Inventiones math. 18, 183–266 (1972)

Rational Points of Abelian Varieties with Values in Towers of Number Fields

Barry Mazur* (Cambridge)

Contents

* Most of the work for this paper was done at the Institut Des Hautes Etudes Scientifiques, whose generosity and hospitality I greatly appreciate. It was also partially supported by a grant from the National Science Foundation – GP-31359.

§ 1. Introduction

a) The Motivating Problem

Let K be a number field. For every prime number p one may define a tower of abelian extensions of K, called the *cyclotomic Γ-extension of K associated to p:*

$$K = K_0 \subset K_1 \subset \cdots \subset K_n \subset \cdots \subset K_\infty = L = \bigcup_{n=0}^{\infty} K_n$$

(cf. § 1 (c)) such that $\mathrm{Gal}(K_n/K)$ is cyclic of order p^n. Set $\Gamma = \mathrm{Gal}(L/K)$.

Let A be an abelian variety over K which has good, ordinary reduction at all primes dividing p. The question motivating the theory presented in this paper is the following: Is the group of rational points $A(L)$ finitely generated?

The classical Mordell-Weil theorem guarantees that $A(K_n)$ is finitely generated for each n, but gives no indication of what to expect when one considers questions concerning asymptotic growth of the group of rational points as one varies the number field.

Here is some reason for hoping that our question has an affirmative answer: Suppose that A is the Jacobian of a curve C. Then $A(L)$ is closely related to the Néron-Severi group of the minimal regular arithmetic surface which is a model for C over the ring of integers in L. Consequently, Iwasawa's magnificent analogy between L and the rational function field of a curve over the algebraic closure of a finite field might lead one to expect that $A(L)$ has a structure similar to that of the Néron-Severi group of a surface over the algebraic closure of a finite field; but the Néron-Severi group of such a surface is finitely generated.

I have found that the axiomatics of the above problem can be kept more clearly in focus if one works more generally with an abelian variety A/K and any Γ-extension L/K satisfying the hypotheses of (6.1) below. We call such a pair $(L/K, A)$ *admissible.*

Much of the information expressing the asymptotic growth of $A(K_n)$ and the p-primary component of the Shafarevitch-Tate group of A, ${}_{p^\infty}Ш_A(K_n)$ is contained in a certain polynomial with p-adic coefficients that we define by means of an essential construction made in § 6. This polynomial, which depends upon a choice of topological generator $\gamma \in \Gamma$, and which we denote $f(L/K, A, \gamma; t)$ or $f(L/K, A; t)$, we call the *characteristic polynomial* of the admissible pair. In the case where L/K is the p-adic cyclotomic Γ-extension, it is reasonable to refer to it as $f_p(A/K; t)$, the *p-adic characteristic polynomial of A/K.*

These polynomials, as defined, could be identically zero. We conjecture that they are never identically zero. Moreover, one can show that if A is of dimension 1, or of CM-type, if $f_p(A/K; t)$ is not identically zero, $A(L)$ is finitely generated (§ 6).

A corollary of one of our main results assures us that $f(L/K, A; t)$ is not identically zero in the case where the two groups

$$A(K), \quad {}_{p^\infty}Ш_A(K)$$

are both finite. This answers our question affirmatively in a large number of cases. It is rather interesting to note that in the cases where we have thereby shown $A(L)$ to be finitely generated, our proof does *not* provide us with an effectively computable upper bound for the rank of $A(L)$.

Our theory is modeled after Iwasawa's, and we define $f(L/K, A; t)$ as the characteristic polynomial of a Γ-module, $H = H_{(L/K, A)}$ which we construct (6.4) for any admissible pair.

The Γ-module $H_{(L/K, A)}$ is defined cohomologically, and is somewhat reminiscent of the classical "Selmer group", but it does differ from it. The structure of the Γ-module H provides us with information concerning the asymptotic growth of the Mordel-Weil and Shafarevitch-Tate groups, for we establish the sequence of exact sequences:

$$(*) \qquad 0 \to A(K_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to H^{\Gamma_n} \to {}_{p^\infty}Ш_A(K_n) \to 0 \quad (n \geqq 0).$$

These exist and are exact *only* modulo finite groups whose orders are bounded, independent of n. In the terminology of § 2(b), they are exact sequences mod $\mathscr{C}$. Here the middle group is the fixed submodule under the action of Γ_n (6.5).

Here are some consequences of (*):

(a) *The rank of $A(L)$ is less than or equal to the number of zeroes of $f(L/K, A; t)$, counting multiplicities, where t runs through all p^n-th roots of unity (all n).*

(b) *If $f(L/K, A; t)$ doesn't vanish on any p^n-th root of unity, then from the classification theorem of Iwasawa,*

$$\log_p(\#\, {}_{p^\infty}Ш_A(K_n)) = \mu p^n + \lambda n + c_n$$

where λ is the degree of $f(L/K, A; t)$, μ is Iwasawa's μ-invariant associated to H, and $|c_n|$ is bounded, independent of n.

For example, if $K = \mathbb{Q}$, A is the modular curve $X_0(11)$ (§ 10) and $p = 5$, we find $f_p(A/\mathbb{Q}; t) = p$, and obtain that $A(L)$ is in fact, finite, and modulo $\mathscr{C}$, the 5-primary component of $Ш_A(K_n)$ is a vector space over $\mathbb{F}_5$ of dimension 5^n.

One can establish a functional equation for $f_p(A/K; t)$ of the type enjoyed by the classical L-series of A/K (§ 7). The p-adic characteristic polynomial of A/K behaves as if it were a p-adic polynomial analogue of the classical L-series of A/K, and of Iwasawa's characteristic polynomials. Indeed, we hope that a close study of these characteristic

polynomials may provide some new perspective on the classical theory of cyclotomic fields and irregular primes.

There are some interesting divergences from the classical theory and one of them is worth describing in detail:

b) The Phenomenon of Anomalous Primes

As in the work of Iwasawa, it is of some interest to consider the base fields $K=\mathbb{Q}(\zeta_p)$ where ζ_p is a primitive p-th root of 1. Ignore the case $p=2$. Fix A an elliptic curve defined over $\mathbb{Q}$. Then the module H decomposes into eigenspaces with respect to the action of the group $\Delta=\mathrm{Gal}(K/\mathbb{Q})$.

All eigenspaces except for the fixed part of Δ behave like the classical theory of irregular primes (§ 8(a)). The significant difference occurs when we examine the fixed part of Δ, or equivalently, when we consider the base field $K=\mathbb{Q}$. If $A/\mathbb{Q}$ is an elliptic curve, say that a prime number p is *anomalous* for A if A has good reduction at p, and the trace of the Frobenius operator associated to A_p is congruent to 1 mod p.

For the anomalous primes of A, we find that the Γ-module H is *necessarily* of infinite order. There is a much more precise result if p is odd, $A(\mathbb{Q})$ is trivial, and the p-primary component of $Ш_A(\mathbb{Q})$ is also trivial. [The Shafarevitch-Tate conjecture would imply that these primes are of density $\frac{1}{2}$ if A has complex multiplication, and of density 1 otherwise.] We show that H is trivial (or equivalently, $A(L)$ is finite, and $Ш_A(K_n)$ has finite p-primary component, of bounded order independent of n) if and only if p is not anomalous for A. If p is anomalous, then H is necessarily infinite, and we prove, further, that H is either an irreducible Γ-module, mod $\mathscr{C}$ or is an extension of one irreducible Γ-module by another irreducible Γ-module. That is, f_p is either irreducible over $\mathbb{Z}_p$ or a product of exactly two irreducibles.

The set of anomalous primes of an elliptic curves seems to be a rather rare set of primes. For example, if A is the modular curve of level 11 the prime $p=5$ is the only anomalous prime. However, for any finite set of primes, one can construct an elliptic curve with respect to which they are all anomalous. Can an elliptic curve possess an infinite number of anomalous primes?

An interesting example to consider is the family of curves

$$A\colon\ y^2=x^3+D$$

where D is a rational integer which is neither a square nor a cube in $\mathbb{Q}(\xi)$ where ξ is a primitive 3-rd root of 1. The curve A admits $\mathbb{Q}(\xi)$ as a field of complex multiplication, an automorphism of order 3 being given by

$$(x, y)\to(\xi x, y).$$

If A has good reduction at p, it is well known that these conditions are equivalent:

(i) A has ordinary reduction at p.

(ii) $p \equiv 1 \bmod 3$.

(iii) p splits in $\mathbb{Q}(\xi)$.

Suppose that A has ordinary reduction at p. The Frobenius endomorphism $\mathbb{F}_p$ then satisfies the equation $x^2 - a_p x + p = 0$. But $\mathbb{F}_p \in \mathbb{Z}[\xi]$, and therefore:

$$a_p^2 - 4p = -3h^2 \quad \text{with } h \in \mathbb{Z}.$$

That is, $p = (3h^2 - a_p^2)/4$. Moreover, if p is anomalous, $a_p = 1$, and therefore p belongs to the quadratic progression

$$q(h) = \frac{3h^2 - 1}{4}.$$

Let p range through the primes of the quadratic progression $q(h)$, and let π, $\bar{\pi}$ denote, indiscriminately, the two solutions of the equation $x^2 - x + p = 0$ in $\mathbb{Z}[\xi]$. Thus, for any p in the quadratic progression $q(h)$, we have two decompositions of p in $\mathbb{Z}[\xi]$:

$$p = \mathbb{F}_p \cdot \bar{\mathbb{F}}_p, \qquad p = \pi\bar{\pi}.$$

After possible relabeling of π and $\bar{\pi}$, we can write: $\mathbb{F}_p = \omega_p \cdot \pi$ where ω_p is a sixth root of 1.

Consequently, p is anomalous if and only if p belongs to the quadratic progression $q(h)$, and $\omega_p = 1$.

As Serre pointed out to me, Hardy and Littlewood [24] have conjectured that $Q(N)$, the number of primes less than N in the quadratic progression $q(h)$ should have the following asymptotic shape:

$$Q(N) \sim C \frac{\sqrt{N}}{\log N} \quad \text{as } N \to \infty$$

where C is a constant explicitly given as an infinite product.

It is also tempting, following the analogue of Kummer's conjecture ([12], § 20.6), to hope that the primes p belonging to $q(h)$ for which $\omega_p = 1$ represents, asymptotically, a nonzero fraction of the total number of primes in $q(h)$ ($\frac{1}{6}$ is a natural guess, but one has hardly enough numerical evidence).

We would then be led to conjecture that if $\mathbf{A.P.}_D(N)$ denotes the number of primes less than N which are anomalous for the elliptic curve A, there is a positive constant C' such that

$$\mathbf{A.P.}_D(N) \sim C' \frac{\sqrt{N}}{\log N} \quad \text{as } N \to \infty$$

and in particular: there should exist an infinite number of anomalous primes for A.

Calculation by computing machine shows that for $N=100000$, $Q(N)=64$ and

$$\mathbf{A.P.}_D(N)=13 \quad \text{for } D=-5$$
$$\mathbf{A.P.}_D(N)=11 \quad \text{for } D=-2.$$

The 13 anomalous primes for $y^2=x^3-5$ which are less than 100000 are:

37	3571	45757
271	5419	50311
919	12097	87211
1951	23497	
2437	25117.	

From the tables of Birch and Swinnerton-Dyer [7] one finds that the curve $A: y^2=x^3-5$ has only a finite number of rational points over $\mathbb{Q}$. In fact, $A(\mathbb{Q})$ is trivial. Consequently the detailed calculations of § 8(c) apply to it.

One is led to wonder about the "distribution" of zeroes of $f_p(A/\mathbb{Q}, t)$ as p varies through the set of anomalous primes. How often is the non-triviality of f_p due to the existence of an infinity of rational points of A in the p-cyclotomic Γ-extension? How often due to the unboundedness of the Shafaravetch-Tate groups? How often for the Γ-modules, $H=H(p)$, is Iwasawa's μ-invariant nontrivial?

c) The Analytic Theory

What is presented in this paper may be called the "algebraic theory". Recently, for certain abelian varieties over $\mathbb{Q}$, Swinnerton-Dyer and I have succeeded in setting up the beginnings of a parallel theory, which might be called the "analytic theory" [42]. I shall describe this theory and point out its relationship with what is done here:

Let $X_0(N)/\mathbb{Q}$ denote the modular curve associated to the subgroup $\Gamma_0(N)\subset \mathbf{PSL}(2,\mathbb{Z})$. Let $J_0(N)/\mathbb{Q}$ denote its Jacobian. Let p be any prime number with respect to which A has ordinary reduction.

Then, dependent upon a fixed choice of topological generator $\gamma\in\Gamma$, Swinnerton-Dyer and I associate to A/K a p-adic analytic power series $L_p(A/K; t)_{(\gamma)}\in\mathbb{Z}_p[[t]]$. If we make the substitution of variables $t\to\gamma^{1-s}$ we obtain a power series in s, $L_p(A/K; s)$ which no longer depends upon γ, and which we call the *p-adic L-series of* A/K.

This p-adic L-series is obtained by means of a construction which associates to any parabolic modular form ω (of weight 2 under $\Gamma_0(N)$ and an eigenvector for the Hecke operators) a p-adic power series: the *p-adic Mellin transform of* ω [42].

The p-adic L-series of A/K satisfies a functional equation of the same type satisfied by the classical L-series. Also, if $A/\mathbb{Q}$ is an elliptic curve,

its p-adic L-series vanishes at $s=1$ if and only if the classical L-series vanishes at $s=1$ [42].

If $A/\mathbb{Q}$ is an abelian variety as above, let $g_p(A/K;t)$ be the unique polynomial with p-adic integral coefficients, of smallest degree, such that

$$L_p(A/K;t)_{(\gamma)}=g_p(A/K;t)\cdot U_p(A/K;t)$$

where: (a) $U_p(A/K;t)$ is a power series in $\mathbb{Z}_p[[t]]$ whose constant term is a p-adic unit.

(b) $g_p(A/K;t)$ is either identically 0, or its highest coefficient is a power of p.

Call $g_p(A/K;t)$ the "*analytically-defined*" *p-adic characteristic polynomial of* A/K.

The parallel between the "algebraic" and the "analytic" theory can be expressed by means of the conjecture that (p odd) the "analytically-defined" p-adic characteristic polynomial of A/K is equal to the p-adic characteristic polynomial of A/K, as defined in this paper.

This conjecture has the air of being unattackable, at present. Nevertheless, it suggests that one develop the "algebraic" and the "analytic" theories, side by side. So far as either of the theories has been developed, this can be done. In particular, we can establish, in the "analytic theory" the analogue of the detailed theory of anomalous primes given in § 8.

A tremendous advantage of the "analytic theory" is that it is amenable to computing machine calculation. J. Davenport, N. Stephens, P. Swinnerton-Dyer and I have studied $g_p(A/\mathbb{Q}(\zeta_p);t)$ for the modular curves $A=X_0(11)$, $X_0(17)$, and all odd ordinary primes $p<350$.

We compute the degree of g_p in these cases (see [42] for complete tables) and we discover that except when $p=5$ and $A=X_0(11)$ it is monic (i.e. the "analytic" μ-invariant is zero).

The pursuit of the parallelism between the two theories is hardly farfetched, in the light of recent work of Iwasawa and Leopold-Kubota [33], nor is it as special as it may sound, in the light of recent conjectures of Weil.

d) Some Unresolved Issues

1. (Supersingular Primes)

Our theory leads us to make a rather detailed study of the norm mapping on the points of an abelian variety with values in a local field, and thence to a study of the fundamental group of certain pro-algebraic groups. Had we settled the questions that arise in this area, in complete generality, we would have been able to extend our theory to include the supersingular primes.

There has been recently some progress in this direction (notably some unpublished work of Hazelwinkel concerning the norm mapping from Γ-extensions of one-parameter formal groups) which suggests that

the situation is remarkably different from the case of ordinary primes. The problems are, of course, much harder.

If A is an elliptic curve with bad reduction of multiplicative type at p, Nacybullin (see [37], 4.9) has settled these questions, using the theory of Tate.

In the analytic theory, as well, we have not been able to treat supersingular primes, and we suspect that for p supersingular, if the p-adic L-series exists, it must have poles in the unit disc.

2. (Higher dimensional analogues: p-adic arithmetic cohomology of varieties over number fields)

We shall emphasize the fact that the theory presented in this paper is a *one-dimensional* theory by a change of notation and viewpoint:

Let V be a proper smooth variety over a number field K and let A denote its Albanese variety.

If $(L/K, A)$ is admissible, set

$$H^1_{(L/K,V)} \underset{\text{def}}{=} H_{(L/K,A)}.$$

This terminology is meant to remind one that $H_{(L/K,A)}$ depends *only* upon the Galois module $H^1_{et}(V_{\bar{K}}, \mathbb{Q}_p/\mathbb{Z}_p)$, where $\bar{K}/K$ is an algebraic closure of K.

It is tempting to hope that one can define, for any $r \geqq 0$, a Γ-module $H^r_{(L/K,V)}$ which depends only upon the Galois module $H^r_{et}(V_{\bar{K}}, \mathbb{Q}_p/\mathbb{Z}_p)$ in a manner analogous to the definition of $H_{(L/K,A)}$.

At first one should be content to define such a Γ-module just for Γ-extensions L/K which satisfy an r-dimensional analogue of the notion of "admissibility" with respect to V. For $r=0$ one should rediscover Iwasawa's theory for the Γ-extension L/K. If L/K is the p-cyclotomic Γ-extension, then the correct definition of H^r above should be called the r-dimensional *p-adic arithmetic cohomology of* V/K.

There is an analogous project in the "analytic theory" which also deserves to be done: Namely, to define the p-adic Mellin transform of parabolic modular forms under $\Gamma_0(N)$ of *arbitrary* weight $k=2r$, which are eigenvectors for the Hecke operators.

e) Some Remarks on the Writing of this Paper

What follows is a mildly revised and extended version of the mimeographed notes [38]. A survey of its contents and an introduction to the cohomological techniques used here can be found in the notes to a course I gave at Orsay [39]. A very good expository treatment of the contents of [38] as well as other related things can be found in Manin's paper [37].

Manin's exposition differs from mine in that he re-expresses my Γ-module H solely in terms of certain diagrams of Galois cohomology groups. This makes the main definitions of this paper accessible, in principle, to anyone with a knowledge of Galois cohomology. It is also important to give such a definition, for a theory whose complexities are decidedly number-theoretic should be as free from theoretical superstructure as possible.

The reader may wonder, then, why, in the rewriting of the notes [38] I persist in defining $H_{(L/K, A)}$ as the cohomology group of a sheaf for the $fpqf$ topology. There are two minor advantages. The first is a technical one: the full cohomological panoply is at one's immediate disposal. Secondly, it is not ad hoc: one has a firmer sense, at the outset, that the definition is appropriate.

I have attempted to give the full details, or references, to everything used in this paper. There is one exception worth signaling: In § 7 I make use of the "flat arithmetic duality theorem" proved by Artin and myself. This theorem is part of a long range project and has not yet appeared. I expect it to appear shortly, however, and certain results preparatory to it have already appeared [5, 40, 41].

In § 4(b), (c), the theory of pro-algebraic groups is taken up from scratch. We redo all the basic definitions so as to be able to work with arbitrary formal groups over nonalgebraically closed residue fields.

In § 4(d), (e) we review the well known relationship between the structure of the formal completion of an ordinary abelian variety and its zeta-function.

The work done in § 4(f) is the key to our main results. There we calculate explicitly the cokernel of the norm mapping from a Γ-extension on ordinary abelian varieties over a local field.

In § 9 we use the cohomological apparatus to refine the classical "technique of first descent" which enables one, in happy circumstances, to compute the group of rational points of an elliptic curve over $\mathbb{Q}$, or over small number fields. The results of this section may be of interest, apart from their use in the present theory (expecially Table 1).

I should like to thank K. Iwasawa and J.-P. Serre for generously allowing me the use of preliminary versions of their manuscripts; and P. Deligne, R. Rasala, P. Swinnerton-Dyer and J. Tate for their useful suggestions.

§ 2. Γ-Modules

a) Classification

In this paragraph we shall consider discrete p-abelian groups. If M is such, its Pontrjagin dual N may be regarded as a compact topological $\mathbb{Z}_p$-module. We say M is of *cofinite type* if N is of finite type as a $\mathbb{Z}_p$-

module. M is of cofinite type if and only if its elements of order p, denoted ${}_pM$, is a finite group. Such a group M has the property that its maximal p-divisible subgroup $\mathrm{div}(M)$ is of finite index, and is isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^\lambda$ for some $\lambda < +\infty$. The integer λ is an invariant of M, called its *corank*.

If M is a discrete p-abelian group whose maximal p-divisible subgroup is of cofinite type (and hence isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^\lambda$ for some $\lambda < +\infty$), we shall say that M is of *finite corank* λ. For any such abelian group M, form $V = N \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Then V is a vector space over $\mathbb{Q}_p$ whose dimension is λ. We refer to V as the $\mathbb{Q}_p$-*space associated to* M.

Let Γ be a topological group isomorphic to $\mathbb{Z}_p$ (as considered by Iwasawa [29]. We follow Iwasawa by not requiring that any isomorphism be specified.) By a Γ-module, one means [29] a discrete p-abelian group M together with a continuous action of Γ on M as a group of antomorphisms. There are some useful equivalent ways of viewing the above structure. Here is one: Define Λ to be the compact topological ring obtained as the projective limit of the group rings,

$$\Lambda = \varprojlim \mathbb{Z}_p[\Gamma/\Gamma_n]$$

where $\Gamma_n \subset \Gamma$ is the unique closed subgroup of index p^n in Γ. To endow M with the structure of a Γ-module is the same as to endow the compact topological $\mathbb{Z}_p$-module N with a continuous (unitary, of course) Λ-module structure. The classification of Γ-modules, then, is equivalent to the classification of compact continuous Λ-modules. Since Λ is isomorphic to a power series ring $\mathbb{Z}_p[[T]]$ (under an isomorphism which sends the image of a topological generator γ of Γ to $1+T$: thus the isomorphism is noncanonical), the classification of Γ-modules follows the pattern of the general classification theory of modules over a regular complete noetherian local ring of dimension two [52].

We shall say that M is Γ-*cofinite*, or *of cofinite type as a* Γ-*module* if M is of finite type as a Λ-module. It is equivalent to ask that M^Γ be of cofinite type. If we let $\mathscr{C}$ stand for the full, thick ([19], 1.11) subcategory of the abelian category of Γ-modules, consisting in those Γ-modules of finite cardinality, Iwasawa gives [29, 30] a precise classification of Γ-modules M which are Γ-cofinite, modulo $\mathscr{C}$.

We shall summarize this classification below, by describing both the discrete Γ-module M and the compact Pontrjagin dual module N regarded as a module over $\mathbb{Z}_p[[T]]$. We will often pass from consideration of the discrete to that of the compact version.

Classification List. The compact $\mathbb{Z}_p[[T]]$-module N (resp. its discrete Pontrjagin dual M), may be written mod $\mathscr{C}$ as a sum of three kinds of modules:

I. Compact. A free $\mathbb{Z}_p[[T]]$-module F of finite rank ρ.

(Resp.) I. Discrete. The Pontrjagin dual of F, Φ, which we may refer to as a "cofree Γ-module of cofree-rank ρ". We have that*

$$\Phi^{\Gamma_n} \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{\rho p^n}.$$

II. Compact. A direct sum of $\mathbb{Z}_p[[T]]$-modules of the form, $\mathbb{Z}/p^{\mu_j}[[T]]$ where $\mu_1 \leqq \mu_2 \leqq \cdots \leqq \mu_s$.

(Resp.) II. Discrete. The Pontrjagin dual B of the above, which has the structure:*

$$B^{\Gamma_n} = \bigoplus_j (p^{-\mu_j}\mathbb{Z}/\mathbb{Z})^{p^n}.$$

III. Compact. A $\mathbb{Z}_p$-module which is free of rank λ, given the structure of a $\mathbb{Z}_p[[T]]$-module, e.g., by stipulating a topologically unipotent action of $1+T$.

(Resp.) III. Discrete. The Pontrjagin dual of the above would be a discrete group isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^\lambda$ with a topologically unipotent action of γ, a topological generator of Γ, specified.*

The data consisting in: $\{\rho$, the set of μ_j's, λ, and the isomorphism class of the representation of Γ in $\mathbf{GL}(\mathbb{Z}_p, \lambda)$ obtained from the module of type III$\}$ are determined by the Γ-module M considered mod $\mathscr{C}$, *and, in turn, determine M up to isomorphism* mod $\mathscr{C}$. *We shall keep the terminology: $\rho =$ cofree rank of M; $\mu = \mu_1 + \mu_2 + \cdots + \mu_s$ the μ-invariant of M.*

Lemma 2.1. *If M is a Γ-cofinite Γ-module,*

(a) *Its invariant ρ is zero if and only if the p-abelian group M is of finite corank. More generally,*

(b) $\operatorname{corank}(M^{\Gamma_n}) = \rho p^n + c$, *for large n, where c is a constant, independent of n.*

(c) *Suppose that M^Γ is a p-divisible group, whose corank is equal to the invariant ρ of M. Then M is cofree of cofree-rank ρ.*

Proof. (a) and (b) follow immediately from the classification theorem quoted above. To see (c) pass to the Pontrjagin dual $\mathbb{Z}_p[[T]]$-module N, and use our hypotheses to find a free $\mathbb{Z}_p[[T]]$-module F on ρ generators and a map $F \to N$ such that,

$$F \oplus_{\mathbb{Z}_p[[T]]} \mathbb{Z}_p \to N \oplus_{\mathbb{Z}_p[[T]]} \mathbb{Z}_p$$

is surjective. An application of Nakayama's lemma gives that $F \to N$ is surjective. If $F \to N$ were not injective, then N could not have a direct summand mod $\mathscr{C}$ whose cofree rank was ρ. Thus $F \to N$ is an isomorphism. Q.E.D.

If M is of finite corank, $\mu(M)=0$ if and only if M is of cofinite type (as an abstract p-abelian group).

Iwasawa defines a *strictly Γ-finite module* M to be one such that M^{Γ_n} is of finite order for all n, [30]. Letting $p^{(e_n)}$ denote its order, one has for sufficiently large n,

$$e_n=\lambda n+\mu p^n+c \qquad ([30], 1.4).$$

To be consistent with our use of the prefix "co-", we shall refer to such a module as a *strictly Γ-cofinite module.*

If γ is a choice of topological generator of Γ, and M is of finite corank, let $\mathrm{char}(t;\gamma,M)$ denote the characteristic polynomial of the operator γ on the associated vector space V of M. We define:

$$f(t;\gamma,M)=p^{\mu(M)}\,\mathrm{char}(t;\gamma,M)$$

and we shall refer to $f(t)=f(t;\gamma,M)$ as the *characteristic polynomial of the Γ-module M*. Set $T=t-1$. Since T is topologically nilpotent, $\mathrm{char}(1+T;\gamma,M)$ is a *distinguished* polynomial in T. That is, it has p-adic integral coefficients, and is congruent to the polynomial $T^\lambda \bmod p$. In the case where M is Γ-cofinite, but has a nonzero cofree rank, the consistent thing to do is to make the convention that $f(t)$ be *identically zero.*

b) Controlled Sequences and Considerations mod $\mathscr{B}$ *and* mod $\mathscr{C}$

Consider the abelian category $\mathscr{A}$ of sequences of abelian groups, $(E_n;\varphi_n)_{n\geq 0}$ where $\varphi_n\colon E_n\to E_{n+1}$ are group homomorphisms. We take morphisms of $\mathscr{A}$ to be compatible systems of homomorphisms. We now consider two full subcategories of $\mathscr{A}$. The category $\mathscr{C}$ is generated by sequences $(E_n;\varphi_n)$ such that the groups E_n are all finite groups whose orders admit an upper bound independent of n. The category $\mathscr{B}$ consists in sequences (E_n,φ_n) such that there is an integer m with the property that $mE_n=0$ for all n. Both $\mathscr{B}$ and $\mathscr{C}$ are thick subcategories of $\mathscr{A}$ (in the sense of [19], 1.11). We introduce the quotient categories $\mathscr{A}/\mathscr{C}$ and $\mathscr{A}/\mathscr{B}$. We shall use the terminology: $\mathscr{B}$-trivial; $\mathscr{B}$-isomorphic; $\mathscr{B}$-exact; etc. to refer to the indicated notions mod $\mathscr{B}$, and similarly mod $\mathscr{C}$. Most of the morphisms we shall consider will be actual morphisms in the category $\mathscr{A}$, and when they are not, we shall signal that fact explicitly.

A *Γ-sequence* will refer to a sequence $(E_n;\varphi_n)$ of $\mathscr{A}$, such that each E_n is endowed with an operation of the group Γ/Γ_n, and the morphisms φ_n are compatible with the induced Γ-actions.

If $(E_n;\varphi_n)$ is a Γ-sequence, form the direct limit, $E=\varinjlim E_n$ which is endowed with the structure of discrete abelian group together with a continuous action of the topological group Γ. We have a new Γ-sequence (E^{Γ_n}) and a morphism of $\mathscr{A}$,

$$E_n\to E^{\Gamma_n}$$

and if the above morphism is a $\mathscr{C}$-isomorphism, we shall say that the Γ-sequence $(E_n; \varphi_n)$ is *controlled.*

c) Γ-Extensions of Fields and of Schemes

By a *local field* we shall mean a finite extension of $\mathbb{Q}_p$ (the p-adic numbers) for some rational prime p. By a *global field* we shall mean a finite extension of $\mathbb{Q}$. Our usage is more restrictive than the usual, in that we have excluded the function fields over finite fields, in the global case, and the power series field over finite fields in the local case.

Fixing the prime p, we shall say that a field extension L/K is a *Γ-extension (associated to p)* if L/K is galois with group Γ ($\approx \mathbb{Z}_p$). For each p there is a unique Γ-extension $\mathbb{Q}_\infty/\mathbb{Q}$ with base field $\mathbb{Q}$, associated to p. This may be described as follows: The extension of $\mathbb{Q}$, $\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}$, obtained by adjoining all p^r-th roots of unity, for all r, has galois group canonically isomorphic to U_p the topological group of p-adic units. In U_p, let Δ denote the torsion subgroup. This group is, for $p \neq 2$, the cyclic group of order $p-1$ consisting of $(p-1)$-st roots of 1. For $p=2$ it is of order 2. Now let $\mathbb{Q}_\infty$ denote the fixed field of Δ in $\mathbb{Q}(\zeta_{p^\infty})$.

If L/K is any Γ-extension and K'/K any finite field extension, then the base change L'/K' is again a Γ-extension. For any number field $K/\mathbb{Q}$ we shall refer to the Γ-extension $K\mathbb{Q}_\infty/K$ obtained by base change as the *cyclotomic Γ-extension over K (associated to p).*

For L/K any Γ-extension let $K_n \subset L$ denote the fixed subfield of $\Gamma_n \subset \Gamma$. We have, then, a tower of fields,

$$K = K_0 \subset K_1 \subset \cdots \subset K_n \subset \cdots \subset L, \qquad L = \bigcup_{n=0}^{\infty} K_n.$$

K_n is a cyclic extension of K of degree p^n. Conversely, any tower of such cyclic extensions K_n/K gives rise to a Γ-extension.

If K is a local or global field, let

$$D = D_0 \subset D_1 \ldots D_n \subset \cdots \subset E$$

denote the rings of integers in the above fields, and

$$X = X_0 \leftarrow X_1 \leftarrow \cdots \leftarrow X_n \leftarrow \cdots \leftarrow Y$$

their associated spectra. We shall refer to Y/X also as a Γ-extension.

Recall from the theory of Γ-extensions [52] that the only primes of X that can possibly ramify in Y are those dividing p, and in the global case at least one such prime must ramify. Let $\Gamma(q)$ denote the inertial subgroup associated to the ramified primes q. Then $\Gamma(q) = \Gamma_{n_q}$ for some integer n_q since the $\Gamma(q)$'s are all nontrivial subgroups in Γ. Set $N = \max(n_q)$ where the q's run through the ramified primes.

Say that a Γ-extension is *special* if any prime q of X is either unramified, or ramifies totally in Y. This is the same as asking that $\Gamma(q)=\Gamma$ for all ramified q. For any Γ-extension, L/K_N is always special, where N is the integer defined above. Thus by the modification of the base $K \to K_N$; $X \to X_N$, we may obtain from any Γ-extension L/K a special Γ-extension. The cyclotomic Γ-extension over any base is special.

d) Bilinear Forms on Γ-Modules

I have tried to eliminate this exceptionally technical section, but I do not see how to obtain the functional equation of § 7 without proving (2.8) below. The technical complication of it arises from the fact that we will be given a $\mathscr{B}$-nondegenerate pairing of the sort defined in (2.6) below, in our applications. This pairing can be dealt with easily if M is Γ-cofinite and $M_n = M^{\Gamma_n}$ has no divisible part (i.e., M is strictly Γ-cofinite, or equivalently: in the mod $\mathscr{C}$ decomposition of the Pontrjagin dual of M into direct sums,

$$\Lambda/(\varphi_1^{e_1}) \oplus \Lambda/(\varphi_2^{e_2}) \oplus \cdots \oplus \Lambda/(\varphi_s^{e_s}),$$

with φ_j irreducible elements of Λ, none of the φ_j's are the irreducible polynomial of a p^r-th root of unity). Indeed the sought-for functional equation ((2.9) below) comes in this case, immediately from ([20], 5.5). It is also unawkward to treat the case where those φ_j which are the irreducible polynomial of a p^r-th root of unity occur all with exponent $e_j = 1$. The possibility of nonsemi-simplicity of the Γ-module M forces us into the complications of the step-wise process below.

We shall now deal with topological $\mathbb{Z}_p$-modules. In this section (and *only* this section) we shall have occasion to work with modules of this sort which are *not necessarily* discrete, or compact. Let * stand for $\mathrm{Hom}_{\mathrm{cont}}(\ ,\mathbb{Q}_p/\mathbb{Z}_p)$. If M is a topological $\mathbb{Z}_p$-module, we say that M is $\mathbb{Q}_p$-finite if $V = \mathbb{Q}_p \otimes_{\mathbb{Z}_p}(M^*)$ (the $\mathbb{Q}_p$-vector space *associated* to M) is finite dimensional. If $M \xrightarrow{\varphi} N$ is a $\mathscr{B}$-isomorphism, (§ 2(b)), φ induces an isomorphism of associated $\mathbb{Q}_p$-vector spaces.

Now suppose we are given a topological $\mathbb{Z}_p$-module M together with a continuous Γ-action. We call such things topological Γ-*modules*, and we try to keep to the terminology of [29]. If M is a $\mathbb{Q}_p$-finite topological Γ-module, let $\chi(M)$ denote the set of characteristic roots of M, counting multiplicities (as in [29]). Denote by $\underline{\chi}(M)$ the subset of $\chi(M)$ obtained by deleting all p^m-th roots of 1, for all m. A Γ-action will be called *idempotent* if it factors through Γ/Γ_n for some n. If $A \to B$ is a morphism of $\mathbb{Q}_p$-finite topological Γ-modules, such that the image of A is closed in B, we shall write $A \approx B$ if both kernel and cokernel have idempotent Γ-actions. Denote by the same symbol the equivalence relation generated. One has immediately: $A \approx B$ implies $\underline{\chi}(A) = \underline{\chi}(B)$.

Let M be a (discrete) Γ-module, supposed $\mathbb{Q}_p$-finite and Γ-cofinite, in what follows.

Set $M_n = M^{\Gamma_n}$, $D_n = \bigcap_k p^k M_n$. Thus D_n is the maximal divisible subgroup of M_n. Since M is Γ-cofinite M_n/D_n is finite. Let $D = \bigcup D_n \subset M$.

Since M is $\mathbb{Q}_p$-finite, one sees that the divisible groups D_n must have bounded corank, which implies that the sequence is stationary, e.g., $D=D_n$ for $n\gg 0$. Consequently, D is an idempotent Γ-module. If we form the exact sequence,

$$0\to D\to M\to M'\to 0, \tag{2.2}$$

$M\approx M'$, and $M=M'$ if and only if M is strictly Γ-cofinite. By the additive formula for λ, M is not strictly Γ-cofinite, if and only if: $\lambda(M')<\lambda(M)$. Consequently if we define $M(0)=M$ and $M(j+1)=M(j)'$, we find that there must be an integer j such that the Γ-module $\tilde{M}=M(j)$ is strictly Γ-cofinite. We have $M\approx\tilde{M}$.

If M is a Γ-cofinite Γ-module, define $M^t=\varinjlim_n M_n^*$, where the sequence is defined by means of the trace maps $v_{n,m}^*$ ([29], § 1):

$$M_{n+1}\xrightarrow{\quad v_{n+1,n}\quad} M_n.$$

The above definition is exactly the definition of the adjoint given in [29], with the exception that we do not require M to be strictly Γ-cofinite. Thus M^t is a topological Γ-module, not necessarily discrete. We do have, however, that M^t is $\mathbb{Q}_p$-finite, since it satisfies the conditions of the following lemma:

Lemma 2.3. *Let W be a $\mathbb{Z}_p$-module which is the union of submodules,*

$$W_n\subset W_{n+1}\subset\cdots\subset W,\qquad n\geqq 0. \tag{2.4}$$

Suppose there are integers μ, and k such that for all n $p^\mu\cdot W_n$ can be generated over $\mathbb{Z}_p$ by no more than k elements.

Then W is $\mathbb{Q}_p$-finite.

Proof. By multiplying everything by p^μ, we can suppose $\mu=0$. We can also, by a sequence of pushouts suppose that the W_n's are all free $\mathbb{Z}_p$-modules. By ignoring a finite number of n's, we can suppose them all of the same rank k. Then the whole sequence (2.4) can be imbedded in $\mathbb{Q}_p^k$. Consequently, $M\subset\mathbb{Q}_p^k$ and since $\mathbb{Q}_p$ is self-dual, M^* is a quotient of $\mathbb{Q}_p^k$, which proves (2.3).

We must now compare M^t with M'^t. Applying $H^i(\Gamma_n,\ )$ to the exact sequence (2.2), one gets

$$0\to D_n\to M_n\to M_n'\to H^1(\Gamma_n, D)$$

and passing to the limit,

$$H^t\to M'^t\to M^t\to D^t\to 0$$

where $H^t=\varinjlim_n H^1(\Gamma_n, D)^*$.

Since both H^t and D^t are idempotent, we have: $M''^t \approx M^t$, from which we deduce that $\tilde{M}^t \approx M^t$. By ([29], 5.5), since $\tilde{M}$ is strictly Γ-cofinite, we have that $\chi(\tilde{M}) = \chi(\tilde{M}^t)$, yielding:

Lemma 2.5. $\underline{\chi}(M) = \underline{\chi}(M^t)$.

Consider the torsion submodule of M^t which we denote M^t_{tors}. We have:

$$M^t_{\text{tors}} = \varinjlim_n (M_n/D_n)^*$$

and consequently, the exact sequence,

$$0 \to M^t_{\text{tors}} \to M^t \to D^t \to 0,$$

which gives us that $M^t_{\text{tors}} \approx M^t$.

Let M and N be Γ-cofinite (discrete) Γ-modules.

(2.6) A *$\mathscr{B}$-bilinear pairing* will mean a $\mathscr{B}$-morphism of sequences,

$$M_n/\mathrm{div}(M_n) \times N_n/\mathrm{div}(N_n) \to \mathbb{Q}/\mathbb{Z}$$
$$(x, y) \to \langle x, y \rangle$$

satisfying the compatibility relations,

(i) $\langle i_{n,m} x, y \rangle = \langle x, \nu_{n,m} y \rangle$ for $x \in M_n$, $y \in N_m$

(ii) $\langle \alpha x, \alpha y \rangle = \langle x, y \rangle$ for $\alpha \in \Gamma$.

In the above, if W is a group, $\mathrm{div}(W)$ refers to the maximal divisible subgroup of W. We sometimes write W/div for $W/\mathrm{div}(W)$.

This is not a symmetric definition in M and N. We will say that the pairing is *$\mathscr{B}$-nondegenerate* if the left and right kernels are finite groups for all n, killed by multiplication by a number m independent of n. We may re-interpret a $\mathscr{B}$-bilinear pairing in terms of $\mathscr{B}$-morphisms of Γ-modules, after a definition. If M is a Γ-module, let $M^{(-)}$ denote the new Γ-module obtained by taking the same underlying topological abelian group M and redefining the operation of Γ by letting $\alpha \in \Gamma$ operate on $M^{(-)}$ as α^{-1} operating on M. Clearly $\chi(M^{(-)}) = \chi(M)^{-1}$. In other words, the involution $u \to u^{-1}$ sends the characteristic roots (counting multiplicities) of M to the characteristic roots of $M^{(-)}$. It is immediate that a $\mathscr{B}$-bilinear pairing between M and N gives us a $\mathscr{B}$-morphism of Γ-modules,

$$M^{(-)\prime} \dashrightarrow N^t_{\text{tors}}.$$

If the bilinear pairing is $\mathscr{B}$-nondegenerate, the above map is a $\mathscr{B}$-isomorphism.

Corollary 2.7. *Let there be a $\mathscr{B}$-nondegenerate bilinear pairing between the Γ-cofinite, $\mathbb{Q}_p$-finite (discrete) Γ-modules, M and N. Then*

$$\chi(M)^{-1}=\chi(N).$$

Corollary 2.8. *Suppose there is a $\mathscr{B}$-nondegenerate bilinear form (i.e., a bilinear self-pairing) on the Γ-cofinite, $\mathbb{Q}_p$-finite discrete Γ-module M. Then*

$$\chi(M)=\chi(M)^{-1}.$$

Proof. If a p^m-th root of unity, ζ, occurs in $\chi(M)$, all algebraic conjugates of ζ over $\mathbb{Q}_p$ occur as well, and to the same multiplicity. But ζ^{-1} is in the conjugacy class. Thus we are reduced to showing $\chi(M)=\chi(M)^{-1}$ which follows from the previous lemma.

It follows, in the above situation, that one has the functional equation for the characteristic polynomial of M with respect to a topological generator $\gamma\in\Gamma$:

$$f_M(t)=\varepsilon\, t^{\lambda} f_M(1/t) \tag{2.9}$$

where $\lambda=\lambda(M)$, and $\varepsilon=(-1)^r$, where r is the multiplicity of the eigenvalue 1.

§ 3. Néron Models and Their Kummer Theory

Let K be a local or global field, D its ring of integers $X=\mathrm{Spec}(D)$ and $j\colon \mathrm{Spec}(K)\to X$ the inclusion. If $A_{/K}$ is an abelian variety defined over K, denote by A the Néron model [47] of $A_{/K}$. Thus A is a smooth commutative group scheme over X such that its generic fibre is isomorphic to $A_{/K}$ and A satisfies the "functorial property":

If S is any smooth scheme over X, the restriction map:

$$\hom_X(S, A)\to \hom_K(S_{/K}, A_{/K})$$

is bijective.

Equivalently, we may say that $A=j_*(A_{/K})$ as sheaves for the smooth topology. (To use the language of Néron [47], A is "faiblement $\mathscr{P}$-simple, $\mathscr{P}$-minimal" for all $\mathscr{P}$ of X. The existence of such Néron models over local and global fields is given by Theorems 2, and 4 respectively of Chapter II of [47].)

We shall refer to A as a *Néron model* over X. Thus, a *Néron model* A is a smooth commutative group scheme over X whose generic fibre is an abelian variety and which satisfies the formula: $A\cong j_* j^* A$, when regarded as a sheaf for the smooth topology.

Given a Néron model A there is a natural open subgroup scheme of A to consider:

For each closed point x of X, the fibre A_x is a smooth commutative group scheme over $k(x)$. Denote by $A_x^0 \subset A_x$ its connected component and $Z_x \subset A_x$ its complement. Since A has nondegenerate reduction for almost all primes, Z_x is nonempty for only a finite number of points x. Thus $Z = \bigcup Z_x$ is a closed subscheme of A. Denote by $A^0 \subset A$ its open complement. It is easily seen that A^0 is stable under the group law, and thus is an open subgroup scheme of A.

It is sometimes easy to find A^0 for elliptic curves, when to avoid a minor elaboration, we suppose them defined over D, a principal ideal domain. The procedure is as follows: we may try to express our elliptic curve over K by an equation of the form,

$$y^2 + a_1 x y + a_3 y + x^3 + a_2 x^2 + a_4 x + a_6 = 0$$

with $a_j \in D$ (a *Weierstrass-model* for the elliptic curve), where the zero-section of its group structure is the point at infinity. One then seeks such a Weierstrass model for which $\mathrm{ord}_{\mathfrak{P}}(\Delta)$ is a minimum for all primes $\mathfrak{P}$ of D. Such an equation exists and is called a *global minimal Weierstrass model.* Upon removal of the singular points of the scheme over D defined by a global minimal Weierstrass model, we obtain a quasi-projective scheme, smooth over D, which admits a unique group structure extending the group law on the fibre over K. There is a canonical isomorphism of this smooth group scheme over D with A^0. Having discovered A^0, one may go on to study A by means of the complete table of possibilities given on p. 123 of [47].

Remark. The subgroup scheme A^0 plays a crucial role in the duality theory for A. See [1].

Let F denote the quotient of A by A^0 regarded as sheaves for the $fpqf$ topology:

$$0 \to A^0 \to A \to F \to 0. \tag{3.1}$$

We have that F is a "skyscraper sheaf". It is zero outside of the finite set of $x \in X$ such that A_x is disconnected. Since A and A^0 are smooth group schemes, the cohomology of the above sequence remains the same if computed for the $fpqf$, smooth, or étale topologies. (GB III [App. 11.1].) Let us describe F completely, as a sheaf for the étale topology. We have:

$$F = \bigoplus_x i_{x*}(F_x)$$

where the direct sum is taken over all x, or equivalently: that finite set of x such that A_x is disconnected. F_x is the finite galois module over $k(x)$ given by A_x/A_x^0. Of course, if the F_x all have trivial Galois action, then the $fpqf$ sheaf F is even representable as a group prescheme.

In any case, its cohomology for any of the three sites listed above is given by:

$$H^q(X,F)=\bigoplus_x H^q(k(x),A_x/A_x^0).$$

Suppose K is a global field. There is a close relation between the Shafarevitch-Tate group $Ш=Ш(K,A)$, (see [67, 68] or the Appendix below for a definition), and $\Sigma=\mathrm{im}\{H^1(X,A^0)\to H^1(X,A)\}$.

The proposition of the Appendix tells us that one has:

$$\begin{array}{ccccccccc} & & H^0(X,F) & \longrightarrow & H^0(X,A^0) & \longrightarrow & H^0(X,A) & \longrightarrow & H^1(X,F) \\ & & & & \searrow & & \nearrow & & \\ (3.2) & 0 & \longrightarrow & Ш & \longrightarrow & \Sigma & \longrightarrow & \Sigma/Ш & \longrightarrow 0 \\ & & & & \swarrow & & \searrow & & \\ & & & 0 & & & 0 & & \end{array}$$

where $\Sigma/Ш$ is a finite group of exponent two, dependent only upon the structure of the group of connected components of $A(K_v)$ where v ranges through all real archimedean primes of K. Thus, the p-primary components of Σ and $Ш$ are equal for odd primes p.

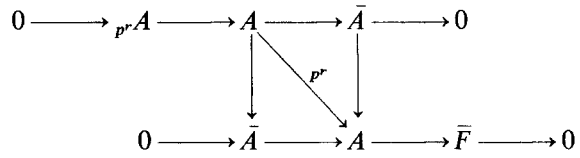
We now consider the map $A\xrightarrow{m}A$ given by multiplication by the integer m. *Suppose that* $A_x^0\xrightarrow{m}A_x^0$ *is an isogeny for all* x. This boils down to the requirement that multiplication by m is an isogeny for all x such that the characteristic of $k(x)$ divides m. Equivalently: $m\colon A^0\to A^0$ is a surjection of $fpqf$ sheaves. Then the kernel of multiplication by m in A, ${}_mA\subset A$, is a flat, quasi-finite, group scheme.

Consider the image, and cokernel, as sheaves for the $fpqf$ topology, pictured below:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & {}_mA & \xrightarrow{m} & A & \longrightarrow & F/m & \longrightarrow & 0 \\ & & & \searrow & \uparrow & \nearrow & & & \\ & & & & {}^mA & & & & \\ & & & \swarrow & & \searrow & & & \\ & & 0 & & & & 0. & & \end{array}$$

Now suppose $m=p^r$. Fixing p, $F/_{p^r}$ and consequently ${}^{p^r}A$ both stabilize for large enough r. Denote those stable sheaves $\bar{F}$ and $\bar{A}$ respectively. We have:

(3.3)



for all $r \geqq r_0$. Let $\tilde{A}$ stand for the inductive limit of the system of quasi-finite group schemes:

$$\to {}_{p^r}A \to {}_{p^{r+1}}A \to \cdots.$$

Regard $\tilde{A}$ as a sheaf for the $fpqf$ topology. It is representable as an ind-quasi-finite group scheme! We have that

$$H^q(X, \tilde{A}) = \varinjlim_r H^q(X, {}_{p^r}A).$$

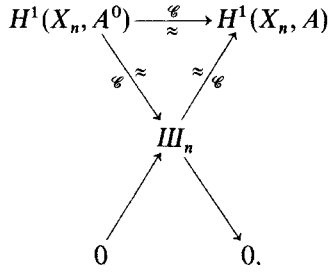
We shall signal all cohomological computations using the exact sequences (3.3) by the catch-phrase: "the Kummer theory for A". One should note that the groupschemes ${}_{p^r}A$ are not necessarily smooth and therefore cohomology with those group schemes as coefficients means $fpqf$ cohomology unless stated otherwise explicitly.

Although we do not use it in this paper, the following remark has relevance to the discussion in §1(d): Let p be a prime such that A_x has good reduction for all $x \in X$ of characteristic p. Then the ind-quasi-finite group scheme A depends only upon the $\mathrm{Gal}(\bar{K}/K)$-module, ${}_{p^\infty}A$. This makes use of the deep theorem of Tate [69] that a p-divisible group over a local field of characteristic zero and residual characteristic p is determined by its Galois module, together with the fact that away from characteristic p, $\tilde{A}$ is étale, and determined by the Néron property: $\tilde{A} = j_* j^* \tilde{A}$.

Now fix a Γ-extension Y/X associated to the prime p. *Suppose that the fibres A_x of the Néron model A are abelian schemes* ("A has non-degenerate reduction") *for all x such that the characteristic of $k(x)$ is p.* Since X_n/X is unramified except at points x for which A has "non-degenerate reduction" it follows that $A \times_X X_n$ is a Néron model over X_n. The base change of both the exact sequence (3.1) and the Kummer theory (3.3) of A, to X_n, give the analogous exact sequence (3.1) and the Kummer theory (3.3) of $A \times_X X_n$. Similarly, the base change of $\tilde{A}$ to X_n yields $\widetilde{A \times_X X_n}$. When it is convenient to denote $A \times_X X_n$ and $\widetilde{A \times_X X_n}$ by the symbols A, and $\tilde{A}$ again, and unlikely to cause confusion, we will do so. (We shall do this principally when these occur as coefficients in cohomology groups.)

Let X be global. Make the further hypothesis that *any* $x \in \mathrm{Supp}(F)$ *splits finitely in the Γ-extension Y/X.* This is automatically satisfied for the cyclotomic Γ-extension.

Then $H^q(X_n, F)$ and $H^q(X_n, \bar{F})$ are $\mathscr{C}$-trivial. Letting $Ш_n$ denote the Shafarevitch-Tate group of A over X_n, we obtain the following consequence from (3.2): The morphisms below are $\mathscr{C}$-isomorphisms.



Consequently either of the groups $H^1(X_n, A^0)$, $H^1(X_n, A)$ represent, up to a bounded amount of error, the Shafarevitch-Tate groups $Ш_n$.

§ 4. The Local Norm Mapping for Commutative Group Schemes

a) Here Is the General Problem

Let L/K be a finite extension of local fields. Let A be a commutative group scheme over K. Determine the cokernel of the norm mapping,

$$A(L) \xrightarrow{N_{L/K}} A(K). \tag{4.1}$$

A full answer is given by local class field theory, when A is the multiplicative group, $\mathbb{G}_m$. It would be very interesting to give a theory of similar precision for the general commutative group scheme A. We do the barest minimum in this direction, by providing a theory when A is an abelian variety with nondegenerate reduction and invertible Hasse matrix [25, 26]. To begin, let us note:

Proposition 4.2. *If L/K is galois, and A is an abelian variety, then Tate local duality* [67], *induces an isomorphism of $H^1(\mathrm{Gal}(L/K), A'(L))$ with the Pontrjagin dual of $A(K)/N_{L/K}A(L)$.*

Here A' denotes the dual abelian variety to A over K.

Proof. This comes from the commutative diagram,

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^1(\mathrm{Gal}(L/K), A'(L)) & \longrightarrow & H^1(K, A') & \longrightarrow & H^1(L, A') \\ & & \downarrow & & \downarrow \approx & & \downarrow \approx \\ 0 & \longrightarrow & (A(K)/N_{L/K}A(L))^* & \longrightarrow & A(K)^* & \xrightarrow{(N_{L/K})^*} & A(L)^* \end{array}$$

where * denotes Pontrjagin duality, and the right hand two vertical maps are the Tate local duality isomorphisms [67].

We next show that it is not too hard to analyze (4.1) when L/K is unramified, and A is an abelian variety over K.

Proposition 4.3. *Let A be a Néron model over* $\mathrm{Spec}(D)$, *where D is the ring of integers in K. Let L/K be unramified, with residue extension l/k. Let F be the finite étale group scheme A_k/A_k^0 over k. Then the natural map,*

$$H^1(\mathrm{Gal}(L/K), A(L)) \to H^1(\mathrm{Gal}(l/k), F)$$

is an isomorphism.

Proof. Let $G = \mathrm{Gal}(L/K) = \mathrm{Gal}(l/k)$. Let E denote the ring of integers in L, with $\mathfrak{n} \subset E$ its maximal ideal. We shall show that each of the natural maps below are isomorphisms, from which our proposition follows

(a) $$H^1(G, A(L)) \to H^1(G, A(l))$$

(b) $$H^1(G, A(l)) \to H^1(G, F).$$

We first give, briefly, the argument for (a). Consider the exact sequence of G-modules,

$$0 \longrightarrow D_r \longrightarrow A(E/\mathfrak{n}^r + 1) \xrightarrow{\pi_r} A(E/\mathfrak{n}^r) \longrightarrow 0.$$

The map π_r is surjective because A is smooth. Its kernel D_r is a finite dimensional vector space over l, on which G acts semi-linearly relative to the canonical action of G on l. Thus D_r is G-cohomologically trivial, and consequently we obtain that

$$H^1(G, A(E/\mathfrak{n}^r)) \to H^1(G, A(l))$$

is an isomorphism for all r, by induction. Now since $A(L) = A(E)$ we conclude (a) by a standard limit argument (CL, XIII, § 3, Lemma 3).

To see (b), merely write

$$0 \to A_k^0 \to A_k \to F \to 0$$

and note that A_k^0 is a connected commutative algebraic group over a finite field, hence cohomologically trivial by Lang's theorem [35]. Q.E.D.

We also have as in [18, 47], ([17], II, § 3):

Corollary 4.4. *If A is an abelian variety with nondegenerate reduction over K, and L/K is unramified, then $N_{L/K}$ of* (4.1) *is surjective.*

Proof. Then its dual A' has good reduction. Consequently $F' = A'_k/(A'_k)^0$ is trivial. Thus by (4.3) $H^1(\mathrm{Gal}(L/K), A'(L))$ is trivial. We then have surjectivity of $N_{L/K}$ by (4.2).

Now concentrate on the case where L/K is totally ramified. Thus $l = k$.

Let A be a commutative group scheme over $\mathrm{Spec}(D)$. In this section we shall let $\hat{A}$ denote its formal completion along its zero section

(SGAD, fasc. 2(b)). We have the exact sequence,

$$0 \to \hat{A}(D) \to A(D) \to A(k) \tag{4.5}$$

where the last arrow is surjective if A is smooth.

Corollary 4.6. *Let A be a Néron model over* Spec(D), *L/K totally ramified of degree d. We have the exact sequence,*

$$\hat{A}(D)/N_{L/K}\,\hat{A}(E) \to A(K)/N_{L/K}\,A(L) \to A(k)/A(k)^d \to 0.$$

The effect of the above corollary is that it allows us to concentrate on the study of the cokernel of the norm mapping for formal Lie group schemes $\Lambda = \hat{A}$ over D.

b) The Theory of Pro-Algebraic Groups

We prepare to apply the general theory of pro-algebraic groups (Serre [55, 56, 57]; Greenberg [17]) to our problem. We shall deal with actual group schemes [49] rather than quasi-algebraic groups [57], so we redo some of the definitions.

In this paragraph we suppose K an arbitrary complete characteristic zero discrete valued field, with ring of integers D, and residue field $D/m = k$ perfect, of characteristic p. We have that $W(k)$ (the Witt ring of k) imbeds naturally in D, making D a free $W(k)$-module of rank e, where e is the absolute ramification index of D (CL, II, § 5, Th. 4).

Denote by $\mathbb{W}_n(\ )$ the functor associating to any ring R/k the ring of Witt vectors of length n with coefficients in R. We have the natural morphisms of functors (CL, II), ([44], App.)

$$\mathbb{W}(\ ) \to \mathbb{W}_n(\ ) \to \text{Ident}.$$

From the construction of $\mathbb{W}_n$ it is clear that $\mathbb{W}_n$ is represented by a ring scheme ([44], App.) whose underlying scheme is affine n-space.

Let M be a module of finite length over $\mathbb{W}(k)$. Consider the functor T: Rings/$k \dashrightarrow$ sets defined by $T(R) = M \otimes_{W(k)} W(R)$. This functor is not necessarily (covariantly) representable by a ring over k. We shall show that there is a universal representable quotient of T. That is, there is a morphism of functors $T \xrightarrow{u} \mathbb{M}$ where $\mathbb{M}$ is covariantly representable, and such that u is universal with respect to morphisms of functors $T \to Q$ with Q representable. In fact, if we write $M \approx \bigoplus_j \mathbb{W}_{n_j}(k)$, we may take $\mathbb{M}$ to be $\oplus \mathbb{W}_{n_j}$ and u to be the natural morphism. It suffices to show this for $M = \mathbb{W}_n(k)$.

What has to be shown is that for any $T \xrightarrow{v} Q$ and all R, as above, the induced map $W(R) \to T(R) \to Q(R)$ depends only upon the first n entries of the Witt vectors in $\mathbb{W}(R)$. Find a polynomial ring $k[X] \to R$ mapping surjectively to R, over k. Find an algebraically closed field Ω

containing $k[X]$. One then has the diagram,

$$\begin{array}{ccc} W(R) & \longrightarrow & Q(R) \\ \uparrow\uparrow & & \uparrow \\ W(k[X]) & \longrightarrow & Q(k[X]) \\ \subseteq \downarrow & & \subseteq \downarrow \\ W(\Omega) & \longrightarrow & Q(\Omega) \end{array}$$

with the designated surjections and injections coming from the nature of W, on the one hand, and representability of Q on the other. Since Ω is algebraically closed (hence a perfect ring, in the terminology of ([CL], Ch. II, § 6)), the morphism,

$$W(\Omega) \to T(\Omega) = W(\Omega)/p^n W(\Omega) = \mathbb{W}_n(\Omega) \to Q(\Omega)$$

clearly does depend only upon the first n entries of the Witt vectors in $\mathbb{W}(\Omega)$. In the light of the above inclusions and surjections, we have the same for $W(R) \to Q(R)$. I am thankful to R. Rasala for conveying to me this intrinsic description of the functor $\mathbb{M}$. (Cf. the structure of a "module-variety" imposed on M in [17].)

Lemma 4.7. *Let $M_1 \times M_2 \times \cdots \times M_r \xrightarrow{\varphi} M$ be a $W(k)$-multilinear map of $W(k)$-modules. Then there is a unique $\mathbb{W}$-multilinear morphism of the functors,*

$$\mathbb{M}_1 \times \mathbb{M}_2 \times \cdots \times \mathbb{M}_r \xrightarrow{\Phi} \mathbb{M}$$

such that $\Phi(k) = \varphi$.

Proof. The $W(k)$-multilinear map φ induced a $\mathbb{W}$-multilinear morphism of functors,

$$T_1 \times T_2 \times \cdots \times T_r \xrightarrow{\varphi} T$$

where $T_j(R) = M_j \otimes_{W(k)} W(R)$, and $T(R) = M \otimes_{W(k)} W(R)$. This factors uniquely through the universal representable quotients, giving Φ above, and uniquely characterizing Φ as well. (Compare [55], § 1, Lemma 1.)

Definition. *Let*

$$\underbrace{M \times M \times \cdots \times M}_{(\delta \text{ times})} \xrightarrow{\varphi_\delta} N$$

be a $W(k)$-multilinear map of $W(k)$-modules. We then say that the composite morphism of functors,

$$\mathbb{M} \xrightarrow{\iota} \underbrace{\mathbb{M} \times \mathbb{M} \times \cdots \times \mathbb{M}}_{(\delta \text{ times})} \xrightarrow{\Phi} \mathbb{N}$$

is algebraic homogeneous (of degree δ).

Let $M \xrightarrow{\varphi} N$ be an arbitrary set-theoretic map between two $W(k)$-modules. An *algebraic expression* for φ is an expression of the form,

$$\varphi = \sum_{\delta=0}^{n} \varphi_\delta \cdot \iota \tag{4.8}$$

where φ_δ are as above.

Such an algebraic expression determines uniquely a morphism of functors,

$$\mathbb{M} \xrightarrow{\Phi} \mathbb{N}$$

such that $\Phi(k)=\varphi$; $\Phi=\sum_0^n \Phi_\delta$.

Note. There may be more than one algebraic expression for φ.

Now let $V=Spf(D[[T_1, \ldots, T_s]])$ regarded as a formal scheme over D with a chosen section: $T_j \mapsto 0$ (for all j). V is then a functor from formal schemes over D to the category of pointed sets. Define the functors,

$$V_n\colon \text{Rings}/k \dashrightarrow \text{Sets} \qquad n \geqq 0 \tag{4.9}$$

by the prescription,

$$V_n(R)=\ker\{V(D/p^n \otimes_{W_n(k)} W_n(R)) \to V(R)\}$$

where the arrow above is induced by the natural map,

$$D/p^n \otimes_{W_n(k)} W_n(R) \to k \otimes_{W_n(k)} R \cong R.$$

We have a natural identification of the set $V_n(R)$ with the s-fold product $J_n(R)^s$, where $J_n(R)$ is the ideal,

$$0 \to J_n(R) \to D/p^n \otimes_{W_n(k)} W_n(R) \to R.$$

If we let π be a uniformizer of D, we may write

$$D/p^n = \bigoplus_0^{n-1} \pi^j W_n(k)$$

which is a direct sum decomposition as a $W_n(k)$-module, and which gives rise to the following decomposition of the $W(R)$-module, $J_n(R)$:

$$J_n(R)=\pi^0 W_{n-1}(R) \oplus \left\{ \bigoplus_{j=1}^{e-1} \pi^j W_n(R) \right\}$$

where we have imbedded $W_{n-1}(R)$ in $W_n(R)$ by means of the ("décalage") operator V: $W_{n-1}(R) \to W_n(R)$ (CL, p. 52). From this description it is clear that $J_n(\,)$ is isomorphic to the canonical functor $\mathbb{M}$ associated to the $\mathbb{W}(k)$-module $M=J_n(k)$. Thus

Lemma 4.10. *The functor $V_n(\ )$ is isomorphic to the canonical functor V_n associated to the $W(k)$-module $V_n(k)$. It is isomorphic to an abelian group scheme whose underlying space is affine space of dimension $s(e\,n-1)$.*

Remarks. 1) Although we started out with a set-valued functor, we have imposed canonically an abelian group structure on it. We may refer to this abelian group structure as the elementary group structure on V_n.

2) (Pro-objects). We refer to [49] for the category of pro-algebraic groups over k. For a general treatment of pro-objects, see [21] or [4]. Let $\mathscr{P}$ denote the category of pro-(*schemes of finite type over k*).

The system $(\mathbf{V}_n)_n$ described above represents an object $\mathbf{V}$ in the category $\mathscr{P}$.

Now suppose we have a formal Lie group scheme Λ over D (SGAD, fasc. 2b).

By a *coordinatization* of Λ we shall mean an isomorphism of the formal schemes $\Lambda \approx V = Spf(D[[T_1, \ldots, T_s]])$ compatible with chosen sections. Given a coordinatized formal Lie group scheme Λ we may express multiplication and inversion by morphisms,

$$\begin{array}{c} V \hat{\times} V \xrightarrow{\mu} V \\ V \xrightarrow{i} V \end{array} \tag{4.11}$$

and these may be expressed in the usual way as formal power series with coefficients in D. Here we have used $\hat{\times}$ to denote product in our category: $V \hat{\times} V$ is the formal spectrum of the completed tensor product of $D[[T_i]]$ with itself over D,

$$V \hat{\times} V \approx Spf(D[[1 \otimes T_i, T_j \otimes 1]]).$$

Define the functors Λ_n: Rings/$k \dashrightarrow$ Groups by the formula,

$$\Lambda_n(R) = \ker\{\Lambda(D/p^n \otimes_{W_n(k)} W_n(R)) \to \Lambda(R)\}.$$

Proposition 4.12. *The functors Λ_n are representable by group schemes of finite type over k (commutative if the formal group Λ is). The system,*

$$\Lambda\colon \cdots \to \Lambda_n \to \Lambda_{n-1} \to \cdots$$

represents an object in the category of pro-algebraic group schemes over k.

Proof. Given an explicit isomorphism $\Lambda \approx V$, we get isomorphisms $\Lambda_n \approx V_n$ for all n, and our proposition follows from (4.10). Being given such an isomorphism, one has two group structures on V_n, its elementary group structure, and the one induced by transport of structure from Λ_n, which may, of course, be different.

If M and N are free $W(k)$-modules of finite rank, and $f\colon M \to N$ a map of sets, we shall say that f is a *power series map* if f can be expressed as a power series with coefficients in $W(k)$, convergent (and equal to f) on all of M. Note that such a power series representation in terms of $W(k)$-bases for M and N is unique (LG, 2.4). Consequently, from a power series map f one obtains, canonically, $W(k)$-multilinear maps,

$$M \times M \times \cdots \times M \xrightarrow[(j \text{ times})]{} N \xrightarrow{\varphi_j} N$$

such that $f = \sum_j \varphi_j \cdot \iota$. Such multilinear morphisms induce morphisms

$$M/p^r \times M/p^r \times \cdots \times M/p^r \xrightarrow{\varphi_j} N/p^r$$

and convergence of f implies that for each r there is a $j(r)$ such that for $j \geqq j(r)$, the above morphism is zero.

Now let K, K' be fields of the sort we are considering, with rings of integers D, D', and both with residue field k. Let

$$V = Spf(D[[T_1, \ldots, T_s]]) \quad \text{and} \quad V' = Spf(D'[[T_1', \ldots, T_{s'}']]).$$

We have that

$$V(D) = \varprojlim_n V_n(k)$$

$$V'(D') = \varprojlim_n V_n'(k)$$

as $W(k)$-modules. Also, the above isomorphisms induced canonical surjections,

$$V_{n+1}(k) \to V(D)/p^n \to V_n(k)$$

$$V_{n+1}'(k) \to V'(D')/p^n \to V_n'(k).$$

Let $f\colon V'(D') \to V(D)$ be a power series map. If we write $f = \sum_0^\infty \varphi_j \circ \iota$, then the multilinear morphisms φ_j induce $W(k)$-multilinear morphisms,

$$V_{n+1}'(k) \times V_{n+1}'(k) \times \cdots \times V_{n+1}'(k) \xrightarrow{\varphi_j} V_n(k) \tag{4.13}$$

for each n, such that (4.13) is zero for $j \geqq j(n)$.

It follows from (4.7) and (4.13) that we may obtain a unique morphism of functors,

$$f_n\colon \mathbf{V}_{n+1}' \to \mathbf{V}_n$$

for each n, whose algebraic expression (4.8) is given by $\sum_0^{j(n)} \varphi_j \cdot \iota$. These morphisms are compatible with projections and therefore induce a morphism of pro-objects,

$$\mathbf{f}\colon \mathbf{V}' \to \mathbf{V}.$$

Examples. 1) If $D' \subset D$, $K' \subset K$, V the base change of V' to D and $i\colon V(D') \to V(D)$ is the natural inclusion. In this case i is actually $W(k)$-

linear, and imbeds $V(D')$ as $W(k)$-direct summand in $V(D)$. The associated morphism on pro-objects,

$$\mathbf{i}\colon \mathbf{V}' \to \mathbf{V}$$

is a monomorphism for the category $\mathscr{P}$.

2) Consider a formal group law (4.11) coming from a coordinatized formal Lie group over D. Then

$$V \hat{\times} V(D) \xrightarrow[\mu]{} V(D)$$

is a power series map, and hence gives rise by our process to a morphism $\boldsymbol{\mu}$ of pro-objects, making the following diagram commutative

$$\begin{array}{ccc} \mathbf{V}\times\mathbf{V}\approx\mathbf{V}\hat{\times}\mathbf{V} & \xrightarrow[\mu]{} & \mathbf{V} \\ \downarrow\approx & & \downarrow\approx \\ \boldsymbol{\Lambda}\times\boldsymbol{\Lambda} & \xrightarrow[\text{mult.}]{} & \boldsymbol{\Lambda} \end{array}$$

where the vertical maps come from our coordinatization. We have a similar diagram with inversion.

3) (The norm mapping). Let L/K be totally ramified, Galois with finite Galois group G. Let Λ be a commutative formal Lie group scheme over D. Let Λ' denote the base change of Λ to E, the ring of integers in L. The group G operates on Λ', on Λ'_n for each n, and on Λ. We seek a homomorphism of pro-algebraic groups $\mathbf{N}_{L/K}$ making the diagram,

$$\begin{array}{ccc} \boldsymbol{\Lambda}' & \xrightarrow[\tau]{} & \boldsymbol{\Lambda}'\times\boldsymbol{\Lambda}'\times\cdots\times\boldsymbol{\Lambda}' \quad (\#G \text{ factors}) \\ \downarrow{\scriptstyle \mathbf{N}_{L/K}} & & \downarrow{\scriptstyle \text{mult.}} \\ \boldsymbol{\Lambda} & \xrightarrow[\mathbf{i}]{} & \boldsymbol{\Lambda}' \end{array} \tag{4.14}$$

commutative. Since $\mathbf{i}$ is a categorical monomorphism, if such a homomorphism exists it must be unique. The map τ is the composite of the diagonal with the automorphism of $\Lambda'\times\Lambda'\times\cdots\times\Lambda'$ which consists in conjugation by g on the g-th factor for all g in G.

To see that $\mathbf{N}_{L/K}$ exists, first note that the fixed subgroup of $\Lambda'(E)$ under the action of G may be identified with $\Lambda(D)$ via the inclusion i. Consequently we have the commutative diagram,

$$\begin{array}{ccc} \Lambda'(E) & \xrightarrow[\tau]{} & \Lambda'(E)\times\Lambda'(E)\times\cdots\times\Lambda'(E) \\ \downarrow{\scriptstyle N_{L/K}} & & \downarrow{\scriptstyle \text{mult.}} \\ \Lambda(D) & \xrightarrow[i]{} & \Lambda'(E). \end{array} \tag{4.15}$$

If we choose a coordinatization $\Lambda \approx V$ and its base change to E, $\Lambda' \approx V'$, (4.15) may be written,

$$\begin{array}{ccc} V'(E) & \xrightarrow{\tau} & V'(E) \times V'(E) \times \cdots \times V'(E) \\ \Big\downarrow{\scriptstyle N_{L/K}} & & \Big\downarrow{\scriptstyle \mu} \\ V(D) & \xrightarrow[i]{} & V'(E). \end{array} \tag{4.16}$$

The map τ is $W(k)$-linear, and μ is a power series map. Therefore $\mu\tau$ is a power series map. Since i is a $W(k)$-linear identification of $V(D)$ with a $W(k)$-direct summand in $V'(E)$, we see that $N_{L/K}$ of (4.16) is a power series map. If we pass from the diagram (4.16) of power series maps to the category of pro-algebraic groups and then pass from V, V' to Λ, Λ' by means of our coordinatization, we obtain the sought- for diagram (4.14).

From (4.14) one immediately has the well known formulae:

(i) $\mathbf{N}_{L/K} \cdot \mathbf{i} = (L:K) \cdot \text{Ident}$.

(ii) $\mathbf{N}_{L/K} \mathbf{N}_{F/L} = \mathbf{N}_{F/K}$ where F/K is a galois extension containing L/K.

How does the functor $\Lambda \dashrightarrow \Lambda$ behave under unramified base change?

1) (Finite unramified extensions). Let L/K be a finite unramified extension of fields of the sort that we are considering, with rings of integer E/D, residue field extension l/k.

Write $V^E = Spf(E[[T_1, \ldots, T_s]])$, and $V^D = Spf(D[[T_1, \ldots, T_s]])$.

Lemma 4.17. $V_n^E \approx V_n^D \times_{\text{Spec}(k)} \text{Spec}(l)$.

Proof. Use that $E = D \otimes_{W(k)} W(l)$.

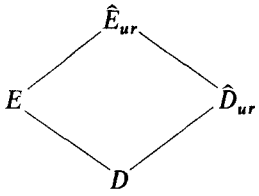
2) (The maximal unramified extension). Let $\hat{K}_{ur}$ denote the completion of the maximal unramified extension of K. Then $\hat{D}_{ur}$, the ring of integers in $\hat{K}_{ur}$ is the completion of $D_{ur} \subset K_{ur}$. The residue field of K_{ur} and $\hat{K}_{ur}$ is $\bar{k}$, the algebraic closure of k. Let $\tilde{V}$ denote the base change of $V = V^D$ to $\hat{D}_{ur}$.

Lemma 4.18. $\tilde{V}_n \approx V_n \times_{\text{Spec}(k)} \text{Spec}(\bar{k})$.

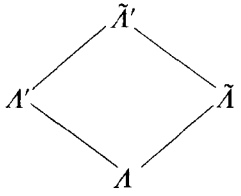
Proof. If m is the maximal ideal of D, then mD_{ur} and $m\hat{D}_{ur}$ are the maximal ideals of D_{ur} and $\hat{D}_{ur}$. Moreover, $D_{ur}/m^n D_{ur} \approx \hat{D}_{ur}/m^n \hat{D}_{ur}$ and $D_{ur} = D \otimes_{W(k)} W(\bar{k})$, from which the above follows.

3) (Commutation of $\mathbf{N}_{L/K}$ with unramified base change). Let L/K be a finite unramified extension, and let $\hat{L}_{ur}/\hat{K}_{ur}$ denote the completions of the maximal unramified extensions. If L/K is galois with group G, so is $\hat{L}_{ur}/\hat{K}_{ur}$. We have the diagram of rings of integers of our four fields,

(4.19)



and let Λ be a commutative formal Lie group scheme over D and let



denote the base changes of Λ to the four rings of (4.19). We have the obvious assertion

Lemma 4.20.

$$\tilde{\Lambda}' \xrightarrow{\mathbf{N}_{\hat{L}_{ur}/\hat{K}_{ur}}} \tilde{\Lambda}$$

is the base change to $\mathrm{Spec}(\bar{k})$ *of the morphism*

$$\Lambda' \xrightarrow{\mathbf{N}_{L/K}} \Lambda.$$

Proof. This follows from checking through the isomorphism of (4.18) and comparing with our characterization of the norm (4.14).

c) Relation with Group Schemes of Finite Type

Let G be a group scheme over D of finite type. It is a theorem of Greenberg [17, § 4] that the functors

$$G_n(R) = G(D/p^n \otimes_{W_n(k)} W_n(R)); \qquad G_n\colon \text{Rings}/k \dashrightarrow \text{Sets}$$

are representable. Thus they yield a pro-algebraic group $\mathbf{G}$:

$$\cdots \to G_n \to G_{n-1} \to \cdots$$

and the definition (4.9) gives us an exact sequence of functors

(4.21)
$$0 \to (\hat{G})_n \to G_n \to G/k \to 0 \qquad n > 0$$

if G is smooth. Here $\hat{G}$ denotes the formal completion of G at the zero-section, and G/k denotes reduction to k. Thus we have an exact sequence of pro-algebraic groups,

(4.22)
$$0 \to \hat{\mathbf{G}} \to \mathbf{G} \to G/k \to 0.$$

Example. Take $G = \mathfrak{G}_{m,D}$ and write $U = \hat{\mathfrak{G}}_{m,D}$. Then (4.22) reads,

$$0 \to \mathbf{U} \to \mathfrak{G}_{m,D} \to \mathfrak{G}_{m,k} \to 0. \tag{4.23}$$

Some terminological complication. If k is algebraically closed, and we pass to the slightly coarser category of pro-(quasi)-algebraic groups (denoted pro-algebraic groups in [55]), the above exact sequence (4.23) is written in Serre [55]:

$$0 \to U^1 \to U_K \to \mathfrak{G}_m \to 0. \tag{4.24}$$

Since we intend to make use of some of the results of [55], the reader should be warned of this shift of terminology. Especially that our U signifies Serre's U^1.

d) Formal Groups of Multiplicative Type

Keeping the terminology of (b), (c) above, let us consider the formal completion of the multiplicative group scheme $U = \hat{\mathfrak{G}}_m$ over D. Then $\mathbf{U}$ is a commutative pro-algebraic group over k represented by a projective system of group schemes whose underlying schemes are isomorphic to affine space (4.12). If we form $\mathbf{U} \times_{\mathrm{Spec}(k)} \mathrm{Spec}(\bar{k})$ we obtain (4.18) the pro-algebraic group over $\bar{k}$, $\tilde{\mathbf{U}}$ where $\tilde{U}$ is the formal completion of $\mathfrak{G}_m$ over $\tilde{D} = \hat{D}_{ur}$.

Let L/K be a finite Galois totally ramified extension of degree p^r, $p = \mathrm{char}\, k$ – with notation as in (b). Let U' denote the base change of U to E.

Consider the kernel,

$$0 \to T \to \mathbf{U}' \xrightarrow[\mathbf{N}_{L/K}]{} \mathbf{U}$$

in the category of pro-algebraic groups over k.

Proposition 4.25. (i) $\mathbf{N}_{L/K}$ *is surjective in the category of pro-algebraic groups.*

(ii) *The pro-algebraic group* $\pi_0(T)$ *is isomorphic to the constant finite group* $G/[G,G]$ *over* $\mathrm{Spec}(D)$. $(G = \mathrm{Gal}(L/K).)$

Proof. By π_0 we mean the functor that associates to an algebraic group over k its group of connected components over $\bar{k}$, regarded as a galois module (or, equivalently, as an étale group) over the field k. This functor π_0 then extends to the category of pro-algebraic groups, taking its values in the category of pro-étale group schemes over k. It is important to us to note that π_0 factors through the category of pro-quasi-algebraic groups, and that regarded as a functor on pro-quasi-algebraic groups over an algebraically closed field k, it is exactly the functor π_0 of [55].

To prove (i), since $\mathbf{U}$ is represented by a projective system of smooth group schemes, it suffices to check that the norm map, $N_{L/K}$: $\mathbf{U}'(\bar{k}) \to$

$\mathbf{U}(\bar{k})$ is surjective. But this map is just the norm map, $N_{\hat{L}_{ur}/\hat{K}_{ur}}$ from the group of 1-units of $\tilde{E}=\hat{E}_{ur}$ to the group of 1-units of $\tilde{D}$. Switching to Serre's notation (4.24) we get the diagram of maps

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U^1(\hat{L}_{ur}) & \longrightarrow & U_{\hat{L}_{ur}} & \longrightarrow & \bar{k}^* & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow{\scriptstyle p^r} & & \\ 0 & \longrightarrow & U^1(\hat{K}_{ur}) & \longrightarrow & U_{\hat{K}_{ur}} & \longrightarrow & \bar{k}^* & \longrightarrow & 0. \end{array}$$

Since the end map is an isomorphism, and the middle is surjective ([55], Corollary to Proposition 1, § 2), we see that the left hand vertical map is surjective.

To prove (ii) we first make the base change to $\bar{k}$. Then pass to pro-quasi-algebraic groups, and consider the diagram,

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & T & \longrightarrow & S & \longrightarrow & \mu_{p^r,\bar{k}} & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \tilde{\mathbf{U}}' & \longrightarrow & \mathbb{G}_{m,\hat{E}_{ur}} & \longrightarrow & \mathbb{G}_{m,\bar{k}} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle N_{\hat{L}_{ur}/\hat{K}_{ur}}} & & \downarrow{\scriptstyle N_{\hat{L}_{ur}/\hat{K}_{ur}}} & & \downarrow{\scriptstyle p^r} & & \\ 0 & \longrightarrow & \tilde{\mathbf{U}} & \longrightarrow & \mathbb{G}_{m,\hat{D}_{ur}} & \longrightarrow & \mathbb{G}_{m,\bar{k}} & \longrightarrow & 0. \\ & & \downarrow & & & & & & \\ & & 0 & & & & & & \end{array}$$

Since $\mu_{p^r,k}$ is a nilpotent group scheme, it follows from the above that $\pi_0(T)\to\pi_0(S)$ is an isomorphism. But S is the pro-quasi-algebraic group that Serre calls V_L and he proves ([55], 2.3, Corollary to Proposition 3) that $\pi_0(S)\underset{\rho}{\cong} G/[G,G]$, and indeed the isomorphism is made precise (cf. loc. cit. 2.2, Remark):

One fixes a uniformizer π of $\hat{L}_{ur}$. To each $\alpha\in G$ one considers $\alpha(\pi)/\pi$, regarded as an element of $S(\bar{k})$. Denoting β: $S(\bar{k})\to\pi_0(S)$ the natural projection, our isomorphism ρ is induced by: $\alpha\mapsto\beta[\alpha(\pi)/\pi]$.

This establishes (ii) once we check that the natural action of the galois group $\mathrm{Gal}(\bar{k}/k)$ on $\pi_0(S)$ is trivial. But that can be seen immediately

from our explicit description of ρ, provided we have chosen our uniformizer π to lie in $L \subset \hat{L}_{ur}$. This we could have done. Q.E.D.

Now let A be a formal Lie group over D and let $\tilde{A}$ denote its base change to $\tilde{D} = \hat{D}_{ur}$, and $\bar{A}$ its fibre over the geometric point $\bar{k}$.

Lemma 4.26. *These are equivalent:*

(i) *Definition. A is of multiplicative type.*

(ii) *$\tilde{A}$ is isomorphic to a finite product $\tilde{U}^d$ of formal multiplicative group schemes, over $\tilde{D}$.*

(iii) *$\bar{A}$ is isomorphic, over $\bar{k}$, to a finite product $\bar{U}^d$ of formal multiplicative group schemes.*

Proof. To show (iii) implies (ii), note that if A satisfies (iii), then $\tilde{A}$ is divisible in the sense of ([69], 2.2). That is, multiplication by p is an isogeny for $\tilde{A}$. Thus we may pass (via the equivalence of the categories of formal divisible groups over $\tilde{D}$ and p-divisible connected groups over $\tilde{D}$ ([69], Proposition 1) to the p-divisible group $\tilde{A}(p)$. Let the superscript # denote duality in the category of p-divisible groups ([69], 2.3). Since the closed fibre of $\tilde{A}(p)$ is $\bar{A}(p)$ which is the constant étale p-divisible group $(\mathbb{Q}_p/\mathbb{Z}_p)^d$ by (iii), we learn that the p-divisible group $\tilde{A}(p)^*$ is étale of height d. But the only étale group scheme of height d over $\tilde{D}$ is the constant group scheme $(\mathbb{Q}_p/\mathbb{Z}_p)^d$. Thus $\tilde{A}(p)$ must be the dual of this latter p-divisible group. This means that $\tilde{A}(p) = \tilde{U}^d(p)$. Passing back to the category of formal group schemes by the inverse of the above natural equivalence gives us that $\tilde{A} = \tilde{U}^d$. Q.E.D.

For G a group scheme locally of finite type over D, we shall say that G is *formally of multiplicative type over D* if the formal completion $\hat{G}$ is of multiplicative type over D.

If G is smooth over D, by Lemma 4.26 the question of whether G is formally of multiplicative type is dependent only upon the geometric fibre of G over the closed point of D.

Lemma 4.27. *If A is an abelian scheme of dimension d over D, these are equivalent:*

1) *A is formally of multiplicative type.*

2) *$A/\bar{k}$ has invertible Hasse matrix* [26].

3) *There are exactly p^d points of order p in $A(\bar{k})$. $p = \mathrm{Char}(k)$ as usual.*

4) *Definition.* A is an *ordinary* abelian scheme over D.

The proof of the equivalence of these assertions is standard in the theory of abelian varieties. The implication 3) $\Rightarrow$ 1) will be of use to us, and so we give a brief proof of it. Let, as above, $\bar{A}(p)$ denote the p-divisible group associated to A ([69], 2.2) over $\bar{k}$. Assertion 3) tells us that the height

of the étale part of $\bar{A}(p)$, $\bar{A}(p)^{\text{ét}}$ is d. Since $\bar{A}(p)$ is isogenous to its dual we therefore learn that $\bar{A}(p)^0$, the connected part of $\bar{A}(p)$, must contain a group of multiplicative type of dimension d. But the p-divisible group $\bar{A}(p)^0$ is of multiplicative type, and (4.26) gives 1). See [14] for a discussion of ordinary abelian varieties over finite fields.

Given a formal Lie group Λ, of multiplicative type over D, of dimension d we shall obtain an invariant, *the twist of Λ over D*, which completely determines Λ. This depends only upon Λ/k, and can be defined as follows: Consider the étale p-divisible group $(\Lambda/k)(p)^{\#}$ which is of height d. Making the base change to $\bar{k}$, we have $\bar{\Lambda}(p)^{\#} \approx (\mathbb{Q}_p/\mathbb{Z}_p)^d$, and choosing such an isomorphism, $\Lambda(p)^{\#}$ determines an action of $\mathrm{Gal}(\bar{k}/k)$ on $(\mathbb{Q}_p/\mathbb{Z}_p)^d$, unique up to equivalence of representations. We shall refer to this action as the *twist of Λ*. If k is finite, the action is determined by the conjugacy class of the image of $\mathrm{Frob} \in \mathrm{Gal}(\bar{k}/k)$, which is thus a matrix $u \in \mathbf{GL}(d, \mathbb{Z}_p)$, up to conjugacy. We call u the *twist matrix*.

Here is a possibly more direct description of u: Note that there is a natural isomorphism, $\mathbb{Z}_p \approx \hom_k(U, U) \approx \hom_{\bar{k}}(\bar{U}, \bar{U})$. Thus we have a natural isomorphism, $\mathbf{GL}(d, \mathbb{Z}_p) \approx \mathrm{aut}_k(U^d, U^d) \approx \mathrm{aut}_{\bar{k}}(\bar{U}^d, \bar{U}^d)$. Choose an isomorphism over $\bar{k}$, j: $\bar{\Lambda} \xrightarrow{\approx} \bar{U}^d$, and for X any scheme over k, let Frob: $\bar{X} \to \bar{X}$ denote the Frobenius automorphism,

$$1 \times \mathrm{Frob}\colon X \times_k \bar{k} \to X \times_k \bar{k}.$$

Then consider the composition,

$$\bar{U}^d \xrightarrow[\mathrm{Frob}^{-1}]{} \bar{U}^d \xrightarrow[j^{-1}]{} \bar{\Lambda} \xrightarrow[\mathrm{Frob}]{} \bar{\Lambda} \xrightarrow[j]{} \bar{U}^d.$$

Since j is a morphism over k, the above composition is an isomorphism over $\bar{k}$, and hence by the natural identification signaled above, it determines an element in $\mathbf{GL}(d, \mathbb{Z}_p)$. A change in the isomorphism j changes this matrix only up to conjugacy. Its conjugacy class is none other than the twist matrix conjugacy class, u.

Now suppose k is a finite field, Λ a formal Lie group over D, of dimension d, of multiplicative type with twist matrix u. Let L/K be a totally ramified finite Galois extension of degree a power of $p = \mathrm{char}(k)$, and with Galois group G. Let Λ' denote the base change of Λ to E, the ring of integers in L, and consider the kernel,

$$0 \longrightarrow T \longrightarrow \bar{\Lambda}' \xrightarrow{\mathbf{N}_{L/K}} \bar{\Lambda} \tag{4.28}$$

in the category of pro-algebraic groups over k.

Proposition 4.29. *The morphism $\mathbf{N}_{L/K}$ is surjective. The underlying abelian group of $\pi_0(T)$ is isomorphic to $G^{ab} \times G^{ab} \times \cdots \times G^{ab}$ (d times), which we may write as $G^{ab} \otimes_{\mathbb{Z}_p} (\mathbb{Z}_p)^d$, and its galois module structure over k may be written, in terms of its latter description, as $1 \otimes_{\mathbb{Z}_p} u = \mathrm{Frob}$.*

Proof. In fact one obtains a canonical isomorphism of galois modules over k, $\pi_0(T) \approx G^{ab} \otimes_{\mathbb{Z}_p} (\mathbb{Z}_p)^d$, upon choosing an isomorphism $\bar{A} \approx \bar{U}^d$, over $\bar{k}$. This follows easily from (4.25)(ii).

Corollary 4.30. *Under the same hypotheses as* (4.29), *we have*

$$A(D)/N_{L/K} A(E) \approx (G^{ab})^d/(1-u)(G^{ab})^d$$

where G^{ab} *stands for* $G/[G,G]$.

Proof. Let us first establish

Lemma 4.31. *Let* X *be a commutative pro-algebraic group scheme over the finite field* k. *Let* $X^0 \subset X$ *denote its connected component* [49]. *Then* $X/X^0 = \pi_0(X)$ *is a pro-object in the category of étale group schemes over* k. *If we form Galois cohomology over* k *then:*

$$H^q(k, X) \xrightarrow{\approx} H^q(k, \pi_0(X)).$$

Proof. If $\{X_j\}$ is a system of commutative group schemes representing the pro-object X, then the system of connected components $\{X_j^0\}$ represents X^0, and the system of quotients $\{\pi_0(X_j)\}$ represents $\pi_0(X)$.

But Lang's [35] theorem gives us an isomorphism,

$$H^q(k, X_j) \xrightarrow{\approx} H^q(k, \pi_0(X_j))$$

for each j, whence the lemma follows.

Now apply $H^q(k, \ )$ to the short exact sequence (4.28) to get, using (4.29),

$$A'(k) \xrightarrow[N_{L/K}(k)]{} A(k) \to H^1(k, T) \to H^1(k, A'). \tag{4.32}$$

But A' is represented by connected group schemes, so (4.31) gives us that $H^1(k, A') = 0$, and combining (4.31), and (4.29) gives that $H^1(k, T) = (G^{ab})^d/(1-u)(G^{ab})^d$. Our corollary then follows from the observation that there are natural isomorphisms of pro-finite groups,

$$\begin{array}{ccc} A'(k) & \xrightarrow[N_{L/K}]{} & A(k) \\ \uparrow \approx & & \uparrow \approx \\ A'(E) & \xrightarrow[N_{L/K}]{} & A(D). \end{array}$$

Corollary 4.33. *Let* L/K *be a totally ramified* Γ*-extension associated to* p. *Let* A *be a formal Lie group of dimension* d *of multiplicative type,*

with twist matrix u, over D. Suppose u has no eigenvalue equal to 1. *Then* $N_{L/K}\Lambda(E)$ *is of finite index in* $\Lambda(D)$, *and*

$$\Lambda(D)/N_{L/K}\Lambda(E) \approx \Gamma^d/(1-u)\Gamma^d.$$

Proof. After our assumptions, the intermediate finite extensions K_m/K of the tower L/K all satisfy the hypotheses of Corollary (4.30). Thus the cokernel of $N_{K_m/K}$ is isomorphic to $(\Gamma/\Gamma_m)^d/(1-u)(\Gamma/\Gamma_m)^d$. By hypothesis, $1-u$ is nonsingular. Thus the order of these groups are constant for large m, and in fact isomorphic to $\Gamma^d/(1-u)\Gamma^d$. Q.E.D.

e) The Twist Matrix of Ordinary Abelian Varieties

In this paragraph we consider abelian varieties over finite fields k. We show that the eigenvalues of the twist matrix of such an abelian variety which is formally of multiplicative type lie among the eigenvalues of the Frobenius endomorphism of A. We shall prove this well known fact (in the more precise assertion of (4.34) and (4.37)) and then in (f) below derive the facts about the cokernel of the norm of abelian schemes that we need for our later work.

Lemma 4.34. *Let A be an ordinary abelian variety of dimension d defined over a finite field k with twist matrix u. Then if* $g(t)$ *is the characteristic polynomial of the Frobenius endomorphism,* π, *we have*

$$g(t) = c\, t^d f(q/t) \cdot f(t)$$

where $f(t)$ *is the characteristic polynomial of the matrix u,* $q = \mathrm{card}(k)$, *and c a nonzero constant.*

Proof. Milne, ([43], § 1) has shown that Weil's definition ([72], IX, § 67, p. 131, and Theorem 35) of the characteristic polynomial of an endomorphism of an abelian variety generalizes nicely to p-divisible groups. Explicitly, let G denote a p-divisible group, [62, 69] over k (which may be taken to be any perfect field). Let e denote an endomorphism of G over k. One says that $P(t)$ is the characteristic polynomial of e if it satisfies these 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

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

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

This polynomial is unique ([72], IX, § 68, Lemma 12) and Milne shows its existence by appealing to the theory of Dieudonné modules. From its definition it is clear that if A is an abelian variety over k, and e an endomorphism over k, then the characteristic polynomial of e, regarded as an endomorphism of A ([72], IX, § 67) is equal to the charac-

teristic polynomial of e regarded as an endomorphism of the p-divisible group $G = A(p)$, associated to A ([69], 2.2).

The following four observations are easily proven:

1. *(Multiplicativity). If e is an endomorphism of a p-divisible group G which operates on an exact sequence of p-divisible groups,*

$$0 \to G_1 \to G \to G_2 \to 0$$

and f_1, f, f_2, denotes the characteristic polynomials of e on the groups G_1, G, G_2, respectively, then,

$$f = f_1 f_2 .$$

2. *If e is an endomorphism of a p-divisible group G, with characteristic polynomial f, then the dual endomorphism $e^{\#}$ of the dual p-divisible group $G^{\#}$ also has characteristic polynomial f.*

3. *If e is an endomorphism of the constant p-divisible group $(\mathbb{Q}_p/\mathbb{Z}_p)^d$, then its characteristic polynomial is the characteristic polynomial of the associated $(d \times d)$-matrix.*

4. *Consider a diagram of p-divisible groups over k, where η is an isogeny:*

$$\begin{array}{ccc} G_1 & \xrightarrow{e_1} & G_1 \\ \downarrow{\scriptstyle \eta} & & \downarrow{\scriptstyle \eta} \\ G_2 & \xrightarrow{e_2} & G_2 \end{array}$$

then the characteristic polynomial of the endomorphism e_1 of G_1 is equal to the characteristic polynomial of the endomorphism e_2 of G_2.

Consider an abelian variety A as in the hypothesis of (4.34) and let

$$0 \to G^0 \to G \to G^{\text{ét}} \to 0 \tag{4.35}$$

be the decomposition of the p-divisible group $G = A(p)$ into connected and étale parts ([69], 1.4), where $p = \text{char}(k)$. Then $G^{\text{ét}}$ is of height d and G^0 is isogeneous to the dual of $G^{\text{ét}}$. The Frobenius endomorphism π operates on the exact sequence of p-divisible groups, (4.35), over $\bar{k}$. Let π^0, and $\pi^{\text{ét}}$ denote the induced endomorphisms on G^0, $G^{\text{ét}}$ respectively.

Let $\eta\colon A' \to A$ denote an isogeny between A' the dual of A, and A, defined over k ([45], Chapter 6, § 2). Then η induces isogenies of p-divisible groups,

$$\begin{array}{ccccccccc} 0 & \longrightarrow & (G^{\text{ét}})^{\#} & \longrightarrow & G^{\#} & \longrightarrow & (G^0)^{\#} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \eta} & & \downarrow{\scriptstyle \eta} & & \downarrow{\scriptstyle \eta} & & \\ 0 & \longrightarrow & G^0 & \longrightarrow & G & \longrightarrow & G^{\text{ét}} & \longrightarrow & 0. \end{array} \tag{4.36}$$

The Frobenius endomorphism operates compatibly on the six members of (4.36), regarded as p-divisible groups over $\bar{k}$. Consequently, if one denotes the operation of the Frobenius endomorphism on $(G^{\text{ét}})^*$ by π^0, we may apply (4) to obtain that the characteristic polynomial of the endomorphism π^0 on $(G^{\text{ét}})^*$ is equal to g^0, the characteristic polynomial of the endomorphism π^0 on G^0.

Applying duality we find, using (2), that the characteristic polynomial of the endomorphism $(\pi^0)^*$ on $G^{\text{ét}}$ is equal to g^0, again.

We now have two endomorphisms, $(\pi^0)^*$ and $\pi^{\text{ét}}$ on $G^{\text{ét}}$, with characteristic polynomials g^0 and $g^{\text{ét}}$. These endomorphism are easily seen to commute, and their composition is multiplication by q. (This can be seen from the definition of duality of p-divisible groups, together with the observation that the Frobenius endomorphism on $\mathbb{G}_m$ is multiplication by q in $\mathbb{G}_m$.)

Now recall that if A, B are any two $(d \times d)$-matrices over a field of characteristic zero, whose composition is qI (I is the identity), then their characteristic polynomials satisfy the relation:

$$f_A(t) = c \cdot t^d \cdot f_B(q/t).$$

Since $G^{\text{ét}}$ is an étale p-divisible group, we may apply (3) to deduce the analogous relationship:

$$g^{\text{ét}}(t) = c \cdot t^d \cdot g^0(q/t).$$

But one also gets, from the definition of the twist matrix, and (3), that

$$g^{\text{ét}}(t) = c \cdot t^d g^0(q/t).$$

Lemma 4.34 then follows from (1).

Corollary 4.37. *Let A be an ordinary abelian scheme over D, with twist u. Then the eigenvalues of the Frobenius endomorphism of A is, counted with multiplicities, $\alpha_1, \ldots, \alpha_n$, $q/\alpha_1, \ldots, q/\alpha_n$, where $\alpha_1, \ldots, \alpha_n$ are the eigenvalues of u.*

Corollary 4.38. *Let A be an ordinary abelian scheme over D with twist u. Then $u-1$ has nonvanishing determinant.*

Proof. The Frobenius endomorphism cannot have eigenvalue 1, for that would imply the existence of an infinite number of rational points of A over the finite field k.

f) The Norm Mapping with Respect to Γ-Extensions for Ordinary Abelian Schemes

Proposition 4.39. *Let A be an ordinary abelian scheme over D (whose residue field k is finite), of dimension d. Let L/K be any Γ-extension. Then $A(K)/N_{L/K}A(L)$ is finite, and consequently so is $H^1(\Gamma, A(L))$.*

If L/K is a totally ramified Γ-extension, then we have, more precisely, the short exact sequence,

$$(4.40) \qquad \Gamma^d/(1-u)\Gamma^d \to A(K)/N_{L/K}A(L) \to p\text{-part of } A(k) \to 0.$$

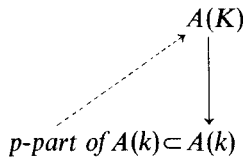
Proof. If L/K is unramified, the proposition follows from (4.3) above. If L/K is ramified, we may find an intermediary subfield K' which is a finite extension of K such that L/K' is a totally ramified Γ-extension. By transitivity of norms, it suffices to prove the proposition for L/K'. We are thus reduced to the case where L/K is a totally ramified Γ-extension.

Then the intermediary extensions K_m/K satisfy the hypotheses of Proposition 4.29. Evaluating the exact sequence (4.6) by means of Corollary 4.30 we get

$$(4.41) \quad (\Gamma/\Gamma_m)^d/(1-u)(\Gamma/\Gamma_m)^d \to A(K)/N_{K_m/K}A(K_m) \to A(k)/A(k)^{p^m} \to 0.$$

But by (4.33) and (4.38) the above groups stabilize for large m, giving (4.39).

Proposition 4.42. *Suppose, in the situation of the preceding proposition, we have that the p-part of $A(k)$ admits a lifting to $A(K)$. That is, we have a dotted arrow making*



commutative, where the vertical arrow is the reduction map. Then if L/K is totally ramified, we may sharpen (4.41) *to the (noncanonically) split exact sequence:*

$$(4.43) \qquad 0 \to \Gamma^d/(1-u)\Gamma^d \to A(K)/N_{L/K}A(L) \to p\text{-part of } A(k) \to 0.$$

Proof. We may regard (4.41) above as the exact sequence of 0-dimensional Tate cohomology groups of the finite group Γ/Γ_m with coefficients in the modules of the short exact sequence,

$$(4.44) \qquad 0 \to \hat{A}(K_m) \to A(K_m) \to A(k) \to 0.$$

But since Γ/Γ_m is a finite p-group, the Tate cohomology groups of Γ/Γ_m with coefficients in the p-part of $A(k)$ are isomorphic to the Tate cohomology groups with coefficients in $A(k)$, and our newly hypothesized lifting then enables us to conclude that the boundary map

$$H^{-1}(\Gamma/\Gamma_m, A(k)) \to \hat{A}(K)/N_{K_m/K}\hat{A}(K_m)$$

of the long exact sequence of Tate cohomology groups is trivial, hence the first arrow of (4.41) is an injection. Q.E.D.

§ 5. Abelian Schemes over Local Bases

For a brief exposition of Hensel rings, see (GT, Chapter III, Section 4). In this paragraph, let X be a Hensel arithmetic scheme. By this we mean the spectrum of D, the ring of integers in a field K, finite over the field of fractions of the Hensel-closure of the localization of $\mathbb{Z}$ at p. Let $\hat{X}$ denote the completion of X, $\hat{K}$ the completion of K. Let $H^r(X,)$ denote cohomology with compact support (SGAA, Fasc. 1, Vol. 4.3), the cohomology being taken for the $fpqf$ site (SGAD, IV, 6.3).

The following lemma collects all the results we shall need concerning the relationship between cohomology groups over Hensel bases to cohomology groups over complete bases.

Lemma 5.1. (i) *(Galois cohomology). The natural map $G_{\hat{K}} \to G_K$ is an isomorphism, and consequently, the induced map on Galois cohomology,*

$$H^r(\bar{K}/K;) \to H^r(\bar{\hat{K}}/\hat{K};)$$

is an isomorphism for any Galois module over K.

(ii) *(Cohomology over fraction fields). Let G be a commutative group scheme of finite type over K. Then*

$$H^r(K, G) \xrightarrow{\approx} H^r(\hat{K}, G) \quad \text{if } r>0.$$

The above isomorphism is true for $r \geqq 0$ if G is finite.

(iii) *(Smooth groups over X). Let G be smooth over X, of finite type. Let G_x be its reduction to the closed point of X and let G_x^0 denote the connected component containing the identity in G_x.*

Then

$$H^r(X, G) \cong H^r(\hat{X}, G) \cong H^r\big(k(x), G_x/G_x^0\big) \quad \text{for } r \geqq 0.$$

In particular, if G_x is connected,

$$H^r(X, G) = H^r(\hat{X}, G) = 0 \quad \text{for } r>0.$$

(iv) *(Relative cohomology for $r>1$).*

Let G be smooth over X, then

$$H^r_!(X, G) = H^r_!(\hat{X}, G) \quad \text{for } r>1.$$

(v) *(Relative cohomology for $r=1$).*

Suppose that G satisfies either of the following two conditions:

(a) *G is an affine finite flat group scheme over X.*

(b) *G is a smooth group over X satisfying the "Néron property": $G \cong j_* j^* G$ as a sheaf for the smooth topology.*

Then

$$H^1_!(X, G) = H^1_!(\hat{X}, G) = 0.$$

(vi) *(Summary of the above results for A a Néron model over X).*

Suppose that A is a Néron model over X, and that

$$0 \to A^0 \to A \to F \to 0$$

is as in (3.1). *Then*

$$H^r(X, A) \cong H^r(\hat{X}, A) \cong H^r(k(x), F) \quad \text{for } r \geqq 0$$

$$H^r_!(X, A) \cong H^r_!(\hat{X}, A) \quad \text{for } r \geqq 1.$$

$$H^1_!(X, A) \cong H^1_!(\hat{X}, A) = 0.$$

Proof. (i) What is meant in (i) is that one chooses an algebraic closure $\bar{\hat{K}}$ of $\hat{K}$, and one takes $\bar{K}$ to be the algebraic closure of K in $\bar{\hat{K}}$. We then get a natural $G_{\hat{K}} = \mathrm{Gal}(\bar{\hat{K}}/\hat{K}) \to G_K = \mathrm{Gal}(\bar{K}/K)$ by restriction. It is an elementary fact that this map is an isomorphism: It is surjective because of the henselian property of the ring of integers of K. It is injective, as may be seen using Krasner's lemma ([29], p. 31, Proposition 4).

(ii) The assertion for finite groups follows from (i). To prove (ii) proceed by induction on $r \geqq 1$. Recall that r-dimensional Galois cohomology groups are torsion groups. For surjectivity, take $h \in H^r(\hat{K}, G)$ which is of order n. The diagram

$$\begin{array}{ccccc} H^r(K, {}_nG) & \longrightarrow & H^r(K, G) & & \\ \downarrow \cong & & & & \\ H^r(\hat{K}, {}_nG) & \longrightarrow & H^r(\hat{K}, G) & \longrightarrow & H^r(\hat{K}, G) \end{array}$$

implies that h is in the image of the vertical map. We have used the fact that ${}_nG$ is finite.

Injectivity for $r \geqq 2$ may be proved by taking $h \in H^r(K, G)$ which is of order n, and considering the diagram

$$\begin{array}{ccccccc} H^{r-1}(K, G) & \longrightarrow & H^{r-1}(K, G) & \longrightarrow & H^r(K, {}_nG) & \longrightarrow & H^r(K, G) \\ \downarrow \cong & & \downarrow \cong & & \downarrow \cong & & \downarrow \cong \\ H^{r-1}(\hat{K}, G) & \longrightarrow & H^{r-1}(\hat{K}, G) & \longrightarrow & H^r(\hat{K}, {}_nG) & \longrightarrow & \hat{H}^r(K, G). \end{array}$$

The first two vertical maps are isomorphisms by the inductive hypothesis. The same diagram can be used to show injectivity for $r = 1$, but one needs an additional fact:

Approximation Lemma. *If n is a positive integer and* $c \in G(\hat{K})$, *there is a* $\tilde{c} \in G(\hat{K})$ *and a* $d \in G(\hat{K})$ *such that*

$$c = \tilde{c} \cdot d^n.$$

Proof. Reducing immediately to the case where G is a connected group, proceed in three steps:

a) *When G Extends to a Group scheme G/X which Satisfies the "Neron Property":*

Then regard c as an element of $G(\hat{X})$. Since G is smooth we may approximate c by a section $\tilde{c} \in G(X)$ such that $c \equiv \tilde{c} \bmod p^r$ for any number $r \geqq 1$ we choose. Thus if $e = c/\tilde{c}$, $e \in \hat{G}(\hat{X})$ where $\hat{G}$ is the formal completion of G along the zero section. Since $\hat{G}(\hat{X})^n$ is an open subgroup of the p-adic analytic group $\hat{G}(\hat{X})$, if r is taken large enough, $e \in \hat{G}(\hat{X})^n$.

b) *Extensions by Unipotent Groups:*

Let $0 \to U \to G \to G' \to 0$ be an exact sequence of K-groups, where U is unipotent and the approximation lemma holds for G'. Then it holds for G.

This follows because U is uniquely divisible for all $n \geqq 1$; therefore the approximation lemma holds for U, and the maps $G(K) \to G'(K)$, $G(\hat{K}) \to G'(\hat{K})$ are surjective.

c) *The General Case:*

After (b) we may suppose that G has no unipotent part. But a recent theorem of Raynaud (*Modèles de Néron*, Comptes Rendus Acad. Sci., Paris t. 262, pp. 345–347, Théorème 3.4) asserts that such a group scheme G/K extends to a group scheme G/X which satisfies the "Néron property". The Approximation lemma then follows from (a).

(iii) Since G is smooth, we may apply (GB, III, App. 11.1) to replace the $fpqf$ cohomology groups occurring in the statement of (5.1) (iii) by étale cohomology groups. Now, since X, and $\hat{X}$ are Hensel-closed, the argument of (4.3) (or, to cite a precise reference: Theorem 4.9, Chapter II of GT) applies, giving that

$$H^r_{\text{ét}}(X, G) = H^r_{\text{ét}}(\hat{X}, G) = H^r(\bar{k}/k, G) \qquad (k = k(x)).$$

Our assertion then follows from Lang's theorem [35], using that k is a finite field, and G^0 is connected.

(iv) This comes directly from (ii) and (iii), by the five-lemma.

(v) Consider the exact sequence,

$$H^0(X, G) \xrightarrow{j^0} H^0(\text{Spec } K, G) \to H^1 \to H^1(X, G) \xrightarrow{j^1} H^1(\text{Spec } K, G).$$

In case (a), note that any section defined over K of G, or of a G-torseur extends over X. Therefore j^0 is surjective and j^1 is injective (we have used that every element of $H^1(X, G)$ is represented by a torseur since G is separated ([51], XI.3.1.1)).

In case (b), since G satisfies the "Néron Property", j^0 is surjective (in fact, it is an isomorphism). Thus we must show that j^1 is injective. We may identify the last two groups with the corresponding étale Cech

cohomology groups, since G is smooth (GB III, App.) and we are considering one-dimensional cohomology (GT, Chapter II, 3.6). Let c be a Cech 1-cocycle in $Z^1(X'/X, G)$ representing a class in $H^1(X, G)$ which goes to zero under j^1. Let the subscript K denote the base change from X to K. We have that $c_K = \delta b_K$, for $b_K: X'_K \to G_K$ a section. By the "Néron property", b_K comes from a unique section, $b: X' \to G$. Set $c' = c - \delta b$. Then $c': X' \times_X X' \to G$ is a morphism such that $c'_K = 0$.

Since $X' \times_X X'$ is smooth over X, and again, G satisfies the "Néron property", c' must be zero. That means that our original c was cohomologous to zero. Q.E.D.

Corollary 5.2. *Let A be an abelian scheme over D. All the maps below are isomorphisms:*

$$\begin{array}{ccccc} H^2(X, \tilde{A}) & \xrightarrow[\eta]{} & {}_{p^\infty}H^2(X, A) & \xleftarrow[j]{} & {}_{p^\infty}H^1(\overline{K}/K; A) \\ \downarrow & & \downarrow & & \downarrow \\ H^2(\hat{X}, \tilde{A}) & \xrightarrow[\hat{\eta}]{} & {}_{p^\infty}H^2(\hat{X}, A) & \xleftarrow[\hat{j}]{} & {}_{p^\infty}H^1(\overline{\hat{K}}/\hat{K}; A) \xrightarrow[\tau]{} \{A'(\hat{K})\}^* \end{array}$$

where $\{\ \}^* = \hom_{\text{cont}}(\ , \mathbb{Q}_p/\mathbb{Z}_p)$ denotes Pontrjagin p-dual, τ is the Tate local duality isomorphism [67], *the map η is the limit of the maps η_n below, coming from the "Kummer theory"* (3.3) *of A,*

$$0 \to H^1(X, A)/_{p^n} \to H^2(X, {}_{p^n}A) \xrightarrow[\eta_n]{} {}_{p^n}H^2(X, A) \to 0.$$

Proof. It follows from (5.1)(vi) that η and its counterpart, $\hat{\eta}$, are isomorphisms. Using the relative cohomological exact sequence (SGAA, Fasc. 1, Vol. 4.3) and (5.1)(v) we see that j and $\hat{j}$ are isomorphisms. The vertical maps are isomorphisms again by (5.1)(v).

Corollary 5.3. *$H^2(X, \tilde{A})$ is a discrete p-abelian group of cofinite type. Its maximal divisible subgroup has corank equal to $[\hat{K}: \mathbb{Q}_p] \cdot \dim A$. Moreover, the quotient by its maximal divisible subgroup, $H^2(X, \tilde{A})/\text{div}$ is dual to ${}_{p^\infty}A'(\hat{K})$.*

Proof. The above assertions are true for $\{A'(\hat{K})\}^*$. Recall that the logarithm mapping (LG, 5.36, Cor. 4) ([69], p. 168) identifies a neighborhood of zero of the p-adic Lie group $A'(\hat{K})$ with a neighborhood of zero of the linear p-adic Lie group $\hat{D}^{\dim(A)}$.

Corollary 5.4. *Let L/K be a Γ-extension. We have the exact sequence,*

$$\begin{aligned} 0 \to \{A'(\hat{K})/\text{norm } A'(\hat{K}_n)\}^* \to H^2(X, \tilde{A}) \xrightarrow[\alpha_n]{} H^2(X_n, \tilde{A})^\Gamma \\ \to [A(\hat{K})/\text{norm } A(\hat{K}_n)] \to 0. \end{aligned} \tag{5.5}$$

Proof. The identification, $H^2_?(X_n, \tilde{A}) \approx \{A'(\hat{K})\}^*$, gives rise to the commutative square,

$$\begin{array}{ccc} H^2_?(X, \tilde{A}) & \xrightarrow{\approx} & \{A'(\hat{K})\}^* \\ \downarrow{\scriptstyle \alpha_n} & & \downarrow{\scriptstyle (\text{norm})^*} \\ H^2_?(X_n, \tilde{A}) & \xrightarrow{\approx} & \{A'(\hat{K}_n)\}^* \end{array}$$

from which it follows that the kernel of α_n is $\{A'(\hat{K})/\text{norm } A'(\hat{K}_n)\}^*$.

To analyze the cokernel of α_n we may identify $H^2_?(X, \tilde{A})$ with ${}_{p^\infty}H^1(\ /\hat{K}, A)$ by $j\eta$ of (5.2) and apply the Hochschild-Serre spectral sequence to the Galois extension $\hat{K}_n/\hat{K}$. Since $H^2(\ /\hat{K}, A)=0$, [67], we obtain that the cokernel of α_n is isomorphic to $H^2(\Gamma/\Gamma_n, A(\hat{K}_n))$ which is itself isomorphic to $A(\hat{K})/\text{norm } A(\hat{K}_n)$ by periodicity of the Tate cohomology of the cyclic group Γ/Γ_n. Q.E.D.

Suppose, at this point, that the decreasing sequence of subgroups, $N_{\hat{K}_n/\hat{K}} A'(\hat{K}_n)$ is stationary for large n. Let N denote the intersection of these subgroups in $A'(\hat{K})$, for all n, (and hence N is $N_{\hat{K}_n/\hat{K}} A'(\hat{K}_n)$ for large n, "the subgroup of universal norms"). If we pass to a direct limit as n goes to ∞ with (5.5), we get:

$$0 \to \{A(\hat{K})/N\}^* \to H^2_?(X, \tilde{A}) \to H^2_?(Y, \tilde{A})^\Gamma \to 0 \tag{5.6}$$

where the right-hand arrow is surjective because, the limit

$$\varinjlim [A(\hat{K})/\text{norm } A(\hat{K}_n)]$$

is taken via the corestriction maps (CL, p. 124) which are eventually zero since norm $A(\hat{K}_n)$ stabilizes for large n, and $A(\hat{K})/N$ is killed by a power of p.

Corollary 5.7. *Let L/K be a totally ramified Γ-extension. Let A be of dimension g, and ordinary (at the closed point of X), with twist matrix u. Suppose that the p-part of $A(k)$ admits a lifting to $A(K)$, (as in (4.42)). Then for every n we have the exact sequence,*

$$0 \to E_n \to H^2_?(X_n, \tilde{A}) \to H^2_?(Y, \tilde{A})^{\Gamma_n} \to 0 \tag{5.8}$$

where E_n is a finite (p-abelian) group obtained as a (noncanonically split) extension,

$$0 \leftarrow \{\Gamma^g/(1-u)\Gamma^g\}^* \leftarrow E_n \leftarrow \{A'(k)\}^* \leftarrow 0. \tag{5.9}$$

Proof. It follows from (4.38) and (4.40) that $N_{\hat{K}_n/K} A'(\hat{K}_n)$ is stationary for large n. Note that if we replace X by X_n, the residue field k doesn't

change. Hence the twist matrix of A over the base X_n is again u. Now apply the previous corollary for the base X_n, and evaluate $A'(\hat{K}_n)/N$ by means of (4.42). The groups E_n are seen to be all (noncanonically) isomorphic for varying n. Q.E.D.

Corollary 5.10. *Let L/K be a totally ramified Γ-extension. Let A be an abelian scheme defined over D, where D is a complete valuation ring, finite and unramified over $\mathbb{Z}_p$ for $p>2$. Suppose A' is of dimension g and ordinary and has twist matrix u. Then the conclusion of* (5.7) *is valid for A: One has the short exact sequence* (5.8) *and the noncanonically split exact sequence* (5.9).

Proof. This follows from (5.7) and the following lemma:

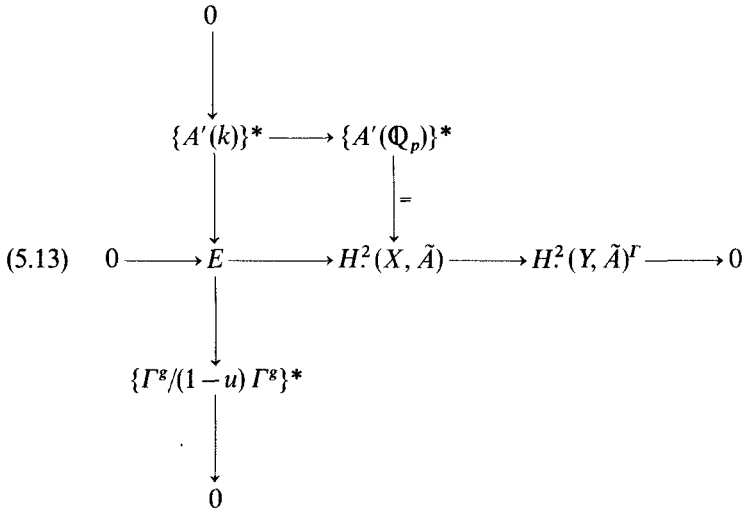
Lemma 5.11. *Let A be an abelian scheme over $X=\mathrm{Spec}(D)$ where D is a complete discrete valuation ring, finite and unramified over $\mathbb{Z}_p$ for $p>2$. Then the reduction map, $A(D)\to A(k)$ induces an isomorphism of p-torsion points.*

Proof. Suppose not. Hence there is an element $\mathbf{a}\in {}_pA(D)$ which goes to zero under the reduction map. We regard $\mathbf{a}$ as a section over D of the finite flat group scheme ${}_pA$. Then $\mathbf{a}$ generates a finite flat subgroup of ${}_pA$. (By taking the Zariski closure of the étale subgroup of $({}_pA\times_{\mathrm{Spec}\,D}\mathrm{Spec}\,K)$ generated by $\mathbf{a}$.) Call this subgroup scheme G. G is of rank p, and is connected, since $\mathbf{a}$ goes to zero under reduction. The question to ask is this: What is the closed geometric fibre $G_{\bar{k}}$ of G? Since $G_{\bar{k}}$ is a connected group scheme of rank p it can be only one of two group schemes: α_p or μ_p. (Note: In the case where A is ordinary, it couldn't be α_p, but also in complete generality:) *It cannot be* α_p, for a simple calculation shows that α_p doesn't lift to any finite flat group scheme over any discrete valuation ring D, unramified over $\mathbb{Z}_p$. In fact, it doesn't lift to D/m^2, where m is the maximal ideal of D. (Example A, §1 of [46].) (This latter fact also follows from the theorem of Oort-Tate [50] which classifies all finite flat group schemes of rank p over complete local noetherian rings.) Thus $G_{\bar{k}}$ must be μ_p, from which it follows that the Cartier dual $\hat{G}$ of G is an étale group scheme over D.

Thus $\hat{G}$ is isomorphic to the constant group scheme over D', some étale extension of D. Thus, G, the Cartier dual of $\hat{G}$, is isomorphic to μ_p over D'. But this is a contradiction because G has a nontrivial section over D' (namely: $\mathbf{a}$), and yet the group scheme μ_p can have no nontrivial section over any unramified extension of $\mathbb{Z}_p$, provided $p>2$. Q.E.D.

Corollary 5.12. *Let L/K be totally ramified. Let A be an ordinary abelian scheme over X of dimension g. Suppose $\hat{K}$ is $\mathbb{Q}_p$, for $p>2$. Then the Pontrjagin dual of $H^2(Y,\tilde{A})$ is a free Λ-module on g generators.*

Proof. Consider the commutative diagram, given to us by (5.10):



Applying Lemma 5.11 we see that the cokernel of $\{A'(k)\}^* \to \{A'(\mathbb{Q}_p)\}^*$ is a p-divisible group, whose rank, after (5.3), is g. From the above diagram we see that this cokernel maps onto $H^2(Y, \tilde{A})^\Gamma$ with finite kernel. Consequently $H^2(Y, \tilde{A})^\Gamma$ is also a p-divisible group of corank g. Since the coranks of $H^2(Y, \tilde{A})^{\Gamma_n}$ are $g p^n$, (2.1)(c) applies to yield our corollary.

We conclude this section with a calculation of the group E_n when $K = \mathbb{Q}_p$ and A is of dimension one. For A of dimension one, consider the characteristic equation of the Frobenius endomorphism acting on $A_{\bar{k}}$: $h(x) = x^2 - a_p x + p$.

The integer a_p is the trace of the Frobenius automorphism operating on one-dimensional ℓ-adic cohomology. The Riemann hypothesis tells us that

$$\text{(R.H.)} \qquad |a_p| \leqq 2(p)^{\frac{1}{2}}.$$

The requirement that A be ordinary is equivalent to the requirement that $a_p \not\equiv 0 \bmod p$, which after (R.H.) above is equivalent (if $p > 2$) to the requirement that $a_p \neq 0$. If A is ordinary, then the twist matrix u is just a unit of $\mathbb{Z}_p$, and u, p/u are the roots of the quadratic polynomial $h(x)$. One has, also, that the order of the group $A(k)$ is just $h(1) = 1 + p - a_p$.

Let $e_p = \mathrm{ord}_p(h(1))$. Note that:

$$e_p = \mathrm{ord}_p(h(1)) = \mathrm{ord}_p(1-u)(1-p/u) = \mathrm{ord}_p(1-u)$$

the last equality coming from the fact that $1 - p/u$ is a unit in $\mathbb{Z}_p$.

Lemma 5.14. (i) *If* $p>2$, *then* $e_p=\mathrm{ord}_p(1-u)=\mathrm{ord}_p(h(1))$ *is either one or zero. We have* $e_p=0$ *if and only if* $a_p\equiv 1 \bmod p$.

(ii) *If* $p=2$, e_p *can take the values* 0, 1, *or* 2.

(iii) *If* $p>5$, $a_p\equiv 1 \bmod p$ *if and only if* $a_p=1$.

Proof. These are all immediate consequences of (R.H.). To see (i), for example it suffices to note that if $p\geqq 3$, the following inequality is impossible by (R.H.):

$$p^2\leqq|h(1)|.$$

Corollary 5.15. *Let* $K/\mathbb{Q}_p$ *be a totally ramified finite extension. Let* $D\subset K$ *denote the ring of integers, and* $X=\mathrm{Spec}(D)$. *Let* Y/X *be a totally ramified* Γ*-extension. Let* A *be an ordinary abelian scheme of dimension one, over* $\mathrm{Spec}(\mathbb{Z}_p)$. *Denote by the same letter its base change to* X. *Then the groups* E_n *of* (5.8) *may be computed as follows:*

(i) E_n *is trivial if* $a_p\not\equiv 1 \bmod p$.

(ii) E_n *is isomorphic to* $\mathbb{Z}/p\oplus\mathbb{Z}/p$ *if* $a_p\equiv 1 \bmod p$.

Remark. We shall use this corollary in two situations (cf. § 8, (a) and (b)). Namely, when $K=\mathbb{Q}_p$, and $K=\mathbb{Q}_p(\zeta_p)$.

Proof. Under our hypotheses, the residue field k of D is the prime field. By (5.11) there is a lifting of the p-torsion points of $A(k)$ to $A(\mathbb{Q}_p)$, and hence to $A(K)$. Thus Corollary 5.7 applies. Since $h(1)$ is the order of $A(k)$, p^{e_p} is the order of $\{A(k)\}^*$. By (5.14)(i), e_p is either 0 or 1. Thus $\{A(k)\}^*\approx\mathbb{Z}/p^{e_p}$. Also, $\Gamma/(1-u)\,\Gamma\approx\mathbb{Z}/p^{e_p}$.

This evaluates the split exact sequence (5.9). Q.E.D.

Corollary 5.16. *Let* $X=\mathrm{Spec}(\mathbb{Z}_p)$, Y/X *a totally ramified* Γ*-extension and* A *an abelian variety of dimension one, ordinary over* X. *Then the exact sequence* (5.8),

$$0\to E\to H^2_?(X,\tilde{A})\to H^2_?(Y,\tilde{A})^\Gamma\to 0$$

may be evaluated as:

(i) $0\to 0\to\mathbb{Q}_p/\mathbb{Z}_p\to\mathbb{Q}_p/\mathbb{Z}_p\to 0$, *if* $a_p\not\equiv 1 \bmod p$

(ii) $0\to\mathbb{Z}/p\oplus\mathbb{Z}/p\to\mathbb{Z}/p\oplus\mathbb{Q}_p/\mathbb{Z}_p\to\mathbb{Q}_p/\mathbb{Z}_p\to 0$, *if* $a_p\equiv 1 \bmod p$.

Proof. This just comes from (5.10), (5.11) and (5.15). We shall need it explicitly for some calculations in § 8.

§ 6. Néron Models over Global Bases

For p a prime number, let Y/X be a Γ-extension, associated to p, over a global base X, which we suppose to be "special". That means (§ 1(c)): any $x\in X$ is either unramified for Y/X or is totally ramified.

Let S denote the (finite) set of such ramified x. Consider a Néron model (§ 3) A over X satisfying the following property:

(6.1) *A_x is an ordinary abelian variety over $k(x)$ for all $x \in S$.*

Also, for all $x \in X$ such that $A_x \neq A_x^0$ (i.e. A_x is not connected) x splits only finitely in Y.

If $(Y/X, A)$ satisfy the above hypotheses, we will simply say that $(Y/X, A)$ is *admissible.*

Recall that if Y/X is the cyclotomic Γ-extension, the second requirement in (6.1) is automatic.

If $(Y/X, A)$ is admissible, the Kummer-theoretic discussion of § 3 applies, yielding that

$$0 \to A(K_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to H^1(X_n, \tilde{A}) \to {}_{p^\infty}H^1(X_n, A) \to 0 \tag{6.2}$$

is $\mathscr{C}$-exact.

Let $T_n \subset X_n$ denote the set of points x of characteristic p.

Proposition 6.3. *Let $(Y/X, A)$ be admissible. One has the exact sequence,*

$$0 \to H^1(X_n, \tilde{A}) \to H^1(X_n - T_n, \tilde{A}) \to \bigoplus_{x \in T_n} H^2_x(X_{n,x}, \tilde{A})$$
$$\downarrow \approx$$
$$\bigoplus_{x \in T_n} H^2_x(\hat{X}_{n,x}, \tilde{A})$$

where $X_{n,x}$ is the henselization of X_n at x.

Proof. Consider the direct limit of long relative cohomological exact sequences for the $fpqf$ cohomology of the pair $(X_n, X_n - T_n)$ with coefficients in ${}_{p^r}A$ $(r \to \infty)$. One has the vertical isomorphism by (5.2). To establish the left-hand zero, and therefore the proposition, we must show that $H^1_x(X_{n,x}, {}_{p^r}A) = 0$ for $x \in T_n$. This follows from (5.1)(v), for if x is of characteristic p, then ${}_{p^r}A$ is finite flat and affine, and so we are in case (a) of (5.1)(v). If x is not of characteristic p, then ${}_{p^r}A$ is an étale separated quasi-finite group scheme which enjoys the "Néron property" (cf. 5.1) (since A does, and $j_* j^*$ is left exact). Therefore we are in case (b).

Proposition 6.4. *Let $(Y/X, A)$ be admissible.*

(i) *The sequence $H^1(X_n, \tilde{A})$ is controlled.*

(ii) *The kernel and cokernel of the map, α_n: $H^1(X_n, \tilde{A}) \to H^1(Y, \tilde{A})^{\Gamma_n}$ are given by:*

$$\ker(\alpha_n) = \ker(\gamma_n)$$

$$\operatorname{cok}(\alpha_n) = \ker(\delta_n)/\operatorname{im}(\gamma_n)$$

where γ_n, δ_n are the maps of diagram (6.6) *below.*

(iii) *Letting* $H = H_{(Y/X,A)}$ *denote the* Γ*-module* $H^1(Y, \tilde{A})$, H *is* Γ*-cofinite, and we have the following sequence* (mod $\mathscr{C}$) *which is exact* (mod $\mathscr{C}$):

$$0 \to A(K_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to H^{\Gamma_n} \to {}_{p^\infty}Ш(K_n) \to 0. \tag{6.5}$$

Proof. Let us establish the following commutative diagram, where all horizontal lines are exact:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & \tilde{A}(L)_{\Gamma_n} & \xrightarrow{\gamma_n} & \prod_{x \in T_n} (E_{n,x}) & & & & \\
 & & \downarrow & \searrow^{\delta_n} & \downarrow & & & & \\
0 & \longrightarrow & H^1(X_n, \tilde{A}) & \longrightarrow & H^1(X_n - T_n, \tilde{A}) & \longrightarrow & \prod_{x \in T_n} H^2(X_{n,x}, \tilde{A}) & \longrightarrow & H^2(X_n, \tilde{A}) \\
 & & \downarrow{\scriptstyle \alpha_n} & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & H^1(Y, \tilde{A})^{\Gamma_n} & \longrightarrow & H^1(Y - T_\infty, \tilde{A})^{\Gamma_n} & \longrightarrow & \prod_{x \in T_\infty} H^2(Y_x, \tilde{A})^{\Gamma_n} & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & 0 & & 0. & & & &
\end{array} \tag{6.6}$$

To explain the terminology, T_∞ refers to the set of primes of Y dividing p. After our assumptions on Y/X, the sets T_∞ and T_n are in one to one correspondence. The two long horizontal lines come from (6.3). The bottom horizontal line has been obtained by passing, in (6.3), to a direct limit ($n \to \infty$). It remains left-exact after passing to fixed subgroups under Γ_n.

The group $\tilde{A}(L)_{\Gamma_n} = H^1(\Gamma_n, H^0(Y, \tilde{A}))$ is the group of coinvariant elements under the action of Γ_n on $\tilde{A}(L)$. The middle vertical sequence of groups remain the same if computed with respect to the étale or the $fpqc$ sites because $\tilde{A}$ is an (inductive system of) étale group schemes over $X_n - T_n$.

If we consider the extensions $X_m - T_m / X_n - T_n$, these are étale Galois extensions for all $m \geqq n$, with group Γ_n/Γ_m. If we form the Hochschild-Serre spectral sequences for these Galois extensions and for the coefficient sheaf $\tilde{A}$ (e.g., GT, III, 4.7), (for either the étale or $fpqf$ sites), and pass to the limit as m goes to infinity, we get the "Hochschild-Serre spectral sequence" for the (pro-)étale extension $Y - T_\infty / X_n - T_n$, with Galois group Γ_n.

The middle vertical sequence of groups in our diagram (6.6) is just the short exact sequence which can be deduced from that Hochschild-

Serre spectral sequence, where we have put the bottom zero in because Γ_n is a group of cohomological dimension one.

The right-hand vertical sequence of groups is just the product, for $x \in T_n$ of the sequences (5.5).

This establishes our diagram.

To prove our proposition, the reader will check that (ii) follows immediately, by diagram-chasing. To see (i) we first note that the order of $\mathrm{cok}(\alpha_n)$, by (ii), is bounded by the order of $\prod_{x \in T_n} E_{n,x}$ and the groups $E_{n,x}$ are all finite groups of order admitting an upper bound independent of n, after (5.5) and (4.40). Moreover, the order of $\ker(\alpha_n)$ is bounded by the order of $\tilde{A}(L)_{\Gamma_n}$, and thus, to finish the proof of (i) we must show this latter group is of finite, bounded order.

Lemma 6.7. *Let M be any discrete p-abelian group of finite corank on which Γ operates continuously. If M^Γ is finite, then the natural map induces an isomorphism:*

$$M_\Gamma \xrightarrow{\approx} (M/\mathrm{div})_\Gamma.$$

Consequently, the order of $\tilde{A}(L)_{\Gamma_n}$ is bounded by that of $\tilde{A}(L)/\mathrm{div}$, which is a finite group.

Proof. The first assertion is elementary: Consider the diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{div} & \longrightarrow & M & \longrightarrow & M/\mathrm{div} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle 1-\gamma} & & \downarrow{\scriptstyle 1-\gamma} & & \downarrow{\scriptstyle 1-\gamma} & & \\
0 & \longrightarrow & \mathrm{div} & \longrightarrow & M & \longrightarrow & M/\mathrm{div} & \longrightarrow & 0 \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & M_\Gamma & \longrightarrow & (M/\mathrm{div})_\Gamma & & \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & 0 & & 0 & &
\end{array}$$

where $\mathrm{div} \subset M$ is, by our assumptions a p-divisible group of finite corank. Since, by our hypothesis the endomorphism $1-\gamma$ has finite kernel on div, it follows that it is a surjective endomorphism of div, whence our first assertion follows. Our second assertion then follows because $\tilde{A}(L)^{\Gamma_n} = \tilde{A}(K_n)$ is a finite group. This concludes the proof of part (i) of (6.4).

To prove (iii) we need a (well-known) lemma.

Lemma 6.8 (the weak Mordell-Weil theorem). *$H^1(X, \tilde{A})$ is of cofinite type as an abelian group.*

Proof. Take S to be a finite set of primes of X containing T, and containing all primes of X at which A has bad reduction. Then since $H^1(X, \tilde{A}) \subset H^1(X-S, \tilde{A})$, it suffices to prove that $H^1(X-S, \tilde{A})$ is of cofinite type. But on $X-S$ we have the following exact sequence of sheaves:

$$0 \to {}_pA \to \tilde{A} \to \tilde{A} \to 0$$

and so it suffices to show that $H^1(X-S, {}_pA)$ is finite. Note that the sheaf ${}_pA$ is a finite étale group scheme over $X-S$. The cohomology group $H^1(X-S, {}_pA)$ remains the same when computed for either the étale or the $fpqf$ topology. Let $Z/X-S$ be a finite, connected, Galois extension, with Galois group G, such that the pullback of ${}_pA$ becomes a constant group scheme over Z. Let $G(p) \subset G$ be a p-Sylow subgroup, associated to the intermediate extension $W/X-S$. Then the canonical map $H^1(X-S, {}_pA) \to H^1(W, {}_pA)$ is injective. The reason for this is that one has a trace map, (SGAA, IX, § 5),

$$H^1(X-S, {}_pA) \to H^1(W, {}_pA) \xrightarrow{Tr} H^1(X-S, {}_pA)$$

such that the indicated composition above is multiplication by the degree of $W/X-S$, which is $(G: G(p))$. But multiplication by the integer $(G: G(p))$, which is prime to p, is an automorphism of the p-abelian group $H^1(X-S, {}_pA)$. Thus it suffices to show that $H^1(W, {}_pA)$ is finite. But ${}_pA$ is now a locally constant $\mathbb{Z}/p$-vector space sheaf over W, which is trivialized by a Galois extension of degree p^r. By the well-known fact (CL, Chapter IX, 1, Theorem 2) that every representation of a p-group on a nontrivial vector space of characteristic p contains the identity representation, we obtain that the sheaf ${}_pA$ over W admits a composition series all factors of which are the constant sheaf $\mathbb{Z}/p$. Thus it suffices to show that $H^1(W, \mathbb{Z}/p)$ is finite. But this latter group just classifies Galois p-extensions of the field of fractions of W which are unramified at all primes of W, and there are, to be sure, only a finite number of such extensions.

Since $H^1(\tilde{X}, A)$ is of cofinite type, we have that $H^1(\tilde{Y}, A)^\Gamma$ is of cofinite type, after (i). Thus $H^1(Y, A)$ is Γ-cofinite. To see the exact sequence asserted in (iii), we need only use (3.2), (6.2) and (i). Q.E.D.

Using the terminology of § 2(a), let $f(L/K, \gamma; t) = f(L/K, A; t)$ denote the characteristic polynomial of $H = H_{(Y/X, A)}$, and refer to it as the *characteristic polynomial of the admissible pair* $(Y/X, A)$.

When is H of finite corank? One might hope, ultimately, to show this to be true in some broad context. Nevertheless, we obtain from the above proposition and the theory of Γ-modules, the following corollary:

Corollary 6.9. *If both $A(K)$ and the p-primary component of $Ш(K)$ are finite, then H is of finite corank.*

A necessary and sufficient condition for H to be of finite corank is that for some n, the rank of $A(K_n)$ equals the rank of $A(K_{n+1})$ and the corank of the p-primary component of $Ш_n$ equals the corank of $Ш_{n+1}$.

Proof. To check that H is of finite rank, it suffices to know that H^Γ is finite. After Proposition 6.4(iii) this latter assertion is equivalent to our first hypotheses. To see the second assertion of the above corollary, one need only note:

Corollary 6.10. *H is of finite corank if and only if the rank of $A(K_n)$ and the corank of $Ш_n$ are bounded from above, independently of n.*

Proof. Again, Proposition 6.4 and the $\mathscr{C}$-exact sequence (6.5).

If the rank of $A(K_n)$ is bounded it is natural to ask the sharper question: Are the groups $A(K_n)$ stationary, for large n? Or, equivalently, is the group of rational points $A(L)$ finitely generated?

Proposition 6.11. *Suppose $(Y/X, A)$ is admissible, and H is of finite corank. Then the group of rational points $A(L)$ is finitely generated if and only if its torsion subgroup $A(L)_{\text{tors}}$ is finite.*

Proof. One way is clear. Now suppose $g=$order of $A(L)_{\text{tors}}$. Let n be large enough so that

$$\text{rank}(A(K_n))=\text{rank}(A(K_n))$$

$$^{\#}\{A(L)_{\text{tors}}\}=^{\#}\{A(K_n)_{\text{tors}}\}$$

for all $m \geqq n$.

Since we have the above equality of ranks, after our hypothesis and (6.10) for any m and any $x \in A(K_m)$, there is an integer h (depending upon m) such that $hx \in A(K_n)$. We shall show that we can always take $h=g$ and this will prove our proposition. We know $A(K_n)=A(K_m)^{\Gamma_n}$. Fix γ a topological generator of Γ. Since $\gamma(hx)=hx$, we have $\gamma(x)=x+e$ with $he=0$. Thus e is a torsion element of $A(K_m)$, so $ge=0$, and hence $\gamma(gx)=gx$. Q.E.D.

When is $A(L)_{\text{tors}}$ a finite group? Using the results of (i) Shimura-Taniyama [65] and (ii) Serre [60, 61] we have:

Proposition 6.12. *$A(L)_{\text{tors}}$ is finite if either:*

(i) *A is an abelian variety with complex multiplication* ([65, 63]), *and L/K is the cyclotomic Γ-extension.*

(ii) *A is an elliptic curve possessing no complex multiplication over $\mathbb{C}$.*

Proof of (i). As usual, if $M=M_\ell$ denotes the points of order a power of ℓ in $A(\bar{K})$, where ℓ is a prime, we let

$$T_\ell=\varprojlim_r \ell^r(M); \qquad V_\ell(A)=V_\ell=T_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

Then T_ℓ is a free $\mathbb{Z}_\ell$-module of rank $2g$, and

$$M_\ell \cong \varinjlim_r T_\ell/\ell^r. \tag{6.13}$$

We shall recall some of the theory of complex multiplication drawing much of our terminology from ([60]). If $\dim(A)=g$, and

$$i\colon E \to \mathrm{End}_K A \otimes \mathbb{Q}$$

is an imbedding of a number field of degree $2g$, we say that A has "complex multiplication by E".

Let B denote the ring of integers in E, and set $B' = B \cap \mathrm{End}_K A$. We have that B' is of finite index in B. $E = B' \otimes_{\mathbb{Z}} \mathbb{Q}$. Regard M_ℓ as a B'-module via the natural operation of $\mathrm{End}_K A$. Let the subscript ℓ denote tensoring with $\mathbb{Z}_\ell$. We obtain a natural B'_ℓ-module structure on M_ℓ, and T_ℓ.

Find a free B_ℓ-module of rank 1, $T_\ell^+ \subset V_\ell$ which contains T_ℓ as a subgroup of finite index. This is possible, since V_ℓ is a free E_ℓ-module of rank 1 ([63], Theorem 5(i)) and T_ℓ is a $\mathbb{Z}_\ell$-sublattice in V_ℓ.

Define: $M_\ell^+ = \varinjlim_r T_\ell^+/\ell^r$, and we have that there is a natural surjective homomorphism of B'_ℓ-modules, $M_\ell \to M_\ell^+$ with finite kernel. Also, $M_\ell^+ \approx E_\ell/B_\ell$ as a B_ℓ-module.

Lemma 6.14. *If ℓ does not divide $[B:B']$ then $B_\ell = B'_\ell$, and $M_\ell \approx E_\ell/B_\ell$, as B_ℓ-modules.*

Proof. This follows from the fact that T_ℓ is torsion free over B_ℓ, which is a finite product of discrete valuation rings, and V_ℓ is free of rank one over E_ℓ.

The ring E_ℓ splits into a product of fields, and we have the corresponding splitting for B_ℓ:

$$\begin{aligned} E_\ell &= \prod_i E_{\ell,i} \\ B_\ell &= \prod_i B_{\ell,i} \end{aligned} \tag{6.15}$$

where the $B_{\ell,i}$ are the rings of integers in the fields $E_{\ell,i}$.

The operation of the Galois group $G_K = \mathrm{Gal}(\bar{K}/K)$ on M_ℓ is via a homomorphism,

$$\rho_\ell\colon G_K \to B_\ell'^* \subset B_\ell^* = \prod_i B_{\ell,i}^*$$

where $B_\ell'^*$ operates on M_ℓ through the B'_ℓ-module space structure of M_ℓ. (This assertion is Corollary 2 of [63].)

Consider $S_\ell = \rho_\ell(G_L) \subset B_\ell^*$. To prove case (i) of our proposition, we must show that the fixed subgroups $(M_\ell)^{S_\ell}$ are finite for all primes ℓ, and trivial for almost all primes ℓ. The properties of S_ℓ which will assure this are given in the following lemma:

Lemma 6.16. *Let $S \subset B'^*_\ell$. Then,*

(a) $(M_\ell)^S$ *is trivial if ℓ does not divide $[B:B']$ and $S = B^*_\ell$.*

(b) $(M_\ell)^S$ *is finite if the projection $S \to B^*_{\ell,i}$ is nontrivial for all i.*

Proof. To see (a), just use Lemma 6.14, and note that the assertion holds for the B_ℓ-module E_ℓ/B_ℓ.

To see (b), use the short exact sequence,

$$0 \to C \to M \to M^+ \to 0$$

where C is of finite cardinality, to note that $(M_\ell)^S$ is finite if and only if $(E_\ell/B_\ell)^S$ is finite. Letting S_i denote the projection of S to $B_{\ell,i}$, we have

$$(E_\ell/B_\ell)^S = \prod_i (E_{\ell,i}/B_{\ell,i})^{S_i}.$$

But, if there is an element $s_i \neq 1$ in S_i, then the i-th factor on the right is finite, for multiplication by $s_i - 1$ has a finite kernel in $E_{\ell,i}/B_{\ell,i}$.

It remains, then, to show:

Lemma 6.17.

(a) $S_\ell = B^*_\ell$ *for all but a finite number of primes ℓ.*

(b) $S_\ell \to B^*_{\ell,i}$ *is nontrivial for all ℓ and all i.*

Proof. Since it suffices to check this for K replaced by any larger field, we may suppose that K contains $E(\zeta_p)$. Let D be the ring of integers in K.

A fundamental fact due to Shimura-Taniyama [65] and paraphrased in [60] (II-27, Theorem 2) may be further paraphrased as follows:

Consider the composition,

$$\eta\colon\ D^*_\ell \xrightarrow{a} I/I^0 \xrightarrow{r} G_K^{ab} \xrightarrow{\rho_\ell} B^*_\ell$$

where I is the ideal class group of K and I^0 is its connected component. If we let $\alpha\colon D^*_\ell \to I$ denote the natural inclusion, the map a is given by $a(x) = \alpha(x^{-1})$. The map r is the reciprocity map ψ_K as given in ([12], p. 173). Then:

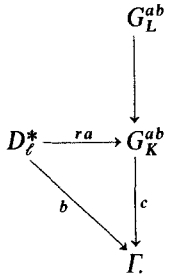
(6.18) For all ℓ there is a subgroup $\tilde{D}^*_\ell \subset D^*_\ell$ which is open of finite index such that $\eta\colon \tilde{D}^*_\ell \to B^*_\ell$ is induced from the canonical norm map $D_\ell \to B_\ell$.

Moreover we may take $\tilde{D}^*_\ell = D^*_\ell$ for all but a finite number of primes ℓ.

One obtains the above quite easily from ([60], II-27, Theorem 2) by taking $\tilde{D}^*_\ell = D^*_\ell \cap U_{\mathfrak{m}}$, where $\mathfrak{m}$ is the modulus guaranteed to exist by loc. cit., Theorem 1.

Now suppose $\ell \neq p$. Since Γ is a pro-p-group and D_ℓ^* has an open pro-ℓ-subgroup of finite index, the map b below is trivial. Consequently the image of D_ℓ in G_K^{ab} actually lies in the image of G_L^{ab}:

(6.19)



Consequently S_ℓ contains $\eta(D_\ell^*)$. But for those primes such that

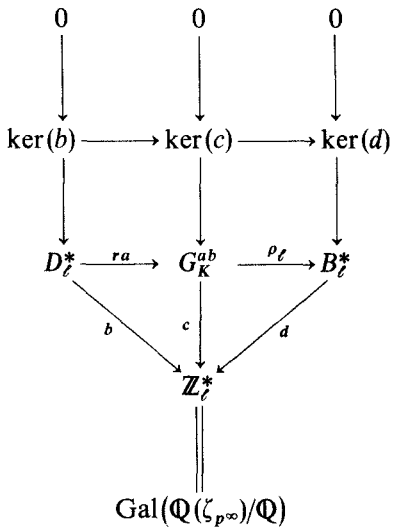
1. $\tilde{D}_\ell^* = D_\ell^*$,
2. E/K is unramified for all primes dividing ℓ,
3. ℓ doesn't divide $[B:B']$,

the map η which is the semi-local norm map by (6.18) is surjective.

Since all but a finite number of ℓ's satisfy 1), 2) and 3) above, we have established part (a) of our lemma. Whether or not ℓ satisfies these conditions, $\eta(\tilde{D}_\ell^*)$ is an open subgroup of B_ℓ^* of finite index, since the image of D_ℓ^* under the norm map is open of finite index. Consequently S_ℓ, which contains $\eta(D_\ell^*)$ is open of finite index. It therefore satisfies the requirement of part (b) of our lemma.

We must now consider $\ell = p$. Let us consider the diagram,

(6.20)



where we have identified $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$ with $\mathbb{Z}_\ell^*$ in the canonical manner. The map c of (6.20) is just the composition of the map c of (6.19) with the canonical inclusion of $\Gamma = \mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}(\zeta_p))$ in $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$. The map d is just the norm mapping. The only circuit in (6.20) whose commutativity is in question is the left-hand lower triangle. But its commutativity follows from the well-known fact that $\wedge^g V_\ell(A) \approx V_\ell(\mathbb{G}_m)$, as $\mathrm{Gal}(\bar{K}/K)$-modules. From the above diagram we see that S_ℓ contains the image of $\ker(b)$ in B_ℓ^*. But also from the above diagram we see that the image of $\ker(b)$ is of finite index in $\ker(d)$, since the norm of D_ℓ^* is of finite index in B_ℓ^*. Thus S_ℓ contains a group of finite index in $\ker(d)$. Since d is the norm mapping, one checks that $\ker(d)$ maps to a subgroup of infinite order in $B_{\ell,i}^*$ for each i. Thus S_ℓ satisfies the condition of part (b) of our lemma. Q.E.D.

Proof of (ii). Now suppose A is an elliptic curve with no complex multiplications (over $\mathbb{C}$). We have the exact sequence of Galois groups:

$$1 \to G_L \to G_K \to \Gamma \to 1. \tag{6.21}$$

From ([61], see introduction) we have that ℓ-adic representation induced by A is a homomorphism $G_K \to \mathbf{GL}(2, \mathbb{Z}_\ell)$ which is surjective for almost all ℓ and whose image is open for all ℓ. It follows that the image of G_L is open for all $\ell \neq p$ since Γ is a pro-p-group and $\mathbf{GL}(2, \mathbb{Z}_\ell)$ is a pro-ℓ-group. Consequently the ℓ-torsion points ${}_{\ell^\infty}A(L)$ are finite for every $\ell \neq p$. Our proposition will be concluded if we show (1) that ${}_\ell A(L) = 0$ for almost all ℓ and (2) that ${}_{p^\infty}A(L)$ is finite. To see (1), consider the exact sequence,

$$1 \to H \to G_K \to \mathbf{PGL}(2, \mathbb{Z}/\ell)$$

where the second homomorphism is composition with the natural projection. Let N be the image of H in Γ. We have:

$$1 \to G_L/G_L \cap H \to G_K/H \to \Gamma/N \to 1.$$

But for almost all ℓ, $G_K/H = \mathbf{PGL}(2, \mathbb{Z}/\ell)$, which contains a simple subgroup of index 2 for $\ell \geqq 5$ ([8], Chapter XX). This tells us that $G_L \to \mathbf{PGL}(2, \mathbb{Z}/\ell)$ is surjective for almost all ℓ.

To see (2), one need only count dimensions of Lie algebras. For by (6.21) above, the Lie algebra of the image of G_L in $\mathbf{GL}(2, \mathbb{Z}_p)$ is at least 3. But if ${}_{p^\infty}A(L)$ were infinite, its dimension could be no greater than 1.

We might also have reasoned directly from ([61], 4.4, Cor. 2).

Corollary 6.22. *Let $(Y/X, A)$ be admissible. Suppose A is of dimension one, and either: Y/X is the cyclotomic extension, or A has no complex*

multiplications. Suppose A has only a finite number of rational points over K and the p-primary component of its Shafarevitch-Tate group over K is finite. Then we have the following refinement of (6.9), (6.10):

The group of rational points $A(L)$ is finitely generated.

§ 7. Arithmetic Duality and the Functional Equation

a) $\mathscr{B}$-Acyclicity

Fix a Γ-extension: $\cdots \to X_n \to X_{n-1} \to \cdots \to X$. Say that a sheaf F over X is $\mathscr{B}$-acyclic if the sequence of p-primary components of $H^1(X_n, F)$ is $\mathscr{B}$-isomorphic to zero (§1, (b)). We may define, similarly, the notions of $\mathscr{B}$-injectivity, $\mathscr{B}$-surjectivity, and $\mathscr{B}$-isomorphism, for a morphism of sheaves $f: E \to F$. Such a morphism clearly induces a $\mathscr{B}$-injection, $\mathscr{B}$-surjection, or $\mathscr{B}$-isomorphism (resp.) on p-primary components of H^1. A sheaf F killed by multiplication by a nonzero integer n is clearly $\mathscr{B}$-acyclic, and, for any sheaf, the map $F \xrightarrow{n} F$, given by multiplication by n is a $\mathscr{B}$-isomorphism. For example, turning to the exact sequences (3.3) for large r, we have that all maps in the central square below are $\mathscr{B}$-isomorphisms.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & {}_{p^r}A & \longrightarrow & A & \longrightarrow & \bar{A} & \longrightarrow & 0 \\ & & & & \downarrow & \searrow^{p^r} & \downarrow & & \\ 0 & \longrightarrow & \bar{A} & \longrightarrow & A & \longrightarrow & \bar{F} & \longrightarrow & 0. \end{array}$$

Now let A be a Néron model over X with nondegenerate reduction on $X-S$. Thus $A/X-S$ is an abelian scheme. Consider the abelian scheme $A'/X-S$ dual to $A/X-S$ (e.g. [45], p. 118). We may extend this to a Néron model A' on all of X. Consider a polarization $\eta: A/X-S \to A'/X-S$ ([45], Chapter 6, § 2). Since A is smooth over X, the functorial property of Néron models (§ 3) assures us that η extends to a morphism $\eta: A \to A'$, over X. A second use of the functorial property shows that η is a homomorphism of groups schemes over X. We shall refer to η *as a polarization of* A/X.

Lemma 7.1. *A polarization $\eta: A \to A'$ is a $\mathscr{B}$-isomorphism.*

Proof. We may find a polarization $\gamma: A' \to A$ such that both compositions $\gamma\eta$ and $\eta\gamma$ are multiplication by an integer n on A and A' respectively.

b) Arithmetic Duality

Let Z be the spectrum of the ring of integers in a number field. M. Artin and I expect to publish, in the near future, a proof of the

Arithmetic flat duality theorem [5][1]. It has the following two theorems as corollaries:

Proposition 7.2. *Let G be a finite flat commutative (affine) group scheme over Z, and let G' denote its Cartier dual. Then the cup-product pairing, defined by Yoneda product:*

$$H^r(Z, G) \times H^{3-r}(Z, G') \to \mathbb{Q}/\mathbb{Z}$$

is a nondegenerate pairing on the p-primary components of the groups involved, for all r, and all odd primes p. If Z is totally complex, it is a nondegenerate pairing on 2-primary components as well. All the groups involved are finite.

Proposition 7.3. *Let A, A' be Néron models over Z which are dual abelian varieties over the generic point of Z. Let p be a prime such that A (and hence A', as well) has nondegenerate reduction at all $q \in Z$ which divide p. Suppose either that p is odd, or Z totally complex. Then the natural cup-product pairing,*

$$H^r({}_{p^\nu}A) \times H^{3-r}({}_{p^\nu}A') \to \mathbb{Q}/\mathbb{Z}$$

is nondegenerate for all r, ν.

Remarks. 1. (7.3) is closly related (for $r=1$) to the pairing introduced by Cassels [11], and to the pairing of [68].

2. The degeneracy of the above pairings, when $p=2$ and Z is not totally complex, may be analyzed. Left and right kernels are $\mathscr{C}$-trivial sequences in ν.

Let us consider, now, Néron models A, A' over $Z=X$, which satisfy the hypotheses of (7.3) for the prime p.

We have the $\mathscr{C}$-exact, $\mathscr{C}$-sequences coming from (3.3):

$$0 \to H^{r-1}(X_n, A) \otimes \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{h} H^r(X_n, \tilde{A}) \to {}_{p^\infty}H^r(X_n, A) \to 0$$

(as sequences in n).

If $\eta: A \to A'$ is a polarization, we have the $\mathscr{B}$-isomorphism,

$$\tilde{\eta}: H^r(X_n, \tilde{A}) \to H^r(X_n, \tilde{A}').$$

[1] This theorem is related to the Etale arithmetic duality theorem of Artin-Verdier [6], and to the local arithmetic duality theorem [40, 41]. In fact, these last two results are ingredients of the proof of the duality theorem.

We may put this into a commutative diagram, of cohomology groups over X_n:

$$\begin{array}{ccccccc} 0 & \longrightarrow & A(X_n)\otimes \mathbb{Q}_p/\mathbb{Z}_p & \longrightarrow & H^1(\tilde{A}) & \longrightarrow & {}_{p^\infty}H^1(A) \longrightarrow 0 \\ & & & & \downarrow{\scriptstyle \tilde{\eta}} & & \downarrow{\scriptstyle \sigma} \\ (7.4) & & & & H^1(\tilde{A}') & & \\ & & & & \downarrow{\scriptstyle d} & & \\ & & & & \varinjlim_{v} H^2({}_{p^v}A)^* & \xrightarrow[h]{} & \varinjlim_{v}({}_{p^\infty}H^1(A)/p^v)^* \end{array}$$

where d is the duality isomorphism coming from (7.3), and the bottom horizontal arrow, h, is induced from the h of the $\mathscr{C}$-exact short exact sequence above, for $r=2$. It remains to justify the existence of σ. Note that the right lower group is $({}_{p^\infty}H^1(A)/\mathrm{div})^*$ which is a finite group.

By the top horizontal line, and the fact that $A(X_n)\otimes\mathbb{Q}_p/\mathbb{Z}_p$ is divisible, one sees that

$$H^1(\tilde{A})/\mathrm{div} \xrightarrow[\mathscr{C}]{\approx} {}_{p^\infty}H^1(A)/\mathrm{div}. \tag{7.5}$$

Thus the composition $h\,d\tilde{\eta}$ factors mod $\mathscr{B}$ through ${}_{p^\infty}H^1(A)$, giving the $\mathscr{B}$-morphism σ:

$${}_{p^\infty}H^1(X_n, A)/\mathrm{div} \xrightarrow{\sigma} ({}_{p^\infty}H^1(X_n, A)/\mathrm{div})^*. \tag{7.6}$$

Since h is a $\mathscr{C}$-surjection, and $\tilde{\eta}$ a $\mathscr{B}$-isomorphism, the morphism σ of (7.6) is a $\mathscr{B}$-surjection. Since ${}_{p^\infty}H^1(X_n, A)/\mathrm{div}$ is finite, a glance at (7.4) shows that (7.6) is also a $\mathscr{B}$-injection. Thus (7.6) is a $\mathscr{B}$-isomorphism, which yields, after (7.6), the $\mathscr{B}$-isomorphism,

$$H^1(X_n, \tilde{A})/\mathrm{div} \xrightarrow[\mathscr{B}]{\approx} (H^1(X_n, \tilde{A})/\mathrm{div})^*. \tag{7.7}$$

That is, we have (2.4) a $\mathscr{B}$-nondegenerate self-pairing on $H = H_{(Y/X, A)}$.

Corollary 7.8. *If $(Y/X, A)$ is admissible (and $H = H_{(Y/X, A)}$ is of finite corank) its characteristic polynomial satisfies a functional equation of the form*

$$f(t) = \varepsilon \cdot t^\lambda f(1/t).$$

Proof. After (7.7) we may apply (2.9).

§ 8. Calculation for General Primes

a) Over Cyclotomic Bases

Let A be an abelian variety of dimension one, over $\mathbb{Q}$. Fix a rational odd prime p, and let $K=\mathbb{Q}(\zeta_p)$, $L=\mathbb{Q}(\zeta_{p^\infty})$. Let L/K give rise to the global cyclotomic Γ-extension which we shall denote $Y(p)/X(p)$. We

shall study the Γ-modules that arise,

$$H = H(p) = H_{(Y(p)/X(p),\, A)}.$$

Recall [31] that there is a natural identification of $\Delta = \mathrm{Gal}(K/\mathbb{Q})$ with the $(p-1)$-st roots of 1 in the ring $\mathbb{Z}_p$ obtained by sending $g \in \Delta$ to the unique $(p-1)$-st root of 1 in $\mathbb{Z}_p$, u, satisfying:

$$g(\zeta_p) = (\zeta_p)^u.$$

One has a natural operation of Δ on H, which commutes with the Γ-module structure of H. Recall that any action of Δ on a p-abelian group M decomposes ([31], § 3) into a direct sum of eigenspaces,

$$M = \bigoplus_{j=0}^{p-2} {}^{(j)}M$$

where the action of $u \in \Delta$ on ${}_jM$ is given by multiplication by u^j.

We have

$$H = \bigoplus_{j=0}^{p-2} {}^{(j)}H, \tag{8.1}$$

this being a direct sum decomposition of Γ-modules. The $\mathscr{B}$-non-degenerate bilinear pairing (7.8) on H puts ${}^jH$ in duality with ${}^{(p-1-j)}H$.

We may identify the eigenspace: $j=0$ in (8.1) with the Γ-module $H_{(Y/X,\, A)}$ coming from the cyclotomic Γ-extension $\mathbb{Q}_\infty/\mathbb{Q}$ associated to the prime p. Thus

$$H = H_{(Y/X,\, A)} \oplus \bigoplus_{j=1}^{p-2} {}^{(j)}H.$$

Proposition 8.2. *Suppose A is neither singular nor supersingular at p. The natural map,*

$${}^{(j)}H^1(X(p), \tilde{A}) \to [{}^{(j)}H(p)]^\Gamma$$

is surjective if either:

(i) $j \neq 0$,

(ii) $j=0$, $a_p \not\equiv 1 \bmod p$ $(a_p = Tr(\mathrm{Frob}_p))$.

Proof. This will follow by considering the j-eigenspaces of the groups occuring in the diagram (6.6), and noting that

$${}^{(j)}H^2(X(p)_p, \tilde{A}) \to {}^{(j)}H^2(Y(p)_p, \tilde{A}) \tag{8.3}$$

is injective in each of the above cases, as may be seen by the following argument: $A(K) \to A(k)$ admits a lifting of the p-part of $A(k)$ because $A(\mathbb{Q}) \to A(k)$ does (5.11), and there is no residue field extension at p. Therefore (5.7) applies, telling us that the kernel of

$H^2(X, \tilde{A}) \to H^2(Y, \tilde{A})^\Gamma$ $(X = \mathrm{Spec}(Z)$, Y/X the cyclotomic Γ-extension), maps isomorphically onto the kernel of

$$H^2(X(p), \tilde{A}) \to H^2(Y(p), \tilde{A})^\Gamma$$

by comparison of the explicit description of the two kernels given by (5.9) and (5.15). Thus if $j \neq 0$ it follows that (8.3) is injective and hence by (6.4)(ii) the map of our proposition is surjective. The remaining case (ii) of our proposition comes from (5.16)(i).

The interest of our proposition is that in the two cases listed in (8.2) one has criteria for the vanishing of the j-eigenspace of $H(p)$, (8.4) below, which are in close analogy to the classical criteria for the vanishing of the j-eigenspace of the Γ-modules of ideal class groups of cyclotomic fields, considered by Iwasawa. The curious difference occurs only when $j=0$ (i.e., when we consider the Γ-extension $\mathbb{Q}_\infty/\mathbb{Q}$) and when we limit ourselves to the rather rare set of primes p such that $a_p \equiv 1 \bmod p$. In fact, for such primes we shall show that $H(p)$ is necessarily of infinite order! ((8.5) below.)

Corollary 8.4. *If* ${}^{(j)}H^1(X(p), \tilde{A})=0$ *in either of the cases* (i), (ii) *of* (8.2), *then* ${}^{(j)}H(p)=0$.

b) Over $\mathbb{Q}$

In this section we let Y/X denote the Γ-extension over $X=\mathrm{Spec}(\mathbb{Z})$, associated to the prime p. Let $H=H(p)$ stand for the Γ-module $H^1(Y, \tilde{A})$.

Proposition 8.5. *Let A be any abelian variety of dimension one over $\mathbb{Q}$, and p a rational odd prime such that A has good reduction at p, there is no nontrivial rational point in $A(\mathbb{Q})$ of order p, and $a_p \equiv 1 \bmod p$. Then the abelian group $H(p)$ is of infinite order. That is, either $A(\mathbb{Q}_\infty)$ is of infinite order, or ${}_{p^\infty}Ш(\mathbb{Q}_\infty)$ is.*

Proof. If $a_p \equiv 1 \bmod p$, then A is ordinary at p. Suppose the conclusion of (8.5) false. Since $H^1(X_n, \tilde{A})$ is controlled, it must then be $\mathscr{C}$-trivial. Thus $A(\mathbb{Q}_n)$ is finite for all n, and ${}_{p^\infty}Ш(\mathbb{Q}_n)$ is $\mathscr{C}$-trivial. It follows from the Kummer theory of A that, for fixed n, $H^1(X_n, {}_{p^\nu}A)$ is a $\mathscr{C}$-trivial sequence, regarded as a sequence in ν.

Since $A/\mathbb{Q}$ is of dimension one, it is self-dual. Therefore, since p is odd, (7.3) tells us that $H^1(X_n, {}_{p^\nu}A)$ and $H^2(X_n, {}_{p^\nu}A)$ are Pontrjagin duals of one another. Thus $H^2(X_n, {}_{p^\nu}A)$ is also $\mathscr{C}$-trivial, regarded as a sequence in ν.

Recall that if H is a discrete Γ-module and M its Pontrjagin dual, regarded as a Λ-module, and $\gamma \in \Gamma$, a topological generator, the module $M/(1-\gamma)M$ is the Pontrjagin dual of H^Γ. For our calculation below, we adopt the terminology $\overline{M}=M/(1-\gamma)M$, and since all cohomology groups will have as coefficient sheaf $\tilde{A}$, we drop the symbol $\tilde{A}$ from our terminology.

Denote the Pontrjagin dual of $H^1(Y-p_\infty)$ by the letter N. Recall that (5.12) the Pontrjagin dual of $H^2(Y_{p_\infty})$ is a free Λ-module on one generator. Let us identify that module with Λ. Thus the Pontrjagin dual

of the exact sequence of Γ-modules,

$$0 \to H(p) \to H^1(Y - p_\infty) \to H^2(Y_{p_\infty}) \tag{8.6}$$

may be written:

$$0 \leftarrow N/\varphi\Lambda \leftarrow N \leftarrow \Lambda \tag{8.7}$$

where φ is the image of $1 \in \Lambda$.

The first thing that we shall claim about the structure of N is that it admits a homomorphism to Λ with finite cokernel,

$$N \xrightarrow{f} \Lambda \to C \to 0. \tag{8.8}$$

There is, in fact, a natural map from N to a free Λ-module on one generator, as follows: If M is a Λ-module of finite type, let $M^\sim$ denote $\mathrm{Hom}_{\mathbb{Z}_p}(M, \Lambda)$. Then $M^\sim$ is endowed naturally with the structure of a Λ-module. (It is denoted M^* in [52].) We have a natural map $M \xrightarrow{f} M^{\sim\sim}$. $M^{\sim\sim}$ is easily seen to be a reflexive Λ-module ([52], 174-08) and ([52], Lemma 6, 174-09) all reflexive Λ-modules are free. It is shown in ([52], Lemma 5) that f has finite cokernel. In fact it has a section mod $\mathscr{C}$, and the kernel of f is the maximal Λ-torsion submodule of M.

To establish (8.8), then, it suffices to show that the rank of $M^{\sim\sim}$ as a free Λ-module is exactly one. But this rank λ can be detected as the unique integer to enjoy the property that

$$\mathrm{corank}\left(H^1(Y - p_\infty)^{\Gamma_n}\right) - \lambda p^n \tag{8.9}$$

is bounded. But if we rewrite the diagram (6.6) in our situation,

$$\begin{array}{ccccccccc}
 & & & & 0 & & 0 & & \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & \tilde{A}(L)_{\Gamma_n} & \longrightarrow & E_n & & \\
 & & & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & H^1(X_n) & \longrightarrow & H^1(X_n - p_n) & \longrightarrow & H^2(X_{n,p_n}) & \longrightarrow & H^2(X_n) \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & H^1(Y)^{\Gamma_n} & \longrightarrow & H^1(Y - p_\infty)^{\Gamma_n} & \longrightarrow & H^2(Y_{p_\infty})^{\Gamma_n} & & \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & 0 & & 0 & &
\end{array} \tag{8.10}$$

and recall that the groups $\tilde{A}(L)_{\Gamma_n}, H^1(X_n), H^2(X_n)$, are finite in our situation, and that we have already computed the corank of $H^2(X_{n,p_n})$, (5.3), one gets;

$$\text{corank}\left(H^1(Y-p_\infty)^{\Gamma_n}\right)=p^n \tag{8.11}$$

which indeed tells us (8.8).

Let us now consider the above diagram, for $n=1$. In (8.12) below we rewrite the Pontrjagin dual of a portion of it. Recall that $\tilde{A}(L)_\Gamma$ has the same order as $\tilde{A}(\mathbb{Q})$, and is therefore trivial, since $A(\mathbb{Q})$ contains no element of order p. Also, the right hand vertical line may be written as case (ii) of (5.16), since $a_p \equiv 1 \bmod p$:

(8.12)

$$\begin{array}{ccc} \overline{N} & \xleftarrow{\sigma - 1} & \mathbb{Z}/p \oplus \mathbb{Z}_p \\ \uparrow & & \uparrow \\ = & & \\ \uparrow & & | \\ \overline{N} & \xleftarrow{\quad} & \mathbb{Z}_p . \end{array}$$

The right-hand vertical arrow can be taken to be the map sending 1 to $0 \oplus p \cdot 1$ (5.16)(ii), and from (8.12) we deduce that the image of φ in $\overline{N}$ is divisible by p. Consequently from (8.8) we get that $\varphi' = f(\varphi)$ is divisible by p in Λ. Consequently φ' is a non-unit in Λ. From (8.8) we learn that

$$N/\varphi\Lambda \to \Lambda/(\varphi') \tag{8.13}$$

has finite cokernel. But the quotient of Λ by any proper principal ideal has infinite order. Thus $\Lambda/(\varphi')$ has infinite order, and after (8.13), N/φ has infinite order. Q.E.D.

Of course, if $A(\mathbb{Q})$ is infinite, we haven't learned much from proposition (8.5). However, if $A(\mathbb{Q})$ is finite, and we restrict attention to those primes p such that $H^1(X, \tilde{A})$ vanishes, we get a finer calculation:

Proposition 8.14. *Let A be a Néron model over* Spec$(\mathbb{Z})$ *such that $A(\mathbb{Q})$ is finite. Let p be an odd prime satisfying these conditions:*

(i) *A has nondegenerate, ordinary reduction at p.*

(ii) *p doesn't divide the order of $A(\mathbb{Q})_{\text{tors}}$.*

(iii) *The p-primary component of $Ш(\mathbb{Q})$ vanishes.*

Then:

(a) *If $a_p \not\equiv 1 \bmod p$, $H(p)$ is trivial (actually, not just* mod $\mathscr{C}$*).*

(b) *If $a_p \equiv 1 \bmod p$,*

the following facts are true about $H(p)$: It is a group of infinite order, and of finite corank. Its Pontrjagin dual must be isomorphic, mod $\mathscr{C}$*, to a*

Λ-module of one of these types:

1) $\Lambda/(\beta)$,

2) $\Lambda/(\beta^2)$,

3) $\Lambda/(\beta)\oplus\Lambda/(\rho)$

where β and ρ are irreducible (nonunit) elements in Λ.

Remarks. If we make a choice of a topological generator of Γ, we may identify Λ with $\mathbb{Z}_p[[T]]$, and then β, ρ may be identified with power series. Since they are determined only up to units in this ring, let us agree to take them as Weierstrass-prepared polynomials. Since they are irreducible, this boils down to two possibilities: The constant polynomial p, or a monic Eisenstein polynomial in $T=t-1$. We may, after these conventions, speak of them as unique polynomials. The characteristic polynomial $f_p(t)$ of $H(p)$, with respect to the same choice of generator of Γ, is just β, β^2, or $\beta\rho$, and, of course, the last sentence in our proposition says that f_p is either irreducible, or expressible as a product of two irreducibles.

Since we already know that f_p satisfies a functional equation, we have a further restriction on the kinds of β and ρ that can occur.

I wonder whether case 2) ever occurs, if $\beta \neq p$. If it does occur, we would have that the representation of Γ on the associated $\mathbb{Q}_p$-vector space of $H(p)$ would not be semi-simple. A particularly ugly situation would be if case 2) occurred with $\beta(t)$ equal to the irreducible polynomial of a p^ν-th root of one. It would be ugly because an analogue (in this p-adic realm) of certain conjectures of Birch and Swinnerton-Dyer, and of Tate, would then be false. Also, the sequence ${}_{p^\infty}Ш(\mathbb{Q}_n)$ would not be controlled.

Proof of Proposition 8.14. Our hypotheses gives us (using 3.3) that $H^1(X, {}_{p^\nu}A)=0$ for all ν. By self-duality of ${}_{p^\nu}A$, and (7.3), we get that $H^2(X, {}_{p^\nu}A)=0$ for all ν. Consequently we have that

$$H^1(X, \tilde{A})=H^2(X, \tilde{A})=0,$$

and the diagram (8.10) simplifies to give:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E & \longrightarrow & H^2(X_p) & \longrightarrow & H^2(Y_{p_\infty})^\Gamma & \longrightarrow & 0 \\ & & \| & & \| & & \| & & \\ 0 & \longrightarrow & H^1(Y)^\Gamma & \longrightarrow & H^1(Y-p_\infty)^\Gamma & \longrightarrow & H^2(Y_{p_\infty})^\Gamma & \longrightarrow & 0. \end{array} \tag{8.15}$$

Case (a). The hypotheses on p tell us that we are in Case (i) of (5.16), and so $E_n=0$. By (8.15), $H^1(Y)^\Gamma=0$, giving that $H^1(Y)=0$. This proves (a). We may also glean from (8.10) the further fact that

$${}_{p^\infty}Ш(\mathbb{Q}_n)\approx \tilde{A}(L)_{\Gamma_n}.$$

Case (b). This is a sharpening of the assertion of the previous proposition. To show that the Pontrjagin dual of $H(p)$, denoted $N/\varphi\Lambda$ in (8.7) above has one of the three listed forms, we shall give a finer analysis of the structure of N.

Lemma 8.16. *Let N be a Λ-module which is not a Λ-torsion module, and such that $\bar{N} = \mathbb{Z}/p \oplus \mathbb{Z}_p$. Then there are three possibilities:*

(i) *$N \approx \Lambda \oplus C$, where C is finite.*

(ii) *$N \approx \Lambda \oplus \Lambda/\psi$, where ψ is an irreducible element in Λ.*

(iii) *N is isomorphic to an ideal $I \subset \Lambda$ such that $(I, 1-\gamma)$ is the maximal ideal, for any topological generator, $\gamma \in \Gamma$.*

Proof of Lemma 8.16. For any such N, $N^{\sim\sim}$ is a free Λ-module of rank one, and so we have the diagram (8.8). Consider, first, the case where f in (8.8) is surjective. Since Λ is free, we have $N = \Lambda \oplus R$, and since $\bar{N} = \bar{\Lambda} \oplus \bar{R}$, we get $\bar{R} = \mathbb{Z}/p$. It follows that R is generated over Λ by one element, so we may write $R = \Lambda/J$ where J is a nontrivial ideal. If J is not principal, then it is primary to the maximal ideal, and we have that R is finite, and therefore N is of the form described in (i) above. If J is principal, generated by ψ, then $\bar{R} = \mathbb{Z}/p$ implies that ψ is irreducible, giving us case (ii).

We may suppose, therefore, that f is not surjective. The image of f is then a proper ideal $I \subset \Lambda$. Since Λ/I is finite, I is primary to the maximal ideal. If R is the kernel of f, we get an exact sequence,

$$0 \to \bar{R} \to \bar{N} \to \bar{I} \to 0,$$

since I is torsion-free as a Λ-module. By our hypothesis, $\bar{N}$ is isomorphic to $\mathbb{Z}/p \oplus \mathbb{Z}_p$, and therefore $\bar{I}$ is a quotient of this latter group. $\bar{I}$ is of infinite order, since I is a nontrivial torsion-free Λ-module. Moreover, $\bar{I}$ cannot be $\mathbb{Z}_p$, because then I would be a principle ideal, contradicting the fact that it is primary to the maximal ideal. This leaves only one last possibility: $\bar{I}$ is isomorphic to $\mathbb{Z}/p \oplus \mathbb{Z}_p$, and consequently, the map $\bar{N} \to \bar{I}$ is an isomorphism, and $\bar{R} = 0$. But then $R = 0$.

Thus we have identified N with I. To conclude that I is of the form described in (iii), we must show that $\overline{\Lambda/I}$ is isomorphic with $\mathbb{Z}/p$.

Consider the standard resolution of the Λ-module $\mathbb{Z}_p$,

$$0 \to \Lambda \xrightarrow{1-\gamma} \Lambda \to \mathbb{Z}_p \to 0.$$

This yields,

$$0 \to \mathrm{Tor}_\Lambda^1(\mathbb{Z}_p, \Lambda/I) \to \Lambda/I \to \Lambda/I \to \overline{\Lambda/I} \to 0,$$

and since Λ/I is finite, the orders of the two extreme groups above are equal.

But we also have the exact sequence,

$$0 \to \mathrm{Tor}_\Lambda^1(\mathbb{Z}_p, \Lambda/I) \to \bar{I} \to \bar{\Lambda} \to \overline{\Lambda/I} \to 0$$

which is evaluated as,

$$0 \to \mathrm{Tor}_\Lambda^1(\mathbb{Z}_p, \Lambda/I) \to \mathbb{Z}/p \oplus \mathbb{Z}_p \to \mathbb{Z}_p \to \overline{\Lambda/I} \to 0.$$

Since the two extreme groups in the above exact sequence have equal orders, it follows that $\overline{\Lambda/I} \approx \mathbb{Z}/p$. Q.E.D.

Now we may get on with the proof of (b). From (5.16)(ii) and (8.15) we see that $\overline{N}$ is isomorphic to $\mathbb{Z}/p \oplus \mathbb{Z}_p$, and the image of φ may be taken to be $0 \oplus p$. Lemma (8.16) applies, and we have that $M = N/\varphi$ give, in case (i), (ii) of the lemma, that M is isomorphic to Λ-modules of type 1), 3) in our proposition. If we are in case (iii) of the lemma, then M is isomorphic mod $\mathscr{C}$ to Λ/φ', and since $\overline{\Lambda/I}$ is $\mathbb{Z}/p$, the image of φ' in $\bar{\Lambda}$ must be equal to p^2 times a generator. Thus φ' is a product of two irreducibles in Λ, and we obtain either case 2) or 3) of our proposition. Q.E.D.

Remark. In the course of the above we have given some information concerning the cohomology groups $H^1(Y - p_\infty, \tilde{A})$ as Γ-modules. To record it, Lemma 8.16 tells us:

Corollary 8.17. *Let $X = \mathrm{Spec}\ \mathbb{Z}$, A an elliptic curve such that $A(\mathbb{Q})$ is finite. Let p be an odd prime number satisfying* (i)–(iii) *of* (8.14).

Then the Λ-module N which is the Pontrjagin dual of $H^1(Y - p_\infty, \tilde{A})$ is isomorphic to one of three types:

(i) *$\Lambda \oplus C$ where C is finite.*

(ii) *$\Lambda \oplus \Lambda/\psi$ where ψ is an irreducible element in Λ.*

(iii) *An ideal I in Λ such that $(I, 1-\gamma)$ is the maximal ideal, for any topological generator, $\gamma \in \Gamma$.*

I have no further information concerning the structure of $H^1(Y - p_\infty, \tilde{A})$. Do all three types occur?

c) The Set of Anomalous Primes of an Elliptic Curve

For A an abelian variety over $\mathbb{Q}$ of dimension one, let us define the set of *anomalous* primes p of A, $\Sigma(A)$, to be the set of primes p such that A has nondegenerate reduction at p, and $a_p \equiv 1 \bmod p$. $\Sigma(A)$ depends only on the isogeny class of A over $\mathbb{Q}$. We have already seen that for those primes of $\Sigma(A)$ not dividing the order of the torsion subgroup of $A(\mathbb{Q})$, either $A(\mathbb{Q}_\infty)$ or ${}_{p^\infty}Ш(\mathbb{Q}_\infty)$ is of infinite order. How many primes p are in $\Sigma(A)$?

We first show, if $A(\mathbb{Q})$ contains a nontrivial element of finite order, that $\Sigma(A)$ is easily found, and somewhat uninteresting.

Lemma 8.18. *If $A(\mathbb{Q})$ contains a nontrivial element of finite order then $\Sigma(A)$ consists either of a single element, or none, or else is contained in the set* $\{2, 3, 5\}$.

Proof. Let s denote an element in $A(\mathbb{Q})$ of prime order, $s^q = 1$. Let p be a prime at which A has good reduction, and $a_p \equiv 1 \bmod p$. The Riemann hypothesis tells us that either $a_p = 1$ or $p = 2, 3$, or 5 and $a_p = 1 - p$. Thus if $a_p \equiv 1 \bmod p$, the number of rational points of A, mod p, is either p or $2p$, and the latter possibility may occur only if $p = 2, 3$, or 5. If we denote again by A the Néron model of A over $\mathrm{Spec}(\mathbb{Z})$, and let G denote the finite flat sub-group scheme of A generated by the section s, we have that G is a finite flat group scheme over $\mathrm{Spec}(\mathbb{Z})$ of order q, possessing a nontrivial section. But $\mu_{2,\mathrm{Spec}\,\mathbb{Z}}$ is the only nonconstant such group scheme. Therefore we learn that s reduces to a nontrivial rational point of order q, modulo p, provided that either p or q differs from 2.

Suppose $q \neq p$. Then the reduction of A modulo p possesses nontrivial rational solutions of order q, and of order p. Hence the number of rational solutions is divisible by qp, hence equal to $2p$, and thus: $q = 2$, $p = 2$, 3, or 5. Consequently, if p is different from 2, 3, or 5, then $q = p$. We have proven (i), and obtained the more precise information: If the torsion subgroup of $A(\mathbb{Q})$ is of composite order, then $\Sigma(A)$ is empty, or consists in $\{3\}$ or $\{5\}$. If it is of prime order q for $q > 5$, then $\Sigma(A)$ is $\{q\}$ or is empty, depending upon whether A has nondegenerate reduction at q.

Lemma 8.19. *Given any finite set of primes P, there is an abelian variety A of dimension one defined over $\mathbb{Q}$, such that $\Sigma(A)$ contains P.*

Proof. By results of Deuring, or more generally, [27, 70], one may find an elliptic curve over the prime field $\mathbb{F}_p$ which possesses exactly p rational points over $\mathbb{F}_p$. Write out these curves as plane cubic curves, for every $p \in P$. One obtains thereby a finite number of homogeneous plane cubic forms with coefficients in the prime fields $\mathbb{F}_p$ for $p \in P$. Now find a homogeneous plane cubic form with integral coefficients, which reduces to each of the described forms modulo p for each $p \in P$. This gives us an elliptic curve whose Jacobian A has the desired property.

Also, if P contains more than three primes, we have that $A(\mathbb{Q})$ is a free abelian group, by (8.18), and therefore Proposition 8.5 applies to them.

§ 9. Some Calculations in the Spirit of the Classical "First Majorization"

It is worth reviewing the classical method of p-descent in terms of the theory of finite flat group schemes over Spec $\mathbb{Z}$, and the $fpqf$ topology, for one often gets the finest results without having to work too hard at the "bad" primes.

We shall concentrate on a tame case. Suppose that A is a Néron model (of dimension 1) over Z, the spectrum of the ring of integers in

a number field K. Let p be a prime such that A has semi-stable reduction at all points of Z of residual characteristic p.

Consider the quasi-finite flat subgroup-scheme ${}_pA$ which is the kernel of multiplication by p in A. For each closed point $s \in Z$, one has

$$({}_pA)_s \cong {}_p(A_s)$$

by associativity of fiber product. Drop the parenthesis and denote the fiber at s by ${}_pA_s$. After our hypothesis, ${}_pA_s$ is a finite group scheme over $s \in S$, and

$$\mathrm{ord}({}_pA_s) \leqq p^2.$$

Definition. *The defect of ${}_pA$ at s is the integer t_s $(0 \leqq t_s \leqq 2)$ such that*

$$\mathrm{ord}({}_pA_s) = p^{(2-t_s)}.$$

It is clear that one has $t_s = 0$ if A has good reduction at s, and $t_s \leqq 1$, if A has multiplicative reduction at s. In this latter case, $t_s = 0$ if and only if p divides the number of components of A_s. This condition is also equivalent to requiring that p divides $\mathrm{ord}_q \Delta$ [48].

We will say that s is a *defective point* for ${}_pA$ if $t_s > 0$. Let T be the set of defective points for ${}_pA$. It is a finite set contained in the set of primes of bad reduction for A. By definition, the *defect* of ${}_pA$ is the integer

$$t = \sum_{s \in T} t_s.$$

The following proposition follows from the above discussion:

Proposition 9.1. *${}_pA$ is a finite (flat) group scheme over Z if and only if its defect is 0. If A is semi-stable, then the defect of ${}_pA$ consists in the number of primes q such that p does not divide $\mathrm{ord}_q \Delta$. Consequently, if A is semi-stable, ${}_pA$ is a finite flat group scheme over Z if and only if (Δ) is a p-th power.*

a) Divisibility by $\mathbb{Z}/p$ and by μ_p

Suppose that $A(K)$ possesses a nontrivial point of order p. One obtains a monomorphism of K-groups:

$$(\mathbb{Z}/p)_K \hookrightarrow A_K.$$

Since $\mathbb{Z}/p$ is smooth over Z, the universal property of the Néron model insures the existence of a morphism over Z,

$$\varphi\colon \mathbb{Z}/p \to {}_pA.$$

The image of φ (i.e. the scheme-theoretic closure of $(\mathbb{Z}/p)_K$) is a finite flat subgroup G of ${}_pA$. Here one is using that Z is the spectrum of a Dedekind domain.

Lemma. *When* $Z = \operatorname{Spec} \mathbb{Z}$,

$$G = \mathbb{Z}/p \qquad \text{if } p \neq 2$$
$$G = \mathbb{Z}/2, \quad \text{or} \quad {}_1\mu_2 \qquad \text{if } p = 2.$$

Proof. This is an elementary application of the theorem of Oort-Tate [50] which classifies finite flat groups of order p. One uses also the fact that G has a nontrivial section.

It is reasonable, then, to consider the following two cases: (*Divisibility by* ${}_1\mu_p$) there is an injection:

$${}_1\mu_p \hookrightarrow {}_pA.$$

(*Divisibility by* $\mathbb{Z}/p$) there is an injection

$$\mathbb{Z}/p \hookrightarrow {}_pA.$$

Note that (if A has good reduction at the primes of characteristic p) the above cases are put in correspondence, one to another, by Cartier duality.

Let $j\colon Z - T \to Z$ be the natural immersion, and:

$$(\mathbb{Z}/p)_! = j_! j^*(\mathbb{Z}/p)$$
$${}_1\mu_{p!} = j_! j^*({}_1\mu_p).$$

Proposition 9.2. *Let* $Z = \operatorname{Spec} \mathbb{Z}$. *In the cases of divisibility by* ${}_1\mu_p$ *and by* $\mathbb{Z}/p$, *one has, respectively, the exact sequences:*

$$0 \to {}_1\mu_p \to {}_pA \to (\mathbb{Z}/p)_! \to 0$$
$$0 \to \mathbb{Z}/p \to {}_pA \to {}_1\mu_{p!} \to 0.$$

Proof. The quotient of ${}_pA$ by ${}_1\mu_p$ (resp., by $\mathbb{Z}/p$) is representable, for we are trying to divide by a finite flat subgroup over Z, and the orbit of every point under the action of this subgroup is contained in an open affine (cf. [39], théorème 1). Let M (resp., N) denote this quotient. By computing orders, we see that M (resp., N) is finite and flat over $Z - T$, and $M_s = N_s = 0$, for all $s \in T$.

Making use, again, of the classification theorem of Oort-Tate [50], we may deduce that if $p \neq 2$, or if $\{2\} \notin Z - T$:

$$M_{|Z-T} \cong (\mathbb{Z}/p)_{|Z-T}$$
$$\hat{N}_{|Z-T} \cong (\mathbb{Z}/p)_{|Z-T} \quad \text{and therefore} \quad N_{|Z-T} = {}_1\mu_{p,\,Z-T}.$$

In the remaining case where $p = 2$, and $\{2\}$ is not a defective point, we must have, by our hypothesis, that A has semistable reduction at 2, and we can deduce the above equalities, as well. The proposition follows.

When is ${}_pA$ expressible as the direct sum

$$ {}_pA \cong \mathbb{Z}/p \oplus \mu_p ? $$

Proposition 9.3. *Let $Z = \operatorname{Spec} \mathbb{Z}$, and A, p as above. Suppose that ${}_pA$ has zero defect. Suppose that either ${}_pA$ is divisible by μ_p and $p \neq 2$, or ${}_pA$ is divisible by $\mathbb{Z}/p$ and p is a regular prime. Then*

$$ {}_pA \cong \mathbb{Z}/p \oplus \mu_p . $$

Remark. The restriction that p be a regular prime is hardly a very restrictive one, for the only known instances of the phenomenon of "divisibility" are for $p = 2, 3, 5, 7$.

Proof. Suppose divisibility by μ_p. Since the defect is zero, by the previous proposition we have that ${}_pA$ is a finite flat group over Z which is an extension of $\mathbb{Z}/p$ by μ_p. We shall show that $\operatorname{Ext}_Z(\mathbb{Z}/p, \mu_p) = 0$. For this, use the sequence:

$$ 0 \to H^0(Z, \mu_p) \to \operatorname{Ext}_Z(\mathbb{Z}/p, \mu_p) \to H^1(Z, \mu_p) \to 0 $$

and the fact that the two flanking groups are zero, if $p > 2$, and $Z = \operatorname{Spec}(\mathbb{Z})$.

Now *suppose divisibility by* $\mathbb{Z}/p$. Again we shall show that

$$ \operatorname{Ext}_Z(\mu_p, \mathbb{Z}/p) = 0 . $$

Let T denote the underlying scheme of μ_p over Z. The natural map,

$$ \operatorname{Ext}_Z(\mu_p, \mathbb{Z}/p) \to H^1(T, \mathbb{Z}/p) $$

is an inclusion, since μ_p is connected (over Z) and $\mathbb{Z}/p$ is constant. Therefore it would suffice to show that $H^1(T, \mathbb{Z}/p)$ vanishes. Since T is the spectrum of $\mathbb{Z}[x]/(x^p - 1)$, it contains two closed subschemes T_0, T_1, corresponding to the two projections

$$ T_0 : \begin{array}{c} \mathbb{Z}[x]/(x^p - 1) \to \mathbb{Z} \\ x \mapsto 1 \end{array} $$

$$ T_1 : \begin{array}{c} \mathbb{Z}[x]/(x^p - 1) \to \mathbb{Z}[\zeta_p] \\ x \to \zeta_p \end{array} . $$

The fibre product of the T_i in T is isomorphic to $\operatorname{Spec}(\mathbb{Z}/p)$ and the union of the T_i's is T.

Since the constant group scheme $\mathbb{Z}/p$ is smooth, it suffices to compute cohomology for the étale topology. But $H^1(T_0, \mathbb{Z}/p) = 0$ because $\mathbb{Z}$ is a principal ideal domain, and $H^1(T_1, \mathbb{Z}/p) = 0$ because p is a regular prime. It follows, after an elementary computation in étale cohomology that $H^1(T, \mathbb{Z}/p) = 0$. Q.E.D.

b) The Calculations

Fix $Z = \operatorname{Spec} \mathbb{Z}$, p a prime, A a Néron model of dimension 1 over Z which has semi-stable reduction at p. Suppose we are either in the case of divisibility by $\mathbb{Z}/p$ or by μ_p.

Let T be the set of defective points. Let F be the cokernel sheaf of p: $A \to A$. If V is a vector space over $\mathbb{F}_p$, let $[V]$ denote $\dim_{\mathbb{F}_p} V$. All cohomology groups considered will be flat cohomology over Z. We will have use for the following symbols:

t = the defect of ${}_pA = \operatorname{card}(T)$,

t' = the number of points of T of characteristic $\equiv 1 \bmod p$,

m = the number of points of Z where A has bad reduction,

a = the number of points of Z where A has additive reduction,

ρ = the rank of $A(\mathbb{Q})$,

$\delta = [{}_pA(\mathbb{Q})]$,

$f_s = [H^0(s, F)] = [H^1(s, F)]$,

$f = [H^0(F)] = [H^1(F)] = \sum_s f_s$,

$\tau = [{}_p Ш]$,

$h = [H^1({}_pA)]$.

Inequalities (9.4)

(a) $\delta \leqq 2$, *and if* $p > 2$, *then* $\delta \leqq 1$.

(b) $\tau \leqq [{}_pH^1(A)]$ *and equality holds if* $p > 2$, *and* $f = 0$.

(c) $t + f \leqq a + m$, *and more precisely:*

(i) $t_s + f_s = 0$ *if* A *has good reduction at* s,

(ii) $t_s + f_s = 1$ *if* A *has multiplicative reduction at* s,

(iii) $t_s + f_s \leqq 2$ *if* A *has additive reduction at* s.

Proofs of the Inequalities. (a) The assertion $\delta = 2$ is equivalent to saying that all p^2 points of order p in A are rational over $\mathbb{Q}$. This can only happen if $p = 2$, because the Galois module of points of order p is self-dual under Cartier duality.

(b) By the proposition of the appendix the odd primary components of $Ш$ are given by the image of $H^1(A^0)$ in $H^1(A)$.

(c) Assertion (i) is clear. Thanks to the hypotheses made about A and p, one has: $A_s^0/(A_s^0)^p = 0$, giving us an exact sequence:

$$0 \to {}_pA_s^0 \to {}_pA_s \to {}_p\Phi_s \to 0.$$

But

$$p^{f_s} \leqq \#({}_p\Phi_s)$$

and

$$\#({}_pA_s^0)=p \quad \text{if } A \text{ has multiplicative reduction at } s$$
$$=0 \quad \text{if } A \text{ has additive reduction at } s.$$

Therefore

$$\#({}_pA_s)\geqq p^{f_s+1},$$

if A has multiplicative reduction at s which proves (c)(ii), and

$$\#({}_pA_s)\geqq p^{f_s},$$

if A has additive reduction at s, which proves (c)(iii).

Proposition 9.5. *We shall suppose divisibility by either $\mathbb{Z}/p$ or μ_p. In the case of divisibility by μ_p,*

$$h-\delta=t-1. \tag{9.5a}$$

In the case of divisibility by $\mathbb{Z}/p$,

$$h-\delta=t'-1-\varepsilon, \tag{9.5b}$$

with $\varepsilon=0$, except for $p=2$. If $p=2$, and if there exists a defective point s of residual characteristic not congruent to 1 mod 4, *then $\varepsilon=1$.*

Proof. To begin, I shall state without proof the values of the higher cohomology groups of $\mathbb{Z}/p$ and μ_p over $\operatorname{Spec}\mathbb{Z}$. For the calculations see [39].

$$H^i(\mathbb{Z}/p)=0 \quad \text{for } i=1,2$$
$$H^1(\mu_p)=0 \quad \text{if } p\neq 2$$
$$=\mathbb{Z}/2 \quad \text{if } p=2 \text{ (the nontrivial } \mu_2\text{-torseur being represented by } \operatorname{Spec}(\mathbb{Z}[\sqrt{-1}]))$$
$$H^2(\mu_p)=0.$$

Proof of (9.5a). From the exact sequence

$$0\to\mu_p\to {}_pA\to(\mathbb{Z}/p)_!\to 0$$

and from the fact that $H^2(\mu_p)=0$, one obtains a six-term exact sequence:

$$0\to H^0(\mu_p)\to H^0({}_pA)\to H^0((\mathbb{Z}/p)_!)\to H^1(\mu_p)\to H^1({}_pA)\to H^1((\mathbb{Z}/p)_!)\to 0.$$

From the results recalled above, we have:

$$[H^1(\mu_p)]-[H^0(\mu_p)]=0$$

and therefore:

$$[H^1({}_pA)]-[H^0({}_pA)]=[H^1((\mathbb{Z}/p)_!)]-[H^0((\mathbb{Z}/p)_!)]. \tag{9.6}$$

The left-hand side is precisely $h-\delta$. To calculate the right-hand side, consider

$$0 \to (\mathbb{Z}/p)_! \to \mathbb{Z}/p \to (\mathbb{Z}/p)_. \to 0$$

where $(\mathbb{Z}/p)_.$ is the skyscraper sheaf whose support is T.

The long cohomological sequence gives:

$$0 \to H^0((\mathbb{Z}/p)_!) \to H^0(\mathbb{Z}/p) \to H^0((\mathbb{Z}/p)_.) \to H^1((\mathbb{Z}/p)_!) \to 0$$

from which one deduces that the right-hand side of (9.6) is $t-1$.

Proof of (9.5 b). From the exact sequence

$$0 \to \mathbb{Z}/p \to {}_pA \to \text{Ш}_{p!} \to 0$$

and the fact that $H^i(\mathbb{Z}/p)=0$ for $i=1, 2$, one obtains:

$$0 \to H^0(\mathbb{Z}/p) \to H^0({}_pA) \to H^0(\text{Ш}_{p!}) \to 0$$

$$H^1({}_pA) \xrightarrow{\approx} H^1(\text{Ш}_{p!})$$

giving:

$$\delta = [H^0(\text{Ш}_{p!})] + 1$$

$$h = [H^1(\text{Ш}_{p!})]$$

and consequently,

$$h-\delta = [H^1(\text{Ш}_{p!})] - [H^0(\text{Ш}_{p!})] - 1.$$

Consider the exact sequence

$$0 \to \text{Ш}_{p!} \to \text{Ш}_p \to \text{Ш}_{p.} \to 0$$

where $\text{Ш}_{p.}$ is the skyscraper sheaf $\bigoplus_{s \in T} \text{Ш}_{p,s}$.

Notice that, in the case of divisibility by $\mathbb{Z}/p$, the point $s=\{p\}$ cannot be defective. For if it were, ${}_pA_s$ would be isomorphic to $(\mathbb{Z}/p)_s$, which is impossible, because, since A has multiplicative reduction at s, ${}_pA^0_{\bar{s}}$ is isomorphic to $\text{Ш}_{p,\bar{s}}$. Therefore, the morphism $\text{Ш}_{p!} \to \text{Ш}_p$ is an open immersion, and $\text{Ш}_{p.}$, regarded as an algebraic space over $\mathbb{Z}$ is étale.

We shall begin by proving (9.5 b) if $p \neq 2$. Since $H^i(\text{Ш}_p)=0$ for $i=0, 1$, the above short exact sequence gives

$$H^0(\text{Ш}_{p!})=0$$

$$H^0(\text{Ш}_{p.}) \cong H^1(\text{Ш}_{p!}).$$

But

$$H^0(\text{Ш}_{p.}) = \bigoplus_{s \in T} H^0(s, \text{Ш}_{p,s}) = (\mathbb{Z}/p)^{t'}$$

because

$$H^0(s, \text{Ш}_{p,s}) = 0 \quad \text{if the characteristic of } s \text{ is } \not\equiv 1 \bmod p$$

$$= \mathbb{Z}/p \quad \text{otherwise.}$$

Our result is then:

$$[H^1(\mu_{p^1})]=t'$$

and we obtain (9.3 b) with $\varepsilon=0$.

When $p=2$, one must consider the exact sequence:

$$0\to H^0(\mu_{2^1})\to H^0(\mu_2)\to H^0(\mu_{2^\cdot})\to H^1(\mu_{2^1})\to H^1(\mu_2)\xrightarrow{\lambda} H^1(\mu_{2^\cdot})$$

giving:

$$[H^1(\mu_{2^1})]-[H^0(\mu_{2^1})]=\ker(\lambda)-[H^0(\mu_2)]+[H^0(\mu_{2^\cdot})].$$

But $[\ker(\lambda)]=1$ if there does not exist a defective point s such that the μ_2-torseur $\mathrm{Spec}\,\mathbb{Z}[\sqrt{-1}]$ is nontrivial at s. Otherwise $\ker(\lambda)=0$. But, the μ_2-torseur $\mathrm{Spec}(\mathbb{Z}[\sqrt{-1}])$ is nontrivial at s if and only if the characteristic of s is not congruent to 1 mod 4.

This establishes (9.5 b).

Proposition 9.7. *Under the hypotheses of* (9.5),

$$\rho+\delta+\tau\leqq h+f$$

(with equality, if $p>2$, and $f=0$).

Proof. Break the Kummer sequence,

$$0\to {}_pA\to A\xrightarrow{p} A\to F\to 0$$

into two short exact sequences,

$$0\to {}_pA\to A\xrightarrow{p}\bar{A}\to 0$$

$$0\to \bar{A}\to A\to F\to 0$$

giving the following commutative diagram of cohomology groups:

$$\begin{array}{ccccccccccccc}
0\to & H^0({}_pA) & \to & H^0(A) & \xrightarrow{p} & H^0(\bar{A}) & \xrightarrow{\mu} & H^1({}_pA) & \to & H^1(A) & \xrightarrow{p} & H^1(\bar{A}) & \to\cdots \\
 & & & \downarrow p & (1) & \downarrow & & & & \downarrow p & (2) & \downarrow & \\
0\to & H^0(\bar{A}) & \to & H^0(A) & \xrightarrow{\nu} & H^0(F) & \to & H^1(\bar{A}) & \to & H^1(A) & & & \to\cdots
\end{array}$$

Set

$$[\mathrm{Im}\,\mu]=h_1,\qquad [\mathrm{cok}\,\mu]=h_2$$

$$[\mathrm{Im}\,\nu]=f_1,\qquad [\mathrm{cok}\,\nu]=f_2$$

and therefore:

$$h_1+h_2=[H^1({}_pA)]=h$$

$$f_1+f_2=[H^0(F)]=f.$$

From the square labelled (1) we deduce: $\delta+\rho=h_1+f_1$. From the square labelled (2) we deduce: $[{}_pH^1(A)]\leqq h_2+f_2$.

From the inequality $\tau \leqq [{}_pH^1(A)]$, one obtains

$$\rho + \delta + \tau \leqq h + f.$$

If $f = 0$, the $F = 0$, and $\bar{A} = A$. Returning to the above exact sequences one may deduce: $\rho + \delta + [{}_pH^1(A)] = h$.

Moreover, if $p > 2$, then (appendix) $\tau = [{}_pH^1(A)]$, giving

$$\rho + \delta + \tau = h. \quad \text{Q.E.D.}$$

Proposition 9.8. *In the case of divisibility by* μ_p,

$$\rho + \tau \leqq t + f - 1. \tag{9.8a}$$

In the case of divisibility by $\mathbb{Z}/p$,

$$\rho + \tau \leqq t' + f - \varepsilon - 1, \tag{9.8b}$$

where ε *is either* 0 *or* 1, *as defined in* (9.3).

Proof. Combine (9.5) and (9.7).

Putting (9.4) and (9.8) together, one has the following useful estimate:

Theorem 9.9. *Under the hypotheses of* (9.5),

$$\rho + \tau \leqq a + m - 1.$$

If one is in the case of divisibility by $\mathbb{Z}/2$ *and if there is a defective point for* ${}_2A$ *of residual characteristic* $\not\equiv 1 \bmod 4$, *then:*

$$\rho + \tau \leqq a + m - 2.$$

Corollary 9.10. *Suppose that A has prime conductor (i.e.* $a + m = 1$*). Suppose that we are in the case of divisibility by* $\mathbb{Z}/p$ *or by* μ_p. *Then* $A(\mathbb{Q})$ *is finite and the p-primary component of Ш is zero.*

Corollary 9.11. *In the case of divisibility by* $\mathbb{Z}/2$, *suppose that there is a defective point s for* ${}_2A$, *of residual characteristic* $\not\equiv 1 \bmod 4$. *Suppose, further that* $a + m \leqq 2$. *Then, again,* $A(\mathbb{Q})$ *is finite, and the 2-primary component of Ш vanishes.*

c) Examples

Our methods apply to a large number of the known curves of low conductor. For example, we may deduce that all the curves in the following table possess only a finite number of rational points (over $\mathbb{Q}$), and the p-primary component of *Ш* vanishes:

Table 1

Conductor	Equation	Δ	p	Divisibility	f	t	t'	ε
11	$y^2+y=x^3-x^2$	-11	5	$\mathbb{Z}/5$	0	1	1	0
11	$y^2+y=x^3-x^2-10x-20$	-11^5	5	$\mathbb{Z}/5\oplus\mu_5$	1	0	0	0
11	$y^2+y=x^3-x^2-7820x-263580$	-11	5	μ_5	0	1	1	0
14	$y^2+xy+y=x^3+4x-6$	$-2^6 7^3$	3	$\mathbb{Z}/3\oplus\mu_3$	1	0	0	0
15	$y^2+xy+y=x^3+x^2$	$-3\cdot 5$	2	$\mathbb{Z}/2$	0	2	2	1
17	$y^2+xy+y=x^3-x^2-x$	17	2	$\mathbb{Z}/2$	0	1	1	0
19	$y^2+y=x^3+x^2-9x-15$	-19^3	3	$\mathbb{Z}/3\oplus\mu_3$	1	0	0	0
20	$y^2=x^3+x^2+4x+4$	$-2^8\cdot 5^2$	3	$\mathbb{Z}/3$	1	1	0	0
21	$y^2+xy=x^3+x$	$-3^2\cdot 7$	2	$\mathbb{Z}/2$	1	1	1	1
26	$y^2+xy+y=x^3-x^2-3x+3$	$-2^7\cdot 13$	7	$\mathbb{Z}/7$	1	1	0	0
26	$y^2+xy+y=x^3-5x-8$	$-2^3\cdot 3^3$	3	$\mathbb{Z}/3\oplus\mu_3$	1	0	0	0
35	$y^2+y=x^3+x^2+9x+1$	-35^3	3	$\mathbb{Z}/3\oplus\mu_3$	1	0	0	0
37	$y^2+y=x^3+x^2-23x-50$	37^3	3	$\mathbb{Z}/3\oplus\mu_3$	1	0	0	0

Remarks. The first three entries in the above table represent a complete isogeny class over $\mathbb{Q}$. The remaining entries are not isogenous to one another.

Much of the information of the table has been culled from the lists of curves of low conductor compiled by Swinnerton-Dyer. These are soon to be published. See also [36]. In the cases where I assert divisibility by $\mathbb{Z}/p\oplus\mu_p$, I have used (9.3).

Concerning the only nonsemi-stable curve in the table ($N=20$), I used that it has:

(a) additive reduction of type $C6$ at $p=2$, giving $f_2=1, t_2=0$,

(b) multiplicative reduction of type $B2$ at $p=5$, giving $f_5=0, t_5=1$, but $t'_5=0$ (cf. [36]).

§ 10. Division by $\mathbb{Z}/p\oplus\mu_p$

A very interesting phenomenon occurs when

$$ {}_pA\cong\mathbb{Z}/p\oplus\mu_p. $$

We shall state the result for Néron models of arbitrary dimension:

Proposition 10.1. *If $(Y/X, A)$ is admissible, and ${}_pA\approx(\mathbb{Z}/p)^g\oplus(\mu_p)^g$ and we denote*

$$ \rho_n=\operatorname{rank}(A(K_n)) $$

$$ \tau_n=[{}_pIII(K_n)], $$

then there is a constant c such that

$$ \rho_n+\tau_n\geqq g((K:\mathbb{Q})/2)\,p^n-c $$

for all n. Consequently, if H is of cofinite rank, its μ-invariant (§2(a)) *is nonzero. In fact,*

$$\mu(H) \geqq g(K:\mathbb{Q})/2.$$

Proof. Use (3.3) for $r=1$ and the base X_n to obtain the following mod $\mathscr{C}$ sequence of groups:

$$0 \to A(K_n)/A(K_n)^p \to H^1(X_n, {}_pA) \to {}_p\text{Ш}(K_n) \to 0.$$

Now use the exact sequence obtained by ordinary Kummer theory:

$$0 \to U(K_n)/U(K_n)^p \to H^1(X_n, \mu_p) \to {}_pH^1(X_n, \mathbb{G}_m) \to 0$$

and the Dirichlet unit theorem for K_n to obtain the asserted lower bound.

Example 1. Consider the family of curves

$$C_d\colon\ x^3+y^3+z^3=dxyz$$

for $d \in \mathbb{Z}$. Let A_d denote the Néron model of C_d.

We may calculate the points of order three (these are all rational over $\mathbb{Z}[\zeta]$) by the following table:

$(0,-1,1)$	$(0,-\zeta,1)$	$(0,-\zeta^2,1)$
$(1,0,-1)$	$(1,0,-\zeta)$	$(1,0,-\zeta^2)$
$(1,-1,0)$	$(1,-\zeta,0)$	$(1,-\zeta^2,0)$

The vertical left-hand column gives us a subgroup scheme of ${}_3A$ over Z isomorphic to the constant group scheme $\mathbb{Z}/3$ over Z. The top right row gives a subgroup scheme isomorphic to μ_3 over Z. This can be seen by using the functorial property of Néron schemes together with the fact that $\mathbb{Z}[\zeta]$ is unramified at primes $p|3$. Thus ${}_3A \approx \mathbb{Z}/3 \oplus \mu_3$.

It follows that the defect of ${}_3A$ vanishes, and therefore (9.8a) $\rho+\tau \leqq f-1$. If we choose $d \in \mathbb{Z}$ such that d^3-3^3 is prime to 3 and square-free, one may show that f (as defined in §9) is simply the number of prime factors of d^3-3^3 which are congruent to 1 mod 3. [An easy excercise shows that, under our assumptions, *any* prime factor of the second term on the right in the formula

$$d^3-3^3=(d-3)(d^2+3d+9)$$

must be congruent to one mod 3.] See [38] for the full details.

Consequently, if we choose d such that $f=1$, we obtain $\rho=\tau=0$, giving:

Proposition 10.2. *Choose an integer d such that d^3-3^3 is prime to* 3, *square-free and has only one prime factor congruent to* 1 mod 3. *Then $A_d(\mathbb{Q})$ is finite, and the* 3*-primary component of $H^1(X, A_d)$ is trivial. If $L/\mathbb{Q}$ is the* 3*-adic Γ-extension, the theory of* §6 *applies: $H^1(X_n, \tilde{A}_d)$ is controlled, $H_{(Y/X, A_d)}$ is of cofinite rank.*

Iwasawa's μ-invariant is nontrivial for $H_{(Y/X, A_d)}$. The order of the 3-primary component of $Ш_n$/Div goes to infinity with n.

Remark. Here are some values for which the above proposition applies: $d=1, \pm 2, 4, -7, 8, -14$. (The values $d=1, \pm 2, 4$ undoubtedly represent curves which are isomorphic to entries in Table 1.) The curve associated to $d=1$ is discussed in [13]. See also [9].

Example 2. Consider the curve

$$y^2+y=x^3-x^2-10x-20.$$

It is the modular curve $X_0(11)$, and the second entry in Table 1. It is easy to see that $(0,0)$ is a point of order 5. It then follows from (9.1) and (9.3) that ${}_5A=\mathbb{Z}/5\times\mu_5$.

One obtains from (9.10) that $A(\mathbb{Q})$ is finite and the 5-primary component of $Ш$ vanishes. It is a consequence of the conjectures of Birch and Swinnerton-Dyer that all of $Ш$ vanishes [66].

Knowing that $A(\mathbb{Q})$ is finite and of order divisible by 5, one can easily see that it is of order 5: Since it has good reduction at 2, and since an elliptic curve over $\mathbb{F}_2$ can have at most 5 rational points, the reduction of $A(\mathbb{Q})$ at $p=2$ is of order 5. Since the kernel of reduction can contain only elements of order 2, it suffices to show that $A(\mathbb{Q})$ has no points of order 2, which is easy enough.

From the proof of (8.18), and the fact that $A(\mathbb{Q})$ is of order 5, we obtain that $a_p \equiv 1 \bmod p$ if and only if $p=5$. Thus, the conjecture that $Ш(\mathbb{Q})=0$ (and the observation that 2 is supersingular implies (8.14a)):

$$H(p)=0 \tag{10.3}$$

for all ordinary primes p such that $p \neq 5$ (and, of course, $p \neq 11$).

The prime $p=5$ is then a quite special prime for A, and we shall give a complete computation of our theory for this prime, independent of any conjectures.

From the fact that $\Delta=-11^5$ we may deduce the structure of the Néron fibre at 11: It is an extension of a finite étale group of order 5 by a group of multiplicative type.

Thus, the Kummer sequence looks like this:

(10.4)

$$\begin{array}{ccccccccc} 0 & \to & \mathbb{Z}/5\times\mu_5 & \longrightarrow & A & \longrightarrow & A^0 & \longrightarrow & 0 \\ & & & & \downarrow & \searrow^{5} & \downarrow & & \\ 0 & \longrightarrow & A^0 & \longrightarrow & A & \longrightarrow & F & \to & 0 \end{array}$$

where F has support at the point of characteristic 11.

The Kummer theory (3.3) for A then yields the exact sequences,

$$
\begin{array}{ccccccccccc}
0 & \longrightarrow & H^0(A^0) & \longrightarrow & H^0(A) & \longrightarrow & \mathbb{Z}/5 & \longrightarrow & H^1(A^0) & \longrightarrow & H^1(A) \\
 & & \downarrow & \searrow^{5} & \downarrow & & & & \downarrow & \searrow^{5} & \downarrow \\
0 & \longrightarrow & \mathbb{Z}/5 & \longrightarrow & H^0(A) & \longrightarrow & H^0(A^0) & \longrightarrow & H^1(A) & \longrightarrow & H^1(A^0) \longrightarrow 0
\end{array}
\tag{10.5}
$$

where cohomology is taken over the base $X=\mathrm{Spec}(\mathbb{Z})$, and we have used the facts $H^r(\mu_5)=H^r(\mathbb{Z}/5)=0$ for $r=1,2$.

From (10.5) we immediately obtain the following facts.

Proposition 10.6. *$H^0(A^0)=0$; $A(\mathbb{Q})\cong\mathbb{Z}/5$; $H^1(A^0)\to Ш(\mathbb{Q})\to H^1(A)$ are isomorphisms; the 5-primary component of $Ш(\mathbb{Q})$ vanishes.*

Corollary 10.7. *$H^1(X,\tilde{A})=0$, where*

$$\tilde{A}=\varinjlim_{5^r} {}_{5^r}A.$$

Proof. From the exact sequence (10.4), we get that

$$H^0(A^0)\to H^1({}_{5^r}A)\to H^1(A)$$

is exact. But the two flanking groups are zero, by (10.6). Q.E.D.

Proposition 10.8. *Let $H=H_{(Y/X,\,A)}$ denote the Γ-module associated to the unique Γ-extension Y/X associated to $p=5$, and our Néron model A of $X_0(11)$. Then the Pontrjagin dual of H is isomorphic to the Λ-module Λ/p. It follows that $A(\mathbb{Q}_\infty)$ is finite, the sequence ${}_{p^\infty}Ш(\mathbb{Q}_n)$ is controlled,*

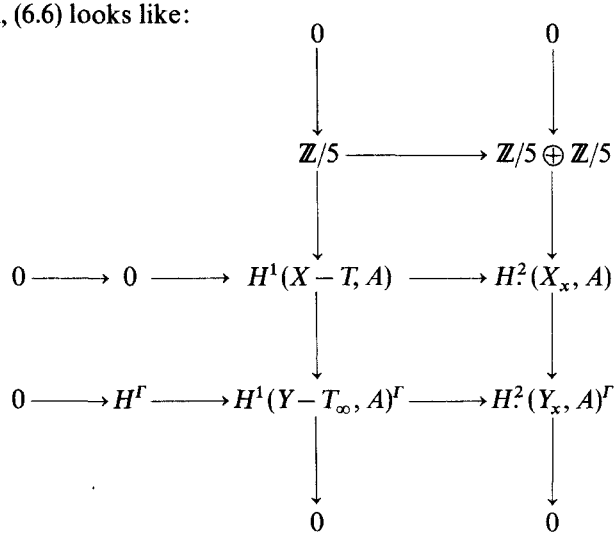
$$H\underset{\mathscr{C}}{\cong}\varinjlim_{n} {}_{p^\infty}Ш(\mathbb{Q}_n),$$

and ${}_{p^\infty}Ш(\mathbb{Q}_n)$ is isomorphic (mod $\mathscr{C}$) *to a vector space over $\mathbb{Z}/p$ of dimension p^n. The characteristic polynomial of H is simply: $f_p=p$.*

Proof. Since ${}_5A\cong\mathbb{Z}/5\times\mu_5$, we learn from (9.1) that Iwasawa's μ-invariant is nonzero for the Γ-module H. Everything will then follow if we show that the order of H^Γ is less than or equal to p. For then it cannot be zero, hence must be p. Hence the Pontrjagin dual of H is a singly generated, irreducible Γ-module whose μ-invariant is nonzero. It must then be isomorphic with Λ/p.

To show $\#(H^\Gamma)\leqq p$ we need only appeal to the diagram (6.6), noting that, since A contains points of order 5, $a_5=1$, and hence we are in Case (ii) of (5.16). Using that $H^1(X,\tilde{A})=0$, and that $A(\mathbb{Q})\cong\mathbb{Z}/5$, the

diagram, (6.6) looks like:



from which our sought estimate is clear. Q.E.D.

Appendix

The Shafarevitch-Tate Group. We shall compare the group *Ш* defined in [67, 68] with the groups $H^1(X, A)$ and $H^1(X, A^0)$.

Let A be an abelian variety over a global field K. Denote by K_v the completion of K with respect to the valuation v. Consider the maps,

$$w_v\colon\ H^1(\mathrm{Spec}(K), A_{/K}) \to H^1(\mathrm{Spec}(K_v), A_{/K_v})$$

and form the two subgroups of $H^1(\mathrm{Spec}(K), A_{/K})$,

$$\Sigma = \bigcap \ker(w_v) \qquad \text{nonarchimedean } v$$
$$Ш = \bigcap \ker(w_v) \qquad \text{all } v.$$

Clearly there is the exact sequence,

$$0 \to Ш \to \Sigma \to \bigoplus_v H^1(\bar{K}_v/K_v; A(\bar{K}_v))$$

the sum on the right being taken over all real archimedean valuations v. Those v for which the topological group $A(\bar{K}_v)$ is connected give no contribution to the right hand summation (Theorem 2.3 of [67]). Thus one sees that $Ш = \Sigma$ if $A(\bar{K}_v)$ is connected for all real valuations v of K, and in any case, the quotient of Σ by *Ш* is a group of exponent 2, of order bounded by the nature of $A_{/K_v}$ for the real valuations v of K.

Let D be the ring of integers of K, $X=\mathrm{Spec}(D)$, j: $\mathrm{Spec}(K)\to X$ the inclusion, and $A_{/\mathrm{Spec}(D)}=A$ the Néron model of $A_{/K}$. Let $0\to A^0\to A\to F\to 0$ be as in §3. Since $A\approx j_*j^*A$ and X is normal, one sees by the remark following the proof of (5.1)(v) that $H^1(X,A)\xrightarrow{i}H^1(\mathrm{Spec}(K),A_{/K})$ is an inclusion.

Proposition. *The inclusion i sends the image of $H^1(X,A^0)\to H^1(X,A)$ isomorphically to Σ.*

Proof. Let I denote the image of $H^1(X,A^0)$ in $H^1(X,A)$. To show that $I\subset\Sigma$, we must show that $I\subset H^1(X,A)$ goes to zero under the diagonal map of the diagram below, where v is any nonarchimedean valuation

$$\begin{array}{ccccc} H^1(X_v,F) & \xleftarrow{\approx} & H^1(X_v,A) & \longrightarrow & H^1(K_v,A) \\ \uparrow & & \uparrow & \nearrow & \uparrow \\ H^1(X,F) & \longleftarrow & H^1(X,A) & \longrightarrow & H^1(K,A). \end{array}$$

But this follows from the indicated isomorphism (which comes from Lang's theorem, [35]) and the fact that I goes to zero in $H^1(X,F)$.

To see that $\Sigma\subset I$, take an element $y\in\Sigma$. Then there is a finite set of primes $S\subset X$ containing all primes of bad reduction for A such that $y\in H^1(X-S,A)$. Consider the diagram,

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^1(X,A) & \longrightarrow & H^1(X-S,A) & \longrightarrow & \bigoplus_{p\in S} H^2(X_p,A) \\ & & \downarrow a & & \downarrow b & & \downarrow \approx \\ 0 & \longrightarrow & \bigoplus_{p\in S} H^1(\hat{X}_p,A) & \longrightarrow & \bigoplus_{p\in S} H^1(K_p,A) & \longrightarrow & \bigoplus_{p\in S} H^2(\hat{X}_p,A) \\ & & \uparrow \approx & & & & \\ & & H^1(X,F) & & & & \end{array}$$

where the horizontal lines are the relative cohomology exact sequence; the zeroes on the left come from (5.1)(v), as does the right-hand vertical isomorphism. The lower left-hand isomorphism comes from (5.1)(v), Lang's theorem [35], and the fact that F has trivial support on $X=S$.

Since $b(y)=0$, y comes from an element in $H^1(X,A)$ which goes to zero in $H^1(X,F)$. Q.E.D.

Remark. We might have made a mild, natural modification of the *fpqf* site X to take into account the archimedean primes. Then we would have had an equality between the image of $H^1(X,A^0)\to H^1(X,A)$ (computed for the modified site X) and the Shafarevitch-Tate group.

References

1. Artin, M.: Auto-duality of the Jacobian. Mineographed notes. Bowdoin Summer Conference in Algebraic Geometry, 1967.
2. [GT] Artin, M.: Grothendieck topologies. Mimeographed notes. Harvard University, 1962.
3. [SGAA] Artin, M., Grothendieck, A.: Séminaire de géometrie algébrique 1963-64. Cohomologie étale des schémas. Mimeographed notes. Institut des Hautes Etudes Scientifiques. Paris.
4. Artin, M., Mazur, B.: Etale homotopy. Lecture Notes in Math. no. 178. Berlin-Heidelberg-New York: Springer 1969.
5. Artin, M., Mazur, B.: Flat arithmetic duality (in preparation).
6. Artin, M., Verdier, J.L.: Etale arithmetic duality. Proceedings of the summer conference in Algebraic Geometry held at Woodshole, Mass. 1965.
7. Birch, B.J., Swinnerton-Dyer, H.P.F.: Notes on elliptic curves I. J. Reine Angew. Math. **212**, 7-25 (1963); II, **218**, 79-108 (1965).
8. Burnside, W.: The theory of groups (2nd Ed.). Cambridge University Press 1911.
9. Cassels, J.W.S.: On a diophantine equation. Acta Arithmetica **6**, 47-52 (1960).
10. Cassels, J.W.S.: Diophantine equations with special reference to elliptic curves. J. London Math. Soc. **41**, 193-291 (1966).
11. Cassels, J.W.S.: Arithmetic on curves of genus one (IV). J. Reine Angew. Math. **211**, 95-112 (1962).
12. Cassels, J.W.S., Fröhlich, A. (eds.): Algebraic number theory. London-New York: Academic Press 1967.
13. Cassels, J.W.S., Sansone, G.: Sur le probleme de M. Werner Mnich. Acta Arithmetica **7**, 187-190 (1961/62).
14. Deligne, P.: Variétés abéliennes ordinaires sur un corps fini. Inventiones math. **8**, 238-243 (1969).
15. [SGAD] Demazure, M., Grothendieck, A.: Schémas en groupes. Séminaire I.H.E.S., 1963-64. Lecture Notes in Math. nos. 151-153. Berlin-Heidelberg-New York: Springer 1970.
16. Eichler, M.: Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktion. Arch. Math. **5**, 355-366 (1954).
17. Greenberg, M.J.: Schemata over local rings. Ann. of Math. **73**, no. 3, 624-648 (1961); II, Ann. of Math. **78**, no. 2, 256-266 (1963).
18. Greenberg, M.J.: Pro-algebraic structure on the rational subgroup of a p-adic abelian variety. Ph. D. thesis. Princeton University 1959.
19. Grothendieck, A.: Sur quelques points d'algèbre homologique. Tohoku Math. J. **9**, 119-221 (1957).
20. [GB III] Grothendieck, A.: Le groupe de Brauer III: exemples et compléments (a continuation of Bourbaki exposés: 290, 297). Published in Dix exposés sur la cohomologie des schémas. Amsterdam: North-Holland Pub. Cie. 1968.
21. Grothendieck, A.: Techniques de déscente et théorèmes d'existence en géometrie algébrique. Séminaire Bourbaki, 12, exp. 195 (1959-60). New York-Amsterdam: Benjamin Inc. 1966.
22. [EGA] Grothendieck, A.: Redigé avec la collaboration de J. Dieudonné, Éléments de géométrie algébrique. Publications Mathematiques, I.H.E.S. 4, 8, 11, 17, 20, 24, 28, 32 Paris (1961-68).
23. [SGA] Grothendieck, A.: Revêtements étales et groupes fondamentaux. Séminaires de Géométrie Algébrique à l'I.H.E.S. (60-61). Lecture Notes in Math. no. 224. Berlin-Heidelberg-New York: Springer 1971.
24. Hardy, G.H., Littlewood, J.E.: Some problems of partitio numerorum III. Acta Math. **44**, 1-70 (1923); reprinted in: G.H.Hardy, Collected papers, vol. 1, Oxford (1966), 561-630.

25. Hasse, H.: Existenz separabler zyklischer unverzweigter Erweiterungskörper vom Primzahlgrade p über elliptischen Funktionenkörpern der Charakteristik p. J. Reine Angew. Math. **172**, 2, 77–85 (1934).
26. Hasse, H., Witt, E.: Zyklischer unverzweigter Erweiterungskörper vom Primzahlgrade p über einem Funktionenkörper der Charakteristik p. Monatshefte für Math. u. Physik **43**, 477–492 (1936).
27. Honda, T.: Isogeny classes of abelian varieties over finite fields. J. Math. Soc. Japan **20**, 83–95 (1968).
28. Igusa, J.: Kroneckerian model of fields of elliptic modular functions. Amer. J. Math. **81**, 561–577 (1959).
29. Iwasawa, K.: On some properties of Γ-finite modules. Ann. of Math. **70**, no. 2, 291–312 (1959).
30. Iwasawa, K.: On Γ-extensions of number fields. Bull. Amer. Math. Soc. **65**, no. 4, 183–226 (1959).
31. Iwasawa, K.: On the theory of cyclotomic fields. Ann. of Math. **70**, no. 3, 530–561 (1959).
32. Iwasawa, K., Sims, C.C.: Computation of invariants in the theory of cyclotomic fields. J. of the Math. Soc. of Japan **18**, nc. 1, 86–96 (1966).
33. Kubota, T., Leopoldt, H.W.: Eine p-adische Theorie der Zetawerte (Teil I). J. Reine Angew. Math. **213**, 228–239 (1964).
34. Lang, S.: Algebraic numbers. Reading, Mass.: Addison-Wesley 1964.
35. Lang, S.: Algebraic groups over finite fields. Amer. J. Math. **78**, no. 3, 555–563 (1956).
36. Ligozat, G.: Fonction L des courbes modulaires. Mimeo. notes. Séminaire Delange-Pisot-Poitou, 1969/70, no. 9. Version to appear: Courbes modulaires de genre 1.
37. Manin, Ju: Cyclotomic fields and modular curves [in Russian]. Uspekhi Mat. Nauk. Tom XXVI **6** (162), 7–71 (1971). Translation to appear in Russian Math. Surveys, London Math. Society.
38. Mazur, B.: Rational points of Abelian varieties with values in towers of number fields. Mimeo. notes, Harvard U. 1969.
39. Mazur, B.: Arithmétique des courbes elliptiques sur les corps cyclotomiques. Mimeographed notes by J.F. Boutot of a course given at Orsay 1970, distributed by I.H.E.S. Paris.
40. Mazur, B.: Local flat duality. Amer. Journal of Math. **92**, 343–361 (1970).
41. Mazur, B., Roberts, L.: Local Euler characteristics. Inventiones math. **9**, 201–234 (1970).
42. Mazur, B., Swinnerton-Dyer, H.P.F.: The p-adic L-series of an elliptic curve (in preparation).
43. Milne, J.S.: Extensions of abelian varieties defined over a finite field. Inventiones math. **5**, 63–84 (1968).
44. Mumford, D.: Lectures on curves on an algebraic surface (with the assistance of G.M. Bergman). Ann. of Math. Studies **59**, Princeton 1966.
45. Mumford, D.: Geometric invariant theory. Ergebnisse Math., Bd. 34. Berlin-Heidelberg-New York: Springer 1965.
46. Mumford, D., Oort, F.: Deformations and liftings of finite commutative group schemes. Inventiones math. **5**, 317–334 (1968).
47. Néron, A.: Modèles mimimaux des variétés abéliennes sur les corps locaux et globaux. Publications Mathematiques, I.H.E.S., no. 21 (1964).
48. Ogg, A.: Elliptic curves and wild ramification. Amer. J. of Math. **89**, 1–21 (1967).
49. Oort, F.: Commutative group schemes. Lecture Notes in Mathematics, no. 15. Berlin-Heidelberg- New York: Springer 1966.
50. Oort, F., Tate, J.: Group schemes of prime order. Ann. Scient. Ec. Norm. Sup., series 4, **3**, 1–21 (1970).
51. Raynaud, M.: Passage au quotient par une relation d'équivalence plate. Proc. of a Conference on Local Fields. Berlin-Heidelberg-New York: Springer 1967.

52. Serre, J.-P.: Classes de corps cyclotomiques. Séminaire Bourbaki no. 174 (1958). New York-Amsterdam: W. A. Benjamin, Inc. 1966.
53. [CG] Serre, J.-P.: Cohomologie Galoisienne. Lecture Notes in Mathematics no. 5. Berlin-Heidelberg-New York: Springer 1964.
54. [CL] Serre, J.-P.: Corps locaux. Paris: Hermann 1962.
55. Serre, J.-P.: Sur les corps locaux à corps résiduel algébriquement clos, 2. Bull. Soc. Math. France **89**, 105–154 (1961).
56. Serre, J.-P.: Corps locaux et isogénies. Séminaire Bourbaki, exposé 185, 1958–59.
57. Serre, J.-P.: Groupes proalgébriques. I.H.E.S., Publication Mathematique no. 7 (1960).
58. Serre, J.-P.: Groupes de Lie ℓ-adiques attachés aux courbes elliptiques. Colloque de Clermont-Ferrand (1964). Mimeographed notes published by I.H.E.S.
59. [LG] Serre, J.-P.: Lie algebras and Lie groups. Lectures at Harvard University, 1964. New York-Amsterdam: W. A. Benjamin Inc. 1965.
60. Serre, J.-P.: Abelian ℓ-adic representations and elliptic curves. Lectures at McGill University. New York-Amsterdam: W. A. Benjamin Inc. 1968.
61. Serre, J.-P.: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. Inventiones math. **15**, 259–331 (1972).
62. Serre, J.-P.: Groupes p-divisibles. Séminaire Bourbaki, exp. 318 (1966–67). New York-Amsterdam: W. A. Benjamin Inc. 1966.
63. Serre, J.-P., Tate, J.: Good reduction of abelian varieties. Ann. of Math. **88**, 492–517 (1968).
64. Shimura, G.: Correspondances modulaires et les fonctions zêta de courbes algébriques. J. Math. Soc. Japan **10**, 1–28 (1958).
65. Shimura, G., Taniyama, Y.: Complex multiplication of abelian varieties and its applications to number theory. Publ. Math. Soc., Japan, no. 6, Tokyo 1961.
66. Swinnerton-Dyer, P.: The conjectures of Birch and Swinnerton-Dyer and of Tate. Proceedings of a Conference on Local Fields, NUFFIC Summer School held at Driebergen in 1966, p. 132–157. Berlin-Heidelberg-New York: Springer 1967.
67. Tate, J.: Duality theorems in Galois cohomology over number fields. Proc. Intern. Congress Math. at Stockholm, 1962, 288–295. Institute Mittag-Leffler Djursholm, Sweden (1963).
68. Tate, J.: On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. Séminaire Bourbaki, exp. 306 (1966). New York-Amsterdam: W. A. Benjamin Inc. 1966.
69. Tate, J.: p-divisible groups. Proceedings of a Conference on Local Fields, NUFFIC Summer School held at Driebergen, p. 158–183 (1966). Berlin-Heidelberg-New York: Springer 1967.
70. Tate, J.: Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda). Séminaire Bourbaki, exp. 352 (1968–69).
71. Tate, J.: Endomorphisms of abelian varieties over finite fields. Inventiones math. **2**, 134–144 (1966).
72. Weil, A.: Varietés abéliennes et courbes algébriques. Paris: Hermann 1948.

B. Mazur
Harvard University
Department of Mathematics
Cambridge, Mass. 02138
USA

(Received June 2, 1972)