The Conjectures of Birch and Swinnerton-Dyer for Constant Abelian Varieties over Function Fields

A thesis presented

by

James Stuart Milne

to

The Department of Mathematics

in partial fulfillment of the requirements

for the degree of

Doctor of Philosophy

in the subject of

Mathematics

Harvard University

Cambridge, Massachusetts

May 1967

Table of Contents

Introduction

Let X be a complete, connected, smooth, algebraic curve over a finite field k, and let K be the function field of X. . Any abelian variety A over K comes from an abelian scheme over the complement in X of a finite set S of closed points of X. Define

$$L_S(s) = \prod_v \frac{1}{P_v((Nv)^{-s})} \qquad (v \in X - S,\ v \text{ closed})$$

where Nv is the number of elements in the residue field k(v) of X at v and $T^{2d}\ P_v(T^{-1})$ is the characteristic polynomial of the Frobenius endomorphism of the fibre A_v relative to k(v). Assume that $L_S(s)$ can be meromorphically continued over the whole s-plane. Then the first conjecture of Birch and Swinnerton-Dyer for this situation is

(A) $L_S(s)$ has a zero at $s = 1$ of order r equal to the rank of the group A(K) of K-rational points of A.

When A is a constant abelian variety, i.e., is defined over k, then this conjecture is an immediate consequence of the results of Tate in [37]. (For the connection, see the final part of the proof of our Theorem 3.)

Birch and Swinnerton-Dyer define another function $L^*(s)$ by an infinite product which differs from the above in only finitely many factors, but which takes account of the behaviour of A at the points of S. Their second conjecture is

$$(B) \qquad L^*(s) \sim \frac{[\text{Ш}]\,|\det\langle a_i', a_j\rangle|}{[A(K)_{\text{tors}}][A^t(K)_{\text{tors}}]}(s-1)^r \quad \text{as} \quad s \longrightarrow 1,$$

where $[\text{Ш}]$ is the order of the Tate-Šafarevič group of A over K, A^t is the dual abelian variety to A, $[A(K)_{\text{tors}}]$ is the order of the torsion part of $A(K)$, $(a_i)_{1\leq i\leq r}$ are bases for $A(K)$ and $A^t(K)$ respectively modulo torsion, and $\langle a_i', a_j\rangle$ is the value of the Néron-Tate height function at the pair a_i', a_j (for more details, discussion, and other references, see [35 §1]).

This conjecture (B) is related to a conjecture of Artin and Tate for the Brauer group of a surface [35,(C)], and their results [35, Theorem 5.2] imply the following statement about (B). Let p be the characteristic of k and $\text{Ш}(\text{non } p)$ the direct sum of the ℓ-primary components of Ш for primes $\ell \neq p$. Then $\text{Ш}(\text{non } p)$ is finite and

$$L^*(s) \sim \frac{p^{\nu}[\underline{|||}(\text{non } p)]\left|\det \langle a_i', a_j\rangle\right|}{[A(K)_{\text{tors}}][A^t(K)_{\text{tors}}]}\,(s-1)^r \text{ as } s \longrightarrow 1,$$

for some integer ν if A is the Jacobian (in particular) of a complete, connected, smooth, algebraic curve defined over k.

Our main result here extends this last statement by proving that conjecture (B) holds for all constant abelian varieties A over K. In particular, this shows that there do exist abelian varieties, at least over function fields, whose Tate-Šafarevič group is finite.

Our approach differs from that of Artin and Tate in that we work directly with the conjecture as stated above and not with the analogue for surfaces. Thus our results are not restricted to Jacobians. Also we use flat cohomology as distinct from étale, and so get information about the "p-part" of the conjecture. It should be noted however that both methods make use of the results of Tate [37], i.e., essentially the first conjecture.

The Tate-Šafarevič group of a constant abelian variety may be interpreted as a certain flat cohomology group, $H^1(X_{fl}, A)$ (§6, Prop. 3). This group is approached via the cohomology groups $H^1(X, A_\nu)$, where A_ν is the kernel of multiplication by p^ν on A. After some preliminaries in §1, a method of representing such cohomology groups in terms of extensions of pro-finite group schemes is given in §2. These extensions, in turn, may be interpreted as extensions of modules over a certain ring (§4), and in §5 we use this interpretation to compute the order of some extension (hence cohomology) groups. In §3, it is shown that the Néron-Tate height pairing may be interpreted cohomologically as a cup product. The Appendix contains two duality theorems. In §6 we use all these results to prove a special case of conjecture (B).

The above remarks are subject to one proviso, viz. that theorem A2 of the Appendix is, at present, not yet completely proven. However, this theorem is used only in §6, and the reader will have no difficulty verifying that the following statement has been completely proved. The Tate-Šafarevič group of any constant abelian variety A over K is finite, conjecture (B) is true for A apart possibly for a power of the characteristic of K, and is exactly true in the generic case when either A or the Jacobian of X has its maximum number of points of order p.

I would like to express my gratitude to Professor J. Tate for his generous encouragement and ready assistance during my work on this thesis. Also I would like to thank Professor F. Oort for several valuable conversations.

1. Preliminaries

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 $(U_i \longrightarrow U)_{i \in I}$ of flat morphisms, locally of finite presentation) and X_{et} denotes the same category with its étale topology [4,IV 6.3][3,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, Appendix] that if the sheaf G on X_{fl} is representable by a smooth group scheme on X, then the canonical maps $H^r(X_{et}, G) \longrightarrow H^r(X,G)$ are isomorphisms. Thus the computations of the cohomology of the multiplicative group $\mathbb{G}_m$ with respect to the étale topology made in [12,2] and [2, Chapter IV] (e.g., $H^1(X_{et},\mathbb{G}_m) \approx \mathrm{Pic}(X)$) hold equally for the f.p.p.f topology. Also [3, VII 4.3], if F is a quasi-coherent O_X-module (in the usual sense of 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

$H^r(X,W(F)) \approx H^r(X_{Zar}, F)$. In particular, if $\mathbb{G}_a$ is the additive group, then $H^r(X,\mathbb{G}_a) \approx H^r(X_{Zar},O_X)$.

We make the convention that all group schemes are to be commutative. If G and H are group schemes over a scheme X, we distinguish the set of morphisms of X-schemes G to H from the set of group homomorphisms by denoting the former as H(G) or $Mor_X(G,H)$ and the latter as $Hom_X(G,H)$.

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 $(U_i \longrightarrow X)_{i\in I}$ (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 $f_{ij} \in F(U_i \times_X U_j)$ 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 $U_i \times_X U_j \longrightarrow U_i$ and $U_i \times_X U_j \longrightarrow U_j$, then (f_{ij}) is a Čech 1-cocycle on X_{fl} with values in F. In this way, the isomorphism classes of principal homogeneous spaces for F are 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 [9, VIII 2.1]. Similarly if G and H are group schemes of finite type over X and G is flat and affine over X, then the group $\mathrm{Ext}_X^1(H,G)$ formed in the category of sheaves over X_{fl} can 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 [26, III.17-7]. This identification cannot be made for the higher Exts. If X is not the spectrum of a field, then $\mathrm{Ext}_X^r(H,G)$ is to be interpreted as extensions of sheaves, whereas if k is a field then $\mathrm{Ext}_k^r(H,G)$ is to be interpreted as extensions of algebraic group schemes over k (or of pro-algebraic or ind-algebraic group schemes if G and H should be such). There are various ambiguities of sign depending on whether $\mathrm{Ext}^r(-,-)$ is defined by means of Yoneda extensions or injective or projective resolutions [19, VII 7]. These we disregard because they do not affect our results.

The Cartier dual of a finite flat group scheme N (over a noetherian scheme) is denoted by N^D. If $G = (G_\nu, i_\nu)$ is a p-divisible group [32],[36], then $G^t = (G_\nu^D, j_\nu^D)$ is its dual and $T_pG = (G_\nu, j_\nu)$ its associated pro-p-group, where

j_ν is the unique homomorphism $G_{\nu+1} \longrightarrow G_\nu$ such that $j_\nu \circ i_\nu = p$. We define the cohomology of a p-divisible group and its associated pro-p-group by

$$H^r(X,G) = \varinjlim_{\nu} H^r(X,G_\nu), \quad H^r(X,T_pG) = \varprojlim_{\nu} H^r(X,G_\nu) .$$

μ_n, $\nu_n(= \mathbb{Z}/n\mathbb{Z})$ and α_p denote the usual finite group schemes [26, I.2]. A finite group scheme N (and consequently a p-divisible group) over a perfect field k can be written uniquely as $N = N_{ee} \oplus N_{ec} \oplus N_{ce} \oplus N_{cc}$ where N_{ec} is the component of N which is étale with connected dual, etc.

If A is an abelian variety then $A(p) = (A_\nu, i_\nu)$ is its associated p-divisible group and $T_pA = T_p(A(p))$ its associated pro-p-group. Note that if the ground field has characteristic $\neq$ p then this last notation agrees with the usual notation [15,VII] (at least up to an equivalence of categories), but if p is the characteristic then T_pA has sometimes been used to denote what is essentially the étale part of the T_pA of our notation.

If C is an abelian group, then ${}_nC$ and $C^{(n)}$ denote respectively the kernel and cokernel of multiplication by n on C, and, for any prime p, $T_pC = \varprojlim_{\nu} p^{\nu} C$ and $C(p)$ = the p-primary component of C.

Consider the situation: X is an algebraic scheme over a finite field k, N an algebraic group scheme over k, and F a sheaf on X_{fl}. We then denote the algebraic closure of k by $\overline{k}$, the Galois group of $\overline{k}/k$ by Γ, $X \otimes_k \overline{k}$ by $\overline{X}$, $N \otimes_k \overline{k}$ by $\overline{N}$, and the inverse image of F on $\overline{X}$ by $\overline{F}$. If F should be the sheaf on X_{fl} defined by N then $\overline{F}$ is the sheaf on $\overline{X}_{fl}$ defined by $\overline{N}$ [3, 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

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

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 $X_{fl} \longrightarrow (\text{spec } k)_{et}$ may be written

$$H^r(\Gamma, H^s(\overline{X},\overline{F})) \Longrightarrow H^{r+s}(X,F)$$

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

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

2. Extensions and Cohomology

Let X be a regular, connected, projective algebraic scheme over an algebraically closed field k, let $\varphi: X \longrightarrow A$ be the canonical morphism of X into its Albanese variety, and let N be an affine algebraic group scheme over k. An exact sequence

$$(2.1) \qquad 0 \longrightarrow N \longrightarrow P \longrightarrow A \longrightarrow 0$$

of algebraic group schemes over k with $P \longrightarrow A$ flat defines on P the structure of a principal homogeneous space over A with respect to the group N. The inverse image of this under φ is a principal homogeneous space over X. Consequently there is a canonical map $\beta_1(N)$: $\mathrm{Ext}^1_k(A,N) \longrightarrow H^1(X,N)$ which we wish to extend to all Exts and cohomology groups.

There are canonical homomorphisms $\mathrm{Ext}^r_k(A,N) \longrightarrow \mathrm{Ext}^r_X(A,N)$ given by base extension (equivalently, by taking the inverse images of the exact sequences as sheaves). Also, there is a canonical element in $H^0(X,A)$, viz. φ, so the Yoneda pairings

$$\begin{tikzcd}
H^{o}(X,A) \times \mathrm{Ext}^{r}_{X}(A,N) \arrow[r] & H^{r}(X,N) \\
\mathrm{Ext}^{r}_{k}(A,N) \arrow[u] \arrow[ur, "\beta_r(N)"'] &
\end{tikzcd}$$

induce homomorphisms $\beta_r(N)$ as in the diagram.

It is easy to see that the two definitions of β_1 coincide. For some flat covering $(U_i \longrightarrow A)_{i \in I}$ there exist sections $p_i \in P(U_i)$, and the principal homogeneous space over A defined by (2.1) corresponds to the Čech cocycle (n_{ij}), $n_{ij} \in N(U_i \times_A U_j)$, $p_i^{\,j}\, n_{ij} = p^i_{\,j}$. Then $(U_{i\,X} = U_i \times_A X \longrightarrow X)$ is a flat covering of X, and the image of (2.1) under either definition of β_1 corresponds to the Cech cocycle (n'_{ij}), where n'_{ij} is the image of n_{ij} under $N(U_i \times_A U_j) \longrightarrow N(U_{i\,X} \times_X U_{j\,X})$.

<u>Theorem 1</u>. $\beta_r(N)$ is an injection all r,and $\beta_1(N)$ an isomorphism,for all finite group schemes N over k if and only if

(a) the Néron-Severi group of X is torsion-free and

(b) $\dim_k(H^1(X,O_X)) = \dim(A)$ $(= \dim_k(\mathrm{Ext}^1_k(A, \mathbb{G}_a))$ [31, VII 17 and 21]).

Remarks. 1. It is obvious from their definition that the β_r form a morphism of connected sequences of functors in N, but in fact they are also functorial in X. For this it suffices to show that the β_r are independent of the choice of the "canonical" morphism $X \longrightarrow A$, or equivalently that $A(k)$ acts trivially on $\mathrm{Ext}_k^r(A,N)$. But it suffices to show this for $\mathbb{G}_m$ and $\mathbb{G}_a$ and $r = 1$ (see the arguments in the proof below) and these follow from [15,III,§3, Proposition 4] and [28, p. 699].

2. Any morphism $X \longrightarrow N$, where N is a finite group scheme over k, is constant, thus $H^0(X,N) = N(k)$ and so is exact (k being algebraically closed). Hence $H^1(X,N)$ is a left exact functor from the category of finite group schemes over k to abelian groups, and as such must be strictly pro-representable [11, 195, 3.1]. Since $\mathrm{Ext}_k^1(A,N)(p) \approx \mathrm{Hom}_k(T_pA,N)$ (as follows immediately from the $\mathrm{Ext}(-,N)$ sequences of $0 \longrightarrow A_\nu \longrightarrow A \xrightarrow{p^\nu} A \longrightarrow 0$, $\nu \geq 0$), the theorem may be interpreted as giving necessary and sufficient conditions for $H^1(X,-)(p)$ to be pro-represented by T_pA all p.

Proof of Theorem. The canonical map $\mathrm{Ext}_k^1(A, \mathbb{G}_m) \longrightarrow H^1(A, \mathbb{G}_m) \approx \mathrm{Pic}\, A$ identifies $\mathrm{Ext}_k^1(A, \mathbb{G}_m)$ with $\mathrm{Pic}^{\bullet} A$, the subgroup of those divisor classes on A which are algebraically equivalent to zero [31, VII 16]. But $\varphi^*: H^1(A, \mathbb{G}_m) \longrightarrow H^1(X, \mathbb{G}_m)$ identifies $\mathrm{Pic}^{\bullet} A$ with the divisor classes on X which are algebraically equivalent to zero, and so, by definition of the Neron-Severi group N.S.(X) of X, coker (φ^*) = N.S.(X). Thus $\beta_1(\mathbb{G}_m)$ gives an exact sequence

$$0 \longrightarrow \mathrm{Pic}^{\bullet} A \xrightarrow{\beta_1} \mathrm{Pic}\, X \longrightarrow \mathrm{N.S.}\ (X) \longrightarrow 0.$$

$\mathrm{Ext}_k^r(A, \mathbb{G}_m) = 0$ for $r \neq 1$ [26, II 14-2] so the exact sequence $0 \longrightarrow \mu_n \longrightarrow \mathbb{G}_m \xrightarrow{n} \mathbb{G}_m \longrightarrow 0$ gives rise to an exact, commutative diagram

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \mathrm{Ext}^1_k(A,\mu_n) \arrow[r] \arrow[d, "\beta_1(\mu_n)"] & \mathrm{Pic}^{\cdot} A \arrow[r, "n"] \arrow[d, "\beta_1(\mathbb{G}_m)"] & \mathrm{Pic}^{\cdot} A \arrow[r] \arrow[d, "\beta_1(\mathbb{G}_m)"] & 0 \arrow[d, "\beta_2(\mu_n)"] \\
0 \arrow[r] & H^1(X,\mu_n) \arrow[r] \arrow[d] & \mathrm{Pic}\ X \arrow[r, "n"] \arrow[d] & \mathrm{Pic}\ X \arrow[r] \arrow[d] & H^2(X,\mu_n) \\
0 \arrow[r] & \mathrm{coker}\ (\beta_1) \arrow[r] \arrow[d] & \mathrm{N.S.}(X) \arrow[r, "n"] \arrow[d] & \mathrm{N.S.}(X) \arrow[d] & \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

Thus $\beta_r(\mu_n)$ is injective all r and n, and $\beta_1(\mu_n)$ is surjective all n if and only if (a) holds.

$$H^r(X,\ \mathbb{G}_a) \approx H^r(X_{Zar},\ O_X) \quad \text{and} \quad \mathrm{Ext}^r_k(A,\ \mathbb{G}_a) = 0 \quad \text{for } r \neq 1$$

[26, II 14-2], so the exact sequence

$$0 \longrightarrow \alpha_{p^n} \longrightarrow \mathbb{G}_a \xrightarrow{F^n} \mathbb{G}_a \longrightarrow 0$$

(where F is the Frobenius endomorphism of $\mathbb{G}_a$) gives an exact commutative diagram (2.2)

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Ext}_k^1(A,\alpha_{p^n}) \arrow[r] \arrow[d, "\beta_1(\alpha_{p^n})"] & \mathrm{Ext}_k^1(A,\mathbb{G}_a) \arrow[r] \arrow[d, "\beta_1(\mathbb{G}_a)"] & \mathrm{Ext}_k^1(A,\mathbb{G}_a) \arrow[r] \arrow[d, "\beta_1(\mathbb{G}_a)"] & \mathrm{Ext}_k^2(A,\alpha_{p^n}) \arrow[r] \arrow[d, "\beta_2(\alpha_{p^n})"] & 0 \arrow[d] \\
0 \arrow[r] & H^1(X,\alpha_{p^n}) \arrow[r] & H^1(X,O_X) \arrow[r, "F^n"] & H^1(X,O_X) \arrow[r] & H^2(X,\alpha_{p^n}) \arrow[r] & H^2(X,O_X)
\end{tikzcd}$$

By [31, VII.19], $\beta_1(\mathbb{G}_a)$ is injective, so $\beta_r(\alpha_{p^n})$ is injective all r and n, and $\beta_1(\alpha_{p^r})$ is surjective if and only if $\beta_1(\mathbb{G}_a)$ maps surjectively onto $H^1(X,O_X)_n$, the subspace of $H^1(X,O_X)$ on which F is nilpotent (see [30, p. 38] for the Jordan decomposition of $H^1(X,O_X)$).

The same argument relative to the sequence

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{G}_a \xrightarrow{1-F} \mathbb{G}_a \longrightarrow 0$$

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

But $H^1(X,O_X) = H^1(X,O_X)_s \oplus H^1(X,O_X)_n$, so we have proved the necessity of the conditions (a) and (b). Moreover we have shown that when (a) and (b) hold, $\beta_r(N)$ is an injection, and $\beta_1(N)$ an isomorphism, for all simple finite group schemes

N over k. The theorem now follows by the standard 5-lemma argument using induction on the length of N.

<u>Corollary 1.</u> For any abelian variety A over k, and any finite group scheme N over k, the canonical map $\mathrm{Ext}_k^1(A,N) \longrightarrow H^1(A,N)$ is an isomorphism.

I.e., any scheme P over A which is a principal homogeneous space for the group N, can be given a group structure in such a way that the sequence $0 \longrightarrow N \longrightarrow P \longrightarrow A \longrightarrow 0$ is exact and induces on P its original N-operation. In particular, if P is reduced and irreducible it is an abelian variety and $P \longrightarrow A$ an isogeny. In this form the statement was first proved by Lang and Serre [16] for N étale and by Miyanishi [20] for N arbitrary.

<u>Corollary 2.</u> If $\varphi: X \longrightarrow A$ is as in the theorem, then $\varphi^*: H^1(A,N) \longrightarrow H^1(X,N)$ is an isomorphism for all finite group schemes N over k if and only if X satisfies conditions (a) and (b) of the theorem (cf. [31, VI.21]).

<u>Proof.</u> Combine Corollary 1 with the Theorem.

Corollary 3. Let X be a complete, connected, regular algebraic curve over an algebraically closed field k, and let J be the Jacobian of X. For any finite group scheme N over k,

$$H^o(X,N) \approx N(k)$$
$$H^1(X,N) \approx \mathrm{Hom}_k\ (T_pJ,\ N)$$
$$H^2(X,N_{cc}) \approx \mathrm{Ext}^1_k\ (T_pJ,\ N)$$
$$H^r(X,\ N) \ =\ 0, \quad r > 2.$$

Proof. The first two isomorphisms have already been proved, and the third follows for α_p from the diagram (2.2) using that $H^2(X,O_X) = 0$ for X a curve. For arbitrary N such that $N = N_{cc}$ it follows by induction on the length. The triviality of the cohomology groups for $r > 2$ is an immediate consequence of $H^r(X,\ \mathbb{G}_m) = 0$ for $r > 1$ [2, IV] and $H^r(X,\ O_X) = 0$ for $r > 1$.

Remark. Let $\varphi\colon\ X \longrightarrow A$ be as in the theorem, and let B be a second abelian variety over k. The diagram

$$\begin{tikzcd}
H^o(X,B) \arrow[r] & H^1(X,B_\nu) \\
\mathrm{Hom}_k(A,B) \arrow[u, "\varphi^*"] \arrow[r, "\delta_B"] & \mathrm{Ext}_k^1(A,B_\nu) \arrow[u, "\beta_1(B_\nu)"']
\end{tikzcd}$$

in which the horizontal arrows are the boundary maps for the sequence

$$\begin{tikzcd}
O \arrow[r] & B_\nu \arrow[r] & B \arrow[r, "p^\nu"] & B \arrow[r] & O
\end{tikzcd}$$

clearly commutes. The diagram

$$\begin{tikzcd}
\mathrm{Hom}_k(A,B) \arrow[rr, "\delta_B"] \arrow[dr, "\gamma"'] & & \mathrm{Ext}_k^1(A,B_\nu) \arrow[dl, "\delta_A"] \\
& \mathrm{Hom}_k(A_\nu,B_\nu) &
\end{tikzcd}$$

where γ is the canonical map and δ_A and δ_B the obvious boundary maps, may be shown without difficulty to commute. By combining these two diagrams and passing to the double limit one gets that the following diagram commutes

$$\begin{tikzcd}
H^o(X,B) \arrow[rr] & & H^1(X,\ T_pB) \\
\mathrm{Hom}_k(A,B) \arrow[u, "\varphi^*"'] \arrow[r, "\gamma"] & \mathrm{Hom}_k(T_pA,T_pB) \arrow[r, phantom, "\approx"] & \mathrm{Ext}_k^1(A,\ T_pB) \arrow[u, "\approx"'] \ .
\end{tikzcd}$$

3. Heights and Cup Products

Throughout this section, X will be a complete, connected, smooth, algebraic curve over an algebraically closed field k. For any pair of sheaves F and G on X_{fl}, there is a spectral sequence [3, V 4.1]

$$H^r(X, \underline{\mathrm{Ext}}^s_X (F, G)) \Longrightarrow \mathrm{Ext}^{r+s}_X(F, G).$$

If N is a finite flat group scheme over X which is killed by p^ν, then there are isomorphisms of sheaves

$$\underline{\mathrm{Ext}}^o_X(N, \mu_{p^\nu}) \xrightarrow{\approx} \underline{\mathrm{Ext}}^o_X (N, \mathbb{G}_m) \xrightarrow{\approx} N^D \qquad [26,16.1] .$$

Thus the edge morphisms of the above spectral sequence give morphisms $\epsilon_s: H^s(X,N^D) \longrightarrow \mathrm{Ext}^s_X (N,\mu_{p^\nu})$ which, when combined with the Yoneda pairings

$$H^r(X,N) \times \mathrm{Ext}^s_X (N, \mu_{p^\nu}) \longrightarrow H^{r+s}(X, \mu_{p^\nu})$$

give cup product pairings

$$H^r(X,N) \times H^s (X, N^D) \longrightarrow H^{r+s}(X, \mu_{p^\nu}).$$

From [2,IV], $H^1(X, \mathbb{G}_m) \approx \text{Pic } X$ and $H^2(X, \mathbb{G}_m) = 0$, so there exists a canonical isomorphism $H^2(X,\mu_{p^\nu}) \xrightarrow{\lambda} \mathbb{Z}/p^\nu\mathbb{Z}$, and the cup product defines a pairing

$$H^r(X,N) \times H^{2-r}(X,N^D) \longrightarrow \mathbb{Z}/p^\nu\mathbb{Z} .$$

Let A be a projective abelian scheme over X. Then [26, I 5.3 and III.19] the dual abelian scheme A^t of A exists and there is an exact commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & A^t_\nu \arrow[r] \arrow[d, "\alpha", "\approx"'] & A^t \arrow[r] \arrow[d, "\beta", "\approx"'] & A^t \arrow[r] \arrow[d, "\beta", "\approx"'] & 0 \\
0 \arrow[r] & \underline{\text{Hom}}_X(A_\nu,\mathbb{G}_m) \arrow[r] & \underline{\text{Ext}}^1_X(A,\mathbb{G}_m) \arrow[r] & \underline{\text{Ext}}^1_X(A,\mathbb{G}_m) \arrow[r] & 0
\end{tikzcd} \tag{3.1}$$

If K is the function field of X, then A(X) may be identified with $A_K(K)$ and $A^t(X)$ with $A^t_K(K)$, so the global symbol $(\ ,\ ) = \Sigma_v (\ ,\ )_v$ ($v \in X$, v closed) of Néron [22, II 12] defines a pairing

$$(\ \ ,\ \ ):\ A(X) \times A^t(X) \longrightarrow \mathbb{Z} .$$

The exact sequences

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

$$0 \longrightarrow A^t_\nu \longrightarrow A^t \xrightarrow{p^\nu} A^t \longrightarrow 0$$

define boundary maps

$$\delta_A : \quad A(X) = H^0(X, A) \longrightarrow H^1(X, A_\nu)$$

$$\delta_{A^t} : A^t(X) = H^0(X, A^t) \longrightarrow H^1(X, A^t_\nu) .$$

Since $\alpha : A^t_\nu \xrightarrow{\approx} \underline{\mathrm{Hom}}_X(A_\nu, \mathbb{G}_m) = \underline{\mathrm{Hom}}_X(A_\nu, \mu_{p^\nu})$, the cup product defines a pairing

$$\smile : H^1(X,A_\nu) \times H^1(X, A^t_\nu) \longrightarrow H^2(X, \mu_{p^\nu}) \approx \mathbb{Z}/p^\nu\mathbb{Z} .$$

<u>Theorem 2</u>. Let $a \in A(X)$ and $x \in A^t(X)$. Then with the above notations, $\delta a \smile \delta x = (x.a) \pmod{p^\nu}$, i.e., the diagram

$$\begin{tikzcd}
A(X) \times A^t(X) \arrow[r, "{(\ ,\ )}"] \arrow[d, "\delta_A \times \delta_{A^t}"] & \mathbb{Z} \arrow[d] \\
H^1(X,A_\nu) \times H^1(X,A^t_\nu) \arrow[r, "\smile"] & \mathbb{Z}/p^\nu\mathbb{Z}
\end{tikzcd}$$

commutes.

Proof. Consider the diagram

(3.2)

$$\begin{tikzcd} A(X) \arrow[d, equal] & \times & A^t(X) \arrow[rr, "{(\ ,\ )}"] \arrow[d, "\beta"] & & \mathbb{Z} \\ H^o(X,A) & \times & \mathrm{Ext}^1_X(A,\mathbb{G}_m) \arrow[rr] & & H^1(X,\mathbb{G}_m) \arrow[u, "\deg"'] \end{tikzcd}$$

in which the lower pairing is the Yoneda pairing and deg is the degree map Pic(X) $\longrightarrow \mathbb{Z}$.

Let $a \in A(X)$ and $x \in A^t(X)$. There is a commutative diagram

$$\begin{tikzcd} A^t(X) \arrow[r, "\beta"] \arrow[dr] & \mathrm{Ext}^1_X(A,\mathbb{G}_m) \arrow[d] \\ & H^1(A,\mathbb{G}_m) \end{tikzcd}$$

[26,III 18.1]

and it is easily seen that if y is the image of x in $H^1(A,\mathbb{G}_m)$, then the value of the Yoneda pairing at the pair a,x is just $a^*(y)$, where $a^*: H^1(A,\mathbb{G}_m) \longrightarrow H^1(X,\mathbb{G}_m)$ is the map induced by $a: X \longrightarrow A$. But $a^*(y)$ can be computed using Cartier divisors (see [21, Lectures 9,10]). Choose a Cartier divisor D whose image in $H^1(A,\mathbb{G}_m)$ is y and which does not contain $a(X)$ in its support. (That this is possible is easily seen by looking at the generic fibre). Let (f_i), $f_i \in \Gamma(U_i, K_A^*)$ be local equations for D. Then

$a^*(y)$ has local equations $(a^*(f_i))$, $a^*(f_i) \in \Gamma(a^{-1}(U_i), K_X^*)$, and so has degree $\Sigma_v \operatorname{ord}_v(a^*(f_v))$ ($v \in X$, closed) where f_v equals some f_i such that $v \in a^{-1}(U_i)$, and ord_v is the valuation of K (mapping onto $\mathbb{Z}$) associated to v. But this, in another language, is exactly Néron's definition of the symbol $i_v(x,a)$ ([22, III 2] and [23]). Thus

$$\deg(a^*(y)) = \Sigma_v \, i_v(x,a) = (x,a) \qquad [22, \text{III 2 Theorem 3}]$$

and we have shown that diagram (3.2) commutes.

Consider the diagram

$$(3.3) \qquad \begin{tikzcd} A^t(X) \arrow[r, "\beta"] \arrow[d, "\delta_{A^t}"'] & \operatorname{Ext}^1_X(A, \mathbb{G}_m) \arrow[d, "k"] \\ H^1(X, A^t_\nu) \arrow[r, "\epsilon_1"] & \operatorname{Ext}^1_X(A_\nu, \mu_{p^\nu}) \end{tikzcd}$$

where k is the map which takes the class of an exact sequence $0 \longrightarrow \mathbb{G}_m \longrightarrow E \longrightarrow A \longrightarrow 0$ to the class of $0 \longrightarrow \mu_{p^\nu} \longrightarrow E_\nu \longrightarrow A_\nu \longrightarrow 0$ with $E_\nu = \ker(p^\nu\colon \ E \longrightarrow E)$.

Let $x \in A^t(X) = H^o(X,A^t)$. For some flat covering $(U_i \longrightarrow X)_{i\in I}$, there exist $x_i \in A^t(U_i)$ such that $p^\nu x_i$ equals the image of x under the map associated by A^t to $U_i \longrightarrow X$. .Write $x_i{}^j$ and $x^i{}_j$ for the images of x_i and x_j respectively under the maps associated by A^t to the projections $U_{ij} = U_i \times_X U_j \longrightarrow U_i$ and $U_{ij} \longrightarrow U_j$. Then $p^\nu(x^i{}_j - x_i{}^j) = 0$ so $x_{ij} = x^i{}_j - x_i{}^j \in A^t_\nu(U_{ij})$ and (x_{ij}) is the Cech 1-cocycle describing the element $\delta_{A^t}(x)$ in $H^1(X,A^t_\nu)$.

We now describe $\epsilon_1\delta(x) \in \mathrm{Ext}^1_X(A_\nu, \mu_{p^\nu})$. $y_{ij} = \alpha(x_{ij})$ is an element of $\mathrm{Hom}_{U_{ij}}(A_\nu, \mathbb{G}_m) = \mathrm{Hom}_{U_{ij}}(A_\nu, \mu_{p^\nu})$. Define E_i on U_i to be the trivial exact sequence

$$0 \longrightarrow \mu_{p^\nu} \longrightarrow \mu_{p^\nu} \times A_\nu \longrightarrow A_\nu \longrightarrow 0.$$

Define a map from the restriction of E_i to U_{ij} to the restriction of E_j to U_{ij} by

$$\begin{tikzcd}
E_i: & 0 \arrow[r] & \mu_{p^\nu} \arrow[r] \arrow[d, equal] & \mu_{p^\nu} \times A_\nu \arrow[r] \arrow[d, "\begin{pmatrix}1 & y_{ij}\\ 0 & 1\end{pmatrix}"] & A_\nu \arrow[r] \arrow[d, equal] & 0 \\
E_j: & 0 \arrow[r] & \mu_{p^\nu} \arrow[r] & \mu_{p^\nu} \times A_\nu \arrow[r] & A_\nu \arrow[r] & 0 .
\end{tikzcd}$$

By descent theory [9, VIII 2.1] we get an extension of A_ν by μ_{p^ν} over X, and the class of this extension in $\mathrm{Ext}^1_X(A_\nu, \mu_{p^\nu})$ is $\epsilon.\delta(x)$. It is now elementary to check, using (3.1), that this class is also $k\beta(x)$, and consequently that (3.3) commutes.

Consider the diagram

$$\begin{tikzcd}
\mathrm{Ext}^1_X(A, \mathbb{G}_m) \arrow[d, "k"'] \arrow[dr, "\delta_{\mathbb{G}_m}"] & \\
& \mathrm{Ext}^2_X(A, \mu_{p^\nu}) \\
\mathrm{Ext}^1_X(A_\nu, \mu_{p^\nu}) \arrow[ur, "\delta_A"'] &
\end{tikzcd} \tag{3.4}$$

where the boundary maps δ are those defined by the sequences

$$\begin{tikzcd}
0 \arrow[r] & \mu_{p^\nu} \arrow[r] & \mathbb{G}_m \arrow[r, "p^\nu"] & \mathbb{G}_m \arrow[r] & 0
\end{tikzcd}$$

$$\begin{tikzcd}
0 \arrow[r] & A_\nu \arrow[r] & A \arrow[r, "p^\nu"] & A \arrow[r] & 0 .
\end{tikzcd}$$

If $x \in \mathrm{Ext}^1_X(A, \mathbb{G}_m)$ is defined by the sequence

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{G}_m \arrow[r, "b"] & E \arrow[r, "c"] & A \arrow[r] & 0
\end{tikzcd}$$

then $\delta_{\mathbb{G}_m}(x)$ and $\delta_A\, k(x)$ are defined by the sequences

$$0 \longrightarrow \mu_{p^{\nu}} \longrightarrow \mathbb{G}_m \xrightarrow{p^{\nu}b} E \xrightarrow{c} A \longrightarrow 0$$

and

$$0 \longrightarrow \mu_{p^{\nu}} \xrightarrow{b} E_{\nu} \xrightarrow{c} A \xrightarrow{p^{\nu}} A \longrightarrow 0 .$$

These two sequences may be shown to be equivalent by, for example, subtracting one from the other and using [19, VII 4.1] to show that the resulting sequence is equivalent to zero. It follows that (3.4) commutes.

The commutativity of (3.2), (3.3) and (3.4) suffices to prove the theorem. We write w.z for the value of the Yoneda pairing at the pair w,z. Let $a \in A(X)$ and $x \in A^t(X)$. By (3.2)

$$\lambda\, \delta_{\mathbb{G}_m}(a.\beta(x)) = (x,a) \pmod{p^{\nu}}$$

where $H^1(X,\mathbb{G}_m) \xrightarrow{\delta_{\mathbb{G}_m}} H^2(X, \mu_{p^{\nu}}) \xrightarrow{\lambda} \mathbb{Z}/p^{\nu}\mathbb{Z}$. But, by the properties of the Yoneda pairing,

$$\begin{tikzcd}
H^o(X,A) \arrow[d, equal] & \times & \mathrm{Ext}^1(A, \mathbb{G}_m) \arrow[d, "\delta_{\mathbb{G}_m}"] \arrow[r] & H^1(X, \mathbb{G}_m) \arrow[d, "\delta_{\mathbb{G}_m}"] \\
H^o(X,A) & \times & \mathrm{Ext}^2(A, \mu_{p^{\nu}}) \arrow[r] & H^2(X, \mu_{p^{\nu}})
\end{tikzcd}$$

commutes, i.e., $\delta_{\mathbb{G}_m}(a.\beta(x)) = a.\delta_{\mathbb{G}_m}\beta(x)$. Thus,

$$\begin{aligned}
\lambda\ \delta_{\mathbb{G}_m}(a.\beta(x)) &= \lambda(a.\delta_{\mathbb{G}_m}\beta(x)) \\
&= \lambda(a.\delta_A k\beta(x)) \qquad \text{by } (3.4) \\
&= \lambda(a.\delta_A\ \epsilon_1\ \delta_{A^t}(x)) \ \text{by } (3.3) \\
&= \lambda(\delta_A(a).\ \epsilon_1\ \delta_{A^t}(x)) \\
&= \delta_A(a) \smile \delta_{A^t}(x)
\end{aligned}$$

by definition of cup products, and this completes the proof of the theorem.

4. Generalities on p-Divisible Groups

In this section we state some general facts about p-divisible groups which are needed for the computations of the next section. Let k be a perfect field of nonzero characteristic. Then [36, Proposition 1] there is a canonical correspondence between connected p-divisible groups over k and certain commutative formal Lie groups, so the results in [18] may be applied to p-divisible groups.

Let G be a p-divisible group over k and φ an endomorphism of G. We say that P(T) is the characteristic polynomial of φ if it satisfies the conditions:

(a) P is monic, has coefficients in $\mathbb{Z}_p$, and is of degree h equal to the height of G.

(b) If $\alpha_1,\ldots,\alpha_h$ are the roots of P in some algebraic closure of $\mathbb{Q}_p$, then

$$\left|\prod_{i=1}^{h} F(\alpha_i)\right|_p = \left|\text{degree } F(\varphi)\right|_p$$

for all polynomials F with coefficients in $\mathbb{Z}$.

The uniqueness of P(T) follows from [40, IX, 68], and its existence from the possibility of representing p-divisible groups by certain modules.

First assume $p \neq$ characteristic of k. Let Γ be the Galois group of the algebraic closure $\bar{k}$ of k over k. The functor $M: N \longmapsto N(\bar{k})$ defines an equivalence between the category of finite group schemes N over k which are killed by a power of p and the category of finite p-primary Γ-modules. Moreover, $[N(\bar{k})]$ equals the rank of N (i.e., the rank of the k-algebra $\Gamma(N,O_N)$). From this we deduce an equivalence $M: G = (G_\nu, i_\nu) \longmapsto \varinjlim_{\nu} G_\nu(\bar{k})$ between the category of p-divisible groups G over k and the category of discrete Γ-modules whose underlying groups are isomorphic to $\oplus^h \mathbb{Q}_p/\mathbb{Z}_p$ some h (and moreover h is the height of G). If φ is an endomorphism of the p-divisible group G, then it is easy to see that the characteristic polynomial of $M(\varphi)$ on $M(G)$ has the properties (a) and (b) above required for it to be the characteristic polynomial of φ on G.

For the rest of this section, we take p = characteristic of k. Let W_k be the ring of infinite Witt vectors over k, and let A_k be the ring of non-commutative polynomials $W_k[F,V]$ with the relations $FV = p = VF$, $Fa = a^\sigma F$, $aV = Va^\sigma$, $a \in W_k$ where σ is the canonical lifting of the

Frobenius automorphism ($\sigma x = x^p$) of k to W_k. There is a contravariant functor $N \longmapsto D_k(N)$ from the category of those algebraic group schemes over k which are unipotent or finite and killed by a power of p to a subcategory of the category of finitely generated left A_k-modules, which is an anti-equivalence of categories [24] [33] [18]. Moreover, if N is of finite rank p^ν over k, then $D_k(N)$ is of length ν as a W_k-module. From this we get an anti-equivalence $G \longmapsto D_k(G)$ from the category of p-divisible groups over k to the category of A_k-modules which are free of finite rank over W_k, and the height of G is equal to the rank of $D_k(G)$ over W_k.

If φ is an endomorphism of G, then $D_k(\varphi)$ commutes with the action of F on $D_k(G)$ and it follows easily that the characteristic polynomial of $D_k(\varphi)$ on $D_k(G)$ has coefficients in $\mathbb{Z}_p$ and is the characteristic polynomial of φ.

Now write $W_k' = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} W_k$, $A_k' = W_k' \otimes_{W_k} A_k$, and $D_k'(G) = A_k' \otimes_{A_k} D(G)$. Note that $A_k' = W_k' [F,F^{-1}]$ with the single relation $Fa = a^\sigma F$. Clearly two p-divisible groups G and H are isogenous over k if and only if $D_k'(G) \approx D_k'(H)$.

Assume now that k is finite with p^a elements. If F_k is the Frobenius endomorphism of the p-divisible group G relative to k, then $D_k(F_k)$ acts on $D_k(G)$ as F^a. We denote its characteristic polynomial by $c_G(T)$. The minimal polynomial $m_G(T)$ of F_k on G may also be defined. It is the monic polynomial of least degree with coefficients in $\mathbb{Z}_p$ such that $m_G(F_k)$ is zero on G. If $D_k'(G)$ is isomorphic to $A'/A'\lambda$ for some left ideal $A'\lambda$ in A', then $A'm_G(F^a)$ is the bound of $A'\lambda$ in the sense of [13, Chapter 3, §6].

We say that a p-divisible group is indecomposable if it cannot be written as a direct sum of two nonzero p-divisible groups.

Proposition 1. (a) Every p-divisible group G is isogenous to a direct sum of indecomposable p-divisible groups, and the decomposition is unique up to isogeny.

(b) If G is indecomposable then $m_G(T)$ is a power of a $\mathbb{Z}_p$-irreducible polynomial. Moreover, there exists an integer e such that

$$D'(\oplus^e G) \approx A'/A'm_G(F^a) .$$

(c) Suppose $D'(G) = A'/A'P(F)$ where

$P(F) = F^{m+n} + b_{m-1}F^{m+n-1} + \cdots + b_{-n}$ and $\mathrm{ord}_p(b_{-n}) = an$.

Then $Q(F,V) := F^m + b_{m-1}F^{m-1} + \cdots + \frac{b_{-n}}{q^n} V^n$ has coefficients in $\mathbb{Z}_p$, and $A/AQ(F,V)$ is the module of a p-divisible group isogenous to G.

Proof. (a) and (b) may be deduced from the corresponding theorems for modules [13, Chapter 3], and (c) by an application of Newton's polygon for non-commutative polynomials.

Remark. If G is the p-divisible group associated to an abelian variety A and φ is an endomorphism of A, then it is clear from their definitions that the characteristic polynomial of φ on A is equal to the characteristic polynomial of the endomorphism of G defined by φ. In particular this shows that $c_G(T)$ has coefficients in $\mathbb{Z}$, but the fact that G comes from an abelian variety places an even stronger condition on $m_G(T)$, viz. that it has no multiple roots. A is isogenous to a direct sum $\oplus A_i$ of simple abelian varieties. The characteristic polynomial of F_k on A_i is a power of a $\mathbb{Z}$-irreducible polynomial f_i, and f_i (F_k) is zero on A_i [37, Theorem 2]. $m_G(T)$ divides the least common multiple of the f_i, which has no multiple roots.

5. Extensions of p-Divisible Groups

We retain the notations of §4 except that k is no longer necessarily of characteristic p, although still finite with q elements and of degree a over the prime field. We refer the reader to [35, 306-19] for the definition of quasi-isomorphism of $\mathbb{Z}_p$-modules and the elementary Lemmas z.1, z.2, z.3, and z.4.

Assume first that G and H are p-divisible groups over k and that p ≠ characteristic of k. If F_k is the Frobenius endomorphism of G relative to k, then $M(F_k)$ acts on M(G) as the canonical topological generator σ_k of Γ. Let f_o: $\mathrm{Hom}_{\bar{k}}(\bar{G},\bar{H})^{\Gamma} \longrightarrow \mathrm{Hom}_{\bar{k}}(\bar{G},\bar{H})_{\Gamma}$ be the map induced by the identity map on $\mathrm{Hom}(\bar{G},\bar{H})$. By [35], Lemma z.4, f_o is a quasi-isomorphism if $\mathrm{rk}_{\mathbb{Z}_p}(\mathrm{Hom}_{\bar{k}}(\bar{G},\bar{H})^{\Gamma})$ equals the multiplicity of 1 as a root of the characteristic polynomial of σ_k on $\mathrm{Hom}_{\bar{k}}(\bar{G},\bar{H})$. This condition is satisfied if 1 is not a multiple root of the minimal polynomial of σ_k on $\mathrm{Hom}(\bar{G},\bar{H})$, or again if no multiple root of $m_G(T)$ or $m_H(T)$ occurs as a root of the other. When this is so,

$$z(f_o) = \left|\prod_{\alpha_i \neq \beta_j} \left(1 - \frac{\beta_j}{\alpha_i}\right)\right|_p = \left|\prod_{\alpha_i \neq \beta_j} \left(1 - \frac{\alpha_i}{\beta_j}\right)\right|_p$$

where $\alpha_1,\ldots,\alpha_g$ and $\beta_1,\ldots,\beta_h$ are the roots of $c_G(T)$ and $c_H(T)$ respectively.

The situation is considerably more complicated when we allow p = characteristic of k.

Proposition 2. Let G and H be p-divisible groups over the field k, and let $\alpha_1,\ldots,\alpha_g$ and $\beta_1,\ldots,\beta_h$ be the roots of $c_G(T)$ and $c_H(T)$ respectively. Let f_r be the map $\mathrm{Ext}^r_{\bar{k}}(\bar{G},\bar{H})^{\Gamma} \longrightarrow \mathrm{Ext}^r_{\bar{k}}(\bar{G},\bar{H})_{\Gamma}$ induced by the identity map on $\mathrm{Ext}^r_{\bar{k}}(\bar{G},\bar{H})$. Assume that no multiple root of $m_G(T)$ or $m_H(T)$ occurs as a root of the other. Then f_r is a quasi-isomorphism all r, $z(f_r) = 1$ all $r \geq 2$, and

$$(5.1)\quad \frac{z(f_o)}{z(f_1)} = \left| q^{\dim(G^t)\dim(H)} \prod_{\alpha_i \neq \beta_j} \left(1 - \frac{\alpha_i}{\beta_j}\right) \right|_p$$

Remark. It will be shown (Lemma 2) that $\mathrm{Ext}^r_{\bar{k}}(\bar{G},\bar{H})_{\Gamma} = 0$ so $\dfrac{z(f_o)}{z(f_1)} = z(f_o) \left| [\mathrm{Ext}^1_{\bar{k}}(\bar{G},\bar{H})^{\Gamma}] \right|_p$.

If $0 \longrightarrow I' \longrightarrow I \longrightarrow I'' \longrightarrow 0$ is an exact sequence of ind-algebraic group schemes over $\bar{k}$, and I' and I" are p-divisible groups then I is also p-divisible, so there corresponds a dual exact sequence

$0 \longrightarrow I''^t \longrightarrow I^t \longrightarrow I'^t \longrightarrow 0$. This defines an isomorphism $\mathrm{Ext}^1_{\bar{k}}(\bar{G},\bar{H}) \approx \mathrm{Ext}^1_{\bar{k}}(\bar{H}^t, \bar{G}^t)$. But

$$\begin{aligned} \mathrm{Ext}^1_{\bar{k}}(\bar{H}^t, \bar{G}^t) &\approx \varprojlim_{\mu} \varinjlim_{\nu} \mathrm{Ext}^1_{\bar{k}}(\bar{H}^D_{\mu}, \bar{G}^D_{\nu}) \quad \text{(cf. [26,I.4-3])} \\ &\approx \varprojlim_{\mu} \varinjlim_{\nu} \mathrm{Ext}^1_{\bar{k}}(\bar{G}_{\nu}, \bar{H}_{\mu}) \\ &\approx \mathrm{Ext}^1_{\bar{k}}(T_p\bar{G}, T_p\bar{H}) \end{aligned}$$

(this last Ext being computed in the category of pro-algebraic group schemes over $\bar{k}$). Since $\mathrm{Hom}_{\bar{k}}(\bar{G}, \bar{H}) \approx \mathrm{Hom}_{\bar{k}}(T_p\bar{G}, T_p\bar{H})$ we could define f_o as the map $\mathrm{Hom}_{\bar{k}}(T_p\bar{G},T_p\bar{H})^{\Gamma} \longrightarrow \mathrm{Hom}_{\bar{k}}(T_p\bar{G},T_p\bar{H})_{\Gamma}$. Take $G = A(p)$ and $H = B(p)$ to be the p-divisible groups associated to abelian varieties A and B. By the final remark of §4, G and H satisfy the conditions of proposition 2. Thus we get the following statement: if A and B are abelian varieties over k, then the map

f_o: $\mathrm{Hom}_{\bar{k}}(T_p\bar{A}, T_p\bar{B})^{\Gamma} \longrightarrow \mathrm{Hom}_{\bar{k}}(T_p\bar{A}, T_p\bar{B})_{\Gamma}$ is a quasi-isomorphism, $\mathrm{Ext}^1_{\bar{k}}(T_p\bar{A}, T_p\bar{B})^{\Gamma}$ is finite, and

$$z(f_o)\left|[\mathrm{Ext}^1_{\bar{k}}(T_p\bar{A}, T_p\bar{B})^{\Gamma}]\right|_p = \left| q^{\dim(A)\dim(B)} \prod_{\alpha_i \neq \beta_j} (1-\frac{\alpha_i}{\beta_j})\right|_p$$

where the α_i and β_j are the roots of the characteristic polynomials of F_k on A and B respectively. This is the form in which the proposition will be used in the next section.

If $p \nmid$ characteristic of k, then the proposition reduces to the statement already proved, so for the rest of this section we assume p = characteristic of k.

Lemma 1. Let G and H be p-divisible groups over $\bar{k}$. Then

$$\mathrm{Ext}^0_{\bar{k}}(G, H) \approx \mathrm{Ext}^0_{A_{\bar{k}}}(D_{\bar{k}}(H), D_{\bar{k}}(G))$$

$$\mathrm{Ext}^1_{\bar{k}}(G, H) \approx \mathrm{Ext}^1_{A_{\bar{k}}}(D_{\bar{k}}(H), D_{\bar{k}}(G))$$

$\mathrm{Ext}^r_{\bar{k}}(G, H) = 0$ for $r \geq 2$ all G,H, and for $r \geq 1$ if either $G_{cc} = 0$ or $H_{cc} = 0$.

($\mathrm{Ext}^r_{A_{\bar{k}}}(-,-)$ is to be computed in some suitably large category of topological left A_k-modules.)

Proof. The first two isomorphisms are obvious from the category anti-equivalences of the last section.

If H is étale, then $\mathrm{Ext}^1_{\bar{k}}(G,H) = 0$ because the category of finite étale group schemes over $\bar{k}$ is equivalent to the category of finite abelian groups, and a p-divisible group (in the usual sense) is injective in the category of p-torsion groups. $\mathrm{Ext}^{1}_{\bar{k}}(G,H) = 0$ for $H = H_{ce}$ by duality.

Now assume $H = H_{cc}$. Let $\mathrm{Ext}^{r}_{\bar{k}-U}(-,-)$ denote the group of extensions formed in the category of unipotent group schemes over $\bar{k}$. The canonical map $\mathrm{Ext}^{2}_{\bar{k}-U}(L,N) \longrightarrow \mathrm{Ext}^{2}_{\bar{k}}(L,N)$ is injective for all unipotent L and N by [19, VII Lemma 4.1]. It is easily seen to be surjective for $L = \alpha_p = N$ by using the exact sequence $0 \longrightarrow \alpha_p \longrightarrow \mathbb{G}_a \longrightarrow \mathbb{G}_a \longrightarrow 0$ and that $\mathrm{Ext}^{2}_{\bar{k}}(\alpha_p, \mathbb{G}_a) = 0$. This suffices to prove surjectivity for all finite L and N, and consequently that $\mathrm{Ext}^{2}_{\bar{k}-U}(L,N) \approx \mathrm{Ext}^{2}_{\bar{k}}(L,N)$ for all such L and N. The map $\mathrm{Ext}^{2}_{\bar{k}-U}(L,N) \longrightarrow \mathrm{Ext}^{2}_{A_{\bar{k}}}(D_{\bar{k}}(N), D_{\bar{k}}(L))$ is injective, so to prove that $\mathrm{Ext}^{2}_{\bar{k}}(G,H) = 0$ we have only to prove that $\mathrm{Ext}^{2}_{A_{\bar{k}}}(D_{\bar{k}}(H), D_{\bar{k}}(G)) = 0$. Since $\mathrm{Ext}^{3}_{\bar{k}}(G,N) = 0$ for all finite group schemes N, we may replace H by a p-divisible isogenous to it, and so assume the existence of an exact sequence

$$0 \longrightarrow A_{\bar{k}} \longrightarrow A_{\bar{k}} \longrightarrow D_{\bar{k}}(H) \longrightarrow 0 .$$

This proves the result.

We may now prove proposition 2 for the case that $G_{cc} = 0$ or $H_{cc} = 0$. Note first that $c_{G^t}(T) = c_G(q/T)$ and $m_{G^t}(T) = m_G(q/T)$ so the proposition is true for the pair G,H if and only if it is true for the pair H^t, G^t. If G and H are both étale then the proof of the proposition is as in the case with $p \neq$ characteristic of k. By duality the proposition follows for $G = G_{ce}$, $H = H_{ce}$. The remaining cases may be checked by very easy calculations.

For the rest of this section we assume that <u>all finite and p-divisible groups are connected with connected duals</u>.

<u>Lemma 2</u>. For all p-divisible groups G and H over k,

$$\operatorname{Ext}^1_{\overline{k}} (\overline{G}, \overline{H})_\Gamma = 0 .$$

<u>Proof</u>. If M and N are finite group schemes over k, then $\operatorname{Ext}^2_{\overline{k}} (\overline{M}, \overline{N})_\Gamma = 0$. This is true for $M = \alpha_p = N$ because $\operatorname{Ext}^2_{\overline{k}} (\alpha_p, \alpha_p) = \overline{k}$, and it follows in general by induction on the lengths of M and N.

If $p^\nu N = 0$, then $\operatorname{Ext}^2_{\overline{k}} (\overline{G}, \overline{N}) \xrightarrow{\approx} \operatorname{Ext}^2_{\overline{k}} (\overline{G}_\nu, \overline{N})$ so $\operatorname{Ext}^2_{\overline{k}} (\overline{G}, \overline{N})_\Gamma = 0$. This shows that in proving the lemma we may replace H by a group isogenous to it. In fact we may assume there is an exact sequence

$$0 \longrightarrow A_k \longrightarrow A_k \longrightarrow D_k\,(H) \longrightarrow 0.$$

This gives, after tensoring with $W_{\bar{k}}$ over W_k, an exact sequence $0 \longrightarrow A_{\bar{k}} \longrightarrow A_{\bar{k}} \longrightarrow D_{\bar{k}}(H) \longrightarrow 0$, and so

$$0 \longrightarrow \mathrm{Hom}\,(\bar{G},\, \bar{H}) \longrightarrow D_{\bar{k}}(\bar{G}) \longrightarrow D_{\bar{k}}(\bar{G}) \longrightarrow \mathrm{Ext}^1_{\bar{k}}(\bar{G},\bar{H}) \longrightarrow 0.$$

But $D_{\bar{k}} \approx W_{\bar{k}} \otimes_{W_k} D_k(G) \approx \oplus^g\, W_{\bar{k}}$ (as a Γ-module) so $D_{\bar{k}}(\bar{G})_\Gamma = 0$, and the lemma follows.

Lemma 3. For finite group schemes L and N over k, there is a spectral sequence

$$H^r(\Gamma,\ \mathrm{Ext}^s_{\bar{k}}\,(\bar{L},\, \bar{N})) \Longrightarrow \mathrm{Ext}^{r+s}_k\,(L,\, N)\ .$$

Proof. Consider the diagram of functors

$$\begin{tikzcd}
(\text{Ind-Gps}) \arrow[rr, "\alpha"] \arrow[dr, "\gamma"'] & & (\Gamma\text{-mdls}) \arrow[dl, "\beta"] \\
& (\text{Ab}) &
\end{tikzcd}$$

where (Ind-Gps) is the category of inductive systems of finite group schemes (connected with connected duals) over k, (Γ-mdls) is the category of discrete Γ-modules, (Ab) is the category of abelian groups,

$\alpha(N) = \mathrm{Hom}_{\bar{k}}\,(\bar{L},\bar{N})$, $\beta(M) = M^\Gamma$, and $\gamma(N) = \mathrm{Hom}_k(L,N)$.

(Ind-Gps) and (Γ-mdls) both have enough injectives, and we claim that the spectral sequence $R^r\beta(R^s\alpha(N)) \Longrightarrow R^{r+s}\gamma(N)$ exists and is the sequence above. For this it suffices to check

(a) $\beta\cdot\alpha = \gamma$, i.e., $\mathrm{Hom}_{\bar{k}}(\bar{L},\bar{N})^{\Gamma} = \mathrm{Hom}_k(L,N)$, but this is clear.

(b) α is left exact and $R^s\alpha(N) = \mathrm{Ext}^s_{\bar{k}}(\bar{L}, \bar{N})$. $N \longmapsto \bar{N} = N \otimes_k \bar{k}$ is exact, so α is left exact. Let I be the injective envelope of α_p. Any other injective in (Ind-Gps) is a direct sum of copies of I [5] and $\bar{I} = I \otimes_k \bar{k}$ is the injective envelope of $\bar{\alpha}_p$. Thus $- \otimes_k \bar{k}$ carries an injective resolution of N to an injective resolution of $\bar{N}$, and (b) follows.

(c) $R^r\beta(M) = H^r(\Gamma,M)$.

(d) $R^r\gamma(N) = \mathrm{Ext}^r_k(L, N)$.

(e) α takes injectives to acyclics. $\alpha(I) = \mathrm{Hom}_{\bar{k}}(\bar{L},\bar{I}) = D_{\bar{k}}(\bar{L})$ [18, §4.2] and $D_{\bar{k}}(\bar{L}) \approx W_{\bar{k}} \otimes_{W_k} D_k(L)$ which is an acyclic Γ-module.

Lemma 4. $\mathrm{Ext}^1_{\bar{k}}(\bar{G}, \bar{H})^{\Gamma}$ is finite all G, H.

<u>Proof</u>. $\mathrm{Hom}_{\overline{k}}(\overline{G}, \overline{H})$ has finite rank over $\mathbb{Z}_p$, so

$$\mathrm{rk}_{\mathbb{Z}_p}(\mathrm{Hom}_{\overline{k}}(\overline{G}, \overline{H})^{\Gamma}) = \mathrm{rk}_{\mathbb{Z}_p}(\mathrm{Hom}_{\overline{k}}(\overline{G}, \overline{H})_{\Gamma}) .$$

$\mathrm{Ext}^2_{\overline{k}}(\overline{G}, \overline{N})^{\Gamma}$ is finite for all finite group schemes N over k, so we may replace H by an isogenous p-divisible group. Thus we may assume there is an exact sequence

$$0 \longrightarrow A_k \longrightarrow A_k \longrightarrow D_k(H) \longrightarrow 0,$$

which gives an exact sequence

$$0 \longrightarrow \mathrm{Hom}_k(G,H) \longrightarrow D_k(G) \longrightarrow D_k(G) \longrightarrow \mathrm{Ext}^1_k(G,H) \longrightarrow 0.$$

Since $D_k(G)$ is finitely generated over $\mathbb{Z}_p$,

$$\mathrm{rk}_{\mathbb{Z}_p}(\mathrm{Hom}(G,H)) = \mathrm{rk}_{\mathbb{Z}_p}(\mathrm{Ext}^1_k(G,H)).$$

Lemma 3 implies the existence of an exact sequence

$$0 \longrightarrow \mathrm{Hom}_{\overline{k}}(\overline{G}, \overline{H})_{\Gamma} \longrightarrow \mathrm{Ext}^1_k(G,H) \longrightarrow \mathrm{Ext}^1_{\overline{k}}(\overline{G}, \overline{H})^{\Gamma} \longrightarrow 0.$$

The first two groups are finitely generated of the same rank over $\mathbb{Z}_p$, therefore the last group is finite.

Thus we have shown that f_r is a quasi-isomorphism for all $r \neq 0$. Let $f\colon \mathrm{Hom}_k(G,H) \longrightarrow \mathrm{Ext}^1_k(G,H)$ be the composite of the maps

$$\mathrm{Hom}_k(G,H) \xrightarrow{\approx} \mathrm{Hom}_{\bar{k}}(\bar{G},\bar{H})^{\Gamma} \xrightarrow{f_o} \mathrm{Hom}_{\bar{k}}(\bar{G},\bar{H})_{\Gamma} \xrightarrow{g} \mathrm{Ext}_k(G,H)$$

where g is the map induced by the spectral sequence of Lemma 3. g is a quasi-isomorphism and $z(g) = z(f_1)^{-1}$. Thus we are reduced to proving the following statement for G and H.

(S): If no multiple root of $m_G(T)$ or $m_H(T)$ occurs as a root of the other, then f is a quasi-isomorphism and

$$(5.2) \qquad z(f) = \left| q^{\dim(G^t)\dim(H)} \prod_{\alpha_i \neq \beta_j} \left(1 - \frac{\alpha_i}{\beta_j}\right) \right|_p \quad .$$

Lemma 5. If G' and H' are p-divisible groups isogenous to G and H respectively, then (S) is true for the pair G',H' if and only if it is true for the pair G,H.

Proof. The $\mathrm{Ext}_k^r(G,-)$ sequence of the given sequence $0 \longrightarrow N \longrightarrow H' \longrightarrow H \longrightarrow 0$ may be broken into exact sequences

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Hom}_k(G,N) \arrow[r] & \mathrm{Hom}_k(G,H') \arrow[r] \arrow[d, "f'"] & \mathrm{Hom}_k(G,H) \arrow[r] \arrow[d, "f"] & C_o \arrow[r] & 0 \\
0 \arrow[r] & C_1 \arrow[r] & \mathrm{Ext}_k^1(G,H') \arrow[r] & \mathrm{Ext}_k^1(G,H) \arrow[r] & \mathrm{Ext}_k^2(G,N) \arrow[r] & 0
\end{tikzcd}$$

$$0 \longrightarrow C_o \longrightarrow \mathrm{Ext}_k^1(G,N) \longrightarrow C_1 \longrightarrow 0 .$$

Thus, $\frac{z(f')}{z(f)} = \left|\frac{[\mathrm{Ext}^1(G,N)]}{[\mathrm{Hom}(G,N)][\mathrm{Ext}^2(G,N)]}\right|_p$ provided the orders occurring on the right are finite.

If $p^\nu N = 0$, then the sequence

$$0 \longrightarrow \mathrm{Hom}_k(G,N) \xrightarrow{p^\nu} \mathrm{Hom}_k(G,N) \longrightarrow \mathrm{Hom}_k(G_\nu,N)$$

shows that $\mathrm{Hom}_k(G,N) = 0$.

The methods of [26,II] suffice to show $\mathrm{Ext}^r_k(\mathbb{G}_a,\mathbb{G}_a) = 0$ all $r \geq 2$ over any perfect field, and from this it follows that $\mathrm{Ext}^2_k(G, \mathbb{G}_a) = 0$. From the sequence

$$0 \longrightarrow A_k \xrightarrow{V} A_k \longrightarrow D_k(\mathbb{G}_a) \longrightarrow 0$$

we get that $\mathrm{Ext}^1_k(G,\mathbb{G}_a) = D_k(G)/VD_k(G)$ is finite, and from

$$0 \longrightarrow \alpha_p \longrightarrow \mathbb{G}_a \longrightarrow \mathbb{G}_a \longrightarrow 0$$

we get an exact sequence

$$0 \longrightarrow \mathrm{Ext}^1_k(G,\alpha_p) \longrightarrow \mathrm{Ext}^1_k(G,\mathbb{G}_a) \longrightarrow \mathrm{Ext}^1_k(G,\mathbb{G}_a) \longrightarrow \mathrm{Ext}^2_k(G,\alpha_p) \longrightarrow 0$$

which shows that the groups $\mathrm{Ext}^1_k(G,\alpha_p)$ and $\mathrm{Ext}^2_k(G,\alpha_p)$ are finite and have the same order. The same conclusion follows with α_p replaced by an arbitrary finite N by induction on the length of N. This shows that $z(f) = z(f')$, as should be so, because the right hand side of (5.2) is unchanged when H is replaced by H'.

The rest of the lemma may be proved by a similar argument, or by duality.

By §4, proposition 1, it now suffices to prove (S) under the following assumptions on G and H.

$$D_k(G) = A/A\lambda_1, \quad \lambda_1 = P_1(F^a, V^a), \quad T^{n_1/a} P_1(T, \tfrac{q}{T}) = m_G(T)$$

$$g = \text{height } (G), \quad n_1 = \dim (G), \quad m_1 = g - n_1 = \dim (G^t)$$

$$D_k(H) = A/A\lambda_2, \quad \lambda_2 = P_2(F^a, V^a), \quad T^{n_2/a} P_2(T, \tfrac{q}{T}) = m_H(T)$$

$$h = \text{height } (H), \quad n_2 = \dim (H), \quad m_2 = h - n_2 = \dim (H^t) .$$

$m_G(T)$ and $m_H(T)$ are each powers of a $\mathbb{Z}_p$-irreducible polynomial.

<u>Case 1</u>. $m_G(T)$ and $m_H(T)$ have no common root.

The sequence

$$0 \longrightarrow A_k \xrightarrow{\lambda_2} A_k \longrightarrow D_k(H) \longrightarrow 0$$

where λ_2 denotes the map defined by multiplication by λ_2, gives an exact sequence

$$0 \longrightarrow \mathrm{Hom}_k(G,H) \longrightarrow A/A\lambda_1 \xrightarrow{\lambda_2} A/A\lambda_1 \longrightarrow \mathrm{Ext}_k^1(G,H) \longrightarrow 0.$$

But multiplication by λ_2 is injective on $A/A\lambda_1$, so $\mathrm{Hom}(G,H) = 0$, and we have only to compute the order of $\mathrm{Ext}^1(G,H)$.

$$z(f) = |[\mathrm{Ext}^1(G,H)]|_p = \left|\det(1\otimes\lambda_2)\right|_p^a = \frac{|\det(m_H(F^a))|_p^a}{|\det(F^{n_2})|_p^a}$$

where

$$\begin{tikzcd}
A'/A'\lambda_1 \arrow[rr, "1 \otimes \lambda_2"] & & A'/A'\lambda_1 \\
& A'/A'\lambda_1 \arrow[ul, "F^{n_2}"] \arrow[ur, "m_H(F^a)"'] &
\end{tikzcd}$$

$$|\det\,(F^{n_2})|_p^a = |\alpha_1 \cdots \alpha_g|_p^{n_2} = |q^{n_1 n_2}|_p$$

$$\left|\det(m_H(F^a))\right|_p^a = \left|\prod(\alpha_i - \beta_j)\right|_p = \left|q^{n_2 g} \prod\left(1 - \frac{\alpha_i}{\beta_j}\right)\right|_p .$$

Thus $z(f) = \left|q^{m_1 n_2} \prod\left(1 - \frac{\alpha_i}{\beta_j}\right)\right|_p$, and the formula is verified for this case.

Case 2. $m_G(T)$ and $m_H(T)$ have a root in common, i.e., are powers of the same $\mathbb{Z}_p$-irreducible polynomial. The condition that no multiple root of one of $m_G(T)$ or $m_H(T)$ is a root of the other implies that $m_G(T)$ and $m_H(T)$ are themselves irreducible, and consequently are equal.

We must first give an explicit description of the map $f\colon \mathrm{Hom}_k(G,H) \longrightarrow \mathrm{Ext}^1_k(G,H)$. The $\mathrm{Ext}^r_{\bar{k}}(-,D_{\bar{k}}(\bar{G}))$ sequence of

$$0 \longrightarrow A_{\bar{k}} \xrightarrow{\cdot\bar{\lambda}_2} A_{\bar{k}} \longrightarrow D_{\bar{k}}(\bar{H}) \longrightarrow 0$$

may be split into short exact sequences

$$(6.3) \qquad 0 \longrightarrow \mathrm{Hom}_{\bar{k}}(\bar{G},\ \bar{H}) \longrightarrow \bar{M} \xrightarrow{\bar{\lambda}_2\cdot} \bar{\lambda}_2\ \bar{M} \longrightarrow 0$$

$$(6.4) \qquad 0 \longrightarrow \bar{\lambda}_2\ \bar{M} \longrightarrow \bar{M} \longrightarrow \mathrm{Ext}^1_{\bar{k}}(\bar{G},\ \bar{H}) \longrightarrow 0$$

where $M = D_k(G)$. These in turn give an exact, commutative diagram

$$\begin{tikzcd}
 & & & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \mathrm{Hom}(\overline{G},\overline{H})^{\Gamma} \arrow[r] \arrow[d, phantom, "\wr"] & M \arrow[r, "\lambda_2 \cdot"] \arrow[d, equal] & (\overline{\lambda}_2\overline{M})^{\Gamma} \arrow[r] \arrow[d] & \mathrm{Hom}(\overline{G},\overline{H})_{\Gamma} \arrow[r] \arrow[d, "g"] & 0 \\
0 \arrow[r] & \mathrm{Hom}(G,H) \arrow[r] & M \arrow[r, "\lambda_2 \cdot"] \arrow[d] & M \arrow[r] \arrow[d] & \mathrm{Ext}^1(G,H) \arrow[r] \arrow[d] & 0 \\
 & & 0 \arrow[r] & \mathrm{Ext}^1(\overline{G},\overline{H})^{\Gamma} \arrow[r] \arrow[d] & \mathrm{Ext}^1(\overline{G},\overline{H})^{\Gamma} \arrow[r] \arrow[d] & 0 \\
 & & & 0 & 0 &
\end{tikzcd}$$

The top row comes from the (6.3) and the serpent lemma, and the third column from (6.4) and the serpent lemma. The rest of the diagram is filled in with the obvious maps. We observe that g is the map given by the spectral sequence of Lemma 4.

The map f may be described as follows: let $u \in \mathrm{Hom}(G,H)$ and regard u as an element of M such that $\lambda_2 u = 0$. u may be written $u = (\sigma_k - 1)v$, $v \in \overline{M}$. $\overline{\lambda}_2 v \in \overline{\lambda}_2\overline{M}$, but

$$(\sigma_k-1)(\lambda_2 v) = \lambda_2(\sigma_k-1)v = \lambda_2 u = 0, \text{ so } \overline{\lambda}_2 v \in (\overline{\lambda}_2\overline{M})^{\Gamma}.$$

Regard $\overline{\lambda}_2 v$ as an element of M, then its image in $\mathrm{Ext}^1(G,H)$ is f(u).

In our case, $\lambda_2 = \lambda_1$ so multiplication by λ_2 is zero on M, and $\mathrm{Hom}(G,H) = A/A\lambda_1 = \mathrm{Ext}(G,H)$. Since $A/A\lambda_1$ is torsion-free, f is a quasi-isomorphism if and only if the corresponding map $A'/A'\lambda_1 \xrightarrow{f} A'/A'\lambda_1$ has nonzero determinant, and then $z(f) = |\det(f)|_p^a$.

Let $u \in A'/A'\lambda_1$ and choose $v \in \overline{A}'/\overline{A}'\lambda_1$ such that $u = \sigma_k v - v$. Then $\sigma_k^i v = iu + v$ for all i. Let

$$P_2(F^a, q^a/F^a) = F^{m_2} + b_{m_2-a}F^{m_2-a} + \cdots + \frac{b_{-n_2}}{F^{n_2}} = F^{-n_2}m_H(F^a) \text{ .}$$

Then $f(u) = P_2(F^a, q^a/F^a)v$

$$= m_2 u F^{m_2} + (m_2-a)b_{m_2-a}uF^{m_2-a} + \cdots \text{ (as } v\lambda_2 = 0)$$

$$= u F^a \frac{d}{dF^a}(F^{-n_2} m_H(F^a))$$

$$= F^{a-n_2} \cdot \frac{d}{dF^a}(m_H(F^a)) \cdot u \text{ .}$$

Clearly f is a quasi-isomorphism, and

$$z(f) = \frac{\left|\det(\frac{d}{dF^a}(m_H(F^a)))\right|_p^a}{\left|\det(F^{n_2-a})\right|_p^a} \qquad \text{where}$$

$$\begin{tikzcd}
A'/A'\lambda_1 \arrow[rr, "f"] & & A'/A'\lambda_1 \\
& A'/A'\lambda_1 \arrow[ul, "F^{n_2-a}"] \arrow[ur, "\frac{d}{dF^a}(m_H(F^a))"'] &
\end{tikzcd}$$

$$\left|\det(F^{n_2-a})\right|_p^a = \left|q^{n_1(n_2-a)}\right|_p$$

$$\left|\det(\frac{d}{dF^a}(m_H(F^a)))\right|_p^a = \left|\prod_{\alpha_i\neq\beta_j}(\alpha_i-\beta_j)\right|_p$$

$$= \left|q^{n_1(g-a)}\prod_{\alpha_i\neq\beta_j}(1-\frac{\alpha_i}{\beta_j})\right|_p .$$

Thus $z(f) = \left|q^{n_1m_2}\prod_{\alpha_i\neq\beta_j}(1-\frac{\alpha_i}{\beta_j})\right|_p$, which completes the proof of the proposition.

6. The Proof of the Conjecture

In this section, X will be a complete, connected, smooth, algebraic curve over a finite field k, K will be the function field of X, and K_v the completion of K corresponding to the closed point v of X.

Proposition 3. For any abelian scheme A over X, there is an exact sequence

$$0 \longrightarrow H^1(X,A) \longrightarrow H^1(\text{spec } K, A_K) \longrightarrow \oplus_v H^1(\text{spec } K_v, A_{K_v})$$

i.e., $H^1(X,A) = Ш(A_K)$, the Tate-Šafarevič group of A_K over K.

Proof. Since A is smooth, we may work with the étale topology. Let π: spec K $\longrightarrow$ X be the canonical inclusion map. For any étale morphism

$$U \longrightarrow X,\ \text{Mor}_K(U_K,A_K) \approx \text{Mor}_X(U_K,A) \approx \text{Mor}_X(U,A) \quad [10, II7.3.6]$$

so the sheaf defined by A on X_{et} is isomorphic to $\pi_* A_K$. By [6, IV §3] the principal homogeneous spaces for A over X may be canonically identified with the principal homogeneous spaces for A_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. A principal homogeneous space for A over $\tilde{K}_v$ may be represented by a projective scheme P over $\tilde{K}_v$ [41], so there exists a projective scheme P' over $\tilde{R}_v$ such that $P \approx P' \otimes_{\tilde{R}_v} \tilde{K}_v$. Let $\hat{R}_v$ be the completion of $\tilde{R}_v$ and $\hat{K}_v$ its field of fractions. By using [8], one sees that the following are equivalent: P has a point in $\tilde{K}_v$; P' has a point in $\tilde{R}_v/t^n\tilde{R}_v = \hat{R}_v/t^n\hat{R}_v$ ($t\tilde{R}_v$ = maximal ideal of $\tilde{R}_v$) for all sufficiently large n; P' has a point in $\hat{R}_v$; P has a point in $\hat{K}_v$. It follows that thereis an exact sequence

$$0 \longrightarrow H^1(X,A) \longrightarrow H^1(\text{spec } K, A_K) \longrightarrow \oplus_v H^1(\text{spec } \hat{K}_v, A_{K_v}) .$$

The injectivity of the canonical maps

$$H^1(\text{spec } K_v, A_{K_v}) \longrightarrow H^1(\text{spec } \hat{K}_v, A_{K_v}) \quad [7, \text{ p. } 265]$$

shows that the sequence remains exact if $\hat{K}_v$ is replaced by K_v.

Let G be a p-divisible group over k. The projective limit of the sequences

$$0 \longrightarrow H^r(\overline{X},\overline{G}_\nu)^\Gamma \longrightarrow H^r(\overline{X},\overline{G}_\nu) \xrightarrow{\sigma_{k-1}} H^r(\overline{X},\overline{G}_\nu) \longrightarrow H^r(\overline{X},\overline{G}_\nu)_\Gamma \longrightarrow 0$$

is a sequence

$$\varprojlim_\nu(H^r(\overline{X},\overline{G}_\nu)^\Gamma) \longrightarrow H^r(\overline{X},T_p\overline{G}) \xrightarrow{\sigma_k-1} H^r(\overline{X},T_p\overline{G}) \longrightarrow \varprojlim_\nu(H^r(\overline{X},\overline{G}_\nu)_\Gamma).$$

Lemma 6. The maps $\varprojlim(H^r(\overline{X},\overline{G}_\nu)^\Gamma) \longrightarrow H^r(\overline{X},T_p\overline{G})^\Gamma$

$$H^r(\overline{X}, T_p\overline{G})_\Gamma \longrightarrow \varprojlim_\nu (H^r(\overline{X},\overline{G}_\nu)_\Gamma)$$

induced by the above sequence are isomorphisms.

Proof. The first isomorphism is a consequence of the left exactness of the projective limit functor. If $r = 0$, or $G_{cc} = 0$, then the groups $H^r(\overline{X}, \overline{G}_\nu)$ are finite and the second isomorphism is immediate. If $r = 2$ and $G = G_{cc}$, then the Hochschild-Serre spectral sequence for $\overline{X}/X$ gives an injection $H^2(\overline{X},\overline{G}_\nu)_\Gamma \longrightarrow H^3(X,G_\nu) = 0$. By corollary 3 to Theorem 1, and (the dual of) Lemma 2,
$H^2(\overline{X}, T_p\overline{G})_\Gamma = \mathrm{Ext}^1_{\overline{k}}(T_p\overline{J}, T_p\overline{G})_\Gamma = 0$, where J is the Jacobian of X. Thus only the map

$H^1(\overline{X}, T_p\overline{G})_\Gamma \longrightarrow \varprojlim_\nu (H^1(\overline{X}, \overline{G}_\nu)_\Gamma)$ with $G = G_{cc}$ remains to be considered. By duality and the above-mentioned corollary, this map will be an isomorphism if $\mathrm{Hom}_{\overline{k}}(\overline{G}, \overline{H})_\Gamma \longrightarrow \varprojlim_\nu (\mathrm{Hom}_{\overline{k}}(\overline{G}_\nu, \overline{H})_\Gamma)$ is an isomorphism for all p-divisible groups G and H over k with $G = G_{cc}$, $H = H_{cc}$.

The sequence

$$0 \longrightarrow G_\nu \longrightarrow G \xrightarrow{p^\nu} G \longrightarrow 0$$

gives exact sequences

$$0 \to \mathrm{Hom}_{\overline{k}}(\overline{G}, \overline{H})^{(p^\nu)} \longrightarrow \mathrm{Hom}_{\overline{k}}(\overline{G}_\nu, \overline{H}) \longrightarrow {}_{p^\nu}\mathrm{Ext}^1_{\overline{k}}(\overline{G}, \overline{H}) \longrightarrow 0$$

and

$$({}_{p^\nu}\mathrm{Ext}^1(\overline{G},\overline{H}))^\Gamma \longrightarrow (\mathrm{Hom}(\overline{G},\overline{H})^{(p^\nu)})_\Gamma \longrightarrow \mathrm{Hom}(\overline{G}_\nu,\overline{H})_\Gamma \longrightarrow ({}_{p^\nu}\mathrm{Ext}^1(\overline{G},\overline{H}))_\Gamma \to 0$$

A direct computation taking $\overline{G}$ and $\overline{H}$ to be p-divisible groups with $D_{\overline{k}}(\overline{G}) = A_{\overline{k}}/A_{\overline{k}}(F^m - V^n)$ and $D_{\overline{k}}(\overline{H}) = A_{\overline{k}}/A_{\overline{k}}(F^{m'} - V^{n'})$ (cf. [18, II §4]) shows that $\mathrm{Ext}^1(\overline{G}, \overline{H})$ is killed by some power of p, and consequently that $({}_{p^\nu}\mathrm{Ext}^1(\overline{G},\overline{H}))_\Gamma = \mathrm{Ext}^1(\overline{G},\overline{H})_\Gamma = 0$ for ν large. Also we know that $\mathrm{Ext}^1(\overline{G},\overline{H})^\Gamma$ is finite (lemma 4) and that $\mathrm{Hom}(\overline{G},\overline{H})$ is a free $\mathbb{Z}_p$-module of finite rank. These facts combine to show that the projective limit of the above exact sequence reduces to the required isomorphism.

<u>Proposition 4</u>. For any abelian variety A over k and any prime p, $\text{Ш}(A_K)(p)$ is finite.

<u>Proof</u>. From the exact sequences

$$0 \longrightarrow A_\nu \longrightarrow A \xrightarrow{p^\nu} A \longrightarrow 0 \qquad\qquad \nu \geq 0$$

we get exact sequences

$$(6.1) \qquad 0 \longrightarrow H^0(X,A)^{(p^\nu)} \longrightarrow H^1(X,A_\nu) \longrightarrow {}_{p^\nu}\text{Ш} \longrightarrow 0$$

whose projective limit,

$$(6.2) \qquad 0 \longrightarrow H^0(X,A) \otimes \mathbb{Z}_p \longrightarrow H^1(X,T_pA) \longrightarrow T_p(\text{Ш}) \longrightarrow 0$$

is also exact (because the groups are finite).

The Hochschild-Serre spectral sequence for $\overline{X}/X$ gives exact sequences

$$(6.3) \qquad 0 \longrightarrow H^0(\overline{X},\overline{A}_\nu)_\Gamma \longrightarrow H^1(X,A_\nu) \longrightarrow H^1(\overline{X}, \overline{A}_\nu)^\Gamma \longrightarrow 0$$

with exact projective limit

$$(6.4)\quad 0 \longrightarrow H^{0}(\overline{X},\ T_p\overline{A})_{\Gamma} \longrightarrow H^{1}(X, T_pA) \longrightarrow H^{1}(\overline{X}, T_p\overline{A})^{\Gamma} \longrightarrow 0 .$$

$A(\overline{k})^{\Gamma} = A(k)$, and $A(\overline{k})_{\Gamma} = 0$ [14], so the exact sequence $0 \longrightarrow A_{\nu}(\overline{k}) \longrightarrow A(\overline{k}) \xrightarrow{p^{\nu}} A(\overline{k}) \longrightarrow 0$ gives an isomorphism, $A(k)^{(p^{\nu})} \approx A_{\nu}(\overline{k})_{\Gamma}$, which in the limit gives $A(k)(p) \approx \varprojlim(A_{\nu}(\overline{k})_{\Gamma}) \approx H^{0}(\overline{X},\ T_p\overline{A})_{\Gamma}$. (6.4) may be written

$$(6.5)\quad 0 \longrightarrow A(k) \longrightarrow H^{1}(X, T_pA) \longrightarrow H^{1}(\overline{X},\ T_p\overline{A})^{\Gamma} \longrightarrow 0.$$

By [15, II §2. Theorem 9] there is an exact sequence

$$(6.6)\quad 0 \longrightarrow A(k) \longrightarrow A(K) \longrightarrow \mathrm{Hom}\ (J,A) \longrightarrow 0 .$$

Consider the diagram

$$(6.7)\quad \begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & & \\
0 \arrow[r] & A(k)\otimes\mathbb{Z}_p \arrow[r] \arrow[d] & A(k)(p) \arrow[r] \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & A(K)\otimes\mathbb{Z}_p \arrow[r] \arrow[d] & H^{1}(X,T_pA) \arrow[r] \arrow[d] & T_p(\text{Ш}) \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & \mathrm{Hom}(J,A)\otimes\mathbb{Z}_p \arrow[r] \arrow[d] & H^{1}(\overline{X},T_p\overline{A})^{\Gamma} \arrow[r] \arrow[d] & T_p(\text{Ш}) \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

where the left hand column comes from (6.6), the middle column is (6.5), the middle row is (6.3) and the maps and exactness of the bottom row are induced by the rest of the diagram. By corollary 3 and the final remark in §2, the map $\mathrm{Hom}(J,A) \otimes \mathbb{Z}_p \longrightarrow H^1(\bar{X},T_p\bar{A})^{\Gamma}$ may be identified with the canonical map $\mathrm{Hom}_k(J,A)\otimes\mathbb{Z}_p \longrightarrow \mathrm{Hom}_{\bar{k}}(T_p\bar{J}, T_p\bar{A})^{\Gamma}$ which, by [37] and [38] is surjective. Thus $T_p(\text{Ш}) = 0$, i.e., the p-divisible part of Ш is zero, and it is known [17] that this implies that the p-primary component of Ш is finite.

Remark. The same argument, with k algebraically closed instead of finite, gives an exact sequence

$$0 \longrightarrow \mathrm{Hom}(J,A) \otimes \mathbb{Z}_p \longrightarrow \mathrm{Hom}(T_pJ,T_pA) \longrightarrow T_p(\text{Ш}) \longrightarrow 0.$$

Thus, $r+r_o = \mathrm{rk}_{\mathbb{Z}_p}(\mathrm{Hom}(T_pJ,T_pA))$ where $r = \mathrm{rk}_{\mathbb{Z}}(A(K))$ and r_o is the corank of the p-divisible part of $\text{Ш}(A_K)$. In particular, if $p \nmid$ characteristic of k, then $r+r_o = 4dg$ where d = dimension of A and g = genus of X, and we recover the formula of Ogg-Šafarevič [25], [27], [29] in this very special case.

Theorem 3. Let A be an abelian variety over k. The conjecture (B) holds for A_K over K.

Proof. Consider the diagram

$$\begin{tikzcd}
A(K) \otimes \mathbb{Z}_p \arrow[r, "e"] \arrow[d, "h"] & \mathrm{Hom}(A^t(K), \mathbb{Z}_p) \arrow[r, phantom, "\approx"] & \mathrm{Hom}(A^t(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p, \mathbb{Q}_p/\mathbb{Z}_p) \\
H^1(\overline{X}, T_p\overline{A})^\Gamma \arrow[r, "f"] & H^1(\overline{X}, T_p\overline{A})_\Gamma \arrow[r, "c"] & \mathrm{Hom}(H^1(\overline{X}, \overline{A}^t(p))^\Gamma, \mathbb{Q}_p/\mathbb{Z}_p) \arrow[u, "g^*"]
\end{tikzcd}$$

where the maps are to be defined.

e is induced by the pairing

$$(\ ,\ ) : A(K) \times A^t(K) \longrightarrow \mathbb{Z}$$

of §3. Because of the difference in the norming of the absolute values, $(a',a) = \frac{\langle a',a \rangle}{\log q}$, where $\langle\ ,\ \rangle$ is the symbol used in the Introduction and [35, §1]. By [35, lemma z.1] and the nondegeneracy of the height pairing, e is a quasi-isomorphism and

$$z(e) = \frac{\left| \det \frac{\langle a_i', a_j \rangle}{\log q} \right|_p}{\left| [A(K)_{tors}] \right|_p}$$

where $(a_i)_{1 \leq i \leq r}$ and $(a_i')_{1 \leq i \leq r}$ are bases for A(K) and $A^t(K)$ respectively, modulo torsion.

h is the diagonal map of the lower left square of (6.7). Since $T_p(Ш) = 0$, h is a quasi-isomorphism, and

$$z(h) = \frac{1}{|[A(k)]|_p} = \frac{1}{|[A(K)_{tors}]|_p} .$$

The isomorphism of the top row is obvious. After passing to the inductive limit and replacing A by A^t, (6.1) and (6.3) read

$$0 \longrightarrow H^o(X,A^t) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow H^1(X,A^t(p)) \longrightarrow Ш'(p) \longrightarrow 0$$

$$0 \longrightarrow H^o(\bar{X},\bar{A}^t(p))_\Gamma \longrightarrow H^1(X, A^t(p)) \longrightarrow H^1(\bar{X},\bar{A}^t(p))^\Gamma \longrightarrow 0$$

where $Ш' = Ш(A^t_K)$. But $H^o(\bar{X},\bar{A}^t(p))_\Gamma = H^1(\Gamma,A^t(\bar{k}))(p) = 0$ and $H^o(X,A^t) \otimes \mathbb{Q}_p/\mathbb{Z}_p \approx A^t(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p$, so there is an exact sequence

$$0 \longrightarrow A^t(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{g} H^1(\bar{X},\bar{A}^t(p))^\Gamma \longrightarrow Ш'(p) \longrightarrow 0 .$$

We define g* to be the dual of g. Since $Ш'(p)$ is finite, g* is a quasi-isomorphism and $z(g^*) = \dfrac{1}{|[Ш'(p)]|_p}$.

f is induced by the identity map on $H^1(\bar{X},T_p\bar{A})$. The cup-products defined in §3 give a map

$$H^1(\bar{X}, \bar{A}_\nu) \longrightarrow \mathrm{Hom}\,(H^1(\bar{X}, \bar{A}^t_\nu), \mathbb{Z}/p^\nu\mathbb{Z})$$

and consequently a map

$$H^1(\bar{X},\bar{A}_\nu)_\Gamma \longrightarrow \mathrm{Hom}(H^1(\bar{X},\bar{A}^t_\nu), \mathbb{Z}/p^\nu\mathbb{Z})_\Gamma \approx \mathrm{Hom}(H^1(\bar{X},\bar{A}^t_\nu)^\Gamma, \mathbb{Z}/p^\nu\mathbb{Z}).$$

The duality theorem in the Appendix shows that the cokernel of this map is

$$H^2(\bar{X}, (\bar{A}_\nu)_{cc})^\Gamma \approx \mathrm{Ext}^1_{\bar{k}}\,(T_p\bar{J}, \bar{A}_\nu)^\Gamma \quad \text{(Cor. 3 to Theorem 1)} .$$

Thus, after passing to the projective limit, we get an exact sequence,

$$0 \longrightarrow H^1(\bar{X},T_p\bar{A})_\Gamma \xrightarrow{c} \mathrm{Hom}(H^1(\bar{X},\bar{A}^t(p))^\Gamma, \mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow \mathrm{Ext}^1_{\bar{k}}(T_p\bar{J},T_p\bar{A})^\Gamma \longrightarrow 0.$$

From the remark following proposition 2, f and c are quasi-isomorphisms and

$$z(f)z(c) = \left| q^{dg} \prod_{\alpha_i \neq \omega_j} \left(1 - \frac{\omega_j}{\alpha_i}\right) \right|_p$$

where d = dimension of A, g = genus of X, q = [k], and $(\alpha_i)_{1\leq i\leq 2d}$ and $(\omega_i)_{1\leq i\leq 2g}$ are the roots of the characteristic polynomial of the Frobenius endomorphism of A and J respectively, relative to k.

Theorem 2 shows that the diagram commutes. Consequently we have proved the formula,

$$\left|q^{dg}\prod_{\alpha_i\neq\omega_j}(1-\frac{\omega_j}{\alpha_i}\right|_p = \left|\text{Ш}'(p)\right|_p\left|\det\frac{\langle a_i', a_j\rangle}{\log q}\right|_p .$$

By replacing A by A^t we get the same formula, except with $\text{Ш}'$ replaced by Ш, so $[\text{Ш}'(p)] = [\text{Ш}(p)]$. Since this formula holds for all primes p, $[\text{Ш}]$ is finite and

$$q^{dg}\prod_{\alpha_i\neq\omega_j}(1-\frac{\omega_j}{\alpha_i}) = [\text{Ш}]\left|\det\frac{\langle a_i',a_j\rangle}{\log q}\right| . \tag{6.8}$$

It remains to relate this to the form of the conjecture stated in the Introduction. We use essentially the notation of [35, §1].

Choose for each closed point v of X a Haar measure μ_v on K_v such that $\mu_v(O_v) = 1$. Choose a non-zero invariant exterior differential form ω of degree d on A 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}.

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

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

with

$$Z(X,\ t) = \frac{\prod_{j=1}^{2g}(1-\omega_j t)}{(1-t)(1-q\,t)} = \prod_v \left(\frac{1}{1-t^{\deg v}}\right)$$

we get a rational expression for L(s),

$$L(s) = \prod_{i=1}^{2d} \prod_{j=1}^{2g} \frac{(1-\omega_j \alpha_i q^{-s})}{(1-\alpha_i q^{-s})(1-\alpha_i q^{1-s})} .$$

Thus the order of the zero of L(s) at s = 1 is equal to the number of pairs (i,j) such that $\alpha_i = \omega_j$. But by [37, Theorem 1a], this last number is equal to r, the rank of A(K)(as the first conjecture of Birch and Swinnerton-Dyer predicts). It is now easy to show that

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

But $[A(K)_{tors}] = [A(k)] = [A^t(K)_{tors}]$, so (B) reduces to the equation (6.8), and the proof is complete.

Corollary. Let $f: Y \longrightarrow X$ be a k-morphism of a surface Y onto a curve X for which conjecture (d) of [35] holds and which is such that the Jacobian of the generic fibre of f is defined over k (for example, f the projection of $X \times_k X'$ onto X, where X' is a smooth, complete, connected, algebraic curve over k). Then the Brauer group of Y is finite and its order is given by the conjecture (C) of [35].

Example (Tate). If E_1 and E_2 are two non-isogenous elliptic curves over a finite field k, then the Brauer group of $E_1 \times E_2$ has $(n_1 - n_2)^2$ elements, where $n_1 = [E_1(k)]$ and $n_2 = [E_2(k)]$. If E is a non-supersingular elliptic curve over k, then the Brauer group of $E \times_k E$ has $(\mathrm{End}_k(E): \mathbb{Z}[F_k])^2$ elements, where F_k is the Frobenius endomorphism of E relative to k.

Appendix: Duality in Flat Cohomology

Let X be a complete, connected, smooth, algebraic curve over a field k, and let $\mathbb{G}_m(p) = (\mu_{p^\nu}, i_\nu)$ be the p-divisible group associated to $\mathbb{G}_m$.

Assume first that k is algebraically closed. The argument of §3 gives, in the limit, a cup product pairing

$$H^r(X,N) \times H^{2-r}(X,N^D) \longrightarrow H^2(X, \mathbb{G}_m(p)) \approx \mathbb{Q}_p/\mathbb{Z}_p$$

for all finite group schemes N over k which are killed by some power of p.

Theorem A1: The cup product defined above is a perfect duality of finite abelian groups, for all finite group schemes N over k which are killed by a power of p, and which are such that $N_{cc} = 0$.

Remark: This last restriction is necessary. $H^0(X,\alpha_p) = 0$ for all X, but $H^2(X,\alpha_p) = 0$ if and only if $H^1(X_{Zar},O_X) \xrightarrow{F} H^1(X_{Zar}, O_X)$ is surjective, i.e., if and only if the Jacobian of X has the maximum number of points of order p [30].

Proof: If $p \neq$ characteristic of k, then the theorem is just a very special case of the étale duality theorem of Grothendieck [39], so for the rest of the proof we assume $p =$ characteristic of k.

Observe that, because of the functorial properties of the cup product, we have only to prove the theorem for N equal to one of the simple group schemes μ_p or $\mathbb{Z}/p\mathbb{Z}$.

For any finite p-primary group scheme N over k, Cartier duality gives an isomorphism $\mathrm{Ext}^1_X(\mathbb{Z}/p^\nu\mathbb{Z},N^D) \xrightarrow{\approx} \mathrm{Ext}^1_X(N,\mu_{p^\nu})$ which, in the limit, becomes $\mathrm{Ext}^1_X(\mathbb{Z},N^D) \approx \mathrm{Ext}^1_X(N,\mathbb{G}_m(p))$. This isomorphism in fact holds with X replaced by any object U of X_{fl}, and is functorial in U, so $\underline{\mathrm{Ext}}^1_X(N, \mathbb{G}_m(p))$ is the sheaf associated to the presheaf

$$U \longrightarrow \mathrm{Ext}^1_U(\mathbb{Z},N^D) = H^1(U,N^D) .$$

But this sheaf is zero [2, II 2.5], so $\underline{\mathrm{Ext}}^1_X(N, \mathbb{G}_m(p)) = 0$. Consequently, the edge morphisms $\epsilon_s\colon H^s(X,N^D) \longrightarrow \mathrm{Ext}^s_X(N, \mathbb{G}_m(p))$ of the spectral sequence $H^r(X, \underline{\mathrm{Ext}}^s_X(N, \mathbb{G}_m(p))) \Longrightarrow \mathrm{Ext}^{r+s}_X(N, \mathbb{G}_m(p))$ are isomorphisms for $s = 0$ and 1, and are injections for $s = 2$.

If $N = \mu_p$ and $r = 0$, or $N = \mathbb{Z}/p\mathbb{Z}$ and $r = 2$, the theorem is obvious, for $H^0(X, \mu_p) = 0$ and $H^2(X, \mathbb{Z}/p\mathbb{Z}) = 0$ (because 1-F is surjective on $H^1(X, O_X)$ [so, p. 38]).

Take $N = \mathbb{Z}/p\mathbb{Z}$ and $r = 0$. Since $\mathrm{Ext}^1_X(\mathbb{Z}, \mathbb{G}_m(p)) = H^1(X, \mathbb{G}_m(p)) \approx \mathrm{Pic}(X)(p)$ is p-divisible, the map $\mathrm{Ext}^2_X(\mathbb{Z}/p\mathbb{Z}, \mathbb{G}_m(p)) \longrightarrow \mathrm{Ext}^2_X(\mathbb{Z}, \mathbb{G}_m(p))$ induced by any non-zero map $\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}$ is injective. This shows that the Yoneda pairing

$$H^0(X, \mathbb{Z}/p\mathbb{Z}) \times \mathrm{Ext}^2_X(\mathbb{Z}/p\mathbb{Z}, \mathbb{G}_m(p)) \longrightarrow H^2(X, \mathbb{G}_m(p))$$

is a perfect duality. The same result follows for the cup product pairing, using that $\epsilon_2\colon\ H^2(X, \mu_p) \longrightarrow \mathrm{Ext}^2_X(\mathbb{Z}/p\mathbb{Z}, \mathbb{G}_m(p))$ is injective and $[H^0(X, \mathbb{Z}/p\mathbb{Z})] = p = [H^2(X, \mu_p)]$.

A very similar argument proves the case $N = \mu_p$ and $r = 2$.

Take $N = \mu_p$ and $r = 1$. It is proved in [30, §2] that the two groups $H^1(X, \mathbb{Z}/p\mathbb{Z}) = \ker(1\text{-}F\colon H^1(X, O_X) \longrightarrow H^1(X, O_X))$ and $H^1(X, \mu_p) = {}_p\mathrm{Pic}\, X$ are dual, and we show that the cup product gives essentially the same pairing.

Let $x \in H^1(X, \mathbb{Z}/p\mathbb{Z})$, and let P be a principal homogeneous space for $\mathbb{Z}/p\mathbb{Z}$ over X whose cohomology class is x. There is a finite Galois covering $\pi: X' \longrightarrow X$, group G say; such that P becomes trivial on X' (e.g., take X' to be the scheme representing P). Let $p \in P(X')$. G operates on X' so it operates on $P(X')$, and the equation $\sigma p = p\,\alpha(\sigma)$ $(\sigma \in G, \alpha(\sigma) \in \mathbb{Z}/p\mathbb{Z})$ defines a homomorphism $\alpha: G \longrightarrow \mathbb{Z}/p\mathbb{Z}$. Moreover, x is the image of α under the map $\operatorname{Hom}(G, \mathbb{Z}/p\mathbb{Z}) = H^1(G, \mathbb{Z}/p\mathbb{Z}) \longrightarrow H^1(X, \mathbb{Z}/p\mathbb{Z})$ given by the Hochschild-Serre spectral sequence of X'/X [3, VIII 8], [6, 3.7.6].

Let p_1 and p_2 be the projections $X' \times_X X' \rightrightarrows X'$. The Čech 1-cocycle corresponding to x is (n), $n \in (\mathbb{Z}/p\mathbb{Z})(X' \times_X X')$, where $p_1^*(y)n = p_2^*(y)$. By [3, VIII 9.1], to give a sheaf F on X is the same as to give a sheaf F' on X' together with an isomorphism $\varphi: p_1^*F' \longrightarrow p_2^*F'$ (satisfying certain conditions). In these terms, the image of x under the map $H^1(X, \mathbb{Z}/p\mathbb{Z}) \longrightarrow \operatorname{Ext}^1_X(\mu_p, \mu_p)$ may be described as the class of the sequence

$E: 0 \longrightarrow \mu_p \longrightarrow (\mu_p \times \mu_p)_t \longrightarrow \mu_p \longrightarrow 0$ where

$E' = (0 \longrightarrow \mu_p \longrightarrow \mu_p \times \mu_p \longrightarrow \mu_p \longrightarrow 0)$ and

$\varphi\colon p_1^*E' \longrightarrow p_2^*E'$ is

$$\begin{tikzcd}
0 \arrow[r] & \mu_p \arrow[r] \arrow[d, equal] & \mu_p \times \mu_p \arrow[r] \arrow[d, "\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}"] & \mu_p \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & \mu_p \arrow[r] & \mu_p \times \mu_p \arrow[r] & \mu_p \arrow[r] & 0
\end{tikzcd} .$$

There is a unique isomorphism $\coprod_{\sigma \in G} X'_\sigma \xrightarrow{q} X' \times_X X'$ $(X'_\sigma = X')$ such that $p_1 q$ restricted to X'_σ is the identity map, and $p_2 q$ restricted to X'_σ is the automorphism of X' induced by σ. Thus, to give an isomorphism $\varphi\colon p_1^*E' \longrightarrow p_2^*E'$ is to give an isomorphism $\varphi'\colon (p_1 q)^*E' \longrightarrow (p_2 q)^*E'$. In the above case, φ' is determined by the following operation of G on E': G operates on the μ_p through its operation on X', and $\sigma \in G$ operates on $\mu_p \times \mu_p$ via the matrices $\begin{pmatrix} \sigma & n_\sigma \sigma \\ 0 & \sigma \end{pmatrix}$ where $y n_\sigma = \sigma y$, i.e., $n_\sigma = \alpha(\sigma)$.

The cohomology sequence of E is

$$H^1(X,\mu_p) \longrightarrow H^1(X,(\mu_p \times \mu_p)_t) \xrightarrow{\gamma} H^1(X,\mu_p) \xrightarrow{\delta} H^2(X,\mu_p)$$

and the composite of δ with the injection $H^2(X, \mu_p) \longrightarrow H^2(X, \mathbb{G}_m(p))$ is the map $H^1(X,\mu_p) \longrightarrow H^2(X,\mathbb{G}_m(p))$

taking an element of $H^1(X,\mu_p)$ to its cup product with x. Thus, tc prove the pairing is a duality, we have only to show that δ is non-zero, or equivalently, that γ is not surjective. But the Hochschild-Serre spectral sequence for X'/X gives a commutative diagram

$$\begin{tikzcd}
H^1(X, \mu_p) \arrow[r] \arrow[d, "\approx"] & H^1(X,(\mu_p \times \mu_p)_t) \arrow[r, "\gamma"] \arrow[d, "\approx"] & H^1(X, \mu_p) \arrow[d, "\approx"] \\
H^1(X',\mu_p)^G \arrow[r] & H^1(X', \mu_p \times \mu_p)^G \arrow[r, "\gamma'"] & H^1(X', \mu_p)^G.
\end{tikzcd}$$

$H^1(X', \mu_p \times \mu_p) \approx {}_p\mathrm{Pic}(X') \times {}_p\mathrm{Pic}(X')$ and $\sigma \in G$ operates by $\sigma(u,v) = (\sigma u + \alpha(\sigma)\sigma v, \sigma v)$. Suppose $v \in {}_p\mathrm{Pic}(X')$ is in the image of γ'. Then v is fixed under G, and there exist elements $u \in {}_p\mathrm{Pic}(X')$ and $\sigma \in G$ such that $\sigma u - u = v$. We shall show that this condition is not satisfied by all $v \in {}_p\mathrm{Pic}(X')^G \approx {}_p\mathrm{Pic}(X)$, and consequently that γ is not surjective.

Let Ω_X be the sheaf of differentials on X, and K the function field of X. Then the cup product pairings

$$< , >: H^1(X_{Zar}, O_X) \times H^0(X_{Zar}, \Omega_X) \longrightarrow H^1(X_{Zar}, \Omega_X) \approx k$$

[31, II 10] are perfect dualities of finite dimensional vector spaces over k. Moreover the map $\theta\colon {}_p\mathrm{Pic}(X) \longrightarrow H^o(X_{Zar}, \Omega_X)$ which takes the class of the divisor D, pD = (f), f ∈ K, to the logarithmic differential $\frac{df}{f}$, gives an isomorphism of ${}_p\mathrm{Pic}(X)$ onto $H^o(X_{Zar}, \Omega_X)^C$, the subset of $H^o(X_{Zar}, \Omega_X)$ of those elements which are fixed under the Cartier operator C [30, §11]. The pairing $\langle\ ,\ \rangle$ induces a perfect duality

$$H^1(X_{Zar}, O_X)^F \times H^o(X_{Zar}, \Omega_X)^C \longrightarrow \mathbb{F}_p$$

and $H^1(X_{Zar}, O_X)^F = H^1(X, \mathbb{Z}/p\mathbb{Z})$. Similar statements hold for X'.

Now let v ∈ Pic (X), and suppose there exists $u \in {}_p\mathrm{Pic}(X')$ and $\sigma \in G$ such that $\sigma u - u = v$. Choose $u_o, v_o \in \mathrm{Pic}(X')$ such that $pu_o = u$ and $pv_o = v$, and choose divisors D_o and D_o' on X' which are in u_o and v_o respectively. Then $D = pD_o \in u$ and $D' = pD_o' \in v$, and $p(D_o' + D_o - \sigma D_c) = (D' + D - \sigma D) = (e)$, some $e \in K'$, i.e., $\theta'(v_o + u_o - \sigma u_o) = \frac{de}{e}$. Write N for both norm maps $K' \longrightarrow K$ and $\mathrm{Pic}(X') \longrightarrow \mathrm{Pic}(X)$. Then $N(D' + D - \sigma D) = pD' = (Ne)$

so $\theta(v) = \frac{d\,Ne}{Ne}$.

$$<x, \theta(v)> = <x, \frac{dNe}{Ne}> = <\pi^*x, \frac{de}{e}> \qquad [31, III\ 2.3]$$
$$= 0$$

for X' was chosen so that $\pi^*x = 0$. But we know from the previous paragraph that there exists a $v \in {}_p\mathrm{Pic}(X)$ such that $<x, \theta(v)> \neq 0$, and this v cannot therefore belong to the image of γ. This completes the proof of this case of the theorem.

Finally, take $N = \mathbb{Z}/p\mathbb{Z}$ and $r = 1$. It is not difficult to show that the pairing is nondegenerate in this case if and only if it is nondegenerate in the previous case. For example, let $x \in H^1(X, \mu_p)$, let $y \in H^1(X, \mathbb{Z}/p\mathbb{Z})$, let $x' \in \mathrm{Ext}^1_X(\mathbb{Z}/p\mathbb{Z}, \mu_p)$ map to x under $\mathrm{Ext}^1_X(\mathbb{Z}/p\mathbb{Z},\mu_p) \longrightarrow \mathrm{Ext}^1_X(\mathbb{Z},\mu_p)$, let $y' \in \mathrm{Ext}^1_X(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z})$ map to y similarly (and assume y' chosen so that it is split by a flat covering of X), let x" be the image of x in $\mathrm{Ext}^1_X(\mathbb{Z}/p\mathbb{Z},\mu_p)$ under the map given by the spectral sequence, and let y" be the image of y in $\mathrm{Ext}^1_X(\mu_p, \mu_p)$ similarly. Then the image of (x',y") in

$\mathrm{Ext}_X^2(\mathbb{Z}/p\mathbb{Z}, \mu_p)$ under the obvious Yoneda pairing is the Cartier dual of the image of (y', x'') under a second Yoneda pairing. Thus one of these images is zero if and only if the other is, and this may be used to prove what is needed.

Corollary: Let W_n be the sheaf of Witt vectors of length n on X_{Zar}. Then the subgroup of elements of $H^1(X_{Zar}, W_n)$ which are fixed under F^n is canonically dual to ${}_{p^n}\mathrm{Pic}(X)$.

Now take k to be a finite field. It may be shown by class field theory, or by using the computations over $\overline{k}$ and the Hochschild-Serre spectral sequence of $\overline{X}/X$, that $H^3(X, \mathbb{G}_m) \approx \mathbb{Q}/\mathbb{Z}$ [12,2]. Consequently, the spectral sequence

$$H^r(X, \underline{\mathrm{Ext}}^s(N, \mathbb{G}_m)) \Longrightarrow \mathrm{Ext}^{r+s}(N, \mathbb{G}_m)$$

and the Yoneda pairing

$$H^r(X,N) \times \mathrm{Ext}^s(N, \mathbb{G}_m) \longrightarrow H^{r+s}(X, \mathbb{G}_m)$$

may be used to define a cup product pairing

$$H^r(X, N) \times H^{3-r}(X, N^D) \longrightarrow H^3(X, \mathbb{G}_m) \approx \mathbb{Q}/\mathbb{Z}$$

for all finite group schemes N over k.

Theorem A2: The cup product defined above is a perfect duality of finite abelian groups, for all finite group schemes N over k.

Proof: For group schemes N such that $N_{cc} = 0$, the theorem is an immediate consequence of theorem A1 and the Hochschild-Serre spectral sequence for $\bar{X}/X$ (at least, assuming that the two cup products are compatible). The only cases left to be proved are $N = \alpha_p$ and r = 1 and 2. It is not difficult to construct a pairing of the two groups $H^1(X,\alpha_p) = \ker(F: H^1(X_{Zar}, O_X) \longrightarrow H^1(X_{Zar}, O_X))$ and $H^2(X,\alpha_p) = \operatorname{coker}(F: H^1(X_{Zar}, O_X) \dashrightarrow H^1(X_{Zar}, O_X))$ which is analogous to the cup product of [34, Th. 2] and which may be shown, using [1, Ch. 6], to be well-defined and non-degenerate. However, we have not yet proven this pairing to be the cup product, and so the proof of Theorem A2 is incomplete at this point.

References

[1] E. Artin and J. Tate, Class field theory, Harvard, 1961.

[2] M. Artin, Grothendieck topologies, Lecture notes, Harvard, 1962.

[3] M. Artin and A. Grothendieck, Cohomologie étale des schémas, Séminaire de Géométrie Algébrique de l'I.H.E.S. 1963/64.

[4] M. Demazure and A. Grothendieck, Schémas en groupes, Séminaire de Géométrie Algébrique de l'I.H.E.S. 1962/64.

[5] P. Gabriel, Objets injectifs dans les catégories abéliennes, Séminaire Dubreil-Pisot, 1958/59, no. 17.

[6] J. Giraud, Cohomologie non-abélienne, Columbia University, 1966.

[7] M. Greenberg, Schemata over Local Rings II, Ann. of Math., 78 (1963), p. 256-266.

[8] M. Greenberg, Rational points in henselian discrete valuation rings, to appear in Publ. Math.

[9] A. Grothendieck, Séminaire de Géométrie Algébrique de l'I.H.E.S., 1960/61.

[10] A. Grothendieck and J. Dieudonne, Éléments de Géométrie Algébrique II, Publ. Math. 8 (1961).

[11] A. Grothendieck, Fondements de la géométrie algébrique, Paris 1962.

[12] A. Grothendieck, Le groupe de Brauer III: Examples et Complements, mimeographed notes, I.H.E.S., 1966.

[13] N. Jacobson, The theory of rings, Mathematical Surveys II, New York 1943.

[14] S. Lang, *Algebraic groups over finite fields*. Amer. J. of Math., *78* (1956), p. 555-563.

[15] S. Lang, *Abelian varieties*, Interscience Tracts no. 7, New York, 1959.

[16] S. Lang and J-P Serre, *Sur les revêtements non ramifiés des variétés algebriques*. Amer. J. of Math., *79* (1957) p. 319-330.

[17] S. Lang and J. Tate, *Galois cohomology and principal homogeneous spaces*, Amer. J. of Math., *80* (1958), p. 659-684.

[18] Yu. I. Manin, *The theory of commutative formal groups over fields of finite characteristic*, Russian Math. Surveys, *18* (1963) p. 1-83.

[19] B. Mitchell, *Theory of Categories*, Academic Press, New York, 1965.

[20] M. Miyanishi, *On the pro-representability of a functor on the category of finite group schemes*, J. Math. Kyoto, *6* (1966), p. 31-48.

[21] D. Mumford, *Lectures on curves on an algebraic surface*. Math. Studies 59, Princeton, 1966.

[22] A. Néron, *Quasi-fonctions et hauteurs sur les variétés abéliennes*, Ann. of Math. *82* (1965), p. 249-331.

[23] A. Néron, *Degré d'intersection en géométrie diophantienne*, Proc. Int. Cong. Math., Moscow (1966).

[24] T. Oda, Thesis, Harvard, 1967.

[25] A. Ogg, *Cohomology of abelian varieties over function fields*. Ann. of Math. (2) *76* (1962), p. 185-212.

[26] F. Oort, *Commutative group schemes*, Lecture Notes in Math., Springer, Berlin, 1966.

[27] M. Raynaud, *Caractéristique d'Euler-Poincaré d'un faisceau et cohomologie des variétés abéliennes*. Séminaire Bourbaki 1964/65, no. 286, 19 pp.

[28] M. Rosenlicht, *Extensions of vector groups by abelian varieties*, Amer. J. Math., **80** (1958), p. 685-714.

[29] I. Šafarevič, *Principal homogeneous spaces defined over a function field*, Amer. Math. Soc. Transl. (2), **37** (1964), p. 85-114.

[30] J-P Serre, *Sur la topologie des variétés algébriques en caracteristique p*. Symposium Internacional de Topologia Algebrica, Mexico, 1956.

[31] J-P Serre, *Groupes algébriques et corps de classes*, Hermann, Paris, 1959.

[32] J-P Serre, *Groupes p-divisible (d'après J. Tate)*, Séminaire Bourbaki 1966/67, no. 318.

[33] A. Sharma, in Séminaire Heidelberg-Strasbourg 1965/6, *Groupes algébriques lineáres*. Publ. IRMA, Strasbourg, 1967.

[34] S. Shatz, *Cohomology of artinian group schemes over local fields*. Ann. of Math. **79** (1964), p. 411-449.

[35] J. Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analogue*. Séminaire Bourbaki 1965/66, no. 306.

[36] J. Tate, *p-divisible groups*, Conference at Driebergen, 1966.

[37] J. Tate, *Endomorphisms of abelian varieties over finite fields*. Invent. Math. **2** (1966), p. 134-144.

[38] J. Tate, *Endomorphisms of abelian varieties over finite fields* (II), in preparation.

[39] J. Verdier, A duality theorem in the étale cohomology of schemes, Amer. Math. Soc., Lecture Notes of the Woods Hole Summer Institute on Algebraic Geometry, July 1964.

[40] A. Weil, Varietés abéliennes et courbes algébriques, Hermann, Paris, 1948.

[41] A. Weil, The field of definition of a variety. Amer. J. Math. 77 (1955), p. 355-391.