Inventiones math. 6, 91 – 105 (1968)

The Tate-Šafarevič Group of a Constant Abelian Variety*

J. S. MILNE (London)

Introduction

If B is an abelian variety over a field K, then the isomorphism classes of principal homogeneous spaces for B over K form an abelian group called the Weil-Châtelet group $\mathrm{WC}(B/K)$ of B over K [17, 33]. Assume that K is a number field or a function field in one variable over a finite field and let K_v denote the completion of K at the prime v of K. Then the elements of $\mathrm{WC}(B/K)$ which, for all primes v of K, are in the kernel of the canonical map $\mathrm{WC}(B/K) \to \mathrm{WC}(B/K_v)$, form a group called the Tate-Šafarevič group $Ш(B/K)$ of B over K. It is of great importance for the arithmetic of B, and in particular for the determination of the points of B with values in K, to know whether this group is finite (for an elementary exposition of this in the case where B has dimension 1, see [4]). It is usually conjectured that in fact $Ш(B/K)$ is finite, and Birch and Swinnerton-Dyer conjecture a relation between its order and certain other numbers coming from the arithmetic of B (see [3, § 1 (B)] for an early form of the conjecture, and [30, Conj. (B)] for the most general form). Apparently, when K is a number field, this conjecture has not been completely proved for a single abelian variety. Our purpose in this paper is to prove that, when K is a function field of the above type, and B is a constant abelian variety over K (i.e. B is defined over the field of constants of K) then $Ш(B/K)$ is finite and its order satisfies the relation conjectured by Birch and Swinnerton-Dyer. This extends a result of Artin and Tate who, by working with an analogue of the conjecture involving the Brauer group of a surface, have shown, in the same situation, that if further B is assumed to be a Jacobian, then the direct sum of the l-primary components of $Ш(B/K)$ (l prime and not equal to the characteristic of K) is finite and has the order predicted by the conjecture of Birch and Swinnerton-Dyer [30, Thm. 5.2].

To prove the main result (Thm. 3) of this paper, we have to do little more than reinterprete the main result of our previous paper [18, Thm. 3]

* This research was partially supported by the National Science Foundation under contract NSF GP 6432.

in the new situation. For this, we use flat cohomology, and we summarize the main facts needed about flat cohomology in § 1. In § 2 we prove a theorem which relates the coverings of a variety to the extensions of its Albanese variety. The main result is proved in § 3, and § 4 contains some further remarks and corollaries.

Throughout the paper, all group schemes will be commutative. If G and H are group schemes over a scheme X, then we distinguish the set of morphisms of X-schemes G to H from the set of group homomorphisms G to H by denoting the former as $H(G)$ or $\mathrm{Mor}_X(G,H)$ and the latter as $\mathrm{Hom}_X(G,H)$. If A is an abelian group (or group scheme) and p is a fixed prime, then we write A_ν and $A^{(\nu)}$ for the kernel and cokernel respectively of the map

$$A \xrightarrow{p^\nu} A, \quad \text{and} \quad A(p) = \varinjlim_{\nu} A_\nu, \qquad T_p A = \varprojlim_{\nu} A_\nu.$$

If A is an abelian variety then $\hat{A}$ is its dual abelian variety. We write Y_X or, when it causes no ambiguity, just Y, for $X \times_S Y$ where X and Y are schemes over S.

It is a pleasure to thank J. Tate, who supervised this work, for many stimulating conversations and valuable suggestions.

§ 1. Flat Cohomology

For any prescheme X, X_{fl} denotes the category of preschemes locally of finite presentation over X with its f.p.p.f. topology (i.e. that for which a fundamental system of coverings is formed by surjective families $(U_i \to U)_{i \in I}$ of flat morphisms, locally of finite presentation) and X_{et} denotes the same category with its étale topology [1], [5, IV, 6.3], [2, VII]. Unless indicated otherwise, all sheaves with respect to one of these topologies will be sheaves of abelian groups, and all cohomology groups will be with respect to the f.p.p.f. topology. Recall [12, App.] that if the sheaf G on X_{fl} is representable by a smooth group scheme over X, then the canonical maps $H^r(X_{\mathrm{et}}, G) \to H^r(X, G)$ are isomorphisms. Thus, the computations of the cohomology of the multiplicative group $\mathbf{G}_m$ with respect to the étale topology made in [1, Chapt. IV] (e.g. $H^1(X_{\mathrm{et}}, \mathbf{G}_m) \approx \mathrm{Pic}(X)$) hold equally for the f.p.p.f. topology. Also [2, VII, 4.3], if F is a quasi-coherent O_X-module (in the usual sense with the Zariski topology), then the functor defined by

$$W(F)(U) = \Gamma(U, F \otimes_{O_X} O_U),$$

U locally of finite presentation over X, is a sheaf on X_{fl}, and

$$H^r(X, W(F)) \approx H^r(X_{\mathrm{Zar}}, F).$$

In particular, if $\mathbf{G}_a$ is the additive group, then $H^r(X, \mathbf{G}_a) \approx H^r(X_{\mathrm{Zar}}, O_X)$ (and we denote this group by $H^r(X, O_X)$).

Let F be a sheaf on X_{fl} and let P be a sheaf of sets on which F operates. P is a principal homogeneous space for F if there exists a covering $(U_i \to X)_{i \in I}$ (for the f.p.p.f. topology) such that P restricted to this covering is isomorphic to F operating on itself in the usual way. There then exist sections $p_i \in P(U_i)$, and if we define $f_{ij} \in F(U_i \times U_j)$ by the equation $p_i{}^j f_{ij} = p^i{}_j$, where $p_i{}^j$ and $p^i{}_j$ are the images of p_i and p_j under the maps associated by F to the projections $U_i \times_X U_j \to U_i$ and $U_i \times_X U_j \to U_j$, then (f_{ij}) is a Cech 1-cocycle on X_{fl} (for the cover (U_i)) with values in F. In this way, the isomorphism classes of principal homogeneous spaces for F can be identified with the elements of $\check{H}^1(X_{fl}, F) \approx H^1(X, F)$ [6, II]. Note that if F is representable by a scheme affine over X, then P is also representable [10, VII, 2.1].

If G is a sheaf on X_{fl}, we write $\mathrm{Ext}^r_X(G, -)$ for the right derived functors of $\mathrm{Hom}_X(G, -)$. Note that if G and H are representable by group schemes of finite type over X with G flat and affine over X, then $\mathrm{Ext}^1_X(H, G)$ may be identified with the group of equivalence classes of extensions of H by G formed in the category of group schemes of finite type over X [23, III, 17-7]. Also that if X is the spectrum of a field, then the condition that G be affine is unnecessary.

Consider the situation: X is a scheme of finite type over a finite field k, N is a group scheme of finite type over k, and F is a sheaf on X_{fl}. We then denote the algebraic closure of k by $\bar{k}$, the Galois group of $\bar{k}/k$ by Γ, $X \otimes_k \bar{k}$ by $\bar{X}$, $N \otimes_k \bar{k}$ by $\bar{N}$, and the inverse image of F on $\bar{X}$ by $\bar{F}$. If F should be the sheaf on X_{fl} defined by N then $\bar{F}$ is the sheaf on $\bar{X}_{fl}$ defined by $\bar{N}$ [2, III, 2.4]. Γ has a canonical topological generator σ_k, and for any discrete Γ-module M we define M^Γ and M_Γ by the exact sequence

$$0 \to M^\Gamma \to M \xrightarrow{\sigma_k - 1} M \to M_\Gamma \to 0.$$

Thus, if M is torsion, M^Γ and M_Γ equal $H^0(\Gamma, M)$ and $H^1(\Gamma, M)$ respectively. The Leray spectral sequence for the morphism $X_{fl} \to (\mathrm{spec}\, k)_{\mathrm{et}}$ may be written

$$H^r(\Gamma, H^s(\bar{X}, \bar{F})) \Rightarrow H^{r+s}(X, F)$$

and in this form is known as the Hochschild-Serre spectral sequence for $\bar{X}/X$. If F is a torsion sheaf, then the groups $H^s(\bar{X}, \bar{F})$ are torsion, and since Γ has cohomological dimension 1, the spectral sequence reduces to exact sequences

$$0 \to H^{r-1}(\bar{X}, \bar{F})_\Gamma \to H^r(X, F) \to H^r(\bar{X}, \bar{F})^\Gamma \to 0.$$

§ 2. Extensions and Cohomology

Throughout this section k will be a field which is either finite or algebraically closed and X will be a smooth, (geometrically) connected, projective scheme of finite type over k. Then there is a "canonical" k-morphism φ of X into its Albanese variety A which is unique up to translation [13, p. 296]. Let G be a group scheme of finite type over k. An element of $\mathrm{Ext}_k^1(A, G)$ may be represented by an exact sequence of group schemes of finite type over k,

$$0 \to G \to P \xrightarrow{p} A \to 0$$

with p faithfully flat. Then P is a principal homogeneous space for G over A, and the inverse image of this under φ is a principal homogeneous space for G over X. Consequently there is a map $\beta_1(G)$: $\mathrm{Ext}_k^1(A, G) \to H^1(X, G)$ which we wish to extend to all Exts and cohomology groups.

The map $X \to \mathrm{spec}(k)$ induces a map $\mathrm{Ext}_k^r(A, G) \to \mathrm{Ext}_X^r(A, G)$ and φ induces a map $\mathrm{Ext}_X^r(A, G) \to H^r(X, G) \approx \mathrm{Ext}_X^r(\mathbf{Z}, G)$. We define $\beta_r(G)$ to be the composite of these two maps. It is easily seen that the two definitions of $\beta_1(G)$ coincide.

Theorem 1. *Let k be an algebraically closed field and let φ: $X \to A$ be as above. Then $\beta_1(N)$ is injective for all finite group schemes N over k; it is surjective, and $\beta_r(N)$ is injective, for all such group schemes if and only if* (a) *the Néron-Severi group of X is torsion-free and* (b) *the dimension of $H^1(X, O_X)$ as a vector space over k equals the dimension of A; when* (a) *and* (b) *are satisfied then $\beta_1(B)$ is an isomorphism for all abelian varieties B over k.*

Remarks. 1. (b) is equivalent to the Picard scheme of X over k being smooth, which is always the case when k has characteristic 0 [11, 236-16].

2. Any morphism $X \to N$, where N is a finite group scheme over k, is constant, and so $H^0(X, N) = N(k)$, which is an exact functor in N (k being algebraically closed). Hence $H^1(X, N)$ is a left exact functor from the category of finite group schemes over k to the category of abelian groups, and as such must be strictly pro-representable [11, 195, Cor. to 3.1]. The $\mathrm{Ext}_k(-, N)$ sequence of

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

gives an isomorphism $\mathrm{Hom}_k(A_\nu, N) \approx \mathrm{Ext}_k^1(A, N)_\nu$ which, in the limit, reads $\mathrm{Hom}_k(T_p A, N) \approx \mathrm{Ext}_k^1(A, N)(p)$. Thus the theorem may be interpreted as giving necessary and sufficient conditions for $H^1(X, -)(p)$ to be pro-represented by $T_p A$ all p.

3. The β_r form a morphism of connected sequences of functors in G. Also they are functorial in (X, φ) in the sense that if

$$\begin{array}{ccc} X & \xrightarrow{\varphi} & A \\ \downarrow & & \downarrow \\ X' & \xrightarrow{\varphi'} & A' \end{array}$$

commutes, then so also does

$$\begin{array}{ccc} \mathrm{Ext}_k^r(A, G) & \to & H^r(X, G) \\ \uparrow & & \uparrow \\ \mathrm{Ext}_k^r(A', G) & \to & H^r(X', G) \end{array}$$

Proof of Theorem. The canonical map $\mathrm{Ext}_k^1(A, \mathbf{G}_m) \to H^1(A, \mathbf{G}_m) = \mathrm{Pic}(A)$ identifies $\mathrm{Ext}_k^1(A, \mathbf{G}_m)$ with $\mathrm{Pic}^0(A)$, the group consisting of those divisor classes on A which are algebraically equivalent to zero [28, VII, 16]. But φ^*: $H^1(A, \mathbf{G}_m) \to H^1(X, \mathbf{G}_m) = \mathrm{Pic}(X)$ identifies $\mathrm{Pic}^0(A)$ with the group of divisor classes on X which are algebraically equivalent to zero, and so the cokernel of φ^* is $\mathrm{NS}(X)$, the Néron-Severi group of X. Thus $\beta_1(\mathbf{G}_m)$ gives an exact sequence

$$0 \to \mathrm{Pic}^0(A) \xrightarrow{\beta_1} \mathrm{Pic}(X) \to \mathrm{NS}(X) \to 0.$$

$\mathrm{Ext}_k^r(A, \mathbf{G}_m) = 0$ for $r \neq 1$ [23, II, 14-2] so the exact sequence

$$0 \to \boldsymbol{\mu}_n \to \mathbf{G}_m \xrightarrow{n} \mathbf{G}_m \to 0$$

gives rise to an exact commutative diagram

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 \to & & \mathrm{Ext}_k^1(A, \boldsymbol{\mu}_n) & \to & \mathrm{Pic}^0(A) & \xrightarrow{n} & \mathrm{Pic}^0(A) & \to & 0 \\ & & \downarrow{\scriptstyle \beta_1(\boldsymbol{\mu}_n)} & & \downarrow{\scriptstyle \beta_1(\mathbf{G}_m)} & & \downarrow{\scriptstyle \beta_1(\mathbf{G}_m)} & & \downarrow{\scriptstyle \beta_2(\boldsymbol{\mu}_n)} \\ 0 \to & & H^1(X, \boldsymbol{\mu}_n) & \to & \mathrm{Pic}(X) & \xrightarrow{n} & \mathrm{Pic}(X) & \to & H^2(X, \boldsymbol{\mu}_n) \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 \to & & \mathrm{coker}(\beta_1(\boldsymbol{\mu}_n)) & \to & \mathrm{NS}(X) & \xrightarrow{n} & \mathrm{NS}(X) & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array}$$

Hence $\beta_r(\boldsymbol{\mu}_n)$ is injective for all r, and $\beta_1(\boldsymbol{\mu}_n)$ is surjective for all n if and only if (a) holds.

This completes the proof of the first two statements of the theorem when k has characteristic 0 (by [23, II, 6-2]).

Now assume that k has characteristic $p \neq 0$, and let F: $\mathbf{G}_a \to \mathbf{G}_a$ be the Frobenius map of $\mathbf{G}_a$ (relative to the prime field). $\mathrm{Ext}_k^r(A, \mathbf{G}_a) = 0$

for $r \neq 1$ [23, II, 14-2], and $\beta_1(\mathbf{G}_a)$: $\mathrm{Ext}_k^1(A, \mathbf{G}_a) \to H^1(X, O_X)$ is injective [28, VII, 19]. If we let $\boldsymbol{\alpha}_{p^n}$ denote the kernel of F^n: $\mathbf{G}_a \to \mathbf{G}_a$, then we get an exact commutative diagram

$$\begin{array}{ccccccccccc}
0 \to & \mathrm{Ext}_k^1(A, \boldsymbol{\alpha}_{p^n}) & \to & \mathrm{Ext}_k^1(A, \mathbf{G}_a) & \to & \mathrm{Ext}_k^1(A, \mathbf{G}_a) & \to & \mathrm{Ext}_k^2(A, \boldsymbol{\alpha}_{p^n}) & \to & 0 \\
& \downarrow{\scriptstyle \beta_1(\boldsymbol{\alpha}_{p^n})} & & \downarrow{\scriptstyle \beta_1(\mathbf{G}_a)} & & \downarrow{\scriptstyle \beta_1(\mathbf{G}_a)} & & \downarrow{\scriptstyle \beta_2(\boldsymbol{\alpha}_{p^n})} & & \downarrow \\
0 \to & H^1(X, \boldsymbol{\alpha}_{p^n}) & \to & H^1(X, O_X) & \to & H^1(X, O_X) & \to & H^2(X, \boldsymbol{\alpha}_{p^n}) & \to & H^2(X, O_X)
\end{array}$$

Thus $\beta_r(\boldsymbol{\alpha}_{p^n})$ is injective all r, and $\beta_1(\boldsymbol{\alpha}_{p^n})$ is surjective for all n, if and only if the image of $\beta_1(\mathbf{G}_a)$ contains $H^1(X, O_X)_n$, the subspace of $H^1(X, O_X)$ on which F is nilpotent (see [27, p. 38] for the Jordan decomposition of $H^1(X, O_X)$).

The same argument relative to the sequence

$$0 \to \mathbf{Z}/p\,\mathbf{Z} \to \mathbf{G}_a \xrightarrow{1-F} \mathbf{G}_a \to 0$$

shows that $\beta_r(\mathbf{Z}/p\,\mathbf{Z})$ is injective all r, and $\beta_1(\mathbf{Z}/p\,\mathbf{Z})$ is surjective if and only if the image of $\beta_1(\mathbf{G}_a)$ contains $H^1(X, O_X)_s$, the subspace of $H^1(X, O_X)$ on which F is bijective.

But $H^1(X, O_X) = H^1(X, O_X)_s \oplus H^1(X, O_X)_n$ and $\dim_k(\mathrm{Ext}_k^1(A, \mathbf{G}_a)) = \dim(A)$ [28, VII, 17, 21], so $\beta_1(\mathbf{Z}/p\,\mathbf{Z})$ and $\beta_1(\boldsymbol{\alpha}_{p^n})$ are surjective if and only if (b) holds. By [23, II, 6-2], this completes the proof of those parts of the theorem involving only finite group schemes.

Now let k have any characteristic, and let B be an abelian variety over k. By [24], $\mathrm{Ext}_k^r(A, B) = 0$ for $r \geqq 2$. Clearly $\beta_0(B)$: $\mathrm{Hom}_k(A, B) \to B(X)$ is injective with divisible cokernel, so the exact sequence

$$0 \to B_\nu \to B \xrightarrow{p^\nu} B \to 0$$

induces an exact commutative diagram

$$\begin{array}{ccccccc}
0 \to & \mathrm{Hom}_k(A, B)^{(\nu)} & \to & \mathrm{Ext}_k^1(A, B_\nu) & \to & \mathrm{Ext}_k^1(A, B)_\nu & \to 0 \\
& \downarrow{\scriptstyle \approx} & & \downarrow{\scriptstyle \beta_1(B_\nu)} & & \downarrow & \\
0 \to & B(X)^{(\nu)} & \to & H^1(X, B_\nu) & \to & H^1(X, B)_\nu & \to 0
\end{array}$$

Since $\mathrm{Ext}_k^1(A, B)$ is torsion, this shows that $\beta_1(B)$ is always injective, and is surjective if $\beta_1(B_\nu)$ is surjective all ν, i.e. if (a) and (b) hold.

Corollary 1. *For any abelian variety A over an algebraically closed field k, and any finite group scheme N over k, the canonical map* $\mathrm{Ext}_k^1(A, N) \to H^1(A, N)$ *is an isomorphism.*

Proof. An abelian variety satisfies (a) and (b) and is its own Albanese variety.

This corollary may be restated as: any scheme P over A which is a principal homogeneous space for the group scheme N can be given a group structure in such a way that the sequence $0 \to N \to P \to A \to 0$ is exact and induces on P its original N-operation. In particular, if P is reduced and irreducible it is an abelian variety and $P \to A$ is an isogeny. In this form, the statement was first proved by Lang and Serre [16] for N étale and by Miyanishi [19] for N arbitrary.

Corollary 2. *In the situation of the theorem,* $\varphi^*: H^1(A,N) \to H^1(X,N)$ *is an isomorphism for all finite group schemes N over k if and only if X satisfies* (a) *and* (b) (cf. [28, VI, 20]).

Proof. Combine Cor. 1 with the Theorem.

We now consider the case of a finite k, and we use the notation introduced in § 1. If N is a finite group scheme over k then we define $H^1_g(X,N)$, the group of "geometric" principal homogeneous spaces for N over X, to be the image of $H^1(X,N)$ in $H^1(\bar X,\bar N)$. Note that the Hochschild-Serre spectral sequence for $\bar X/X$ gives an exact sequence

$$0 \to N(\bar k)_\Gamma \to H^1(X,N) \to H^1(\bar X,\bar N)^\Gamma \to 0$$

so $H^1_g(X,N) \approx H^1(\bar X,\bar N)^\Gamma$, or again, $H^1_g(X,N) \approx H^1(X,N)/H^1(\Gamma, N(\bar k))$. Notice that $H^1_g(X,N)$ is a left exact functor from the category of finite group schemes over k to the category of abelian groups. We write $\gamma_1(N)$ for the composite of $\beta_1(N)$: $\mathrm{Ext}^1_k(A,N) \to H^1(X,N)$ with the surjection $H^1(X,N) \to H^1_g(X,N)$.

Corollary 3. *If* $\varphi: X \to A$ *is as in the first paragraph, k is finite, and $\bar X$ satisfies conditions* (a) *and* (b) *of Theorem* 1, *then*

$$\gamma_1(N):\ \mathrm{Ext}^1_k(A,N) \to H^1_g(X,N)$$

is an isomorphism for all finite group schemes N over k. Moreover, for any abelian variety B over k, $\beta_1(B)$: $\mathrm{Ext}^1_k(A,B) \to H^1(X,B)$ *is an isomorphism.*

Proof. There is a commutative diagram

$$\begin{array}{ccc} \mathrm{Ext}^1_k(A,N) & \xrightarrow{\approx} & \mathrm{Ext}^1_{\bar k}(\bar A,\bar N)^\Gamma \\ \downarrow{\scriptstyle \gamma_1(N)} & & {\scriptstyle\approx}\downarrow{\scriptstyle \beta_1(\bar N)} \\ H^1_g(X,N) & \xrightarrow{\approx} & H^1(\bar X,\bar N)^\Gamma \end{array}$$

The top arrow may be seen to be an isomorphism by observing that there is a Γ-isomorphism

$$\mathrm{Ext}^1_{\bar k}(\bar A,\bar N) \approx \mathrm{Hom}_{\bar k}(T_p\bar A,\bar N) \quad \text{and} \quad \mathrm{Hom}_{\bar k}(\bar A_\nu,\bar N)^\Gamma \approx \mathrm{Hom}_k(A_\nu,N).$$

To prove the last statement of the corollary, we observe first that there is an isomorphism

$$\gamma_1\colon \operatorname{Ext}^1_k(A, B(p)) \to \varinjlim H^1_g(X, B_\nu).$$

But, in the limit,

$$0 \to H^1(\Gamma, B_\nu(\bar{k})) \to H^1(X, B_\nu) \to H^1_g(X, B_\nu) \to 0$$

reads

$$0 \to H^1(\Gamma, B(\bar{k})(p)) \to H^1(X, B(p)) \to H^1_g(X, B(p)) \to 0.$$

By [28, VI, 4], $H^1(\Gamma, B(\bar{k}))=0$, so $H^1(X, B(p)) \approx H^1_g(X, B(p))$ and the result follows.

Finally we observe that if K is a function field in one variable with finite field of constants k, then there exists a smooth, connected, projective, algebraic curve X over k with function field K, and $\bar{X}$ is automatically connected and satisfies conditions (a) and (b) of Thm. 1.

§ 3. The Tate-Šafarevič Group

If we combine Cor. 3 of the last section with Thm. 3 of [18], we get the following result.

Theorem 2. *Let X be a smooth, geometrically connected, projective scheme over a finite field k of q elements and assume that $\bar{X}=X\otimes_k \bar{k}$ satisfies conditions* (a) *and* (b) *of Thm.* 1. *If B is an abelian variety over k, then $H^1(X,B)$ is finite, and its order $[H^1(X,B)]$ satisfies the relation*

$$q^{d(A)\,d(B)} \prod_{a_i \neq b_j} \left(1-\frac{a_i}{b_j}\right) = [H^1(X,B)]\,|\det\langle \alpha_i, \beta_j\rangle|$$

where A is the Albanese variety of X, $d(A)$ and $d(B)$ are the dimensions of A and B, $(a_i)_{1\le i\le 2d(A)}$ and $(b_i)_{1\le i\le 2d(B)}$ are the roots of the characteristic polynomials of the Frobenius endomorphisms of A and B relative to k, $(\alpha_i)_{1\le i\le r}$ and $(\beta_i)_{1\le i\le r}$ are bases for $\operatorname{Hom}_k(A,B)$ and $\operatorname{Hom}_k(B,A)$, and $\langle \alpha_i, \beta_j\rangle$ is the trace of the endomorphism $\beta_j\alpha_i$ of A.

For the remainder of this section we assume that X is the curve associated to a function field K as in the last paragraph of § 2, and that A, B, etc. are as in the above theorem. For any prime v of K (equivalently, any closed point of X) we write K_v for the completion of K at v.

Our aim is to relate $H^1(X,B)$ to $\text{Ш}(B/K)$ and $\det\langle\alpha_i,\beta_j\rangle$ to the determinant of the Néron-Tate height pairing $B(K)\times\hat{B}(K)\to\mathbf{R}$ in such a way as to deduce the special case of the conjecture of Birch and Swinnerton-Dyer.

Lemma 1. *For any abelian scheme $\mathcal{B}$ over X, there is an exact sequence*

$$0 \to H^1(X,\mathcal{B}) \to H^1(\operatorname{spec}(K), \mathcal{B}_K) \to \oplus_v H^1(\operatorname{spec}(K_v), \mathcal{B}_{K_v})$$

i.e. $H^1(X,\mathcal{B}) = \text{Ш}(\mathcal{B}_K/K)$, *the Tate-Šafarevič group of $\mathcal{B}_K$ over K.*

Proof. Since $\mathscr{B}$ is by definition smooth, we may work with the étale topology. Let π: spec$(K)\to X$ be the inclusion of the generic point of X. For any étale morphism $U\to X$,

$$\operatorname{Mor}_K(U_K,\mathscr{B}_K)\approx\operatorname{Mor}_X(U_K,\mathscr{B})\approx\operatorname{Mor}_X(U,\mathscr{B}) \qquad [9, \text{II}, 7.3.6]$$

so the sheaf defined by $\mathscr{B}$ on X_{et} is isomorphic to $\pi_*\mathscr{B}_K$.

By [6, IV, § 3] the principal homogeneous spaces for $\mathscr{B}$ over X may be canonically identified with the principal homogeneous spaces for $\mathscr{B}_K$ over K which are split by the inverse image (under π) of some étale cover of X, or equivalently, which have a point in $\tilde{K}_v$ all v, where $\tilde{K}_v$ is the field of fractions of the strictly local ring $\tilde{R}_v$ of X at v (in an older terminology, $\tilde{K}_v$ is a maximal unramified extension of K at v). Thus there is an exact sequence

$$0\to H^1(X,\mathscr{B})\to H^1(\operatorname{spec}(K),\mathscr{B}_K)\to\oplus_v H^1(\operatorname{spec}(\tilde{K}_v),\mathscr{B}_{\tilde{K}_v})$$

(this can also be derived using the Leray spectral sequence of π).

A principal homogeneous space for A over $\tilde{K}_v$ may be represented by a projective scheme P over $\tilde{K}_v$ [34], [9, IV, 2.7.1], so there exists a projective scheme P' over $\tilde{R}_v$ such that $P\approx P'\otimes_{\tilde{R}_v}\tilde{K}_v$. Let $t\tilde{R}_v$ be the maximal ideal of $\tilde{R}_v$,

$$\hat{R}_v=\varprojlim_n \tilde{R}_v/t^n\tilde{R}_v$$

the completion of $\tilde{R}_v$, and $\hat{K}_v$ the field of fractions of $\hat{R}_v$. From [8, Cor. 2 to Thm. 1] and [9, II, 7.3.8] one sees that the following assertions are equivalent: P has a point in $\tilde{K}_v$; P' has a point in $\tilde{R}_v$; P' has a point in $\tilde{R}_v/t^n\tilde{R}_v=\hat{R}_v/t^n\hat{R}_v$ for all sufficiently large n; P' has a point in $\hat{R}_v$; P has a point in $\hat{K}_v$. Thus the sequence above remains exact if $\tilde{K}_v$ is replaced by $\hat{K}_v$.

Finally, the canonical maps $H^1(\operatorname{spec}(K_v),\mathscr{B}_{K_v})\to H^1(\operatorname{spec}(\hat{K}_v),\mathscr{B}_{\hat{K}_v})$ are injective [7, p. 265], so $\hat{K}_v$ in the sequence may be replaced by K_v, and the lemma is proved.

Thus, in Thm. 2, $H^1(X,B)$ may be replaced by $Ш(B/K)$ (when X is a curve).

If v is a prime of K, then we write ord_v for the corresponding additive valuation of K which maps K^* onto Z. Let

$$(\ ,\ )=\sum_v(\ ,\ )_v$$

be the pairing $B(K)\times\hat{B}(K)\to\mathbf{R}$ which corresponds, as described in [21, II, 12] to these valuations. (There is a confusion of signs here which we may safely disregard.)

Let γ: $\operatorname{Hom}_k(A,B)\to B(K)$ be the composite of φ^*: $\operatorname{Hom}_k(A,B)\to B(X)$ with π^*: $B(X)\to B(K)$ and similarly (noting that there is an isomorphism $A\approx\hat{A}$, which is canonical) let γ': $\operatorname{Hom}_k(B,A)\to\hat{B}(K)$ be the composite of

$$\operatorname{Hom}_k(B,A)\to\operatorname{Hom}_k(\hat{A},\hat{B})\xrightarrow{\varphi^*}\hat{B}(X)\xrightarrow{\pi^*}\hat{B}(K).$$

Lemma 2. *Let* $\alpha\in\operatorname{Hom}_k(A,B)$ *and* $\beta\in\operatorname{Hom}_k(B,A)$. *Then the trace* $\langle\alpha,\beta\rangle$ *of* $\beta\alpha$ *as an endomorphism of* A *is equal to* $(\gamma(\alpha),\gamma'(\beta))$.

Proof. We may replace k by its algebraic closure since this affects neither the height nor the trace.

We give all schemes Y over k base points p_Y (the base point of an abelian variety is its zero, and the base point of X is $\varphi^{-1}(p_A)$). A divisorial correspondence on $Y\times Z$ is an element $\delta\in\operatorname{Pic}(Y\times Z)$ which is zero on $Y\times\{p_Z\}$ and $\{p_Y\}\times Z$.

Let δ_1 be the divisorial correspondence on $X\times A$ such that

$$(1_X\times\varphi)^*(\delta_1)=\operatorname{class}(\Delta-X\times\{p_X\}-\{p_X\}\times X),$$

where Δ is the diagonal of $X\times X$, and let $\eta=(1_X\times\beta)^*(\delta_1)$, which is a divisorial correspondence on $X\times B$ (cf. [20]). Then $\beta\alpha$: $A\to A$ corresponds to the divisorial correspondence $(1_X\times\alpha\varphi)^*(\eta)$ on $X\times X$, so [14, VI, § 3, Thm. 6],

$$\langle\alpha,\beta\rangle=\deg\big((1_X\times\alpha\varphi)^*(\eta)\cdot\Delta\big)=\deg\big(\alpha_1^*(\eta)\big)$$

where $\alpha_1: X\to X\times B$ is the map defined by 1_X and $\alpha\varphi$. But if η is written as a Cartier divisor, and $\deg(\alpha_1^*(\eta))$ is written as a sum of local terms $\sum n_v$, then it is easily seen that $n_v=i_v(\gamma(\alpha),\gamma'(\beta))$ with i_v as in [21, III, 2]. But

$$(\gamma(\alpha),\gamma'(\beta))=\sum_v i_v(\gamma(\alpha),\gamma'(\beta))$$

[21, III, 2, Thm. 3], so the lemma is proved. (Alternatively, one may use [15, Prop. 4] to relate the trace directly to Tate's definition of the height pairing.)

If we combine Thm. 2 with Lemmas 1 and 2, and observe that γ and γ' are isomorphisms modulo torsion, then we get the following result.

Theorem 3. *Let* K *be a function field in one variable with finite field of constants* k, *and let* B *be a constant abelian variety over* K. *Then the Tate-Šafarevič group of* B *over* K *is finite and its order* $[\text{Ш}(B/K)]$ *satisfies the relation*

$$q^{gd}\prod_{a_i\neq b_j}\left(1-\frac{a_i}{b_j}\right)=[\text{Ш}(B/K)]\,|\det(p_i,p_j')|$$

where q is the number of elements of k, g is the genus of K/k, d is the dimension of B, $(a_i)_{1\leqq i\leqq 2g}$ and $(b_i)_{1\leqq i\leqq 2d}$ are the roots of the characteristic polynomials of the Frobenius endomorphisms of A and B relative to k (where A is the Jacobian of a smooth, projective model X/k for K), $(p_i)_{1\leqq i\leqq r}$ and $(p'_i)_{1\leqq i\leqq r}$ are bases for $B(K)$ and $\hat{B}(K)$ modulo torsion, and $(\ ,\ )$: $B(K)\times\hat{B}(K)\to\mathbf{R}$ is the height pairing described above.

For the convenience of the reader, we give the formalism which relates the above theorem to the form of the conjecture of Birch and Swinnerton-Dyer given in [30, Conj. (B)]. We use essentially the same notation as in [30, § 1].

Choose for each prime v of K a Haar measure μ_v on K_v such that $\mu_v(R_v)=1$ if R_v is the ring of integers of K_v. Choose a non-zero invariant differential form ω of degree d on B defined over k. Then v is "good" for ω and μ for all v. Hence

$$L^*(s)=|\mu|^d\, L(s)=|\mu|^d\prod_v \frac{1}{P_v(N_v^{-s})}.$$

$|\mu|$ is the measure of the quotient by K of the adèle ring of K, relative to the measure

$$\mu=\prod_v \mu_v.$$

This is easily seen to equal q^{g-1}.

Clearly also

$$P_v(T)=\prod_{i=1}^{2d}(1-b_i^{\deg(v)}T) \quad\text{and}\quad N_v=q^{\deg(v)}.$$

By comparing the expression (valid for $\mathrm{Re}(s)>\frac{3}{2}$)

$$L(s)=\prod_v\prod_{i=1}^{2d}\frac{1}{(1-b_i^{\deg v}q^{-(\deg v)s})}=\prod_{i=1}^{2d}\prod_v\frac{1}{(1-b_i^{\deg v}q^{-(\deg v)s})}$$

with the known expressions for the zeta function of X,

$$Z(X,T)=\frac{\prod_{i=1}^{2g}(1-a_i T)}{(1-T)(1-qT)}=\prod_v\left(\frac{1}{1-T^{\deg(v)}}\right)$$

we get a rational expression for $L(s)$,

$$L(s)=\prod_{j=1}^{2d}\prod_{i=1}^{2g}\frac{(1-a_i b_j q^{-s})}{(1-b_j q^{-s})(1-b_j q^{1-s})}=\prod_{j=1}^{2d}\prod_{i=1}^{2g}\frac{\left(1-\frac{a_i}{b_j}q^{1-s}\right)}{(1-b_j q^{-s})(1-b_j q^{1-s})}.$$

Thus the order of the zero of $L(s)$ at $s=1$ is equal to the number of pairs (i, j) such that $a_i = b_j$. But by [31, Thm. 1a], this last number is equal to r, the rank of $B(K)$. It is now easy to show that

$$\lim_{s\to 1} \frac{L(s)}{(s-1)^r} = \frac{q^d (\log q)^r}{[B(k)]^2} \prod_{a_i \neq b_j} \left(1 - \frac{a_i}{b_j}\right).$$

But $[B(K)_{\mathrm{tors}}] = [B(k)] = [\hat{B}(K)_{\mathrm{tors}}]$, and our height pairing is $\log q$ of the height pairing in [30], so the statement of [30, Conj. (B)] reduces, in this particular case, to Thm. 3.

Corollary. *Let Y be the product of two smooth, projective, connected, algebraic curves X_1 and X_2 over a finite field k. Then the Brauer group of Y is finite and its order satisfies the relation conjectured in* [30, (C)].

Proof. By [30, (d)] we know that the corollary is equivalent to Thm. 3 with B equal to the Jacobian of the generic fibre of the projection $X_1 \times_k X_2 \to X_1$.

In special cases this gives the order of the Brauer group of $X_1 \times_k X_2$ very explicitly. For example, if X_1 and X_2 are non-isogenous elliptic curves with n_1 and n_2 k-rational points respectively, then the Brauer group of $X_1 \times_k X_2$ has $(n_1 - n_2)^2$ elements; if $X_1 = X = X_2$ is a non-supersingular elliptic curve, then the Brauer group of $X_1 \times_k X_2$ has $(\mathrm{End}_k(X) : \mathbf{Z}[F_k])^2$ elements, where F_k is the Frobenius endomorphism of X relative to k.

§ 4. Further Remarks and Corollaries

(1) Let X, K, A, and B be as in Thm. 3, but now suppose that k is algebraically closed. It is easy to derive an exact sequence

$$0 \to \mathrm{Hom}_k(A, B) \otimes \mathbf{Z}_p \to \mathrm{Hom}_k(T_p A, T_p B) \to T_p(\mathrm{Ext}^1_k(A, B)) \to 0$$

and we have seen (Thm. 1) that $\mathrm{Ext}^1_k(A, B) \approx H^1(X, B)$. The argument of Lemma 1 implies that $H^1(X, B) \approx Ш(B/K)$, so there is an exact sequence

$$0 \to \mathrm{Hom}_k(A, B) \otimes \mathbf{Z}_p \to \mathrm{Hom}_k(T_p A, T_p B) \to T_p(Ш(B/K)) \to 0.$$

Thus $r + r_0 = \mathrm{rank}_{\mathbf{Z}_p}(\mathrm{Hom}_k(T_p A, T_p B))$ where $r = \mathrm{rank}_{\mathbf{Z}}(B(K))$ and r_0 is the corank of the p-divisible part of $Ш(B/K)$. In particular, if $p \neq$ characteristic of k, then $r + r_0 = 4dg$ where d is the dimension of B and g the genus of X. Thus we recover the formula of Ogg-Šafarevič [22], [26], [25, Thm. 3(ii)] in this special case, but when $p =$ characteristic of k $\mathrm{rank}_{\mathbf{Z}_p}(\mathrm{Hom}_k(T_p A, T_p B)) \neq 4dg$. This suggests that there should be some more general formula for the corank of the p-divisible part of Ш(B/K), holding for all B, and valid for all primes p.

(2) Thm. 3 implies that the Tate-Šafarevič group of any abelian variety B over a function field K (in one variable over a finite field), which becomes constant after a finite Galois extension L/K, is finite. Indeed, even $H^1(\mathrm{Gal}(L/K), B(L))$ is finite because, by the Mordell-Weil theorem, $B(L)$ is finitely generated.

(3) In the situation of Thm. 3, we have Ш$(B/K) \approx \mathrm{Ext}_k^1(A, B)$ and Ш$(\hat{B}/K) \approx \mathrm{Ext}_k^1(A, \hat{B})$ which, by the autoduality of the category of abelian varieties over k, is isomorphic to $\mathrm{Ext}_k^1(B, A)$. But by [18, Thm. 2], $\mathrm{Ext}_k^1(A, B)$ is dual to $\mathrm{Ext}_k^1(B, A)$ so, for constant abelian varieties, Ш(B/K) is dual to Ш$(\hat{B}/K)$. This extends the duality of Cassels-Tate [29, Thm. 3.2] to all p-primary components of Ш(B/K) and Ш$(\hat{B}/K)$ (when B is constant).

(4) Let X be a smooth, projective, geometrically connected, algebraic curve over a finite field k. Grothendieck and Verdier [32] have shown that if the characteristic of k does not divide n, then the cup product defines a duality

$$H^r(X, \mu_n) \times H^{3-r}(X, \mu_n) \to H^3(X, \mathbf{G}_m) \approx \mathbf{Q}/\mathbf{Z}.$$

By combining Cor. 4 to Thm. 1 with [18, Lemma 3] and with a result from the author's thesis, one gets that there is a duality

$$H^r(X, N) \times H^{3-r}(X, N') \to \mathbf{Q}/\mathbf{Z}$$

for all finite group schemes N over k (where N' denotes the Cartier dual of N). (But when $N = \alpha_p$ it is not clear how to interpret our pairing in cohomological terms.) We would expect in fact that the cup product will define a duality

$$H^r(X, N) \times H^{3-r}(X, N') \to H^3(X, \mathbf{G}_m) \approx \mathbf{Q}/\mathbf{Z}$$

for all quasi-finite flat group schemes N over X.

It should be noted however that the expected analogue of this duality when k is algebraically closed, viz

$$H^r(X, N) \times H^{2-r}(X, N') \to H^2(X, \mathbf{G}_m(p)) \approx \mathbf{Q}_p/\mathbf{Z}_p$$

(N p-primary) is false in general. For $H^0(X, \alpha_p) = 0$ whereas

$$H^2(X, \alpha_p) = \mathrm{coker}(F\colon H^1(X, O_X) \to H^1(X, O_X))$$

is zero if and only if the Jacobian of X has its maximum number of points of order p.

References

1. Artin, M.: Grothendieck topologies, Lecture notes, Harvard 1962.
2. –, et A. Grothendieck: Cohomologie étale des schémas. Séminaire de Géométrie Algébrique de l'I.H.E.S. 1963/64.
3. Birch, B., and H. Swinnerton-Dyer: Notes on elliptic curves (II). J. reine u. angew. Math. **218**, 79–108 (1965).
4. Cassels, J.: Diophantine equations with special reference to elliptic curves. Journ. London Math. Soc. **41**, 193–291 (1966).
5. Demazure, M., et A. Grothendieck: Schémas en groupes. Séminaire de Géometrie Algébrique de l'I.H.E.S. 1962/64.
6. Giraud, J.: Cohomologie non-abélienne. Columbia University, 1966.
7. Greenberg, M.: Schemata over local rings II. Ann. of Math. **78**, 256–266 (1963).
8. – Rational points in henselian discrete valuation rings. Publ. Math. **31**, 59–64 (1966).
9. Grothendieck, A., et J. Dieudonné: Elements de géométrie algébrique. Publ. Math. (1959).
10. – Séminaire de géométric algébrique de l'I.H.E.S., 1960/61.
11. – Fondements de la géométrie algébrique. Paris: Secrétariat Mathématique, 11 rue Pierre Curie 1962.
12. – Le groupe de Brauer III: Examples et complements, mimeographed notes, I.H.E.S., 1966.
13. Lang, S.: Unramified class field theory over function fields in several variables. Annals of Math. **64** (2), 285–325 (1956).
14. – Abelian varieties. Interscience Tracts, no. 7. New York: Interscience 1959.
15. –, and A. Néron: Rational points of abelian varieties in function fields. Amer. J. Math. **81**, 95–118 (1959).
16. –, et J.-P. Serre: Sur les revêtements non ramifiés des variétés algébriques. Amer. J. Math. **79**, 319–330 (1957).
17. –, and J. Tate: Principal homogeneous spaces over abelian varieties. Amer. J. Math. **80**, 659–684 (1958).
18. Milne, J.: Extensions of abelian varieties defined over a finite field. Inventiones math. **5**, 63–84 (1968).
19. Miyanishi, M.: On the pro-representability of a functor on the category of finite group schemes. J. Math. Kyoto **6**, 31–48 (1966).
20. Mumford, D.: A remark on Mordell's conjecture. Amer. J. Math. **87**, 1007–1016 (1965).
21. Néron, A.: Quasi-functions et hauteurs sur les variétés abéliennes. Ann. of Math. **82**, 249–331 (1965).
22. Ogg, A.: Cohomology of abelian varieties over function fields. Ann. of Math. (2) **76**, 185–212 (1962).
23. Oort, F.: Commutative group schemes. Lecture notes in Math. 15. Berlin-Heidelberg-New York: Springer 1966.
24. –, and T. Oda: Higher extensions of abelian varieties. Nagoya Math. J. **31**, 81–88 (1968).
25. Raynaud, M.: Caractéristique d'Euler-Poincaré d'un faisceau et cohomologie des variétés abéliennes. Séminaire Bourbaki 1964/65, no. 286, 19 pp.
26. Šafarevič, I.: Principal homogeneous spaces defined over a function field. Amer. Math. Soc. Transl. (2), **37**, 85–114 (1964).
27. Serre, J.-P.: Sur la topologie des variétés algébriques en caracteristique *p*. Symposium Internacional de Topologia Algebrica, Mexico, 1956.
28. – Groupes algébriques et corps de classes. Paris: Hermann 1959.
29. Tate, J.: Duality theorems in galois cohomology over number-fields. Proc. Intern. Congress Math. Stockholm, 1962, 288–295.

30. Tate, J.: On the conjectures of Birch and Swinnerton-Dyer and a geometric analogue. Seminaire Bourbaki 1965/66, no. 306.
31. – Endomorphisms of abelian varieties over finite fields. Inventiones math. **2**, 134–144 (1966).
32. Verdier, J.: A duality theorem in the étale cohomology of schemes: Proceedings of a conference on local fields. Berlin-Heidelberg-New York: Springer 1967.
33. Weil, A.: On algebraic groups and homogeneous spaces. Amer. J. Math. **77**, 497–512 (1955).
34. – The field of definition of a variety. Amer. J. Math. **78**, 509–524 (1956).

Dr. J. S. Milne
Department of Mathematics
University College London
Gower Street
London, W.C. 1 (England)

(Received April 9, 1968)