II. The Main theorem

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

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

we can rewrite this

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

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

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

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.