1968a

Inventiones math. 5, 63—84 (1968)

Extensions of Abelian Varieties Defined Over a Finite Field

J. S. MILNE (London)*

Introduction

Let A and B be abelian varieties over a finite field k, and let $T_p A$ and $T_p B$ be their associated pro-p-groups (see §1 for this notation). The main theorem of TATE [12] (as completed in [13] for p = characteristic of k) states that the canonical map

$$\boldsymbol{Z}_p \otimes \mathrm{Hom}_k(A, B) \to \mathrm{Hom}_k(T_p A, T_p B)$$

is an isomorphism for all primes p. This has as consequences that the rank of $\mathrm{Hom}_k(A,B)$ as a free $\boldsymbol{Z}$-module can be computed from the characteristic polynomials $c_A(T)$ and $c_B(T)$ of the Frobenius endomorphisms of A and B [12], Thm. 1a, and that the p-primary component of $\mathrm{Ext}_k^1(A,B)$ is finite for all primes p. In this paper we show (Thm. 3) that the group $\mathrm{Ext}_k^1(A,B)$ is itself finite, and give a formula for its order in terms of the roots of $c_A(T)$ and $c_B(T)$ and the determinant of the bilinear form

$$\mathrm{Hom}_k(A,B) \times \mathrm{Hom}_k(B,A) \to \boldsymbol{Z}$$

which takes two homomorphisms to the trace of their composite. Moreover, we show (Thm. 2) that $\mathrm{Ext}_k^1(A,B)$ is dual to $\mathrm{Ext}_k^1(B,A)$ and that the compact group $\hat{\boldsymbol{Z}} \otimes \mathrm{Hom}_k(A,B)$ ($\hat{\boldsymbol{Z}} = \varprojlim \boldsymbol{Z}/n\boldsymbol{Z}$) is dual to the discrete group $\mathrm{Ext}_k^2(A,B)$. Thus $\mathrm{Ext}_k^2(A,B)$ is a divisible group of corank equal to the rank of $\mathrm{Hom}_k(A,B)$.

In a second paper we will apply these results to the arithmetic of constant abelian varieties over function fields. In particular, we will show that if A is the Jacobian of a smooth, complete, algebraic curve X over k, then $\mathrm{Ext}_k^1(A,B)$ is isomorphic to the Tate-Šafarevič group, Ш(B), of B regarded as an abelian variety over the function field of X, and the resulting formula for the order of Ш(B) is that predicted by the conjectures of BIRCH and SWINNERTON-DYER [10], Conj (B).

Our general method of proof in this paper is to reduce a problem concerning abelian varieties to one concerning p-divisible groups, and then to use the Dieudonné modules of the p-divisible groups or the

* This research was partially supported by the National Science Foundation under contract NSF GP 6432. The paper is based partly on the author's Ph. D. thesis at Harvard University.

groups of points in an algebraically closed field to solve the problem. Section 1 contains preliminary material on p-divisible groups over finite fields and the structure of their Dieudonné modules. In section 2 we prove a duality result for extension groups of p-divisible groups from which we deduce the above dualities for extension groups of abelian varieties. In the final section we compute the order of $\mathrm{Ext}_k^1(A,B)$, the most difficult steps again being computations involving p-divisible groups.

In this paper, all group schemes are commutative. k is a finite field with q elements and of degree a over the prime field. $\bar{k}$ is the algebraic closure of k, and if X is a scheme over k then $\bar{X}=X\otimes_k\bar{k}$. The Galois group of $\bar{k}/k$ is Γ, and σ_k is the canonical topological generator of Γ. If Z is an abelian group,

$$_nZ=\ker(Z\xrightarrow{n}Z), \qquad Z^{(n)}=\mathrm{coker}(Z\xrightarrow{n}Z),$$

$$Z(p)=\varinjlim_{\nu}{}_{p^\nu}Z, \qquad T_pZ=\varprojlim_{\nu}{}_{p^\nu}Z$$

and $[Z]$ is the cardinality of Z. $|\ |_p$ and ord_p are the multiplicative and additive p-adic valuations of $\boldsymbol{Q}$, normed so that $|p|_p=1/p$ and $\mathrm{ord}_p(p)=1$.

I would like to express my gratitude to J. TATE for much encouragement and many useful and stimulating conversations during my work on this paper.

§ 1. Preliminaries on p-Divisible Groups

The Cartier dual of a finite group scheme L over k will be denoted by L^D. If (G_ν, i_ν) is a p-divisible group [8, 11], then $G^t=(G_\nu^D, j_\nu^D)$ is its dual, and $T_pG=(G_\nu, j_\nu)$ is its associated pro-p-group scheme, where j_ν is the unique homomorphism $G_{\nu+1}\to G_\nu$ such that $i_\nu j_\nu=p$. When $p\neq$ characteristic of k, then the G_ν are étale, and hence T_pG can be identified with the Γ-module

$$\varprojlim_{\nu} G_\nu(\bar{k}),$$

which is a free $\boldsymbol{Z}_p$-module of rank equal to the height of G, and in particular is a pro-p-group in the usual sense; however, if $p=$characteristic of k, then T_pG must (in general) be considered as a profinite group scheme over k. Nevertheless we shall throughout the rest of this paper refer to T_pG simply as a pro-p-group (over k) by the analogous abuse of language which has become standard in the case of the term "p-divisible group (over k)". If A is an abelian variety over k, 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. A finite group scheme L (and consequently a p-divisible group) over k can be written uniquely as $L=L_{ee}\oplus L_{ec}\oplus L_{ce}\oplus L_{cc}$ where L_{ec} is the component of L which is étale with connected Cartier dual, etc. [7], I.2.

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

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

(b) If $a_1, \ldots, a_n$ are the roots of $\varphi(T)$ in some algebraic closure of $\boldsymbol{Q}_p$, then

$$\left|\prod_{i=1}^{h} \psi(a_i)\right|_p = |\operatorname{degree} \psi(\alpha)|_p$$

for all polynomials ψ with coefficients in $\boldsymbol{Z}$.

By [3], VII, § 1, lemma 1, the conditions (a) and (b) determine $\varphi(T)$ uniquely. If $p \neq$ characteristic of k, then the characteristic polynomial of the endomorphism of

$$T_p(G)(\bar{k}) = \varprojlim_{v} G_v(\bar{k})$$

induced by α satisfies (a) and (b). The existence of $\varphi(T)$ when $p=$ characteristic of k requires the use of the Dieudonné module of G. 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 $FV=p=VF$, $Fc=c^\sigma F$, $cV=Vc^\sigma$ $(c \in W_k)$ where σ is the unique automorphism of W_k inducing the automorphism $x \mapsto x^p$ on k. There is a contravariant functor $L \mapsto D_k(L)$ from the category of finite p-primary group schemes over k to the category of left A_k-modules of finite length over W_k, which is an anti-equivalence of categories [4]; [9], Thm. 8.4; [6], Cor. 3.16. Moreover, if L is of rank p^v over k, then $D_k(L)$ is of length v as a W_k-module. From this, it follows that there is an anti-equivalence $G \mapsto D_k(G)$ from the category of p-divisible groups over k to the category of left A_k-modules which are free of finite rank over W_k, and the height of G equals the rank of $D_k(G)$ over W_k. The endomorphism $D_k(\alpha)$ of $D_k(G)$ induced by α commutes with the action of F on $D_k(G)$, and it follows that its characteristic polynomial $\varphi(T)$ has coefficients in $\boldsymbol{Z}_p$. Also, if $\psi \in \boldsymbol{Z}[T]$, then

$$\begin{aligned} |\deg \psi(\alpha)|_p &= |\operatorname{rank}(\ker \psi(\alpha))|_p \\ &= p^{-v}, \qquad \text{where } v = \operatorname{length}_{W_k}(\operatorname{coker} D_k(\psi(\alpha))) \\ &= \left|\prod \psi(a_i)\right|_p \end{aligned}$$

where $a_1, \ldots, a_h$ are the roots of $\varphi(T)$. Thus $\varphi(T)$ is the characteristic polynomial of α on G.

Now write

$$W'_k = \mathbf{Q}_p \otimes_{\mathbf{Z}_p} W_k,$$

$$A'_k = W'_k \otimes_{W_k} A_k,$$

and

$$D'_k(G) = A'_k \otimes_{A_k} D_k(G).$$

Note that

$$A'_k \approx W'_k[F, F^{-1}]$$

with the single relation $Fc = c^\sigma F$. Clearly two p-divisible groups G and H are isogenous over k if and only if $D'_k(G) \approx D'_k(H)$. Also, an A'_k-module M' which is finite dimensional over W'_k equals $D'_k(G)$ for some p-divisible group G if and only if it contains a W_k-submodule M, stable under F and pF^{-1} such that

$$M' = W'_k \otimes_{W_k} M.$$

If F_k is the Frobenius endomorphism of G relative to k, then $D_k(F_k)$ acts on $D_k(G)$ as F^a if p = characteristic of k, and F_k acts on $T_p G(\bar{k})$ as σ_k if $p \neq$ characteristic of k. We write $c_G(T)$ for the characteristic polynomial of F_k on G. We will also need the notion of the minimal polynomial $m_G(T)$ of F_k on G. This we define to be the monic polynomial of least degree with coefficients in $\mathbf{Z}_p$ such that $m_G(F_k)$ is zero on G. If p = characteristic of k, and

$$D'_k(G) \approx A'_k / A'_k \lambda$$

then $A'_k\, m_G(F^a)$ is the bound of $A'_k \lambda$ in the sense of [2], III, 6.

If G is the p-divisible group associated to an abelian variety A, and α is an endomorphism of A, then it is clear from their definitions that the characteristic polynomial of α on A is equal to the characteristic polynomial of the endomorphism of G defined by α. In particular, this shows that $c_G(T)$ has coefficients in $\mathbf{Z}$. Also, in this case, $m_G(T)$ cannot have multiple roots, for 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 $\mathbf{Q}$-irreducible polynomial φ_i with $\varphi_i(F_k)$ zero on A_i [12], Thm. 2e, and $m_G(T)$ divides the least common multiple of the φ_i.

We will say that a p-divisible group is indecomposable if it is not isogenous to a direct sum of two non-zero p-divisible groups.

Theorem 1. *Let k be a field with p^a elements and let G be a p-divisible group over k.*

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

(b) *Suppose G is indecomposable. Then $m_G(T)$ is a power of a $\mathbf{Z}_p$-irreducible polynomial, $D'_k(G)$ is of the form $A'_k/A'_k\,\lambda$, and there exists an integer e such that*

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

(c) *Suppose $D'_k(G) = A'_k/A'_k\,\lambda$ where*

$$\lambda(F) = F^h + b_{h-1}F^{h-1} + \cdots + b_0.$$

Then $\operatorname{ord}_p(b_0) = n$ *for some n with $m = h - n \geqq 0$,*

$$\mu(F,V) = F^m + b_{h-1}F^{m-1} + \cdots + b_n + \cdots + \frac{b_0}{p^n}V^n$$

has coefficients in W_k, and $A/A\,\mu(F,V)$ is the module of a p-divisible group isogenous to G.

(d) *If G is indecomposable and*

$$D'_k(G) \approx A'_k/A'_k\,\lambda$$

where

$$\lambda = F^m + \cdots + b_0 + \cdots + b_{-n}F^{-n}, \qquad \operatorname{ord}_p(b_{-n}) = n,$$

then $\operatorname{ord}_p(b_0) = 0$ *if and only if G or its dual is étale.*

(e) *If $a_1, a_2, \ldots$ are the roots of $c_G(T)$ (resp. $m_G(T)$) then q/a_1, $q/a_2, \ldots$ are the roots of $c_{G^t}(T)$ (resp. $m_{G^t}(T)$).*

Proof. (a) Apply the Krull-Schmidt Theorem to $D'_k(G)$.

(b) Follows from [2], III, Thms. 13, 19, 20.

(c) Define the Newton polygon of a polynomial

$$\lambda = c_m F^m + \cdots + c_0 + \cdots + c_{-n}F^{-n} \in W'_k[F, F^{-1}] = A'_k$$

to be the lower convex envelope of the set of points $(c_i, \operatorname{ord}_p(c_i))$ in $\mathbf{R} \times \mathbf{R}$. For any $s \in \mathbf{Q}$, define $l_s(\lambda)$ to be the length (in the direction of the x-axis) of the side of the Newton polygon of λ which has the slope s, and define

$$\operatorname{ord}_s(\lambda) = \min_i\left(\operatorname{ord}_p(c_i) - s\,i\right).$$

Then, for $\lambda, \mu \in A'_k$,

$$l_s(\lambda\mu) = l_s(\lambda) + l_s(\mu)$$

$$\operatorname{ord}_s(\lambda\mu) = \operatorname{ord}_s(\lambda) + \operatorname{ord}_s(\mu).$$

The image of A under the canonical inclusion $A_k \to A'_k$ consists of those polynomials $\lambda(F, F^{-1})$ such that $\operatorname{ord}_0(\lambda) \geqq 0$, $\operatorname{ord}_{-1}(\lambda) \geqq 0$.

Suppose that $M' = A'_k / A'_k \lambda$, $\lambda = F^h + \cdots + b_0$, $\operatorname{ord}_p(b_0) = n$, contains a W_k-submodule M, stable under F and pF^{-1}, and such that $M' = W'_k \otimes_{W_k} M$. $1, F, F^2, \ldots, F^{h-1}$ is a basis for M' over W'_k so, after multiplying M by a power of p, we may assume

$$p^{-c}(W_k 1 + \cdots + W_k F^{h-1}) \supset M \supset (W_k 1 + \cdots + W_k F^{h-1})$$

some $c \in \mathbf{Z}$. Since M is stable under F, there exist polynomials $\lambda_j(F)$ with $\deg(\lambda_j) < h$, $\operatorname{ord}_0(\lambda_j) \geqq -c$, and $\mu \in A'_k$ such that

$$F^j = \mu \lambda + \lambda_j$$

i.e.

$$F^j - \lambda_j = \mu \lambda .$$

If some coefficient of λ is not an integer, then there exists an $s > 0$ such that $l_s(\lambda) \neq 0$. Then $l_s(\lambda \mu) > 0$. But

$$l_s(F^j - \lambda_j) = 0 \quad \text{for} \quad s > \frac{c}{j-(h-1)} .$$

Thus $\operatorname{ord}_0(\lambda) = 0$.

A similar argument using the stability of M under pF^{-1} shows that $\operatorname{ord}_{-1}(F^{-n}\lambda) = 0$.

(d) If $\operatorname{ord}_p(b_0) = 0$, then there exist units

$$u_1, \ldots, u_m, v_1, \ldots, v_n$$

in $W_{\bar{k}}$ such that

$$\lambda(F) = (F - u_1) \ldots (F - u_m)(1 - p v_1 F^{-1}) \ldots (1 - p v_n F^{-1})$$

(cf. [1], IV, 6, Lemma 10) and so, G splits over $\bar{k}$ into a product of p-divisible groups which are étale or have étale duals.

(e) This follows from the statement [6], Prop. 3.22:

$$D_k(G^t) \approx \operatorname{Hom}_{W_k}(D_k(G), W_k)$$

as W_k-modules, and the endomorphisms induced by the operation of F^a and V^a on $D_k(G^t)$ are adjoint to those induced by V^a and F^a respectively on $D_k(G)$.

§ 2. Duality

We write

$$\operatorname{Ext}^r_k(Z_1, Z_2) \,(\text{resp., } \operatorname{Ext}^r_{k,\nu}(Z_1, Z_2), \operatorname{Ext}^r_{A_k}(Z_1, Z_2), \operatorname{Ext}^r_{A_k,\nu}(Z_1, Z_2))$$

for the group of equivalence classes of r-fold extensions of Z_1 by Z_2 in the category of algebraic group schemes over k (resp. of finite group schemes over k killed by p^ν, of A_k-modules, of A_k-modules killed by p^ν). Also, if Z_1 or Z_2 is an ind-algebraic group scheme (resp. pro-algebraic group scheme) then $\mathrm{Ext}_k^r(Z_1, Z_2)$ denotes the group formed in the category of ind-algebraic (resp. pro-algebraic) group schemes over k. Finally, if G and H are p-divisible groups over k, we write

$$\mathrm{Ext}_k^r(T_p G, H) = \varinjlim_{\nu} \mathrm{Ext}_{k,\nu}^r(G_\nu, H_\nu).$$

Before constructing the pairing for Theorem 2, we will need two lemmas. If Z is a Γ-module, then Z^Γ and Z_Γ denote the kernel and cokernel respectively of $\sigma_k - 1\colon Z \to Z$.

Lemma 1. *If K and L are finite group schemes over k, then there is an exact sequence*

$$0 \longrightarrow \mathrm{Hom}_{\bar{k}}(\bar{K}, \bar{L})_\Gamma \xrightarrow{f_1} \mathrm{Ext}_k^1(K, L) \xrightarrow{f_2} \mathrm{Ext}_{\bar{k}}^1(\bar{K}, \bar{L})^\Gamma \longrightarrow 0$$

where f_2 is the map defined by base extension $k \to \bar{k}$, and f_1 is defined as follows: let $\alpha\colon \bar{K} \to \bar{L}$; then $f_1(\alpha)$ is the class of the extension of K by L over k which, after base extension $k \to \bar{k}$, becomes

$$0 \longrightarrow \bar{L} \longrightarrow \bar{L} \oplus \bar{K} \longrightarrow \bar{K} \longrightarrow 0$$

with σ_k acting on the centre term as the matrix

$$\begin{pmatrix} \sigma_k & \alpha\sigma_k \\ 0 & \sigma_k \end{pmatrix}.$$

Proof. It is easy to see, using descent, that f_2 is surjective, and that f_1 is well-defined and injective. Suppose

$$0 \longrightarrow L \xrightarrow{\beta} E \xrightarrow{\gamma} K \longrightarrow 0$$

is an extension of K by L which has a section $\rho\colon \bar{K} \to \bar{E}$ over $\bar{k}$. Then $\gamma(\rho^{\sigma_k} - \rho) = 0$, so there is a unique $\alpha\colon \bar{K} \to \bar{L}$ such that $\beta\alpha = \rho^{\sigma_k} - \rho$, and $f_1(\alpha)$ is the class of the original extension.

Lemma 2. *If G is a p-divisible group over k, and L is a finite group scheme over k with $L_{cc} = L$, then*

$$\mathrm{Ext}_k^r(L, G) = 0 = \mathrm{Ext}_k^r(T_p G, L) \qquad \textit{for } r \geqq 2.$$

Proof. The arguments of [7], II, suffice to show that

$$\mathrm{Ext}_k^r(\mathbf{G}_a, \mathbf{G}_a) = 0, \qquad r \geqq 2,$$

for any perfect field k. Thus $\mathrm{Ext}_k^r(\boldsymbol{\alpha}_p, \boldsymbol{\alpha}_p) = 0$ for $r \geqq 3$, and it follows that

$$\mathrm{Ext}_k^r(L, G) = 0 = \mathrm{Ext}_k^r(T_p G, L) \qquad \text{for } r \geqq 3.$$

Let $\mathrm{Ext}_{k-a}^r(K, L)$ be the group of extensions of K by L in the category of affine algebraic group schemes over k. The canonical map

$$\mathrm{Ext}_{k-a}^r(K, L) \longrightarrow \mathrm{Ext}_k^r(K, L)$$

is bijective for $r=1$, injective for $r=2$ (cf. [5], VII, Lemma 4.1) and bijective for $r=2$ and $K=L=\boldsymbol{G}_a$. Hence it is bijective for $r=2$ and finite group schemes K and L, and so, from the category anti-equivalence [6], § 3, we get an injection

$$\operatorname{Ext}_k^2(K, L) \to \operatorname{Ext}_{A_k}^2(D_k(L), D_k(K)).$$

Since $\operatorname{Ext}_k^3(L,K)=0$ all finite K, in proving $\operatorname{Ext}_k^2(L,G)=0$ we may replace G by an isogenous p-divisible group. Thus we may assume (Thm 1a, b) the existence of an exact sequence

$$0 \to A_k \to A_k \to D_k(G) \to 0.$$

But this implies that

$$\operatorname{Ext}_{A_k}^2(D_k(G), D_k(L))=0$$

and consequently that

$$\operatorname{Ext}_k^2(L, G)=0.$$

A similar argument shows that

$$\operatorname{Ext}_k^2(T_p G, L)=0.$$

We now construct pairings

$$\operatorname{Ext}_k^r(T_p G, L) \times \operatorname{Ext}_k^{1-r}(L, G) \to \boldsymbol{Q}_p/\boldsymbol{Z}_p$$

for $r=0, 1$, where G is a p-divisible group over k and L is a finite group scheme over k.

$$\operatorname{Ext}_k^r(T_p G, L) = \varinjlim_{\nu} \operatorname{Ext}_{k,\nu}^r(G_\nu, L), \qquad r=0,1,$$

and

$$\operatorname{Ext}_k^r(L, G) = \varinjlim_{\nu} \operatorname{Ext}_{k,\nu}^1(L, G_\nu), \qquad r=0,1$$

(e.g. if $p^\nu L=0$ and

$$0 \to G \to E \to L \to 0$$

is exact, then so also is

$$0 \to G_\nu \to E_\nu \to L \to 0,$$

where $E_\nu = \ker(p^\nu\colon E \to E)$), so there are Yoneda pairings

$$\operatorname{Ext}_k^r(T_p G, L) \times \operatorname{Ext}_k^{1-r}(L, G) \to \operatorname{Ext}_k^1(T_p G, G)$$

and it suffices to construct a homomorphism

$$\eta\colon \operatorname{Ext}_k^1(T_p G, G) \to \boldsymbol{Q}_p/\boldsymbol{Z}_p.$$

Assume first that G is étale. By Lemma 1,

$$f_1\colon \operatorname{Hom}_{\bar{k}}(T_p \bar{G}, \bar{G})_\Gamma \xrightarrow{\approx} \operatorname{Ext}_k^1(T_p G, G).$$

If

$$\alpha=(\alpha_\nu)\in \operatorname{Hom}_{\bar{k}}(T_p\bar{G},\bar{G}),$$

then we write

$$T_\nu(\alpha_\nu)\in \boldsymbol{Z}/p^\nu \boldsymbol{Z}$$

for the trace of

$$\alpha_\nu(\bar{k})\colon\ G_\nu(\bar{k})\to G_\nu(\bar{k}),$$

and

$$T(\alpha)=\big(T_\nu(\alpha_\nu)\big)\in \varinjlim \boldsymbol{Z}/p^\nu \boldsymbol{Z}=\boldsymbol{Q}_p/\boldsymbol{Z}_p.$$

Since

$$T(\alpha^{\sigma_k})=T(\alpha),$$

T defines a map

$$\operatorname{Hom}_{\bar{k}}(T_p\bar{G},\bar{G})_\Gamma\to \boldsymbol{Q}_p/\boldsymbol{Z}_p$$

and we define η to be the composite of this map with f_1^{-1}.

If G^t is étale, then

$$\operatorname{Ext}^1_k(T_pG,G)\approx \operatorname{Ext}^1_k(T_pG^t,G^t),$$

so this case reduces to the above.

In constructing η when $G=G_{cc}$ we will use the Dieudonné module of G. Assume that p=characteristic of k, and let M_ν and N_ν be two A_k-modules which are free of finite rank over $W_k/p^\nu W_k$. Any extension E of N_ν by M_ν defining an element of $\operatorname{Ext}^1_{A_k,\nu}(N_\nu, M_\nu)$ can be written, as a sequence of W_k-modules, as

$$0\to M_\nu\to M_\nu\oplus N_\nu\to N_\nu\to 0.$$

E is then described completely by giving a pair (β,α) of W_k-semilinear maps $N_\nu\to M_\nu$ such that F and V act on $M_\nu\oplus N_\nu$ as the matrices

$$\begin{pmatrix}F&\beta\\0&F\end{pmatrix}\quad\text{and}\quad\begin{pmatrix}V&\gamma\\0&V\end{pmatrix}.$$

In this situation, we write $E\leftrightarrow(\beta,\gamma)$. The following hold.

(P_1) $(\beta,\gamma)\leftrightarrow$some such E if and only if

$$\beta V+F\gamma=0=\gamma F+V\beta.$$

(P_2) If $E\leftrightarrow(\beta,\gamma)$ and $E'\leftrightarrow(\beta',\gamma')$, then E is equivalent to E' if and only if there exists $\delta\colon N_\nu\to M_\nu$ (W_k-linear) such that

$$\beta-\beta'=F\delta-\delta F$$
$$\gamma-\gamma'=V\delta-\delta V.$$

(P_3) If $E\leftrightarrow(\beta,\gamma)$, and $\rho\colon M_\nu\to M'_\nu$ is A_k-linear, then $\rho_* E\leftrightarrow(\rho\,\beta,\rho\,\gamma)$. If $\rho\colon N'_\nu\to N_\nu$ is A_k-linear, then $\rho^* E\leftrightarrow(\beta\,\rho,\gamma\,\rho)$.

(P_4) If $E \leftrightarrow (\beta, \gamma)$ and $E' \leftrightarrow (\beta', \gamma')$, then

$$E \pm E' \leftrightarrow (\beta \pm \beta', \gamma \pm \gamma').$$

(P_5) Let M and N be A_k-modules which are free of finite rank over W_k, let $M_\nu = M/p^\nu M$, $M_{\nu+1} = M/p^{\nu+1} M$, $N_\nu = N/p^\nu N$, $N_{\nu+1} = N/p^{\nu+1} N$ and let $i: M_{\nu+1} \to M_\nu$ be the map induced by $1: M \to M$, and $j: N_\nu \to N_{\nu+1}$ the map induced by $p: N \to N$. Then

$$\begin{array}{ccc} \mathrm{Hom}_{W_k,\sigma}(M_\nu, N_\nu) \times \mathrm{Hom}_{W_k,\sigma^{-1}}(M_\nu, N_\nu) & \longrightarrow & \mathrm{Ext}^1_{A_k,\nu}(M_\nu, N_\nu) \\ \downarrow & & \downarrow \\ \mathrm{Hom}_{W_k,\sigma}(M_{\nu+1}, N_{\nu+1}) \times \mathrm{Hom}_{W_k,\sigma^{-1}}(M_{\nu+1}, N_{\nu+1}) & \longrightarrow & \mathrm{Ext}_{A_k,\nu+1}(M_{\nu+1}, N_{\nu+1}) \end{array}$$

commutes, where the vertical map is induced by i and j, and the horizontal maps take (β, γ) to the class of $E \leftrightarrow (\beta, \gamma)$.

(P_6) Let M and N be as in (P_5) and assume that F and V are nilpotent on N_ν. If E is an extension of M_ν by N_ν then there exists an $\alpha: N_\nu \to M_\nu$ (W_k-linear) such that $E \leftrightarrow (-\alpha F, V\alpha)$.

Proof. For the first two steps of the proof we will not assume that N_ν is of the form $N/p^\nu N$.

First take $\nu = 1$ and $N_1 = k$ with F and V acting as zero. Let $E \leftrightarrow (\beta, \gamma)$. By ($P_1$), $\beta(1)$ and $\gamma(1)$ are elements of M_1 such that $F\gamma(1) = 0 = V\beta(1)$. Choose b and c in M mapping to $\beta(1)$ and $\gamma(1)$ under $M \to M_1$. Then there exist b' and c' in M such that

$$Fc = pc' = FVc', \qquad Vb = pb' = VFb'.$$

But F and V are injective on M, hence $c = Vc'$ and $b = Fb'$. Choose maps $\alpha, \delta: k \to M_1$ such that $\alpha(1) = c' - b' \pmod p$ and $\delta(1) = b' \pmod p$, then $\beta = F\delta$ and $\gamma = V\alpha + V\delta$.

Again take $\nu = 1$, but assume (P_6) true for modules of W_k-length less than that of N_1. Then $N_1 = N_1' \oplus k$, where F and V act as matrices

$$\begin{pmatrix} F & \varphi \\ 0 & 0 \end{pmatrix}, \qquad \begin{pmatrix} V & \psi \\ 0 & 0 \end{pmatrix}$$

some $\varphi, \psi: k \to N$ with $F\psi = 0 = V\varphi$. Let $E \leftrightarrow (\beta, \gamma)$ be an extension of N_1 by M_1 where $\beta = (\beta_1, \beta_2)$, $\gamma = (\gamma_1, \gamma_2)$: $N_1' \oplus k \to M_1$. By (P_1),

$$\beta_1 V + F\gamma_1 = 0, \qquad \gamma_1 F + V\beta_1 = 0$$
$$\beta_1 \psi + F\gamma_2 = 0, \qquad \gamma_1 \varphi + V\beta_2 = 0$$

and we seek (δ_1, δ_2) and (α_1, α_2): $N_1' \oplus k \to M_1$ such that

$$(\beta_1, \beta_2) = -(\alpha_1 F, \alpha_1 \varphi) + (F\delta_1 - \delta_1 F, F\delta_2 - \delta_1 \varphi)$$
$$(\gamma_1, \gamma_2) = (V\alpha_1, V\alpha_2) + (V\delta_1 - \delta_1 V, V\delta_2 - \delta_1 \psi).$$

By the induction assumption, we can choose α_1, δ_1 to satisfy the first components of these equations. Thus we may assume $\beta_1 = -\alpha_1 F$, $\gamma_1 = V\alpha_1$, $\delta_1 = 0$. We are left with

$$(\alpha_1 \varphi + \beta_2) \quad \text{and} \quad \gamma_2 : k \longrightarrow M_1$$

satisfying

$$F\gamma_2 = 0, \quad V(\alpha_1 \varphi + \beta_2) = 0$$

and seek $\delta_2 : k \to M_1$ such that

$$\alpha_1 \varphi + \beta_2 = F\delta_2$$

$$\gamma_2 = V\alpha_2 + V\delta_2 .$$

But this is the problem solved in the first part of the proof.

We now prove the general case by induction on ν. Let $E \leftrightarrow (\beta, \gamma)$ be an extension of N_ν of M_ν. From the induction assumption applied to $M_\nu/p^{\nu-1} M_\nu$ and $N_\nu/p^{\nu-1} N_\nu$ we get that there exist α' and δ' such that

$$p(\beta + \alpha' F + F\delta' - \delta' F) = 0$$

and

$$p(\gamma - V\alpha' + V\delta' - \delta' V) = 0$$

so we may assume to begin with that $p\beta = 0 = p\gamma$. Then $\beta = j\beta'' i$ and $\gamma = j\gamma'' i$ some β'', γ'' where

$$i: M_\nu \longrightarrow M/pM \quad \text{and} \quad j: N/pN \longrightarrow N_\nu$$

are induced by 1 and $p^{\nu-1}$ respectively. There exist δ'' and α'' such that

$$\beta'' + \alpha'' F + F\delta'' - \delta'' F = 0$$

$$\gamma'' - V\alpha'' + V\delta'' - \delta'' V = 0$$

and it follows that

$$\beta'' + j\alpha'' iF + Fj\delta'' i - j\delta'' iF = 0$$

$$\gamma'' - Vj\alpha'' i + Vj\delta'' i - j\delta'' iV = 0 .$$

This completes the proof of (P_6).

Let G be a p-divisible group over k such that $G = G_{cc}$. (P_{1-6}) imply the existence of a homomorphism

$$h: \varinjlim_{\nu} \operatorname{Hom}_{Wk}(D_k(G_\nu), D_k(G_\nu)) \longrightarrow \operatorname{Ext}^1_k(T_p G, G)$$

which is surjective, functorial, and such that $\alpha = (\alpha_\nu)$ is in the kernel if and only if $-\alpha_\nu F = F\delta_\nu - \delta_\nu F$, $V\alpha_\nu = V\delta_\nu - \delta_\nu V$ some δ_ν, all ν. Consider $S_\nu T_\nu(\alpha_\nu)$ where $T_\nu(\alpha_\nu)$ is the trace of α_ν as a map of free $W_k/p^\nu W_k$-modules, and S_ν is the map

$$W_k/p^\nu W_k \to \mathbf{Z}/p^\nu \mathbf{Z}$$

induced by the trace of $k/\mathbf{F}_p$. The conditions on α_ν when $h(\alpha)=0$ imply that

$$T_\nu(\alpha_\nu) = T_\nu(\delta_\nu) - T_\nu(\delta_\nu)^\sigma,$$

and so

$$S_\nu T_\nu(\alpha_\nu) = S_\nu\big(T_\nu(\delta_\nu) - T_\nu(\delta_\nu)^\sigma\big) = 0.$$

Thus

$$\varinjlim S_\nu T_\nu\colon \varinjlim \mathrm{Hom}_{W_k}(D_k(G_\nu), D_k(G_\nu)) \to \mathbf{Q}_p/\mathbf{Z}_p$$

and h induce a well-defined map

$$\eta\colon \mathrm{Ext}_k^1(T_p G, G) \to \mathbf{Q}_p/\mathbf{Z}_p.$$

Consequently, we have defined, for all p-divisible groups G over k and all finite group schemes L, pairings

$$\mathrm{Ext}_k^r(T_p G, L) \times \mathrm{Ext}_k^{1-r}(L, G) \to \mathbf{Q}_p/\mathbf{Z}_p$$

for $r=0, 1$. Moreover, if

$$0 \to L' \to L \to L'' \to 0$$

is an exact sequence of finite group schemes, then the pairings are compatible, in an obvious sense, with the corresponding long exact sequences of $\mathrm{Ext}_k(T_p G, -)$ and $\mathrm{Ext}_k(-, G)$.

Lemma 3. *The pairings*

$$\mathrm{Ext}_k^r(T_p G, L) \times \mathrm{Ext}_k^{1-r}(L, G) \to \mathbf{Q}_p/\mathbf{Z}_p$$

defined above are non-degenerate for $r=0$ *and* 1.

Proof. Observe that all paired groups are finite. For example, if $p^\nu L=0$, there is an exact sequence

$$0 \to \mathrm{Hom}_k(L, G) \to \mathrm{Ext}_k^1(L, G_\nu) \to \mathrm{Ext}_k^1(L, G) \to 0$$

and $\mathrm{Ext}_k^1(L, G_\nu)$ is finite by Lemma 1 and [7], II, 14-2.

If we assume L is étale then we may take G to be étale also. The pairing

$$\mathrm{Hom}_{\bar{k}}(T_p \bar{G}, \bar{L}) \times \mathrm{Hom}_{\bar{k}}(\bar{L}, \bar{G}) \to \mathrm{Hom}(T_p \bar{G}, \bar{G}) \xrightarrow{T} \mathbf{Q}_p/\mathbf{Z}_p$$

is non-degenerate, and induces non-degenerate pairings

$$\mathrm{Hom}_{\bar{k}}(T_p \bar{G}, \bar{L})^\Gamma \times \mathrm{Hom}_{\bar{k}}(\bar{L}, \bar{G})_\Gamma \to \mathbf{Q}_p/\mathbf{Z}_p$$

$$\mathrm{Hom}_{\bar{k}}(T_p \bar{G}, \bar{L})_\Gamma \times_{\bar{k}} (\bar{L}, \mathrm{Hom}\, \bar{G})^\Gamma \to \mathbf{Q}_p/\mathbf{Z}_p$$

which, because

$$\mathrm{Hom}_{\bar{k}}(T_p \bar{G}, \bar{L})^\Gamma \approx \mathrm{Hom}_k(T_p G, L)$$

and

$$\mathrm{Hom}_{\bar{k}}(T_p \bar{G}, \bar{L})_\Gamma \approx \mathrm{Ext}_k^1(T_p G, L), \quad \text{etc.},$$

may be identified with the pairings of the lemma.

If the dual of L is étale, then the non-degeneracy follows from the above case.

Now assume $L = L_{cc}$ and $G = G_{cc}$. If $L = \alpha_p$ [7], I, 2-11, and $D_k(G) \approx A_k / A_k \lambda$ some $\lambda \in A_k$ (cf. Thm. 1), then each of the pairings of the lemma may be identified with the pairings

$$k \times k \longrightarrow \boldsymbol{F}_p$$

which takes two elements of k to the trace of their product, and this is non-degenerate.

Note that for a p-divisible group G of the above type,

$$[\mathrm{Ext}_k^1(\alpha_p, G)] = [\mathrm{Hom}_k(\alpha_p, G)].$$

Thus, in proving this equality for an arbitrary p-divisible group H, we may assume there exists an exact sequence

$$0 \longrightarrow \alpha_p \longrightarrow G \longrightarrow H \longrightarrow 0$$

and that the equality holds for G (for any isogeny with kernel $L = L_{cc}$ is a composite of isogenies with kernels α_p). But now the equality follows for H by writing the $\mathrm{Ext}_k^r(\alpha_p, -)$ sequence of the above short exact sequence, using Lemma 2, and observing (cf. [7], II, 14-2) that $\mathrm{Ext}_k^r(\alpha_p, \alpha_p)$ is a vector space over k of dimension 1, 2 or 1 according as $r = 0$, 1, or 2.

It is clear from the description of $\mathrm{Ext}_k^1(\alpha_p, H)$ given by (the proof of) (P_6), that the left kernel of

$$\mathrm{Hom}_k(T_p H, \alpha_p) \times \mathrm{Ext}_k^1(\alpha_p, H) \longrightarrow \boldsymbol{Q}_p / \boldsymbol{Z}_p$$

is zero. Hence

$$[\mathrm{Hom}_k(T_p H, \alpha_p)] \leqq [\mathrm{Ext}_k^1(\alpha_p, H)] = [\mathrm{Hom}_k(\alpha_p, H)] = [\mathrm{Hom}_k(T_p H^t, \alpha_p)]$$

all H, so equality holds, and the right kernel is also zero. A similar argument proves the lemma for $r = 1$ in the case $L = \alpha_p$.

The lemma follows for an arbitrary L by using induction on the length of L and the compatibility of the pairing with the $\mathrm{Ext}_k^r(-, G)$ and $\mathrm{Ext}_k^r(T_p G, -)$ sequences.

Theorem 2. *For all abelian varieties A and B over k,* $\mathrm{Ext}_k^1(A, B)$ *is dual to* $\mathrm{Ext}_k^1(B, A)$*, and the compact group* $\hat{\boldsymbol{Z}} \otimes \mathrm{Hom}_k(A, B)$ *is dual to the discrete group* $\mathrm{Ext}_k^2(B, A)$.

Remark. By [7], II, 12.1, $\mathrm{Ext}_k^r(A, B)$ is torsion for $r > 0$, and we prove below that $\mathrm{Ext}_k^1(A, B)\,(p)$ is finite for all p. In § 3 we prove that $\mathrm{Ext}_k^1(A, B)$ is itself finite.

Proof. From the $\mathrm{Ext}_k^r(A,-)$ sequence of

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

we get an exact sequence

$$0 \longrightarrow \mathrm{Hom}_k(A,B)^{(p^\nu)} \longrightarrow \mathrm{Ext}_k^1(A,B_\nu) \longrightarrow {}_{p^\nu}\mathrm{Ext}_k^1(A,B) \longrightarrow 0.$$

But

$$\mathrm{Ext}_k^1(A,B_\nu) \approx \mathrm{Hom}_k(T_p A, B_\nu)$$

is finite, so

$${}_{p^\nu}\mathrm{Ext}_k^1(A,B)$$

is finite, and

$$\mathrm{Ext}_k^1(A,B)(p)$$

is finite if and only if its p-divisible subgroup is zero. On passing to the projective limit with the sequences

$$0 \longrightarrow \mathrm{Hom}_k(A,B)^{(p^\nu)} \longrightarrow \mathrm{Hom}_k(T_p A, B_\nu) \longrightarrow {}_{p^\nu}\mathrm{Ext}_k^1(A,B) \longrightarrow 0$$

we get

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

By [12] and [13], the first map of this sequence is surjective, and so

$$T_p(\mathrm{Ext}_k^1(A,B)) = 0,$$

and the p-divisible subgroup of $\mathrm{Ext}_k^1(A,B)$ is zero.

There is an isomorphism

$$\boldsymbol{Z}_p \otimes \mathrm{Hom}_k(A,B) \approx \mathrm{Hom}_k(T_p A, T_p B).$$

From the $\mathrm{Ext}_k(-,B)$ sequence of

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

we get, using that

$$\mathrm{Hom}_k(A_\nu, B) = \mathrm{Hom}_k(A_\nu, B_\nu),$$

an exact sequence

$$0 \longrightarrow \mathrm{Hom}_k(A,B)^{(p^\nu)} \longrightarrow \mathrm{Hom}_k(A_\nu, B_\nu) \longrightarrow {}_{p^\nu}\mathrm{Ext}_k^1(A,B) \longrightarrow 0$$

and, in the limit, an exact sequence

$$0 \longrightarrow \mathrm{Hom}_k(A,B) \otimes (\boldsymbol{Q}_p/\boldsymbol{Z}_p) \xrightarrow{h} \mathrm{Hom}_k(T_p A, B(p)) \longrightarrow \mathrm{Ext}_k^1(A,B)(p) \longrightarrow 0.$$

Thus $\mathrm{Ext}_k^1(A,B)(p)$ is isomorphic to the quotient of $\mathrm{Hom}_k(T_p A, B(p))$ by its p-divisible subgroup. Similar arguments show that $\mathrm{Ext}_k^1(B,A)(p)$ is isomorphic to the torsion subgroup of

$$\mathrm{Ext}_k^1(T_p B, T_p A)$$

and

$$\mathrm{Ext}_k^2(B, A)(p) \approx \mathrm{Ext}_k^1(T_p B, A(p)).$$

Lemma 3 implies the existence of non-degenerate pairings

$$\mathrm{Hom}_k(T_p A, T_p B) \times \mathrm{Ext}_k^1(T_p B, A(p)) \longrightarrow \boldsymbol{Q}_p/\boldsymbol{Z}_p$$

$$\mathrm{Ext}_k^1(T_p A, T_p B) \times \mathrm{Hom}_k(T_p B, A(p)) \longrightarrow \boldsymbol{Q}_p/\boldsymbol{Z}_p$$

which, together with the above isomorphisms, imply the theorem.

§ 3. The Order of $\mathrm{Ext}_k^1(A, B)$

We now prove the main result of the paper.

Theorem 3. *If A and B are abelian varieties over a finite field k, then*

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

where $d(A)$ and $d(B)$ are the dimensions of A and B,

$$(a_i)_{1 \leqq i \leqq 2\,d(A)}$$

and

$$(b_i)_{1 \leqq i \leqq 2\,d(B)}$$

are the roots of the characteristic polynomials of the Frobenius endomorphisms of A and B relative to k,

$$(\alpha_i)_{1 \leqq i \leqq r}$$

and

$$(\beta_i)_{1 \leqq i \leqq r}$$

are bases for $\mathrm{Hom}_k(A, B)$ *and* $\mathrm{Hom}_k(B, A)$, *and $\langle \alpha_i, \beta_j \rangle$ is the trace of the endomorphism $\beta_j \alpha_i$ of A.*

Proof. We refer the reader to [10], 306-19, for the definition of a quasi-isomorphism h of $\boldsymbol{Z}_p$-modules, $z(h)$, and for the elementary Lemmas z.1, z.2, z.3, and z.4.

Consider the diagram

$$(*) \qquad \begin{array}{ccl} \boldsymbol{Z}_p \otimes \mathrm{Hom}_k(A, B) & \xrightarrow{\;t\;} & \mathrm{Hom}(\mathrm{Hom}_k(B, A), \boldsymbol{Z}_p) \\ \approx \big\downarrow & & \xrightarrow{\;\approx\;} \mathrm{Hom}(\mathrm{Hom}_k(B, A) \otimes \boldsymbol{Q}_p/\boldsymbol{Z}_p, \boldsymbol{Q}_p/\boldsymbol{Z}_p) \\ \mathrm{Hom}_k(T_p A, T_p B) & \xrightarrow{\;g_1\;} & \mathrm{Ext}_k^1(T_p A, T_p B) \qquad \big\uparrow h^* \\ & & \xrightarrow{\;\approx\;} \mathrm{Hom}(\mathrm{Hom}_k(T_p B, B(p)), \boldsymbol{Q}_p/\boldsymbol{Z}_p) \end{array}$$

in which the maps are to be described.

The left hand isomorphism is the canonical map (cf. the proof of Thm. 2). The map t is induced by the pairing

$$\langle\,,\rangle\colon \operatorname{Hom}_k(A,B)\times\operatorname{Hom}_k(B,A)\to \boldsymbol{Q}_p/\boldsymbol{Z}_p$$

defined in the statement of the theorem. The non-degeneracy of the pairing

$$\operatorname{End}_k(A\times B)\times\operatorname{End}_k(A\times B)\to\boldsymbol{Z}$$

induced by the trace (cf. [3], V, § 3) implies the non-degeneracy of $\langle\,,\rangle$ using that

$$\operatorname{End}_k(A\times B)=\operatorname{End}_k(A)\times\operatorname{Hom}_k(A,B)\times\operatorname{Hom}_k(B,A)\times\operatorname{End}_k(B).$$

Hence (Lemma z.4), t is a quasi-isomorphism and

$$z(t)=|\det(\langle\alpha_i,\beta_j\rangle)|_p.$$

The map h^* is the dual of the map h in the proof of Thm. 2, and so

$$z(h^*)=z(h)^{-1}=|[\operatorname{Ext}_k^1(A,B)(p)]|_p^{-1}.$$

The map

$$g_1\colon \operatorname{Hom}_k(T_pA,T_pB)\to\operatorname{Ext}_k^1(T_pA,T_pB)$$

is as defined in Lemma 4 below for all p-divisible groups. From the remarks preceding Thm. 1, $A(p)$ and $B(p)$ satisfy the conditions of Lemma 4, and so

$$z(g_1)=\left|q^{d(A)\,d(B)}\prod_{a_i\neq b_j}\left(1-\frac{a_i}{b_j}\right)\right|_p.$$

It follows from Lemma 5 below that the diagram commutes, and hence that $z(t)=z(g_1)\,z(h^*)$ i.e.

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

Since this holds for all primes p, the formula of the theorem is proved.

Lemma 4. *Let G and H be p-divisible groups over k. Let*

$$g\colon \operatorname{Hom}_k(G,H)\to\operatorname{Ext}_k^1(G,H)$$

be the composite of the inclusion

$$\operatorname{Hom}_k(G,H)\to\operatorname{Hom}_{\bar k}(\bar G,\bar H),$$

the surjection

$$\operatorname{Hom}_{\bar k}(\bar G,\bar H)\to\operatorname{Hom}_{\bar k}(\bar G,\bar H)_\Gamma,$$

and

$$\varprojlim_\nu\varprojlim_\mu f_{\mu,\nu}\colon \operatorname{Hom}_{\bar k}(\bar G,\bar H)_\Gamma\to\operatorname{Ext}_k^1(G,H)$$

where

$$f_{\mu,\nu}\colon \operatorname{Hom}_{\bar{k}}(\bar{G}_\nu, \bar{H}_\mu)_\Gamma \to \operatorname{Ext}^1_k(G_\nu, H_\mu)$$

is the f_1 of Lemma 1. Similarly, let

$$g_1\colon \operatorname{Hom}_k(T_p G, T_p H) \to \operatorname{Ext}^1_k(T_p G, T_p H)$$

be the composite of

$$\operatorname{Hom}_k(T_p G, T_p H) \to \operatorname{Hom}_{\bar{k}}(T_p \bar{G}, T_p \bar{H}) \to \operatorname{Hom}_{\bar{k}}(T_p \bar{G}, T_p \bar{H})_\Gamma$$

and

$$\varprojlim_\mu \varinjlim_\nu f_{\mu,\nu}.$$

Then, if no multiple root of $m_G(T)$ or $m_H(T)$ occurs as a root of the other, g and g_1 are quasi-isomorphisms and

$$z(g) = \left| q^{d(G)\, d(H^t)} \prod_{a_i \neq b_j} \left(1 - \frac{a_i}{b_j}\right) \right|_p = z(g_1)$$

where $d(G)$ and $d(H^t)$ are the dimensions of G and H^t, and

$$(a_i)_{1 \leqq i \leqq h(G)}$$

and

$$(b_i)_{1 \leqq i \leqq h(H)}$$

are the roots of $c_G(T)$ and $c_H(T)$ ($h(G)$ and $h(H)$ are the heights of G and H).

Proof. It follows easily from Theorem 1e and the existence of a commutative diagram

$$\begin{array}{ccc} \operatorname{Hom}_k(G, H) & \approx & \operatorname{Hom}_k(T_p H^t, T_p G^t) \\ \downarrow g & & \downarrow g_1 \\ \operatorname{Ext}^1_k(G, H) & \approx & \operatorname{Ext}^1_k(T_p H^t, T_p G^t) \end{array}$$

that the formula for $z(g)$ holds if and only if the formula for $z(g_1)$ holds.

Assume first that G and H are étale. Then

$$\operatorname{Hom}_{\bar{k}}(T_p \bar{G}, T_p \bar{H})_\Gamma \to \operatorname{Ext}^1_k(T_p G, T_p H)$$

is an isomorphism, and $z(g) = z(e)$ where e is the map

$$\operatorname{Hom}_{\bar{k}}(T_p \bar{G}, T_p \bar{H})^\Gamma \to \operatorname{Hom}_{\bar{k}}(T_p \bar{G}, T_p \bar{H})_\Gamma$$

induced by the identity map of

$$\operatorname{Hom}_{\bar{k}}(T_p \bar{G}, T_p \bar{H}).$$

The characteristic polynomials of σ_k acting on $T_p \bar{G}$ and $T_p \bar{H}$ are $c_G(T)$ and $c_H(T)$. It follows, by taking

$$A = \mathrm{Hom}_{\bar{k}}(T_p \bar{G}, T_p \bar{H})$$

and $\theta = \sigma_k - 1$ in [10], Lemma z.4, that

$$z(e) = \left| \prod_{a_i \neq b_j} \left(1 - \frac{b_j}{a_i}\right) \right|_p = \left| \prod_{a_i \neq b_j} \left(1 - \frac{a_i}{b_j}\right) \right|_p .$$

All other cases of the lemma follow by similarly elementary arguments except the case $G = G_{cc}$, $H = H_{cc}$, so, for the remainder of the proof we work only with this case.

We show first that, if H is isogenous to H', then the lemma is true for H if and only if it is true for H'. We may assume the isogeny to be of the form

$$0 \longrightarrow \alpha_p \longrightarrow H' \longrightarrow H \longrightarrow 0 .$$

The $\mathrm{Ext}_k^r(G, -)$ sequence of this sequence may be broken into exact sequences,

$$\begin{array}{ccccccccc} 0 \longrightarrow \mathrm{Hom}_k(G, \alpha_p) \longrightarrow & \mathrm{Hom}_k(G, H') & \longrightarrow & \mathrm{Hom}_k(G, H) & \longrightarrow & C_0 & \longrightarrow 0 \\ & \downarrow g' & & \downarrow g & & & \\ 0 \longrightarrow C_1 \longrightarrow & \mathrm{Ext}_k^1(G, H') & \longrightarrow & \mathrm{Ext}_k^1(G, H) & \longrightarrow & \mathrm{Ext}_k^2(G, \alpha_p) & \longrightarrow 0 \end{array}$$

$$0 \longrightarrow C_0 \longrightarrow \mathrm{Ext}_k^1(G, \alpha_p) \longrightarrow C_1 \longrightarrow 0$$

($\mathrm{Ext}_k^2(G, H) = 0$ because $\mathrm{Ext}_k^2(G_v, H) = 0$ all v, by Lemma 2). Thus

$$\frac{z(g')}{z(g)} = \left| \frac{[\mathrm{Ext}_k^1(G, \alpha_p)]}{[\mathrm{Hom}_k(G, \alpha_p)]\,[\mathrm{Ext}_k^2(G, \alpha_p)]} \right|_p$$

provided the orders occurring on the right are finite. It is easily seen that $\mathrm{Hom}_k(G, \alpha_p) = 0$.

From the sequence

$$0 \longrightarrow A_k \xrightarrow{V} A_k \longrightarrow D_k(G_a) \longrightarrow 0$$

we get that

$$\mathrm{Ext}_k^1(G, G_a) \approx \mathrm{Ext}_{A_k}^1(D_k(G_a), D_k(G)) \approx D_k(G)/V D_k(G)$$

is finite (indeed, its length as a W_k-module is equal to the dimension of G^t). From $\mathrm{Ext}_k^r(G_a, G_a) = 0$, $r \geqq 2$, we get that $\mathrm{Ext}_k^2(G, G_a) = 0$, and hence from

$$0 \longrightarrow \alpha_p \longrightarrow G_a \longrightarrow G_a \longrightarrow 0$$

we get an exact sequence

$$0 \to \operatorname{Ext}_k^1(G, \boldsymbol{\alpha}_p) \to \operatorname{Ext}_k^1(G, \boldsymbol{G}_a) \to \operatorname{Ext}_k^1(G, \boldsymbol{G}_a) \to \operatorname{Ext}_k^2(G, \boldsymbol{\alpha}_p) \to 0.$$

This shows that $\operatorname{Ext}_k^1(G, \boldsymbol{\alpha}_p)$ and $\operatorname{Ext}_k^2(G, \boldsymbol{\alpha}_p)$ are finite, and have the same order. Consequently, $z(g) = z(g')$, as should be so, because $c_H(T) = c_{H'}(T)$ and $d(H^t) = d(H'^t)$.

A similar argument shows that, in proving the lemma, we may replace G by a isogenous group. Thus (Thm. 1), it suffices to prove the lemma under the following assumptions on G and H.

$$D_k(G) = A_k/A_k\lambda_1, \quad \lambda_1 = \mu_1(F^a, V^a), \quad T^{n_1/a}\mu_1(T, q/T) = m_G(T)$$
$$h_1 = h(G), \quad n_1 = d(G), \quad m_1 = h_1 - n_1 = d(G^t),$$
$$D_k(H) = A_k/A_k\lambda_2, \quad \lambda_2 = \mu_2(F^a, V^a), \quad T^{n_2/a}\mu_2(T, q/T) = m_H(T)$$
$$h_2 = h(H), \quad n_2 = d(H), \quad m_2 = h_2 - n_2 = d(H^t).$$

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

Case 1. $m_G(T)$ and $m_H(T)$ have no common root. The sequence

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

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

$$0 \to \operatorname{Hom}_k(G, H) \to A_k/A_k\lambda_1 \xrightarrow{\lambda_2} A_k/A_k\lambda_1 \to \operatorname{Ext}_k^1(G, H) \to 0.$$

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

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

where

$$\begin{array}{ccc} A'_k/A'_k\lambda_1 & \xrightarrow{1 \otimes \lambda_2} & A'_k/A'_k\lambda_1 \\ {\scriptstyle F^{n_2}} \nwarrow & & \nearrow {\scriptstyle m_H(F^a)} \\ & A'_k/A'_k\lambda_1 & \end{array}$$

$$|\det(F^{n_2})|_p^a = |a_1 \dots a_{h_1}|_p^{n_2} = |q^{n_1 n_2}|_p,$$

$$\left| \det(m_H(F^a)) \right|_p^a = \left| \prod (a_i - b_j) \right|_p = \left| q^{n_2 h_1} \prod \left(1 - \frac{a_i}{b_j}\right) \right|_p.$$

Thus

$$z(f) = \left| q^{n_1 m_2} \prod \left(1 - \frac{a_i}{b_j}\right) \right|_p,$$

and the formula is verified for this case.

Case 2. $m_G(T)$ and $m_H(T)$ have a root in common, i.e. they are powers of the same $\mathbf{Z}_p$-irreduciple 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

$$g\colon \operatorname{Hom}_k(G,H)\longrightarrow \operatorname{Ext}^1_k(G,H).$$

Write $M=D_k(G)$ and $\bar{M}=D_{\bar{k}}(G)$, so $\bar{M}\approx W_{\bar{k}}\otimes_{W_k} M$ [6], 3.16. The $\operatorname{Ext}^r_k(-,M)$ sequence of

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

is

$$0\longrightarrow \operatorname{Hom}_k(G,H)\longrightarrow M \xrightarrow{\lambda_2\cdot} M\longrightarrow \operatorname{Ext}^1_k(G,H)\longrightarrow 0$$

and the

$$\operatorname{Ext}^r_{\bar{k}}(-,\bar{M})$$

sequence of

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

is

$$0\longrightarrow \operatorname{Hom}_{\bar{k}}(\bar{G},\bar{H})\longrightarrow \bar{M} \xrightarrow{\bar{\lambda}_2\cdot} \bar{M}\longrightarrow \operatorname{Ext}^1_{\bar{k}}(\bar{G},\bar{H})\longrightarrow 0.$$

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

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

The image of $\lambda_2 v$ under $M\to\operatorname{Ext}^1_k(G,H)$ is $f(u)$.

In our case, $\lambda_2=\lambda_1$, so multiplication by λ_2 is zero on M, and

$$\operatorname{Hom}_k(G,H)=A/A\lambda_1=\operatorname{Ext}_k(G,H).$$

Since $A/A\lambda_1$ is torsion-free, g is a quasi-isomorphism if and only if the corresponding map

$$g\colon A'_k/A'_k\lambda_1\longrightarrow A'_k/A'_k\lambda_1$$

has non-zero determinant, and then

$$z(g)=|\det(g)|_p^a.$$

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

$$\lambda_2(F,pF^{-1})=F^{m_2}+b_{m_2-a}F^{m_2-a}+\cdots+b_{-n_2}F^{-n_2}=F^{-n_2}m_H(F^a).$$

Then

$$\begin{aligned} g(u) &= \lambda_2(F, pF^{-1})\,v \\ &= m_2\, u\, F^{m_2} + (m_2 - a)\, b_{m_2-a}\, u\, F^{m_2-a} + \cdots \qquad (\text{as } v\,\lambda_2 = 0) \\ &= u\, F^a \frac{d}{dF^a}\left(F^{-n_2}\, m_H(F^a)\right) \\ &= F^{a-n_2} \frac{d}{dF^a}\left(m_H(F^a)\right) u\,. \end{aligned}$$

Clearly g is a quasi-isomorphism, and

$$z(g) = \frac{\left|\det\left(\dfrac{d}{dF^a}\left(m_H(F^a)\right)\right)\right|_p^a}{|\det(F^{n_2-a})|_p^a}$$

where

$$\begin{array}{ccc} A'_k/A'_k\,\lambda_1 & \xrightarrow{\quad g \quad} & A'_k/A'_k\,\lambda_1 \\ & \nwarrow^{F^{n_2-a}} \qquad \nearrow_{\frac{d}{dF^a}(m_H(F^a))} & \\ & A'_k/A'_k\,\lambda_1 & \end{array}$$

But

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

and

$$\begin{aligned} \left|\det\left(\frac{d}{dF^a}\left(m_H(F^a)\right)\right)\right|_p^a &= \Big|\prod_{a_i \neq b_j} (a_i - b_j)\Big|_p \\ &= \left|q^{n_1(h_1-a)} \prod_{a_i \neq b_j}\left(1 - \frac{a_i}{b_j}\right)\right|_p. \end{aligned}$$

Thus

$$z(f) = \left|q^{n_1 m_2} \prod_{a_i \neq b_j}\left(1 - \frac{a_i}{b_j}\right)\right|_p,$$

which completes the proof of the lemma.

To complete the proof of Theorem 3, we have only to show that the diagram (*) commutes. This reduces easily to the following lemma.

Lemma 5. *If G is a p-divisible group over k, then*

$$\begin{array}{ccc} \mathrm{Hom}_k(G_\nu, G_\nu) & & \\ \Big\downarrow g & \searrow^{T_\nu} & \\ & & \mathbf{Z}/p^\nu\,\mathbf{Z} \\ & \nearrow_{\eta_\nu} & \\ \mathrm{Ext}_{k,\nu}(G_\nu, G_\nu) & & \end{array}$$

commutes, where T_v is the trace map (see § 2), g is the composite of

$$\mathrm{Hom}_k(G_v, G_v) \longrightarrow \mathrm{Hom}_{\bar{k}}(\bar{G}_v, \bar{G}_v)_\Gamma$$

with f, (see Lemma 1), and η_v is as in § 2.

Proof. If G or its dual is étale, then this is immediate from the definition of η_v. Thus we may assume $G = G_{cc}$. Let $M_v = D_k(G_v)$, let

$$\gamma \in \mathrm{Hom}_{A_k}(M_v, M_v)$$

and choose $\beta \in \mathrm{Hom}_{W_{\bar{k}}}(\bar{M}_v, \bar{M}_v)$ such that $\beta - \beta^{\sigma_k} = \gamma$. Then $g(\gamma)$ is the class of the extension $E \leftrightarrow (-\alpha F, V\alpha)$ where $-\alpha F = F\beta - \beta F$ and $V\alpha = V\beta - \beta V$. From this,

$$\eta_v(g(\gamma)) = S_v T_v(\alpha) = S_v(T_v(\beta) - T_v(\beta)^\sigma) = T_v(\beta) - T_v(\beta)^{\sigma_k} = T_v(\gamma).$$

References

1. GABRIEL, P.: Sur les catégories abéliennes localement noethériennes et leurs applications aux algèbres etudiées par Dieudonné, in Séminaire J.-P. Serre, 1960.
2. JACOBSON, N.: The theory of rings. Mathematical Surveys II. New York: Interscience 1943.
3. LANG, S.: Abelian varieties. Interscience Tracts No. 7. New York: Interscience 1959.
4. MANIN, YU. I.: The theory of commutative formal groups over fields of finite characteristic. Russian Math. Surveys **18**, 1–83 (1963).
5. MITCHELL, B.: Theory of categories. New York: Academic Press 1965.
6. ODA, T.: Abelian varieties over a perfect field and Dieudonné modules. Thesis, Harvard University, 1967.
7. OORT, F.: Commutative group schemes. Lecture Notes in Math. 15. Berlin-Heidelberg-New York: Springer 1966.
8. SERRE, J.-P.: Groupes *p*-divisible (d'après J. TATE). Séminaire Bourbaki, 1966/67, No. 318.
9. SHARMA, P.: In: Séminaire Heidelberg-Strasbourg 1965/66, Groupes algébriques linéaires. Publ. IRMA, Strasbourg, 1967.
10. TATE, J.: On the conjectures of BIRCH and SWINNERTON-DYER and a geometric analogue. Séminaire Bourbaki, 1965/66, No. 306.
11. — *p*-divisible groups. Notes of the Conference at Driebergen, 1966, to be published by Springer.
12. — Endomorphisms of abelian varieties over finite fields. Inventiones math. **2**, 134–144 (1966).
13. — Endomorphisms of abelian varieties over finite fields, (II). To appear, Inventiones math.

Dr. J. S. MILNE
Department of Mathematics
University College
London W.C. 1
Great Britain

(Received September 16, 1967)