Bull. Sc. math., 2e *série*,
96, 1972, p. 333-338.

CONGRUENCE SUBGROUPS OF ABELIAN VARIETIES

BY

JAMES STUART MILNE (*)
[Ann Arbor]

ABSTRACT. — It is shown that the congruence subgroup problem, when correctly stated, has a positive solution for abelian schemes over normal integral schemes which are of finite type over the rational integers.

1. Statements

Let V be an integral normal scheme of finite-type over spec $\mathbf{Z}$, let K be the field of rational functions of V, and let A be an abelian scheme over V. The group $A(V)$ of sections of A over V is finitely generated because it may be regarded as a subgroup of $A(K)$, and $A(K)$ is finitely generated by the Mordell-Weil theorem [3]. Consider a system $\Sigma = (v_i, n_i)_{i \in I}$ in which I is a finite set, the v_i are closed points of V, and the n_i are positive integers. Let O_v be the local ring of V at v and let $O_{v,n}$ be O_v modulo the nth power of its maximal ideal. $O_{v,n}$ is finite when v is closed because $O_{v,1} = k(v)$ is finite and O_v is noetherian. There are canonical maps $A(V) \to A(O_{v,n})$ and the congruence subgroup of $A(V)$ defined by Σ is $A(V)_\Sigma = \operatorname{Ker}(A(V) \to \prod_{i \in I} A(O_{v_i, n_i}))$. Clearly $A(V)_\Sigma$ is a subgroup of finite index in $A(V)$.

THEOREM. — *Every subgroup of finite index in $A(V)$ contains a congruence subgroup $A(V)_\Sigma$ for some Σ.*

Before proving the theorem, we deduce two slightly weaker statements and make some remarks.

COROLLARY 1. — *Let K be a global field [i. e. a finite extension of $\mathbf{Q}$ or of $\mathbf{F}_q(X)$ some q] and let A be an abelian variety over K. Let S be a finite set of primes of K. If $A(K)$ is embedded diagonally in the compact*

(*) This work was supported by the Science Research Council, and written while the author was a visitor at Kings College, London.

group $\prod_{v \notin S} A(K_v)$, *where* K_v *is the completion of* K *at a non-trivial prime* v, *then the topology induced on* $A(K)$ *is that defined by its subgroups of finite index.*

Proof. — Choose V to be a non-empty open subscheme of the spectrum of the ring of integers of K (number field case) or the integral normal curve canonically associated to K (function field case) so that A has good reduction at every closed point of V and S is disjoint from the set of primes of K corresponding to closed points of V. There is an abelian scheme A_V over V whose generic fibre is A. Moreover $A_V(V) = A(K)$, $A(R_v) = A(K_v)$ (where R_v = ring of integers in K_v), and the topology on $A(K_v)$ induced by that of K_v corresponds to the topology on $A(R_v)$ induced by the subgroups $\operatorname{Ker}(A(R_v) \to A(O_{v,n}))$, $n \geqq 0$. Thus the corollary follows from the theorem.

COROLLARY 2. — *A subgroup* H *of finite index in* $A(V)$ *contains a congruence subgroup of the form* $A(V)_\Sigma$ *with* $\Sigma = (v_i, n_i)_{i \in I}$, $n_i = 1$ *all* i, *whenever one of the two following conditions holds :*

(*a*) *the structure map* $\varphi : V \to \operatorname{spec} \mathbf{Z}$ *is dominating; or*

(*b*) $\varphi(V)$ *consists of one point* (p) *of* spec $\mathbf{Z}$, *and* p *does not divide the index* $(A(V) : H)$ *of* H *in* $A(V)$.

Proof. — (*a*) Let U be the open subscheme $\varphi^{-1}(\operatorname{spec} \mathbf{Z}[m^{-1}])$ of V where $m = (A(V) : H)$. Because of our assumption, U is non-empty. $A(V)$ may be regarded as a subgroup of $A(U)$, and there is a subgroup H' of $A(U)$ such that $H' \cap A(V) = H$ and $(A(U) : H')$ divides a power of m, e. g. take $H' = mA(U) + H$. It suffices to prove the corollary for H' and U i. e. we may assume to begin with that the characteristic p_v of $k(v)$ does not divide $(A(V) : H)$ for any $v \in V$.

By the theorem, $H \supset A(V)_\Sigma$ for some $\Sigma = (v_i, n_i)_{i \in I}$. Then $A(O_{v_i, n_i})$ is an extension of $A(O_{v_i, 1})$ by a group which has order a power of p_v. Thus, if $\Sigma' = (v_i, n_i')_{i \in I}$ with $n_i' = 1$ all i, then $(A(V)_{\Sigma'} : A(V)_\Sigma)$ is a product of powers of p_{v_i} for $i \in I$, $v_i \in V$. It follows that $H \supset A(V)_{\Sigma'}$.

(*b*) This may be proved by the same argument as in the preceding paragraph.

REMARK 1. — Corollary 2 is false without the condition (*a*) or (*b*). The simplest example is given by taking $A = A_0 \times_{\operatorname{spec} \mathbf{F}_p} V$ where V is a scheme over $\mathbf{F}_p$ and A_0 is a super-singular elliptic curve, for then p does not divide the order of $A(k(v))$ for any v. Thus, if $pA(V) \neq A(V)$, then $H = pA(V)$ cannot satisfy corollary 2. More generally, the methods of [4] can be used to show that, without the conditions, corollary 2 is false for any constant abelian scheme (over a curve say) for which $A(V)$ is infinite.

2. — Corollary 1 is due to SERRE [6] in the case of a number field. Corollary 2 is entirely due to SERRE, and may be proved by an easy modification of the methods of [6]. (I am grateful to Professor SERRE for pointing this out to me.) The only contribution of this paper is to extend these methods so that they work in the generality of the theorem.

2. The proof

Let N be a finite flat commutative group scheme over V and let $N_K = N \times_V \text{spec}\,(K)$ be the generic fibre of N/V. There is a canonical exact sequence of finite group schemes over K, $0 \to N_K^0 \to N_K \to N_K^{et} \to 0$, in which N_K^0 is connected and N_K^{et} is étale [of course, if char $(K) = 0$ or char (K) does not divide the order of N, then $N_K = N_K^{et}$ and much of what follows is trivial]. We will say that this sequence extends over V if there is an exact sequence of finite flat group schemes $0 \to N' \to N \to N'' \to 0$ over V which has generic fibre $0 \to N_K^0 \to N_K \to N_K^{et} \to 0$ and which has N'' étale over V. By considering orders inside N_K and N_K^{et}, and using the facts that a finite morphism is flat or étale over an open set, one shows easily that $0 \to N_K^0 \to N_K \to N_K^{et} \to 0$ always extends over a non-empty open subscheme of V, and that such an extension is unique.

If F is a sheaf for the flat (f. p. p. f.) topology on V, define $\overline{H}^1(V, F) = \text{Ker}\,(H^1(V, F) \to \prod_{v \in V_0} H^1(R_v, F))$ where V_0 is the set of closed points of V, R_v is the completion of the local ring O_v, and all cohomology groups are with respect to the flat topology.

PROPOSITION 1. — *Let N be such that $0 \to N_K^0 \to N_K \to N_K^{et} \to 0$ extends over V, and* fix $v \in V_0$. *Then there is a homomorphism $\varphi(N)$ from the kernel of $\overline{H}^1(V, N) \to \overline{H}^1(V, N'')$ into $N''(R_v)/N(R_v)$ which is injective and functorial in N.*

Proof. — Let P be a non-trivial principal homogeneous space for N' over V. P_K has no point in K for otherwise, V being normal, P would have a point in V. P_K is a local scheme whose residue field is a non-trivial purely inseparable extension of K. As V is an excellent scheme [1; IV, 7.8], spec $(R_v \otimes_{O_v} K) \to \text{spec}\,K$ is geometrically regular, and hence P_K has no point in $R_v \otimes_{O_v} K$. Since all elements of $H^1(V, N')$ are representable, this shows that the map $H^1(V, N') \to H^1(R_v, N')$ is injective. The proposition now follows by an easy diagram chase from the exact commutative diagram

$$\begin{array}{ccccccc}
 & & 0 & & & & \\
 & & \downarrow & & & & \\
 & & H^1(V, N') & \longrightarrow & H^1(V, N) & \longrightarrow & H^1(V, N'') \\
 & & \downarrow & & \downarrow & & \downarrow \\
N(R_v) & \longrightarrow & N''(R_v) & \longrightarrow & H^1(R_v, N') & \longrightarrow & H^1(R_v, N) \longrightarrow H^1(R_v, N'')
\end{array}$$

Fix a separable algebraic closure $\overline{K}$ of K and let G be the fundamental group of V corresponding. G is thus identified with a quotient group of the Galois group of $\overline{K}$ over K. If N is an étale commutative group scheme over V, then there is a canonical isomorphism $H^1(G, N(\overline{K})) \to H^1(V, N)$.

PROPOSITION 2. — *$\overline{H}^1(V, N)$ is finite for any finite flat commutative group scheme N over V.*

Proof. — For any non-empty open subscheme U of V, the map $H^1(V, N) \to H^1(U, N)$ is injective because both groups can be embedded in $H^1(K, N_K)$ (c. f. an argument in the above proof). Thus we may assume that $0 \to N_K^0 \to N_K \to N_K^{et} \to 0$ extends over V. Since $N''(R_v)$ is finite, proposition 1 now allows us to assume that N is étale over V. With the notation of [6; I, 2.2.3], $\overline{H}^1(V, N) \subset H^1_*(G, N(\overline{K}))$ (*see* the proof of [6; I, Proposition 8]; for facts on the density of Frobenius automorphisms in non-zero characteristic, *see* [2]). $H^1_*(G, N(\overline{K}))$ is finite by [6; I, Cor. to Proposition 6].

Fix a prime number p, let A be an abelian scheme over V, and let $A_{p^m} = \mathrm{Ker}\,(p^m : A \to A)$.

PROPOSITION 3. — *If $\varprojlim_m H^1(V, A_{p^m}) = 0$ then, for any n, $p^n A(V)$ is a congruence subgroup of $A(V)$.*

Proof. — The exact sequence (for the flat topology)

$$0 \to A_{p^n} \to A \xrightarrow{p^n} A \to 0$$

gives rise to a coboundary map $d : A(V) \to H^1(V, A_{p^n})$ whose kernel is $p^n A(V)$.

LEMMA. — *There is a congruence subgroup of $A(V)$ whose image under d is contained in $\overline{H}^1(V, A_{p^n})$.*

Proof. — Let $(x_i)_{i \in I}$ be the set of elements of $d(A(V))$ which are not contained in $\overline{H}^1(V, A_{p^n})$. I is finite because $A(V)$ is finitely generated. For each $i \in I$ there is a $v_i \in V_0$ such that x_i has non-zero image in $H^1(R_{v_i}, A_{p^n})$. Let his image be represented by the principal homogeneous space P_i. If $P_i(R_{v_i,n})$ were non-empty for all n then $\varprojlim_n P_i(R_{v_i,n})$ would be non-empty because the sets $P_i(R_{v_i,n})$ are finite, and this would imply that $P_i(R_{v_i})$ is non-empty, which is not so. Thus there is an integer n_i such that $P_i(R_{v_i,n_i})$ is empty, i. e. such that the image of x_i in $H^1(R_{v_i,n_i}, A_{p^n})$ is non-zero. Let $\Sigma = (v_i, n_i)_{i \in I}$. If

$x \in A(V)_{\geq}$ then the image of $d(x)$ in $H^1(R_{v_i, n_i}, A_{p^n})$ is zero because the diagram

$$\begin{array}{ccc} A(V) & \longrightarrow & H^1(V, A_{p^n}) \\ \downarrow & & \downarrow \\ A(O_{v_i, n_i}) = A(R_{v_i, n_i}) & \longrightarrow & H^1(R_{v_i, n_i}, A_{p^n}) \end{array}$$

commutes. Thus $d(x) \neq x_i$ for any i, and so $d(x) \in \overline{H}^1(V, A_{p^n})$. The rest of the proof of the proposition is the same as the proof of [6; I, Thm. 2].

Fix a prime p and define $T_p = \varprojlim_n (A_{p^n})^{et}_K$. This may be regarded as a free $\mathbf{Z}_p$-module of rank 2 dim (A) [$p \neq$ char (K)] or of rank $\leq$ dim A ($p =$ char (K)), on which the Galois group H of $\overline{K}$ over K acts. Let I be the kernel of the canonical map $H \to G$.

PROPOSITION 4. — *If the sequence* $0 \to (A_p)^0_K \to (A_p)_K \to (A_p)^{ét}_K \to 0$ *extends over* V, *then* I *acts trivially on* T_p.

Proof. — Fix an integer n, and let K_n be the smallest subfield of $\overline{K}$ containing K such that $A^{ét}_{p^n}(K_n) = A^{et}_{p^n}(\overline{K})$. It will suffice to show that V_n, the normalization of V in K_n, is étale over V. V_n is finite over V because K_n is separable over K and so it suffices to show that $V_n \otimes_{O_v} R_v$ is étale over spec R_v for any point v of V. Let

$$0 \to A(p)^0 \to A(p) \to A(p)^{et} \to 0$$

be the canonical exact sequence of p-divisible groups arising from $A(p)$ over R_v, and let $0 \to A_{K_v}(p)^0 \to A_{K_v}(p) \to A_{K_v}(p)^{et} \to 0$ arise similarly from $A_{K_v}(p)$ over K_v. The isomorphism $A_{K_v}(p) \to A(p)_{K_v}$ (1) induces an injection $A_{K_v}(p)^0 \to (A(p)^0)_{K_v}$ and hence a surjection

$$A_{K_v}(p)^{ét} \to (A(p)^{et})_{K_v}.$$

From our assumption, the order of the maximal étale quotient of A_p is the same as the order of the maximal étale quotient of $(A_p)_{K_v}$. Thus $A(p)^{et}$ and $A_{K_v}(p)^{et}$ have the same height, $A(p)^0$ and $A_{K_v}(p)^0$ have the same height, the injection $A_{K_v}(p)^0 \to (A(p)^0)_{K_v}$ is an isomorphism, and finally, $A_{K_v}(p)^{et} \to (A(p)^{et})_{K_v}$ is an isomorphism. If follows that $A^{ét}_{p^n} \otimes_{R_v} K_v \approx (A_{p^n})^{et}_{K_v}$, which proves that $V_n \otimes_{O_v} R_v$ is étale over spec R_v.

Let G_p be the image of G in $GL(T_p)$ and $\mathfrak{g}_p$ the Lie algebra of G_p, which we may regards as a subalgebra of $\mathfrak{gl}(V_p)$, $V_p = \mathbf{Q}_p \otimes_{\mathbf{Z}_p} T_p$.

---

(1) $A(p)$ is the p-divisible group associated to A over R_v, $A(p)_{K_v}$ the generic fibre of $A(p)$, and $A_{K_v}(p)$ the p-divisible group associated to A_{K_v}.

PROPOSITION 5.

$$H'_*(\mathfrak{g}_p, V_p) = 0 \Rightarrow H^1_*(G_p, T_p) = 0$$
$$\Rightarrow \varprojlim H^1\left(V, A^{et}_{p^n}\right) = 0 \Rightarrow \varprojlim \overline{H}'(V, A_{p^n}) = 0.$$

Proof. — Let U be a non-empty open subscheme of V such that $0 \to (A_p)^0_K \to (A_p)_K \to (A_p)^{et}_K \to 0$ extends over U. For any closed point v of U the action of the Frobenius element of v on T_p is well-defined up to conjugacy (apply proposition 4 with $V = U$). Moreover, its characteristic polynomial $P(T)$ divides the characteristic polynomial $Q(T)$ of the Frobenius endomorphism of $A \times_{k'} \operatorname{spec}(k(v))$. In fact the roots of $P(T)$ are exactly the roots of $Q(T)$ which are p-adic units [5; Thm. 7]. By using this, the first two implications may be proved exactly as in [6; I, Thm. 3].

Next I claim that for any closed point v of U, $\bigcup_n A^{et}_{p^n}(K_v)$ is finite. Indeed, $\bigcup_n A^{et}_{p^n}(K_v) = \bigcup_n A^{et}_{p^n}(k(v)) = A(k(v))(p)$ as $k(v)$ is perfect. It follows that $\varprojlim A^{et}_{p^n}(K_v) = 0 = \varprojlim (A^{et}_{p^n}(K_v)/A_{p^n}(K_v))$. Thus $\varprojlim \overline{H}^1(V, A_{p^n}) \to \varprojlim \overline{H}^1(V, A^{et}_{p^n})$ is injective by proposition 1.

PROPOSITION 6. — $H^n(\mathfrak{g}_p, V_p) = 0$, *all* $n \geqq 0$.

Proof. — The proof of [6, II, Thm. 2] carries over completely.

It is now possible to prove the theorem. It suffices to consider a subgroup H of the form $p^n A(V)$, but, for such an H, the theorem follows from propositions 6, 5 and 3.

REFERENCES

[1] GROTHENDIECK (A.) et DIEUDONNÉ (J.). — *Éléments de Géométrie algébrique.* — Publ. math. I. H. E. S., 1960.

[2] LANG (S.). — Sur les série L d'une variété algébrique, *Bull. Soc. math. Fr.*, t. 84, 1956, p. 385-407.

[3] LANG (S.). — *Diophantine Geometry.* — Interscience Tracts No 11. Interscience Publishers, New York-London, 1962.

[4] MILNE (J.). — *The Tate-Šafarevič group of a constant abelian variety*, vol. 6, 1968, p. 91-105.

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

[6] SERRE (J.-P.). — Sur les groupes de congruences des variétés abéliennes, I. *Izv. Nauk. S. S. S. R. Ser. Mat.*, vol. 28, 1964, p. 3-20, II; *Ibid.*, vol. 35, 1971, p. 731-737.

(Texte reçu le 8 juin 1972.)

James Stuart MILNE,
University of Michigan,
Department of Mathematics,
Ann Arbor,
Mich 48104 (États-Unis).