COMPOSITIO MATHEMATICA

MICHAEL HARRIS

p-adic representations arising from descent on abelian varieties

Compositio Mathematica, tome 39, n° 2 (1979), p. 177-245

<http://www.numdam.org/item?id=CM_1979__39_2_177_0>

COMPOSITIO MATHEMATICA, Vol. 39, Fasc. 2, 1979, pag. 177–245

P-ADIC REPRESENTATIONS ARISING FROM DESCENT ON ABELIAN VARIETIES

Michael Harris*

The proof of the Mordell-Weil Theorem, which asserts that the group of rational points of an abelian variety over (for example) a number field is finitely generated, is traditionally divided into two parts (Cf. [6]), deriving from the theory of heights and from Kummer theory, respectively. Kummer theory already provides the so-called "weak" Mordell-Weil Theorem, namely, that, given an integer n, and an abelian variety A over the number field K, the *Selmer group* $S_n(A, K)$, defined either in terms of Galois or of flat cohomology, is finite. There is a natural imbedding of $A(K)/nA(K)$ in $S_n(A, K)$, so that the number of $\mathbf{Z}/n\mathbf{Z}$ independent elements of $S_n(A, K)$ provides an upper bound for the rank of the $\mathbf{Z}$-free part of $A(K)$; the Tate-Shafarevich conjecture affirms that these numbers *coincide* for all but finitely many n. It is therefore of the utmost interest to compute the group $S_n(A, K)$; this process is known as *descent*.

The Selmer group $S_n(A, K)$ is defined in terms of H^1 (Galois or flat) with coefficients in the group (scheme) $A[n]$ of n-division points of A. This can only be computed, in general, by trivializing $A[n]$ as a Galois module; i.e., by passing to the field $K(A[n])$ over which the points of $A[n]$ become rational, and computing $S_n(A, K(A[n]))^{\mathrm{Gal}(K(A[n])/K)}$. This will in general be different from $S_n(A, K)$, although there is a natural map $S_n(A, K) \to S_n(A, K(A[n]))^{\mathrm{Gal}(K(A[n])/K)}$. However, we have proved the following theorem:

Effectivity Theorem (2.9 in the text): Let p be a prime number such that, at every place v of K dividing p, A has good ordinary reduction at v. (We then say *A is ordinary at p.*) Then, as $n \to \infty$, the kernel and cokernel of the natural map

* Partially supported by an NSF Graduate Fellowship.

0010-437X/79/05/0177-69 $00.20/0

$$S_{p^n}(A, K) \to S_{p^n}(A, K(A[p^n]))^{\mathrm{Gal}(K(A[p^n])/K)}$$

have order *bounded independently of n.*

It is therefore natural to consider the *canonical tower* $K \subset K_0 \subset \cdots \subset K_n \subset \cdots \subset K_\infty$, where $K_i = K(A[p^{i+1}])$, $K_\infty = \bigcup_i K_i$, and to study the $\tilde{G} = \mathrm{Gal}(K_\infty/K)$-module $S_{p^\infty}(A, K_\infty) = \lim_{n\to\infty} S_{p^n}(A, K_{n-1})$, in case A is ordinary at p. We note that $S_{p^\infty}(A, K_\infty)$ is the same whether we take K or any of the K_n as ground field, and we may therefore hope that an investigation of $S_{p^\infty}(A, K_\infty)$ will provide effective information about the asymptotic growth of the Mordell-Weil groups $A(K_n)$ as $n \to \infty$.

When K_∞ is replaced by an extension k/K with $\mathrm{Gal}(k/K) = \Gamma \simeq \mathbf{Z}_p$, the analogous questions were considered by Mazur [28], who based his theory, in turn, on Iwasawa's theory of modules over $\Lambda_\Gamma \overset{\text{def.}}{=} \varprojlim_{U \text{ open in } \Gamma} \mathbf{Z}_p[\Gamma/U]$. We develop (§1) the analogous theory for Λ_G, defined in the same way, when G is any torsion-free compact p-adic Lie group, and investigate the structure of $S_{p^\infty}(A, K_\infty)$ as Λ_G-module, where $G = \mathrm{Gal}(K_\infty/K_0)$.

The theory of Λ_G, in conjunction with the descent techniques of Mazur [28], enables us, in certain cases (§5 in the text) to exhibit asymptotic *upper bounds* for the Mordell-Weil rank of an elliptic curve over the intermediate fields of its canonical tower. These upper bounds can be derived for any abelian variety A which satisfies the

Conjecture (4.6 in the text): If A is ordinary at p, then the Pontryagin dual of $S_{p^\infty}(A, K_\infty)$ is a *torsion* module over Λ_G.

This is a weaker version of a conjecture of Mazur ([28]; Cf. 5.1.1, in the text). We have only been able to prove this conjecture when A is an elliptic curve with complex multiplication and K is an abelian extension of the CM field (5.13), and for several particular classes of elliptic curves (§5A and B). What evidence we have for the conjecture is presented in 4.7, which also provides a somewhat more explicit description of $S_{p^\infty}(A, K_\infty)$.

Here is an outline of our major results, in the order in which they are presented:

In §1, we develop the theory of Iwasawa algebras, relying heavily upon the work of Lazard [24] and some elementary noncommutative and commutative algebra in our proofs of weak analogues of Iwasawa's structure theorems.

Chapter II, §2, introduces the infinite descent theory, à la Mazur

[28], in the context of the canonical tower of an abelian variety. In particular, we prove the Effectivity Theorem for abelian varieties ordinary at p; our proof makes use of the Weil-Riemann hypothesis for abelian varieties, and of a cohomological lemma of Serre [41].

In §3, we generalize the fundamental work of Iwasawa, and prove analogues (Theorems 3.3 and 3.9) of Theorems 5 and 17 of [21], for any Galois extension K'/K, $[K: \mathbf{Q}] < \infty$, such that

(1) $\mathrm{Gal}(K'/K)$ is a torsion-free pro-p p-adic Lie group, and

(2) Only finitely many primes in K ramify in K'.

(In 3.9, we assume, as does Iwasawa, that K' contains the p^nth roots of unity for all n.) This theory is applied to the canonical tower of an abelian variety in the subsequent §, but it is also relevant to the p-adic extensions defined by Deligne in [10]. A primary task for the future is to find a substitute for $S_{p^\infty}(A, K_\infty)$ in Deligne's context.

In §4, we state the conjecture described above, and present the relevant evidence. We also generalize (4.9) an observation of Coates and Wiles [9], (Theorem 11) which plays a major role in their work on the Birch–Swinnerton–Dyer Conjecture.

Examples of elliptic curves satisfying Conjecture 4.6 are produced in §5, mostly by explicit calculation. A particularly interesting example (5.7) makes use of a recent theorem of Ferrero [13] on the vanishing of Iwasawa's μ-invariant. The conjecture is verified (5.13) for CM-curves, under the restrictions described above; our proof makes use of Brumer's work on Leopoldt's conjecture [5]; the reader will note the affinity with work of Coates–Wiles [9] and Vishik [40].

The Appendix presents a number of simple computations of first descents for elliptic curves over $\mathbf{Q}$. Particular attention is paid to the cases, neglected in the main text, of supersingular reduction, and of the prime $p = 2$.

I take this opportunity to express my gratitude to Professor Barry Mazur, who supervised the thesis of which this paper is a part, not only for the manifest influence of his work on this paper, but also for his encouragement and for the frequency with which he could be reached for advice. Of the many others with whom I discussed this work, I am particularly indebted to R. Greenberg and D. Kazhdan, both of whom helped me to clarify certain crucial misconceptions, and to K. Ribet, who pointed out that Serre's paper [41] could be used to simplify my original proof of the key Lemma 2.6.4.

Notation

We make use of the following (fairly standard) notation:

When K is a field, $\bar{K}$ will denote its algebraic closure (all our fields will be perfect). If v is a valuation on K, K_v will denote the completion of K at v.

If S is a scheme, and v a point on S of codimension one (or, if S is affine, a rank one valuation of the affine algebra of S), then S_v will denote the spectrum of the completion at v of the local ring of S at v. If X is a sheaf for some topology on S_v, then $H^i_v(S_v, X)$ will be cohomology with support at the closed point of S_v.

If K is a field, and if X is a $\mathrm{Gal}(\bar{K}/K)$-module (continuous or discrete), then we write $H^i(K, X)$ instead of $H^i(\mathrm{Gal}(\bar{K}/K), X)$.

If S is a set, then $|S|$ will denote its cardinality, whether or not S is known *a priori* to be finite.

If K is a local or global field, O_K will designate its integer ring; if K is global, $K_{\mathbf{A}}$ will be the adele ring of K.

We employ the standard notation $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{F}_q$, $\mathbf{G}_m$, μ_p, etc.

§1. Groups algebras of p-analytic groups

In this section we develop the most elementary properties of the algebras which arise naturally in the infinite descent theory; the algebras and their representations are investigated more intimately in [50]. Here we are content to refer to the paper of Lazard [24] for the bulk of our needed results.

1.1. By a *p-analytic group* we mean a p-adic analytic Lie group which is a *torsion free pro-p group*. Our examples will be closed subgroups of the kernel of the reduction map $GL(n, \mathbf{Z}_p) \to GL(n, \mathbf{F}_p)$; such a group will be called *standard*. (For $p = 2$, one is restricted to subgroups of the kernel of reduction mod 4.) If G is a p-analytic group, its structure of profinite group is expressed by the formula $G = \varprojlim_U G/U$, where U runs over the family of open subgroups of G and the maps are the obvious ones. Then the *Iwasawa algebra*, or completed group algebra, of G, is the ring $\Lambda_G = \varprojlim_U \mathbf{Z}_p[G/U]$, U as above.

This will often be denoted Λ, when there is no ambiguity. The interest of Λ derives from the following theorem:

1.2. Theorem ([24], p. 61): *Let M be a complete $\mathbf{Z}_p$-module with*

continuous left G action. Then M has a unique continuous left Λ_G-structure which extends the action of G (via the inclusion of G in Λ_G).

1.3. Following [14] and [12] we define the *left Krull dimension* of a ring R to be the Krull dimension of the partially-ordered set of its left ideals. Recall that this means the following: a partially ordered set $\mathcal{S}$ has Krull dimension zero if it satisfies the descending chain condition and if there is at least one non-trivial inequality $a < b$; it has Krull dimension at most $n+1$ if and only if for every strictly decreasing sequence of elements $a_1 > a_2 > a_3 \cdots$ the following condition is satisfied:

(1.3.1) For i sufficiently large, the set $\{s \in \mathcal{S}: a_{i+1} \leq s \leq a_i\}$ has Krull dimension at most n.

The following facts can be found in [14] and [12], 3.5:

(1.3.2) If R is commutative, and Noetherian, this is equivalent to the standard definition.

(1.3.3) If R is filtered, then Krull dim $R \leq$ Krull dim $Gr(R)$.

1.4. The ring Λ_G has a natural collection of two-sided ideals: for any normal open subgroup U of G, the ideal I_U is that generated by $\{u-1; u \in U\}$. These form a basis for the topology of Λ, in a neighborhood of zero.

For the moment, let $G_i = \mathrm{Ker}(GL(k, \mathbf{Z}_p) \to GL(k, \mathbf{Z}/p^{i+1}\mathbf{Z}))$, $G = G_0$ (for $p = 2$, let $G = G_1$). Any element $g \in G$ defines a one-parameter subgroup of G (the closure of $\{g^n \mid n = 0, \pm 1, \pm 2, \ldots\}$); call this $\langle g \rangle$. The tangent space $T_{\langle g \rangle}(1)$ at the identity maps to a subgroup containing $\langle g \rangle$ via the standard formula for the exponential map (by tangent space, we actually mean the $\mathbf{Z}_p$-submodule of the tangent space where the exponential map converges); this proves

(1.4.1) If $g \in G_i$, then there exists $h \in G$ such that $h^{p^i} = g$.

(1.4.2) If $g \in G_i - G_{i+1}$, then $g^p \in G_{i+1} - G_{i+2}$. One knows similarly that

(1.4.3) The subgroup of commutators $[G_i, G_j] \subset G_{i+j}$.

1.4.4. Now let H be a p-analytic subgroup of G. The generators of the Lie algebra of H give rise by exponentiation to generators $\nu_i \in H$, $i = 1, \ldots, n = \dim H$, such that, if $X_i = \nu_i - 1 \in \Lambda_H$, then every element of Λ_H has a unique development ([24], p. 165)

$$(1.4.4.1) \qquad \lambda = \sum_{\alpha} A_\alpha X_1^{\alpha_1} X_n^{\alpha_2} \cdots X_n^{\alpha_n},\ \alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n),\ A_\alpha \in \mathbf{Z}_p.$$

Choose a small rational number ϵ, and, with $H = G$ above, let w_ϵ be the valuation on Λ_G such that $w_\epsilon(X_i) = 1 - \epsilon$, $w_\epsilon(p) = 1$. Then

(1.4.1–3) imply that $Gr(\Lambda_G)$, with respect to the filtration induced by w_ϵ, is a ring of *commutative* polynomials in k^2+1 variables over $\mathbf{F}_p$ (Cf. [24], p. 165; the extra variable, of course, comes from the uniformizer p), if ϵ is chosen correctly. (For $p=2$, this requires an additional argument.) Such a filtration induces a filtration on Λ_H such that $\mathrm{Gr}(\Lambda_H) = \mathbf{F}_p[\bar{p}, \bar{X}_1, \ldots, \bar{X}_n]$ where $\bar{}$ denotes image in the associated graded of an element of Λ_H. Then we conclude by (1.3.2, 1.3.3).

1.5. PROPOSITION: *Let H be as above. Then Λ_H is a noetherian local ring, without zero-divisors, of left Krull dimension at most $n+1$.*

PROOF: What is not immediate can be found in Bourbaki's *Commutative Algebra*, III, §2.

1.6. COROLLARY (Nakayama Lemma): *Let H act continuously on the discrete $\mathbf{Z}_p$-module M. If M^H is cofinite over $\mathbf{Z}_p$, then M is cofinite over Λ_H (here M is cofinite means that the Pontryagin dual M' of M is finitely generated).*

PROOF: Let m be the maximal idea of $\Lambda = \Lambda_H$. By assumption, M' is compact, and M'/mM' is a finite group. The argument of [43] Lemma 4, does not depend on commutativity of Λ, and gives the result in this case.

1.7. COROLLARY: *Suppose, in the situation of* 1.6., *that M^H is actually a* finite *group. Then M' is a torsion module over Λ_H, where M' is the Pontryagin dual of M.*

PROOF: By Proposition 1.5, the set of torsion elements of M' forms a Λ-submodule (Cf. [12], 3.6.9). We may thus assume that M' is *torsion-free.*

(i) M' is a submodule of a finitely generated free Λ-module. In fact, 1.5 and Goldie's Theorem ([12], 3.6.12) imply that Λ has a skewfield of fractions K. Then $K \otimes_\Lambda M'$ is a left vector space over K, with generators $v_1, \ldots, v_r$, say. Let $m_j = \Sigma_i a_{ij} s_{ij}^{-1} v_i$ be a set of generators for M', imbedded in $K \otimes_\Lambda M'$, where the a_{ij}'s and s_{ij}'s are in Λ. If we can find s_i's in Λ such that there exist b_{ij}'s in Λ with $s_i b_{ij} = s_{ij}$, then the free Λ-module generated by $\{s_1^{-1} v_i\}$ contains M'. But such s_i's and b_{ij}'s must exist – the existence is needed in the proof of Goldie's Theorem (Cf. [12], 3.6.9).

(ii) We may assume, then, that M' is a submodule of Λ^r, for some integer r. Then, with respect to the filtration induced by w_ϵ (Cf. 1.4.4), $Gr(M') \subset Gr(\Lambda^r)$, and in particular is a torsion-free $Gr(\Lambda) = \mathbf{F}_p[\bar{p}, \bar{X}]$

module ($\bar{X} = (\bar{X}_1, \ldots, \bar{X}_n)$). Let J be the ideal generated by $\bar{X}$; localize everything at J. The hypothesis is that $Gr(M')_J = JGr(M')_J$ (since $\bar{p}$ has become invertible). By the ordinary Nakayama lemma, $Gr(M')_J = 0$. Since $Gr(M')$ is torsion-free, it is also zero. Then M' is zero.

1.8. We retain the notation of 1.4. We are going to prove an asymptotic formula for torsion Λ-modules which will be applied in the sequel to provide asymptotic bounds for Mordell–Weil ranks of abelian varieties in the towers generated by their p^n-division points. Such bounds should be regarded as weak analogues of Iwasawa's class number formula [21].

Let $\Omega = \mathbf{F}_p[\![H]\!] = \Lambda/p\Lambda$. We are goint to prove for Ω results of the sort we sketched for Λ in 1.4. We define the envelope of H in G, written env(H), to be the largest subgroup of G in which H is open; it is the largest subgroup arising from exponentiation along the directions contained in the Lie algebra of H.

We assume from now on that $p \neq 2$, to save us a great deal of trouble. If $H' = \text{env}(H)$, let w be the valuation on $\Omega_{H'}$ (obvious notation), for which $w(X_i) = 1$.

1.8.1. LEMMA: *With respect to the filtration defined by w, $Gr(\Omega_{H'})$ is commutative. (And consequently, so is $Gr(\Omega_H)$.)*

PROOF: Let $H'_i = H' \cap G_i$. We first show that if $h \in H'_j$, then $w(h-1) \geq p^j$. In fact, by 1.4.1, $h = s^{p^j}$, some $s \in H'$ (because $H' = \text{env}(H')$). Write $s = \Pi\gamma_i^{r_i}$, where $\gamma_i = 1 + X_i$ and r_i are p-adic integers. Then $h = (\Pi(1+X_i)^{r_i})^{p^j}$. Expanding this out (if you like, you can approximate the r_i's by rational integers and take the limit) the cross terms appear with coefficients divisible by p, and we are left with $1 + \Sigma_{|\alpha|=p^j} C_\alpha X^\alpha$ as the dominant term (C_i are constants). Incidentally, the fact that w is a *filtration* depends on such a computation; we have blithely been assuming its truth (armed with reference [24]).

A quick computation shows that $[X_i, X_j] = ((\gamma_i, \gamma_j) - 1)\gamma_j\gamma_i$ (where $(\ ,\ )$ means commutator in the group). Then by the result of the preceding paragraph and 1.4.3, we are are done. Note how we have used the fact that $p \neq 2$ in order to get the commutator into a sufficiently high filtration. Note also how setting $w_\epsilon(p)$ slightly bigger than $w_\epsilon(X_i)$ in 1.4.4 makes up for the fact that in Λ we do not have at our disposal that $p = 0$.

1.9. PROPOSITION: *In the notation of* 1.4, *let K be a normal*

subgroup of H such that H/K can also be imbedded in $\mathrm{Ker}(GL(k', \mathbf{Z}_p) \to GL(k', \mathbf{F}_p))$ *for some k'. Let M be a compact Λ-module such that $M/\Lambda_H I_K$ is a finitely generated torsion $\Lambda_{H/K}$-module. Then M is a finitely generated torsion Λ_H-module.*

Similarly, if M/pM is a finitely generated torsion Ω_H-module, then M is a finitely generated torsion Λ_H-module.

PROOF: That M is finitely generated follows from 1.6. The assumption on H/K implies that $\mathrm{Gr}(\Lambda_H)/\mathrm{Gr}(\Lambda_H)\mathrm{Gr}(I_K) = \mathrm{Gr}(\Lambda_{H/K})$ is an integral domain, hence that $J' = \mathrm{Gr}(\Lambda_H)\mathrm{Gr}(I_K)$ is a prime ideal in $\mathrm{Gr}(\Lambda_H)$. Of course, the ideal generated by $\bar{p}$ (Cf. 1.4.4) is a prime in $\mathrm{Gr}(\Lambda_H)$. Now follow the proof of 1.7, replacing localization at J in step (ii) by localization at J' (resp. at $\bar{p}\mathrm{Gr}(\Lambda_H)$).

1.10. THEOREM: *Let M be a finitely generated compact $\Lambda = \Lambda_H$-module, M' its discrete Pontryagin dual. Let $n = \dim H$, and $H_i = H \cap G_i$, in the notation of* 1.4. *The vector space $\mathbf{Q}_p \otimes_{\mathbf{Z}_p} M/I_{H_i}M$ has finite dimension d_i. Then the following two conditions are equivalent* (Cf. [21], p. 256):

(i) M is a torsion Λ-module.

(ii) $d_i = O(p^{(n-1)i})$.

PROOF: (i) implies (ii): We may replace M by $N = M/M^*$, where M^* is the p-primary torsion submodule of M; this does not alter the d_i's. Then M/pM is a compact torsion $\Omega = \Omega_H$-module, with Pontryagin dual $M'[p] = p$-torsion submodule of M'. But d_i is at most equal to $M'[p]^{H_i}$ (d_i comes from the free, hence flat, part of $M/I_{H_i}M$, and thus persists mod p); we are done by

1.10.1. LEMMA: *Let M be a finitely generated compact torsion module over $\Omega = \Omega_H$, with discrete Pontryagin dual M'. Then $\dim_{\mathbf{F}_p} M'^{H_i} = O(p^{(n-1)i})$, where $n = \dim H$ and $H_i = H \cap G_i$.*

PROOF: M'^{H_i} is dual to $M/I_{H_i}M = M_{H_i}$, so we can forget about M'. We may assume that $H = \mathrm{env}(H)$. Otherwise, letting $H' = \mathrm{env}(H)$, we may induce up to H'-i.e., tensor on the left with $\Lambda_{H'}$; if we call the result M^*, then M^* is clearly a torsion $\Lambda_{H'}$-module (Cf. 1.11 below for the trivial proof), and M_{H_i} is a submodule of $M^*_{H_i}$, so that estimates for the latter give stronger estimates for the former.

Thus we may assume that all the X_i's have the same valuation $w(X_i) = 1$. Now $I_{H_j} \supset \{(1 + X_i)^{p^j} - 1\} = \{X_i^{p^j}\}$. Thus $\mathrm{Gr}(I_{H_j})$ contains (with notation analogous to that of 1.4.4) every polynomial divisible

by $X_i^{p^j}$ for some i, and in particular contains $\mathrm{Gr}(I_H)^{np^j} \overset{\text{def}}{=} \underline{m}^{np^j}$, where n is as usual $\dim H = \dim(\mathrm{Gr}(\Omega))$. Now $\mathrm{Gr}(M)$ is a finitely generated torsion $\mathrm{Gr}(\Omega)$-module. So for t sufficiently large, $\mathrm{Gr}(M)/\underline{m}^t\mathrm{Gr}(M)$ has dimension given by $\chi_M(t)$, where χ_M is the Hilbert polynomial of $\mathrm{Gr}(M)$, of degree at most $n-1$. Letting $t = np^j$, we see that $\mathrm{Gr}(M)/\mathrm{Gr}(I_{H_j})\mathrm{Gr}(M)$, which as an abstract vector space is isomorphic to M_{H_j}, is a quotient of a vector space of dimension $O((np^j)^{n-1})$; this gives the required estimate.

(ii) implies (i); Assuming as usual that M is torsion-free, hence contained in a free Λ-module (Cf. the proof of 1.7), we derive a contradiction: Since $M \subset \Lambda^r$ for some integer r, $\mathrm{Gr}(M) \subset \mathrm{Gr}(\Lambda)^r$.

1.10.2. LEMMA: *Let M be a finitely generated module over $R = k[X_0, X_1, \ldots, X_n]$, k a field, such that M is torsion-free. Then M can be imbedded in a free R-module V such that* $\mathrm{Supp}(V/M) \supset \mathrm{Supp}(R/X_0R)$.

PROOF: Let U be the open subset of $\mathrm{Spec}(R)$ on which M is locally free; then U contains the generic point of every hypersurface (since the local ring of such a point is a DVR). Thus the complement of U is of codimension two. Choose a hypersurface containing $\mathrm{Spec}(R) - U$ and transversal to $\mathrm{supp}(R/X_0R)$; call it H, and its complement W. Then $M \otimes_R \Gamma(W, \mathcal{O}_W)$ is $\Gamma(W, \mathcal{O}_W)$-projective, hence a direct summand of a free $\Gamma(W, \mathcal{O}_W)$-module B; and an R-lattice in B containing M will be the desired V.

We apply this lemma to $\mathrm{Gr}(M)$ and $\mathrm{Gr}(\Lambda) = \mathbf{F}_p[\bar{p}, \bar{X}_1, \ldots, \bar{X}_n]$, letting $\bar{p}$ play the role of X_0. We have the exact sequence (write $\tilde{M}$ for $\mathrm{Gr}(M)$)

$$0 \to \tilde{M} \to V \to V/\tilde{M} \to 0 \tag{1.10.3}$$

giving rise to the exact sequence (we continue to write $R = \mathrm{Gr}(\Lambda)$, and now set $J_j = \mathrm{Gr}(I_{H_j})$

$$\mathrm{Tor}_1^R(R/J_j, V/\tilde{M}) \to \tilde{M}/J_j\tilde{M} \to V/J_jV \to (V/\tilde{M})/J_j(V/\tilde{M}) \tag{1.10.4}$$

We claim that $T_j = \mathrm{Tor}_1^R(R/J_j, V/\tilde{M})$ satisfies

$$\dim_{\mathbf{F}_p} T_j/\bar{p}T_j = O(p^{(n-1)d}). \tag{1.10.5}$$

In fact, J_j is generated by n elements (coming from $(1+X_i)^{p^j} - 1$, $i = 1, \ldots, n$, Cf. 1.4.4), so that a free resolution for R/J_j begins

$$R^n \to R \to R/J_j \to 0. \tag{1.10.6}$$

T_j will be a subquotient of $R^n \otimes_R (V/\tilde{M})$, and will thus *remain* torsion when tensored with $R/\bar{p}R$, thanks to our choice of V. (1.10.4) then follows from 1.10.1.

Now $\tilde{M}/J_j\tilde{M}$, as a finitely generated $\mathbf{F}_p[\bar{p}]$-module, has a free part and a torsion part; we are given that the free part has rank $O(p^{(n-1)j})$, and we know that the torsion part is in the image of T_j, hence when reduced mod $\bar{p}$ has dimension $O(p^{(n-1)j})$. Thus, as a $\mathrm{Gr}(\Omega)$-module, $\tilde{M}/\bar{p}\tilde{M} = N$ satisfies

$$\dim_{\mathbf{F}_p} N/J_jN = O(p^{(n-1)j}); \tag{1.10.7}$$

we write J_j again for the image of J_j in $\mathrm{Gr}(\Omega)$. But in $\mathrm{Gr}(\Omega)$, J_j is generated by $\{\bar{X}_i^{p^j} \mid i = 1, \ldots, n\}$, hence is contained in $\bar{m}^{p^j}$, where $\bar{m}$ is the ideal generated by $\{X_1, \ldots, X_n\}$. By the Hilbert polynomial, $\dim_{\mathbf{F}_p} N/\bar{m}^{p^j} \leq \dim_{\mathbf{F}_p} N/J_jN = O(p^{(n-1)j})$ implies N is a torsion $\mathrm{Gr}(\Omega)$ module. As in part (i) of the proof of 1.7, this implies M/pM is a torsion Ω-module, hence by 1.9, M is a torsion Λ-module.

1.10.8. REMARK: We may refine Lemma 1.10.1, and consequently Theorem 1.10, as follows: we have shown that, if M is a finitely generated compact torsion Ω-module, and if M' is the Pontryagin dual of M, then $\dim_{\mathbf{F}_p} M'^{H_i} \leq \chi_M(np^i)$, where $n = \dim H$ and χ_M is the Hilbert polynomial of $\mathrm{Gr}(M)$, considered as a $\mathrm{Gr}(\Omega)$-module. Hence, if the support of $\mathrm{Gr}(M)$ is of codimension k in $\mathrm{Spec}(\mathrm{Gr}(\Omega))$, we may replace the estimates in 1.10.1 by $\dim_{\mathbf{F}_p} M'^{H_i} = O(p^{(n-k)i})$, and thus, we may replace (ii) of 1.10 with

$$d_i = O(p^{(n-k)i}). \tag{1.10.8.1}$$

When H is commutative, one need not reduce (mod p), nor need one appeal to Gr: the support of M on $\mathrm{Spec}(H) = \mathrm{Spec}(\mathbf{Z}_p[\![X_1, \ldots, X_n]\!])$ will have a codimension k, and 1.10.8.1 will hold for this k.

1.11. PROPOSITION: *Let K be any p-analytic subgroup of H, M a compact finitely generated module over Λ_K. Then* $\mathrm{Ind}_K^H(M)$ *is finitely generated over Λ_H, and M is torsion over Λ_K if and only if* $\mathrm{Ind}_K^H(M)$ *is torsion over Λ_H.*

PROOF: Let $\{m_i\}$ be a set of Λ_K-generators of M. Then $\{1 \otimes m_i\}$ is a set of Λ_H-generators of $\mathrm{Ind}_K^H(M)$, and they are annihilated already by elements of Λ_K if M is a torsion Λ_K-module. On the other hand, if M is torsion-free, then so is $\mathrm{Ind}_K^{\mathrm{env}(K)\cap H_M}$, since $\Lambda_{\mathrm{env}(K)\cap H}$ is free over Λ_K;

thus we may assume that $K = \mathrm{env}(K) \cap H$. Then $\mathrm{Gr}(\Lambda_H)$ is *smooth* over $\mathrm{Gr}(\Lambda_K)$, and in particular faithfully flat; so if $\mathrm{Gr}(M)$ is torsion-free over $\mathrm{Gr}(\Lambda_K)$, then $\mathrm{Gr}(\mathrm{Ind}_K^H(M))$ is torsion-free over $\mathrm{Gr}(\Lambda_H)$, and $\mathrm{Ind}_K^H(M)$ is torsion-free over Λ_H.

1.12. TERMINOLOGY: Let M be a discrete Λ-module, M' its compact Pontryagin dual. If M' is finitely generated over Λ, we say M is *cofinite*; this is to say that M^H, up to a finite group is isomorphic to $(\mathbf{Q}_p/\mathbf{Z}_p)^t$ for some integer t. If M' is Λ-torsion, we say M is *cotorsion*. The category of compact torsion Λ-modules will be denoted $\mathcal{T}$. We shall always understand by a torsion module a *finitely generated* torsion module.

Finally, let M be a compact Λ-torsion module; if $\mathrm{Supp}(\mathrm{Gr}(M))$ is of codimension at least two in $\mathrm{Spec}(\mathrm{Gr}(\Lambda))$, we say M is *trivial mod* $\mathscr{C}$, and we let $\mathscr{C}$ be the full, necessarily thick, subcategory of $\mathcal{T}$ of modules trivial mod $\mathscr{C}$; we employ the usual conventions in dealing with quotient categories. If M is compact and trivial mod $\mathscr{C}$, its Pontryagin dual will be called *cotrivial mod* $\mathscr{C}$. As in 1.11, we see that being trivial mod $\mathscr{C}$ commutes with induction. Similarly, the properties of being cotorsion or cotrivial mod $\mathscr{C}$ commute with *coinduction*, where $\mathrm{Coind}_K^H M = \mathrm{Hom}_{\Lambda_K}(\Lambda_H, M)$ with its usual left Λ_H-module structure.

§2. Mazur's descent theory and the canonical tower

Here we recall Mazur's formulation of the classical theory of infinite descent for abelian varieties in terms of flat cohomology, following [28] more or less literally. In that paper, Mazur proves that Iwasawa theory provides valuable information about the growth of Mordell-Weil groups of abelian varieties over $\mathbf{Z}_p$-extensions, where p is a prime at which the abelian variety has ordinary reduction. In this section, we derive analogous results on the growth of the Mordell-Weil group over the particular p-analytic Galois extension obtained by adjoining the p^n-division points to the ground field for all n.

2.1. Let K be a number field, A_K an abelian variety over K. If $S = \mathrm{Spec}(O_K)$, O_K the ring of integers in K, we denote by A the Néron model of A_K over S. It is known that, over an open subset of S, A is proper and has connected fibers; thus, if we define F_n, n a positive integer, by the exactness of the sequence of *fppf* sheaves on S

$$0 \longrightarrow A[n] \longrightarrow A \xrightarrow{\times n} A \longrightarrow F_n \longrightarrow 0 \tag{2.1.1}$$

($A[n]$ is the kernel of multiplication by n), then, if A has semi-stable reduction at all points of characteristic dividing n, then F_n is a skyscraper sheaf with finite fibers, not in general representable, such that if q is a number relatively prime to n, then q does not divide the order of any stalk of F_n. This is true in particular if n is a power of the prime p, and A has good reduction at all points of characteristic p.

Break up (2.1.1) into the following diagram, whose rows are exact sequences of *fppf* abelian sheaves on S:

(2.1.1.1)(n)
$$\begin{array}{ccccccccc} 0 & \longrightarrow & A[n] & \longrightarrow & A & \longrightarrow & \bar{A} & \longrightarrow & 0 \\ & & & & \downarrow & \searrow^{+_n} & \downarrow & & \\ & & 0 & \longrightarrow & \bar{A} & \longrightarrow & A & \longrightarrow & F_n \longrightarrow 0 \end{array}$$

This gives rise to the exact cohomology sequences

(2.1.2)(n)
$$0 \to H^0(S, \bar{A})/H^0(S, A) \to H^1(S, A[n]) \to \mathrm{Ker}(H^1(S, A) \to H^1(S, \bar{A})) \to 0$$

(2.1.3.1)(n)
$$0 \to H^0(S, \bar{A}) \to H^0(S, A) \to H^0(S, F_n)$$

(2.1.3.2)(n)
$$H^0(S, F_n) \to H^1(S, \bar{A}) \to H^1(S, A) \to H^1(S, F_n)$$

Let $n = p^r$ and take the direct limits, over r, of the three sequences above. Evidently, at any given point, F_n has order bounded above by the number of connected components of the Néron fiber. We want to find sharp bounds for H^0 and H^1 of F_n. First of all, we note that $H^i(S, F_n) = \bigoplus_{x \in \mathrm{Supp}\, F_n} H^i(\mathrm{Gal}(\overline{k(x)}/k(x)), F_{n,x})$, where $k(x)$ is the residue field at x, $\overline{k(x)}$ its algebraic closure – this is true because F_n is a skyscraper sheaf, and because cohomology of A and $\bar{A}$ computed for the flat or étale topologies give the same results (Cf. App., 1.0.2.3), and by the five lemma, the same is true of F_n.

2.1.3.3. We record, for future reference, that $H^i(S, F_n)$ has order bounded *independently* of n, which follows immediately from the corresponding assertion for F_n itself.

(2.1.4) In this paragraph only, we assume K is *local*, $S = \mathrm{Spec}(O_K)$ as before. We let $K_n = K(A[p^{n+1}])$, $K_\infty = K(A[p^\infty])$, in the obvious notation, and S_n, S_∞ the corresponding Spec's of integer rings. A does not lift to a Néron model over S_n in general, but we shall denote all the Néron models by the letter A. In any case, there is a map from the lift of A over S_n to the Néron model of A over S_n, so that it makes sense to take direct limits over n of cohomology groups of A. Similar

considerations apply to the F's, which will also all be denoted by the same letter.

We assume that the residue characteristic of S is not p. Then the formal group of A maps to zero in F_{p^r} for any r; thus the number of elements of order p^n in F_{p^r} is bounded by p^{2gn}, where g is the dimension of A. Moreover, let $F = F_{p^\infty}$; the map $A[p^\infty](S_\infty) \to F(S_\infty)$ is surjective, and Lang's theorem [25] on the vanishing of cohomology of connected groups implies

(2.1.4.1) $H^i(S_\infty, A[p^\infty]) \to H^i(S_\infty, F)$ is surjective for all i, and an isomorphism for $i > 0$.

Let $D = \mathrm{Gal}(K_\infty/K_0)$; we want to prove that $H^i(S_\infty, F) = \varinjlim_n H^i(S_n, F)$ are cotorsion Λ_D-modules for $i = 0, 1$. It suffices to prove that they are quotients of $\mathbf{Z}_p$-modules of the form $(\mathbf{Q}_p/\mathbf{Z}_p)^k$ for some finite k. By (2.1.4.1), this is evident for $i = 0$, and by (2.1.4.1), it suffices to prove that $H^1(S_\infty, A[p^\infty])$ is of the form $(\mathbf{Q}_p/\mathbf{Z}_p)^k$. But $A[p^n]$, as a group scheme over S_i, $i \geq n-1$, is finite and flat (even étale): in fact, we prove this in 2.2.1 below (this eccentricity of sequence does not lead to any logical fallacies); by (App., 1.0.2.2) $H^1(S_\infty, A[p^n]) = 0$ for all n, and the local cohomology sequence gives rise to an imbedding of $H^1(S_\infty, A[p^\infty])$ in $H^1(K_\infty, A[p^\infty]) \simeq \mathrm{Hom}(\mathrm{Gal}(\bar{K}_\infty/K_\infty), A[p^\infty])$. Since the residue characteristic of S is different from p, class field theory implies that this last module is of the required form (the abelian $\mathbf{Z}_p$-extensions of K form a one-dimensional family). We have proved

2.1.5. PROPOSITION: *The Λ_D-modules $H^i(S_\infty, F) = \lim_{\vec{n}} H^i(S_n, F)$ are cotorsion, for $i = 0.1$. If D is of p-adic dimension at least two, then the Pontryagin duals of the above modules are even trivial* mod $\mathscr{C}$.

PROOF: We have only to verify the last statement; but the (compact) modules in question are of finite $\mathbf{Z}_p$-rank; upon passing to $\mathrm{Gr}(\Lambda)$, our assertion becomes clear.

2.1.6. REMARK: This result, or one equivalent to it – namely, that the infinite descent involves very little ramification at the bad primes – could have been obtained with less trouble using, for example, the methods of [6] and not bothering with the Néron model and flat cohomology; however, we do gain something by working with the Néron model when we deal with ramification at p.

2.2. We return to our previous notation; thus K is a number field, S the spectrum of its ring of integers. If G is an abelian group, we let

$G[n]$ denote its n-torsion subgroup, and $G[p^\infty]$ its p-primary torsion subgroup. The same notation holds for group schemes; however, $A[p^\infty]$, if A is an abelian variety, will often be written $\tilde{A}$; this can of course be interpreted as the *p-divisible group* associated to A. We denote the dimension of A by g. *A is to have good reduction at all primes dividing p.*

Let $K_n = K(A[p^{n+1}])$, $K = \bigcup_n K_n$; this will be called the *canonical tower* associated to the information $\{A, K, p\}$. We let S_n be $\mathrm{Spec}(O_{K_n})$, O_{K_n} the ring of integers in K_n, and define S_∞ likewise. Set $G_i = \mathrm{Gal}(K_\infty/K_i)$, $G = G_0$, and $\tilde{G} = \mathrm{Gal}(K_\infty/K)$. Then G is a p-analytic group of the type considered in 1.4, and G_i is its associated filtration. Unless otherwise specified, Λ will mean Λ_G for this particular G.

The Néron model varies with the S_i; in particular, to each S_i is associated an $F_{p^\infty,i}$, which we abbreviate F_i. The universal property of the Néron model implies that, if $j > i$, then $F_i \times_{S_i} S_j$ maps to F_j; thus we may speak of M_0 and M_1, where $M_\epsilon = \lim_{i\to\infty} H^\epsilon(S_i, F_i) = H^\epsilon(S_\infty, F_\infty)$.

2.2.1. LEMMA: *Let v be a place of S, w a place of S_∞, dividing v, such that F_∞ is non-trivial at w. Then w is ramified over v, and the inertia group is infinite.* (Cf. [16]).

PROOF: The hypothesis implies that A has bad reduction at w (for convenience, we continue to write A over S_∞, even though it is in general not the same group scheme); similarly, A has bad reduction at w_n, the restriction of w to S_n. Thus the connected component of the identity of A over the residue field of w_n does not have $p^{2g(n+1)}p^{n+1}$-division points; here we use the assumption that v is prime to p; i.e., that A has good reduction at primes dividing p.)

Let $B_n = (\mathbf{Z}/p^{n+1})^{2g}/S_n$ be the (étale) constant group scheme over S_n. By definition of K_n, the generic fiber of B_n imbeds in A_{K_n}; by the Néron property, this extends to a map of B_n into A over S_n; the closure of the image of B_n is a finite flat subgroup scheme of order $p^{(n+1)2g}$ over S_n (Cf. [37], 2.1); call it Ξ. Now Ξ must be étale over w_n, which is of characteristic prime to p; and since it is finite, we conclude that the fiber of A over w_n does have $p^{2g(n+1)}p^{n+1}$-division points, thus, for n sufficiently large, cannot be the lift of the fiber of A over v. But Néron models remain Néron models over unramified base extensions. Thus w_n is ramified over v for n sufficiently large. To conclude that the inertia group of w/v is infinite, we may repeat the argument, replacing S by S_n, v by w_n, and remarking that the hypothesis of the lemma remains the same.

2.3. COROLLARY: *The Pontryagin duals of M_0 and M_1 are trivial mod $\mathscr{C}$ as Λ-modules.*

PROOF: It suffices to prove this for each place v of S at which F has a non-trivial stalk; we may thus assume F has only *one* non-trivial stalk (at v, say). Let w be a place of S_∞ over v; then $M_\epsilon = \mathrm{Coind}_{D_w}^{G} H^\epsilon(S_{\infty,w}, F_\infty)$, where D_w is the decomposition group of w and $S_{\infty,w}$ is the completion at w. But we have already proved that the local module is cotorsion; moreover, D_w maps onto the unramified cyclotomic $\mathbf{Z}_p$-extension, and contains an infinite inertia subgroup; thus 2.1.5 implies that the local modules are cotrivial mod $\mathscr{C}$. Then, as in 1.12, we conclude that the induced module has the same properties over Λ_G as the original module has over Λ_{D_w}.

2.4. COROLLARY: *The "Kummer sequence"*

$$(2.4.1) \qquad 0 \to A(S_\infty) \otimes \mathbf{Q}_p/\mathbf{Z}_p \to H^1(S_\infty, \tilde{A}) \to Ш(A, K_\infty)[p^\infty] \to 0$$

is exact mod $\mathscr{C}$.

PROOF: This will follow from (2.1.2), (2.1.3.1-2), and (2.3), once we can identify Ш with $H^1(S, A)[p^\infty]$ (mod $\mathscr{C}$). But the obstruction to this identification is bounded by $H^1(S_\infty, F_\infty)$ ([28], Appendix).

2.5. We want to prove that the sequence of Λ-modules (2.4.1) is a sequence of "controlled" modules, in a sense to be made explicit later, but analogous to that utilized by Mazur in [28]; the purpose of this is to assure that $H^1(S_\infty, \tilde{A})^{G_i}$ is sufficiently close to $H^1(S_i, \tilde{A})$ – i.e., that one can descend diophantine information over the top of the tower to recover diophantine information in the individual layers. In order that this be possible, we have now to assume that A *has ordinary reduction at all primes dividing* p; otherwise, there is no way of knowing *a priori* that the sequence is controlled. We begin with a completely general lemma:

2.5.1. LEMMA: *Let H be a p-analytic group, M a discrete representation of H whose Pontryagin dual is a free $\mathbf{Z}_p$-module on m generators. Then, for every q, $H^q(H, M)$ is cofinite (i.e., its Pontryagin dual is finitely generated) over $\mathbf{Z}_p$, and the number of generators can be bounded in terms of* $\dim H = n$ *and* m.

PROOF: For every q, $H^q(H, M)$ is a p-primary torsion module.

However, the sequence

$$0 \longrightarrow M[p] \longrightarrow M \xrightarrow{\times p} M \longrightarrow 0 \tag{2.5.1.1}$$

is exact, by hypothesis, and $M[p]$ is a finite elementary abelian p-group. From (2.5.1.1) we obtain the exact cohomology sequences

$$H^q(H, M[p]) \longrightarrow H^q(H, M) \xrightarrow{\times p} H^q(H, M), \tag{2.5.1.2}$$

so that the number of congenerators of $H^q(H, M)$ is bounded by $\dim_{\mathbf{F}_p} H^q(H, M[p])$. As H module, $M[p]$ has a composition series all of whose quotients are one-dimensional over $\mathbf{F}_p$ (because H is a pro-p group); by devissage we are reduced to showing that $\dim_{\mathbf{F}_p} H^q(H, \mathbf{F}_p)$ ($\mathbf{F}_p$ necessarily has trivial H action) is bounded by a number depending only on n; in fact, it is bounded by the binomial coefficient $\binom{n}{q}$ ([24], V, 2.2.3.5).

We have in mind the following diagram, as in [28], p. 231:

$$\begin{array}{ccccccc}
 & & & & H^1(G_n, \tilde{A}(K_\infty)) & \prod_i \Psi_i & \\
 & & & & \downarrow & \downarrow & \\
0 \to H^1(S_n, \tilde{A}) & \to & H^1(S_n - T_n, \tilde{A}) & \to & \prod_{v_i \in T_n} H^2(S_{n,v_i}, \tilde{A}) & & \\
\varphi \downarrow & & \downarrow & & \downarrow & & \\
0 \to H^1(S_\infty, \tilde{A})^{G_n} & \to & H^1(S_\infty - T_\infty, \tilde{A})^{G_n} & \to & \prod_{w_i | v_i} (\mathrm{Coind}_{D_{w_i}}^{G_n}(H^2(S_{\infty,w_i}, \tilde{A})))^{G_n} & & \\
 & & \downarrow & & & & \\
 & & H^2(G_n, \tilde{A}(K_\infty)) & & & &
\end{array}$$

Here T_n is the set of primes of S_n ramified in S_∞, T_∞ the set of primes of S_∞ ramified over S_n, D_{w_i} the decomposition group of a typical w_i, and Ψ_i is defined as the kernel of $H^2(S_{n,v_i}, \tilde{A}) \to H^2(S_{\infty,w_i}, \tilde{A})^{D_{w_i}}$. The horizontal sequences are the long exact sequences of local cohomology; the first vertical sequence is the baseline of the Hochschild-Serre spectral sequence for étale extensions, and the second vertical sequence is exact by design.

By a simple diagram chase, we see that

(2.6.1) The order (resp. the number of generators) of $\ker \varphi$ is bounded above by the order (resp. the number of generators) of $H^1(G_n, \tilde{A}(K_\infty))$.

(2.6.2) The order (resp. the number of generators) of $\operatorname{coker} \varphi$ is bounded above by the order (resp. the number of generators) of

$H^2(G_n, \tilde{A}(K_\infty)) \oplus \Pi_i \Psi_i$. We are going to prove that the groups $H^\epsilon(G_n, \tilde{A}(K_\infty))$, $\epsilon = 1, 2$, and the groups Ψ_i, for all i, are *finite*; thus $\ker \varphi$ and $\operatorname{coker} \varphi$ are *finite. This theorem makes strong use of the hypothesis of ordinary reduction at primes dividing p.* Moreover, we shall prove that the number of generators of each of the groups $H^\epsilon(G_n, \tilde{A}(K_\infty))$, $\epsilon = 1, 2$, and Ψ_i is *bounded* independently of i and n; thus the number of generators of $\ker \varphi$ will be bounded, independently of n, and the number of generators of $\operatorname{coker} \varphi$ will be at most proportional to the number of elements of T_n, which is at most $p^{n(\dim G - 2)}$, up to a constant multiple. The techniques will be somewhat different from those of Mazur, and will depend upon a cohomological lemma of Serre [41] and the Weil-Riemann hypothesis for abelian varieties.

2.6.3. LEMMA: *The groups $H^\epsilon(G_n, \tilde{A}(K_\infty))$ are finite, $\epsilon = 1, 2$, and the number of generators of each of these groups is bounded independently of n.*

PROOF: The first statement is a theorem of Serre ([41], corollary to Theorem 2); we have used the fact that, if T_p is the Tate module of A and if $V_p = T_p \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$, then $\tilde{A} = V_p/T_p$. The second assertion follows immediately from 2.5.1.

2.6.4. LEMMA: *Let K be a p-adic field, with integer spectrum S; let A be an ordinary abelian scheme over S, let $L = K(A[p^\infty])$, and let $G = \operatorname{Gal}(L/K)$. Then, for all $n \geq 0$, $H^n(G, \tilde{A}(L))$ is a finite group.*

PROOF: As in the proof of the theorem of Serre referred to above, we need only prove that, if $\mathfrak{G}$ is the Lie algebra of G, then $H^n(\mathfrak{G}, V_p) = 0$, where V_p is, as before, the $\mathbf{Q}_p$-vector space generated by the Tate module of A. (The key is the comparison theorem of Lazard [24], *V*, 2.4.9). Since A is ordinary, we may choose a Frobenius element $F \in G$, and we may even assume that F fixes the subextension of L/K generated by the p^rth roots of unity, for all r (this is because the unipotent radical of G, considered as a subgroup of $GL(2g, \mathbf{Z}_p)$, $g = \dim A$, fixes the maximal unramified subextension of L *and* the p-cyclotomic extension of K). Then the eigenvalues of F on $V_p(A)$ will be algebraic integers $\lambda_1, \ldots, \lambda_{2g}$, which can be identified with the unit roots of (the H^1-part of) the zeta function of the reduction of A at the closed point of S, and with the inverses of these unit roots. By the Weil-Riemann hypothesis for abelian varieties, if q is the number of elements in the residue field of K, then

all the λ_i's will have complex absolute values equal to $q^{\pm 1/2}$, and in particular the product of k λ_i's will never be equal to the product $k+1$ λ_i's. Let $x \in \mathfrak{H}$ be $\log F$; then we have shown that x satisfies the hypothesis (P_n) of Theorem 1 of [41], for all n; the lemma then follows from that theorem.

2.7. LEMMA: *In the notation of* 2.6, *let* v_i *be an element of* T_n *of characteristic* p. *Then* Ψ_i *is a finite group, the number of whose generators is bounded independently of* n.

PROOF: For the sake of the proof of this lemma, we let K be a local field, S its integer spectrum, S_n the integer spectrum of $K_n = K(A[p^n])$, S' the integer spectrum of $L = \bigcup_n K_n$, and $G_n = \mathrm{Gal}(L/K_n)$; the divergence from our standard notation will be of no significance. We may then rewrite 2.6 in this local setting:

$$\begin{array}{ccccccccc} & & & & H^1(G_n, \tilde{A}(L)) & \longrightarrow & \Psi & & \\ & & & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & H^1(S_n, \tilde{A}) & \longrightarrow & H^1(K_n, \tilde{A}) & \longrightarrow & H^2(S_n, \tilde{A}) & \longrightarrow & 0 \\ & & \downarrow f & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & H^1(S', \tilde{A})^{G_n} & \longrightarrow & H^1(L, \tilde{A})^{G_n} & \longrightarrow & H^2(S', \tilde{A})^{G_n} & \longrightarrow & 0 \\ & & & & \downarrow & & & & \\ & & & & H^2(G_n, \tilde{A}) & & & & \end{array} \tag{2.7.1}$$

Here Ψ is just the previous Ψ_i, where the v_i and i have been suppressed, since we are in a purely local situation. The horizontal sequences are exact; the zeroes appear on the right because $H^2(S_n, \tilde{A}) = 0$, by local flat duality [29]. A diagram chase shows that, if coker f is finite, then so is $\Psi/(\mathrm{Im}\, g)$; since $\mathrm{Im}\, g$ is finite by 2.6.4, we need only show that coker f is finite to prove the lemma. Moreover, for any m, we have the commutative diagram (with exact rows)

$$\begin{array}{ccccccc} 0 & \longrightarrow & A(S_m) \otimes \mathbf{Q}_p/\mathbf{Z}_p & \longrightarrow & H^1(S_m, \tilde{A}) & \longrightarrow & H^1(S_m, A) \\ & & \| & & \downarrow & & \\ 0 & \longrightarrow & A(K_m) \otimes \mathbf{Q}_p/\mathbf{Z}_p & \longrightarrow & H^1(K_m, \tilde{A}) & & \end{array} \tag{2.7.2}$$

the equality on the left follows from the Néron property, and the whole sequence derives from the Kummer sequence 2.1.1 (F vanishes

because A has good reduction at primes dividing p). Since $H^1(S_m, A) = 0$ (by Lang's Theorem and the fact that A is connected), we see that coker f = coker $(A(K_n) \otimes \mathbf{Q}_p/\mathbf{Z}_p \xrightarrow{f'} (A(L) \otimes \mathbf{Q}_p/\mathbf{Z}_p)^{G_n})$.

Now we write, for each integer m, the exact sequences

$$(2.7.3.1) \qquad 0 \longrightarrow A[p^m] \longrightarrow A(L) \longrightarrow p^m A(L) \longrightarrow 0$$

$$(2.7.3.2) \qquad 0 \longrightarrow p^m A(L) \longrightarrow A(L) \longrightarrow A(L) \otimes \mathbf{Z}/p^m\mathbf{Z} \longrightarrow 0$$

Taking G_n-cohomology of 2.7.3.2, we imbed $(A(L) \otimes \mathbf{Z}/p^m\mathbf{Z})^{G_n}/(A(K_n) \otimes \mathbf{Z}/p^m\mathbf{Z})$ in $H^1(G_n, p^m A(L))$; and G_n-cohomology of 2.7.3.1 gives rise to the exact sequence

$$(2.7.3.3) H^1(G_n, A(L)) \longrightarrow H^1(G_n, p^m A(L)) \longrightarrow H^2(G_n, A[p^m]).$$

We want to know that Ψ is finite, and this will follow from the statements

$$(2.7.3.4) \qquad \varinjlim_m H^2(G_n, A[p^m]) \text{ is finite.}$$

$$(2.7.3.5) \qquad H^1(G_n, A(L)) \text{ is finite.}$$

Of these, 2.7.3.4 follows from 2.6.4. Let H be the inertia subgroup of G_n, of codimension one. By Hochschild-Serre, we need only show $H^1(G_n/H, A(L^H))$ and $H^1(H, A(L))^{G_n/H}$ are finite.

First, L^H/K_n is unramified by definition, and $G_n/H = \mathrm{Gal}(L^H/K_n)$; then $H^1(G_n/H, A(L^H)) = 0$, by [28], Prop. 4.3.

Write $A(L)$ as an extension

$$0 \longrightarrow A^0(L) \longrightarrow A(L) \xrightarrow{r} A^{\text{ét}}(L) \longrightarrow 0;$$

here r is the reduction at the closed point of S'. As H-modules, there is an exact sequence

$$0 \longrightarrow A^0(L) \longrightarrow (L^\times)^g \xrightarrow{\text{val}} \mathbf{Q}^g \longrightarrow 0; \quad (g = \dim A)$$

by Hilbert's Theorem 90, there is an isomorphism

$$\mathbf{Q}^g/(\text{val}((L^H)^\times)^g) \simeq H^1(H, A^0(L));$$

as G_n-module, the left-hand side is $A^0(L)_{\text{tors}}$, and so $H^0(G_n/H, H^1(H, A^0(L)))$ is finite. We have only to prove that $H^0(G_n/H, H^1(H, A^{ét}(L))$ is finite. But, since G_n/H is of cohomological dimension one, the natural restriction map (from Hochschild-Serre)

$$H^1(G_n A^{ét}(L)) \to H^0(G_n/H, H^1(H, A^{ét}(L)))$$

is surjective; and the left-hand group is just $H^1(G_n, \tilde{A}^{ét}(L))$, which is finite by Serre's Theorem, as in 2.6.4 (the eigenvalues of Frobenius on $\tilde{A}^{ét}(L)$ are a subset of the eigenvalues on $V_p(A)$).

This proves that Ψ_i is finite; the statement about the number of generators follows from 2.5.1 and the fact that the number of generators of Ψ_i is bounded by the number of generators of various cohomology groups of the type discussed in 2.5.1.

2.8. In order to complete the program described in 2.6, we have still to prove that Ψ_i is finite when v_i is of residue characteristic $l \neq p$. For this paragraph, we let K be an l-adic field, S its integer spectrum. We shall prove that $H^2_!(S, \tilde{A})$ is finite, and that the number of its generators depends only on A, and not on K. In fact, we have the local cohomology sequence

$$H^1(K, \tilde{A}) \to H^2_!(S, \tilde{A}) \to H^2(S, \tilde{A}); \tag{2.8.1}$$

we cannot set $H^2(S, \tilde{A}) = 0$ because A is not necessarily an abelian scheme over S. By Tate's local duality theorem [46] the exact sequence arising from 2.1.1 gives rise to

$$0 \to A(K) \otimes \mathbf{Q}_p/\mathbf{Z}_p \to H^1(K, \tilde{A}) \to (A(K) \otimes \mathbf{Z}_p)^* \to 0; \tag{2.8.2}$$

here * denotes Pontryagin dual, and A is the dual abelian variety to A. Since K is of residue characteristic prime to p, 2.8.2 implies that $H^1(K, \tilde{A})$ is finite, and the number of its generators depends only on A. On the other hand, for r sufficiently large, $H^2(S, \bar{A})$, where $\bar{A}$ is as in sequence (2.1.1.1)(p^r), vanishes by Lang's Theorem; then the sequences 2.1.1.1 imply $H^2(S, \tilde{A})$ is a subgroup of $H^2(S, A)[p^\infty] \simeq \varinjlim_r H^2(S, F_{p^r})$, which, as we saw in 2.1.4, is of finite order, depending only on A.

We summarize 2.6–2.8 as follows:

2.9. THEOREM: *Let φ_j be the natural map $H^1(S_j, \tilde{A}) \to H^1(S_\infty, \tilde{A})^{G_j}$, in the notation of* 2.2. *Then the number of generators of* $\ker \varphi_j$ *is*

bounded, independently of j, and the number of generators of coker φ_j *is* $O(p^{(\dim G-2)j})$.

PROOF: We have proved all but the last statement. As noted in 2.6, the number of generators of coker φ_j will be proportional to the number of elements in T_j, which is $O(\max_{v\in T}[G: D_vG_j])$; here T is the set of primes in K which ramify in K, and D_v is the decomposition group of such a prime. But D_v is of dimension at least two: in fact, K_∞ contains an infinite unramified extension at each v (for $v \nmid p$, this is true because A has good ordinary reduction at p; for $v \mid p$, there is the cyclotomic $\mathbf{Z}_p$-extension); and of course, the inertia group at each prime v is of dimension at least one. The theorem follows immediately.

2.10.1. COROLLARY: $H^1(S_\infty, \tilde{A})$ *is a cofinite* Λ_G*-module. Moreover, if* $H^1(S_0, \tilde{A})$ *is finite, i.e., if* $A(K_0)$ *and* $Ш(A, K_0)[p^\infty]$ *are finite, then* $H^1(S_\infty, \tilde{A})$ *is a cotorsion* Λ_G*-module.*

PROOF: The first assertion follows from 1.6, 2.9, and the weak Mordell-Weil theorem which asserts (in conjunction with 2.1.3.3) that $H^1(S_0, \tilde{A})$ is finitely cogenerated as a $\mathbf{Z}_p$-module. The second assertion follows from 2.9 and 1.7.

2.10.2. REMARK: $H^1(S_\infty, \tilde{A})$ will be cofinite even when A does not have ordinary reduction at all primes dividing p; Cf. 4.10, below.

2.11. COROLLARY: *The free rank of the Mordell-Weil group of* A *over* K_n *is bounded above by the cofree rank of* $H^1(S_\infty, \tilde{A})^{G_n}$; *if the Tate-Shafarevich conjecture is true, i.e., if* $Ш(K_n, A)$ *is finite, then these ranks are in fact equal. In particular, if* $H^1(S_\infty, \tilde{A})$ *is a cotorsion* Λ_G*-module, then*

(2.11.1) *Mordell-Weil rank of* A *over* $K_n = O(p^{n(\dim G-1)})$.

PROOF: All the assertions are immediate consequences of 2.9, with the exception of 2.11.1, which follows from 1.10.

2.12. The above corollaries indicate that one loses no information about Mordell-Weil groups by passing to an extension which trivializes the Galois module $A[p^\infty]$ (p a prime *ordinary* for A) and retaining the Galois module structure of the group of descents over

this extension. We give a few more details on this group of descents in §4; in principle, it is easier to compute once $A[p^\infty]$ has been trivialized.

§3. Iwasawa theory for p-analytic extensions

An ingredient in our computation of descents is the prior determination of the Galois group of the p-Hilbert class field of the summit K_∞ of the canonical tower; this Galois group will be called the *Iwasawa module* of the canonical tower. In this section, we prove, among other things, that the Iwasawa module is a torsion Λ-module. When Λ is commutative, this result is due to Ralph Greenberg [17]. Our use of Kummer theory is modeled on that of Iwasawa [21].

3.1. PROPOSITION: *Let K'/K be an extension of p-adic fields, with K finite over $\mathbf{Q}_p(\zeta_p)$, such that $H = \mathrm{Gal}(K'/K)$ is p-analytic, of the type considered in* 1.4. *Let M be the maximal abelian pro-p extension of K', and let $X = \mathrm{Gal}(M/K')$ be endowed with its natural structure as $\Lambda = \Lambda_H$-module. Then X is finitely generated over Λ.*

PROOF: Let K'' be the cyclotomic $\mathbf{Z}_p$-extension of K', $H' = \mathrm{Gal}(K''/K)$, M', X' the corresponding structures for K''. It is sufficient to prove the Proposition for K'', H', X': In fact, Λ_H is naturally a quotient of $\Lambda_{H'}$, and $\Lambda_H \otimes_{\Lambda_{H'}} X'$ maps to X with at most one-dimensional cokernel (generated by $\mathrm{Gal}(K''/K')$. We may thus assume that K' contains the p^nth roots of unity for all n, and drop the extra $'$.

By Kummer theory, it suffices to prove that $K'^\times \otimes \mathbf{Q}_p/\mathbf{Z}_p$ is cofinite; i.e., that $(K'^\times/(K'^\times)^p)^H$ is a *finite group*. Consider the exact sequences

$$0 \longrightarrow K'^\times/W \xrightarrow{p} K'^\times \longrightarrow K'^\times/(K'^\times)^p \longrightarrow 0 \tag{3.1.1}$$

$$0 \longrightarrow W \longrightarrow K'^\times \longrightarrow K'^\times/W \longrightarrow 0 \tag{3.1.2}$$

where W is the group of pth roots of unity. Taking cohomology in (3.1.1), we obtain the exact sequence $K^\times \to (K'^\times/(K'^\times)^p)^H \to H^1(H, K'^\times/W)$; the left-hand term is finitely generated, and (3.1.2) and Hilbert's Theorem 90 give an imbedding of $H^1(H, K'^\times/W)$ in $H^2(H, W)$, which is finite because H is p-analytic.

3.2. PROPOSITION: *Let K'/K be an extension of number fields, with K finite over $\mathbf{Q}(\zeta_p)$, such that $H = \mathrm{Gal}(K'/K)$ is p-analytic, of the type considered in* 1.4. *Assume that only a finite set T of primes in K ramify in K', and let M be the maximal abelian pro-p extension of K', unramified outside T; endow $X = \mathrm{Gal}(M/K')$ with its natural structure as $\Lambda = \Lambda_H$-module. Then X is finitely generated over Λ.*

PROOF: As in 3.1, we are reduced to proving that the subgroup $\mathcal{M}$ of $K^\times/(K^\times)^p$, represented by elements whose pth roots generate extensions of K' unramified outside T, is finite. As in [21], p. 273, $x \in K^\times$, $x(\mathrm{mod}(K^\times)^p) \in \mathcal{M}$ if and only if the principal T-ideal (i.e., that part of the ideal prime to T) generated by x becomes a pth power in K'; since K' is unramified outside T, the T-ideal (x) is already a pth power in the ideal group of K. Then, as in [21], p. 275, there is an exact sequence

$$(3.2.1) \qquad 0 \longrightarrow E_T \otimes \mathbf{Z}/p\mathbf{Z} \longrightarrow \mathcal{M} \longrightarrow C_T[p] \longrightarrow 0,$$

where E_T is the finitely generated group of T-units and C_T is the finite group of T-ideal classes of K. Since the end terms of (3.2.1) are finite, so is $\mathcal{M}$.

3.2.2. COROLLARY: *In the situation of* 3.2., *let L be the maximal unramified pro-p abelian extension of K'; let* $\mathrm{Iw}(K'/K) = \mathrm{Gal}(L/K')$, *endowed with its natural structure as Λ-module; then* $\mathrm{Iw}(K'/K)$ *is finitely generated over Λ.*

$\mathrm{Iw}(K'/K)$ will be called the *Iwasawa module* of the extension K'/K. We know even more about it:

3.3. THEOREM: *In the situation of* 3.2., $\mathrm{Iw}(K'/K)$ *is a torsion Λ-module.*

PROOF: Let $H = \mathrm{Gal}(K'/K)$ be an extension $1 \to R \to H \to J \to I$, with R solvable and J semisimple; we first prove the theorem with H replaced by J, K' replaced by $K'' = K'^R$. We know that $\mathrm{Iw}(K''/K)_J = \mathrm{Iw}(K''/K)/I_J\mathrm{Iw}(K''/K)$, where I_J is the augmentation ideal, is finitely generated over $\mathbf{Z}_p$ by 3.2. Suppose it has a $\mathbf{Z}_p$-free quotient, say $N = \mathrm{Gal}(L/K'')$, where L is unramified over K''. Then $W = \mathrm{Gal}(N/K)$ will be a central extension of J by N. We use the following lemma:

3.3.1. LEMMA: *Let J be a semi-simple p-analytic group of the type*

considered in 1.4, *and let* W *be a central extension of* J *by* $\mathbf{Z}_p^s$. *If* $[J, J]$ *is the derived subgroup of* J, *then there is a homomorphism* $[J, J] \xrightarrow{\gamma} W$ *such that, if* $W \xrightarrow{\alpha} J$ *is the natural map, then* $\alpha \circ \gamma$ *is the identity (i.e.,* W *splits on* $[J, J]$). *Moreover,* $W/\gamma[J, J]$ *is an abelian group.*

PROOF: By Levi's Theorem, the corresponding extension of Lie algebras splits; thus W splits on some open subgroup U of J. Since U is of finite index in J, the cocycle defining W in $H^2(J, \mathbf{Z}_p^s)$ is of finite order: in fact, because $H^1(U, \mathbf{Z}_p^s) = \mathrm{Hom}(U, \mathbf{Z}_p^s) = 0$, the Hochschild-Serre spectral sequence implies that the cocycle lifts from $H^2(J/U, \mathbf{Z}_p^s)$. (N.B.: We are dealing with *continuous* cohomology.) Say this cocycle is killed by p^n. Then, in the exact sequence

$$H^1(J, \mathbf{Z}_p^s/p^n\mathbf{Z}_p^s) \xrightarrow{\theta} H^2(J, \mathbf{Z}_p^s) \xrightarrow{\times p^n} H^2(J, \mathbf{Z}_p^s), \tag{3.3.1.1}$$

our cocycle is in the image of θ. But $H^1(J, \mathbf{Z}_p^s/p^n\mathbf{Z}_p^s) = \mathrm{Hom}(J, \mathbf{Z}_p^s/p^n\mathbf{Z}_p^s)$, and any element of the latter group dies in $H^1([J, J], \mathbf{Z}_p^s/p^n\mathbf{Z}_p^s)$. The sequence (3.3.1.1) maps into the corresponding sequence with J replaced by $[J, J]$; thus any cocycle in the image of θ dies in $H^2([J, J], \mathbf{Z}_p^s)$. The last statement is now a consequence of

3.3.1.2. SUBLEMMA: *Let* Y *be a central extension of the finite abelian* p*-group* G *by* $\mathbf{Z}_p^s$. *Then* Y *is an abelian group.*

PROOF: This is clear when G is cyclic. Now if H is any subgroup of G, $H^1(H, \mathbf{Z}_p^s) = \mathrm{Hom}(H, \mathbf{Z}_p^s) = 0$; consequently, if $G = H \times H'$, the Hochschild-Serre spectral sequence gives us a decomposition

$$H^2(G, \mathbf{Z}_p^s) \cong H^2(H, \mathbf{Z}_p^s) \times H^2(H', \mathbf{Z}_p^s),$$

and by induction, if G is the product of cyclic groups $G = H_1 \times H_2 \times \cdots \times H_r$, then $H^2(G, \mathbf{Z}_p^s) \cong \prod_1^r H^2(H_i, \mathbf{Z}_p^s)$; it follows that $H^2(G, \mathbf{Z}_p^s)$ is generated by abelian groups, and since the Baer sum of two abelian groups is again abelian, we are done.

We apply 3.3.1 to the extension L/K; it implies that $[J, J]$ lifts to a (necessarily normal) subgroup J' of W; $L^{J'}$ will be an *abelian* extension of K, and $\mathrm{Gal}(L^{J'}/K)$ will have the same free rank as $\mathrm{Iw}(K''/K)_J$. Let, for each $v \in T$, I_v be the inertia group of v in $L^{J'}$; I_v will be a finitely generated $\mathbf{Z}_p$-module, whose free rank is strictly less than the dimension of G. The quotient of $\mathrm{Gal}(L^{J'}/K)$ by the subgroup gener-

ated by the I_v will be the Galois group of an unramified abelian extension of K, and is therefore finite. We thus see that $\dim_{\mathbf{Q}_p} \mathbf{Q}_p \otimes_{\mathbf{Z}_p} \mathrm{Iw}(K''/K)_J \leq |T|$. Let $K'' = \bigcup_n K_n$, where $K_n = K''^{J_n}$, and where J_n is a filtration of J as in 1.4. Then the same argument gives

$$\dim_{\mathbf{Q}_p} \mathbf{Q}_p \otimes_{\mathbf{Z}_p} \mathrm{Iw}(K''/K)_{J_n} \leq |T_n|(\dim J), \tag{3.3.2}$$

where T_n is the set of primes of K_n lying over T. But every prime in T is ramified in K'', by assumption; in particular, for each prime $v \in T$, there is a subgroup $D_v \subset J$, of dimension at least one, which is the decomposition group of some prime of K'' dividing v. The number of primes of T_n lying over v will be $[J : J_n D_v] = O(p^{n(\dim J - \dim D_v)})$. Combining this with 3.3.2, we find (since T is *finite*)

$$\dim_{\mathbf{Q}_p} \mathbf{Q}_p \otimes_{\mathbf{Z}_p} \mathrm{Iw}(K''/K)_{J_n} = O(p^{n(\dim J - 1)}); \tag{3.3.3}$$

it then follows from 1.10 that $\mathrm{Iw}(K''/K)$ is torsion over Λ_J.

We now induct on the $\mathbf{Z}_p$-composition factors of R. Our task is thus reduced to proving the following statement:

3.3.4. LEMMA: *Let E/K be an extension, as in* 3.2, *such that* $\mathrm{Iw}(E/K)$ *is a torsion Λ_H-module, where* $H = \mathrm{Gal}(E/K)$. *Let $E' \supset E$ be a Galois extension of K, as in* 3.2, *with* $\mathrm{Gal}(E'/K) = H'$, $\mathrm{Gal}(E'/E) \simeq \mathbf{Z}_p$. *Then* $\mathrm{Iw}(E'/K)$ *is a torsion $\Lambda_{H'}$-module.*

PROOF: We more or less follow the argument of Greenberg [17]. Write $\Gamma = \mathrm{Gal}(E'/E)$, and let $X = \mathrm{Iw}(E'/K)_\Gamma$. Now X is the Galois group of an abelian extension $\tilde{M}/E'$ fixed by Γ; and since Γ has cohomological dimension one, $\tilde{M}$ is the lift of an abelian extension M/E with Galois group X; note that $\tilde{M}$ is unramified over E'. It follows that the only primes ramifying in M/E are those which ramify in E'/E; let T_E be the set of such primes. Then each $v \in T_E$ has an inertia group I_v of $\mathbf{Z}_p$-rank one in M/E; we are given that the quotient of X by the subgroup R generated by the I_v is torsion over Λ_H; it then follows from 1.9 that we will be done if we can find a $\Lambda_{H'}$-torsion submodule of $\mathrm{Iw}(E'/K)$ which maps onto R. Let D_v be the decomposition group of v in H'. Since only finitely many primes of K ramify in E', we may assume all the v's divide the same prime w of K. Then choose any such v, and choose a subgroup $\tilde{I}_v$ of $\mathrm{Iw}(E'/K)$ which reduces isomorphically to I_v. If v also divides w, then $v' = hv$ for some $h \in H'$; thus the $\Lambda_{H'}$-module generated by $\tilde{I}_v$ maps onto R;

but $\tilde{I}_v$ will be fixed by D_v; thus R is a quotient of $(\Lambda_{H'}/I_{D_v}\Lambda_{H'})^s$ for some s, and in particular is torsion.

3.4. Since Λ has a skew-field of fractions $\mathcal{K}$, we can associate to any finitely generated Λ-module M a numerical invariant, the *rank* of M, by setting $\operatorname{rank} M = \dim_{\mathcal{K}} \mathcal{K} \otimes_\Lambda M$. If $\Lambda = \Lambda_H$, let H_i be the usual filtration of H, and let I_{H_i}, as usual, be the (two-sided) ideal in Λ generated by $\{h - 1 \mid h \in H_i\}$.

3.4.1. LEMMA: *Let m be the rank of the finitely generated Λ-module M. Then* $\dim_{\mathbf{Q}_p} \mathbf{Q}_p \otimes_{\mathbf{Z}_p} M/I_{H_i}M = m[H : H_i] + O(p^{(n-1)i})$; *here* $n = \dim H$. (Note: $[H : H_i] = O(p^{ni})$).

PROOF: If M is Λ-free of rank m, then the conclusion of the lemma is obvious (without the $O(p^{(n-1)i})$). In general, if $T(M)$ is the torsion submodule of M, there is an exact sequence

$$T(M)/I_{H_i}T(M) \longrightarrow M/I_{H_i}M \longrightarrow (M/T(M))/I_{H_i}(M/T(M)) \longrightarrow 0; \tag{3.4.1.1}$$

it follows from 1.10 (applied to the leftmost term of 3.4.1.1) that we may assume M is torsion-free. Thus we may assume that there exists a free, rank m Λ-module V (resp. V') containing (resp. contained in) M, such that V/M (resp. M/V') is a torsion Λ-module. We have

$$M/I_{H_i}M \longrightarrow V/I_{H_i}V \longrightarrow (V/M)/I_{H_i}(V/M) \longrightarrow 0 \tag{3.4.1.2}$$

and

$$V'/I_{H_i}V' \longrightarrow M/I_{H_i}M \longrightarrow (M/V')/I_{H_i}(M/V') \longrightarrow 0. \tag{3.4.1.3}$$

From 3.4.1.2 and 1.10 (applied to V/M) we conclude that

$$\dim_{\mathbf{Q}_p} \mathbf{Q}_p \otimes_{\mathbf{Z}_p} M/I_{H_i}M \geq m[H : H_i] + O(p^{(n-1)i});$$

from 3.4.1.3 and 1.10 (applied to M/V') we obtain the reverse inequality, and the lemma follows.

3.5. Let X be as in 3.2; we want to compute the rank of X. We are going to have to assume that K' contains the p^nth roots of unity for all n. Then Kummer theory sets X in duality with a subgroup $\mathcal{M}$ of $K'^{\times} \otimes \mathbf{Q}_p/\mathbf{Z}_p$. If $\mathcal{M}^{H_i} \simeq (\mathbf{Q}_p/\mathbf{Z}_p)^{d_i} \oplus$ (finite group), then the rank of X will be that number m such that $d_i = m[H : H_i] + O(p^{(n-1)i})$. Let T be as in 3.2; then, as in ([21], p. 275), there is an exact sequence

$$0 \longrightarrow E_T \otimes \mathbf{Q}_p/\mathbf{Z}_p \longrightarrow \mathcal{M} \longrightarrow A_T \longrightarrow 0, \tag{3.5.1}$$

where E_T is the group of T-units of K' and A_T is the p-part of the group of T-ideal classes (i.e., ideal classes represented by ideals prime to T) of K'. In both cases, the group for K' is the direct limit of the corresponding groups for subfields of K' finite over K.

We first show that A_T contributes nothing to the rank of X.

3.6. PROPOSITION: *The module A_T is cotorsion over Λ.*

PROOF: Iwasawa's proof of the analogous theorem for the cyclotomic $\mathbf{Z}_p$-extension is very long, owing to the number of technical facts about $\Lambda_{\mathbf{Z}_p}$-modules which enter into the proof. We sketch the generalization of these facts to Λ_G in the following paragraph; the details are easy to check. (Cf. [21]).

Thus, let $\nu_{i,j} \in \Lambda_{H_i} \subset \Lambda$ be an element whose image in $\mathbf{Z}_p[H_i/H_j]$ is equal to $\Sigma_{h \in H_j/H_i} h$. Then $\nu_{i,j} I_{H_i}$ is evidently contained in I_{H_j}, and so $x \to \nu_{i,j} x$ induces a map $f_{i,j}: M/I_{H_i}M \to M/I_{H_j}M$, if M is any compact Λ-module. These maps do not depend on the choice of $\nu_{i,j}$, and satisfy the compatibility $f_{j,k} \circ f_{i,j} = f_{i,k}$; thus they give rise to a direct system $\varinjlim_{f_{i,j}}(M/I_{Hi}M) = M^?$. Suppose we are given, for each pair $i, j, i < j$, a commutative diagram of Λ-modules, with exact rows:

$$\begin{array}{ccccc} M/I_{H_i}M & \longrightarrow & N_i & \longrightarrow & 0 \\ \downarrow f_{i,j} & & \downarrow & & \\ M/I_{H_j}M & \longrightarrow & N_j & \longrightarrow & 0 \end{array} \tag{3.6.1}$$

where N_i, N_j are *finite groups*; then $M^?$ maps onto $\varinjlim N_i = N^?$, and $N^?$ is a discrete Λ-module, with compact Pontryagin dual $N^!$. Now the map $g \to g^{-1}$ in H gives rise to a $\mathbf{Z}_p$-linear involution of Λ, which we denote by $\lambda \to \lambda^!$. The compatibility in notation is that, if λ annihilates every element of M, then $\lambda^!$ annihilates every element of $N^!$ (the action of H on the Pontryagin dual $\mathrm{Hom}(A, \mathbf{Q}_p/\mathbf{Z}_p)$ is given by $g(f(x)) = f(g^{-1}x)$, where $x \in A$, $g \in H$, and $f \in \mathrm{Hom}(A, \mathbf{Q}_p/\mathbf{Z}_p)$); in other words, $N^!$ is a torsion Λ-module.

Let A_i be the p-part of the ideal class group of K_i, and let $A = \varinjlim_i A_i$. If L_i is the maximal unramified abelian p-extension of K_i, there are canonical maps $\mathrm{Iw}(K'/K)/I_{H_i}\mathrm{Iw}(K'/K) \to \mathrm{Gal}(K'L_i/K') \to A_i = \mathrm{Gal}(L_i/K_i)$. Of these, the first is surjective, and the second has

cokernel isomorphic to $\mathrm{Gal}(L_i \cap K'/K_i)$, which has at most $n = \dim H$ generators (cf. [21]). Theorem 7 applies in the present case as well, to provide a commutative diagram (Cf. [48], 11.3)

$$\begin{array}{ccc} \mathrm{Iw}(K'/K)/I_{H_i}\mathrm{Iw}(K'/K) & \longrightarrow & 0 \\ \Big\downarrow f_{i,j} & & \Big\downarrow \text{inclusion} \\ \mathrm{Iw}(K'/K)/I_{H_j}\mathrm{Iw}(K'/K) & \longrightarrow & 0 \end{array} \qquad j \geq i$$

Thus we have an exact sequence $\mathrm{Iw}(K'/K)^? \xrightarrow{\varphi} A \to \varprojlim_i (\mathrm{Gal}(L_i \cap K'/K_i)) \to 0$; the cokernel term is evidently cotorsion, and by 3.3 and the preceding argument, so is $\mathrm{Im}\,\varphi$; thus A, and hence its submodule A_T, is a cotorsion Λ-module.

3.7. We conclude from (3.5.1) and 3.6 that our task is to compute $(E_T \otimes \mathbf{Q}_p/\mathbf{Z}_p)^{H_i}$, up to $O(p^{(n-1)i})$; in fact, it suffices to compute the divisible part, by 3.4.1. We may as well replace E_T with E_T/W, where W is the group of roots of unity in K'. Let $\mathbf{Z}' = \mathbf{Z}\left[\frac{1}{p}\right]$; then there is an exact sequence

$$(3.7.1) \qquad 0 \longrightarrow E_T/W \longrightarrow E_T/W \otimes \mathbf{Z}' \longrightarrow E_T/W \otimes \mathbf{Q}_p/\mathbf{Z}_p \longrightarrow 0$$

which gives rise to an injection

$$(3.7.2) \qquad (E_T/W \otimes \mathbf{Q}_p/\mathbf{Z}_p)^{H_i}/(E_T/W \otimes \mathbf{Z}')^{H_i} \otimes \mathbf{Q}_p/\mathbf{Z}_p \hookrightarrow H^1(H_i, E_T/W).$$

The exact sequence $0 \to W \to E_T \to E_T/W \to 0$, combined with 2.5.1 applied to W, gives rise to an exact sequence

$$B_1 \longrightarrow H^1(H_i, E_T) \longrightarrow H^1(H_i, E_T/W) \longrightarrow B_2,$$

where B_1 and B_2 are cogenerated by a set of finite cardinality independent of i. Thus, in computing the contribution of $H^1(H_i, E_T/W)$ to the rank of X, it suffices to compute the divisible part of $H^1(H_i, E_T)$:

3.7.3. Lemma: *There is an isomorphism* $\mathrm{Ker}(A_{T,i} \to A_T) \to H^1(H_i, E_T)$; *in particular,* $H^1(H_i, E_T)$ *is finite, hence has no divisible part.* (Here $A_{T,i}$ is the T-ideal class group of K_i.)

PROOF: Let $E_{T,i}$ be the T-unit group of K_i; let $I_{T,i}$ and $P_{T,i}$ be respectively the T-ideal group and principal T-ideal group of K_i, and let $I_T = \varinjlim_i I_{T,i}$, $P_T = \varinjlim_i P_{T,i}$. The exact sequence

$$1 \longrightarrow E_T \longrightarrow K'^{\times} \longrightarrow P_T \longrightarrow 1 \tag{3.7.3.1}$$

gives, thanks to Hilbert's theorem 90, an isomorphism $P_T^{H_i}/P_{T,i} \simeq H^1(H_i, E_T)$ (note that $K'^{\times H_i} = K_i^{\times}$). Now $I_T^{H_i} = I_{T,i}$, because only ideals in T ramify in K'/K_i; since $P_T \subset I_T$, it follows that $P_T \subset I_{T,i}$, and thus consists precisely of those ideals in K_i which become principal in K'. Thus $P_T^{H_i}/P_{T,i}$ is the group of ideal classes of K_i which become principal in K', i.e. $P_T^{H_i}/P_{T,i} = \mathrm{Ker}(A_{T,i} \to A_T)$.

3.8. It remains only to compute the divisible part of $(E_T/W \otimes \mathbf{Z}')^{H_i} \otimes \mathbf{Q}_p/\mathbf{Z}_p$. Now $(E_T/W \otimes \mathbf{Z}')^{H_i}$ is just $E_{T,i}/W \cap E_{T,i} \otimes \mathbf{Z}'$; in other words, we have only to compute the free rank of $E_{T,i}$ as $\mathbf{Z}$-module. Let T_i be the set of points of S_i dividing primes in T. Note that K_i is totally imaginary (it contains the pth roots of unity). We conclude that

$$\text{rank } E_{T,i} = \tfrac{1}{2}[K:\mathbf{Q}][H:H_i] + |T_i| - 1. \tag{3.8.1}$$

Since each prime in T has a non-trivial inertia group in H, we see that $|T_i| = O(p^{(n-1)i})$. Summarizing, we have

3.9. THEOREM: *Let K''/K be an extension of the number field K, $[K:\mathbf{Q}]$ finite. Assume that $H = \mathrm{Gal}(K'/K)$ is p-analytic of the type considered in* 1.4. *Assume furthermore that K contains the pth roots of unity, and that K' contains the p^nth roots of unity for all n. Assume, finally, that the set T of primes of K ramifying in K' is finite. Let X be the Galois group of the maximal abelian p-extension of K' in which only primes dividing primes in T ramify. Then the rank of X as a $\Lambda = \Lambda_H$-module is exactly $\frac{1}{2}[K:\mathbf{Q}]$.*

3.10. REMARK: We have proved the weakest possible result, in the sense that we have failed to examine the torsion part of X, and we have neglected to characterize further the nature of possible imbeddings of X/(torsion) in free Λ-modules; such concerns figure significantly in the work of Iwasawa, and in that of others who have followed him (Cf. especially [21], [8], [19]). We hope to be able to return to these questions.

3.11. Finally, we work out the local analogue of 3.9; i.e., we

compute the Λ_H-rank of the module X in 3.1, assuming K' contains the p^nth roots of unity for all n. As before, we have to compute the $\mathbf{Z}_p$ coranks of $(K'^{\times} \otimes \mathbf{Q}_p/\mathbf{Z}_p)^{H_i}$; as in 3.7, the difference between the latter group and $(K'^{H_i})^{\times} \otimes \mathbf{Q}_p/\mathbf{Z}_p$ is measured by $H^1(H_i, K'^{\times}/W)$, where W is the group of roots of unity in K'; and this difference is insignificant. Since $(K'^{H_i})^{\times}$ has $\mathbf{Z}_p$-rank equal to $[K:\mathbf{Q}_p][H:H_i]$, we conclude, via 3.4.1, that

3.12. PROPOSITION: *The module X in* 3.1 *has Λ_H-rank $[K:\mathbf{Q}_p]$, if H contains the p^nth roots of unity for all n.*

§4. Untwisting the wild ramification

We are now ready to compute the descent modules $H^1(S_\infty, \tilde{A})$, introduced in Section 2, in terms of class field theory of the sort described in Section 3. In this section we examine the contribution ot the descent of the wild ramification at primes dividing p; in Section 5 we obtain examples for which this contribution is represented by a torsion Λ-module.

4.0. NOTATION, Part I: We recall that A_K is an abelian variety over a number field K, of dimension d, and A is its Néron model over $\mathrm{Spec}(O_K) = S$. We have chosen an *odd* prime p such that at every point of S of residue characteristic p, A has good ordinary reduction; associated to this information we have the canonical tower of number fields $K \subset K_0 \subset K_1 \subset \cdots \subset K_i \subset \cdots \subset K_\infty$, with notation as in 2.2; thus $G_i = \mathrm{Gal}(K_\infty/K_i)$ is p-analytic for $i = 0, 1, \ldots$. We write $G = G_0$, and $\tilde{G} = \mathrm{Gal}(K_\infty/K)$.

We are going to assume that $K = \mathbf{Q}$; although it would be relatively straightforward to treat the general case, it would require an unjustifiable prodigality with notation – unjustifiable because (at the moment) there are no examples available in which the module of descents is Λ-torsion, except when $K = \mathbf{Q}$.

The primes of S_i dividing p will be denoted $\mathcal{P}_{i,s}$. To each such $\mathcal{P}_{i,s}$ is associated a free rank d $\mathbf{Z}/p^{i+1}\mathbf{Z}$-submodule of the group (or group scheme) $A[p^{i+1}](S_i)$: namely, the connected component of the latter at $\mathcal{P}_{i,s}$. This rank d module will be denoted $L_{i,s}$. The primes of S_∞ dividing p will be denoted v, or v_s; the corresponding submodule of $\tilde{A}$ isomorphic to $(\mathbf{Q}_p/\mathbf{Z}_p)^d$ will be called L_v (resp. L_s). If v divides $\mathcal{P}_{i,s}$, then evidently $L_{i,s} \subset L_v$. To an L_v corresponds a parabolic subgroup of $GL(2d, \mathbf{Z}_p)$, denoted P_{L_v}; the canonical imbedding of $\tilde{G}$ in

$GL(2d, \mathbf{Z}_p)$ represents the decomposition group D_v as a subgroup of P_{L_v}. We say that a $\mathfrak{P}_{i,s}$ *belongs to* the stabilizer P_L of a rank d submodule L of $\mathbf{Z}_p^{2d}$ if P_L is P_{L_v} for some $v \in S_\infty$ dividing $\mathfrak{P}_{i,s}$.

4.1. As in 2.2.1, we find that, over S_i, $A[p^{i+1}]$ is a finite flat subgroup scheme of A (we continue to write A for the Néron model, regardless of the base scheme), and in particular is étale away from primes dividing p. By local flat duality [29], $H^1_{\cdot}(S_{i,\mathfrak{P}_{i,s}}, A[p^{i+1}])$ vanishes; the local cohomology sequences for $(\mathbf{Z}/p^{i+1})^{2d}$ and $A[p^{i+1}]$ then give

$$\begin{array}{ccccc} 0 \longrightarrow & H^1(S_i, (\mathbf{Z}/p^{i+1}))^{2d} & \to & H^1(S_i - T_i, (\mathbf{Z}/p^{i+1})^{2d}) \\ & \downarrow & & \| \\ 0 \longrightarrow & H^1(S_i, A[p^{i+1}]) & \longrightarrow & H^1(S_i - T_i, A[p^{i+1}]) \\ & & \longrightarrow & \oplus_s H^2_{\cdot}(S_{i,\mathfrak{P}_{i,s}}, A[p^{i+1}]) \end{array} \tag{4.1.1}$$

here T_i is the set of primes of S_i dividing p. (We are making use of App., 1.0.2.4.) It follows from (4.1.1) that $H^1(S_i, A[p^{i+1}])$ contains as a subgroup $\mathrm{Hom}(C(K_i), (\mathbf{Z}/p^{i+1})^{2d})$, where $C(K_i)$ is the ideal class group of K_i; in the limit, then, there is an imbedding

$$\mathrm{Hom}(\mathrm{Iw}(K_\infty/K_0), (\mathbf{Q}_p/\mathbf{Z}_p)^{2d}) \to H^1(S_\infty, \tilde{A});$$

this is an imbedding of $\Lambda = \Lambda_G$-modules if G acts on $(\mathbf{Q}_p/\mathbf{Z}_p)^{2d}$ by its representation on $\tilde{A}$. We know already (3.3) that the left-hand side is a cotorsion Λ-module; we are now concerned with its cokernel, which we represent as

$$\begin{aligned} &\varinjlim_i(\mathrm{Coker}(\mathrm{Hom}(C(K_i), (\mathbf{Z}/p^{i+1})^{2d}) \to H^1(S_i, A[p^{i+1}]))) \\ &\overset{\text{def.}}{=} \varinjlim_i(H^1(S_i, A[p^{i+1}])/J_i) \\ &\overset{\text{def.}}{=} \varinjlim_i \Phi_i. \end{aligned}$$

Now 4.1.1 represents Φ_i as a subgroup of $H^1(S_i - T_i, (\mathbf{Z}/p^{i+1})^{2d})/(\mathrm{Im}\, J_i)$, which in turn can be realized as $\mathrm{Hom}(K_{i\mathbf{A}}^\times/K_i^\times(U_{S_i-T_i}), (\mathbf{Z}/p^{i+1})^{2d})/(\mathrm{Im}\, J_i)$; here $K_{i\mathbf{A}}^\times$ is the idèle group of K_i and, if V is a subset of S_i, then $U_V = \prod_{v \in V} U_v$, where U_v is the local unit group at v. The assertion with which this paragraph began is an obvious consequence of class field theory. Let the bottom line of (4.1.1) be rewritten $0 \to A \to B \to C$; then there is a commutative diagram

$$
\begin{array}{ccccccc}
0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C \\
 & & \downarrow & & \beta\downarrow & & \| \\
0 & \longrightarrow & \oplus_s H^1(S_{i,\mathscr{P}_{i,s}}, A[p^{i+1}]) & \xrightarrow{\gamma} & \oplus_s H^1(K_{i,\mathscr{P}_{i,s}}, A[p^{i+1}]) & \longrightarrow & C
\end{array}
\tag{4.1.2}
$$

From (4.1.2), we conclude that Φ_i is that subgroup of B whose image under β is contained in the image of γ; all these identifications are mod J_i (unramified extensions).

Let $\mathscr{P}$ be a typical $\mathscr{P}_{i,s}$. We have assumed that A is *ordinary* at $\mathscr{P}$. Thus $A[p^{i+1}] \simeq (\mathbf{Z}/p^{i+1})^d \times (\mu_{p^{i+1}})^d$ over $S_{i,\mathscr{P}}$, the latter factor being canonically imbedded. The portion of γ arising from $\mathscr{P}$ may then be imbedded in the diagram (4.1.3) below:

$$
\begin{array}{ccccccccc}
0 & \to & (H^1(S_{i,\mathscr{P}}, \mu_{p^{i+1}}))^d & \longrightarrow & H^1(S_{i,\mathscr{P}}, A[p^{i+1}]) & \longrightarrow & (H^1(S_{i,\mathscr{P}}, \mathbf{Z}/p^{i+1}))^d & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & (\mathrm{Hom}(K_{i,\mathscr{P}}^{\times}, \mathbf{Z}/p^{i+1}))^d & \to & \mathrm{Hom}(K_{i,\mathscr{P}}^{\times}, (\mathbf{Z}/p^{i+1})^{2d}) & \to & (\mathrm{Hom}(K_{i,\mathscr{P}}^{\times}, \mathbf{Z}/p^{i+1}))^d & \to & 0
\end{array}
\tag{4.1.3}
$$

Now

(4.1.3.1) The image of the right-hand map consists of unramified extensions of $S_{i,\mathscr{P}}$.

(4.1.3.2) Kummer theory gives us the exact sequence $U_{\mathscr{P}}/U_{\mathscr{P}}^{p^{i+1}} \hookrightarrow H^1(S_{i,\mathscr{P}}, \mu_{p^{i+1}}) \to H^1(S_{i,\mathscr{P}}, \mathbf{G}_m)$; the rightmost term vanishes, because $\mathbf{G}_m$ is smooth and connected. Thus the image of the left-hand map in (4.1.3) consists of extensions obtained by taking p^{i+1}st roots of elements of U; in terms of class field theory, these are represented by maps from $K_{i,\mathscr{P}}^{\times}$ to $\mathbf{Z}/p^{i+1}$ (in our situation, coming in d-tuples) which vanish on $U_{\mathscr{P}}^{\perp}$, the orthogonal complement to $U_{\mathscr{P}}$ under the norm residue mapping. We note for the future that $U_{\mathscr{P}}^{\perp} \subset U_{\mathscr{P}}$.

(4.1.3.3) Since the subgroup scheme $(\mu_{p^{i+1}})^d \subset A[p^{i+1}]$ is exactly $L_{i,s}$, if $\mathscr{P} = \mathscr{P}_{i,s}$, we obtain the following characterisation of the image of γ.

4.2. Lemma: *With the natural identifications, the image of* γ *in* (4.1.2) *may be realized as*

$$
\left\{ f \in \mathrm{Hom}\left(\prod_s (K_{i,\mathscr{P}_{i,s}}^{\times}/U_{\mathscr{P}_{i,s}}^{\perp}), (\mathbf{Z}/p^{i+1})^{2d} \right) \mid f(U_{\mathscr{P}_{i,s}}) \subset L_{i,s} \right\}. \tag{4.2.1}
$$

4.3. The group in (4.2.1) has a subgroup $N_i = \mathrm{Hom}(\Pi_s(K_{i,\mathscr{P}_{i,s}}^{\times}/U_{\mathscr{P}_{i,s}}), (\mathbf{Z}/p^{i+1})^{2d})$; the group J_i of 4.1 is taken into N_i under the natural map; moreover, any element of A (Cf. 4.1.2) which maps to N_i induces an unramified homomorphism of

$\Pi_s \mathrm{Gal}(\bar{K}_{i,\mathcal{P}_{i,s}}/K_{i,\mathcal{P}_{i,s}})$ into $(\mathbf{Z}/p^{i+1})^{2d}$; i.e., comes from J_i. Thus we may naturally identify Φ_i with a submodule of $(4.2.1)/N_i$; but this is just

$$(4.3.1)\quad \left\{ f \in \mathrm{Hom}\left(\prod_s U_{\mathcal{P}_{i,s}}/U^{\perp}_{\mathcal{P}_{i,s}}, (\mathbf{Z}/p^{i+1})^{2d} \,\middle|\, f(U_{\mathcal{P}_{i,s}}) \subset L_{i,s} \right\} \overset{\text{def.}}{=} \Omega_i.$$

We record what we have done to this point:

4.3.2. MNEMONIC: The module $H^1(S_\infty, \tilde{A})$ is an extension of $\varinjlim_i \Phi_i \subset \varinjlim_i \Omega_i$ by $\mathrm{Hom}(\mathrm{Iw}(K_\infty/K_0), \tilde{A})$.

4.4. We may identify the Ω_i of 4.3.1 with a coinduced $\Lambda/I_{G_i}\Lambda$-module, namely with

$$(4.4.1)\qquad \mathrm{Coind}_{P_L \cap \tilde{G}/P_L \cap G_i}^{\tilde{G}/G_i} \left(\mathrm{Hom} \prod_s{}^{L} U_{\mathcal{P}_{i,s}} \Big/ U^{\perp}_{\mathcal{P}_{i,s}}, L \right).$$

Here $\prod_s^L$ means the product is taken over those s such that $\mathcal{P}_{i,s}$ belongs to P_L; the L chosen must be a rank d submodule such that the set of $\mathcal{P}_{i,s}$ belonging to P_L is not empty. Thus all the decomposition groups $D_{i,s}$ of the $\mathcal{P}_{i,s}$ appearing in 4.4.1 are contained in $P_L \cap \tilde{G}$, and conversely, any element of $\tilde{G}$ which lies in P_L must stabilize the set of $\mathcal{P}_{i,s}$ which belong to P_L; thus 4.4.1 has a meaning which evidently identifies it with Ω_i. Taking the limit, we obtain

$$(4.4.2)\qquad \varinjlim_i \Omega_i \simeq \mathrm{Coind}_{P_L \cap \tilde{G}}^{\tilde{G}} \left(\mathrm{Hom} \prod_s{}^{L} U_v/U_v^{\perp}, L \right);$$

here $U_v = \varprojlim_{v|\mathcal{P}_i} U_i$, the inverse limit being taken with respect to the norm maps; $U_v^{\perp}$ is defined similarly, and the remaining notation is defined according to the plane of 4.4.1. Now $\varinjlim_i \Omega_i$ is represented, by means of 4.4.2, as a submodule of

$$(4.4.3)\quad \mathrm{Coind}_{P_L \cap \tilde{G}}^{\tilde{G}} \left(\mathrm{Hom} \prod_v{}^{L} U_v/U_v^{\perp}, \tilde{A} \right) \simeq \mathrm{Hom}(\mathrm{Ind}_{D_v \cap \tilde{G}}^{\tilde{G}}(U_v/U_v^{\perp}), \tilde{A}),$$

where D_v is the decomposition group of some $v \in S_\infty$. Now, U_v is isomorphic, via local class field theory, to the module X of 3.1 *a priori*, it is only isomorphic up to something of $\mathbf{Z}_p$-rank one, coming from the maximal (local) unramified p-extension; but this is already contained in $K_{\infty,v}$, because A is ordinary); and U_v has $\mathbf{Z}_p$-rank at most one; thus $U_v/U_v^{\perp}$ has $\Lambda_{D_v \cap G}$-rank equal to $[K_{0,v}:\mathbf{Q}_p]$, by 3.11, where $K_{0,v}$ is the completion of K_0 at the restriction to K_0 of v. It follows

that $\mathrm{Ind}_{D_v \cap \tilde{G}}^{\tilde{G}}(U_v/U_v^+)$ has Λ_G-rank equal to $[K_0:\mathbf{Q}]$, and therefore that the right-hand side of 4.4.3 has Λ_G-corank equal to $2d[K_0:\mathbf{Q}]$. Similarly, the right-hand side of 4.4.2 has Λ_G-corank equal to $d[K_0:\mathbf{Q}]$.

4.5. We are now ready to globalize. First, denote the right-hand side of 4.4.3 (resp. 4.4.2) by Y_0 (resp. Y_1). Let Y_2 be the submodule of Y_0 consisting in homomorphisms which are trivial on the subgroup $\bar{E}$ of $\mathrm{Ind}_{D_v \cap \tilde{G}}^{\tilde{G}}(U_v/U_v^+)$, where $\bar{E}$ is the closure of the (inverse limit with respect to norm maps of the) global units. We make two claims:

4.5.1. Y_2 has Λ_G-corank equal to $d[K_0:\mathbf{Q}]$.

4.5.2. In the notation of 4.3, $\varinjlim \Phi_i = Y_1 \cap Y_2$, where Y_1 and Y_2 are considered as submodules of Y_0.

PROOF OF 4.5.1: It suffices to prove that $\mathrm{Ind}_{D_v \cap \tilde{G}}^{\tilde{G}}(U_v)/\bar{E}$ has rank $[K_0:\mathbf{Q}]/2$. Let X be as in 3.2, with $K'/K = K_\infty/K_0$ (for now). X is a Galois group, and class field theory identifies $\mathrm{Ind}_{D_v \cap \tilde{G}}^{\tilde{G}}(U_v)/\bar{E} \simeq (\prod_v U_v)/\bar{E}$ with the subgroup X' of X which fixes L, the maximal abelian p-extension of K_∞ ramified only at the primes in T-{primes dividing p}, in the notation of 3.2. Now $\mathrm{Gal}(L/K_\infty)$ can be shown to be a torsion Λ_G-module by the same techniques used to prove 3.3. (Alternatively, the difference between $\mathrm{Gal}(L/K_\infty)$ and $\mathrm{Iw}(K_\infty/K_0)$ is given by the inertia groups of the primes lying over primes in T but not dividing p; but these inertia groups are trivial, because the maximal p-extension of $K_{0,w}$, for any $w \in T$, not dividing p, is already contained in $K_{\infty,w'}$, for w' an extension of w to K_∞; we conclude by invoking 3.3.) Thus rank X' = rank $X = [K_0:\mathbf{Q}]/2$, by 3.9.

The truth of 4.5.2 is evident.

Thus $\varinjlim_i \Phi_i$ is cotorsion if and only if $Y_1 \cap Y_2$ is, and by the rank computations in 4.4 and 4.5.1, this is true if and only if $Y_1 + Y_2$ is a Λ_G-submodule of Y_0 of maximum corank. Encouraged by the fact that our rank computations allow the possibility that $Y_1 \cap Y_2$ be cotorsion, we state the following

4.6. CONJECTURE: *$H^1(S_\infty, \tilde{A})$ is a cotorsion module, when A has good ordinary reduction at p.*

In Section 5, we find examples of elliptic curves for which the conjecture is satisfied; we note that the conjecture is a consequence

of a conjecture of Mazur in [28] on the analogue for the cyclotomic $\mathbf{Z}_p$-extension (this is 5.1.1, below); and we prove the conjecture for elliptic curves with complex multiplication, in case K is abelian over the complex multiplication field; our proof makes essential use of Brumer's work [5] on Leopoldt's conjecture, with which 4.6 has evident structural similarities.

We summarize those results we have proved in this section:

4.7. THEOREM: *Let A be an abelian variety over $\mathbf{Q}$ ordinary at p. Let $\mathbf{Q} \subset K_0 \subset K_1 \subset \cdots \subset K_\infty$ be the canonical tower associated to A, and let S_i be the integer spectrum of K_i. Let $G = \mathrm{Gal}(K_\infty/K_0)$. Then $H^1(S_\infty, \tilde{A})$ is an extension by $\mathrm{Hom}(\mathrm{Iw}(K_\infty/K_0), \tilde{A})$ of the following module*:

$$(4.7.1) \qquad \left\{ f \in \mathrm{Hom}\left(\left(\prod_v U_v \Big/ U_v^{\perp} \right) \Big/ E, \tilde{A} \right) \Big| f(U_v) \subset L_v \right\},$$

where v runs through the primes of S_∞ dividing p, U_v, $U_v^{\perp}$, and $\bar{E}$ are as in 4.4 *and* 4.5, *and L_v is the connected component of $\tilde{A}$ at v; this is an extension of modules over $\tilde{G} = \mathrm{Gal}(K_\infty/\mathbf{Q})$. Furthermore, $\mathrm{Hom}(\prod_v U_v/U_v^{\perp}, \tilde{A})$ is a Λ_G-module Y_0 whose Pontryagin dual has (torsion-free) rank $2d[K_0:\mathbf{Q}]$, where $d = \dim A$; and the submodules Y_1, Y_2 of Y_0 defined by the conditions that $f(U_v) \subset L_v$ (resp. $f(\bar{E}) = 0$) are each of corank $d[K_0:\mathbf{Q}]$: $H^1(S_\infty, \tilde{A})$ is cotorsion if and only if Y_1 and Y_2 generate Y_0 (up to cotorsion modules), and in any case* (4.7.1) $= Y_1 \cap Y_2$.

4.8. The usefulness of this theorem is that one can (in principle) compute $\mathrm{Iw}(K_\infty/K_0)$ and (4.7.1) and therefore compute $H^1(S_\infty, \tilde{A})$. The usefulness of the latter is demonstrated, in some cases, by Proposition 5.10, below, which states that, once one knows $H^1(S_\infty, \tilde{A})$ as a G-module, one also knows the divisible part of $H^1(S', \tilde{A})$, when S' is the integer spectrum of any finite extension K' of K contained in K_∞. The Tate-Shafarevich conjecture is that the number of copies of $\mathbf{Q}_p/\mathbf{Z}_p$ contained in $H^1(S', \tilde{A})$ is exactly the Mordell-Weil rank of A over K'. We conclude this section with a simple proof of a proposition which (in the case of complex multiplication) plays a major role in the work of Coates and Wiles on the Birch-Swinnerton-Dyer conjectures [9]:

4.9. PROPOSITION: *Let x be an element of $A(K_\infty)$ of infinite order, and let V be the image* (mod $\mathscr{C}$) *of $x \otimes \mathbf{Q}_p/\mathbf{Z}_p$ in $H^1(S_\infty, \tilde{A})$, under the*

map described in 2.4.1. *Then* V *is not contained in the image of* $\mathrm{Hom}(\mathrm{Iw}(K_\infty/K_0), \tilde{A})$ *under the map described in Theorem* 4.7. *More precisely, let* x *be an element of* $A(K_{\infty,v})$, *where* v *lies over* p *and* $K_{\infty,v}$ *is the completion of* K_∞ *at* v; *assume* x *is of infinite order. Then* x *is not infinitely divisible by* p *in* $A(K_{\infty,v})$.

PROOF: The map described in 2.4.1 arises from dividing points x of infinite order in $A(K_\infty)$ by high powers of p and considering the Galois cocycle (which also represents a flat cohomology class) $f_\sigma = \sigma(x/p^t) - x/p^t$, for $\sigma \in \mathrm{Gal}(\bar{K}_\infty/K_\infty)$; the latter assertion of the proposition is that this cocycle does not split when restricted to $K_{\infty,v}$, hence defines a non-trivial extension of $K_{\infty,v}$ which is necessarily ramified (for t sufficiently large). Since the extension is ramified, it cannot come from a homomorphism of the Iwasawa module into $\tilde{A}$; thus the second assertion is a stronger form of the first. We prove the second; thus we may assume K, K_0, K_∞ are all *local*. We may as well assume x is defined over K_0 (otherwise replace K by a larger field). In this case, the local analogue of diagram 2.6 implies that the kernel of $H^1(S_0, \tilde{A}) \to H^1(S_\infty, \tilde{A})^G$ is bounded above by $H^1(G, \tilde{A}(K_\infty))$; the latter is a Galois cohomology group. If we know that $H^1(G, \tilde{A}(K_\infty))$ is finite, we will be done; but this is 2.6.4.

4.10. REMARK: Note that, in 4.1.1, we give an imbedding of $H^1(S_i, \tilde{A})$ in $H^1(S_i - T_i, \tilde{A})$; taking this to the limit, we obtain an imbedding of $H^1(S_\infty, \tilde{A})$ in $H^1(S_\infty - T_\infty, \tilde{A}) \simeq \mathrm{Hom}(X, \tilde{A})$, where X is the module in 3.2. This does not depend on the fact that A is ordinary, and since X is finitely generated over Λ, we see that $H^1(S_\infty, \tilde{A})$ is finitely generated over Λ in any case; we can even replace S_∞ by the integer spectrum in any p-analytic extension of K (because the property of finite generation both lifts and descends for maps $G \to G'$). However, it is not clear whether $H^1(S_\infty, \tilde{A})$ has any interesting properties (from the point of view of K) unless A is ordinary.

§5. Examples of torsion Λ-modules

A. Relations with Mazur's theory

5.1. Our first aim is to demonstrate that examples of torsion modules of the type studied by Mazur give rise to torsion modules of our type. Let A be, as usual, (the Néron model of) an abelian variety

over the number field K; let K_n, K_∞ be as in Section 2. Then K_n contains $C_n = K_0(\zeta_{p^{n+1}})$, where ζ_k is a kth root of unity. Let $C = \cup C_n$; then $\Gamma = \mathrm{Gal}(C/K_0) \simeq \mathbf{Z}_p$; we let $H = \mathrm{Gal}(K_\infty/C)$, $C = \mathrm{Gal}(K_\infty/K_0)$, so that $G/H = \Gamma$. The infinite descent module $H^1(S_\infty, \tilde{A})$ (notation as in Section 2) is a $\Lambda = \Lambda_G$-module, which we call X; then X^H is a Λ_Γ-module. Let Z_n be the spectrum of the ring of integers in C_n, $Z = \varprojlim Z_n$ the spectrum of the ring of integers in C. There is a natural map $Y = H^1(Z, \tilde{A}) \to X^H$.

5.1.1. PROPOSITION: *Under the usual assumption that A has good ordinary reduction at p, the kernel and cokernel of the map $Y \xrightarrow{f} X^H$ are finitely cogenerated. It follows that if Y is a cotorsion Λ_Γ-module, then X is a cotorsion Λ-module.*

PROOF: Let $\Gamma_n = \mathrm{Gal}(C/C_n)$. In diagram (2.6), replace S_n with Z_n, G_n with the inverse image under $G \to \Gamma$ of Γ_n, and modify the remaining notation correspondingly. Denote the resulting diagram (2.6′, n), and denote the map which takes the place of φ in (2.6) by f_n. Then (since $\varinjlim$ is exact) Ker (resp. Coker) f is just $\varinjlim_n (\mathrm{Ker}\, f_n)$ (resp. $\varinjlim_n (\mathrm{Coker}\, f_n)$). By 2.9, the number of cogenerators of Ker (resp. Coker)f_n as $\mathbf{Z}_p$-module is bounded independently of n, which implies the first assertion of the proposition. The second is then a consequence of 1.9.

5.2. Mazur's paper [28] contains a number of examples of elliptic curves over $\mathbf{Q}$ whose associated descent modules over the cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}$ are torsion Λ_Γ-modules; however, we need this information over the cyclotomic $\mathbf{Z}_p$-extension of K_0 (mainly because $\mathrm{Gal}(K_0/\mathbf{Q})$ acts as a non-trivial group of automorphisms of $\Lambda = \Lambda_G$; we will have more to say about this later). Our first set of examples will be in the case $p = 3$, and the elliptic curve $A/\mathbf{Q}$ is *divisible* over $\mathrm{Spec}(\mathbf{Z}) = S$ by the finite flat group scheme $\mathbf{Z}/3 \oplus \boldsymbol{\mu}_3$. Recall that this means that the subgroup scheme $A[3] \subset A$ (the Néron model) is globally isomorphic to $\mathbf{Z}/3 \oplus \boldsymbol{\mu}_3$, which translates into a condition on the Galois group action on $A[3]$ and a condition on the numbers of connected components of the degenerate fibers of A. In this case $K_0 = C_0 = \mathbf{Q}(\zeta_3)$, and $\mathrm{Gal}(\mathbf{Q}(\zeta_3)/\mathbf{Q}) = \Delta$ acts on everything; since Δ is of order 2, we may speak of the + and − parts of any Δ-module: they are the $+1$ and -1 eigenspaces for the action of Δ.

We repeat the Kummer sequence (2.1.1):

$$0 \longrightarrow A[3^r] \longrightarrow A \xrightarrow{\times 3^r} A \longrightarrow F_{3^r} \longrightarrow 0. \tag{2.1.1}$$

Regard this as a sequence for the étale topology of Z (notation as in 5.1). Then Δ acts on (2.1.1). Now Z is unramified over all primes in S for which A has bad reduction; it follows that $F_{3^r/Z} = F_{3^r/S} \times_S Z$. Consequently, by (2.1.2–2.1.3)

(5.2.1) $H^1(Z, A[3^r])$ is of finite index in $H^1(Z, \tilde{A})[3^r]$.

We denote by (5.2.1+) (resp. (5.2.1−)) the corresponding statement with a + (resp. a −) affixed to each group in (5.2.1).

5.2.2. LEMMA: *$H^1(Z, \tilde{A})^-$ is a cotorsion Λ-module.*

PROOF: It will suffice to show that $H^1(Z, \tilde{A})^-[3]$ is a finite group; by (5.2.1−) we will know this once we know $H^1(Z, A[3])^- = H^1(Z, \mathbf{Z}/3 \oplus \mu_3)^-$ is finite. By a theorem of Iwasawa [22] the class number of Z_n is prime to 3 for all n (3 is a regular prime); thus $H^1(Z, \mathbf{Z}/3) = 0$. Furthermore, if Z_n^+ is the integer spectrum of the maximal totally real subfield of C_n, then, as in I, 1.1, $H^1(Z_n, \mu_3)^+ = H^1(Z_n^+, \mu_3)$ (Z_n/Z_n^+ is tamely ramified, so the Hochschild-Serre spectral sequence is valid, and gives $0 \to H^1(\mathrm{Gal}(Z_n/Z_n^+), \mu_3) \to H^1(Z_n^+, \mu_3) \to H^1(Z_n, \mu_3)^+ \to H^2(\mathrm{Gal}(Z_n/Z_n^+), \mu_3)$, whose end terms are evidently trivial). Then the Kummer sequence $0 \longrightarrow \mu_3 \longrightarrow \mathbf{G}_m \xrightarrow{\times 3} \mathbf{G}_m \longrightarrow 0$ gives rise to the exact cohomology sequence

$$0 \longrightarrow E_k/3E_k \longrightarrow H^1(\mathrm{Spec}(O_k), \mu_3) \longrightarrow H^1(\mathrm{Spec}(O_k), \mathbf{G}_m)[3] \longrightarrow 0 \tag{5.2.2.1}$$

Here k is either C_n or its maximal totally real subfield. Now H^1 with coefficients in $\mathbf{G}_m$ is the ideal class group, which we have seen is trivial. We have written E_k for the group of units in k; if $k = C_n$, $E_k/3E_k$ is (by Dirichlet's theorem) a vector space over $\mathbf{F}_3$ of rank 3^n, whereas if k is the maximal real subfield of C_n, $E_k/3E_k$ is of rank $3^n - 1$ (the difference comes from the presence in C_n of a third root of unity). It follows that $H^1(Z_n, \mu_3)^+$ is of index 3 in $H^1(Z_n, \mu_3)$, or that $H^1(Z, \mathbf{Z}/3 \oplus \mu_3)^-$ is of order 3.

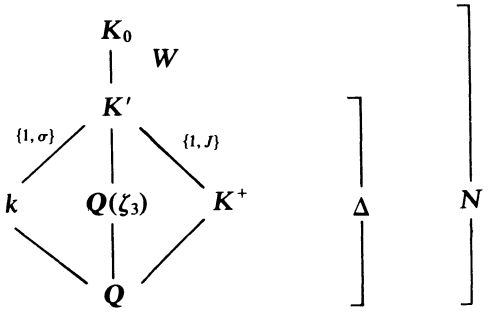
5.3. THEOREM: *Let A be an elliptic curve over $\mathbf{Q}$ which is divisible over* Spec($\mathbf{Z}$) *by $\mathbf{Z}/3 \oplus \mu_3$. Suppose that $A(\mathbf{Q})$ and $Ш(A, \mathbf{Q})[3^\infty]$ are finite groups. Then the module X (see 5.1 for notation) is a cotorsion Λ-module.*

PROOF: It suffices, by 5.1.1, to prove that Y is a cotorsion Λ_Γ-module. It is shown in [28], §6 that, under our hypotheses, Y^+ is a cotorsion Λ_Γ-module. By 5.2.2, Y^- is a cotorsion Λ_Γ-module. Hence Y is a cotorsion Λ_Γ-module.

5.4. REMARK: In [28] a number of examples of curves satisfying the hypotheses of the theorem are exhibited; there are, for example, curves with the conductor 14, 19, 26, 35, and 37. Mazur also describes, in [28], a means for generating still more examples.

5.5. REMARK: We have developed our descent theory only for curves with good reduction at the relevant prime. However, our Y^- is in fact $H^1(Z^+, \tilde{A}^*)$, where A^* is the unique curve over $\mathbf{Q}$, distinct from A, which becomes isomorphic to A over $\mathbf{Q}(\zeta_3)$. Here A^* has bad additive reduction at 3. It is easy enough to exhibit an A such that $A^*(\mathbf{Q})$ is of infinite order: the curve with conductor 19 is such an A ([1], p. 82). Mazur's examples of torsion Λ_Γ-modules all come from elliptic curves over $\mathbf{Q}$ with *finite* Mordell-Weil groups over $\mathbf{Q}$; but they all have good reduction.

5.6. We now consider a not very different case: suppose the representation of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ on A[3] is via the group N = the normalizer of a split Cartan subgroup of $GL(2, \mathbf{F}_3)$. Then N is a group of order 8, and contains the subgroup of homotheties $W = \pm 1$; $N/W = \Delta$ is isomorphic to the Klein 4-group. The field $K' = K_0^W$ is thus a biquadratic extension of $\mathbf{Q}$. Since $\det(W) = \{1\}$, K' contains $\mathbf{Q}(\zeta_3)$, by general principles. Since N is not contained in a Borel subgroup of $GL(2, \mathbf{F}_3)$, [39], implies that the prime 3 splits in the field fixed by the Cartan subgroup contained in N; this field is an imaginary quadratic extension of $\mathbf{Q}$, and hence we call it k. The non-trivial element in $\mathrm{Gal}(K'/k)$ is called σ, and complex conjugation in K' is called J. The fixed field of J is called K^+. The following picture may help:



The group N is associated to a pair of $\mathbf{F}_3$-lines in $A[3]$, say L_1, L_2. If 3 splits into $\mathcal{P}_1\mathcal{P}_2$ in k, then (possibly renumbering) we may assume that L_1 (resp. L_2) is the kernel of reduction of $A[3]$ at $\mathcal{P}_1$ (resp. $\mathcal{P}_2$). Let S' be the integer spectrum of K', let Z' be the cyclotomic $\mathbf{Z}_3$-extension of S', with Galois group Γ, and let $C' = C^W$, $C'_n = C_n^W$. The superscripts + and − will refer to the action of W.

Our aim is to prove that $H^1(Z, A[3])^-$ is a finite group; this will imply that $H^1(Z, \tilde{A})^-$ is a torsion Λ_Γ-module (with zero Iwasawa μ-invariant, in fact). Now as a finite flat group scheme, $A[3] = L_1 \oplus L_2$ (at least, over k), so it will suffice to prove (by symmetry) that $H^1(Z, L_1)^-$ is finite; we drop the subscript 1, then, and refer only to L and the prime $\mathcal{P}$ over which L is a connected group scheme.

Let Z_n be as in 5.1, and $Z'_n = Z_n^W$. Let T_n (resp. T'_n) be the set of points of Z_n (resp. Z'_n) dividing $\mathcal{P}$. Then, since L is finite and flat, $H^1_!(Z_{n,v}, L)$ and $H^1_!(Z'_{n,v}, L)$ are both trivial; here $Z_{n,v}, Z'_{n,v}$ are the completions (or localizations – by [28], 5.1 it makes no difference to $H^1_!$) at v of the respective schemes, and the assertion is proved in [29]. Thus $H^1(Z_n, L)^-$ imbeds in $H^1(Z_n - T_n, L)^-$. Now, over $Z_n - T_n$, L is *étale*; thus $H^1(Z_n - T_n, L) = \mathrm{Hom}(\Theta_n, L)$ where Θ_n is the Galois group of the maximal abelian extension of C_n of exponent 3 unramified away from T_n. Since W acts as -1 on L, we see that $H^1(Z_n - T_n, L)^- = \mathrm{Hom}(\Theta'_n, \mathbf{Z}/3)$, where Θ'_n is the Galois group of the maximal abelian extension of C'_n of exponent 3 unramified away from T'_n. So we have only to prove that $|\Theta'_n|$ is bounded independently of n.

The maximal abelian unramified extension of exponent 3, over C'_n, has Galois group B_n, a quotient of Θ'_n. But B, the Galois group of the maximal abelian unramified 3-extension of C', is a torsion Λ_Γ-module, by classical Iwasawa theory, and $|B_n|$ will be bounded, independently of n, if and only if Iwasawa's μ-invariant vanishes for B. Recall the definition of the μ-invariant: it is the number of copies of $\Lambda_\Gamma/p\Lambda_\Gamma$ which imbed (mod $\mathcal{C}$) in a compact torsion Λ_Γ-module. The μ-invariant in question here is the invariant μ_3 of the field K', which vanishes, by a theorem of Ferrero [13], because K' is abelian over $\mathbf{Q}$. (Here μ_3 is the μ-invariant of the Λ_Γ-module $\mathrm{Iw}(C'/K')$.)

Now let Ξ_n be the kernel of the natural map $\Theta'_n \to B_n$. If $g \in \Xi_n$, then g is in the inertia group of some point in T'_n for some abelian extension of C'_n of exponent 3 which is unramified away from T'_n. Now the element J of $\mathrm{Gal}(K'/K^+)$ takes abelian extensions of C'_n unramified away from T'_n to abelian extensions of C'_n unramified outside JT'_n, where JT'_n = {points of Z'_n dividing 3} − $\{T'_n\}$. Since $JT'_n \cap T'_n = \phi$, we see that if $0 \neq g \in \Xi_n$, then $g + Jg$, *qua* element of the Galois group U_n of the maximal abelian extension of C'_n, of

exponent 3, unramified outside 3, is non-trivial. There is thus an imbedding of Ξ_n in U_n, and in fact in U_n^J. Now U_n^J is the Galois group of the maximal abelian extension of $C_n'^J = C_n^+$, of exponent 3, unramified outside 3. Let $C^+ = \bigcup_n C_n^+$, $U^J = \lim_{\vec{n}} U_n^J$ the Galois group of the maximal abelian extension of C^+ of exponent 3 unramified outside 3. Then U^J is a Λ_Γ-module, with regard to the natural $\Gamma = \mathrm{Gal}(C^+/K^+)$ action. If we can prove that U^J is a torsion Λ_Γ-module with trivial μ-invariant, then it will follow that $|U_n^J|$, and hence $|\Xi_n|$ and $|\Theta_n|$, are bounded independently of n. Now since K^+ is real and abelian over $\mathbf{Q}$, [5] and class field theory imply U^J is torsion (Cf. [18]), and it follows from [18], Prop. 1, that the μ-invariant of U^J is trivial if the μ-invariant of $\mathrm{Iw}(C'/K')$ is trivial; then Ferrero's theorem applies again, and we conclude

5.7. THEOREM: *Let A be an elliptic curve over $\mathbf{Q}$, with good ordinary reduction at 3, such that the representation of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ on $A[3]$ is via the group N = the normalizer of a split Cartan subgroup of $GL(2, \mathbf{F}_3)$. Let W be the center of N, $K_0 = \mathbf{Q}(A[3])$, $K_\infty = \mathbf{Q}(\tilde{A})$, $G = \mathrm{Gal}(K_\infty/K_0)$, S_∞ the integer spectrum of K_∞, and $X = H^1(S_\infty, \tilde{A})$. If X^- is the -1 eigenspace for the action of W on X, then X^- is a cotorsion Λ_G-module. Moreover, if Y^- is the -1 eigenspace for the action of W on $Y = H^1(Z, \tilde{A})$, where Z is the cyclotomic $\mathbf{Z}_3 = \Gamma$-extension of K_0, then Y^- is a cotorsion Λ_Γ-module, whose Iwasawa μ invariant is trivial.*

5.8. REMARK: Although this example seems rather special, the method of proof applies in any case where the appropriate μ-invariant (of an Iwasawa-type situation) vanishes. For example, suppose the representation of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ acts on $A[p]$, where A is an elliptic curve over $\mathbf{Q}$, as the normalizer of a split Cartan subgroup of $GL(2, \mathbf{F}_p)$; as usual, let $K_0 = \mathbf{Q}(A[p])$, C the cyclotomic $\mathbf{Z}_p = \Gamma$-extension of K_0, Z the integer spectrum of C. Let $k \subset K_0$ be the imaginary quadratic field fixed by the Cartan subgroup of $GL(2, \mathbf{F}_p)$; p splits as $\mathfrak{P}_1\mathfrak{P}_2$ in k. Let M be the maximal abelian p-extension unramified outside $\mathfrak{P}_1$, and let $\Theta = \mathrm{Gal}(M/C)$. It is not difficult to show that Θ is a torsion Λ_Γ-module (we do so in Part C, below), and by the arguments in 5.7, we may derive the following proposition:

5.8.1. PROPOSITION: *The μ-invariant of Θ is zero if and only if $H^1(Z, \tilde{A})$ is a torsion Λ_Γ-module with zero μ-invariant.*

This proposition applies in particular to elliptic curves over **Q** with complex multiplication and ordinary reduction at p. In this connection it would be interesting to compute (for small p) the p-adic L-series, associated by Mazur and Swinnerton-Dyer to A in [33]. According to conjectures raised in that paper, this series is divisible by p if and only if the μ-invariant of $H^1(Z, \tilde{A})^{\mathrm{Gal}(K_0/\mathbf{Q})}$ is different from zero. Other curves to which the proposition applies are parametrized by the **Q**-rational points of the modular curve $X_{\mathrm{split}}(p)$, discussed in [30].

In Part C, below, we prove a related result for elliptic curves with complex multiplication.

B. Effective descent and more examples

The examples treated in Part A are somewhat unsatisfying, since they derive their torsion properties from the initial Γ-extension, and do not exhibit the properties of torsion modules over non-commutative rings. Here we obtain examples, arising from descent on elliptic curves, of torsion modules over $\Lambda_{PGL(2,\mathbf{Z}_p)}$ and in so doing strengthen the computations of Section 2 somewhat in the case of elliptic curves.

5.9. NOTATION: The notations K_0, K_n, K_∞, S_0, S_n, S_∞, A, G, and G_n will have their usual meaning. For simplicity we assume A is an elliptic curve; then G will be identified with its image in $GL(2, \mathbf{Z}_p)$. The subgroup of diagonal matrices in G will be called D, and K^{DG_n} will be called PK_n; PS_n, PK_∞, and PS_∞ will have the obvious significance. G/D will be called PG, and G_nD/D will be called PG_n. The module $H^1(S_\infty, \tilde{A})$ will be called X, and $H^1(PS_\infty, \tilde{A})$ will be called PX.

5.10. PROPOSITION: *The maps* $H^1(S_n, \tilde{A}) \to X^{G_n}$ *and* $H^1(S_n, \tilde{A}) \to PX^{PG_n}$ *have finite kernel and cokernel.*

5.10.1. COROLLARY: *If* $H^1(S_0, \tilde{A})$ *is finite, then* PX *is a cotorsion* Λ_{PG}*-module.*

PROOF OF COROLLARY: This follows from 1.7 immediately. As in [28] and in Section 2, $H^1(S_0, \tilde{A})$ will be finite precisely when the Mordell-Weil and (p-primary part of the) Tate-Shafarevich groups of A over K_0 are finite.

PROOF OF 5.10: The statement about X^{G_n} follows from 2.9, as does the assertion that $H^1(S_n, \tilde{A}) \to PX^{PG_n}$ has finite kernel. Since $H^1(S_n, \tilde{A}) \xrightarrow{f} PX^{PG_n} \xrightarrow{f'} X^{G_n}$ has finite cokernel, in order to prove that f has finite cokernel, it will be enough to prove that f' has finite kernel. But, as in 2.6, this kernel is bounded by $H^1(D, \tilde{A})$, which is finite because D has only finitely many fixed points in $\tilde{A}$, and because D is (topologically) cyclic.

5.10.1. REMARKS: If we are willing to accept the Tate-Shafarevich conjecture, we will have examples of torsion modules over Λ_{PG} (and the asymptotic bounds on Mordell-Weil rank which follow from the torsion property) as soon as we find elliptic curves over K_0 with *finite* Mordell-Weil groups over K_0. For example, there is a curve of conductor 14 over $\mathbf{Q}$ with two 3-isogenies and a rational point of order 3; consequently, the 3-division points of this curve A are defined over $\mathbf{Q}(\zeta_3)$. Now both A and its twist A^* over $\mathbf{Q}(\zeta_3)$ have finite Mordell-Weil groups over $\mathbf{Q}$. (The twist has conductor 126 and this information is provided by Table 1 in [1]); thus $A(\mathbf{Q}(\zeta_3))$ is finite.

5.11. It is impossible to find an elliptic curve over $\mathbf{Q}$, divisible by $\mathbf{Z}/3 \oplus \mu_3$, which has finite Mordell-Weil group and trivial Tate-Shafarevich group over $\mathbf{Q}(\zeta_3)$, so that it requires a second descent in each of these cases to verify the 3-primary part of the Tate-Shafarevich conjecture (and thus provide an example of a torsion module over Λ_{PG}). In order to avoid this, we choose the curve $X_0(20)$, which as two fortunate properties:

(5.11.1) It has potential good reduction at 2.

(5.11.2) It is divisible by $\mathbf{Z}/3$.

These can be read off the table in [1]; they imply

(5.11.1′) $X_0(20)$ has good reduction at the primes dividing 2 in $K_0 = \mathbf{Q}(A[3])$, if $A = X_0(20)$. ([44], §2)

(5.11.2′) The prime dividing 3 splits completely in $K_0/\mathbf{Q}(\zeta_3)$, which is totally ramified at 2.

In fact, by 5.11.2, the representation of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ on $A[3]$ is given in matrix form as $\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$. Now locally at 3, $A[3]$ has a canonical line defined within it, namely the kernel of reduction mod 3 (A is ordinary at 3 because it is divisible by $\mathbf{Z}/3$). This line and also the line generated by the point of order 3 rational over $\mathbf{Q}$ are fixed by $\mathrm{Gal}(\bar{\mathbf{Q}}_3/\mathbf{Q}_3)$, which thus acts on $A[3]$ (in the same coordinates as

above) via the matrices $\begin{pmatrix} 1 & 0 \\ 0 & * \end{pmatrix}$. Since A acquires good reduction over K_0, K_0 must be ramified over $\mathbf{Q}$, thus over $\mathbf{Q}(\zeta_3)$; but K_0 is a cyclic cubic extension of $\mathbf{Q}(\zeta_3)$.

5.11.3. We conclude as well that there are three primes v_1, v_2, and v_3 lying over 3 in K_0, and that, in the coordinates introduced above, the kernels of the reduction maps mod v_i are generated by the vectors $(i, 1)$ $i = 0, 1, 2$.

5.11.4. Finally, one reads from the tables that the prime 5, at which A has (multiplicative) bad reduction, is *defective* for 3, i.e., that the number of components of the Néron model of A at 5 is prime to 3; since this can certainly not be true over K_0, and since the Néron model lifts over unramified base extensions, we conclude that $K_0/\mathbf{Q}(\zeta_3)$ is totally ramified at 5 as well. Note that 2 and 5 stay prime in $\mathbf{Q}(\zeta_3)/\mathbf{Q}$. Of course $K_0/\mathbf{Q}(\zeta_3)$ is unramified away from 2 and 5. Combining these data, we see there are altogether at most four (and in fact only three) cyclic cubic extensions of $\mathbf{Q}(\zeta_3)$ unramified away from 2 and 5 (parametrized by lines in $(\mathbf{F}_3)^2 = U_2/3U_2 \times U_5/3U_5$, where U_p is the group of local units at p), that only two of them (at most) are ramified both at 2 and 5, and only $\mathbf{Q}(\zeta_3, \sqrt[3]{10})$ splits completely at 3. So we know that $K_0 = \mathbf{Q}(\zeta_3, \sqrt[3]{10})$. (We have here used that the class number of $\mathbf{Q}(\zeta_3)$ is one.)

5.11.5. The 3-class number of K_0 is one. In fact, the class number of $\mathbf{Q}(\sqrt[3]{10})$ is one (Cf. [7]), hence so is that of each of its conjugates; it follows that any 3-ideal class must be transformed to its inverse by any involution in $\mathrm{Gal}(K_0/\mathbf{Q})$, and must thus be fixed by $\mathrm{Gal}(K_0/\mathbf{Q}(\zeta_3))$. It must thus be representable by a product of primes ramifying in $K_0/\mathbf{Q}(\zeta_3)$, i.e. dividing 2 and 5; but primes dividing 2 and 5 are principal in $\mathbf{Q}(\sqrt[3]{10})$ and stay prime in $K_0/\mathbf{Q}(\sqrt[3]{10})$.

5.11.6. The units of K_0 generate a subspace of dimension three in $\prod_i U_{v_i}/U_{v_i}^{\perp} \cdot U_{v_i}^3$; here v_i are as in 5.11.3, U_{v_i} is the group of local units at v_i, and $U_{v_i}^{\perp}$ represents the annihilator of U_{v_i} under the norm residue symbol (i.e., the units in U_{v_i} whose cube roots generate unramified extensions of K_{v_i}). In fact, this is equivalent to saying (by Kummer theory) that the cube root of any unit in K_0 which is not itself a cube in K_0 generates a ramified extension of K_0, and that this is necessarily so follows from 5.11.5.

5.11.7. Over K_0, A has bad reduction only at the prime dividing 5 (which is unique, by 5.11.4); that is the only point at which the Néron fiber is disconnected, and there the three-part of the group of components is of order exactly three. (In any case, the group of components is cyclic, since the bad reduction is multiplicative.) The

descent arguments of [28] apply (specifically, 9.7 of that paper, which does not in fact rely on the hypothesis that the ground field is **Q**): if ρ is the Mordell-Weil rank of A over K_0, τ the $\mathbf{F}_3$-rank of the elements of its Tate-Shafarevich group of order 3, and $\delta = 2$ is the rank of the group of 3-division points of A defined over K_0, then

$$(5.11.7.1) \qquad \rho + \tau + \delta = \rho + \tau + 2 \leq \dim_{\mathbf{F}_3}(H^1(S_0, A[3])) + 1$$

5.11.8. LEMMA: *$H^1(S_0, A[3])$ is of order* 3.

PROOF: We know that $A[3]$ is finite and flat over S_0, and is thus étale over $S_0 - \{v_1, v_2, v_3\}$. Moreover, over each v_i, $A[3] \simeq \mathbf{Z}/3 \oplus \mu_3$; the kernels of the reduction maps are generated (in the coordinates of 5.11.2') by $e_i = (i, 1)$. Since $A[3]$ splits over S_0, the H^1 is a Galois cohomology group, and consists of maps to $A[3]$ of the idèles $K_{0,\mathbf{A}}^{\times}$, which vanish on $K_0^{\times}$ and on the local units at primes different from $\{v_1, v_2, v_3\}$; since the connected parts of $A[3]$ at primes dividing 3 are of multiplicative type, these maps must also vanish on the $U_{v_i}^{\perp}$ (Cf. 5.11.6); and finally, these maps must take U_{v_i} to the line generated by e_i for each i. In fact, since K_0 has class number prime to three, we are dealing with

$$\left\{ f \in \mathrm{Hom}\left(\left(\prod_i U_{v_i} \Big/ U_{v_i}^{\perp} \cdot U_{v_i}^3 \right) \Big/ (\text{Image of global units}), A[3] \right) \Big| f(U_{v_i}) \in \mathbf{F}_3 \cdot e_i \right\}.$$

An easy combinatorial argument, using 5.11.6, completes the proof.

From 5.11.7.1, 5.11.8, and 5.10.1, we conclude

5.12. COROLLARY: *The Λ_{PG} and Λ_G-modules of "infinite descent" over the towers of PK_n's and K_n's associated to the curve $A = X_0(20)$ and the prime* 3 *are cotorsion modules.*

C. Elliptic curves with complex multiplication

Our aim is to prove the following theorem, and to derive various consequences from it:

5.13. THEOREM: *Let A be an elliptic curve over the field K, with complex multiplication by the imaginary quadratic field k; suppose*

$K(A_{\text{tors}}) = \bigcup_n K(A[n])$ is an abelian extension of k. Then conjecture 4.6 *is true for A/K, for any prime p at which A has ordinary reduction. In other words, if S_∞ is the integer spectrum of $K_\infty = \bigcup_i K(A[p^i])$, then $H^1(S_\infty, \tilde{A})$ is a cotorsion Λ_G-module, where $G = \text{Gal}(K_\infty/K(A[p]))$.*

5.13.1. COROLLARY: *If Λ_G is regarded as the ring of power series over $\mathbf{Z}_p$ in two variables (Cf.* [17]*), then the support of X, the Pontryagin dual of $H^1(S_\infty, A)$, on $\text{Spec}(\Lambda_G)$, is (up to codimension two) equal to a divisor $D_{A/K,p}$ on $\text{Spec}(\Lambda_G)$.*

5.13.2. Since Λ_G has unique factorization, we may choose an element $f_{A/K,p} \in \Lambda_G$, whose divisor is $D_{A/K,p}$; this is called the *p-adic characteristic function* of A/K, and is well defined up to a unit in Λ_G.

5.13.3. LEMMA: *Let K'/K be a $\mathbf{Z}_p$-extension of K contained in K_∞. (In other words, K' is the lift to K of a $\mathbf{Z}_p$-extension of k.) Let S' be the integer spectrum of K', and let $H' = H^1(S', \tilde{A})$; let $G' = \text{Gal}(K_\infty/K')$. Suppose K' is not contained in the field obtained by adjoining the π^n-division points of A to K, for all n; here π is one of the primes of k lying over p in $\mathbf{Q}$ (there are two, because p is ordinary for A* ([26], p. 176)*, and π acts on $\tilde{A}$ via the complex multiplication. Then the map*

$$H' \longrightarrow H^1(S_\infty, \tilde{A})^{G'} \tag{5.13.3.1}$$

has finite kernel and cokernel.

PROOF: One knows from diagram 2.6 that the kernel of 5.13.3.1 is bounded above by $H^1(G', \tilde{A}(K_\infty))$. By the Hochschild-Serre spectral sequence, we may replace G' by its open subgroup $U \simeq \mathbf{Z}_p$, and prove that $H^1(U, \tilde{A}(K))$ is finite. By hypothesis, U has only finitely many fixed points in $\tilde{A}$ (otherwise K' would be contained in a field such as was forbidden in the statement of the lemma); thus the Herbrand quotient gives us the required result.

As for the cokernel, that is bounded (by [28], §6) by the inverse limit over i of $\bigoplus_{v|p}(A(K'_{i,v}) \bigcap_{L \subset K} N_{L_w/K_{i,v}}(A(L_w))$, *if A has good reduction at every prime of K*; here K'_i is finite/K for each i, and $K' = \bigcup K'_i$; N is the norm map, and w is an extension of v to the (finite) extension L/K'_i. The arguments of [28], §§4–6, imply that each of the summands in the above expression has, for each i, order bounded by a number which depends only on the number of p-

primary division points of A defined over $K'_{i,v}$; by hypothesis, this is bounded independently of i. Moreover, p splits finitely in K' (because it splits finitely in K_∞, by the theory of complex multiplication); this is sufficient to prove the lemma if A has everywhere good reduction.

If A does not have everywhere good reduction, then [44] there is an extension K''/K', finite, of order prime to p, such that A has good reduction everywhere over K''; moreover, K'' is contained in K_∞. We have proved that, if H'' is to K'' as H' is to K', then $H' \to H^1(S_\infty, \tilde{A})^{\mathrm{Gal}(K_\infty/K'')}$ has finite cokernel. We have thus only to show that $H' \xrightarrow{f} H''^{\mathrm{Gal}(K''/K')}$ has finite cokernel. In fact, since $\mathrm{Gal}(K''/K)$ is of order prime to p, App., Prop. 1.1, shows that f is even an isomorphism. This completes the proof.

5.13.4. The action of $\mathrm{Gal}(K_0/K) \overset{\text{def.}}{=} \Delta$ on $H^1(S_\infty, \tilde{A})$, where K_0 is, as usual, $K(A[p])$, is semi-simple, since $p \nmid |\Delta|$; thus, $H^1(S_\infty, \tilde{A}) = \bigotimes H^\chi$, where H^χ is the χ-isotypic component of $H^1(S_\infty, \tilde{A})$. Each H^χ has a well-defined p-adic characteristic function written $f_{A/K,p,\chi}$. On the other hand, for each $\mathbf{Z}_p$-extension K'/K contained in K_∞, Mazur has defined a p-adic characteristic function of one variable (which he chooses to be polynomial; Cf. [28]; namely, a generator (as always, mod $\mathscr{C}$) of the ideal in $\Lambda_{\mathrm{Gal}(K'/K)}$ which annihilates $H^1(S', \tilde{A})$; here S' is the integer spectrum of K'. Call this function $f_{A,K'/K,p}$; if we look at the extension $K'K_0/K$, we can also define functions $f_{A,K'K_0/K,p,\chi}$. Now each such K' is associated with a unique linear divisor in $\mathrm{Spec}(\Lambda_G)$: namely, there is a surjective map $G \to \mathrm{Gal}(K'/K)$, and thus a map $\Lambda_G \to \Lambda_{\mathrm{Gal}(K'/K)}$, giving rise to an imbedding $\mathrm{Spec}(\Lambda_{\mathrm{Gal}(K'/K)}) \to \mathrm{Spec}(\Lambda_G)$ as a linear divisor. We may restrict functions in Λ_G to that divisor, and obtain functions of one variable. The result is

5.12.5. COROLLARY: *For all but finitely many $\mathbf{Z}_p$-extensions K'/K contained in K_∞,*

$$f_{A,K'K_0/K,p,\chi} = f_{A/K,p,\chi} \mid D_{K'}, \text{ (with one exception to be described)}$$

(5.13.5.1)

up to a unit in $\Lambda_{\mathrm{Gal}(K'/K)}$, where $D_{K'}$ is the linear divisor associated with K' on $\mathrm{Spec}(\Lambda_G)$.

PROOF: If $I_{K'}$ is the ideal of the divisor $D_{K'}$, then 5.13.3 implies that, for all but two fields K', $(H^1(S', \tilde{A}))^* \simeq H^1(S_\infty, \tilde{A}))^* \otimes \Lambda_G/I_{K'}$ (mod

$\mathscr{C}$); this mod $\mathscr{C}$ refers to modules over $\Lambda_{\mathrm{Gal}(K'/K)}$, and * means Pontryagin dual. This is enough to prove 5.13.5.1 for all K' such that $D_{K'}$ does not contain any cycle in $\mathrm{Supp}(H^1(S_\infty, \tilde{A})^*) - D_{A/K,p}$; the problem is that $f_{A/K,p}$ does not notice codimension two cycles. This proves the corollary, with one exception: if infinitely many $D_{K'}$ contain such a cycle, then $\mathrm{Supp}(H^1(S_\infty, \tilde{A})^*)$ has an isolated codimension two component with support at the origin of $\mathrm{Spec}(\Lambda_G)$. By 5.10, this implies that $H^1(S_0, \tilde{A})$ contains an infinitely divisible element (S_0 is the integer spectrum of K_0): i.e., either $A(K_0)$ or $Ш(A, K_0)$ is of infinite order.

5.13.6. COROLLARY: *For all but finitely many $\mathbf{Z}_p$-extensions K'/K contained in K_∞, $A(K')$ is finitely generated.*

PROOF: We know that $A(K')$ is finitely generated if and only if $f_{A,K'/K,p}$ is not identically zero: indeed, in that case, $H^1(S', \tilde{A})$ will be a torsion $\Lambda_{\mathrm{Gal}(K'/K)}$-module, and the assertion follows from Iwasawa's classification of such modules [21], noting that $A(K') \otimes \mathbf{Q}_p/\mathbf{Z}_p$ is contained (up to a finite group) in $H^1(S', \tilde{A})$. Now, by 5.13.5 (and even by the weaker injectivity in 5.13.3), $f_{A,K'/K,p}$ will be identically zero only when $D_{K'} \subset D_{A/K,p}$, which can be true only for finitely many K'.

5.13.7. REMARK: Mazur [31] has constructed examples of K' as above for which $A(K')$ is not finitely generated; a generalization of his construction to the non-complex multiplication case forms the subject matter of [51].

5.13.8. REMARK: It is a conjecture of Mazur [28] that $A(K')$ is always finitely generated when K' is the cyclotomic $\mathbf{Z}_p$-extension of K. Moreover, he conjectures, that, in this cyclotomic case, the function $f_{A,K'/K,p}$ is (up to a unit in Λ) equal to the p-adic L-function of the elliptic curve, constructed by him and Swinnerton-Dyer in [33]; this p-adic L-function is a power series in one p-adic variable, which is defined for every elliptic curve which admits a parametrization by modular functions (i.e., a Weil curve). Now Manin-Vishik [27] and Katz [23] have defined p-adic L-functions of two variables, for any p-adic character of the idele classes of the CM field k; moreover, Katz has demonstrated that his function of two variables, when specialized to an appropriate line, restricts to the function of Mazur and Swinnerton-Dyer (with a slight modification).

It now remains to prove Theorem 5.13. We remark that such a result is implicit in the work of Coates and Wiles [9] and Vishik [49]; moreover, they have also made use of Brumer's theorem, and

obtained relations between the module considered here (restricted to one variable) and the p-adic L-functions of Katz.

PROOF OF 5.13: We let the ideal (p) split into π and π' in k; then the p-divisible group $\tilde{A}$ splits as a direct sum (over K) $\tilde{A} = \tilde{A}_1 \oplus \tilde{A}_2$ where $\tilde{A}_1$ is the π-divisible part and $\tilde{A}_2$ the π'-divisible part. By symmetry, it suffices to prove that $H^1(S_\infty, \tilde{A}_1)$ is cotorsion.

Now $\tilde{A}_1$ is étale over S_0-{primes dividing π}. So the theory developed in Section 4 allows us to represent $H^1(S_\infty, \tilde{A}_1)$ as a subgroup of $\mathrm{Hom}(X_1, \tilde{A}_1)$, where X_1 is the Galois group (over K_∞) of the maximal abelian p-extension of K_∞, unramified away from π. We will be done if we can show that X_1 is Λ-torsion.

Let K' be the splitting field of $\tilde{A}_1$, and let L' be the maximal abelian p-extension of K', unramified outside π. Then K' is a $\mathbf{Z}_p$-extension of K_0, ramified only at π; thus L'/K_0 is ramified only at π. Now, let $H = \mathrm{Gal}(K'/K_0)$; K'_i the ith intermediate field of the $\mathbf{Z}_p$-extension K'/K_0, and $H_i = \mathrm{Gal}(K'/K'_i)$. Let $X' = \mathrm{Gal}(L'/K')$. We want to show that X' is a torsion Λ_H-module, i.e., that $\dim \mathbf{Q}_p \otimes X'_{H_i}$ is bounded, independently of i; lower H_i means coinvariants. Now X'_{H_i} is a quotient of the Galois group of the maximal abelian extension of K'_i contained in L'; in other words, a quotient of the Galois group of the maximal abelian p-extension of K'_i unramified outside π. Class field theory identifies the latter with $K'^{\times}_{i\mathbf{A}}/(K'^{\times}_i \prod_{v|\pi} U_v)$, i.e. the quotient of the idèle classes by the local units away from π. Up to the finite ideal class group, this can be identified with $(\prod_{v|\pi} U_v)/\bar{E}$; here $\bar{E}$ is the closure (in the π-units) of the global units. Now Brumer has proved [5] that the rank of $\bar{E}$ is one less than the rank of $\prod_{v|\pi} U_v$. (He only claims to have proved that the rank of the closure of E in $\prod_{v|p} U_v$ is the same as the $\mathbf{Z}$-rank of E; but what he in fact proves, via the argument of Ax [4], is that there is an element $e \in E$ such that, given any imbedding $\varphi(e) \in \bar{\mathbf{Q}}_p$, the translates of $\varphi(e)$ by $\mathrm{Gal}(K'_i/k)$ generate a group which, under the logarithm map, is taken to a submodule of $\bar{\mathbf{Q}}_p$ of $\mathbf{Z}_p$-rank $|\mathrm{Gal}(K'_i/k)| - 1$. Since $\mathrm{Gal}(K'_i/k)$ does not interchange imbeddings over π and π', his argument gives the stronger result.) Since this is independent of i, we have shown that X' is torsion over Λ_H.

Now let $G' \subset G$ be $\mathrm{Gal}(K_\infty/K')$; we will be done, by 1.9, if we show that $X_{1G'}$ is torsion over Λ_H. But X_{1H} is a quotient of the maximal abelian extension of K' contained in K_∞. The only difference, then, between X_{1H} and the module X', which we already know to be torsion, comes from ramification at π'. Now, there are only finitely

many primes in K' lying over π', because K' contains an infinite residue field extension at every prime over π' (adjoining all the p-division points of the reduction of A mod π'). And each of them has an inertia group in X_{1H} of $\mathbf{Z}_p$-rank at most one: if $X_1 = \mathrm{Gal}(L/K_\infty)$, then, since L/K is unramified outside π, all the π' ramification happens in K_∞/K', which is of $\mathbf{Z}_p$-rank one. This completes the proof.

5.13.9. REMARK: If $K = \mathbf{Q}$, then $\mathrm{Gal}(k/\mathbf{Q})$ acts on $H^1(S_\infty, \tilde{A})$ by "interchanging the variables."

APPENDIX

§1. Some tame descents: $p \neq 2$

1.0. ORIENTATION: E will be an elliptic curve, almost always over $\mathbf{Q}$. By abuse of notation, we shall allow the letter E also to denote the Néron model [34] of E over $\mathbf{Z}$, and, by further abuse, over any finite covering of $\mathbf{Z}$, or over any completion thereof. Of course, the Néron model is not invariant under base change; we follow the convention of 2.1.4 with regard to maps between the cohomology groups of Néron models.

1.0.2. Let S be a Dedekind scheme, with generic point $j: X \to S$. We say the *fppf* sheaf F/S satisfies the *Néron property* if, as a sheaf on the smooth site over S,

$$F \xrightarrow{\sim} j_* j^* F. \tag{1.0.2.1}$$

The Néron model on an abelian variety over S is the prototypical example of such a sheaf. If A is such a Néron model, let $A[n]$ be subgroup scheme of A which is the kernel of multiplication by n; then $A[n]$ also satisfies 1.0.2.1 (because j_* and j^* are left exact). Suppose v is a closed point of S of residue characteristic prime to n. Then $A[n]$ is a quasi-finite smooth group scheme over S_v, where S_v is either the henselization or the completion of S at v. It follows that ([28], 5.1 (v) (b)), in either case,

$$H^1_!(S_v, A[n]) = 0; \tag{1.0.2.2}$$

here $H^1_!$ is local cohomology in the *fppf* topology with support at the closed point of S_v. In general, our cohomology will be in the *fppf* topology unless otherwise noted. We remark that, if G is a smooth

commutative group scheme over S, then ([15], 11.7)

$$H^i_{\text{étale}}(S, G) = H^i_{fppf}(S, G), \quad \text{for all } i; \tag{1.0.2.3}$$

we shall use this information freely in the sequel. Finally, if A has good reduction at v, then for any n, $A/S_v \xrightarrow{\times n} A/S_v$ is surjective; then the five-lemma and [28], 5.1 (iv) and (v)(b) yield

$$H^i(S_v, A[n]) \text{ is the same for } S_v \text{ the completion and } S_v \tag{1.0.2.4}$$

the henselization of S at v, when $r \geq 2$.

We mention this because, in the long global exact sequence of relative cohomology in the flat topology, the natural relative cohomology terms are those over the henselized base; we shall, however, make all our local computations over the p-adic numbers, and this is legitimate because of 1.0.2.4.

We have in mind the following proposition:

1.1. PROPOSITION: *Let A denote either an elliptic curve over the number field K or its Néron model over the integer spectrum $Z = \operatorname{Spec}(O_K)$. Let L/K be the field of p-division points of $A/K: L = K(A[p])$; let S be the integer spectrum of L. Suppose A has good reduction at all primes dividing p, and suppose $G = \operatorname{Gal}(L/K)$ has order prime to p. Then, for all n, the natural map*

$$H^1(Z, A[p^n]) \longrightarrow H^1(S, A[p^n])^G \tag{1.1.1}$$

is an isomorphism.

PROOF: Let T'(resp. T'^*) be the set of primes in Z(resp. S) of residue characteristic p and let T''(resp. T''^*) be the set of points in Z(resp. S), of residue characteristic different from p, which ramify in S(resp. over Z). We have the following diagram of exact local cohomology sequences (the zeroes on the left by 1.0.2.2 and [28], 5.1, (v)(a)):

$$\begin{array}{ccccccc} 0 \longrightarrow & H^1(Z, A[p^n]) & \longrightarrow & H^1(Z-T, A[p^n]) & \xrightarrow{\oplus d_v} & \bigoplus_{v \in T} H^2_v(Z_v, A[p^n]) \\ & & & \downarrow u & & \downarrow \oplus f_v \\ 0 \longrightarrow & H^1(S, A[p^n])^G & \longrightarrow & H^1(S-T^*, A[p^n])^G & \xrightarrow{\oplus d^G_w} & \left(\bigoplus_{w \in T^*} H^2_w(S_w, A[p^n])\right)^G \end{array} \tag{1.1.2}$$

Here T(resp. T^*) is $T' \cup T''$(resp., $T'^* \cup T''^*$), and the local cohomology groups may be taken over *completed* bases (by 1.0.2.4). Since $A[p^n]$ is *étale* away from T and T^*, the middle terms can be considered to be *étale* cohomology groups, and then the Hochschild-Serre spectral sequence ([45], VIII, 8.4) implies that Ker u(resp. Coker u) is bounded by $H^1(G, A[p^n])$(resp. $H^2(G, A[p^n])$ which both vanish because $|G|$ is prime to p. Thus u is an isomorphism.

We now claim that, if $v \in T'$, then

$$f_v : H^2_!(Z_v, A[p^n]) \to \left(\bigoplus_{w|v} H^2_!(S_w, A[p^n])\right)^G$$

is an isomorphism. Upon completing 1.1.2 at v we obtain

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^1(Z_v, A[p^n]) & \longrightarrow & H^1(K_v, A[p^n]) & \longrightarrow & H^2_!(Z_v, A[p^n]) & \longrightarrow & 0 \\ & & \downarrow r & & \downarrow r' & & \downarrow r'' & & \\ 0 & \longrightarrow & \bigoplus_{w|v} H^1(S_w, A[p^n])^G & \longrightarrow & \bigoplus_{w|v} H^1(L_w, A[p^n])^G & \longrightarrow & \bigoplus_{w|v} H^2_!(S_w, A[p^n]))^G & \longrightarrow & 0 \end{array} \tag{1.1.3}$$

The zeroes on the right appear because of local flat duality [29]: $A[p^n]$ is finite and flat at primes dividing p; and because $X \mapsto X^G$ is an *exact* functor on the category of abelian p-groups. Now, r' is an isomorphism, by the Hochschild-Serre spectral sequence again; and local flat duality implies that the extreme terms of each row are dual (because $A[p^n]$ is self-Cartier dual), and in particular have the same order. Hence $r'' = f_v$ is an isomorphism (by diagram chasing).

We will be done if we can account for the contribution of the $v \in T''$. Now, d_v(resp. d_w) factors through $H^1(K_v, A[p^n])$(resp. $H^1(L_w, A[p^n])$). We claim that, if $v \in T''$, then

$$H^1(K_v, A[p^n]) \longrightarrow \left(\bigoplus_{w|v} H^1(L_w, A[p^n])\right)^G = 0$$

(the former equality follows, once again, from Hochschild-Serre); if we can show this, we will be done, by diagram chasing. This is completely local, and we may use Shapiro's lemma to assume $G = \mathrm{Gal}(L_w/K_v)$. Over L_w, the sequence $0 \longrightarrow A[p] \longrightarrow A[p^n] \longrightarrow A[p^{n-1}] \longrightarrow 0$ is exact; by induction, therefore, we need only consider the case $n = 1$. Since $A[p]$ splits over L_w, $H^1(L_w, A[p]) \xrightarrow{\sim} \mathrm{Hom}(\mathrm{Gal}(\overline{L_w}/L_w), A[p]) \xrightarrow{\sim} \mathrm{Hom}(L_w^\times/(L_w^\times)^p, A[p])$; the latter isomorphism follows from local class field theory. We shall show that the inertia group G' of L_w/K_v fixes no element of $\mathrm{Hom}(L_w^\times/(L_w^\times)^p, A[p])$; thus we may assume L_w/K_v is totally ramified. Since L_w contains a primitive pth root of unity, this implies that K_v does as well. Thus G acts trivially on the (two-dimensional) $\mathbf{F}_p$-vector

space $L_w^\times/(L_w^\times)^p$. It now remains only to show that G has no fixed point in $A[p]$. But if it did, then, if $g \in G$, it must have an eigenvalue = 1, considered as an element of $\mathrm{Aut}(A[p])$. But $\det(g) = 1$, since g fixes the pth roots of unity. So both eigenvalues of g are = 1, and since G acts semisimply on $A[p]$, G must act trivially on $A[p]$. But then $K_v = K_v(A[p]) = L_w$, which contradicts the assumption that $v \in T''$.

1.2. We apply the Proposition to the case $K = \mathbf{Q}$, $n = 1$. Then, letting $Z = \mathrm{Spec}(\mathbf{Z})$, S as in 1.1, we see that, in order to compute $H^1(Z, A[p])$, it suffices to compute the $G = \mathrm{Gal}(L/\mathbf{Q})$ invariants in $H^1(S, A[p])$. Let V be $A[p]$, considered as a Galois module, and let V^* be the contragradient representation to V. Since V is self-Cartier dual, the Galois modules V and $V^* \otimes \mu_p$ are isomorphic; here μ_p is, as usual, the group of pth roots of unity. For the remainder of this section, *p will be an odd prime.*

Choose a basis of $A[p](L)$ over $\mathbf{F}_p$: this amounts to a map of the generic fiber of the constant scheme/S $\mathbf{Z}/p \otimes V$ into the generic fiber of A/S. By the Néron property (1.0.2.1), this extends to a global map of $\mathbf{Z}/p \otimes V$ into $A[p]$. The image of $\mathbf{Z}/p \otimes V$ is a finite flat subgroup scheme of A (over S), by [37], 2.1; in particular, $A[p]$ is étale and constant at all points of residue characteristic different from p (because all finite flat group schemes of order n are étale and constant away from the support of n).

1.3. The Cartier dual of the map $\mathbf{Z}/p \otimes V \to A[p]$ is a map $A[p] \to \mu_p \otimes V^*$; as above, this is an isomorphism away from residue characteristic p, and (by notation) an isomorphism as G-modules. For simplicity of notation, we set $U = S - T'^*$, and let $S_p = \coprod_{v|p} S_v$, $L_p = \bigoplus_{v|p} L_v$. Composing the two maps in the first sentence of this paragraph, we obtain a commutative diagram of long exact local cohomology sequences:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & H^1(S, \mathbf{Z}/p \otimes V) & \longrightarrow & H^1(U, \mathbf{Z}/p \otimes V) & \longrightarrow & H^2_?(S_p, \mathbf{Z}/p \otimes V) & \longrightarrow & \cdots \\
 & & \downarrow f & & \| & & \downarrow f' & & \\
0 & \longrightarrow & H^1(S, \mu_p \otimes V^*) & \longrightarrow & H^1(U, \mu_p \otimes V^*) & \longrightarrow & H^2_?(S_p, \mu_p \otimes V^*) & \longrightarrow & '''
\end{array}$$

(1.3.1)

$$\begin{array}{ccccccc}
\cdots & \longrightarrow & H^2(S, \mathbf{Z}/p \otimes V) & \longrightarrow & H^2(U, \mathbf{Z}/p \otimes V) & \longrightarrow & H^3_?(S_p, \mathbf{Z}/p \otimes V) \\
 & & \downarrow f'' & & \| & & \downarrow g \\
\cdots & \longrightarrow & H^2(S, \mu_p \otimes V^*) & \longrightarrow & H^2(U, \mu_p \otimes V^*) & \longrightarrow & H^3_?(S_p, \mu_p \otimes V^*)
\end{array}$$

By local flat duality, g is dual to $H^0(S_p, \mathbf{Z}/p \otimes V) \to H^0(S_p, \mu_p \otimes V^*)$, and is thus an isomorphism. By global arithmetic flat duality [3], f and f'' are dual to one another. Since G is an exact functor in our situation, this and diagram chasing imply

$$2\dim(\operatorname{coker} f^G) = \dim(\ker f'^G); \tag{1.3.2}$$

here dim means dimension as $\mathbf{F}_p$-vector spaces.

We again complete 1.3.1 at p:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^1(S_p, \mathbf{Z}/p \otimes V)^G & \longrightarrow & H^1(L_p, \mathbf{Z}/p \otimes V)^G & \longrightarrow & H^2(S_p, \mathbf{Z}/p \otimes V)^G & \longrightarrow & 0 \\ & & \downarrow j & & \| & & \downarrow f'^G & & \\ 0 & \longrightarrow & H^1(S_p, \mu_p \otimes V^*)^G & \longrightarrow & H^1(L_p, \mu_p \otimes V^*)^G & \longrightarrow & H^2(S_p, \mu_p \otimes V^*)^G & \longrightarrow & 0 \end{array} \tag{1.3.3}$$

The zeroes on the right arise, as in 1.1.3, from the local flat duality theorem, which also implies that the map j is dual to the map f'^G.

Now, over L_p, $\mathbf{Z}/p \otimes V \xrightarrow{\sim} A[p]$, and so $H^1(L_p, \mathbf{Z}/p \otimes V)^G \xrightarrow{\sim} H^1(L_p, A[p])^G$, which is in turn isomorphic (by Hochschild-Serre) to $H^1(\mathbf{Q}_p, A[p])$. This can be computed by means of the exact sequence over $\mathbf{Q}_p$

$$0 \longrightarrow A[p] \longrightarrow A \xrightarrow{\times p} A \longrightarrow 0,$$

whose cohomology exact sequence reduces, in dimension one, to

$$0 \longrightarrow A(\mathbf{Q}_p)/pA(\mathbf{Q}_p) \longrightarrow H^1(\mathbf{Q}_p, A[p]) \longrightarrow H^1(\mathbf{Q}_p, A)[p] \longrightarrow 0, \tag{1.3.4}$$

where, for any abelian group M, $M[p]$ is the subgroup of M of elements killed by p. Tate's local duality theorem [46] implies that the left-hand term of 1.3.4 is dual to the right-hand term. There are two cases:

(1) If p is *anomalous* (Cf. [28]), then $A(\mathbf{Q}_p)$ has a subgroup of order p, which is unique because $p \neq 2$ (by Cartier duality). This is mapped isomorphically onto the p-part of $A[\mathbf{F}_p]$; the kernel of $A(\mathbf{Q}_p) \to A(\mathbf{F}_p)$ is a compact one-dimensional Lie group over $\mathbf{Z}_p$. Thus, when p is anomalous, the ends of 1.3.4 have dimension 2, and so the middle has dimension 4, as does the middle of each row of 1.3.3.

(2) If p is *not anomalous*, the same computation shows that only the kernel of $A(\mathbf{Q}_p) \to A(\mathbf{F}_p)$ contributes to the p-part of $A(\mathbf{Q}_p)$, and so in this case the middle terms in 1.3.4 and 1.3.3 each have dimension 2.

We want to compute the end terms of 1.3.3; it suffices by local flat duality to compute the left-hand terms, and even to compute $H^1(S_p, \mathbf{Z}/p \otimes V)^G$. By Shapiro's lemma, we may assume S_p is connected. Since $H^1(S_p, \mathbf{Z}/p)$ is, by local class field theory, isomorphic to (setting $O = O_{L_p}$) $\mathrm{Hom}(L_p^\times/O^\times, \mathbf{Z}/p)$, we see that

$H^1(S_p, \mathbf{Z}/p \otimes V)^G \xrightarrow{\sim} \mathrm{Hom}_G(L_p^\times/O^\times, V)$; G acts trivially on the valuation group $L_p^\times/O^\times$, so $\mathrm{Hom}_G(L_p^\times/O^\times, V)$ has dimension equal to dim V^G, i.e., to one if p is anomalous for A, to zero if not. We may rewrite 1.3.3, using dimensions only:

(1.3.5)

p anomalous					p not anomalous				
0	1	4	3	0	0	0	2	2	0
0	3	4	1	0	0	2	2	0	0

In either case, $\dim(\ker f'^G) = 2$; by 1.3.2, this implies

$$\dim H^1(S, \boldsymbol{\mu}_p \otimes V^*)^G = \dim H^1(S, \mathbf{Z}/p \otimes V)^G + 1.$$

But by definition, f^G factors as $H^1(S, \mathbf{Z}/p \otimes V)^G \xrightarrow{f'} H^1(S, A[p])^G \xrightarrow{f''} H^1(S, \boldsymbol{\mu}_p \otimes V^*)^G$; since all these groups are subgroups of $H^1(U, A[p])^G$, both f' and f'' are injections. Now, by global class field theory, $H^1(S, \mathbf{Z}/p \otimes V) \xrightarrow{\sim} \mathrm{Hom}_G(\mathrm{Cl}(L), V)$, where $\mathrm{Cl}(L)$ is the ideal class group of L. We denote by h_V the dimension of $\mathrm{Hom}_G(\mathrm{Cl}(L), V)$, which must be described differently according as V is or is not an absolutely irreducible G-module. Taking into account 1.1, we have proved

1.4. THEOREM: *Let A be an elliptic curve over $\mathbf{Q}$ with good reduction at p; let $G = \mathrm{Gal}(\mathbf{Q}(A[p])/\mathbf{Q})$ have order prime to p. Let $Z = \mathrm{Spec}(\mathbf{Z})$, and denote by A the Néron model of A over $\mathbf{Z}$. In the notation of* 1.3, *$\dim H^1(Z, A[p]) = h_V$ or $h_V + 1$.*

1.5. One knows that the group G is a subgroup of $GL(2, \mathbf{F}_p)$ of order prime to p, $p \neq 2$. Thus ([39], 2.6), either G' is contained in the normalizer of a Cartan subgroup; or else the image of G in $PGL(2, \mathbf{F}_p)$ is A_4, A_5, or S_4. If one wants to compute $H^1(Z, A[p])$ exactly, one has to do this case by case. We shall carry this out only for curves which are *supersingular* at p; the other cases are essentially simpler, but may require more computation.

1.6. We now assume, in addition to the hypotheses of Theorem 1.4, that A is *supersingular* at p; i.e., that it has no points of order p which do not reduce to zero (mod p); i.e., that the formal group of its reduction (mod p) have height two. This implies that $\mathrm{Gal}(\mathbf{Q}_p(A[p])/\mathbf{Q}_p)$ acts on $A[p]$ as the normalizer of a non-split Cartan subgroup of $GL(2, \mathbf{F}_p)$ ([39], Proposition 12: it cannot be contained in the non-split Cartan subgroup itself, because there is no tamely ramified extension of $\mathbf{Q}_p$ of degree p^2-1). We let C be the non-split Cartan subgroup; then C is the inertia group of $\mathrm{Gal}(\mathbf{Q}_p(A[p])/\mathbf{Q}_p)$; we see that $\mathbf{Q}_p(A[p])$ is the maximal abelian tamely and totally ramified extension of k_p, where k_p is the unique unramified quadratic extension of $\mathbf{Q}_p$. Thus there is only one prime $\pi \in L = \mathbf{Q}(A[p])$ which lies over p.

Serre has computed the action of the unit group of k_p on $A[p]$, given by the local reciprocity map $U_{k_p} \to \mathrm{Gal}(L_\pi/k_p)$; here U_{k_p} is the group of elements of k_p of absolute value one. His results are as follows: By local class field theory, the local reciprocity map factors as follows:

$$U_{k_p} \longrightarrow U_{k_p}/(1+pO) \xrightarrow{\sim} \mathbf{F}_q^\times \xrightarrow{\varphi}_{\sim} \mathrm{Gal}(L_\pi/k_p);$$

we have set $O =$ the integer ring in k_p, and $q = p^2$. Let θ be the *fundamental character* of $\mathbf{F}_q^\times$, with values in μ_{q-1}: $\theta(x)$ is the Teichmuller representative of x in k_p. Then, if $t \in L_\pi$, $t^{q-1} = p$, the theory of the local symbol implies that, when $x \in \mathbf{F}_q^\times$,

$$t^{\varphi(x)} = \theta(x^{-1})t, \tag{1.6.1}$$

and, if $V = tO_\pi/t^2O_\pi$, where O_π is the integer ring in L_π, then

(1.6.2) As $G \xrightarrow{\sim} \mathbf{F}_q^\times$ modules, V and $A[p]$ are equivalent;

i.e., $\mathbf{F}_q^\times$ acts on $A[p]$ via the inverse of the fundamental character. (For all this, Cf. [39], Propositions 3 and 12.) For future reference, we remark that V is evidently isomorphic, as G-module, to $(1+tO_\pi)/(1+t^2O_\pi)$; the two terms in this quotient are regarded as subgroups of $L_\pi^\times$.

Note that the V defined here is isomorphic to the V defined in 1.2.

1.7. With notation as in 1.3, we have the commutative diagram

$$
\begin{array}{ccc}
0 \longrightarrow H^1(S, A[p])^G & \longrightarrow & H^1(U, A[p])^G \\
\downarrow & & \downarrow \\
0 \longrightarrow H^1(S_\pi, A[p])^G & \longrightarrow & H^1(L_\pi, A[p])^G
\end{array} \tag{1.7.1}
$$

Thus, $H^1(S, A[p])^G$ is just the subgroup of $H^1(S, \mu_p \otimes V^*)^G$ which, under the natural map to $H^1(L_\pi, A[p])$, is taken to the image of $H^1(S_\pi, A[p])^G$. For the moment, then, we shall be concerned with the computation of $H^1(S_\pi, A[p])^G$.

1.7.2. We let t be as in 1.6. We let E be the group of units of L_π, and set $E_i = \{x \in E \mid x \equiv 1 \pmod{t^i}\}$. This filtration induces a natural filtration of E/E^p, with associated graded $Gr = \oplus Gr_i$, where $Gr_i = E_i/E_{i+1}E^p$. One computes easily (Cf. [38], Proposition 6) that $Gr_i = 0$ for $i > p(p+1)$, and for $i = mp$, $m = 0, \ldots, p$; for all other i, Gr_i is of dimension two, except for $i = (p+1)p$, in which case Gr_i is of dimension one. Moreover, if θ is as in 1.6, then the action of $\mathbf{F}_q^\times$ on Gr_i, when the former is identified (via φ, as in 1.6) with $\mathrm{Gal}(L_\pi/k_p)$, is given by $\theta^{-i} = (x \mapsto \theta(x^{-i}))$, for i prime to p. Now, since $A[p]$ is split over L_π, $H^1(L_\pi, A[p])$ is just $\mathrm{Hom}(\mathrm{Gal}(\bar{L}_\pi/L_\pi), A[p]) = \mathrm{Hom}(L_\pi^\times, A[p])$, by local class field theory. And $\mathrm{Hom}(L_\pi^\times, A[p])^G$ can be written as $\mathrm{Hom}(L_\pi^\times/(L_\pi^\times)^p, V)^G$. Now, G acts trivially on the value group, so the latter is just $\mathrm{Hom}(E/E^p, V)^G$; only those i for which the action of G on Gr_i is the same as that on V contribute to this latter group. But we know that $\mathrm{Gal}(L_\pi/k_p)$ acts as θ^{-1} on V, and as θ^{-i} on Gr_i; and θ^{-1} and θ^{-i} are the same representation over $\mathbf{F}_p$ if and only if either $i \equiv 1 \pmod{q-1}$: i.e., they are the same representation even over $\mathbf{F}_q$; or if they are conjugate over $\mathbf{F}_p$; i.e., if and only if $1 \equiv pi \pmod{q-1}$. For $i < (p+1)p$, this is possible only for $i = 1, p, p^2$, and p^2+p-1; since Gr_i is trivial for the middle two, we see that only Gr_1 and Gr_{p^2+p-1} contribute to $\mathrm{Hom}(E/E^p, V)^{\mathrm{Gal}(L_\pi/k_p)}$. Each of these contributes a two dimensional subspace to the latter space; but $\mathrm{Hom}(Gr_i, V)^G$ is of dimension one only for $i = 1, p^2+p-1$. We summarize this computation as follows:

1.7.3. The group $H^1(L_\pi, A[p])^G$ is of dimension two, generated by the images of $\mathrm{Hom}(Gr_i, A[p])^G$, where $i = 1, p^2+p-1$.

1.7.4. We claim now that, under the above identification, $H^1(S_\pi, A[p])^G = \mathrm{Hom}(E_1/E_2, A[p])^G$, of dimension one. We prove this by reference to a result of Roberts [38].

Thus, let C be a cyclic subgroup scheme of $A[p]$, of order p. Since A is supersingular at p, C is neither étale nor of multiplicative type; it is therefore of type $G_{a,b}$, in the language of Oort and Tate [36], with neither a nor b a unit in L_π. Since, over L_π, C has a generator, it must

be of the form $G_{a,b}$ with a and b equal to $(p-1)$st powers in L_π. Note that, in the Tate–Oort notation, a and b are two elements of L_π with product p; they can be chosen to be $a = t^{(p-1)i}$, $b = t^{(p-1)j}$, with $i+j = p+1$, and with $i, j \geq 1$. (Actually, it is easy to see, using the discriminant, that we must have $i = 1, j = p$, but we will not need that.)

If C' is any quotient of $A[p]$ of order p (e.g., its quotient by the flat subgroup scheme C), then C' must be of the form $G_{b,a}$. In fact, $A[p]$ is homogeneous under $\mathbf{F}_q^\times$; thus all cyclic subgroups, and thus all cyclic quotient groups, are isomorphic. Roberts' Theorem 1 [38] states that, under any map $G_{b,a} \to \boldsymbol{\mu}_p$, the induced map $H^1(S_\pi, G_{b,a}) \to H^1(S_\pi, \boldsymbol{\mu}_p)$ has image equal to the image of E_{pi} in E/E^p, where $a = t^{(p-1)i}$, and where $H^1(S_\pi, \boldsymbol{\mu}_p)$ is identified with E/E^p via Kummer theory: taking cohomology of the exact sequence $0 \longrightarrow \boldsymbol{\mu}_p \longrightarrow \mathbf{G}_m \xrightarrow{\times p} \mathbf{G}_m \longrightarrow 0$, we obtain $E/E^p \xrightarrow{\sim} H^1(S_\pi, \boldsymbol{\mu}_p)$, because $H^1(S_\pi, \mathbf{G}_m)$ vanishes (S_π is the spectrum of a ring with unique factorization). But $H^1(S_\pi, \boldsymbol{\mu}_p)$ is also identified with a subgroup of $\mathrm{Hom}(L_\pi^\times, \boldsymbol{\mu}_p)$, by local class field theory (the local norm residue symbol). Formula (6) of Chapter 12, §1 of [2] indicates immediately that under the norm residue pairing $E/E^p \otimes E/E^p \to \boldsymbol{\mu}_p$, the orthogonal complement of the image of E_i is E_j, where $i+j = p+1$. Thus, $H^1(S_\pi, \boldsymbol{\mu}_p) \xrightarrow{\sim} \mathrm{Hom}(L_\pi^\times/E_{p(p+1)}, \boldsymbol{\mu}_p)$; and so the image of $H^1(S_\pi, G_{b,a})$ in $\mathrm{Hom}(L_\pi^\times, \mathbf{Z}/p)$ is equal, thanks to Roberts, to $\mathrm{Hom}(L_\pi^\times/E_{pj}, \mathbf{Z}/p)$, where $a = t^{(p-1)j}$. (Warning: [38] contains a major misprint; for the correct statement, Cf. [32]).

It follows, therefore, that if $f \in \mathrm{Hom}(L_\pi^\times, A[p])$ comes from an element of $H^1(S_\pi, A[p])$, then it must, under any map $A[p] \to C'$, with C' cyclic of order p, vanish on E_{pj}, where j is some integer at most equal to p. This says that Gr_{p^2+p-1} cannot contribute to $H^1(S_\pi, A[p])$, and *a fortiori* cannot contribute to $H^1(S_\pi, A[p])^G$. But, by diagram 1.1.3, $\dim H^1(S_\pi, A[p])^G = 1/2 \dim H^1(L_\pi, A[p])^G$ (we are using local flat duality again), which equals one, by 1.7.3. Thus the image of $H^1(S_\pi, A[p])^G$ in $H^1(L_\pi, A[p])^G$ is just the (one-dimensional) image of $\mathrm{Hom}(Gr_1, A[p])^G$.

1.8. Combining all this, wee see that, regarded idèlically, $H^1(S, A[p])^G$ is $\mathrm{Hom}(L_\mathbf{A}^\times/L^\times E_2 \times \prod_{v \neq \pi} U_v, A[p])^G$; here $L_\mathbf{A}^\times$ is the idèle group of L, E_2 is as above, and U_v is the unit group at the place v. Let B be the group on the left in the above Hom; then there is an exact sequence (with E as in 1.7)

$$0 \longrightarrow E/E_2E_L \longrightarrow B \longrightarrow Cl(L) \longrightarrow 0; \tag{1.8.1}$$

here E_L is the group of units of L, considered as a subgroup of E, and $Cl(L)$ is the ideal class group of L. The subgroup of $\mathrm{Hom}(B, A[p])^G$ vanishing on E has dimension h_V, in the notation of 1.4. This will be all of $\mathrm{Hom}(B, A[p])^G$, unless the following conditions are satisfied:

(1.8.1.1): The sequence 1.8.1., when tensored with $\mathbf{F}_p$, becomes a split sequence of $\mathbf{F}_p$-vector spaces; i.e., the map $\mathrm{Hom}(E/E_2E_L, \mathbf{F}_p) \to \mathrm{Ext}^1_{\mathbf{Z}}(Cl(L), \mathbf{F}_p)$, coming from 1.8.1, is trivial.

(1.8.1.2): $E_2E_L \neq E$; i.e., there is no global unit in L congruent to 1 (mod π) which is not congruent to 1 (mod π^2).

1.9. Corollary: *Suppose, in the situation of* 1.4, *that A is supersingular at p. Then* $\dim H^1(Z, A[p])$ *is h_V or $h_V + 1$, and is equal to the latter if and only if conditions* (1.8.1.1) *and* (1.8.1.2) *are satisfied.*

1.10. Remark: Elliptic curves satisfying the hypotheses of the corollary are easy to find: one need only consider elliptic curves with complex multiplication over the imaginary quadratic field (with class number one) k, and choose primes p which remain prime in k. One expects, however (Cf. [30]), that there will not be many others.

§2. More tame descents: $p = 2$

2.0. We now assume $p = 2$; otherwise the assumptions are the same: namely, A is an elliptic curve over $\mathbf{Q}$, with good reduction at 2; and $G = \mathrm{Gal}(L/\mathbf{Q})$ is of order prime to 2, where $L = \mathbf{Q}(A[2])$. We assume, moreover, that $L \neq \mathbf{Q}$; the case $L = \mathbf{Q}$ has been treated in [28]. Then G is a non-trivial subgroup of $GL(2, \mathbf{F}_2)$, of order prime to two; i.e., G is cyclic of order 3. Thus L is abelian cubic over $\mathbf{Q}$, so neither the real prime nor the prime 2 ramifies in L. If A were not ordinary at 2, then $A[2]$ would contain a subgroup scheme isomorphic to the infinitesimal additive group scheme α_2, which is impossible, because α_2 does not lift over unramified extensions of $\mathbf{Q}_2$ (Cf. [35]). Thus, as in [39], the image of $\mathrm{Gal}(\bar{\mathbf{Q}}_2/\mathbf{Q}_2)$ in $GL(A[2])$ is contained in a Borel subgroup of the latter, hence is trivial, since G is of order prime to 2. We record these facts:

2.1. Lemma: *A has ordinary reduction at* 2, *and* 2 *and the real prime of* $\mathbf{Q}$ *split completely in L.*

We denote the primes of L over 2 by the symbols π_i, $i = 1, 2, 3$, and the archimedean primes of L by r_1, r_2, r_3.

2.2. Unfortunately, for $p = 2$, the global arithmetic duality theorem does not give an exact pairing between H^1 and H^2. However, we still have diagram 1.3.1 in our case, and we still know that g is an isomorphism, hence that

$$\text{In diagram 1.3.1, } \dim(\operatorname{coker} f) + \dim(\ker f'') = \dim(\ker f'). \tag{2.2.1}$$

In our case, G has only two representations: V, and the trivial representation I; in particular, $V \simeq V^*$, so we shall suppress the distinction between them.

Let Y be the group of (global) units of L. If $L_{r_i}^+$ is the connected component of the identity in $L_{r_i}^\times$, let $W_i = L_{r_i}^\times / L_{r_i}^\times$, $i = 1, 2, 3$, and let $W = \bigoplus_{i=1}^{3} W_i$. We distinguish two cases:

$$\begin{aligned} &\text{Case (a): The natural map } Y \to W \text{ is not surjective.} \\ &\text{Case (b): The natural map } Y \to W \text{ is surjective.} \end{aligned} \tag{2.2.2}$$

In either case, the subgroup (± 1) of Y has non-trivial image in W, so the image of Y is at least of dimension one. Since W is isomorphic to the regular representation of G over $\mathbf{F}_2$, we see that in case (a), $\dim(\operatorname{Im}(Y)) = 1$, in case (b), $\dim(\operatorname{Im}(Y)) = 3$. In terms of the idèles, let D be the subgroup of $L_{\mathbf{A}}^\times$, the idèles of L, positive at each r_i and of absolute value one at each finite prime. Then, by class field theory, $H^1(S, \mathbf{Z}/2) \xrightarrow{\sim} \operatorname{Hom}(L_{\mathbf{A}}^\times / L^\times D, \mathbf{Z}/2)$. But there is a natural map $L_{\mathbf{A}}^\times / L^\times D \to Cl(L)$, the ideal class group of L, and then the cokernel of the induced map $\operatorname{Hom}(Cl(L), \mathbf{Z}/2) \to \operatorname{Hom}(L_{\mathbf{A}}^\times / L^\times D, \mathbf{Z}/2) \xrightarrow{\sim} H^1(S, \mathbf{Z}/2)$ is naturally dual to the cokernel of the map $Y \to W$ described above. Thus, if $H = \operatorname{Hom}(Cl(L), \mathbf{Z}/2)$, then, as G-spaces,

$$\begin{aligned} H^1(S, \mathbf{Z}/2) &\simeq H \oplus V \quad \text{in case (a) of 2.2.2} \\ &\simeq H \qquad \text{in case (b) of 2.2.2.} \end{aligned} \tag{2.2.3}$$

2.2.4. Lemma: $H^G = 0$; i.e., as G-space $H \simeq V^{h/2}$, $h = \dim Cl(L)$[2].

Proof: We have only to prove that there is no unramified quadratic extension K/L fixed by G. But if there were, then, since 2 and 3 are relatively prime, K, being a Galois extension of $\mathbf{Q}$, would descend to an unramified quadratic extension of $\mathbf{Q}$, which is impossible. The

second assertion follows from the "classification of representations of G."

2.2.5. COROLLARY: $\dim H$ *is even.*

2.3. Meanwhile, the Kummer sequence $0 \longrightarrow \mu_2 \longrightarrow \mathbf{G}_m \xrightarrow{\times 2} \mathbf{G}_m \longrightarrow 0$ gives rise to the exact sequence of cohomology over S

$$0 \longrightarrow Y/Y^2 \longrightarrow H^1(S, \mu_2) \longrightarrow Cl(L)[2] \longrightarrow 0. \tag{2.3.1}$$

As G-space $Y/Y^2 \simeq V \oplus I$: In fact, the representation of G on $Y/(\pm 1)$ is a non-trivial homomorphism $G \to GL(2, \mathbf{Z})$; since G is of order 3, this must be non-trivial (mod 2). Thus

2.3.1. As G-space, $H^1(S, \mu_2) \xrightarrow{\sim} H \oplus V \oplus I$.

2.4. Now, if C is either $\mathbf{Z}/2$ or μ_2, then $H^1(S, C \otimes V) \xrightarrow{\sim} H^1(S, C) \otimes V$, as G-space. But $\dim(V \otimes V)^G$ is evidently two, and $\dim(I \otimes V)^G = 0$. Thus, in case (a) of 2.2.2, the map f^G: $H^1(S, \mathbf{Z}/2 \otimes V)^G \to H^1(S, \mu_2 \otimes V)^G$ (coming from 1.3.1) is an isomorphism; hence so is each of the maps $H^1(S, \mathbf{Z}/2 \otimes V)^G \to H^1(S, A[2])^G \to H^1(S, \mu_2 \otimes V)^G$. It follows from 2.2.3 that, if $h = \dim Cl(L)[2]$, then

2.4.1. In case (a) of 2.2.2, $\dim H^1(S, A[2])^G = h + 2$.

2.4.2. It follows from our construction that the composite map

$$\begin{aligned} H^1(S, A[2])^G &\longrightarrow \mathrm{Hom}(W, V)^G \xrightarrow{\sim} \bigoplus_i H^1(K_{r_i}, A[2])^G \\ &\xrightarrow{\sim} H^1(\mathbf{R}, A[2]) \end{aligned} \tag{2.4.2.2}$$

is *surjective* in case (a) (here $\mathbf{R}$ is regarded as the unique archimedean completion of $\mathbf{Q}$, and the last isomorphism is Hochschild-Serre).

2.5. Assume now we are in case (b) of 2.2.2. Returning to 1.3.1, we see (by 2.2 and 2.3) that $\mathrm{coker}(f) \simeq \mathrm{Hom}(V \oplus I, V)$, which is of dimension 6. Now f' is dual, by local flat duality [29], to the map

$$f'^* : \bigoplus_i H^1(S_{\pi_i}, \mathbf{Z}/2 \otimes V) \longrightarrow \bigoplus_i H^1(S_{\pi_i}, \mu_2 \otimes V). \tag{2.5.1}$$

But $S_{\pi_i} = \mathrm{Spec}(\mathbf{Z}_2)$, and the Kummer sequence gives $H^1(S_{\pi_i}, \boldsymbol{\mu}_2) \simeq \mathbf{Z}_2^\times/(\mathbf{Z}_2^\times)^2$, for all i; since $\dim H^1(S_{\pi_i}, \mathbf{Z}/2) = 1$ (there is only one unramified quadratic extension of $\mathbf{Q}_2$), it follows (by counting) that $\dim(\mathrm{coker}\, f'^*) = \dim(\ker f') = 6$. These two computations, combined with 2.2.1, imply that the map f'' in 1.3.1 is an *isomorphism*. We may thus replace 1.3.1 by the following bigger diagram:

$$\begin{array}{ccccccccc}
0 \to H^1(S, \mathbf{Z}/2 \otimes V)^G & \to & H^1(U, \mathbf{Z}/2 \otimes V)^G & \to & H^2_?(S_2, \mathbf{Z}/2 \otimes V)^G & \to & M & \to & 0 \\
\downarrow & & \| & & \downarrow & & \| & & \\
0 \to H^1(S, A[2])^G & \longrightarrow & H^1(U, A[2])^G & \longrightarrow & H^2_?(S_2, A[2])^G & \longrightarrow & M & \to & 0 \\
\downarrow & & \| & & \downarrow & & \| & & \\
0 \to H^1(S, \boldsymbol{\mu}_2 \otimes V)^G & \to & H^1(U, \boldsymbol{\mu}_2 \otimes V)^G & \to & H^2_?(S_2, \boldsymbol{\mu}_2 \otimes V)^G & \to & M & \to & 0
\end{array}$$

In this case, 2 is evidently anomalous for A (2 splits in L). Of course $\dim H^2_?(S_2, A[2])^G = 1/2 \dim H^1(L_2, A[2])^G$ (by 1.1.3 and local flat duality), and is thus 2 in this anomalous case; by 1.3.5, the column of $H^2_?$ has dimensions (reading from top to bottom) 3, 2, 1. Thus $\dim H^1(S, A[2])^G = \dim H^1(S, \mathbf{Z}/2 \otimes V)^G + 1 = h + 1$, where h is as above. Combining this with 2.4.1, and with 1.1, we obtain

2.6. THEOREM (preliminary version): *Let A be an elliptic curve over $\mathbf{Q}$ with $A[2](\mathbf{Q}) = 0$, and square discriminant; let $L = \mathbf{Q}(A[2])$; let $h = \dim Cl(L)[2]$. If all the units in L whose norm (over $\mathbf{Q}$) $= 1$ are totally positive, then $\dim H^1(Z, A[2]) = h + 2$. Otherwise, $\dim H^1(Z, A[2]) = h + 1$. (We assume, as always, good reduction at 2).*

PROOF: If the discriminant of A is a rational square, then so is $j(A) - 1728$. To say that $\mathrm{Gal}(L/\mathbf{Q})$ is cyclic cubic is to say that A comes from a rational point on a certain modular curve, namely the double covering of the j-line whose function field is contained in the field of modular functions of level 2; and it is known (Cf. [26] Chapter 18, §6) that this double covering is parametrized by $\sqrt{j - 1728}$. Thus our condition on A, that $\mathrm{Gal}(L/\mathbf{Q})$ is cyclic cubic, is equivalent to saying that its discriminant be a square in $\mathbf{Q}$. We have only to remark that the condition that all the units (of norm 1) be totally positive is exactly our case (a) of 2.2.2.

2.7. Since L is totally real, $A(\mathbf{R})$ contains all the 2-division points of $A(\mathbf{C})$; i.e., $A(\mathbf{R})$ has two connected components. In our case, we have the exact sequence 1.3.4, with $p = \infty$.

$$0 \longrightarrow A(\mathbf{R})/A(\mathbf{R})^0 \xrightarrow{\delta} H^1(\mathbf{R}, A[2]) \xrightarrow{q} H^1(\mathbf{R}, A)[2] \longrightarrow 0 \tag{2.7.1}$$

Here $A(\mathbf{R})^0$ is the connected component of the identity in $A(\mathbf{R})$, of index two in $A(\mathbf{R})$; thus Tate's duality theorem (or the observation that $H^1(\mathbf{R}, A[2]) = \mathrm{Hom}(\mathrm{Gal}(\mathbf{C}/\mathbf{R}), A[2]))$ implies that the middle term is of dimension two, and the right-most term of dimension one. Let $j: H^1(Z, A[2]) \simeq H^1(S, A[2])^G \to H^1(\mathbf{R}, A[2])$ be the natural localization map; we have seen (2.4.2.2) that j is surjective in case (a). Let $\beta = q \circ j: H^1(Z, A[2]) \to H^1(\mathbf{R}, A)[2]$; then we have

(2.7.2) dim Ker $\beta = b + 1$ in case (a) of 2.2.2; in particular, the dimension is *odd*.

We remark that the Selmer group is a subgroup of $H^1(Z, A[2])$ contained in Ker β (more or less); this we shall clarify in the sequel.

2.8. Assume now we are in case (b) of 2.2.2. We claim that, in this case, the map $H^1(S, \boldsymbol{\mu}_2 \otimes V)^G \xrightarrow{j'} H^1(\mathbf{R}, A[2])$ (defined because $A[2] \simeq \boldsymbol{\mu}_2 \otimes V$ over $\mathbf{R}$) is surjective, with kernel $H^1(S, \mathbf{Z}/2 \otimes V)^G$. In fact, all the elements of the last group are unramified at infinity, and $\mathrm{codim}(H^1(S, \mathbf{Z}/2 \otimes V)^G$ in $H^1(S, \boldsymbol{\mu}_2 \otimes V)^G) = 2$ (Cf. 2.5); thus, in order to establish our claim, it suffices to show that j' is surjective. But we have the commutative diagram (arising from Kummer):

$$\begin{array}{ccc} Y/Y^2 & \longrightarrow & H^1(S, \boldsymbol{\mu}_2) \\ \downarrow & & \downarrow r \\ W & \simeq & H^1(S_\infty, \boldsymbol{\mu}_2) \end{array} \tag{2.8.1}$$

where Y and W are as in 2.2 (so the left-hand vertical map, and consequently the right-hand vertical map, is surjective), and where $S_\infty = \mathrm{Spec}(L \otimes_{\mathbf{Q}} \mathbf{R})$. That j' is surjective follows from the surjectivity of r.

Let K/L be the class field corresponding to $H^1(S, \boldsymbol{\mu}_2)$ and let $g_i \in \mathrm{Gal}(K/L)$ generate the inertia group (of order two) of the real prime r_i in L. The g_i's are distinct – they generate $\mathrm{Gal}(K/H)$, where H is the Hilbert 2 class field of L, of index $2^3 = [H^1(S, \boldsymbol{\mu}_2): H^1(S, \mathbf{Z}/2)]$ in K – and are conjugate under the action of G. The kernel of $q \circ j'$ is generated by $\ker j: H^1(S, A[2])^G \to H^1(\mathbf{R}, A[2])$, and by the homomorphism $\xi: \mathrm{Gal}(K/H) \to A[2]$; described as follows: We know

that $H^1(\mathbf{R}, A[2]) \simeq \mathrm{Hom}(\mathrm{Gal}(\mathbf{C}/\mathbf{R}), A[2]) \simeq \mathrm{Hom}((\pm 1), A[2])$. The kernel of q is then a homomorphism which takes -1 to a point e; when L_{r_i} is identified with $\mathbf{R}$, this point is called e_i, and it is then evident that the conjugation which takes r_i to r_j takes e_i to e_j. The homomorphism ξ takes the element g_i of $\mathrm{Gal}(K/H)$ to e_i; this is well-defined up to an element of $\ker j$.

2.8.2. We want a more explicit description of the point e referred to above. Now, if $x \in A(\mathbf{R}) - A(\mathbf{R})^0$, then, in the notation of 2.7.1, $\delta(x)_\sigma = \sigma(x) - x' \in A[2]$, where $2x' = x$ on A, $x' \in A(\mathbf{C})$, $\sigma \in \mathrm{Gal}(\mathbf{C}/\mathbf{R})$. We may represent A over $\mathbf{C}$ as $\mathbf{C}/\mathscr{L}$, where $\mathscr{L}$ is the lattice generated by $\{1, \tau\}$; to say that $A(\mathbf{R}) \neq A(\mathbf{R})^0$ is to say that $1/2\mathscr{L}$ is fixed by $\mathrm{Gal}(\mathbf{C}/\mathbf{R})$; i.e., that τ can be chosen to be purely imaginary. Then the image of $\tau/2$ in $\mathbf{C}/\mathscr{L}$ is in $A(\mathbf{R}) - A(\mathbf{R})^0$, and $\delta(\tau/2)_\sigma = \tau/2$, for σ the generator of $\mathrm{Gal}(\mathbf{C}/\mathbf{R})$. Thus e is the image of $\tau/2$.

One sees from this description that e is *functorial* with respect to $\mathbf{R}$-isomorphisms of elliptic curves.

2.8.3. Since the g_i's generate $\mathrm{Gal}(K/H)$, $g_1 + g_2 + g_3 \neq 0$. There is only one non-trivial G-orbit in $\mathrm{Gal}(K/H) \simeq I \oplus V$ with that property; but the inertia groups of the $\pi_i \mid 2$ also generate $\mathrm{Gal}(K/H)$ and their generators also form a G-orbit; thus the sets coincide. Thus g_i generates the inertia group of some π_j, and we shall say that r_i and π_i are *linked.*

We let ξ be the element of $H^1(S, \boldsymbol{\mu}_2 \otimes V)^G$ described above; we want to know when it comes from an element of $H^1(S, A[2])^G$, i.e., when it restricts to an element of $H^1(S_{\pi_i}, A[2])$ for each i. Since E has ordinary reduction at each π_i, if I_{π_i} designates the inertia subgroup of $\mathrm{Gal}(\bar{L}_{\pi_i}/L_{\pi_i})$, then

$$H^1(S_{\pi_i}, A[2]) \simeq H^1(S_{\pi_i}, \mathbf{Z}/2 \times \boldsymbol{\mu}_2)$$
$$= \{f \in \mathrm{Hom}(\mathrm{Gal}(\bar{L}_{\pi_i}/L_{\pi_i}), A[2]) \mid f(I_{\pi_i}) \subset \boldsymbol{\mu}_2\} \cap H^1(S_{\pi_i}, \boldsymbol{\mu}_2 \times \boldsymbol{\mu}_2).$$

Certainly ξ restricts to an element of $H^1(S_{\pi_i}, \boldsymbol{\mu}_2 \times \boldsymbol{\mu}_2)$; and it takes g_i, the generator of inertia, to the point e_i. Thus $\xi \in H^1(S, A[2])^G$ if and only if e_i reduces to the identity (mod π_i). That is,

2.6. Theorem (Final Version): *Let A, L and h be as in the preliminary version of* 2.6. *If all the units in L of norm (over $\mathbf{Q}$) $= 1$ are totally positive, then the kernel of the canonical localization map $\beta : H^1(Z, A[2]) \to H^1(\mathbf{R}, A)[2]$ is of dimension $h + 1$. Otherwise,* $\ker \beta$ *is of dimension $h + 1$ or h, according as the following statement is or is not true*:

(**) *Suppose* π_i *and* r_i *are linked, and* e_i *is the point of* 2.8.2 *associated with* r_i; *then* e_i *reduces to the identity* (mod π_i).

If the designated dimension is $h+1$, we say the curve A is *somewhat odd*; recall that $h+1$ must be an odd number. When $\ker \beta$ is equal to the Selmer group, then the number of first 2-descents of $A/\mathbf{Q}$ is odd, which should imply that A has an infinite number of rational points. We elaborate upon this in the immediate sequel.

2.9. THEOREM: *Let* $A/\mathbf{Q}$ *be as in Theorem* 2.6, *with discriminant* D^2, $D \in \mathbf{Z}$. *Suppose the following conditions are satisfied*:

(*a*) *If* p *is a prime such that* $p^3 \mid D$, *then* p *stays prime in* $L = \mathbf{Q}(A[2])$.

(*b*) *The prime* 3 *does not divide* D.

(*c*) A *has multiplicative reduction nowhere.*

(*d*) A *is somewhat odd.*

(*e*) $Ш(A, \mathbf{Q})$ *is finite, and* $Ш(A, \mathbf{Q})[2]$ *has* $\mathbf{F}_2$ *dimension* s.

Then A *has a rational point over* $\mathbf{Q}$ *of infinite order. In fact, if* $\rho = \dim_{\mathbf{Q}}(A(\mathbf{Q}) \otimes \mathbf{Q})$, *then* $\rho + s = h + 1$, *with* h *as in Theorem* 2.6.

PROOF: We recall the properties of the classical Selmer group, or group of first descents. If p is a prime, then there is an exact sequence (Cf. [3]):

$$0 \longrightarrow A(K)/pA(K) \longrightarrow S_p(A, K) \longrightarrow Ш(A, K)[p] \longrightarrow 0; \tag{2.9.1}$$

here A is any abelian variety over the number field K, $S_p(A, K)$, the Selmer group, is very close to $H^1(S, A[p])$, where S is the integer spectrum of K, and $Ш(A, K)[p]$ has a non-degenerate $\mathbf{F}_p$-linear symplectic form (in particular, has even dimension), if $Ш(A, K)$ is finite. For simplicity, we let A be an elliptic curve, $K = \mathbf{Q}$. We have the following exact sequence over the étale site of Spec($\mathbf{Z}$):

$$0 \longrightarrow A[2] \longrightarrow A \xrightarrow{\times 2} A \longrightarrow F \longrightarrow 0. \tag{2.9.2}$$

The skyscraper sheaf F measures the 2-disconnectedness of the bad fibers of A. Since A has good reduction at 2 and 3, (a) and (c) imply, via the Kodaira-Néron list of possibilities for F (Cf. [47]) that F has support at a set of primes in Spec($\mathbf{Z}$) which stay prime in L. At each of these primes, F is a $G = \mathrm{Gal}(L/\mathbf{Q})$-module isomorphic to V, the

non-trivial two-dimensional representation of G: in fact, the points of order two would otherwise not generate non-trivial extensions of the residue fields at these primes. Thus $H^0(Z, F) = H^1(Z, F) = 0$ (cohomology of this skyscraper sheaf is nothing but Galois cohomology over the residue fields at its support); this implies, thanks to [28], Proposition 9.7 and Appendix), that $S_2(A, K) \simeq \operatorname{Ker} \beta \subset H^1(Z, A[2])$, with β as in 2.6. By 2.6 and assumption (d), $\dim S_2(A, K)$ is odd; by assumption (e), $\dim Ш(A, \mathbf{Q})[2] = s$ is even. Thus $A(\mathbf{Q})/2A(\mathbf{Q})$ has odd dimension; since we have assumed $A(\mathbf{Q})$ has no 2-torsion, $A(\mathbf{Q})$ must be infinite. The formula for ρ follows immediately from 2.9.1.

2.10. COROLLARY: *Suppose A satisfies* (a)–(c) *of* 2.9, *and that $A(\mathbf{Q})$ has a point (necessarily of infinite order) whose image in $A(\mathbf{R})$ is not in the connected component of the identity. Then A is somewhat odd.*

PROOF: The assumption is that, in the following commutative diagram:

$$\begin{array}{ccccc} 0 & \longrightarrow & A(\mathbf{Q})/2A(\mathbf{Q}) & \longrightarrow & H^1(Z, A[2]) \\ & & \Big\downarrow j' & & \Big\downarrow J \\ 0 & \longrightarrow & A(\mathbf{R})/2A(\mathbf{R}) & \xrightarrow[j'']{} & H^1(\mathbf{R}, A[2]) \end{array}$$

(the top row is part of exact sequence 2.9.1, by assumptions (a)–(c) of 2.9), the map $j'' \circ j'$, hence the map J, has non-zero image. It follows from the computations of 2.7 and 2.8 that A must be somewhat odd.

2.11. EXAMPLE: Let A be the curve, in generalized Weierstrass form,

$$y^2 + xy = x^3 - 36x - 1. \tag{2.11.1}$$

Here the discriminant is D^2, where $D = 13.133$. Away from 2, A can be written

$$Y^2 = p(x) = x^3 + x^2/4 - 36x - 1;\ Y = y + x/2. \tag{2.11.2}$$

L is the splitting field of $p(x)$; $p(x + 1)$ is an Eisenstein polynomial at 13, and $p(x + 11)$ at 133, so both primes of bad reduction are ramified in K, and indeed E has additive reduction at both 13 and 133, as the Eisenstein polynomials demonstrate (they also demonstrate that A

has no rational 2-division points over **Q**). Thus A satisfies conditions (a)–(c) of 2.9. The point $(x, y) = (-2, 9)$ on A is not in the connected component of the identity of $A(\mathbf{R})$: in fact, for $x = 0$, $p(x)$ is negative, hence A has no points over **R** with $x = 0$. The point $(-2, 8)$ on 2.11.2, corresponding to the point $(-2, 9)$ on 2.11.1, is thus to the left of the y axis; but the connected component of the identity (= the point at infinity) is to the right of the y-axis. By Corollary 2.10, A is somewhat odd. This is scarcely of any interest in itself, as one sees immediately (by reducing mod 2 and 3) that $P = (-2, 9)$ is of infinite order. However, we have the following:

2.12. PROPOSITION: *Let d be a positive square-free integer congruent to* 1 (mod 8); *let A_d be the twist of A by the unique element of* $H^1(\mathrm{Gal}(\mathbf{Q}(\sqrt{d})/\mathbf{Q}), \mathrm{Aut}(A))$; *$A_d$ has equation*

$$y^2 + xy = x^3 + 1/4(d-1)x^2 - 36d^2x - d^3.$$

Then A_d is somewhat odd.

PROOF: Over $\mathbf{Q}(\sqrt{d})$, there is an isomorphism $A \simeq A_d$, given (in the coordinates of 2.11.2) by $(x, y) \mapsto (dx, d^{3/2}Y)$. The assumption is that this is already defined over $\mathbf{Z}_2$ and over **R**; it thus preserves the points e_i associated to the real primes of L in 2.8.2, and the points which reduce to the identity (mod π_i), the primes dividing 2 in L. It thus preserves the condition (**), and the Proposition follows from our knowledge that A is already somewhat odd.

2.13. COROLLARY: *Let d be as in Proposition* 2.12, *satisfying further that* $3 \nmid d$ (*this condition is probably irrelevant*), *and that all primes dividing d stay prime in* $\mathbf{Q}(A[2])$. *Then either* $Ш(\mathbf{Q}, A_d)$ *is of infinite order, or* $A_d(\mathbf{Q})$ *is of infinite order.*

PROOF: The discriminant of A_d is D^2, where $D = 13.133 \cdot d^3$; A_d evidently has additive reduction at primes dividing d, and by 2.12 it is somewhat odd. The corollary follows from 2.9.

2.13.1. REMARK: Neal Koblitz programmed the computer to find a point on A_{17}; 17 is the first admissible d. The computer found the following point: $(x, y) = \left(-\frac{273}{4}, 638\right)$.

REFERENCES

[1] *Modular Functions of One Variable IV, Lecture Notes in Mathematics*, 476 (1975).

[2] E. ARTIN and J. TATE: *Class Field Theory*, New York: Benjamin (1967).

[3] M. ARTIN and B. MAZUR: "Flat Arithmetic Duality," to appear.

[4] J. AX: "On the Units of an Algebraic Number Field," *Ill. J. Math.*, 9 (1965) 584–589.

[5] A. BRUMER: "On the Units of Algebraic Number Fields," *Mathematika*, 14, 121–124, (1967).

[6] J.W.S. CASSELS, "Diophantine Equations with Special Reference to Elliptic Curves," *J. Lon. Math. Soc.*, 41, 193–291, (1966).

[7] J.W.S. CASSELS: "The Rational Solutions of the Diophantine Equation $Y^2 = X^3 - D$," *Acta Math.*, 82, 243–273, (1950).

[8] J. COATES: "On K_2 and Some Classical Conjectures in Algebraic Number Theory," *Ann. of Math.*, 95, 99–116, (1972).

[9] J. COATES and A. WILES, "On the Conjecture of Birch and Swinnerton-Dyer," *Inv. Math.*, 39, 223–251, (1977).

[10] P. DÉLIGNE: "Formes Modulaires et Représentations ℓ-Adiques," Sem. Bourbaki 1968/69, N$^{\underline{o}}$ 355, *Lecture Notes in Mathematics*, 179 (1971).

[11] P. DÉLIGNE and M. RAPOPORT: "Les Schémas de Modules de Courbes Elliptiques," in *Modular Functions of One Variable II, Lecture Notes in Mathematics*, 349, (1973).

[12] J. DIXMIER: *Algèbres Enveloppantes*, Paris: Gauthier-Villars (1974).

[13] B. FERRERO: "Iwasawa Invariants of Abelian Number Fields," to appear.

[14] P. GABRIEL: "Des Catégories Abeliens," *Bull. Soc. Math. France*, 90, 323–448, (1962).

[15] A. GROTHENDIECK: "Le Groupe de Brauer III: Exemples et Compléments," in Dix Exposés sur la Cohomologie des Schémas, Amsterdam: North-Holland, (1968).

[16] A. GROTHENDIECK: "Modèles de Néron et Monodromie," in SGA 7, *Lecture Notes in Mathematics*, 288, (1972).

[17] R. GREENBERG: "The Iwasawa Invariants of Γ-Extensions of a Fixed Number Field," *Am. J. Math.*, 95, 204–214, (1973).

[18] R. GREENBERG: "On p-Adic L--Functions and Cyclotomic Fields II," Nagoya Math. J., 67, 139–158 (1977).

[19] R. GREENBERG: On the Iwasawa Invariants of Totally Real Number Fields," *Am. J. Math.*, 98, 263–284, (1976).

[20] M. HAZEWINKEL: "On Norm Maps for One Dimensional Formal Groups I: The Cyclotomic Γ-Extension" Netherlands School of Economics, Econometric Institute, Report 7206, (1972).

[21] K. IWASAWA: "On $\mathbf{Z}_\ell$-Extensions of Algebraic Number Fields," *Ann. of Math.*, 98, 246–326, (1973).

[22] K. IWASAWA: "A Note on Class Numbers of Algebraic Number Fields," *Abh. Math. Sem. Univ. Hamburg*, 20, 257–58, (1956).

[23] N. KATZ: "P-Adic Interpolation of Real Analytic Eisenstein Series," *Ann. of Math.*,.104, 459–571, (1976).

[24] M. LAZARD: "Groupes Analytiques p-Adiques," *Publ. Math. I.H.E.S.*, 26, (1965).

[25] S. LANG: "Algebraic Groups over Finite Fields," *Ann. J. Math.*, 78, 553–563, (1956).

[26] S. LANG: *Elliptic Functions*, Reading, Mass.: Addison-Wesley, (1973).

[27] JU. I. MANIN and M.M. VISHIK: "P-Adic Hecke Series of Imaginary Quadratic Fields," (Trans.) *Math. U.S.S.R. Sbornik*, 24, 345–371, (1974).

[28] B. MAZUR: "Rational Points of Abelian Varieties with Values in Towers of Number Fields," *Inv. Math.*, 18, 183–266, (1972).

[29] B. MAZUR: "Local Flat Duality," *Am. J. Math.*, 92, 343–361, (1970).

[30] B. MAZUR: "Rational Points of Modular Curves," in *Modular Functions of One Variable V, Lecture Notes in Mathematics*, 601, (1977).
[31] B. MAZUR: "Trees of Rational Points of Elliptic Curves," unpublished manuscript.
[32] B. MAZUR and L. ROBERTS: "Local Euler Characteristics," *Inv. Math.*, 9, 201–234, (1970).
[33] B. MAZUR and P. SWINNERTON-DYER: "Arithmetic of Weil Curves," *Inv. Math.*, 25, 1–61, (1974).
[34] A. NÉRON: "Modèles Minimaux des Variétés Abéliennes sur les Corps Locaux et Globaux," *Publ. Math. I.H.E.S.*, 21, (1964).
[35] F. OORT and D. MUMFORD: "Deformations and Liftings of Finite, Commutative Group Schemes," *Inv. Math.*, 5, 317–334, (1968).
[36] F. OORT and J. TATE: "Group Schemes of Prime Order," *Ann. Sci. E.N.S.*, 3, 1–21, (1970).
[37] M. RAYNAUD: "Schemas en Groupes de Type (p, . . ., p)," *Bull. Soc. Math. France*, 102, 241–280, (1974).
[38] L.G. ROBERTS: "The Flat Cohomology of Group Schemes of Rank p," *Am. J. Math.*, 95, 688–702, (1973).
[39] J.-P. SERRE: "Propriétés Galoisiennes des Points d'Ordre Fini des Courbes Elliptiques," *Inv. Math.*, 15, 259–331, (1972).
[40] J.-P. SERRE: "Classes de Corps Cyclotomiques," *Sém. Bourbaki*, N° 174, (1958), New York: Benjamin (1966).
[41] J.-P. SERRE: "Sur les Groupes de Congruence des Variétés Abéliennes II," *Izv. Akad. Nauk S.S.S.R.*, Ser. Mat., Tom 35, 731–737, (1971).
[42] J.-P. SERRE: *Abelian ℓ-Adic Representations and Elliptic Curves*, New York: Benjamin, (1968).
[43] J.-P. SERRE: "Groupes Analytiques p-Adiques," *Sém. Bourbaki*, 1963/64, N° 270, Secretariat Mathematiques, 11 Rue Pierre Curie, Paris 6e, (1964).
[44] J.-P. SERRE and J. TATE: "Good Reduction of Abelian Varieties," *Ann. of Math.*, 88, 492–517, (1968).
[45] *Séminaire de Geometrie Algebrique de Bois Marie, Lecture Notes in Mathematics*, 269, 270, 305, (1972).
[46] J. TATE: "Duality Theorems in Galois Cohomology over Number Fields," *Proc. Int. Cong. Math. Stockholm*, 1962, 288–295. Institute Mittag-Leffler, Djursholm, Sweden, (1963).
[47] J. TATE: "Algorithm for Determining the Type of a Singular Fiber in an Elliptic Pencil," in [1], 33–52.
[48] J. TATE: "Global Class Field Theory," in *Algebraic Number Theory*, J.W.S. Cassels and A. Fröhlich, eds., New York: Academic Press, (1967).
[49] M.M. VISHIK: "The p-adic Zeta-Function of an Imaginary Quadratic Field and the Leopoldt Regulator," (Russian), *Mat. Sbornik*, 102 (144), 173–181, (1977).
[50] M. HARRIS: "P-adic Representations of p-adic Groups," to appear in J. of Algebra.
[51] M. HARRIS: "Systematic Growth of Mordell-Weil Groups of Abelian Varieties in Towers of Number Fields," to appear in Inv. Math.

(Oblatum 21–XII–1977 & 22–IX–1978)

Department of Mathematics
Brandeis University
Waltham, Ma. 02154