline{K}), \mathbf{Z}/N\mathbf{Z})\end{array}$$

"Substituting" into the exact sequence (3.2), we find a canonical short exact sequence

$$\begin{aligned}(3.4)\qquad 0 &\to \mathrm{Hom}\left(T(\mathrm{Alb}_{X/K}(\overline{K})), \mathbf{Z}/N\mathbf{Z}\right)\\ &\to \mathrm{Hom}\left(\pi_1(X \otimes \overline{K})^{ab}, \mathbf{Z}/N\mathbf{Z}\right) \to \mathrm{Hom}\left(C^\vee(\overline{K}), \mathbf{Z}/N\mathbf{Z}\right) \to 0\end{aligned}$$

Passing to the *direct* limit as N grows multiplicatively, we obtain a canonical short exact sequence

$$\begin{aligned}(3.5)\qquad 0 &\to \mathrm{Hom}\left(T(\mathrm{Alb}_X(\overline{K}), \mathbf{Q}/\mathbf{Z}\right)\\ &\to \mathrm{Hom}\left(\pi_1(X \otimes \overline{K})^{ab}, \mathbf{Q}/\mathbf{Z}\right) \to \mathrm{Hom}\left(C^\vee(\overline{K}), \mathbf{Q}/\mathbf{Z}\right) \to 0.\end{aligned}$$

Taking its Pontryagin dual, we find the required exact sequence (3.2). QED

To complete the reduction of Theorem 2 to the case of abelian varieties, we simply notice that the exact sequence of lemma 5 yields, upon passage to coinvariants, an exact sequence

$$(3.6) \qquad (C^\vee(\overline{K}))_{\mathrm{Gal}(\overline{K}/K)} \to \mathrm{Ker}\,(X/K) \to \mathrm{Ker}\,(\mathrm{Alb}_{X/K}/K) \to 0$$

whose first term, being a quotient of the finite group $C^\vee(\overline{K})$, is finite. QED

Remark. In the course of the proof of Lemma 5, we appealed to the "well-known" vanishing of $\mathrm{Ext}^1(\mu_N, A)$ over an algebraically closed field, for an abelian variety A and any integer $N > 1$. Here is a simple proof. It is enough to prove this vanishing when N is either prime to the characteristic p of K, or, in case $p > 0$, when $N = p$.

Suppose first N prime to p. Because the ground-field is algebraically closed, we have $\mu_N \simeq \mathbf{Z}/N\mathbf{Z}$, so it is equivalent to prove the vanishing of $\mathrm{Ext}^1(\mathbf{Z}/N\mathbf{Z}, A)$. We will prove that *this* group vanishes for every integer $N > 1$. Consider such an extension:

$$0 \to A \to E \to \mathbf{Z}/N\mathbf{Z} \to 0$$

Pass to $\overline{K}$-valued points

$$0 \to A(\overline{K}) \to E(\overline{K}) \to \mathbf{Z}/N\mathbf{Z} \to 0$$

and consider the endomorphism "multiplication by N". Because the group $A(\overline{K})$ is N-divisible, the snake lemma gives an exact sequence

$$0 \to A(\overline{K})_N \to E(\overline{K})_N \to \mathbf{Z}/N\mathbf{Z} \to 0$$

But a point in $E(\overline{K})_N$ which maps onto "1" $\in \mathbf{Z}/N\mathbf{Z}$ is precisely a splitting of our extension.

Next consider the case $N = p = \mathrm{char}\,(K)$. We give a proof due to Barry Mazur. Using the *f.p.p.f.* exact sequence

$$0 \to A_p \to A \to A \to 0\,.$$

to compute $\mathrm{Ext}(\mu_p, -)$, we obtain a short exact sequence

$$0 \to \mathrm{Hom}\,(\mu_p, A) \to \mathrm{Ext}^1(\mu_p, A_p) \to \mathrm{Ext}^1(\mu_p, A) \to 0$$

To prove that $\mathrm{Ext}^1(\mu_p, A) = 0$, we will show that the groups $\mathrm{Hom}\,(\mu_p, A)$ and $\mathrm{Ext}^1(\mu_p, A_p)$ are both finite, of the same order. Trivially, we have $\mathrm{Hom}\,(\mu_p, A) = \mathrm{Hom}\,(\mu_p, A_p)$. Because we are over an algebraically closed field, and A_p is killed by p, its toroidal biconnected-etale decomposition looks like

$$A_p \simeq (\mu_p)^a \times (\text{biconnected}) \times (\mathbf{Z}/p\mathbf{Z})^b; \qquad [\text{in fact } a = b]\,.$$

Only the μ p's in A_p can "interact" with μ_p. Thus we are reduced to showing that $\mathrm{Hom}\,(\mu_p, (\mu_p)^a)$ and $\mathrm{Ext}^1(\mu_p, (\mu_p)^a)$ are both finite of the same cardinality p^a.

By Cartier duality, it is equivalent to show that both Hom $(\mathbf{Z}/p\mathbf{Z}, \mathbf{Z}/p\mathbf{Z})$ and $\mathrm{Ext}^1(\mathbf{Z}/p\mathbf{Z}, \mathbf{Z}/p\mathbf{Z})$ have order p, and this is obvious (resolve the "first" $\mathbf{Z}/p\mathbf{Z}$ by

$$0 \to \mathbf{Z} \xrightarrow{p} \mathbf{Z} \to \mathbf{Z}/p\mathbf{Z} \to 0) .$$

For another proof in this case, cf. Oort, [10], 85.

IV. Absolute Finiteness theorems

Theorem 3. *Let $\mathcal{O}$ be the ring of integers in a finite extension K of $\mathbf{Q}$. Let X be a smooth $\mathcal{O}$-scheme of finite type whose geometric generic fibre $X \otimes_{\mathcal{O}} \overline{K}$ is connected, and which maps surjectively to* Spec $(\mathcal{O})$ *(i.e. for every prime $\mathfrak{p}$ of $\mathcal{O}$, the fibre over $\mathfrak{p}$, $X \otimes_{\mathcal{O}} (\mathcal{O}/\mathfrak{p})$, is non empty). Then the group $\pi_1(X)^{ab}$ is finite.*

Proof. This follows immediately from Theorem 1 and global classfield theory, according to which $\pi_1(\mathrm{Spec}(\mathcal{O}))^{ab}$, the galois group of the maximal unramified abelian extension of K, is *finite.* QED

Theorem 4. *Let $\mathcal{O}$ be the ring of integers in a finite extension K of $\mathbf{Q}$, $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ a finite set of primes of $\mathcal{O}$, $N = p_1 \ldots p_n$ the product of their residue characteristics, and $\mathcal{O}[1/\mathfrak{p}_1 \ldots \mathfrak{p}_n]$ the ring of "integers outside $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$" in K. Let X be a smooth $\mathcal{O}[1/\mathfrak{p}_1 \ldots \mathfrak{p}_n]$-scheme of finite type, whose geometric generic fibre $X \otimes_{\mathcal{O}} \overline{K}$ is connected, and which maps surjectively to* Spec $(\mathcal{O}[1/\mathfrak{p}_1 \ldots \mathfrak{p}_n])$ *(i.e. for every prime $\mathfrak{p} \notin \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$, the fibre*

$$X \otimes (\mathcal{O}/\mathfrak{p})$$

is non-empty). Then the group $\pi_1(X)^{ab}$ is the product of a finite group and a pro-N group.

Proof. Again an immediate consequence of Theorem 1 and global classfield theory, according to which $\pi_1(\mathrm{Spec}(\mathcal{O}[1/\mathfrak{p}_1 \ldots \mathfrak{p}_n]))^{ab}$, the galois group of the maximal abelian, unramified outside $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$-extension of K is finite times pro-N. QED

THEOREM 5. *Let S be a normal, connected noetherian scheme, whose function field K is absolutely finitely generated. Let $f: X \to S$ be a smooth surjective morphism of finite type whose geometric generic fibre is connected, and which admits a cross-section $X \overset{\varepsilon}{\underset{\leftarrow}{\curvearrowright}} S$. Then there are only finitely many connected finite etale X-schemes Y/X which are galois over X with abelian galois group of order prime to* char (K) *and which are completely decomposed over the marked section. If in addition we suppose X/S proper, we can drop the proviso "of order prime to* char (K)".

Proof. This is just the concatenation of Theorems 1 and 2 with the physical interpretation (1.3) of the group Ker (X/S) in the presence of a section. QED

V. APPLICATION TO l-ADIC REPRESENTATIONS

Let l be a prime number, $\overline{\mathbf{Q}}_l$ an algebraic closure of $\mathbf{Q}_l$. By an l-adic representation ρ of a topological group π, we mean a finite-dimensional continuous representation

$$\rho: \pi \to GL(n, \overline{\mathbf{Q}}_l)$$

whose image lies in $GL(n, E_\lambda)$ for some finite extension E_λ of $\mathbf{Q}_l$.

THEOREM 6. (cf. Grothendieck, *via* [2], 1.3). *Let K be an absolutely finitely generated field, X/K a smooth, geometrically connected K-scheme of finite type, $\bar{x}$ a geometric point of $X \otimes \overline{K}$, x the image geometric point of $\bar{x}$ in X. Let l be a prime number, and ρ an l-adic representation of $\pi_1(X, x)$;*

$$\rho: \pi_1(X, x) \to GL(n, \overline{\mathbf{Q}}_l).$$

Let G be the Zariski closure of the image $\rho(\pi_1(X \otimes \overline{K}, \bar{x}))$ of the geometric fundamental group $\pi_1(X \otimes \overline{K}, \bar{x})$ in $GL(n, \overline{\mathbf{Q}}_l)$ and G^0 its identity component. Suppose that either l is different from the characteristic p of K, or that X/K is proper. Then:

(1) *the radical of G^0 is unipotent, or equivalently:*

(2) *if the restriction of ρ to the geometric fundamental group $\pi_1(X \otimes \overline{K}, \bar{x})$ is completely reducible, then the algebraic group G^0 is semi-simple.*

Proof. By Theorem 1, for $l \neq p$, or by Theorem 2 if $l = p$ and X/K is *proper*, we know that the l-part of Ker (X/K) is finite i.e. (cf. Lemma 1) the image of $\pi_1(X \otimes \overline{K}, \bar{x})$ in $\pi_1(X)^{ab}$ is the product of a finite group and a group of order prime to l. Given this fact, the proof proceeds exactly as in (Deligne [2], 1.3). QED

Remarks. (1) This theorem is the group-theoretic version of Grothendieck's local monodromy theorem (cf. Serre-Tate ([15], Appendix) for a precise statement, as well as the proof) with X/K "replacing" the spectrum of the fraction field E of a henselian discrete valuation ring with residue field K, and with $\pi_1(X \otimes \overline{K})$ "replacing" the inertia subgroup I of Gal $(\overline{E}/E)$. The "extra" feature of the "local" case is that the quotient of I by a normal pro-p subgroup is abelian. Therefore any l-adic representation ρ of I, with $l \neq p$, becomes *abelian* when restricted to a suitable open subgroup of I, and hence the associated algebraic group G^0 is automatically abelian. In particular, the radical of G^0 is G^0 itself.

(2) If X/K is itself an abelian variety A/K, then $\pi_1(A \otimes \overline{K}, \bar{x})$ is abelian. Therefore if l is any prime, and ρ any l-adic representation of $\pi_1(A \otimes \overline{K}, \bar{x})$, the associated algebraic groups G and G^0 will be abelian; hence if ρ is the restriction to $\pi_1(A \otimes \overline{K}, \bar{x})$ of an l-adic representation of $\pi_1(\grave{A}, x)$, then G^0 is unipotent, i.e. the restriction of ρ to an open subgroup of $\pi_1(A \otimes \overline{K}, \bar{x})$ is *unipotent* (compare Oort [11], 2).

(3) Can one give an example of X/K proper smooth and geometrically connected over an absolutely finitely generated field K of characteristic $p > 0$ whose fundamental group $\pi_1(X, x)$ admits an n-dimensional p-adic representation with $n \geqslant 2$ (resp. $n \geqslant 3$) for which the associated algebraic group G^0 is $SL(n)$ (resp. $SO(n)$)? Can we find an abelian scheme A over such an X, all of whose fibres have the same p-rank $n \geqslant 2$, for which the associated p-adic representation of $\pi_1(X, x)$ has $G^0 = SL(n)$? (cf. Oort [11] for the case of p-rank zero).

REFERENCES

[0] ARTIN, M., A. GROTHENDIECK and J. L. VERDIER. *Théorie des Topos et Cohomologie Etale des Schémas* (SGA 4), Tome 3. Springer Lecture Notes 305, 1973.

[1] BLOCH, S. Algebraic K-theory and class-field theory for arithmetic surfaces. *To appear in Annals of Math.*

[2] DELIGNE, P. La conjecture de Weil II. *Pub. Math. IHES 52* (1980).

[3] GROTHENDIECK, A. *Revêtements Etales et Groupe Fondamental* (SGA I). Springer Lecture Notes, 224, 1971.

[4] LANG, S. *Diophantine Geometry*. Interscience Publishers, New York, 1962.

[5] —— On the Lefshetz principle. *Ann. of Math. 64* (1956), pp. 326-327.

[6] —— Unramified class field theory over function fields in several variables. *Ann. of Math. 64* (1956), pp. 286-325.

[7] —— Sur les séries L d'une variété algébrique. *Bull. Soc. Math. France 84* (1956), pp. 385-407.

[8] LANG, S. et J. P. SERRE. Sur les revêtements non ramifiés des variétés algébriques. *Amer. J. Math.* (1957), pp. 319-330.

[9] MUMFORD, D. *Abelian Varieties*. Oxford University Press, 1970.

[10] OORT, F. *Commutative group schemes*. Springer Lecture Notes 15, 1966.

[11] —— Subvarieties of Moduli Spaces. *Inv. Math. 24* (1974), pp. 95-119.

[12] PARSHIN, A. H. Abelian coverings of arithmetic schemes. *Doklady Akad. Nauk. Tome 243 No. 4* (1978), 855-858; English translation in *Soviet Mathematics, Doklady, Vol. 19* (1978), 1438-1442.

[13] SERRE, J.-P. Quelques propriétés des variétés abéliennes en car. p. *Amer. J. Math. vol. 80* (1958), pp. 715-739.

[14] —— *Groupes algébriques et corps de classes*. Hermann, Paris, 1959.

[15] SERRE, J.-P. and J. TATE. Good reduction of abelian varieties. *Annals Math. 88, No. 3* (1968), pp. 492-517.

[16] WEIL, A. *Courbes algébriques et variétés abéliennes*. Hermann, Paris, 1971.

[17] IMAI, H. A remark on the rational points of abelian varieties with values in cyclotomic $\mathbf{Z}_p$-extensions. *Proc. Japan Acad. 51* (1975), pp. 12-16.

[18] KUBOTA, T. On the field extension by complex multiplication. *Trans. AMS 118, No. 6* (1965), pp. 113-122.

[19] RIBET, K. Division fields of abelian varieties with complex multiplication. *Mémoire, Soc. Math. France, 2e Série, n° 2* (1980), pp. 75-94.

[20] MAZUR, B. Modular curves and the Eisenstein ideal. *Publ. IHES 47* (1977), 33-186.

(Reçu le 20 janvier 1981)

Nicholas M. Katz

Fine Hall
Department of Mathematics
Princeton University
Princeton, N.J. 08544, USA

Serge Lang

Mathematics Department
Box 2155 Yale Station
New Haven, Conn. 06520
USA

Ribet, Kenneth A.

APPENDIX: TORSION POINTS OF ABELIAN VARIETIES IN CYCLOTOMIC EXTENSIONS

L'Enseignement Mathématique, Vol.27 (1981)

APPENDIX: TORSION POINTS OF ABELIAN VARIETIES IN CYCLOTOMIC EXTENSIONS

by Kenneth A. RIBET [1])

Let k be a number field, and let $\bar{k}$ be an algebraic closure for k. For each prime p, let K_p be the subfield of k obtained by adjoining to k all p-power roots of unity in $\bar{k}$. Let K be the compositum of all of the K_p, i.e., the field obtained by adjoining to k *all* roots of unity in $\bar{k}$.

Suppose that A is an abelian variety over k. Mazur has raised the question of whether the groups $A(K_p)$ are finitely generated [4]. In this connection, H. Imai [1] and J.-P. Serre [5] proved (independently) that the *torsion subgroup* of $A(K_p)$ is finite for each p. The aim of this appendix is to prove that more precisely one has the following theorem, cf. [3], §II, Remark 3.

THEOREM 1. *The torsion subgroup* $A(K)_{\text{tors}}$ *of* $A(K)$ *is finite.*

Let G be the Galois group $\text{Gal}(\bar{k}/k)$ and let H be its subgroup $\text{Gal}(\bar{k}/K)$. For each positive integer n, let $A[n]$ be the kernel of multiplication by n in $A(\bar{k})$. For each prime p, let V_p be the $\mathbf{Q}_p$-adic Tate module attached to A. If M is one of these modules, we denote by M^H the set of elements of M left fixed by H. Since H is normal in G, M^H is stable under the action of G on M.

Because of the structure of the torsion subgroup of $A(\bar{k})$, one sees easily that Theorem 1 is equivalent to the conjunction of the following two statements:

THEOREM 2. *For all but finitely many primes* p, *we have* $A[p]^H = 0$.

THEOREM 3. *For each prime* p, *we have* $V_p^H = 0$.

Indeed, Theorem 2 asserts the vanishing of the p-primary part of $A(K)_{\text{tors}}$, while Theorem 3 asserts the finiteness of this p-primary part.

---

[1]) Partially supported by National Science Foundation contract number MCS 80-02317.

In proving these statements, we visibly have the right to replace k by a finite extension of k. Therefore, using ([SGA 71], IX, 3.6) we can (and will) assume that A/k is semistable. Next, consider the largest subextension k' of K/k which is unramified at all finite places of k.

LEMMA. *For each prime p, let L_p be the largest extension of k in K which is unramified at all places of k except for primes dividing p and the infinite places of k. Then L_p is the compositum $k'K_p$.*

Proof. Let A be the Galois group Gal (K/k), viewed as a subgroup of $\hat{\mathbf{Z}}^*$. We consider $\hat{\mathbf{Z}}^*$ as the direct product of its two subgroups $\mathbf{Z}_p^*$ and $\prod_{l \neq p} \mathbf{Z}_l^*$. Let I (resp. J) be the subgroup of A generated by the inertia groups of A for primes of k which divide p (resp. which do not divide p). Then I is a subgroup of Z_p^*, while J is a subgroup of $\prod_{l \neq p} \mathbf{Z}_l^*$. The product $I \times J$ is the subgroup of A generated by all inertia groups of A. We have $J = \text{Gal}\,(\bar{k}/L_p)$, $I \times J = \text{Gal}\,(\bar{k}/k')$, and Gal $(\bar{k}/K_p) = A \cap \left(\prod_{l \neq p} \mathbf{Z}_l^*\right)$. Now Gal $(\bar{k}/k'K_p)$ is the intersection of the two Galois groups Gal $(\bar{k}/k')$ and Gal $(\bar{k}/K_p)$. Putting these facts together, we prove the desired assertion.

We now replace k by its finite extension k'. With this replacement made, K_p becomes equal to L_p. Furthermore, for odd primes p, the largest extension of k in K which is unramified outside p and infinity and which has degree prime to p is the field obtained by adjoining to k the p-th roots of unity in $\bar{k}$.

Proof of Theorem 2. We shall consider only primes p which are odd, unramified in k, and such that A has good reduction at at least one prime of k dividing p. Let p be such a prime and v a prime of k over p at which A has good reduction. Suppose that the G-module $A\,[p]^H$ is non-zero, and let W be a simple G-submodule of this module. The algebra $\text{End}_G W$ is a finite field $\mathbf{F}$, and the action of G on W is given by a character

$$\phi : G \to \mathbf{F}^*$$

since the action of G on $A\,[p]^H$ is abelian. (Here the point is simply that G/H is an abelian group.) In particular, the image of G in Aut $(A\,[p])$ has order prime to p. On the other hand, the character ϕ is unramified at primes of k not dividing p because A/k is semistable. By the discussion following the lemma, we know that ϕ factors through the quotient Gal $(k(\mu_p)/k)$ of G; here, μ_p denotes the group of p-th roots of unity. In particular, ϕ must have order dividing $p - 1$, so that its

values lie in the prime field $\mathbf{F}_p$. Since W was chosen to be simple, its dimension over $\mathbf{F}_p$ must be 1; i.e., W is a group of order p.

Let $\chi: G \to \mathbf{F}_p^*$ be the mod p cyclotomic character, i.e., the character giving the action of G on μ_p. Since ϕ factors through Gal $(k(\mu_p)/k)$, we may write ϕ in the form χ^n, where n is an integer mod $(p-1)$. We claim that n can only be 0 or 1.

To verify this claim, it is enough to check that it is true after we replace G by an inertia group I in G for the prime v, since χ is totally ramified at v. We remark that W is the I-module associated to a finite flat commutative group scheme $\mathscr{W}$ over the ring of integers of the completion of k at v, since v is such that A has good reduction at v. Because $\mathscr{W}$ has order p, the classification of Tate-Oort ([8], especially pp. 15-16) applies to $\mathscr{W}$. Because v is absolutely unramified, the classification shows immediately that $\mathscr{W}$ is either étale or the dual of an étale group. In the former case, I acts trivially on W; in the latter case, I acts on W via χ. This completes the verification of the claim.

Thus, if Theorem 2 is false, there are infinitely many primes p for which $A[p]$ contains a G-submodule isomorphic to either $\mathbf{Z}/p\mathbf{Z}$ or to μ_p. Of course, the former case can occur only a finite number of times, since $A(k)$ is finite. One way to rule out the latter case is to argue that whenever μ_p is a submodule of $A[p]$, the group $\mathbf{Z}/p\mathbf{Z}$ is a quotient of the dual of $A[p]$, which is the kernel of multiplication by p on the abelian variety $A^\vee$ dual to A. In other words, if μ_p occurs as a submodule of $A[p]$, then there is an abelian variety isogenous to $A^\vee$ (and therefore in fact to A) which has a rational point of order p over k. Therefore p is a divisor of the order of a finite group that may be specified in advance, viz. the group of rational points of any reduction of A at a good unramified prime of k of residue characteristic different from 2. (See the appendix to Katz's recent paper [2] for a discussion of this point.)

Proof of Theorem 3. Suppose that p is a prime such that V_p^H is non-zero. We again choose W to be an irreducible G-submodule (i.e., $\mathbf{Q}_p[G]$-submodule) of V_p^H. Because the action of G on W is abelian, and because W is simple, each element of G acts semisimply on W. Since A/k is semistable, it follows that the homomorphism

$$\rho: G \to \mathrm{Aut}(W)$$

giving the action of G on W is unramified at all primes of k not dividing p. Therefore, ρ factors through Gal (K_p/k) in view of the lemma and the subsequent replacement $k \to k'$. In other words, starting from the hypothesis that the p-torsion subgroup of $A(K)$ is infinite, we have deduced that the p-torsion subgroup of $A(K_p)$ is infinite.

Of course, this situation is ruled out by the theorem of Imai and Serre mentioned above. Nevertheless, we will sketch for the reader's convenience an argument which leads to a contradiction. Let v be a place of k dividing p, and let $D \subset G$ be a decomposition group for v. By ([SGA 71], IX, Prop. 5.6), the D-module V_p is an extension of D-modules attached to p-divisible groups over the integer ring of the completion of k at v. Because of Tate's theory [7], the semisimplification V_p^{ss} of the D-module V_p has a Hodge-Tate decomposition. (Here we should remark that submodules and quotients of Hodge-Tate modules are again Hodge-Tate.) Since W is semisimple as a D-module (because semisimple and *abelian* as a G-module), W may be viewed as a submodule of V_p^{ss}. Therefore, W is a Hodge-Tate module.

By ([6], III, Appendix), we know that ρ is a locally algebraic abelian representation of G. Using this information, plus the fact that ρ factors through Gal (K_p/k), we find that there is an open subgroup G_0 of G with the following property: the restriction of ρ to G_0 is the direct sum of 1-dimensional representations, each described by an integral power χ_p^n of the standard cyclotomic character $\chi_p : G \to \mathbf{Z}_p^*$. After replacing k by a finite extension, we may assume that G_0 is G. Take a prime w of k which is prime to p and such that A has good reduction at w. Let $g \in G$ be a Frobenius element for w. The eigenvalues of $\rho(g)$ will be integral powers of $\chi_p(g)$, i.e., of the norm Nw of w. However, by a well known theorem of Weil, these eigenvalues all have archimedian absolute values equal to $(Nw)^{1/2}$. This contradiction completes the proof of Theorem 3.

REFERENCES

[1] IMAI, H. A remark on the rational points of abelian varieties with values in cyclotomic $\mathbf{Z}_p$ extensions. *Proc. Japan Acad. 51* (1975), 12-16.

[2] KATZ, N. Galois properties of torsion points on abelian varieties. *Invent. Math. 62* (1981), 481-502.

[3] KATZ, N. and S. LANG. Finiteness theorems in geometric classfield theory.

[4] MAZUR, B. Rational points of abelian varieties with values in towers of number fields. *Invent. Math. 18* (1972), 183-266.

[5] SERRE, J.-P. Letters to B. Mazur, January, 1974.

[6] —— *Abelian l-adic Representations and Elliptic Curves.* New York: Benjamin 1968.

[7] TATE, J. *p*-divisible groups. In: *Proceedings of a Conference on Local Fields.* Berlin-Heidelberg-New York: Springer-Verlag 1967.

[8] TATE, J. and F. OORT. Group schemes of prime order. *Ann. scient. Éc. Norm. Sup., 4^e série 3* (1970), 1-21.

[SGA 71] *Groupes de Monodromie en Géométrie Algébrique* (séminaire dirigé par A. Grothedieck avec la collaboration de M. Raynaud et D. S. Rim). *Lecture Notes in Math. 288* (1972).

(Reçu le 20 janvier 1981)

Kenneth A. Ribet

U.C. Berkeley
Mathematics Department
Berkeley, Ca. 94720
USA