Advanced Studies in Pure Mathematics 17, 1989
Algebraic Number Theory — in honor of K. Iwasawa
pp. 97–137

Iwasawa Theory for p-adic Representations

Ralph Greenberg

To Professor Kenkichi Iwasawa on his seventieth birthday

Several years ago Mazur and Wiles proved a fundamental conjecture of Iwasawa which gives a precise link between the critical values of the Riemann zeta function (and, more generally, Dirichlet L-functions) and the ideal class groups of certain towers of cyclotomic fields. Probably the first hint of such a link is Kummer's well-known criterion for irregularity of primes. In Iwasawa's theory one defines for each prime p certain modules over the Iwasawa algebra Λ (which we will describe in Section 1). Iwasawa's conjecture then relates the structure of these Λ-modules to the p-adic L-functions constructed by Kubota and Leopoldt which interpolate critical values of Dirichlet L-functions. Mazur realized that, following Iwasawa's model, one could formulate a similar conjecture for an elliptic curve E (defined over $\boldsymbol{Q}$) and for any prime p where E has good, ordinary reduction. Mazur and Swinnerton-Dyer constructed p-adic L-functions attached to E for such p (assuming E is a Weil curve). The Iwasawa modules which Mazur's conjecture relates to these p-adic L-functions are defined in terms of Selmer groups for E, again in towers of cyclotomic fields. This time the hint of such a relationship is the Birch and Swinnerton-Dyer conjecture.

There are now several other cases where p-adic analogues of complex L-functions have been constructed—for example, Manin's p-adic L-functions attached to classical modular forms. It seems worthwhile then to search for appropriate Iwasawa modules in a much more general context and that is our purpose in this paper. We will consider a compatible system of l-adic representations $V=\{V_l\}$ over $\boldsymbol{Q}$. Thus V_l is a finite dimensional vector space over $\boldsymbol{Q}_l$ (the l-adic numbers) of dimension $d=d_V$ on which $G_{\boldsymbol{Q}}=\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$ acts. (For any field k, G_k denotes $\mathrm{Gal}(\bar{k}/k)$, where $\bar{k}$ is an algebraic closure of k.) If q is any prime, then one can also consider V_l as a representation space of $G_{\boldsymbol{Q}_q}$ by choosing a place $\bar{q}$ of $\bar{\boldsymbol{Q}}$ over q and identifying $G_{\boldsymbol{Q}_q}$ with the decomposition group for that place. We will usually assume that p is an "ordinary" prime for V in the follow-

Received February 5, 1988.

ing sense: there should exist a filtration F^iV_p of $\boldsymbol{Q}_p$-subspaces of $V_p (i \in \boldsymbol{Z})$ with the properties:

$$(1)\quad \begin{array}{ll} \text{(a)} & F^{i+1}V_p \subseteq F^iV_p;\ F^iV_p = V_p \text{ for } i \ll 0 \\ & \qquad\qquad F^iV_p = 0 \text{ for } i \gg 0 \\ \text{(b)} & F^iV_p \text{ is invariant for the action of } G_{\boldsymbol{Q}_p}. \text{ The inertia subgroup} \\ & I_{\boldsymbol{Q}_p} \text{ of } G_{\boldsymbol{Q}_p} \text{ acts on } gr^i(V_p) = F^iV_p/F^{i+1}V_p \text{ by } \chi_p^i. \end{array}$$

Here of course χ_p denotes the homomorphism of $G_{\boldsymbol{Q}_p}$ to $\boldsymbol{Z}_p^\times$ giving the action on the group μ_{p^∞} of p-power roots of unity. The filtration (but not its existence) depends on the choice of place of $\bar{\boldsymbol{Q}}$ over p. The properties (a) and (b) would clearly characterize it.

Choose a lattice $T_p \subseteq V_p$ which is invariant under the action of $G_{\boldsymbol{Q}}$. Then $G_{\boldsymbol{Q}}$ acts on $A_p = V_p/T_p$ which as a group is just $(\boldsymbol{Q}_p/\boldsymbol{Z}_p)^d$. T_p is its "Tate module". Let $\boldsymbol{Q}_\infty$ denote the cyclotomic $\boldsymbol{Z}_p$-extension of $\boldsymbol{Q}$. Thus $\boldsymbol{Q}_\infty \subseteq \boldsymbol{Q}(\mu_{p^\infty})$ and $\Gamma = \mathrm{Gal}(\boldsymbol{Q}_\infty/\boldsymbol{Q})$ is isomorphic to $\boldsymbol{Z}_p$. For each place v of $\boldsymbol{Q}_\infty$ (including the unique place v_p above p), choose a place $\bar{v}$ of $\bar{\boldsymbol{Q}}$ over v and let I_v and D_v denote the inertia and decomposition group for $\bar{v}$ in $G_{\boldsymbol{Q}_\infty}$. Our object of study in this paper will be the following group (which we will call a Selmer group):

$$(2)\quad S_{A_p}(\boldsymbol{Q}_\infty) = \{\sigma \in H^1(\boldsymbol{Q}_\infty, A) \mid \sigma \text{ is locally trivial at all places } v \text{ of } \boldsymbol{Q}_\infty\}$$

For $v \nmid p$ (including the infinite places), a cocycle σ is "locally trivial at v" if

$$(3)\quad \sigma \in \ker\left(H^1(\boldsymbol{Q}_\infty, A_p) \longrightarrow H^1(I_v, A_p)\right),$$

where the arrow is the restriction map.

For $v = v_p$, locally trivial means σ is in the kernel of the composite map:

$$(4)\quad H^1(\boldsymbol{Q}_\infty, A_p) \longrightarrow H^1(I_v, A_p) \longrightarrow H^1(I_v, A_p/F^+A_p)$$

where we define $F^+V_p = F^1V_p$ and F^+A_p is its image in A_p. The definition is easily seen to be independent of the choice of places of $\bar{\boldsymbol{Q}}$, but does in fact depend on the choice of lattice T_p. Also, in (3), one could replace I_v by D_v since D_v/I_v has (profinite) order prime to p. In (4), it will be useful at times to replace I_v by D_v. This will define a possibly smaller subgroup of $H^1(\boldsymbol{Q}_\infty, A_p)$, which we will call the "strict" Selmer group. We will also consider the Selmer group $S_{A_p}(\boldsymbol{Q})$ (and its strict version) defined by using decomposition and inertia groups in $G_{\boldsymbol{Q}}$.

Now Γ acts on $S_{A_p}(\boldsymbol{Q}_\infty)$ (by its natural action on $H^1(\boldsymbol{Q}_\infty, A_p)$). Since

$S_{A_p}(\boldsymbol{Q}_\infty)$ is a p-primary torsion group, we can regard it as a (discrete) $\boldsymbol{Z}_p$-module and hence a Λ-module, where Λ denotes the completed group algebra for Γ over $\boldsymbol{Z}_p$ (the Iwasawa algebra). If S is any discrete Λ-module (or $\boldsymbol{Z}_p$-module), then the Pontryagin dual $\hat{S}$ is a compact Λ-module. We say S is cofinitely generated as a Λ-module (or $\boldsymbol{Z}_p$-module) if $\hat{S}$ is finitely generated over Λ (or $\boldsymbol{Z}_p$). We then define $\mathrm{corank}_\Lambda(S)$ as $\mathrm{rank}_\Lambda(\hat{S})$, $\mathrm{corank}_{\boldsymbol{Z}_p}(S)$ as $\mathrm{rank}_{\boldsymbol{Z}_p}(\hat{S})$. If $\hat{S}$ is Λ-torsion, we say S is Λ-cotorsion. We will prove that $S_{A_p}(\boldsymbol{Q}_\infty)$ is always cofinitely generated as a Λ-module.

One can also define an L-function $L_V(s)$ for the compatible system V. For every prime q, let $(V_l)_{\mathrm{unr}}$ denote the maximal *quotient* of V_l on which the action of $G_{\boldsymbol{Q}_q}$ is unramified. Define (for any $l \neq q$)

$$(5) \qquad E_q(T) = \det(I - \mathrm{Frob}(q)T : (V_l)_{\mathrm{unr}}).$$

Here Frob (q) is the *arithmetic* Frobenius automorphism. The definition of a compatible system is that, for all q outside a finite set and for $l \neq q$, the action of $G_{\boldsymbol{Q}_q}$ on V_l is unramified and the polynomial $E_q(T)$ has coefficients in $\boldsymbol{Q}$ and is independent of l. We will also want to assume this statement about $E_q(T)$ even for q in the finite exceptional set. The q's for which $\deg(E_q(T)) < d$, that is, for which the action of $G_{\boldsymbol{Q}_q}$ on V_l $(l \neq q)$ is ramified, we will say are ramified for V. For $\mathrm{Re}(s) \gg 0$, define

$$(6) \qquad L_V(s) = \prod_q E_q(q^{-s})^{-1},$$

assuming something about the roots of $E_q(T)$ for convergence. Serre [26] and Deligne [4] describe the expected properties for this L-function, at least if V arises from an algebraic variety or, more generally, a motive over $\boldsymbol{Q}$. Notice however that our definition of $L_V(s)$ differs somewhat from theirs. To reconcile the two, one can simply regard V as arising from l-adic homology for some motive instead of l-adic cohomology. We will assume that V does in fact arise in this way from some motive over $\boldsymbol{Q}$, although, as far as possible, we will describe the properties we need solely in terms of V.

One expects that $L_V(s)$ can be analytically continued to a meromorphic function on the complex plane which satisfies a functional equation of a certain form. Let $\Gamma_V(s)$ be the expected Γ-factor (which we will say more about later). Let $V^* = \{V_l^*\}$, where $V_l^* = \mathrm{Hom}_{\boldsymbol{Q}_l}(V_l, \boldsymbol{Q}_l(1))$. Here $\boldsymbol{Q}_l(1)$ is the 1-dimensional $\boldsymbol{Q}_l$-space on which $G_{\boldsymbol{Q}}$ acts by the cyclotomic character χ_l. It is not hard to verify that V^* is also a compatible system over $\boldsymbol{Q}$. The conjectured functional equation should have the form

$$(7) \qquad \alpha_V^{2-s}\Gamma_V(2-s)L_V(2-s) = \pm\alpha_{V^*}^{s}\Gamma_{V^*}(s)L_{V^*}(s)$$

for certain constants α_V, α_{V^*}. We write the functional equation in the above way to focus on the behavior of $L_V(s)$ at $s=1$, which seems convenient for formulating our conjectures and results. But replacing V by the Tate twist $V(1-n)=\{V_l(1-n)\}$ and noting that $L_{V(1-n)}(s)=L_V(s+n-1)$ will give appropriate statements about $L_V(s)$ at $s=n$, for any integer n. Let r_V denote the order of pole for $\Gamma_V(s)$ at $s=1$. Since $\Gamma_V(s)$ has no zeros, $r_V \geq 0$. Often r_V is also the order of vanishing of $L_V(s)$ at $s=1$, but not always. (We mention two examples: (1) $V=\{\boldsymbol{Q}_l(1)\}$, $L_V(s)=\zeta(s-1)$, $r_V=1$, but $\zeta(0)=-\frac{1}{2}$. (2) $V=\{V_l(E)\}$, E an elliptic curve/$\boldsymbol{Q}$, $L_V(s)=$the Hasse-Weil L-function $L_E(s)$, $r_V=0$, but $L_V(1)$ can vanish.) Now, if φ is any even Dirichlet character, the twisted L-series $L_V(s, \varphi)$ should also satisfy a functional equation similar to (7), with the same Γ-factor, relating $L_V(2-s, \varphi)$ to $L_{V^*}(s, \varphi^{-1})$. If we let φ vary over the characters of $\Gamma=\mathrm{Gal}(\boldsymbol{Q}_\infty/\boldsymbol{Q})$, regarded as Dirichlet characters, it seems reasonable to conjecture that $L_V(s, \varphi)$ will have a zero of order exactly r_V at $s=1$, except possibly for finitely many φ. Sometimes this is easy to verify. A more subtle case is $L_E(s)$. Rohrlich [22] has proved the above conjecture in this case (i.e. $L_V(1, \varphi) \neq 0$ for all but finitely many $\varphi \in \hat{\Gamma}$) if E is a Weil curve.

Now our general philosophy is that the behavior of the L-functions $L_V(s, \varphi)$ at $s=1$ ($\varphi \in \hat{\Gamma}$) should somehow be reflected in the structure of the Selmer groups $S_{V_p/T_p}(\boldsymbol{Q}_\infty)$. Thus, the above remarks suggest the following conjecture. We assume p is ordinary for V and T_p is any $G_{\boldsymbol{Q}}$-invariant lattice.

Conjecture 1. *$S_{V_p/T_p}(\boldsymbol{Q}_\infty)$ has Λ-corank equal to r_V.*

We will be able to prove the following weaker result by making use of Tate's calculation of Euler-Poincaré characteristics and also the conjectural description of r_V in terms of quantities attached to the representation space V_p. We will have to also assume that V is pure in the sense that it arises from a motive of pure weight. We believe the above conjecture even without this assumption, but its seems to be a more subtle question then.

Theorem 1. *If V is pure, then* $\mathrm{corank}_\Lambda (S_{V_p/T_p}(\boldsymbol{Q}_\infty)) \geq r_V$.

It is especially interesting to consider the case where $r_V=r_{V^*}=0$. Then $L_V(1)$ and $L_{V^*}(1)$ are critical values in the sense of Deligne [4]. Deligne defines a number Ω_V as a determinant of periods coming from the Betti and de Rham realizations of the motive from which V arises. He conjectures that $L_V(1)/\Omega_V$ is rational. For $\varphi \in \hat{\Gamma}$, the values $L_V(1, \varphi)$ are also critical. It is reasonable to hope that for an ordinary prime p there should exist a p-adic L-function $L_p(\varphi, V)$ with the following properties. It should be defined for all but finitely many $\varphi \in \mathrm{Hom}_{\mathrm{cont}}(\Gamma, \boldsymbol{C}_p^\times)$ and have values

in $\boldsymbol{C}_p$, where $\boldsymbol{C}_p$ denotes the completion of $\bar{\boldsymbol{Q}}_p$. We fix embeddings of $\bar{\boldsymbol{Q}}$ into $\boldsymbol{C}$ and into $\boldsymbol{C}_p$. It should satisfy

(8)
(a) If $\varphi \in \hat{\Gamma}$, then $L_p(\varphi, V)=A_\varphi L_V(1, \varphi)$ for certain $A_\varphi \in \boldsymbol{C}$.
(b) There exists an element θ_V in the quotient field of Λ such that $L_p(\varphi, V)=\varphi(\theta_V)$ for all $\varphi \in \mathrm{Hom}_{\mathrm{cont}}(\Gamma, \boldsymbol{C}_p^\times)$ where $\varphi(\theta_V)$ is defined.

If $\varphi \in \mathrm{Hom}_{\mathrm{cont}}(\Gamma, \boldsymbol{C}_p^\times)$, then φ can be extended to a ring homomorphism $\varphi: \Lambda \to \boldsymbol{C}_p$. If $\theta_V=\lambda_V/\kappa_V$ with $\lambda_V, \kappa_V \in \Lambda$, $\kappa_V \neq 0$, we define

$$\varphi(\theta_V)=\varphi(\lambda_V)/\varphi(\kappa_V) \qquad \text{if } \varphi(\kappa_V) \neq 0.$$

$\hat{\Gamma}$ is the set of elements of finite order in $\mathrm{Hom}_{\mathrm{cont}}(\Gamma, \boldsymbol{C}_p^\times)$. Also, θ_V would be uniquely determined by (a) and (b). In this volume, Coates and Perrin-Riou discuss the existence of such p-adic L-functions. In particular, they describe conjecturally what the interpolation factors A_φ should be. They will involve Ω_V^{-1} in order for the right side in (a) to be in $\bar{\boldsymbol{Q}}$ so that it can be embedded in $\boldsymbol{C}_p$. But we want to mention what A_{φ_0} should be in case p is unramified for V. (Here φ_0 is the trivial character.) In this case, the Euler factors for p in $L_V(s)$ and $L_{V^*}(s)$ are of the form:

$$(9) \qquad \prod_{i=1}^{d}(1-\alpha_i p^{-s})^{-1} \quad \text{and} \quad \prod_{i=1}^{d}(1-\alpha_i^* p^{-s})^{-1}.$$

One should take

$$(10) \qquad A_{\varphi_0}=\Omega_V^{-1} \prod\nolimits_{+}(1-\alpha_i p^{-1}) \prod\nolimits_{+}(1-\alpha_i^* p^{-1})$$

where the $+$ indicates that the products should be over the α_i's and α_i^*'s with valuation >0. Also, one would conjecture that θ_V itself is in Λ unless the p-adic representations V_p or V_p^* of $G_{\boldsymbol{Q}}$ have some subquotient which is a p-adic representation factoring through Γ. These subquotients allow one to define canonically a rather simple $\kappa_V \in \Lambda$ such that $\lambda_V=\kappa_V\theta_V$ should be in Λ. We describe this κ_V in Section 1. We must also point out here that the fact that Ω_V is only defined in [4] up to a factor in $\boldsymbol{Q}^\times$ creates the same ambiguity in the definition of $L_p(\varphi, V)$.

If one chooses a $G_{\boldsymbol{Q}}$-invariant lattice T_p in V_p, then one can define one in V_p^* by $T_p^*=\mathrm{Hom}_{\boldsymbol{Z}_p}(T_p, \boldsymbol{Z}_p(1))$. If both r_V and r_{V^*} are zero, Conjecture 1 implies that both $S_{V_p/T_p}(\boldsymbol{Q}_\infty)$ and $S_{V_p^*/T_p^*}(\boldsymbol{Q}_\infty)$ will be Λ-cotorsion modules. Thus one can consider the characteristic ideals for their Pontryagin duals. Now we have an automorphism $\lambda \to \lambda^\iota$ of Λ induced from the automorphism $\iota: \gamma \to \gamma^{-1}$ of Γ. If S is any Λ-module, we define S^ι as the

Λ-module with the same underlying set as S but with Λ acting through ι. Using Tate's global duality theorems, we will prove that if $S_{V_p/T_p}(\boldsymbol{Q}_\infty)$ is Λ-cotorsion, then so is $S_{V_p^*/T_p^*}(\boldsymbol{Q}_\infty)$. We also prove the following relationship between these Selmer groups.

Theorem 2. *Assume $L_V(1)$ and $L_{V^*}(1)$ are critical values and that $S_{V_p/T_p}(\boldsymbol{Q}_\infty)$ is Λ-cotorsion. Then $\hat{S}_{V_p/T_p}(\boldsymbol{Q}_\infty)$ and $\hat{S}_{V_p^*/T_p^*}(\boldsymbol{Q}_\infty)^\iota$ have the same characteristic ideal.*

We think of Theorem 2 as a reflection of the fact that the functional equations should relate $L_V(1,\varphi)$ to $L_{V^*}(1,\varphi^{-1})$. This should also be reflected in a functional equation for the p-adic L-functions (for a good choice of Ω_V and Ω_{V^*}) which takes the form:

$$L_p(\varphi, V)=u_\varphi L_\varphi(\varphi^{-1}, V^*) \tag{11}$$

for some $u_\varphi \in \boldsymbol{C}_p^\times$ with absolute value 1. This would give $\lambda_V = u\lambda_{V^*}^\iota$, where $u \in \Lambda^\times$. Thus the following conjecture would seem to be compatible with functional equations.

Conjecture 2. *The Λ-module $\hat{S}_{V_p/T_p}(\boldsymbol{Q}_\infty)$ has characteristic ideal (λ_V).*

The above conjecture is imprecise in that the structure of the Selmer group can change if one chooses a different lattice T_p. The characteristic ideal will then change at most by multiplication by a power of p. Perrin-Riou calculates this change elsewhere in this volume. The choice of Ω_V can also change the ideal (λ_V) similarly. For each choice of T_p, there should be a natural way of defining Ω_V up to a factor in $\boldsymbol{Q}^\times$ with numerator and denominator prime to p which would make Conjecture 2 more precise.

Conjecture 1 is true when $d_V=1$, in which case it is simply a translation of well-known results of Iwasawa. Conjecture 2 is essentially Iwasawa's conjecture, which, for odd p, was proved by Mazur and Wiles in [19]. If E is an elliptic curve/$\boldsymbol{Q}$, one obtains a compatible family of l-adic representations by taking

$$V=V(E)=\{V_l(E)\}, \qquad \text{where } V_l(E)=T_l(E)\otimes \boldsymbol{Q}_l.$$

Here $T_l(E)$ is the Tate module for E and so $V_l(E)/T_l(E)\cong E_{l^\infty}$. Conjectures 1 and 2 are equivalent to conjectures of Mazur made in [16]. The observation that, for an elliptic curve E with ordinary reduction at p, the p-primary subgroup of the classical Selmer group for E over $\boldsymbol{Q}_\infty$ can be described just in terms of the Galois module $E_{p^\infty}=V_p(E)/T_p(E)$ and the observation that this description works in Iwasawa's case were for us the main motivation for our conjectures.

We intend to continue to study in subsequent papers various aspects of the structure of Selmer groups, some of which are: nontriviality of Selmer groups, anomalous primes and exceptional zeros, non-primitive Selmer groups, and Selmer groups in special cases such as Artin representations and symmetric powers of Tate modules for elliptic curves. As a reader will find, our approach will tend to be very much in the spirit of classical Iwasawa theory. However, there should be many fruitful ways to think about the special values of L-functions. Certainly geometric and algebraic objects attached to the algebraic varieties or motives from which the L-functions come should be part of the picture. The article by P. Schneider in this volume provides another point of view which, although still in the spirit of Iwasawa theory, brings a much more geometric perspective to the subject.

We are grateful to many people, too numerous to mention, with whom we have had valuable discussions related to the topic of this paper. We especially want to thank John Coates for many helpful ideas and stimulating discussions. We also are grateful to the Université de Paris-Sud and to M.S.R.I. for their hospitality and the C.N.R.S. and N.S.F. for their support of this research.

§ 1. Classical Iwasawa theory

For each prime l, the action of $G_{\boldsymbol{Q}}$ on the l-power roots of unity μ_{l^∞} defines a character χ_l: $G_{\boldsymbol{Q}} \to \boldsymbol{Z}_l^\times$. For any $n \in \boldsymbol{Z}$, let $\boldsymbol{Q}_l(n)$ denote the 1-dimensional space over $\boldsymbol{Q}_l$ on which $G_{\boldsymbol{Q}}$ acts by χ_l^n. Then $\boldsymbol{Q}(n)=\{\boldsymbol{Q}_l(n)\}$ is a compatible system of l-adic representations over $\boldsymbol{Q}$. Every prime p is ordinary for $\boldsymbol{Q}(n)$. Let p be an odd prime. Then $\boldsymbol{Q}_\infty \subseteq K_\infty = \boldsymbol{Q}(\mu_{p^\infty})$ and $\Delta = \mathrm{Gal}(K_\infty/\boldsymbol{Q}_\infty)$ is isomorphic to $(\boldsymbol{Z}/p\boldsymbol{Z})^\times$. Since $|\Delta|$ is prime to p, the restriction map gives an isomorphism

$$H^1(\boldsymbol{Q}_\infty, \mu_{p^\infty}^n) \longrightarrow H^1(K_\infty, \mu_{p^\infty}^n)^\Delta = \mathrm{Hom}_\Delta(\mathrm{Gal}(K_\infty^{ab}/K_\infty), \mu_{p^\infty}^n),$$

where $\mu_{p^\infty}^n = \boldsymbol{Q}_p(n)/\boldsymbol{Z}_p(n)$ and K_∞^{ab} is the maximal abelian extension of K_∞. Δ acts on $\mathrm{Gal}(K_\infty^{ab}/K_\infty)$ by inner automorphisms. Let M_∞ denote the maximal abelian pro-p extension of K_∞ unramified at all places of K_∞ not lying over p. Let $X_\infty = \mathrm{Gal}(M_\infty/K_\infty)$. If $\sigma \in H^1(\boldsymbol{Q}_\infty, \mu_{p^\infty}^n)$, the local triviality conditions (3) mean that the restriction of σ is in $\mathrm{Hom}_\Delta(X_\infty, \mu_{p^\infty}^n)$. Let $\omega = \chi_p|_\Delta$. The characters of Δ are ω^k, $0 \leq k \leq p-2$, all of which have values in $\boldsymbol{Z}_p^\times$. Then $X_\infty = \oplus X_\infty^{\omega^k}$, where $X_\infty^{\omega^k}$ is the submodule of X_∞ on which Δ acts by ω^k. Clearly,

$$\mathrm{Hom}_\Delta(X_\infty, \mu_{p^\infty}^n) = \mathrm{Hom}(X_\infty^{\omega^k}, \mu_{p^\infty}^n)$$

where $k \equiv n \pmod{p-1}$. If n is positive, then $F^+\boldsymbol{Q}_p(n)=\boldsymbol{Q}_p(n)$, $F^+\mu_{p^\infty}^n=\mu_{p^\infty}^n$, and so

$$S_{\mu_{p^\infty}^n}(\boldsymbol{Q}_\infty) \cong \mathrm{Hom}\,(X_\infty^{\omega^k}, \mu_{p^\infty}^n) \tag{12}$$

for any $n \equiv k \pmod{p-1}$, $n \geq 1$. The isomorphism is in fact a Γ-isomorphism. If $n \leq 0$, then $F^+\boldsymbol{Q}_p(n)=0$ and so, letting L_∞ denote the maximal abelian pro-p extension of K_∞ unramified everywhere and letting $Y_\infty = \mathrm{Gal}\,(L_\infty/K_\infty)$, we have

$$S_{\mu_{p^\infty}^n}(\boldsymbol{Q}_\infty) = \mathrm{Hom}\,(Y_\infty^{\omega^k}, \mu_{p^\infty}^n) \tag{13}$$

for any $n \equiv k \pmod{p-1}$, $n \leq 0$. Now Iwasawa proves in [12] that the Galois groups $X_\infty^{\omega^k}$ have Λ-rank equal to 1 if k is odd, 0 if k is even. The Λ-modules $Y_\infty^{\omega^k}$ are Λ-torsion for all k.

If $V=\boldsymbol{Q}(n)$, then $L_V(s)=\zeta(s-n)$. The Γ-factor is $\Gamma((s-n)/2)$ and so we have $r_V=1$ if n is odd and positive, but $r_V=0$ otherwise. Iwasawa's results are equivalent to the assertion that $S_{\mu_{p^\infty}^n}(\boldsymbol{Q}_\infty)$ has Λ-corank $r_{\boldsymbol{Q}(n)}$. Now $V^*=\boldsymbol{Q}(1-n)$ and the values $L_V(1)=\zeta(1-n)$ and $L_{V^*}(1)=\zeta(n)$ are a pair of critical values precisely when n (or $1-n$) is positive and even. We assume $n>0$ and $n \equiv k \pmod{p-1}$ for some fixed even k, $0 \leq k \leq p-2$. The Kubota-Leopoldt p-adic L-function $L_p(s, \omega^k\varphi)$ has the property

$$L_p(1-n, \omega^k\varphi) = (1-\varphi(p)p^{n-1})L(1-n, \varphi)$$

for all characters $\varphi \in \hat{\Gamma}$. Here, as usual, φ as well as the numbers $L(1-n, \varphi)$ are regarded in $\boldsymbol{C}$ or in $\boldsymbol{C}_p$ using the fixed embeddings $\bar{\boldsymbol{Q}} \to \boldsymbol{C}$, $\bar{\boldsymbol{Q}} \to \boldsymbol{C}_p$. Iwasawa proved in [11] that, if one chooses a topological generator γ_0 of Γ, then there exist elements $G_k(T)$, $H_k(T) \in \boldsymbol{Z}_p[[T]]$ such that

$$L_p(1-n, \omega^k\varphi) = \frac{G_k(\varphi(\gamma_0)u_0^n - 1)}{H_k(\varphi(\gamma_0)u_0^n - 1)}$$

where $H_k(T)=T$ if $k=0$, $H_k(T)=1$ otherwise. Here we are putting $u_0 = \chi_p(\gamma_0)$ (identifying Γ with $\mathrm{Gal}\,(K_\infty/\boldsymbol{Q}(\mu_p))$. Now the isomorphism $\boldsymbol{Z}_p[[T]] \to \Lambda$, $T \to \gamma_0 - 1$, sends $G_k((1+T)u_0^n - 1)$, $H_k((1+T)u_0^n - 1)$ to elements λ_V, κ_V of Λ. Putting $\theta_V = \lambda_V\kappa_V^{-1}$, we have for any $\varphi \in \hat{\Gamma}$,

$$\varphi(\theta_V) = A_\varphi L_V(1, \varphi)$$

where $A_\varphi = (1-\varphi(p)p^{n-1})$. (Of course, $\varphi(p)=0$ if $\varphi \neq \varphi_0$.) For all $\varphi \in \mathrm{Hom}_{\mathrm{cont}}\,(\Gamma, \boldsymbol{C}_p^\times)$ (except the one φ such that $\varphi(\gamma_0)=u_0^{-n}$ if $k=0$), we define

$$L_p(\varphi, V) = \varphi(\theta_V),$$

which gives a p-adic L-function for $V=\boldsymbol{Q}(n)$ satisfying (8).

One version of Iwasawa's conjecture states that $G_k(T)$ is a characteristic power series for $X_\infty^{\omega^k}$ as a $\boldsymbol{Z}_p[[T]]$-module (where T acts as γ_0-1). This is a consequence of the Mazur-Wiles theorem. The Pontryagin dual of $S_{\mu_{p^\infty}^n}(\boldsymbol{Q}_\infty)$ is $X_\infty^{\omega^k}(-n)$ which has $G_k((1+T)u_0^n-1)$ as a characteristic power series. Thus as a Λ-module, $\hat{S}_{\mu_{p^\infty}^n}(\boldsymbol{Q}_\infty)$ has characteristic ideal (λ_V), which is Conjecture 2.

For $V^*=\boldsymbol{Q}(1-n)$, $n>0$ and even, and any $\varphi\in\hat{\Gamma}$, we have

$$L_{V^*}(1,\varphi)=L(n,\varphi)=\frac{\tau(\varphi)}{2(n-1)!\,f_\varphi^n}(2\pi i)^n L(1-n,\varphi^{-1})$$

where $\tau(\varphi)$ is the Gaussian sum for φ, f_φ the conductor of φ. Thus, one can define a p-adic L-function with the properties:

(a) $L_p(\varphi, V^*)=A_\varphi L_{V^*}(1,\varphi)$ for $\varphi\in\hat{\Gamma}$,
where $A_\varphi=\Omega_{V^*}^{-1}f_\varphi^n\tau(\varphi)^{-1}(1-\varphi^{-1}(p)p^{n-1})$, $\Omega_{V^*}=(2\pi i)^n/2(n-1)!$

(b) $L_p(\varphi, V^*)=\varphi(\theta_{V^*})$ for all (but one) $\varphi\in\mathrm{Hom}_{\mathrm{cont}}(\Gamma, \boldsymbol{C}_p^\times)$.

In (b), one simply takes $\theta_{V^*}=\lambda_{V^*}\kappa_{V^*}^{-1}$, where $\lambda_{V^*}=\lambda_V^\iota$, $\kappa_{V^*}=\kappa_V^\iota$ so that $\varphi(\theta_{V^*})=\varphi^{-1}(\theta_V)$. Then the functional equation (11) holds with $u_\varphi=1$. Now there is an equivalent (perhaps more familiar) version of Iwasawa's conjecture involving the Galois groups $Y_\infty^{\omega^k}$ for k odd. It is this form of the conjecture which Mazur and Wiles proved. The classical spiegelungsatz allows one to prove the equivalence of the two versions by showing that $X_\infty^{\omega^k}\sim(Y_\infty^{\omega^{1-k}})^\iota(1)$ as Λ-modules, when k is even. (The notation $\sim$ means there is a Λ-homomorphism with finite kernel and cokernel.) All of this is explained for example in [7]. It follows that, for $n>0$, n even,

$$S_{\mu_{p^\infty}^n}(\boldsymbol{Q}_\infty)\sim S_{\mu_{p^\infty}^{1-n}}(\boldsymbol{Q}_\infty)^\iota. \tag{14}$$

This makes Theorem 2 clear in this case as well as the equivalence of Conjecture 2 for $V=\boldsymbol{Q}(n)$ and for $V^*=\boldsymbol{Q}(1-n)$.

All of the above remarks are of course valid more generally. If χ: $G_{\boldsymbol{Q}}\to\bar{\boldsymbol{Q}}^\times$ is any character of finite order, let $E=\boldsymbol{Q}(\chi)$ be the field generated by the values of χ. Then χ gives a 1-dimensional representation of $G_{\boldsymbol{Q}}$ over E and one obtains a compatible system of l-adic representations $W=\{W_l\}$, where $W_l=E\otimes\boldsymbol{Q}_l$. For every $n\in\boldsymbol{Z}$, we can consider $V=\{V_l\}$, $V_l=W_l\otimes\boldsymbol{Q}_l(n)$. We have $d_V=[E:\boldsymbol{Q}]$. The field E acts on each V_l, the action commuting with that of $G_{\boldsymbol{Q}}$. Every prime p is ordinary at least if one broadens the definition by requiring only that a subgroup of finite index in $I_{\boldsymbol{Q}_p}$ act as described in (b) of (1). Let $\mathfrak{D}$ denote the ring of integers of E. Let $E_p=E\otimes\boldsymbol{Q}_p=\oplus_\pi E_\pi$, $\mathfrak{D}_p=\mathfrak{D}\otimes\boldsymbol{Z}_p=\oplus_\pi\mathfrak{D}_\pi$ be the the natural decompositions, where π runs over the places of E dividing p. Choose a lattice T_p in V_p which is a $\mathfrak{D}$-submodule and hence $\mathfrak{D}_p$-submodule. We

have decompositions $V_p = \oplus V_\pi$, where $V_\pi = V_p \otimes_{E_p} E_\pi$ and, if $A_p = V_p/T_p$, $A_p = \oplus A_\pi$ with $A_\pi = A_p \otimes_{\mathfrak{D}_p} \mathfrak{D}_\pi$. Each A_π is a $G_{\boldsymbol{Q}}$-module. The Selmer group also has a decomposition

$$S_{A_p}(\boldsymbol{Q}_\infty) = \bigoplus_\pi S_{A_\pi}(\boldsymbol{Q}_\infty), \tag{15}$$

where the Selmer groups for the A_π's are defined just as for A_p. (In general, if some V_p has a filtration satisfying (1), and if E is a field of $G_{\boldsymbol{Q}}$-endomorphisms of V_p, then $F^i V_p$ must be E-invariant so that one gets a filtration of each V_π and thus a decomposition (15).)

Now each $S_{A_\pi}(\boldsymbol{Q}_\infty)$ can be described as a Γ-module in terms of certain Galois groups in a way very much like (12) and (13). Again, results of Iwasawa imply Conjecture 1. Assume that $L_V(1)$ is a critical value. Let χ_π denote the $\boldsymbol{C}_p$-valued character obtained from χ by the embedding $E \to E_\pi \subseteq \boldsymbol{C}_p$. One can define a π-adic L-function $L_\pi(\varphi, V)$ essentially as a product of Kubota-Leopoldt p-adic L-functions for χ_π and its conjugates over $\boldsymbol{Q}_p$. As above, it will correspond to some $\theta_{V_\pi} = \lambda_{V_\pi} \kappa_{V_\pi}^{-1}$, where $\lambda_{V_\pi}, \kappa_{V_\pi} \in \Lambda$. The Mazur-Wiles theorem then states that $\hat{S}_{A_\pi}(\boldsymbol{Q}_\infty)$ has characteristic ideal (λ_{V_π}). In general, it would not be difficult to formulate Conjcture 2 for compatible systems of λ-adic representations, λ varying over the places of some fixed number field E. We should also say something about $p=2$. Iwasawa's conjecture still implies Conjecture 2 provided one defines the p-adic L-function $L_p(\varphi, V)$ by modifying the A_φ's by a factor of $(1/2)^{d_v}$ and provided one includes, as we have, the infinite places of $\boldsymbol{Q}_\infty$ in defining the Selmer group.

Finally we want to give a canonical definition of κ_V where V is any compatible system of l-adic representations such that $L_V(1)$ is critical. Denote by $V_p^{(i)}$ $(1 \leq i \leq t)$ the $G_{\boldsymbol{Q}}$-irreducible subquotients in a composition series for V_p. If for some i, the representation on $V_p^{(i)}$ factors through Γ, then one can show that $V_p^{(i)}$ is a π-component in a representation of the form described above for some character χ, for some $n \in \boldsymbol{Z}$, and for some π. The associated π-adic L-function will determine an element $\theta_{V^{(i)}} = \lambda_{V^{(i)}} \kappa_{V^{(i)}}^{-1}$, where in this case $\lambda_{V^{(i)}}$ is known to be an invertible element of Λ. (For $p=2$, this is true if one makes the appropriate modification.) We take $\lambda_{V^{(i)}} = 1$, which defines uniquely an element $\kappa_{V^{(i)}}$ of Λ. It is actually a generator for the characteristic ideal of the Pontryagin dual of $V_p^{(i)}/T_p^{(i)}$ as a Λ-module, where $T_p^{(i)}$ is a $G_{\boldsymbol{Q}}$-invariant lattice. For any i such that $(V_p^{(i)})^*$ gives a representation factoring through Γ, we get as above an element $\kappa_{(V^{(i)})^*}$, whose image under ι we define to be $\kappa_{V^{(i)}}$. For other i's, take $\kappa_{V^{(i)}} = 1$. Then $\kappa_V = \prod_{i=1}^t \kappa_{V^{(i)}}$ would seem to be a reasonable candidate for a denominator for the θ_V in (8). (Added in proof. We have realized recently that in order to have a conjecture which is preserved by

exact sequences of ordinary p-adic representations one should define κ_V so that it is a generator of the product of characteristic ideals of the Pontryagin duals of $(V_p/T_p)(\boldsymbol{Q}_\infty)$ and of $(V_p^*/T_p^*)^\iota(\boldsymbol{Q}_\infty)$. We intend to discuss this in detail in a subsequent paper.)

§ 2. Selmer groups for elliptic curves

Let E be an elliptic curve defined over $\boldsymbol{Q}$. The Hasse-Weil L-function $L_E(s)$ is actually $L_V(s)$, where $V=V(E)$ is the compatible system of l-adic representations for E. The classical Selmer group for E over $\boldsymbol{Q}_\infty$ is a torsion group whose p-primary subgroup $S_{p^\infty}(\boldsymbol{Q}_\infty, E)_{\text{class.}}$ is contained in $H^1(\boldsymbol{Q}_\infty, E_{p^\infty})$. It can be described just in terms of the Galois module E_{p^∞}. This is discussed in a much more general context in [1], and so we will be rather sketchy here. Assume that E has good, ordinary reduction at p. If $\bar{p}$ is a place of $\bar{\boldsymbol{Q}}$ over p, then one has the reduction map $E_{p^\infty}\to\bar{E}_{p^\infty}$ whose kernel we denote by $E^1_{p^\infty}$. (It depends on the choice of $\bar{p}$.) Both $E^1_{p^\infty}$ and $\bar{E}_{p^\infty}$ are isomorphic to $\boldsymbol{Q}_p/\boldsymbol{Z}_p$. The action of $G_{\boldsymbol{Q}_p}$ is unramified on $E_{p^\infty}/E^1_{p^\infty}$. One then gets a filtration $0\subset V_p^1\subset V_p$ where $I_{\boldsymbol{Q}_p}$ acts by χ_p^0 on V_p/V_p^1 and by χ_p^1 on V_p^1 (since the determinant is χ_p). Thus p is ordinary for V and $F^+V_p=V_p^1$, $F^+E_{p^\infty}=E^1_{p^\infty}$.

Now if F is any number field, the classical p^∞-Selmer group for E is defined by

$$S_{p^\infty}(F, E)=\ker\left(H^1(F, E_{p^\infty})\longrightarrow\prod_v H^1(F_v, E(\bar{F}_v))\right)$$

where v runs over all places of F. F_v denotes the union of the completions at v of finite extensions of $\boldsymbol{Q}$ contained in F. One can consider the map

$$H^1(F, E_{p^\infty})\longrightarrow\prod_v H^1(F_v, E_{p^\infty}).$$

To describe the p^∞-Selmer group, it is enough to determine for each v the kernel of the map

$$H^1(F_v, E_{p^\infty})\longrightarrow H^1(F_v, E(\bar{F}_v))_{p\text{-primary}} \tag{16}$$

If v lies over some prime $l\neq p$, then this map is an isomorphism as one can easily see by using Lutz's theorem that $E(\mathscr{F})$ is an l-adic Lie group for any finite extension $\mathscr{F}/\boldsymbol{Q}_l$. If v is an infinite place, (16) is also an isomorphism. For v lying over p, consider the Kummer sequence

$$0\longrightarrow E(F_v)\otimes\boldsymbol{Q}_p/\boldsymbol{Z}_p\xrightarrow{\kappa}H^1(F_v, E_{p^\infty})\longrightarrow H^1(F_v, E(\bar{F}_v))_{p\text{-primary}}\longrightarrow 0.$$

If $P\in E(F_v)$, then $P\otimes(a/p^n)$ gives the cocycle $\sigma: g\to g(Q)-Q$ for $g\in G_{F_v}$,

where $Q \in E(\bar{F}_v)$ is such that $p^n Q = aP$. If $g \in I_{F_v}$ (the inertia subgroup of G_{F_v}), then clearly $\sigma(g) \in E^1_{p^\infty}$. If F_v contains a ramified $\boldsymbol{Z}_p$-extension of $\boldsymbol{Q}_p$ (such as $(\boldsymbol{Q}_\infty)_{v_p}$) then it turns out that the image of κ (which is the kernel in (16)) is exactly the set of cocycles σ having the property that $\sigma|_{I_{F_v}}$ takes values in $E^1_{p^\infty}$, or equivalently (since I_{F_v} acts trivially on $E_{p^\infty}/E^1_{p^\infty}$) such that $\sigma|_{I_{F_v}}$ is in the kernel of the map

$$H^1(I_{F_v}, E_{p^\infty}) \longrightarrow H^1(I_{F_v}, E_{p^\infty}/E^1_{p^\infty}).$$

In particular, it follows that $S_{p^\infty}(\boldsymbol{Q}_\infty, E)_{\text{class.}}$ is precisely the group $S_{E_{p^\infty}}(\boldsymbol{Q}_\infty)$ attached to $E_{p^\infty} = V_p(E)/T_p(E)$ by (2), (3) and (4). In (4), one could equally well use the decomposition group D_v in place of I_v because of the fact that D_v/I_v acts nontrivially on $E_{p^\infty}/E^1_{p^\infty}$. (This is true since $\bar{E}_{p^\infty} \not\subseteq \bar{E}(\boldsymbol{Z}/p\boldsymbol{Z})$.) Hence $S_{E_{p^\infty}}(\boldsymbol{Q}_\infty)_{\text{strict}}$ and $S_{E_{p^\infty}}(\boldsymbol{Q}_\infty)$ are the same.

Now if E is a Weil curve, then Mazur and Swinnerton-Dyer construct a p-adic L-function for E, assuming E has good, ordinary reduction at p. Up to a factor, this has the properties (8), where one takes $A_{\varphi_0} = \Omega_E^{-1}(1-\alpha p^{-1})(1-\alpha p^{-1})$ and $A_\varphi = \Omega_E^{-1}\beta^{-n}\tau(\varphi^{-1})$, if φ has conductor p^n, $n>0$. Here $\tau(\varphi^{-1})$ is the Gaussian sum, α is the root of the Euler factor for p which has positive valuation for the fixed embedding $\bar{\boldsymbol{Q}} \to \boldsymbol{C}_p$, $\beta = p\alpha^{-1}$ is the unit root, and $\Omega_E = \int_{E(\boldsymbol{R})} \omega$, ω a Neron differential for E. Also $\theta_{V(E)}$ is in $p^{-t}\Lambda$ for some t, but it doesn't seem to be known that $\theta_{V(E)}$ itself belongs to Λ. A conjecture of Glenn Stevens implies this, at least when p is odd. (See [28].)

In [16], Mazur constructs a Γ-module which is closely related to the classical Selmer group. It should be pseudo-isomorphic to the Γ-module $\hat{S}_{p^\infty}(\boldsymbol{Q}_\infty, E)_{\text{class.}}$ and hence to $\hat{S}_{E_{p^\infty}}(\boldsymbol{Q}_\infty)$. Mazur conjectures that this module is Λ-torsion and that, for odd p, λ_V generates its characteristic ideal. The result of Rohrlich mentioned in the introduction shows that at least $\lambda_V \neq 0$. Also, if E has complex multiplication and $p>2$, Rubin [23] has recently proven that $\hat{S}_{p^\infty}(\boldsymbol{Q}_\infty, E)_{\text{class.}}$ is Λ-torsion and is annihilated by λ_V^2.

It is interesting to consider the case where E has multiplicative reduction at p. The Tate parametrization of $E(\bar{\boldsymbol{Q}}_p)$ allows one to describe the $G_{\boldsymbol{Q}_p}$-module E_{p^∞}. One can map μ_{p^∞} to a subgroup $E^1_{p^\infty}$ and the action of $G_{\boldsymbol{Q}_p}$ on $E_{p^\infty}/E^1_{p^\infty}$ will be unramified (through a character of order ≤ 2). We again get a filtration $0 \subseteq V_p^1 \subseteq V_p$ having the same properties as before and so p is ordinary for $V(E)$ with $F^+V_p = V_p^1$. The classical Selmer group $S_{p^\infty}(\boldsymbol{Q}_\infty, E)_{\text{class.}}$ coincides with $S_{E_{p^\infty}}(\boldsymbol{Q}_\infty)_{\text{strict}}$, but this is not always the same as $S_{E_{p^\infty}}(\boldsymbol{Q}_\infty)$. The definition of these groups gives an exact sequence.

$$(17) \qquad 0 \longrightarrow S_{E_{p^\infty}}(\boldsymbol{Q}_\infty)_{\text{strict}} \longrightarrow S_{E_{p^\infty}}(\boldsymbol{Q}_\infty) \xrightarrow{\rho} H^1(D_v/I_v, E_{p^\infty}/E^1_{p^\infty})$$

where $v=v_p$, $D_v=G_{(\boldsymbol{Q}_\infty)_v}$. The final term in (17) is nonzero only when D_v/I_v acts trivially on $E_{p^\infty}/E^1_{p^\infty}$, that is, when E has split multiplicative reduction at p. This term is then the Γ-module $\boldsymbol{Q}_p/\boldsymbol{Z}_p$ with trivial action of Γ. It will be clear later that, if $S_{E_{p^\infty}}(\boldsymbol{Q}_\infty)$ is Λ-cotorsion, the map ρ is actually surjective and the two Selmer groups will differ. If λ generates the characteristic ideal for $\hat{S}_{E_{p^\infty}}(\boldsymbol{Q}_\infty)$, then $\varphi_0(\lambda)=0$. The p-adic L-function for E constructed in [18] gives an Iwasawa function λ_E with this same property, even if $L_E(1)\neq 0$. In [13], Jones constructs a different Λ-module which also reflects the "extra zero". As he pointed out to us, the characteristic ideal of his module will be the same as that for $\hat{S}_{E_{p^\infty}}(\boldsymbol{Q}_\infty)$. However, the modules themselves are not pseudo-isomorphic in general.

If E has supersingular reduction at p, the situation seems completely mysterious at present. Assuming E is a Weil curve, there is a p-adic L-function attached to E, but it isn't of the form 8 (*b*). It is not at all clear how to relate it to the Selmer groups for E in the tower of subfields of $\boldsymbol{Q}_\infty$.

§ 3. Local Galois cohomology groups

Let K be a finite extension of $\boldsymbol{Q}_p$ and let K_∞ be some $\boldsymbol{Z}_p$-extension of K. We will consider a G_K-module A which is isomorphic to $(\boldsymbol{Q}_p/\boldsymbol{Z}_p)^d$ as a group. $H^1(K_\infty, A)$ is a discrete Γ-module (where $\Gamma=\mathrm{Gal}(K_\infty/K)$) and hence a Λ-module. We will prove the following result about its structure.

Proposition 1. *$H^1(K_\infty, A)\sim \hat{\Lambda}^r\oplus A^*(K_\infty)^\iota$ as Λ-modules, where $r=[K\colon \boldsymbol{Q}_p]d$.*

Here $A^*=\mathrm{Hom}_{\boldsymbol{Z}_p}(T_A, \mu_{p^\infty})$, where T_A denotes the Tate module for A. Also, for any field $\mathscr{K}$ and any $G_{\mathscr{K}}$-module M, we use the notation $M(\mathscr{K})$ for $H^0(G_{\mathscr{K}}, M)=M^{G_{\mathscr{K}}}$. Later, we will also write $\mathscr{K}(M)$ for the extension of $\mathscr{K}$ fixed by the kernel of the action of $G_{\mathscr{K}}$ on M.

Our proof relies on the following observation. Let S be a discrete Γ-module which is a p-primary abelian group. Let $X=\hat{S}=\mathrm{Hom}_{\boldsymbol{Z}_p}(S, \boldsymbol{Q}_p/\boldsymbol{Z}_p)$, which will be a compact Λ-module. S will be cofinitely generated over Λ if and only if S^Γ is cofinitely generated over $\boldsymbol{Z}_p$. We assume this is the case. Let $Y=\Lambda/(f)$, where $f=f_0^a$, f_0 an irreducible element of Λ, $a\geq 1$. We assume $(f_0)\neq(p)$ so that Y is a free $\boldsymbol{Z}_p$-module of rank $\deg(f)=a\deg(f_0)$, which is just the degree of the first unit term if one applies an isomorphism $\Lambda\to\boldsymbol{Z}_p[[T]]$. All the tensor products that appear here and later in this paper are over $\boldsymbol{Z}_p$. Then $S\otimes Y=\mathrm{Hom}_{\mathrm{cont}}(X, \boldsymbol{Q}_p/\boldsymbol{Z}_p)\otimes Y=\mathrm{Hom}_{\mathrm{cont}}(X, (\boldsymbol{Q}_p/\boldsymbol{Z}_p)\otimes Y)$. One sees that $(S\otimes Y)^\Gamma=\mathrm{Hom}_\Lambda(X, (\boldsymbol{Q}_p/\boldsymbol{Z}_p)\otimes Y)$. (Since X is finitely generated over Λ, Λ-homomorphisms will be continuous.) The $\boldsymbol{Z}_p$-corank will be the $\boldsymbol{Z}_p$-rank of the Tate module of this last group which is $\mathrm{Hom}_\Lambda(X, Y)$. If $X=\Lambda$, this rank will be $\deg(f)$. If $X=\Lambda/(g)$.

where $g=g_0^b$, g_0 irreducible and not divisible by p, then $\mathrm{Hom}_\Lambda(X, Y)$ has $\boldsymbol{Z}_p$-rank 0 unless $(f_0)=(g_0)$. In this last case, the $\boldsymbol{Z}_p$-rank is $(\min(a, b))$ $\times \deg(f_0)$. If X is a finitely generated as a Λ-module and if $p \notin \mathrm{Supp}(X)$, then X is pseudo-isomorphic to a sum $\Lambda^r \oplus \sum_{i=1}^t \Lambda/(g_i)$, where the g_i's are powers of irreducibles as above. The value of r and the ideals (g_i) that occur are clearly determined if one knows the $\boldsymbol{Z}_p$-corank of $(S\otimes Y)^\Gamma$ for all Y of the above type. If $p \in \mathrm{Supp}(X)$, this information would determine $X/X_{\boldsymbol{Z}_p\text{-torsion}}$ and hence the maximal divisible subgroup S_{div} as Λ-modules, up to pseudo-isomorphism.

Let $S=H^1(K_\infty, A)$. For any Y as above, let $B=A\otimes Y$ so that $B\cong (\boldsymbol{Q}_p/\boldsymbol{Z}_p)^{d_B}$, where $d_B=\deg(f)d_A$, $d_A=d$. As a Γ-module, $S\otimes Y=H^1(K_\infty, A)\otimes Y\cong H^1(K_\infty, B)$ as one sees from the definition of the action of Γ on cocycles. Let $S_B=H^1(K_\infty, B)$. We have the inflation-restriction exact sequence

$$(18)\qquad 0\longrightarrow H^1(\Gamma, B(K_\infty))\longrightarrow H^1(K, B)\longrightarrow H^1(K_\infty, B)^\Gamma\longrightarrow 0$$

where the final 0 is because $H^2(\Gamma, B(K_\infty))=0$. ($\Gamma\cong \boldsymbol{Z}_p$.) Now $B=\cup_n B_n$, $B_n=\{b\in B \mid p^n b=0\}$. The exact sequence $0\to B_n\to B\xrightarrow{p^n} B\to 0$ gives us another exact sequence

$$(19)\qquad 0\longrightarrow B(K)/p^nB(K)\longrightarrow H^1(K, B_n)\longrightarrow H^1(K, B)_{p^n}\longrightarrow 0$$

where the subscript p^n denotes the kernel of multiplication by p^n. Since $H^1(K, B_n)$ is finite, (19) shows that $H^1(K, B)$ has only finitely many elements of order p and must have finite $\boldsymbol{Z}_p$-corank. Thus the same is true for S_B^Γ (by (18)) and therefore S_B is cofinitely generated over Λ. It is known that G_{K_∞} has p-cohomological dimension 1. (This is a consequence of the fact that the p-primary subgroup of the Brauer group of K_∞ is trivial. See Serre [27].) Thus the map $H^1(K_\infty, B)\xrightarrow{p^n} H^1(K_\infty, B)$ is surjective since $H^2(G_{K_\infty}, B_n)=0$. It follows that S is divisible and $\hat{S}$ has μ-invariant equal to 0.

We calculate the $\boldsymbol{Z}_p$-corank of $H^1(K, B)$ by using Tate's calculation of Euler-Poincaré characteristics. If M is a G_K-module of order p^m, then

$$(20)\qquad \chi(M)=\prod_{i=0}^{2} |H^i(K, M)|^{(-1)^i}=p^{-m[K:\boldsymbol{Q}_p]}.$$

Also, $H^2(K, M)$ is dual to $H^0(K, M^*)$, where $M^*=\mathrm{Hom}(M, \mu_{p^\infty})$. Therefore,

$$(21)\qquad |H^1(K, M)|=p^{m[K:\boldsymbol{Q}_p]}\,|H^0(K, M)|\cdot|H^0(K, M^*)|.$$

Now $B(K)\cong(\boldsymbol{Q}_p/\boldsymbol{Z}_p)^b\oplus$ (a finite group) and $B(K^*)\cong(\boldsymbol{Q}_p/\boldsymbol{Z}_p)^{b^*}\oplus$ (a finite

group), for some $b, b^* \geq 0$. Taking $M=B_n$ (which has order $p^{d_B n}$), (21) gives

$$|H^1(K, B_n)| = p^{cn+O(1)}, \qquad c=d_B[K: Q_p]+b+b^*. \tag{22}$$

Since the order of $B(K)/p^n B(K)$ is bounded as $n\to\infty$, (19) and (22) show that

$$H^1(K, B) \cong (\boldsymbol{Q}_p/\boldsymbol{Z}_p)^c \oplus (\text{a finite group}). \tag{23}$$

But $H^1(\Gamma, B(K_\infty))$ has $\boldsymbol{Z}_p$-corank equal to b and so, by (18),

$$\operatorname{corank}_{\boldsymbol{Z}_p}(S_B^\Gamma) = d_B[K: Q_p]+b^* = r \deg(f)+b^*.$$

Let S' be the Λ-module on the right side in Proposition 1. Then $(S'\otimes Y)^\Gamma$ has $\boldsymbol{Z}_p$-corank equal to $r\deg(f)+\operatorname{corank}_{\boldsymbol{Z}_p}((A^*(K_\infty)^\iota\otimes Y)^\Gamma)$. It is enough to prove that this last term is b^*, which is just an exercise in linear algebra. Letting $V_A = T_A\otimes\boldsymbol{Q}_p$, $V_B = T_B\otimes\boldsymbol{Q}_p$, $V_Y = Y\otimes\boldsymbol{Q}_p$, we have an isomorphism of G_K-modules

$$V_B^* = \operatorname{Hom}_{\boldsymbol{Q}_p}(V_A\otimes V_Y, \boldsymbol{Q}_p(1)) \cong \operatorname{Hom}_{\boldsymbol{Q}_p}(V_A, \boldsymbol{Q}_p(1))\otimes V_{Y^\iota} \cong V_{A^*}\otimes V_{Y^\iota}.$$

The dimension of the G_K-invariant subspace of V_B^* is b^*. For $V_{A^*}\otimes V_{Y^\iota}$, it is (first taking G_{K_∞}-invariants)

$$\operatorname{corank}_{\boldsymbol{Z}_p}((A^*(K_\infty)\otimes Y^\iota)^\Gamma) = \operatorname{corank}_{\boldsymbol{Z}_p}((A^*(K_\infty)^\iota\otimes Y)^\Gamma).$$

Proposition 1 follows.

Corollary 1. *If $A^*(K_\infty)$ is finite, then $X=\hat{H}^1(K_\infty, A)$ is isomorphic to a Λ-submodule of Λ^r of finite index. The quotient Λ^r/X is isomorphic to a Λ-submodule of $A^*(K_\infty)$.*

Proof. $S=H^1(K_\infty, A)$ is divisible and so X has no $\boldsymbol{Z}_p$-torsion. The finiteness of $A^*(K_\infty)$ shows that X has no Λ-torsion. Thus, the structure theory of Λ-modules implies that $X\subseteq\Lambda^r$. Let $Z=\Lambda^r/X$. Let $\Gamma_n=\Gamma^{p^n}$, K_n = the fixed field for Γ_n. If $n\gg 0$, Γ_n will act trivially on Z. It follows easily that Z is isomorphic to the $\boldsymbol{Z}_p$-torsion subgroup of $X/(\gamma_0^{p^n}-1)X$ (as a Γ/Γ_n-module). Thus $T_n = S^{\Gamma_n}/(S^{\Gamma_n})_{\text{div}}$ is isomorphic to $\hat{Z}$ for large n. We use the exact sequence (18) with Γ replaced by Γ_n, B replaced by A. This shows that T_n is a homomorphic image of $H^1(K_n, A)/H^1(K_n, A)_{\text{div}}$. For any $m\geq 0$, we have the exact sequence

$$H^1(K_n, A) \xrightarrow{p^m} H^1(K_n, A) \longrightarrow H^2(K_n, A_m) \longrightarrow H^2(K_n, A)_{p^m} \longrightarrow 0. \tag{24}$$

Since $A^*(K_\infty)$ is finite, the order of $H^0(K_n, A_m^*)$ and hence of $H^2(K_n, A_m)$ is

bounded as $m \to \infty$. Hence $H^2(K_n, A)$ is finite. But G_{K_n} has p-cohomological dimension 2 and so $H^3(K_n, A_m)=0$, which implies that $H^2(K_n, A)$ must be divisible. It follows that $H^2(K_n, A)=0$. Thus, using (24), one sees that T_n is a homomorphic image of $H^2(K_n, A_m)$ for $m \gg 0$ and therefore Z is isomorphic to a subgroup of $A_m^*(K_n) \subseteq A^*(K_\infty)$. All of the maps are Γ/Γ_n and hence Γ-homomorphisms.

Corollary 2. *If $A^*(K_\infty)=0$, then $\hat{H}^1(K_\infty, A)$ is a free Λ-module of rank $d[K: \boldsymbol{Q}_p]$.*

Now let K be a finite extension of $\boldsymbol{Q}_l$, $l \neq p$. There is just one $\boldsymbol{Z}_p$-extension of K—the cyclotomic $\boldsymbol{Z}_p$-extension K_∞ which is in fact unramified over K. The above arguments still apply except that now, if M is a G_K-module which is finite of p-power order, the Euler-Poincaré characteristic is 1. We get the following result.

Proposition 2. *$H^1(K_\infty, A) \sim A^*(K_\infty)^\iota$ as Λ-modules. If $A^*(K_\infty)$ is finite, then $H^1(K_\infty, A)=0$.*

One should compare the preceding results with Theorem 25 of [12] which deals with the special case $A=\boldsymbol{Q}_p/\boldsymbol{Z}_p$ with G_K acting trivially, but is more precise.

In the proof of Theorem 2, we will need the following properties of Tate's local duality. Let M be a finite G_K-module of order p^m, where K is a finite extension of $\boldsymbol{Q}_p$. Tate proves there is a perfect pairing

$$H^1(K, M) \times H^1(K, M^*) \longrightarrow \boldsymbol{Q}_p/\boldsymbol{Z}_p. \tag{25}$$

Let N be a G_K-submodule of M, $N^\perp$ its orthogonal complement in M^*. The injective map $N \xrightarrow{a} M$ induces a surjective map $M^* \xrightarrow{b} N^* = M^*/N^\perp$. The maps a and b induce maps

$$\alpha: H^1(K, N) \longrightarrow H^1(K, M) \quad \text{and} \quad \beta: H^1(K, M^*) \longrightarrow H^1(K, N^*)$$

which are adjoint. Thus $\mathrm{Im}(\alpha)$ and $\ker(\beta)$ are orthogonal complements for the pairing (25). Also $\ker(\beta)$ is the image of the map $H^1(K, N^\perp) \to H^1(K, M^*)$ induced from the inclusion $N^\perp \to M^*$. These remarks will be useful to us in the following case. Suppose V_p is a representation space over $\boldsymbol{Q}_p$ for G_K which is ordinary in the sense described in (1), where one replaces $G_{\boldsymbol{Q}_p}$, $I_{\boldsymbol{Q}_p}$ by G_K, I_K. Then so is V_p^*. F^+V_p and $F^+V_p^*$ are orthogonal complements under the pairing $V_p \times V_p^* \to \boldsymbol{Q}_p(1)$. Letting $A=V_p/T_p$, $A^*=V_p^*/T_p^*$, A_n, and A_n^* be as before, we define F^+A, F^+A_n, F^+A^*, $F^+A_n^*$ in the obvious way. Then $(F^+A_n)^\perp = F^+A_n^*$ under $A_n \times A_n^* \to \mu_{p^n}$. We define $F^+H^1(K, A_n)$ to be the image of $H^1(K, F^+A_n)$ in $H^1(K, A_n)$ and

similarly define $F^+H^1(K, A_n^*)$. Then $F^+H^1(K, A_n)$ and $F^+H^1(K, A_n^*)$ are orthogonal complements under the pairing (25) for $M=A_n$.

Let K now be a finite extension of $\boldsymbol{Q}_l$, $l \neq p$. We still have a pairing (25). Let $H^1_{\text{unr.}}(K, M)$ denote the kernel of the restriction map $H^1(G_K, M) \to H^1(I_K, M)$, which is also the image under inflation of $H^1(G_K/I_K, M^{I_K})$. Then $H^1_{\text{unr.}}(K, M)$ and $H^1_{\text{unr.}}(K, M^*)$ are orthogonal complements under (25). This is proved in [27] under the assumption that I_K acts trivially on M. But the same proof works without this assumption.

§ 4. Global Galois cohomology groups

Let K now be a finite extension of $\boldsymbol{Q}$. Let K_∞ be any $\boldsymbol{Z}_p$-extension of K. Let V_p be a representation space over $\boldsymbol{Q}_p$ for G_K of dimension d, T_p a G_K-invariant lattice, and $A=V_p/T_p \cong (\boldsymbol{Q}_p/\boldsymbol{Z}_p)^d$. Let $\text{Ram}(V_p)$ denote the set of places of K which are ramified in $K(A)/K$. We assume $\text{Ram}(V_p)$ is finite. Let Σ be a finite set of places of K containing $\text{Ram}(V_p)$, all places over p, and all infinite places. Let K_Σ denote the maximal extension of K unramified outside Σ. Thus A is a $\text{Gal}(K_\Sigma/K)$-module. Now $K_\infty \subseteq K_\Sigma$ since only places over p can be ramified in K_∞/K. We will study the structure of the discrete Γ-modules $H^1(K_\Sigma/K_\infty, A)$ and $H^2(K_\Sigma/K_\infty, A)$. For each real place v of K, let $d_v^\pm$ be the dimension of the ± 1 eigenspace for a complex conjugation above v acting on V_p. Define

$$\delta(K, V_p) = \sum_{v \text{ complex}} d + \sum_{v \text{ real}} d_v^- . \tag{26}$$

Our first result is the following

Proposition 3. *The Λ-modules $H^1(K_\Sigma/K_\infty, A)$ and $H^2(K_\Sigma/K_\infty, A)$ are cofinitely generated. We have*

$$\text{corank}_\Lambda(H^1(K_\Sigma/K_\infty, A)) - \text{corank}_\Lambda(H^2(K_\Sigma/K_\infty, A)) = \delta(K, V_p).$$

Note that $H^0(K_\Sigma/K_\infty, A) = A(K_\infty)$ and so has Λ-corank zero. We owe to P. Schneider the suggestion to study these Λ-coranks by means of their Euler-Poincaré characteristic. Write $A = \bigcup_n A_n$ as before. The groups $H^i(K_\Sigma/K, A_n)$ are finite for $0 \leq i \leq 2$ of order $|H_n^i|$, say. Tate has calculated the Euler-Poincaré characteristic $\chi_n = \prod_{i=0}^2 |H_n^i|^{(-1)^i}$, which turns to out be given by

$$\begin{aligned} \chi_n &= \prod_{v \text{ complex}} |A_n|^{-1} \prod_{v \text{ real}} |A_n/A_n(K_v)|^{-1} \\ &= p^{-\delta n + e}, \quad \text{where} \quad \delta = \delta(K, V_p). \end{aligned} \tag{27}$$

The quantity e is zero unless $p=2$ and is then at least independent of n for $n \geq 1$. Actually e becomes quite relevant when examining the finer

structure of our Selmer groups for $p=2$.

We denote $H^i(K_\Sigma/K, A)$ and $H^i(K_\Sigma/K, A_n)$ more briefly by $H^i(A)$, $H^i(A_n)$. For $i=1, 2$, we have the exact sequences:

$$0\longrightarrow H^{i-1}(A)/p^nH^{i-1}(A)\longrightarrow H^i(A_n)\longrightarrow H^i(A)_{p^n}\longrightarrow 0. \tag{28}$$

We see that $H^i(A)$ is cofinitely generated over $\boldsymbol{Z}_p$ for $0\leq i\leq 2$ with $\boldsymbol{Z}_p$-corank c_i, say. Hence $H^{i-1}(A)/p^nH^{i-1}(A)$ has bounded order as $n\to\infty$. It follows from (27) and (28) that

$$c_0-c_1+c_2=-\delta. \tag{29}$$

We also have the Hochschild-Serre spectral sequences [10]:

$$0\longrightarrow H^1(\Gamma, A(K_\infty))\longrightarrow H^1(K_\Sigma/K, A)\longrightarrow H^1(K_\Sigma/K_\infty, A)^\Gamma\longrightarrow 0 \tag{30}$$

$$0\longrightarrow H^1(\Gamma, H^1(K_\Sigma/K_\infty, A))\longrightarrow H^2(K_\Sigma/K, A)\longrightarrow H^2(K_\Sigma/K_\infty, A)^\Gamma \longrightarrow 0 \tag{31}$$

which result from the fact that Γ has cohomological dimension 1. The fact that $H^1(K_\Sigma/K_\infty, A)$ and $H^2(K_\Sigma/K_\infty, A)$ are cofinitely generated as Λ-modules follows from (30), (31).

Let $Y_u=\Lambda/(\gamma_0-u)$, where γ_0 is a topological generator of Γ and u is any principal unit in $\boldsymbol{Z}_p$. If S is a discrete Λ-module of Λ-corank s, then $(S\otimes Y_u)^\Gamma$ will have $\boldsymbol{Z}_p$-corank s for all but finitely many u's. The exceptional u's are those such that $(\gamma_0-u)\in \mathrm{Supp}\,(\hat{S})$. Now, as Λ-modules, $H^i(K_\Sigma/K_\infty, A)\otimes Y_u\cong H^i(K_\Sigma/K_\infty, A\otimes Y_u)$ for $0\leq i\leq 2$. The cohomology groups $H^1(\Gamma, A(K_\infty)\otimes Y_u)$ and $H^1(\Gamma, H^1(K_\Sigma/K_\infty, A\otimes Y_u))$ are finite for all but finitely many u's. If we replace A by $A\otimes Y_u$, then we will have the quantities $c_i=c_i(u)$ which satisfy $c_0(u)-c_1(u)+c_2(u)=-\delta$ by (29). For u outside some finite set, $c_0(u)=0$, $c_1(u)=\mathrm{corank}_\Lambda(H^1(K_\Sigma/K_\infty, A))$ and $c_2(u)=\mathrm{corank}_\Lambda(H^2(K_\Sigma/K_\infty, A))$. This gives Proposition 3.

If $p\neq 2$, then $\mathrm{Gal}\,(K_\Sigma/K)$ has p-cohomological dimension 2. In particular, $H^3(K_\Sigma/K, A_n\otimes Y_u)=0$ which implies that $H^2(K_\Sigma/K, A\otimes \mathbf{Y}_u)$ is divisible. Hence, by (31), $H^2(K_\Sigma/K_\infty, A\otimes Y_u)^\Gamma$ is also divisible. Letting $S=H^2(K_\Sigma/K_\infty, A)$, we have that $(S\otimes Y_u)^\Gamma$ is divisible and hence $\hat{S}/(\gamma_0-u)\hat{S}$ is $\boldsymbol{Z}_p$-torsion-free for all u. This easily implies that $\hat{S}$ is a free Λ-module.

Proposition 4. *If p is* odd, *then $H^2(K_\Sigma/K_\infty, A)$ is a cofree Λ-module.*

Consider $A=\boldsymbol{Q}_p/\boldsymbol{Z}_p$ with G_K acting trivially. Then $\delta=r_2$, the number of complex places of K. Let M_Σ denote the maximal abelian pro-p extension of K_∞ contained in K_Σ. Then $H^1(K_\Sigma/K_\infty, A)=\mathrm{Hom}_{\mathrm{cont}}(X_\Sigma, \boldsymbol{Q}_p/\boldsymbol{Z}_p)$, where $X_\Sigma=\mathrm{Gal}\,(M_\Sigma/K_\infty)$. The assertion that $\mathrm{rank}_\Lambda(X_\Sigma)=r_2$ is easily seen to be equivalent to the weak Leopoldt conjecture for K_∞/K, which states

that $\mathrm{rank}_{\boldsymbol{Z}}(E_{K_n})-\mathrm{rank}_{\boldsymbol{Z}_p}(\bar{E}_{K_n})$ is bounded as $n\to\infty$. Here K_n is the n-th layer in K_∞/K, E_{K_n} the unit group, and $\bar{E}_{K_n}$ its topological closure in $\prod_{v|p}(K_n)_v^\times$. It is true if K_∞/K is the cyclotomic $\boldsymbol{Z}_p$-extension—a result of Iwasawa in this case. For $A=\mu_{p^\infty}$, we have $\delta=r_1+r_2=$the number of infinite places of K. Proposition 3 gives $\mathrm{corank}_\Lambda(H^1(K_\Sigma/K_\infty, A))\geq r_1+r_2$, but equality does not necessarily hold and so $\mathrm{corank}_\Lambda(H^2(K_\Sigma/K_\infty, A))$ can be positive. This happens if Σ contains finite places which are completely decomposed in K_∞/K. Then, the rank of the group of Σ-units of K_n will grow more rapidly then $\mathrm{rank}_{\boldsymbol{Z}}(E_{K_n})$. If $\alpha\in K_\infty^\times$ is any Σ-unit, one gets cocycles $g\to(\sqrt[p^n]{\alpha})^{g-1}$ in $H^1(K_\Sigma/K_\infty, \mu_{p^\infty})$, which is then easily seen to have Λ-corank$>r_1+r_2$. However this also cannot happen if K_∞/K is the cyclotomic $\boldsymbol{Z}_p$-extension. It seems reasonable to make the following conjecture.

Conjecture 3. *Let K_∞/K be the cyclotomic $\boldsymbol{Z}_p$-extension, p an odd prime. Then $H^2(K_\Sigma/K_\infty, A)=0$.*

For $p=2$, one would conjecture at least that the Λ-corank is 0. These conjectures would be consequences of Iwasawa's well-known conjecture that the μ-invariant of a cyclotomic $\boldsymbol{Z}_p$-extension vanishes. Knowing this for K'_∞/K', where $K'=K(A_1)(\mu_p)$ (or $K(A_1)(\mu_4)$ if $p=2$) and $K'_\infty=K'K_\infty$ would be sufficient, as one can verify by using results in [10] and [32].

Assume that $H^2(K_\Sigma/K_\infty, A)=0$. Then (31) shows that

$$H^1(\Gamma, H^1(K_\Sigma/K_\infty, A))\cong H^2(K_\Sigma/K, A). \tag{32}$$

Let $S=H^1(K_\Sigma/K_\infty, A)$. If p is odd, (32) implies that $H^1(\Gamma, S)=S/(\gamma_0-1)S$ is divisible and hence that $\hat{S}^\Gamma$ has no $\boldsymbol{Z}_p$-torsion. It follows that S has no nontrivial finite Λ-submodules. We get the following proposition (which was suggested to us by the arguments and results in Wingberg [32]):

Proposition 5. *Assume that p is odd and that $H^2(K_\Sigma/K_\infty, A)=0$. Then $\hat{H}^1(K_\Sigma/K_\infty, A)$ has no nontrivial finite Λ-submodules.*

(32) also allows one to study the Λ-torsion submodule of $\hat{H}^1(K_\Sigma/K_\infty, A)$. It can be rather nontrivial. Still assuming the vanishing of the H^2, one can produce quotients of $H^1(K_\Sigma/K_\infty, A)$ which are Λ-cotorsion modules of the form occurring in Propositions 1 and 2. We will not go into this here though.

§ 5. Generalized Selmer groups

We continue making the assumptions at the beginning of Section 4. For every place $\bar{\pi}$ of $\bar{\boldsymbol{Q}}$ over p, let $W_{\bar{\pi}}$ be a subspace of V_p. We assume

that $W_{g(\bar{\pi})}=g(W_{\bar{\pi}})$ for all $g \in G_K$. In particular, $W_{\bar{\pi}}$ is invariant under the action of the decomposition group $D_{\bar{\pi}}$ for $\bar{\pi}$ in G_K. We let $C_{\bar{\pi}}$ denote the image of $W_{\bar{\pi}}$ in $A=V_p/T_p$. For any field K', $K \subseteq K' \subseteq \bar{\boldsymbol{Q}}$, define

$$S_A(K', \{C_{\bar{\pi}}\})=\{\sigma \in H^1(K', A) \mid \sigma \text{ locally trivial at all places of } K'\}. \tag{32}$$

Here we say σ is locally trivial at a place v of K' if $\sigma \in \ker(H^1(K', A) \to H^1(I_{\bar{v}}, A))$ for $v \nmid p$, and if $\sigma \in \ker(H^1(K', A) \to H^1(I_{\bar{\pi}}, A/C_{\bar{\pi}}))$ for $v=\pi$, a place of K' lying over p. In these conditions, we pick a place $\bar{v}$ (or $\bar{\pi}$) of $\bar{\boldsymbol{Q}}$ lying over v. $I_{\bar{v}}$ (or $I_{\bar{\pi}}$) denotes the inertia subgroup for that place. The definition is independent of the choice of places of $\bar{\boldsymbol{Q}}$. We also define a strict version $S_A^{\text{str.}}(K', \{C_{\bar{\pi}}\})$ using the decomposition group $D_{\bar{\pi}}$ instead of $I_{\bar{\pi}}$. Also, if K'/K is Galois, then $\mathrm{Gal}(K'/K)$ acts on $S_A(K', \{C_{\bar{\pi}}\})$ by inner automorphisms.

Now let $K'=K_\infty$, a $\boldsymbol{Z}_p$-extension of K. We will assume that every finite place of Σ is finitely decomposed in K_∞/K. This would be true if K_∞ is the cyclotomic $\boldsymbol{Z}_p$-extension of K which is the case that primarily interests us. Let Σ_∞ denote the places of K_∞ lying above those of Σ. Put $\varepsilon=\varepsilon(K, V_p, \{C_{\bar{\pi}}\})=\sum_\pi [K_\pi : \boldsymbol{Q}_p] \operatorname{codim}(C_{\bar{\pi}})$, where the sum is over the places π of K dividing p and $\operatorname{codim}(C_{\bar{\pi}})=\dim_{\boldsymbol{Q}_p}(V_p/W_{\bar{\pi}})$, $\bar{\pi}$ any place of $\bar{\boldsymbol{Q}}$ over π. Let $\delta=\delta(K, V_p)$. The "Selmer group" $S_A(K_\infty, \{C_{\bar{\pi}}\})$ can be regarded as a discrete Λ-module.

Proposition 6. *$S_A(K_\infty, \{C_{\bar{\pi}}\})$ is cofinitely generated as a Λ-module. Its Λ-corank is at least $\delta-\varepsilon$.*

Proof. Suppose v is a place of K_∞ not in Σ_∞. Then $I_{\bar{v}}$ acts trivially on V_p and so $H^1(I_{\bar{v}}, A)=\mathrm{Hom}(I_{\bar{v}}, A)$. A cocycle $\sigma \in H^1(K_\infty, A)$ is locally trivial at v if and only if $\sigma|_{I_{\bar{v}}}$ is identically zero. This would then be true for all $\bar{v}$ over v. It follows that σ is locally trivial at all such v precisely when $\sigma \in H^1(K_\Sigma/K_\infty, A)$. Thus $S_A(K_\infty, \{C_{\bar{\pi}}\}) \subseteq H^1(K_\Sigma/K_\infty, A)$, which already proves that the Selmer group is cofinitely generated over Λ. We have the following exact sequence:

$$0 \longrightarrow S_A(K_\infty, \{C_{\bar{\pi}}\}) \longrightarrow H^1(K_\Sigma/K_\infty, A) \longrightarrow H^{1,\text{inert.}}_\Sigma \tag{33}$$

where we define $H_\Sigma=\coprod_{v \nmid p} H^1((K_\infty)_v, A) \oplus \coprod_{v|p} H^1((K_\infty)_v, A/C_{\bar{v}})$ and $H^{1,\text{inert.}}_\Sigma$ is the image of H_Σ under the restriction maps to $\coprod_{v \nmid p} H^1(I_{\bar{v}}, A) \oplus \coprod_{v|p} H^1(I_{\bar{v}}, A/C_{\bar{v}})$. The sums here are over the places v in Σ_∞. Since Γ permutes the elements of Σ_∞, both H_Σ and $H^{1,\text{inert.}}_\Sigma$ are Γ-modules. The contribution to $H^{1,\text{inert.}}_\Sigma$ coming from the infinite places is of exponent 2 and so is Λ-cotorsion. Proposition 2 shows that the contribution from the finitely many places $v \in \Sigma_\infty$ not over p has finite $\boldsymbol{Z}_p$-corank and also is Λ-cotorsion.

Now fix a place π of K dividing p. Let Γ_π denote the decomposition group for the places v of K_∞ over π, $\Gamma_\pi \subseteq \Gamma$. For any such place v, $H^1((K_\infty)_v, A/C_{\bar{v}})$ is a Γ_π-module whose Λ_π-corank is $[K_\pi: \boldsymbol{Q}_p]$ codim $(C_{\bar{\pi}})$. Here $\bar{v}=\bar{\pi}$, $A/C_{\bar{\pi}} \cong (\boldsymbol{Q}_p/\boldsymbol{Z}_p)^c$, where $c=$codim $(C_{\bar{\pi}})$, $\Lambda_{\bar{\pi}}$ is the Iwasawa algebra for $\Gamma_\pi = \mathrm{Gal}((K_\infty)_v/K_\pi)$. The assertion about the above Λ_π-corank is a consequence of Proposition 1. The image of $H^1((K_\infty)_v, A/C_{\bar{v}})$ in $H^{\text{inert.}}_\Sigma$ has the same Λ_π-corank because the kernel of the restriction map is easily seen to be Λ_π-cotorsion. There are $[\Gamma: \Gamma_\pi]$ such places v. Their contribution to $H^{\text{inert.}}_\Sigma$ will have Λ-corank also equal to $[K_\pi: \boldsymbol{Q}_p]$ codim $(C_{\bar{\pi}})$. It follows that $H^{\text{inert.}}_\Sigma$ has Λ-corank ε. Proposition 6 then follows from Proposition 3.

Let $V_p^{\text{ind.}}$ denote the representation of $G_{\boldsymbol{Q}}$ induced from V_p. Thus $\dim_{\boldsymbol{Q}_p}(V_p^{\text{ind.}}) = d[K: \boldsymbol{Q}]$. Only finitely many primes will be ramified in $V_p^{\text{ind.}}$. Let $v_1, v_2, \cdots, v_t$ be the places of K lying above some fixed place q of $\boldsymbol{Q}$. Let $\bar{v}_1, \bar{v}_2, \cdots, \bar{v}_t$ be places of $\bar{\boldsymbol{Q}}$ above each v_i. Denote by $D_{\bar{v}_i}(\boldsymbol{Q})$ and $D_{\bar{v}_i}(K)$ the decomposition groups for $\bar{v}_i$ in $G_{\boldsymbol{Q}}$ and G_K, respectively. The index $[D_{\bar{v}_i}(\boldsymbol{Q}): D_{\bar{v}_i}(K)]$ is the local degree $[K_{v_i}: \boldsymbol{Q}_q]$. Put $\bar{v}=\bar{v}_1$ and choose $g_i \in G_{\boldsymbol{Q}}$, $1 \leq i \leq t$, such that $g_i(\bar{v})=\bar{v}_i$. Then $D_{\bar{v}_i}(\boldsymbol{Q}) = g_i D_{\bar{v}}(\boldsymbol{Q}) g_i^{-1}$. Let U_i denote the representation of $D_{\bar{v}_i}(\boldsymbol{Q})$ induced from the representation V_p of $D_{\bar{v}_i}(K)$. We then get a representation U_i' of $D_{\bar{v}}(\boldsymbol{Q})$ by conjugation with g_i. Now $D_{\bar{v}}(\boldsymbol{Q})$ acts on the coset space $G_{\boldsymbol{Q}}/G_K$ as permutations with t orbits, represented by g_i^{-1}, $1 \leq i \leq t$, each having length $[K_{v_i}: \boldsymbol{Q}_q]$. One finds that, as representation spaces for $D_{\bar{v}}(\boldsymbol{Q})$, $V_p^{\text{ind.}} \cong \oplus_{i=1}^t U_i'$. If $q=\infty$, these remarks show that

$$\delta(K, V_p) = \dim_{\boldsymbol{Q}_p}((V_p^{\text{ind.}})^-) = \delta(\boldsymbol{Q}, V_p^{\text{ind.}}). \tag{34}$$

If $q=p$, we can define a subspace $W_{\bar{p}}^{\text{ind.}}$ (we write $\bar{p}$ for $\bar{v}$) of $V_p^{\text{ind.}}$ invariant under $D_{\bar{p}}(\boldsymbol{Q})$ as follows. In U_i, one has the $D_{\bar{v}_i}(\boldsymbol{Q})$-invariant subspace Ind $(W_{\bar{v}_i})$, which has codimension $[K_{v_i}: \boldsymbol{Q}_p]$ codim $(W_{\bar{v}_i})$. One gets a corresponding $D_{\bar{p}}(\boldsymbol{Q})$-subspace of U_i'. The direct sum of these subspaces defines $W_{\bar{p}}^{\text{ind.}}$. We then have

$$\varepsilon(\boldsymbol{Q}, V_p^{\text{ind.}}, \{W_{\bar{p}}^{\text{ind.}}\}) = \dim_{\boldsymbol{Q}_p}(V_p^{\text{ind.}}/W_p^{\text{ind.}}) = \varepsilon(K, V_p, \{W_{\bar{\pi}}\}). \tag{35}$$

Assume now that $K \cap \boldsymbol{Q}_\infty = \boldsymbol{Q}$ and let $K_\infty = K\boldsymbol{Q}_\infty$, the cyclotomic $\boldsymbol{Z}_p$-extension. The G_K-invariant lattice T_p of V_p defines a $G_{\boldsymbol{Q}}$-invariant lattice $T_p^{\text{ind.}}$ in $V_p^{\text{ind.}}$. Let $A^{\text{ind.}} = V_p^{\text{ind.}}/T_p^{\text{ind.}}$. Then one has the following result.

Proposition 7. *$S_{\Lambda^{\text{ind.}}}(\boldsymbol{Q}_\infty, \{C_p^{\text{ind.}}\}) \cong S_\Lambda(K_\infty, \{C_{\bar{\pi}}\})$ as Λ-modules.*

Here, of course, $\Gamma = \mathrm{Gal}(\boldsymbol{Q}_\infty/\boldsymbol{Q})$ has been identified in the obvious way with $\mathrm{Gal}(K_\infty/K)$. The proof is entirely group theoretic. We will just

sketch it. There is a natural isomorphism:

$$H^1(K_\infty, A) \xrightarrow{\sim} H^1(\boldsymbol{Q}_\infty, A^{\text{ind.}}). \tag{36}$$

Let v be any place of $\boldsymbol{Q}_\infty$. Let $I=I_{\bar{v}}(\boldsymbol{Q}_\infty)$ be the inertia subgroup of $G_{\boldsymbol{Q}_\infty}$ for $\bar{v}$. I acts on $G_{\boldsymbol{Q}_\infty}/G_{K_\infty}$ with orbits represented by g_i^{-1}, $1\leq i\leq t$, say. Let I_i' denote the stabilizer of g_i^{-1}, $I_i'\subseteq I$. Put $I_i=g_iI_i'g_i^{-1}=(g_iIg_i^{-1})\cap G_{K_\infty}$, which is an inertia group in G_{K_∞} for some place $\bar{v}_i$ of $\bar{\boldsymbol{Q}}$ above v. The $\bar{v}_i|_{K_\infty}$'s give all the places of K_∞ above v at least once. Just as previously, we get a decomposition $V_p^{\text{ind.}}\cong\oplus_{i=1}^t U_i'$ for the action of I. This gives a natural isomorphism:

$$\bigoplus_{i=1}^{t} H^1(I_i, A) \xrightarrow{\sim} H^1(I, A^{\text{ind.}}). \tag{37}$$

The isomorphisms (36), (37) commute with the natural restriction maps from the left and right terms of (36) to those of (37). If $v=v_p$, one also has an isomorphism

$$\bigoplus_{i=1}^{t} H^1(I_i, A/C_{\bar{v}_i}) \xrightarrow{\sim} H^1(I, A^{\text{ind.}}/C_{\bar{v}}^{\text{ind.}}). \tag{38}$$

Again the natural restriction maps commute. Proposition 7 follows.

If $V=\{V_l\}$ is a compatible system of l-adic representations over K, then $V^{\text{ind.}}=\{V_l^{\text{ind}}\}$ will be one over $\boldsymbol{Q}$. The L-function $L_V(s)$ (defined by an Euler product over the places of K) will equal $L_{V^{\text{ind.}}}(s)$ and so $r_V=r_{V^{\text{ind.}}}$, where the notation should be self-explanatory. We say p is ordinary for V if, for every place π of K over p, V_p has a filtration $F_{\bar{\pi}}^iV_p$ satisfying (1) with $G_{\boldsymbol{Q}_p}$, $I_{\boldsymbol{Q}_p}$ replaced by G_{K_π}, I_{K_π} (having chosen a place $\bar{\pi}$ of $\bar{\boldsymbol{Q}}$ over π). One can then define a Selmer group $S_A(K_\infty)$ by taking $W_{\bar{\pi}}=F_{\bar{\pi}}^+V_p$. Many of our subsequent arguments and results will go through for an arbitrary $\boldsymbol{Z}_p$-extension K_∞ satisfying our previous assumption, but from now on we will concentrate on the cyclotomic $\boldsymbol{Z}_p$-extension. We will also take $\boldsymbol{Q}$ as our base field, which is somewhat justified by the following remarks. For each i, the $F_{\bar{\pi}}^iV_p$'s allow one to define (as described above) a subspace $F_p^iV_p^{\text{ind.}}$ of $V_p^{\text{ind.}}$. In that way, one obtains a filtration satisfying (1) provided p is unramified in K. Hence, in this case, p is ordinary for $V_p^{\text{ind.}}$. (If p is ramified in K, (1) holds if one replaces $I_{\boldsymbol{Q}_p}$ by a subgroup of finite index. This unfortunately will interfere with several of our later arguments.) One can define the Selmer group $S_{A^{\text{ind.}}}(\boldsymbol{Q}_\infty)$. Assuming $K\cap\boldsymbol{Q}_\infty$ and $K_\infty=K\boldsymbol{Q}_\infty$, Proposition 7 states that $S_A(K_\infty)=S_{A^{\text{ind.}}}(\boldsymbol{Q}_\infty)$.

§ 6. The conjectural value of r_V

Consider a nonsingular projective variety X over $\boldsymbol{Q}$. For a fixed m,

$0 \leq m \leq 2\dim(X)$, one has a compatible system of l-adic representations $V = \{V_l\}$ over $\boldsymbol{Q}$, where

$$V_l = \mathrm{Hom}_{\boldsymbol{Q}_l}(H^m_{et}(X, \boldsymbol{Q}_l), \boldsymbol{Q}_l).$$

The L-function attached to X and m in [26] is $L_V(s)$. One has a Hodge decomposition $H^m(X, \boldsymbol{C}) = \oplus H^{ij}(X, \boldsymbol{C})$, where $i, j \geq 0$, $h^{ij} = \dim_{\boldsymbol{C}}(H^{ij}(X, \boldsymbol{C}))$ is zero if $i+j \neq m$. This is an example of a motive/$\boldsymbol{Q}$ of pure weight m. In terms of V, pure weight amounts to the assertion that the eigenvalues of a Frobenius for l ($l \neq p$, $l \notin \mathrm{Ram}(V)$) on V_p all have absolute value $l^{m/2}$, which is the Riemann hypothesis. (An arbitrary p-adic representation V_p of $G_{\boldsymbol{Q}}$ could be said to be pure of weight m if it has this last property.) Now there is a $\boldsymbol{C}$-linear action of complex conjugation c on $H^m(X, \boldsymbol{C})$ which interchanges $H^{ij}(X, \boldsymbol{C})$ and $H^{ji}(X, \boldsymbol{C})$. One has $h^{ij} = h^{ji}$. If m is even, put $k = m/2$ and let $h^{kk}((-1)^e)$ for $e = 0$ or 1 be the dimension of the $(-1)^e$-eigenspace for c acting on $H^{kk}(X, \boldsymbol{C})$. On $H^m(X, \boldsymbol{C})$, the $(-1)^e$-eigenspace for c has dimension $d((-1)^e) = \sum_{i<j} h^{ij} + h^{kk}((-1)^e)$. The conjectured Γ-factor is

$$\Gamma_V(s) = \Big(\prod_{i<j} \Gamma(s-i)^{h^{ij}}\Big)\Gamma\Big(\frac{s-k}{2}\Big)^{h^{kk}((-1)^k)}\Gamma\Big(\frac{s-k+1}{2}\Big)^{h^{kk}((-1)^{k-1})} \tag{39}$$

The order of the pole of $\Gamma_V(s)$ at $s = n$ is 0 if $n > k$. For $n \leq k$, it is

$$\sum_{\substack{i \geq n \\ i<j}} h^{ij} + h_{kk}((-1)^n) = d((-1)^n) - \sum_{i<n} h^{ij}$$

Faltings has proven that one has a Hodge-Tate decomposition $H^m_{et}(X, \boldsymbol{Q}_p) \otimes \boldsymbol{C}_p = \oplus_{i=0}^m \boldsymbol{C}_p(-i)^{h^{ij}}$ where $\boldsymbol{C}_p(t)$ denotes the 1-dimensional $\boldsymbol{C}_p$-space $\boldsymbol{C}_p \otimes \boldsymbol{Q}_p(t)$ with diagonal action of $G_{\boldsymbol{Q}_p}$ (which acts on the second factor by χ_p^t). Thus

$$V_p \otimes \boldsymbol{C}_p \cong \bigoplus_{\substack{i=0 \\ i+j=m}}^{m} \boldsymbol{C}_p(i)^{h^{ij}}.$$

According to [4], 0.3, $d((-1)^e)$ equals the dimension of the $(-1)^e$-eigenspace for a complex conjugation acting on $H^m_{et}(X, \boldsymbol{Q}_p)$ and so on V_p.

Consider $V(1-n) = \{V_l(1-n)\}$. Then $L_{V(1-n)}(s) = L_V(s+n-1)$. One has a Hodge-Tate decomposition $V_p(1-n) \otimes \boldsymbol{C}_p \cong \oplus_i \boldsymbol{C}_p(i+1-n)^{h^{ij}}$. The order of the pole of $\Gamma_{V(1-n)}(s)$ at $s = 1$ is 0 for $n > k$ and $\dim(V_p^-) - \sum_{i+1-n \leq 0} h^{ij}$ for $n \leq k$. (This last quantity is ≤ 0 for $n > k$.) These remarks should apply to the L-function for any motive/$\boldsymbol{Q}$ of pure weight. Changing notation, if V arises from a motive of pure weight and if one has a Hodge-Tate decomposition

$$V_p \otimes \boldsymbol{C}_p \cong \bigoplus_{i \in \boldsymbol{Z}} \boldsymbol{C}_p(i)^{h_i}, \tag{40}$$

then the value of r_V should be

$$r_V = \max\left(\dim\left(V_p^-\right) - \sum_{i \leq 0} h_i,\ 0\right). \tag{41}$$

If V is not of pure weight, it seems reasonable to believe that each V_p has a $G_{\boldsymbol{Q}}$-composition series whose subquotients $V_p^{(s)}$, $1 \leq s \leq t$, are of pure weight. Then one should have $r_V = \sum_{s=1}^{t} r_{V_p^{(s)}}$, with $r_{V_p^{(s)}}$ defined as in (41).

If V_p has a Hodge-Tate decomposition (40), then so will V_p^* with Hodge-Tate numbers $h_i^* = h_{1-i}$. Thus $\sum_{i \leq 0} h_i + \sum_{i \leq 0} h_i^* = \dim(V_p)$. Also $\dim(V_p^-) + \dim((V_p^*)^-) = \dim(V_p)$. It follows easily that $r_V = r_{V^*} = 0$ implies

$$\dim\left(V_p^-\right) = \sum_{i \leq 0} h_i. \tag{42}$$

The converse is true if V is of pure weight.

Assume p is ordinary for V. Let $h_i = \dim(F^i V_p / F^{i+1} V_p)$. Then $V_p \otimes \boldsymbol{C}_p$ will have a decomposition (40). One can verify this as follows. Let $W_i = F^i V_p / F^{i+1} V_p$. Then $G_{\boldsymbol{Q}_p^{\text{unr.}}}$ acts W_i on by χ_p^i, where $\boldsymbol{Q}_p^{\text{unr.}}$ denotes the maximal unramified extension of $\boldsymbol{Q}_p$. Thus $W_i(-i)$ is a representation of $\mathrm{Gal}(\boldsymbol{Q}_p^{\text{unr.}}/\boldsymbol{Q}_p)$. The Frobenius automorphism acts on a basis $\{w_i\}$, $1 \leq i \leq h = h_i$, of $W_i(-i)$ by a matrix $\varphi \in \mathrm{GL}_h(\boldsymbol{Z}_p)$. Let $\mathscr{A}$ denote the completion of the ring of integers of $\boldsymbol{Q}_p^{\text{unr.}}$ (in $\boldsymbol{C}_p$). It is not difficult to show there is a matrix $\psi \in GL_h(\mathscr{A})$ such that $\psi^{\text{Frob.}} \varphi = \psi$. (Here Frob. is the Frobenius automorphism in $\mathrm{Gal}(\boldsymbol{Q}_p^{\text{unr.}}/\boldsymbol{Q}_p)$, which acts on $\mathscr{A}$.) Letting $k = \boldsymbol{Z}/p\boldsymbol{Z}$, one uses the facts that $H^1(k, GL_h(\bar{k})) = 0$ and $H^1(k, M_h(\bar{k})) = 0$ ($M_h(\bar{k})$ = the additive group of $h \times h$ matrices) to inductively construct matrices ψ_n such that $\psi_n^{\text{Frob.}} \varphi \equiv \psi_n \pmod{p^n \mathscr{A}}$ and such that $\psi = \lim \psi_n$ exists. Then ψ has the above property. One can replace the above basis by $\{\psi(w_i)\}$, on which $\mathrm{Gal}(\boldsymbol{Q}_p^{\text{unr.}}/\boldsymbol{Q}_p)$ acts trivially. Thus $W_i \cong \boldsymbol{C}_p(i)^{h_i}$. It is enough then to use Tate's result from [30] that no nontrivial extensions exist between $\boldsymbol{C}_p(i)$'s for different values of i.

Assume that p is ordinary for V and also that $p \notin \mathrm{Ram}(V)$. Let $\alpha_1, \alpha_2, \cdots, \alpha_d$ be the eigenvalues of Frob. on any V_l, $l \neq p$. One would conjecture that the α_j's can be recovered from the action of $G_{\boldsymbol{Q}_p}$ on V_p in the following way. Let ord_p be the p-adic valuation on $\bar{\boldsymbol{Q}}_p$ normalized so that $\mathrm{ord}_p(p) = 1$. Frob. acts on $W_i(-i)$ with eigenvalues u_s, $1 \leq s \leq h_i$, say. The numbers $p^i u_s$ should be precisely those α_j's (counting multiplicity) such that $\mathrm{ord}_p(\alpha_j) = i$. This is at least true if V is as in the first paragraph of this section and if X has good reduction at p. (We are grateful to B. Messing for explaining this to us.) One consequence would be that

the number of α_j's with $\mathrm{ord}_p(\alpha_j)=i$ is exactly h_i, which is closer to a more familiar meaning of the term ordinary.

§ 7. Selmer groups for ordinary primes

We return to the situation in the introduction. The prime p is assumed to be ordinary for the compatible system $V=\{V_l\}$ over $\boldsymbol{Q}$. Let $\bar{p}$ be a place of $\bar{\boldsymbol{Q}}$ over p and let F^iV_p be the corresponding filtration. Define $W_{\bar{p}}=F^+V_p$ and $C_{\bar{p}}$ its image in $A=V_p/T_p$. Then

$$\begin{aligned}\delta(\boldsymbol{Q}, V_p)&=\dim(V_{\bar{p}}^-)\\ \varepsilon(\boldsymbol{Q}, V_p, \{C_{\bar{p}}\})&=\mathrm{codim}(F^+V_p)=\sum_{i\leq 0}h_i.\end{aligned}\tag{43}$$

Proposition 6 shows that $S_A(\boldsymbol{Q}_\infty)=S_A(\boldsymbol{Q}_\infty, \{C_{\bar{p}}\})$ is cofinitely generated over Λ and has Λ-corank $\geq \dim(V_{\bar{p}}^-)-\sum_{i\leq 0}h_i$ and hence $\geq r_V$ if V is of pure weight. This proves Theorem 1.

We assume now that $L_V(1)$ is a critical value, but not necessarily that V is pure. Let Σ be a finite set of primes of $\boldsymbol{Q}$ containing $\mathrm{Ram}(V)\cup\{p, \infty\}$. Then the Λ-module $H^1(\boldsymbol{Q}_\Sigma/\boldsymbol{Q}_\infty, A)$ has Λ-corank $\geq\delta=\delta(\boldsymbol{Q}, V_p)$. The Λ-modules H_Σ and $H_\Sigma^{\mathrm{inert.}}$ (defined just after (33)) both have Λ-corank equal to $\varepsilon=\varepsilon(\boldsymbol{Q}, V_p, \{C_{\bar{p}}\})$. By (42), $\delta=\varepsilon$. If $S_A(\boldsymbol{Q}_\infty)$ is in fact Λ-cotorsion, then there would be several consequences. First of all, it would follow that $\mathrm{corank}_\Lambda(H^1(\boldsymbol{Q}_\Sigma/\boldsymbol{Q}_\infty, A))=\delta$. By Propositions 3 and 4, this would imply Conjecture 3 when $K=\boldsymbol{Q}$. Also, the map $H^1(\boldsymbol{Q}_\Sigma/\boldsymbol{Q}_\infty, A)\to H_\Sigma$ would have a cokernel which is Λ-cotorsion. We will say that V is p-critical if $L_V(1)$ is a critical value and if $S_A(\boldsymbol{Q}_\infty)$ is Λ-cotorsion. It is not hard to show that this is independent of the choice of T_p.

For any $t\leq 1$, consider the generalized Selmer group $S_A(\boldsymbol{Q}_\infty, \{F^tA\})$. It is easier to study the Λ-submodule $S_A^{\mathrm{str.}}(\boldsymbol{Q}_\infty, \{F^tA\})$ (defined by using the decomposition subgroup $D_{\bar{p}}$ of $G_{\boldsymbol{Q}_\infty}$ instead of the inertia subgroup $I_{\bar{p}}$), which will have the same Λ-corank. We have an exact sequence.

$$0\longrightarrow S_A^{\mathrm{str.}}(\boldsymbol{Q}_\infty)\longrightarrow S_A^{\mathrm{str.}}(\boldsymbol{Q}_\infty, \{A\})\xrightarrow{\lambda} H^1(D_{\bar{p}}, A/F^+A)\tag{44}$$

We continue to assume V is p-critical. The middle term has Λ-corank δ, by Proposition 6. The final term has Λ-corank ε and hence the cokernel of the map λ is Λ-cotorsion. We should point out that we are using the identification

$$\Gamma=\mathrm{Gal}(\boldsymbol{Q}_\infty/\boldsymbol{Q})=\mathrm{Gal}((\boldsymbol{Q}_\infty)_{v_p}/\boldsymbol{Q}_p)\tag{45}$$

when considering these global and local objects as Λ-modules. Here v_p is

the unique place of $\boldsymbol{Q}_\infty$ over p. The map $H^1(D_{\bar{p}}, A/F^+A) \to H^1(D_{\bar{p}}, A/F^tA)$ is surjective (since $cd_p(D_p)=1$). In the exact sequence

$$(46) \qquad 0 \longrightarrow S_A^{\text{str.}}(\boldsymbol{Q}_\infty, \{F^tA\}) \longrightarrow S_A^{\text{str.}}(\boldsymbol{Q}_\infty, \{A\}) \xrightarrow{\lambda_t} H^1(D_{\bar{p}}, A/F^tA),$$

the final map has a Λ-cotorsion cokernel and so we get the following result.

Proposition 8. *Assume that V is p-critical. Then for $t \leq 1$, the generalized Selmer group $S_A(\boldsymbol{Q}_\infty, \{F^tA\})$ has Λ-corank equal to* $\dim_{\boldsymbol{Q}_p}(F^tV_p/F^1V_p)$.

It will be useful to examine the difference between these Selmer groups and their strict versions. Put $\bar{A}_t = A/F^tA$ and let $K_t = \ker(H^1(D_{\bar{p}}, \bar{A}_t) \to H^1(I_{\bar{p}}, \bar{A}_t))$. Then $K_t \cong H^1(D_{\bar{p}}/I_{\bar{p}}, \bar{A}_t^{I_{\bar{p}}})$ and so has finite $\boldsymbol{Z}_p$-corank. For any discrete cofinitely generated Λ-module H, there will be a maximal quotient H/H_0 which is Λ-cotorsion. (It corresponds to the Λ-torsion submodule of $\hat{H}$.) Let $H = H^1(D_{\bar{p}}, \bar{A}_t)$. Under the assumption of Proposition 8, we have that $H_0 \subseteq \text{Im}(\lambda_t)$. We will show that $(K_t)_{\text{div}} \subseteq H_0$. Let $C_t = (\bar{A}_t^{I_{\bar{p}}})_{\text{div}}$. Then it is easy to verify that $(K_t)_{\text{div}}$ is contained in $\text{Im}(H^1(D_{\bar{p}}, C_t) \to H^1(D_{\bar{p}}, \bar{A}_t))$. Now $I_{\bar{p}}$ acts by $\chi_p|_{I_{\bar{p}}}$ on C_t^* and so $C_t^*(\boldsymbol{Q}_\infty)$ is finite (zero if $p \neq 2$). Corollary 1 of Proposition 1 shows that $\hat{H}^1(D_{\bar{p}}, C_t)$ is Λ-torsion free. It follows that the image of $H^1(D_{\bar{p}}, C_t)$ is contained in H_0. This implies that $(K_t)_{\text{div}} \subseteq H_0$. Since $\lambda_t^{-1}(K_t) = S_A(\boldsymbol{Q}_\infty, \{F^tA\})$, (46) gives an exact sequence of Λ-modules.

$$(47) \qquad 0 \longrightarrow S_A^{\text{str.}}(\boldsymbol{Q}_\infty, \{F^tA\}) \to S_A(\boldsymbol{Q}_\infty, \{F^tA\}) \longrightarrow K_t$$

where the last map has finite cokernel. Let f_0 denote a topological generator for $D_{\bar{p}}/I_{\bar{p}}$. Then K_t is the cokernel of $f_0 - 1$ acting on $\bar{A}_t^{I_{\bar{p}}}$; the kernel is $\bar{A}_t^{D_{\bar{p}}} = \bar{A}_t((\boldsymbol{Q}_\infty)_{v_p})$. Thus $\hat{K}_t$ and $\bar{A}_t((\boldsymbol{Q}_\infty)_{v_p})^\wedge$ will be Λ-modules with the same characteristic ideal. In particular, for $t=1$, we have the following result.

Proposition 9. *Assume V is p-critical. Then the Pontryagin duals of $S_A(\boldsymbol{Q}_\infty)/S_A^{\text{str.}}(\boldsymbol{Q}_\infty)$ and $\bar{A}((\boldsymbol{Q}_\infty)_{v_p})$ are Λ-modules with the same characteristic ideal. Here $\bar{A} = A/F^+A$.*

One consequence of the above proposition concerns so-called exceptional or trivial zeros of p-adic L-functions—zeros that occur at φ_0 because of the vanishing of the interpolation factor A_{φ_0}. If this occurs, Conjecture 2 would predict that $\varphi_0(\lambda)=0$, where λ is a generator of the characteristic ideal of $\hat{S}_A(\boldsymbol{Q}_\infty)$, and hence that $S_A(\boldsymbol{Q}_\infty)^\Gamma$ contains a subgroup isomorphic to $\boldsymbol{Q}_p/\boldsymbol{Z}_p$. Assume that $p \notin \text{Ram}(V)$. According to (10), $A_{\varphi_0}=0$ precisely when some α_i or α_i^* is equal to p. Now, $\{\alpha_i^* | 1 \leq i \leq d\} = \{p\alpha_i^{-1} | 1 \leq i \leq d\}$, counting multiplicities, and so if some α_i or α_i^* equals 1, it should be true

that λ is divisible by $\gamma_0 - 1$. If some α_i is 1, this actually follows from Proposition 9 if one assumes the conjecture described at the end of Section 6, since then $gr^0(V_p)^{G_{\mathbf{Q}_p}} = (V_p/F^+V_p)^{G_{\mathbf{Q}_p}}$ and therefore $\bar{A}^{G_{\mathbf{Q}_p}} = \bar{A}(\mathbf{Q}_p) = \bar{A}((\mathbf{Q}_\infty)_{v_p})^\Gamma$ would be infinite. This conclusion also follows if some α_i^* is 1, as we will explain in the next section. We also want to mention the following corollary to Proposition 9.

Corollary. *Assume that V is p-critical. Let $e = \dim_{\mathbf{Q}_p}((V_p/F^+V_p)^{G_{\mathbf{Q}_p}})$. Then the characteristic ideal of $\hat{S}_A(\mathbf{Q}_\infty)$ is contained in $(\gamma_0 - 1)^e$.*

This should be clear since $\bar{A}(\mathbf{Q}_p)$ would have $\mathbf{Z}_p$-corank e.

We have one more consequence of the exact sequence (44). We will need to make the reasonable assumption that the numbers $h_i = \dim(gr^i(V_p))$ ($i \in \mathbf{Z}$) are independent of the (ordinary) prime p.

Proposition 10. *Assume that* $\mathrm{Ram}(V)$ *contains no finite prime and that V is p-critical. If $p \gg 0$, then $\hat{S}_A(\mathbf{Q}_\infty)$ contains no nontrivial finite Λ-submodule.*

Proof. We pointed out earlier that, if V is p-critical and if p is odd, then $H^2(\mathbf{Q}_\Sigma/\mathbf{Q}_\infty, A) = 0$. Here we can take $\Sigma = \{p, \infty\}$. By Proposition 5, $\hat{H}^1(\mathbf{Q}_\Sigma/\mathbf{Q}_\infty, A)$ has no nontrivial finite Λ-submodules. Now let i_V denote the minimal i such that $h_i > 0$. Let $m_V = |i_V| + 1$ if $i_V \leq 0$, $m_V = 0$ otherwise (that is, if $F^+V_p = V_p$). Now $(V_p/F^+V_p)^*$ has a filtration where $I_{\bar{p}}$ acts on the subquotients by characters ω^a, $1 \leq a \leq m_V$. If $p - 1 > m_V$, it follows that $((\bar{A})^*)^{I_{\bar{p}}} = 0$ and hence $(\bar{A})^*((\mathbf{Q}_\infty)_{v_p}) = 0$. Corollary 2 to Proposition 1 then states that $H^1(D_{\bar{p}}, \bar{A})$ is a cofree Λ-module. It follows that the map λ in (44) will be surjective. If p is odd, then $S_A^{\mathrm{str.}}(\mathbf{Q}_\infty, \{A\}) = H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_\infty, A)$. Letting $X = \hat{S}_A^{\mathrm{str.}}(\mathbf{Q}_\infty)$ and dualizing the sequence (44), we get an exact sequence

$$0 \longrightarrow \Lambda^s \longrightarrow \hat{H}^1(\mathbf{Q}_\Sigma/\mathbf{Q}_\infty, A) \longrightarrow X \longrightarrow 0.$$

That X contains no nontrivial finite submodule follows from the following observation.

Lemma. *Let Y be a finitely generated Λ-module, Z a free Λ-submodule. If Y contains no nontrivial finite Λ-submodule, then the same is true for Y/Z.*

Suppose Y_0 is a Λ-submodule of Y such that $Z \subseteq Y_0$ and Y_0/Z is finite and nonzero. The structure theory of Λ-modules implies that Y_0 is of finite index in some free Λ-module Z'. Then $Z \subseteq Z'$ with finite index, which is not possible. This proves the lemma. As for $\hat{S}_A(\mathbf{Q}_\infty)$ itself, note

that $p > m_V$ implies that $\bar{A}^{I_\mathfrak{p}} = F^0A/F^+A$, which is a divisible group. It follows that $K_1 = H^1(D_\mathfrak{p}/I_\mathfrak{p}, \bar{A}^{I_\mathfrak{p}})$ is also divisible. The discussion preceding Proposition 9 shows that the final map in (47) is surjective. Dualizing, we get an exact sequence

$$0 \longrightarrow \hat{K}_1 \longrightarrow \hat{S}_A(\boldsymbol{Q}_\infty) \longrightarrow X \longrightarrow 0$$

but $\hat{K}_1$ is $\boldsymbol{Z}_p$-torsion free and Proposition 10 follows easily. We see that $p > \max(m_V + 1, 2)$ is sufficient.

It should be possible to remove at least the assumption on $\mathrm{Ram}(V)$ from the above proposition, but we haven't succeeded in doing this. The above proof would work if the local cohomology groups $H^1((\boldsymbol{Q}_\infty)_v, A)$ $(v \mid l, l \in \mathrm{Ram}(V), l \neq p)$ vanished for $p \gg 0$, which is often the case, but not always. (See Proposition 2.)

§ 8. The proof of Theorem 2

We begin by summarizing the results of Tate that we will need. (See [9] or [29].) Let F be a finite extension of $\boldsymbol{Q}$ and let Σ be a finite set of places of F containing those over p and ∞. Let M be a finite $\mathrm{Gal}(F_\Sigma/F)$-module of p-power order. For $0 \leq i \leq 2$, let

$$P_i(M) = P_i(F, \Sigma, M) = \coprod_{v \in \Sigma} H^i(F_v, M).$$

The restriction map

$$\lambda_M^{(i)} : H^i(F_\Sigma/F, M) \longrightarrow P_i(M)$$

has kernel $K_i(M)$ and image $G_i(M)$, say. Let $M^* = \mathrm{Hom}(M, \mu_{p^\infty})$, also a $\mathrm{Gal}(F_\Sigma/F)$-module. There is a perfect pairing (local Tate duality)

$$P_1(M) \times P_1(M^*) \longrightarrow \boldsymbol{Q}_p/\boldsymbol{Z}_p. \tag{48}$$

$G_1(M)$ and $G_1(M^*)$ are orthogonal complements under (48). $K_2(M)$ is dual to $K_1(M^*)$ and so has the same order. Also the cokernel of $\lambda_M^{(2)}$ is dual to $H^0(F_\Sigma/F, M^*)$ and therefore again has the same order.

We take $F = \boldsymbol{Q}$. Let N be a $G_{\boldsymbol{Q}_p}$-submodule of M, $N^\perp$ its complement in M^*. Let L_p denote the image of $H^1(\boldsymbol{Q}_p, N)$ in $H^1(\boldsymbol{Q}_p, M)$ and let L_p^* be the image of $H^1(\boldsymbol{Q}_p, N^\perp)$ in $H^1(\boldsymbol{Q}_p, M^*)$. For $v \neq p$, let $L_v = H^1_{\mathrm{unr.}}(\boldsymbol{Q}_v, M)$, $L_v^* = H^1_{\mathrm{unr.}}(\boldsymbol{Q}_v, M^*)$. For the moment, we assume p is odd so that there will be no contribution to P_1 for $v = \infty$. Define $L = \coprod_v L_v \subseteq P_1(M)$, $L^* = \coprod_v L_v^* \subseteq P_1(M^*)$, where v runs over all places in Σ. The remarks at the end of Section 3 show that L and L^* are orthogonal complements in (48). For brevity, we let $G = G_1(M)$, $G^* = G_1(M^*)$. We see

then that GL and $G^* \cap L^*$ will be orthogonal complements in the pairing (48).

We assume the equality of the global and local Euler-Poincaré characteristics $\chi_{\text{glob}}(M)$ and $\chi_{\text{loc}}(M/N)$, where we consider M/N as a $G_{\boldsymbol{Q}_p}$-module. Equivalently, $[M: M(\boldsymbol{R})]=[M: N]$. Let

$$S=(\lambda_M^{(1)})^{-1}(L), \qquad S^*=(\lambda_{M^*}^{(1)})^{-1}(L^*). \tag{49}$$

Clearly $|S|=|K_1(M)| \cdot |G \cap L|$ and similarly for $|S^*|$. Let us define $g_i=|H^i(\boldsymbol{Q}_\Sigma/\boldsymbol{Q}, M)|$, $l_i(v)=|H^i(\boldsymbol{Q}_v, M)|$ for $v \in \Sigma$, $v \neq p$. Let $k_i=|K_i(M)|$. Similarly define $g_i^*, l_i^*(v)$, and k_i^*. Finally, for any finite $G_{\boldsymbol{Q}_p}$-module $\mathcal{M}$, put $h_i(\mathcal{M})=|H^i(\boldsymbol{Q}_p, \mathcal{M})|$.

With this notation, one finds that

$$[H^1(\boldsymbol{Q}_p, M): L_p]=h_1(M/N)h_2(N)^{-1}h_2(M)h_2(M/N)^{-1} \tag{50}$$

and, for $v \neq p$,

$$[H^1(\boldsymbol{Q}_v, M): L_v]=l_2(v). \tag{51}$$

One gets (51) from the facts that $l_1(v)=l_0(v)l_2(v)$ and that $|L_v|=|H^1(\boldsymbol{Q}_v^{\text{unr.}}/\boldsymbol{Q}_v, M^{I\boldsymbol{Q}_v})|=|H^0(\boldsymbol{Q}_v^{\text{unr.}}/\boldsymbol{Q}_v, M^{I\boldsymbol{Q}_v})|=l_0(v)$. (50) and (51) imply that

$$[P_1(M): L]=\chi_{\text{loc}}(M/N)^{-1}h_0(M/N)h_0(M^*/N^\perp)^{-1}|P_2(M)|. \tag{52}$$

Now $|P_2(M)|=g_2k_2^{-1}g_0^*$. We find that

$$\begin{aligned}|S|&=k_1|G \cap L|=k_1|G| \cdot |L| \cdot |GL|^{-1}\\ &=k_1|G| \cdot |L| \cdot |P_1(M)|^{-1}|G^* \cap L^*|=k_1|G| \cdot [P_1(M): L]^{-1} \cdot |S^*|(k_1^*)^{-1}.\end{aligned}$$

Noting that $k_1|G|=\chi_{\text{glob}}^{-1}(M)g_0g_2$ and that $k_1^*=k_2$, we obtain the formula

$$|S|g_0^{-1}h_0(M/N)=|S^*|(g_0^*)^{-1}h_0(M^*/N^\perp), \tag{53}$$

which will be the basis for our proof of Theorem 2.

Now let B denote a $\text{Gal}(\boldsymbol{Q}_\Sigma/\boldsymbol{Q})$-module isomorphic to $(\boldsymbol{Q}_p/\boldsymbol{Z}_p)^{d_B}$ as a group. As before, we have $B=\cup_n B_n$. Let $d_B^-=\text{corank}_{\boldsymbol{Z}_p}(B/B(\boldsymbol{R}))$. Suppose that $D=\cup_n D_n$ is a $G_{\boldsymbol{Q}_p}$-submodule of B which is divisible and such that $\text{corank}_{\boldsymbol{Z}_p}(B/D)=d_B^-$. We can apply the preceding calculation to $M=B_n$, $N=D_n$, at least if p is odd. Let $B^*=\cup_n B_n^*, D^\perp=\cup_n D_n^\perp \subseteq B^*$. As in (49), we define S_n, S_n^*. We will consider the groups $S_B^{\text{str.}}(\boldsymbol{Q})$, $S_{B^*}^{\text{str.}}(\boldsymbol{Q})$ defined in Section 5, using $K=K'=\boldsymbol{Q}$, $C_{\bar{p}}=D(\text{or } D^\perp)$. By (28), one has homomorphisms

$$S_n \longrightarrow S_B^{\text{str.}}(\boldsymbol{Q})_{p^n}, \qquad S_n^* \longrightarrow S_{B^*}^{\text{str.}}(\boldsymbol{Q})_{p^n} \tag{54}$$

with kernels whose orders are bounded as $n\to\infty$. As for the cokernels, one must look at the kernels of the maps $H^1(\boldsymbol{Q}_p, B_n/D_n)\to H^1(\boldsymbol{Q}_p, B/D)$ and, for $v\in\Sigma$, $v\neq p$, $H^1(I_{\boldsymbol{Q}_v}, B_n)\to H^1(I_{\boldsymbol{Q}_v}, B)$. These kernels have bounded order as $n\to\infty$ and therefore, since Σ is finite, so do the cokernels in (54).

We can now use (53) to relate the $\boldsymbol{Z}_p$-coranks of $S_B^{\text{str.}}(\boldsymbol{Q})$ and $S_{B^*}^{\text{str.}}(\boldsymbol{Q})$, which we denote by $s(B)$ and $s(B^*)$. The groups S_n, S_n^* will have orders $p^{s(B)n+O(1)}$, $p^{s(B_n^*)+O(1)}$, respectively. Similarly, the growth of the orders of $H^0(\boldsymbol{Q}, B_n)$, $H^0(\boldsymbol{Q}, B_n^*)$, $H^0(\boldsymbol{Q}_p, B_n/D_n)$, and $H^0(\boldsymbol{Q}_p, B_n^*/D_n^\perp)$ is given by the $\boldsymbol{Z}_p$-coranks of $B(\boldsymbol{Q})$, $B^*(\boldsymbol{Q})$, $\bar{B}(\boldsymbol{Q}_p)$, and $\bar{B}^*(\boldsymbol{Q}_p)$, respectively, where we have put $\bar{B}=B/D$, $\bar{B}^*=B^*/D^\perp$. Then we have

$$(55)\qquad \begin{aligned} &s(B)-\operatorname{corank}_{\boldsymbol{Z}_p}(B(\boldsymbol{Q}))+\operatorname{corank}_{\boldsymbol{Z}_p}(\bar{B}(\boldsymbol{Q}_v))\\ &\quad=s(B^*)-\operatorname{corank}_{\boldsymbol{Z}_p}(B^*(\boldsymbol{Q}))+\operatorname{corank}_{\boldsymbol{Z}_p}(\bar{B}^*(\boldsymbol{Q}_p)).\end{aligned}$$

Now let V be a compatible system of l-adic representations over $\boldsymbol{Q}$. Choose a finite set Σ as before. Assume that $L_V(1)$ is critical and that p is ordinary for V. Let $A=V_p/T_p$. We will study the Selmer group $S_A^{\text{str.}}(\boldsymbol{Q}_\infty)$ by means of the $\boldsymbol{Z}_p$-coranks of $(S_A^{\text{str.}}(\boldsymbol{Q}_\infty)\otimes Y)^\Gamma$, where $Y=\Lambda/(f)$. We let $f=f_0^a$, where f_0 is any irreducible element of Λ, $(f_0)\neq(p)$, and where $a\geq 1$. As observed before, $H^1(\boldsymbol{Q}_\infty, A)\otimes Y\cong H^1(\boldsymbol{Q}_\infty, B)$ as Λ-modules, where $B=A\otimes Y$. Note that B is a $G_{\boldsymbol{Q}}$-module and that $B\cong A^{\deg(f)}$ as a $G_{\boldsymbol{Q}_\infty}$-module. If one defines $F^+B=(F^+A)\otimes Y$, then it is obvious that $S_A^{\text{str.}}(\boldsymbol{Q}_\infty)\otimes Y\cong S_B^{\text{str.}}(\boldsymbol{Q}_\infty)$ as Λ-modules. Since $d_A^-=\operatorname{corank}_{\boldsymbol{Z}_p}(A/F^+A)$, we have $d_B^-=\operatorname{corank}_{\boldsymbol{Z}_p}(B/F^+B)$ and so we can apply our previous remarks, taking $D=F^+B$. In particular, (45) holds.

Consider the restriction map

$$(56)\qquad S_B^{\text{str.}}(\boldsymbol{Q})\xrightarrow{\rho} S_B^{\text{str.}}(\boldsymbol{Q}_\infty)^\Gamma.$$

The kernel is $H^1(\Gamma, B(\boldsymbol{Q}_\infty))\cap S_B^{\text{str.}}(\boldsymbol{Q})$. Now $B(\boldsymbol{Q}_\infty)=A(\boldsymbol{Q}_\infty)\otimes Y$. If $A(\boldsymbol{Q}_\infty)$ is infinite, we let $V_p^0=V_p(\boldsymbol{Q}_\infty)$ be the corresponding subspace, on which $G_{\boldsymbol{Q}}$ acts through Γ. Suppose that W_p is some $G_{\boldsymbol{Q}}$-irreducible subquotient of V_p^0. Then W_p^* is one for V_p^*. Some subgroup $I'_{\boldsymbol{Q}_p}$ of finite index in $I_{\boldsymbol{Q}_p}$ will act on W_p^* by χ_p^i, where $i\in\boldsymbol{Z}$. Now $r_{V^*}=0$ and $\dim((W_p^*)^-)=1$. The definition of r_{V^*} and (41) show that $i\leq 0$. But then $I'_{\boldsymbol{Q}_p}$ acts on W_p by χ_p^t with $t\geq 1$. This shows that $V_p^0\subseteq F^+V_p$. Hence $A(\boldsymbol{Q}_\infty)_{\text{div}}\subseteq F^+A$, $B(\boldsymbol{Q}_\infty)_{\text{div}}\subseteq F^+B$ and so $H^1(\Gamma, B(\boldsymbol{Q}_\infty)_{\text{div}})\subseteq S_B^{\text{str.}}(\boldsymbol{Q})$. Thus, since $H^1(\Gamma, B(\boldsymbol{Q}_\infty)_{\text{div}})$, $H^1(\Gamma, B(\boldsymbol{Q}_\infty))$, and $H^0(\Gamma, B(\boldsymbol{Q}_\infty))=B(\boldsymbol{Q})$ have the same $\boldsymbol{Z}_p$-corank, we have

$$(57)\qquad \operatorname{corank}_{\boldsymbol{Z}_p}(\operatorname{Im}(\rho))=s(B)-\operatorname{corank}_{\boldsymbol{Z}_p}(B(\boldsymbol{Q})).$$

Now $B(\boldsymbol{Q})$ is finite except possibly if every "root" φ *of* f_0 (where $\varphi\in$

$\mathrm{Hom}_{\mathrm{cont}}(\Gamma, \boldsymbol{C}_p^{\times})$) is such that $\varphi\chi_p^t$ is of finite order for some $t \geq 1$. It will be useful to point out that in this case $H^0(\boldsymbol{Q}_p, \bar{B}) = \bar{B}(\boldsymbol{Q}_p)$ will have $\boldsymbol{Z}_p$-corank zero. So in (55), some of the terms must be zero.

The map $H^1(\boldsymbol{Q}, B) \xrightarrow{\rho} H^1(\boldsymbol{Q}_\infty, B)^\Gamma$ is surjective. A cocycle $\sigma \in H^1(\boldsymbol{Q}, B)$ satisfies the local triviality condition at a place $v \nmid p$ if and only if $\rho(\sigma)$ does, because v is unramified in $\boldsymbol{Q}_\infty/\boldsymbol{Q}$. At p, one must consider

$$H^1(\Gamma, \bar{B}((\boldsymbol{Q}_\infty)_{v_p})) = \ker\left(H^1(\boldsymbol{Q}_p, \bar{B}) \longrightarrow H^1((\boldsymbol{Q}_\infty)_{v_p}, \bar{B})\right), \tag{58}$$

which has the same $\boldsymbol{Z}_p$ -corank as $\bar{B}(\boldsymbol{Q}_p)$. If this $\boldsymbol{Z}_p$-corank is zero, then the cokernel of ρ in (56) will be finite.

For all but finitely many (f_0), one sees easily that the $\boldsymbol{Z}_p$-coranks appearing in (55) are zero except for $s(B)$ and $s(B^*)$. One then has

$$\mathrm{corank}_{\boldsymbol{Z}_p}(S_B^{\mathrm{str.}}(\boldsymbol{Q}_\infty)^\Gamma) = \mathrm{corank}_{\boldsymbol{Z}_p}(S_{B^*}^{\mathrm{str.}}(\boldsymbol{Q}_\infty)^\Gamma). \tag{59}$$

This and the fact that $B^* = A^* \otimes Y^t$, where $Y^t = \Lambda/(f^t)$ and that $\deg(f^t) = \deg(f)$, imply the following result.

Proposition 11. *If $L_V(1)$ and $L_{V^*}(1)$ are a pair of critical values, then $S_{V_p/T_p}(\boldsymbol{Q}_\infty)$ and $S_{V_p^*/T_p^*}(\boldsymbol{Q}_\infty)$ have the same Λ-corank.*

We assume now that these Λ-corank are zero (that is, V and hence V^* are p-critical.) Fix f_0. Let $f_0^{s_0}$, $f_0^{t_0}$, $f_0^{s_0+t_0}$ be the exact powers of f_0 in the characteristic ideals of $\hat{S}_A^{\mathrm{str.}}(\boldsymbol{Q}_\infty)$, $\hat{A}((\boldsymbol{Q}_\infty)_{v_p})$, and $\hat{S}_A(\boldsymbol{Q}_\infty)$, respectively. (See Proposition 9.) For A^* and for f_0^t, we define similarly s_0^*, t_0^*. Let $Y_a = \Lambda/(f_0^a)$ for any $a \geq 1$. Put $B_a = A \otimes Y_a$. Then $B_a^* = A^* \otimes Y_a^t$. The discussion in Section 3 shows that, for $a \gg 0$,

$$\begin{aligned}
&\mathrm{corank}_{\boldsymbol{Z}_p}(S_{B_a}^{\mathrm{str.}}(\boldsymbol{Q}_\infty)^\Gamma) = s_0 \deg(f_0)\\
&\mathrm{corank}_{\boldsymbol{Z}_p}(S_{B_a^*}^{\mathrm{str.}}(\boldsymbol{Q}_\infty)^\Gamma) = s_0^* \deg(f_0^t) = s_0^* \deg(f_0)\\
&\mathrm{corank}_{\boldsymbol{Z}_p}(\bar{B}_a(\boldsymbol{Q}_p)) = t_0 \deg(f_0),\\
&\mathrm{corank}_{\boldsymbol{Z}_p}(\bar{B}_a^*(\boldsymbol{Q}_p)) = t_0^* \deg(f_0).
\end{aligned} \tag{60}$$

Except for the powers of p, Theorem 2 is the assertion $s_0 + t_0 = s_0^* + t_0^*$. This will follow from (55), (57), and (60), if we prove the following lemma.

Lemma. *Assume that $S_A(\boldsymbol{Q}_\infty)$ is Λ-cotorsion. Then the restriction map*

$$S_{B_a}^{\mathrm{str.}}(\boldsymbol{Q}_\infty) \xrightarrow{\rho_a} S_{B_a}^{\mathrm{str.}}(\boldsymbol{Q}_\infty)^\Gamma \tag{61}$$

has finite cokernel if $a \gg 0$.

Proof. We can assume that $\bar{B}_a(\boldsymbol{Q}_p)$ is infinite. (If this is true for one $a \geq 1$, it is true for all.) Then $H^0(\boldsymbol{Q}, B_a) = B_a(\boldsymbol{Q})$ and $H^1(\Gamma, B(\boldsymbol{Q}_\infty))$ will both be finite. Hence the map $H^1(\boldsymbol{Q}, B_a) \xrightarrow{\rho_a} H^1(\boldsymbol{Q}_\infty, B_a)^\Gamma$ is surjective with finite kernel. For brevity, let $S_a(\boldsymbol{Q})$, $S_a(\boldsymbol{Q}_\infty)$ denote $S^{\text{str.}}_{B_a}(\boldsymbol{Q})$, $S^{\text{str.}}_{B_a}(\boldsymbol{Q}_\infty)^\Gamma$, respectively. Let $S'_a(\boldsymbol{Q}) = \rho_a^{-1}(S_a(\boldsymbol{Q}_\infty)^\Gamma)$. One has an exact sequence

$$0 \longrightarrow S_a(\boldsymbol{Q}) \longrightarrow S'_a(\boldsymbol{Q}) \longrightarrow H^1(\Gamma, \bar{B}_a((\boldsymbol{Q}_\infty)_{v_p})). \tag{62}$$

Tensoring the obvious exact sequence $0 \to Y_a \to Y_{2a} \to Y_a \to 0$ with A gives an exact sequence $0 \to B_a \to B_{2a} \to B_a \to 0$. The resulting maps $H^1(\boldsymbol{Q}, B_a) \to H^1(\boldsymbol{Q}, B_{2a})$, $S_a(\boldsymbol{Q}) \xrightarrow{\alpha} S_{2a}(\boldsymbol{Q})$, and $S'_a(\boldsymbol{Q}) \xrightarrow{\alpha'} S'_{2a}(\boldsymbol{Q})$ have finite kernels. But, by (60), the Λ-coranks of these Selmer groups are bounded and so the cokernels of the maps α and α' will be finite if $a \gg 0$.

Let H_a denote the last term in (62). Again, according to (60), the $\boldsymbol{Z}_p$-corank of H_a is constant if $a \gg 0$. But tensoring the above exact sequence of Y's with $\bar{A}((\boldsymbol{Q}_\infty)_{v_p})$ and taking cohomology give an exact sequence

$$H_a \xrightarrow{\lambda} H_{2a} \longrightarrow H_a \longrightarrow 0.$$

It follows that $\ker(\lambda)$ is of finite index in H_a, if $a \gg 0$. Then (62) and what we said about α and α' imply that $S_a(\boldsymbol{Q})$ is of finite index in $S'_a(\boldsymbol{Q})$, which proves the lemma.

There is no difficulty in modifying the preceding arguments for $p = 2$. It is enough to verify (55). One can include the groups L_∞, L^*_∞ defined in (63) below as factors in L, L^*. Also $B_n/B_n(\boldsymbol{R})$ will have order $2^{d_B \bar{n} + O(1)}$. (53) will hold for S_n and S^*_n, up to a factor 2^{e_n}, where $e_n = O(1)$, which doesn't affect the conclusions about the $\boldsymbol{Z}_p$-coranks of $S^{\text{str.}}_B(\boldsymbol{Q})$ and $S^{\text{str.}}_{B^*}(\boldsymbol{Q})$.

To complete the proof of Theorem 2, we must compare Iwasawa's μ-invariants for $\hat{S}^{\text{str.}}_A(\boldsymbol{Q}_\infty)$ and $\hat{S}^{\text{str.}}_{A^*}(\boldsymbol{Q}_\infty)$. Fix $n \geq 1$. For each $m \geq 0$, we consider

$$S_n(\boldsymbol{Q}_m) \subseteq H^1(\boldsymbol{Q}_m, A_n), \qquad S^*_n(\boldsymbol{Q}_m) \subseteq H^1(\boldsymbol{Q}_m, A^*_n)$$

which are defined by (49), but now with $F = \boldsymbol{Q}_m$, $M = A_n$, and $L = L(\boldsymbol{Q}_m)$, $L^* = L^*(\boldsymbol{Q}_m)$ defined in essentially the same way as before:

$$L = \prod_v L_v \subseteq P_1(\boldsymbol{Q}_m, \Sigma_m, A_n),$$

where Σ_m is the set of places over those in Σ. For finite $v \in \Sigma_m$, the defi-

nition of L_v should be clear. (Take $N=F^+A_n$ for the unique place $v=v_p$ over p.) For the infinite places v, we have $(\boldsymbol{Q}_m)_v=\boldsymbol{R}$. We take

$$L_v=\ker\,(H^1(\boldsymbol{R}, A_n)\longrightarrow H^1(\boldsymbol{R}, A)). \tag{63}$$

The L_v^*'s and $L^*=\prod_v L_v^*$ are defined similarly. It is crucial that L and L^* be orthogonal complements under (48) and so we must verify that, for each $v\mid\infty$, $L_v^\perp=L_v^*$ for the perfect pairing

$$H^1(\boldsymbol{R}, A_n)\times H^1(\boldsymbol{R}, A_n^*)\longrightarrow \boldsymbol{Z}/2\boldsymbol{Z}. \tag{64}$$

For this purpose we can of course assume $p=2$. Hence $A\cong(\boldsymbol{Q}_2/\boldsymbol{Z}_2)^d$. For the action of $G_{\boldsymbol{R}}$, we have $A^+=A(\boldsymbol{R})\cong(\boldsymbol{Q}_2/\boldsymbol{Z}_2)^{d^+}\oplus(\boldsymbol{Z}/2\boldsymbol{Z})^{f^+}$ and $A^-\cong(\boldsymbol{Q}_2/\boldsymbol{Z}_2)^{d^-}\oplus(\boldsymbol{Z}/2\boldsymbol{Z})^{f^-}$, say. Consider the exact sequence (for $n\geq 1$)

$$0\longrightarrow A(\boldsymbol{R})/2^nA(\boldsymbol{R})\longrightarrow H^1(\boldsymbol{R}, A_n)\longrightarrow H^1(\boldsymbol{R}, A)\longrightarrow 0, \tag{65}$$

where the final zero is because $H^1(\boldsymbol{R}, A)$ has exponent 2. (65) implies that $|L_v|=2^{f^+}$. Also, it is clear that $|L_v^*|=2^{f^-}$. One also verifies easily that $|H^1(\boldsymbol{R}, A)|=2^{f^-}$. Hence $|L_v|\cdot|L_v^*|=|H^1(\boldsymbol{R}, A_n)|$. We have maps $A_{2n}\xrightarrow{a}A_n$, $A_n\xrightarrow{b}A_{2n}$, where b is inclusion and ba is multiplication by 2^n. For the resulting maps $H^1(\boldsymbol{R}, A_{2n})\xrightarrow{\alpha}H^1(\boldsymbol{R}, A_n)$, $H^1(\boldsymbol{R}, A_n)\xrightarrow{\beta}H^1(\boldsymbol{R}, A_{2n})$, we have $\beta\alpha=0$. Thus $\mathrm{Im}\,(\alpha)\subseteq\ker\,(\beta)\subseteq L_v$. On the other hand, we have the inclusion map $A_n^*\xrightarrow{c}A_{2n}^*$, which is adjoint to a. Thus the resulting map $H^1(\boldsymbol{R}, A_n^*)\xrightarrow{\gamma}H^1(\boldsymbol{R}, A_{2n}^*)$ is the adjoint of α and so we have $\mathrm{Im}\,(\alpha)^\perp=\ker\,(\gamma)\subseteq L_v^*$. But comparing orders shows that $\mathrm{Im}\,(\alpha)=L_v$ and $\mathrm{Im}\,(\alpha)^\perp=L_v^*$ and so $L_v^\perp=L_v^*$. It will also be useful to point out that $[H^1(\boldsymbol{R}, A_n): L_v]=2^{f^-}$ and that $[A_n: A_n(\boldsymbol{R})]=2^{nd^--f^+}$.

The calculations that led us to (53) work without change for $S_n(\boldsymbol{Q}_m)$ and $S_n^*(\boldsymbol{Q}_m)$ if p is odd. For $p=2$, we must make the following remarks. The index $[H^1(\boldsymbol{R}, A_n): L_v]$ is no longer $l_2(v)$ (which is $l_1(v)=2^{f^+-f^-}$), but is 2^{f^-}. Thus, in (52), one must replace $|P_2(A_n)|$ by $(2^{-f^+})^{[\boldsymbol{Q}_m:\boldsymbol{Q}]}|P_2(A_n)|$. Also, $[A_n: A_n(\boldsymbol{R})]=[A_n: F^+A_n]\cdot 2^{-f^+}$, and so $\chi_{\mathrm{glob}}(A_n)=\chi_{\mathrm{loc}}(A/F^+A_n)\cdot 2^{f^+[\boldsymbol{Q}_m:\boldsymbol{Q}]}$. These changes cancel each other and we still get (53) for $S_n(\boldsymbol{Q}_m)$ and $S_n^*(\boldsymbol{Q}_m)$.

Let $X=\hat{S}_A^{\mathrm{str.}}(\boldsymbol{Q}_\infty)$ and $X^*=\hat{S}_{A^*}(\boldsymbol{Q}_\infty)$. Let $\mu_n(X)$, $\mu_n(X^*)$ be the μ-invariants for the Λ-modules X/p^nX, X^*/p^nX^* which are Pontryagin duals of $S_A^{\mathrm{str.}}(\boldsymbol{Q}_\infty)_{p^n}$, $S_{A^*}^{\mathrm{str.}}(\boldsymbol{Q}_\infty)_{p^n}$, respectively. The natural maps

$$S_n(\boldsymbol{Q}_m)\longrightarrow S_A^{\mathrm{str.}}(\boldsymbol{Q}_m)_{p^n}\longrightarrow S_A^{\mathrm{str.}}(\boldsymbol{Q}_\infty)_{p^n}^{\Gamma_m},$$

$$S_n^*(\boldsymbol{Q}_m)\longrightarrow S_{A^*}^{\mathrm{str.}}(\boldsymbol{Q}_m)_{p^n}\longrightarrow S_{A^*}^{\mathrm{str.}}(\boldsymbol{Q}_\infty)_{p^n}^{\Gamma_m}.$$

turn out to have kernels and cokernels which are bounded as $m \to \infty$ (for fixed n). Here $\Gamma_m = \mathrm{Gal}(\boldsymbol{Q}_\infty/\boldsymbol{Q}_m)$. There are a number of points which need to be considered to verify this, but all are quite simple. The g_0's and h_0's in (53) are also bounded as $m \to \infty$. It follows that $\mu_n(X) = \mu_n(X^*)$ for any $n \geq 1$. Now, noting that $\mu_n(\Lambda) = p^n$, $\mu_n(\Lambda/p^t\Lambda) = \min(t, n)$, we find again that X and X^* have the same Λ-rank (Proposition 11) and also, if X and X^* are Λ-torsion, they must have the same μ-invariant. This completes the proof of Theorem 2,

Actually, we would expect that

$$S_A(\boldsymbol{Q}_\infty) \sim S_{A^*}(\boldsymbol{Q}_\infty)^\iota \tag{66}$$

when V is p-critical. If $A = E_{p^\infty}$, where E is an elliptic curve/$\boldsymbol{Q}$ with good, ordinary reduction at p, then (66) in fact follows from our arguments, which become considerably simpler in this case. First of all, as we pointed out in Section 2, $S_{E_{p^\infty}}(\boldsymbol{Q}_\infty) = S^{\mathrm{str.}}_{E_{p^\infty}}(\boldsymbol{Q}_\infty)$. Also (55) becomes $s(B) = s(B^*)$. The map (56) has finite kernel and cokernel. Thus (59) holds. In fact, we obtain (66) without the assumption that $S_A(\boldsymbol{Q}_\infty)$ is Λ-cotorsion. If E has multiplicative reduction at p, then one encounters a difficulty only for $(f_0) = (\gamma_0 - 1)$. But since $E^*_{p^\infty} \cong E_{p^\infty}$ (the Weil pairing) and since $(\gamma_0 - 1) = (\gamma_0 - 1)^\iota$, one still has (66). These results are also proved in [16] and [13] but in a rather more general context.

We also expect that the map (61) in the lemma has finite cokernel for all $a \geq 1$, still assuming that A arises from a compatible system of l-adic representations over $\boldsymbol{Q}$. In some cases, this is related to questions in transcendental number theory. For example, take $A = E_{p^\infty}$ where E has split multiplicative reduction at p. Then, if q_E is the Tate period, the finiteness of the cokernel turns out to follow from Manin's conjecture that $\log_p(q_E) \neq 0$. We will discuss this in [8].

Finally, we can add to our comments in Section 7 concerning the phenomenon of exceptional zeros. Following the notation there, if some α_i^* is 1, then (conjecturally) $(V_p^*/F^+V_p^*)^{G_{\boldsymbol{Q}_p}}$ would have positive dimension e^*, say. Therefore $(\gamma_0 - 1)^{e^*}$ will divide a generator of the characteristic ideal of $\hat{S}_{A^*}(\boldsymbol{Q}_\infty)$ and hence of $\hat{S}_A(\boldsymbol{Q}_\infty)$.

§ 9. Some remarks, questions, and examples

We want to end by discussing various points without making any attempt at generality. In many of our remarks, we will allow ourselves to be rather speculative.

I. *Selmer groups over* $\boldsymbol{Q}$. Let $V = \{V_l\}$ be a compatible system of l-adic representations over $\boldsymbol{Q}$. We will assume that $V_p^{G_{\boldsymbol{Q}}} = 0$. Let $A_p =$

V_p/T_p, where T_p is any $G_{\boldsymbol{Q}}$-invariant lattice. The map $H^1(\boldsymbol{Q}, A_p) \xrightarrow{\rho} H^1(\boldsymbol{Q}_\infty, A_p)^\Gamma$ has zero kernel and zero cokernel. Assume that p is ordinary for V and that $S_{A_p}(\boldsymbol{Q}_\infty)$ has Λ-corank r_V. Let $X=\hat{S}_{A_p}(\boldsymbol{Q}_\infty)$. There is a certain quotient $X_0 \cong \boldsymbol{Z}_p^{r_V}$ of X on which Γ acts trivially (the obvious quotient of $X/X_{\Lambda\text{-torsion}}$). This defines a subgroup of $S_{A_p}(\boldsymbol{Q}_\infty)^\Gamma$ (which is actually contained in $S_{A_p}^{\mathrm{str.}}(\boldsymbol{Q}_\infty)^\Gamma$, as one verifies easily). Applying ρ^{-1}, one obtains a canonical subgroup

$$S_{A_p}^{\mathrm{can}}(\boldsymbol{Q}) \subseteq H^1(\boldsymbol{Q}, A_p), \qquad S_{A_p}^{\mathrm{can}}(\boldsymbol{Q}) \cong (\boldsymbol{Q}_p/\boldsymbol{Z}_p)^{r_V} \tag{67}$$

Given this, one can easily construct another $G_{\boldsymbol{Q}}$-representation space W_p which fits into an exact sequence

$$0 \longrightarrow V_p \longrightarrow W_p \longrightarrow U_p \longrightarrow 0, \tag{68}$$

where $U_p=\boldsymbol{Q}_p^{r_V}$ (on which $G_{\boldsymbol{Q}}$ acts trivially) and where $S_{A_p}^{\mathrm{can}}(\boldsymbol{Q})$ can be recovered as the image of the induced map $U_p \to H^1(\boldsymbol{Q}, A_p)$. The local conditions (3) and (4) have the following meaning: If $v \mid l$, $l \neq p$, then (68) splits as an exact sequence of I_v-spaces. If $v=v_p$, then the exact sequence

$$0 \longrightarrow V_p/F^+V_p \longrightarrow W_p/F^+V_p \longrightarrow U_p \longrightarrow 0 \tag{69}$$

of D_{v_p}-spaces splits. It follows that if $l \neq p$, then $l \in \mathrm{Ram}\,(V_p)$ if and only if $l \in \mathrm{Ram}\,(W_p)$. Also, if one had $S_{A_p}^{\mathrm{can}}(\boldsymbol{Q}) \subseteq S_{A_p}(\boldsymbol{Q})$, which we suspect must be true, then (69) would split as a sequence of $G_{\boldsymbol{Q}_p}$-spaces. This would allow one to define a filtration on W_p satisfying (1) and so one could say that W_p is ordinary. Without the above inclusion, W_p would still satisfy (1) except that $I_{\boldsymbol{Q}_p}$ would only act *unipotently* on $gr^0(W_p)$. It seems reasonable to ask if there is a natural subgroup of $H^1(\boldsymbol{Q}, A_p)$ satisfying (67), and hence a corresponding W_p, for every prime p. This is at least true in the extreme case $F^+V_p=V_p$ (i.e. $r_V=\dim\,(V_p^-)$).

II. *Elliptic curves.* Let E be an elliptic curve defined over $\boldsymbol{Q}$. Assume that E has good, ordinary reduction at p. Then the restriction map $S_{E_{p^\infty}}(\boldsymbol{Q}) \to S_{E_{p^\infty}}(\boldsymbol{Q}_\infty)^\Gamma$ has finite kernel and cokernel. $S_{E_{p^\infty}}(\boldsymbol{Q})$ is quite close to the classical Selmer group for E over $\boldsymbol{Q}$, but it may differ (again by finite groups). The $\boldsymbol{Z}_p$-coranks will be the same. Let $r=\mathrm{rank}_{\boldsymbol{Z}}\,(E(\boldsymbol{Q}))$. Then one has the Kummer map

$$E(\boldsymbol{Q}) \otimes (\boldsymbol{Q}_p/\boldsymbol{Z}_p) \longrightarrow S_{E_{p^\infty}}(\boldsymbol{Q}). \tag{70}$$

As in I, this subgroup of $H^1(\boldsymbol{Q}, E_{p^\infty})$ allows one to construct an extension W_p of $V_p(E)$ by $\boldsymbol{Q}_p^r$. (This would be possible for every p.) The field which is cut out by W_p will be $\boldsymbol{Q}(E_{p^\infty})$ $((1/p^n)P;\ P \in E(\boldsymbol{Q}))$. Now consider

the generalized Selmer group $S_{E_{p^\infty}}(\boldsymbol{Q}_\infty, \{E_{p^\infty}\})$ (where one simply forgets the local condition at v_p). It should have Λ-corank 1. (By Proposition 8, this would be true if one knew that $S_{E_{p^\infty}}(\boldsymbol{Q}_\infty)$ were Λ-cotorsion.) Assuming this, one obtains a canonically defined subgroup $S^{\text{can}} \subseteq H^1(\boldsymbol{Q}, E_{p^\infty})$, $S^{\text{can}} \cong \boldsymbol{Q}_p/\boldsymbol{Z}_p$. One can prove that, if $r>0$, then $S^{\text{can}} \subseteq S_{E_{p^\infty}}(\boldsymbol{Q})$ and hence, if the p-primary subgroup of the Tate-Shafarevich group Ш$(E, \boldsymbol{Q})$ is finite as conjectured, one gets a canonical subgroup of $E(\boldsymbol{Q}) \otimes (\boldsymbol{Q}_p/\boldsymbol{Z}_p)$. Perhaps it has some meaning.

If E is a modular elliptic curve, then the Hasse-Weil L-function $L_E(s)$ (over $\boldsymbol{Q}$) has an analytic continuation and functional equation with Γ-factor $\Gamma(s)$. There is one critical value, at $s=1$, where of course $L_E(s)$ is conjectured to vanish to order r. Because of the functional equation, $L_E(s)$ vanishes at $s=1-n$, $n \geq 1$, to order exactly 1. If one considers the Tate twist $V=V(E)(n)$, then $r_V=1$. If E has ordinary reduction at p, then p is ordinary for V and $F^+V_p=V_p$. Hence $S_{A_p}(\boldsymbol{Q}_\infty)=S_{A_p}(\boldsymbol{Q}_\infty, \{A_p\})$, which one can actually consider for any prime p (ordinary or not). Here $A_p = V_p(E)(n)/T_p(E)(n)$. The Selmer group $S_{A_p}(\boldsymbol{Q}_\infty)$ will have Λ-corank $r_n \geq 1$, according to Proposition 6, but one should undoubtedly have $r_n=1$. In any case, one sees easily that r_n depends only on the residue class of n modulo $(p-1)$ (or modulo 2, if $p=2$), since the isomorphism class of the $G_{\boldsymbol{Q}_\infty}$-space $V_p(E)(n)$ does. The fact that $\text{ord}_{s=1}(L_V(s)) = \text{ord}_{s=1-n}(L_E(s)) = 1$ tempts us to conjecture more precisely that the $\boldsymbol{Z}_p$-corank of $S_{A_p}(\boldsymbol{Q}_\infty)^\Gamma$ (or equivalently of $S_{A_p}(\boldsymbol{Q})$, since the map $S_{A_p}(\boldsymbol{Q}) \xrightarrow{\rho} S_{A_p}(\boldsymbol{Q}_\infty)^\Gamma$ is obviously surjective now) should also be exactly 1, which amounts to the assertion that both $r_n=1$ and R_n^Γ is finite, where R_n denotes the maximal Λ-cotorsion quotient of $S_{A_p}(\boldsymbol{Q}_\infty)$.

Let Π be a finite set of primes. It is interesting to consider the non-primitive L-function $L_E(s)_\Pi$, where one simply omits the Euler factors for all $q \in \Pi$. Let $m=$ the number of $q \in \Pi$ where E has split multiplicative reduction. (The Euler factor is then $(1-q^{-s})$.) Then $\text{ord}_{s=1-n}(L_E(s)_\Pi)$ is $1+m$ when $n=1$, but is still just 1 when $n \geq 2$. One can also consider the non-primitive Selmer group $S_{A_p}(\boldsymbol{Q})_\Pi$, which is defined by omitting the local triviality condition for all $q \in \Pi$. When $n=1$, one can show that $S_{A_p}(\boldsymbol{Q})_\Pi$ has $\boldsymbol{Z}_p$-corank $\geq 1+m$. For $n \geq 2$, $S_{A_p}(\boldsymbol{Q})$ and $S_{A_p}(\boldsymbol{Q})_\Pi$ will have the same $\boldsymbol{Z}_p$-corank for any Π. To see this, one verifies that $H^0(\boldsymbol{Q}_l, A_p^*) = A_p^*(\boldsymbol{Q}_l)$ is finite for every $l \neq p$ (and $n \geq 2$), which implies that $H^1_{\text{unr.}}(\boldsymbol{Q}_l, A_p)$ has finite index in $H^1(\boldsymbol{Q}_l, A_p)$. Hence $H^1(\boldsymbol{Q}_l, A_p)_{\text{div}} \subseteq H^1_{\text{unr.}}(\boldsymbol{Q}_l, A_p)$ from which one gets

$$H^1(\boldsymbol{Q}, A_p)_{\text{div}} = S_{A_p}(\boldsymbol{Q})_{\text{div}}. \tag{71}$$

Obviously, these remarks can be made more general. As a simple example,

take $A_p=\boldsymbol{Q}_p/\boldsymbol{Z}_p$ considered as a trivial G_K-module, where $[K:\boldsymbol{Q}]<\infty$. For the same reason as above, elements of $H^1(K, A_p)_{\text{div}}$ automatically satisfy the local triviality condition at the places of K not dividing p. One recovers the familiar fact that only places over p can be ramified in a $\boldsymbol{Z}_p$-extension of K.

III. *Symmetric powers.* Let E be an elliptic curve/$\boldsymbol{Q}$ with good, ordinary reduction at p. The Euler factor in $L_E(s)$ is $(1-\alpha p^{-s})(1-\beta p^{-s})$, where $\alpha\beta=p$. We let β be the unit root for a fixed embedding $\bar{\boldsymbol{Q}}\to\boldsymbol{C}_p$. Let φ and ψ be the characters giving the action of $G_{\boldsymbol{Q}_p}$ on $gr^1(V_p(E))$ and $gr^0(V_p(E))$, respectively. Then $\varphi\psi=\chi_p$. The character ψ is unramified and $\beta=\psi(\text{Frob.})$. For any $n\geq 1$, let $V=\text{Sym}^n(V(E))=\{V_l\}$, where V_l is the n-th symmetric power of the $G_{\boldsymbol{Q}}$-representation space $V_l(E)$. Then p is ordinary for V and the Hodge-Tate numbers $h_i=\dim(gr^i(V_p))$ are 1 for all i, $0\leq i\leq n$. The action of $G_{\boldsymbol{Q}_p}$ on $gr^i(V_p)$ is given by the character $\varphi^i\psi^{n-i}$, Among the Tate twists of V, the critical values are: $L_{V(-k)}(1)$ if $n=2k+1$, $L_{V(-k)}(1)$ and $L_{V(-(k-1))}(1)$ if $n=2k$, k odd. If $4\mid n$, there are no critical values. If n is odd, the value $L_{V(-k)}(1)$ is a central critical value and can vanish. (In fact, we have reason to believe that $\text{ord}_{s=1}(L_{V(-k)}(s))\to\infty$ as $n\to\infty$.) On the other hand, if n is even, the critical values should be nonzero. (Of course, none of the expected analytic properties are known in general for these L-functions.)

For $n=2$, the p-adic L-functions for V and for $V^*=V(-1)$ have been constructed by Coates and Schmidt [3]. For any $n=2k$ with k odd, the conjectured p-adic L-functions attached to $V(-k)$ and $V(-(k-1))$ (which is $V(-k)^*$) should vanish at φ_0 since in the product (10), one of the eigenvalues will be $\alpha^k\beta^k p^{-(k-1)}=p$. Since just this one factor in (10) is zero and since the critical values themselves should be nonzero, one would certainly believe that φ_0 will be a simple zero for each of the p-adic L-functions. Let $A_p=V_p/T_p$ for any choice of $G_{\boldsymbol{Q}}$-invariant lattice T_p. Now $G_{\boldsymbol{Q}_p}$ acts on $gr^0(V_p(-k))$ trivially and on $gr^1(V_p(-(k-1)))$ by χ_p. The corollary to Proposition 9 and the remark at the end of Section 8 show that $S_{A_p(-k)}(\boldsymbol{Q}_\infty)^\Gamma$ and $S_{A_p(-(k-1))}(\boldsymbol{Q}_\infty)^\Gamma$ both have $\boldsymbol{Z}_p$-corank≥ 1. The above remarks suggest that we should have equality. However, based on our experience in classical Iwasawa theory, we would guess that $S_{A_p(-k)}(\boldsymbol{Q})$ and $S_{A_p((-(k-1))}(\boldsymbol{Q})$ are finite groups whose orders are somehow related to the critical values $L_{V(-k)}(1)$ and $L_{V(-(k-1))}(1)$.

IV. *Modular forms.* As an example, consider $L_{f_{12}}(s)=\sum_{n=1}^{\infty}\tau(n)n^{-s}$, where $f_{12}=\sum_{n=1}^{\infty}\tau(n)q^n$ is the normalized cusp form of weight 12, level 1. Let $V=V(f_{12})=\{V_l\}$ be the corresponding compatible system over $\boldsymbol{Q}$, defined by Deligne. We have $d_V=2$, $\text{Ram}(V)=\varnothing$, $\Gamma_V(s)=\Gamma(s)$ and $L_V(s)=L_{f_{12}}(s)$. The functional equation relates $L_{f_{12}}(s)$ and $L_{f_{12}}(12-s)$. The

critical values are $L_{f_{12}}(k)$, $1 \leq k \leq 11$. If $p \nmid \tau(n)$, Mazur and Wiles have proved that there is a filtration on V_p satisfying (1) where the characters of $I_{\mathbf{Q}_p}$ that occur are χ_p^0, χ_p^{11}. (See [31], where a much more general result is proven). One then has a filtration on $V_p(1-k)$. The characters of $I_{\mathbf{Q}_p}$ that occur here are: χ_p^{1-k}, χ_p^{12-k}. Hence $F^+V_p(1-k)$ has dimension equal to 2 for $k \leq 0$, 1 for $1 \leq k \leq 11$, and 0 for $k \geq 12$. This situation seems quite analogous to that for elliptic curves. Conjecture 1 states that $S_{A_p(1-k)}(\mathbf{Q}_\infty)$ should be Λ-cotorsion for $1 \leq k \leq 11$, where, as usual, $A_p = V_p/T_p$ for some choice of lattice T_p. Since the corresponding L-values $L_{V(1-k)}(1) = L_{f_{12}}(k)$ and also the interpolation factor A_{φ_0} are all nonzero, Conjecture 2 implies that $S_{A_p(1-k)}(\mathbf{Q}_\infty)^\Gamma$ and hence $S_{A_p(1-k)}(\mathbf{Q})$ are finite. ($H^0(\mathbf{Q}, A_p(1-k))$ is finite because the $G_\mathbf{Q}$-space V_p is irreducible.) For $k \leq 0$, $S_{A_p(1-k)}(\mathbf{Q}_\infty)$ should have Λ-corank 1, but for $k \geq 12$, it is not clear what to expect. Perhaps they will be finite. If one considers instead the cusp form $f_{26} = \sum a_n q^n$ of weight 26, level 1, then $L_{f_{26}}(13) = 0$ because of the sign in the functional equation. If $V = V(f_{26})$ and if $p \nmid a_p$, then Conjecture 2 implies that $S_{A_p(-12)}(\mathbf{Q})$ is infinite.

Let $p = 691$, $V = V(f_{12})$. The Ramanujan congruence $\tau(l) \equiv 1 + l^{11} \pmod{691}$ implies that $\alpha(1-k) = \{a \in A_p(1-k) \mid pa = 0\}$ is reducible as a $G_\mathbf{Q}$-representation space over $\mathbf{Z}/p\mathbf{Z}$. Up to homothety, one can verify that there are two choices for a $G_\mathbf{Q}$-invariant lattice. Let T_p denote the one which gives the exact sequenc

$$0 \longrightarrow \mu_p^{12-k} \longrightarrow \alpha(1-k) \longrightarrow \mu_p^{1-k} \longrightarrow 0. \tag{72}$$

Let T_p' be the other lattice, $A_p' = V_p/T_p'$, and $\alpha'(1-k)$ the corresponding subgroup of $A_p'(1-k)$ so that

$$0 \longrightarrow \mu_p^{1-k} \longrightarrow \alpha'(1-k) \longrightarrow \mu_p^{12-k} \longrightarrow 0 \tag{73}$$

is exact. One can verify that (72) and (73) do not split as sequences of $G_\mathbf{Q}$-modules.

Assume that $1 \leq k \leq 11$ and that k is odd. Then $\mu_p^{12-k} \subseteq F^+A_p$ and so one has a Λ-homomorphism

$$H^1(\mathrm{Gal}(M_\infty/\mathbf{Q}_\infty), \mu_p^{12-k}) \longrightarrow S_{A_p}(\mathbf{Q}_\infty). \tag{74}$$

which has finite kernel (trivial if $k \neq 1$). Here M_∞ is as in Section 1. The discussion there shows that the first term in (74) is a $(\Lambda/p\Lambda)$-module with corank 1 since $12-k$ is odd. (We use here the known vanishing of Iwasawa's μ-invariant for the Λ-module $\mathrm{Gal}(M_\infty/K_\infty)_{\Lambda\text{-torsion}}$.) As a consequence, it is obvious that the Λ-module $\hat{S}_{A_p(1-k)}(\mathbf{Q}_\infty)$, assuming it is Λ-torsion, will have a positive μ-invariant μ_k, say. According to Perrin-Riou's result in [21], the μ-invariant of $\hat{S}_{A_p'(1-k)}(\mathbf{Q}_\infty)$ is $\mu_k' = \mu_k - 1$. We

believe that it should be zero. (More generally, for any compatible system V, and any odd prime p ordinary for V, it seems reasonable to conjecture that the μ-invariant for $\hat{S}_{V_p/T_p}(\boldsymbol{Q}_\infty)$ will be positive if and only if V_p/T_p contains a $G_{\boldsymbol{Q}}$-submodule α of exponent p such that

$$\dim_{\boldsymbol{Z}/p\boldsymbol{Z}}(\alpha^-)-\operatorname{codim}_{\boldsymbol{Z}/p\boldsymbol{Z}}(F^+\alpha)>0. \tag{75}$$

Here α^- is the (-1)-eigenspace for a complex conjugation in $G_{\boldsymbol{Q}}$ and $F^+\alpha = F^+V_p\cap\alpha$ (which may depend on the choice of place above p). The argument above and the proof of Proposition 6 show that (75) is sufficient.)

For each odd k, $1\leq k\leq 11$, the p-adic L-functions constructed by Manin in [14] and [15] (defined in terms of the critical values $L_{f_{12}}(k,\varphi)$, $\varphi\in\hat{\Gamma}$) turn out to be rather simple when $p=691$ in the following sense. If λ_k is the corresponding element of Λ (for any suitable choice of $\Omega_k = \Omega_{V(1-k)}$), then $\lambda_k = p^a\cdot u$, for some $a\geq 0$ and some $u\in\Lambda^\times$. (We are grateful to Glenn Stevens for proving this for us.) Hence we would expect that (74) is a pseudo-isomorphism and that $S_{A'_p(1-k)}(\boldsymbol{Q}_\infty)$ is finite. Proposition 10 would then apply, showing that (74) is surjective and that

$$S_{A'_p(1-k)}(\boldsymbol{Q}_\infty)=0,\quad 1\leq k\leq 11,\quad k \text{ odd}. \tag{76}$$

If this assertion is true, it would have an interesting consequence, which we now explain.

Suppose $\sigma\in S_{A'_p(1-k)}(\boldsymbol{Q})$ has order p and that $\sigma|_{\boldsymbol{Q}_\infty}$ is nontrivial. There would be a cocycle $\sigma_0\in H^1(\boldsymbol{Q},\alpha'(1-k))$ which is mapped to σ by the inclusion $\alpha'(1-k)\subseteq A'_p(1-k)$. Let $K=\boldsymbol{Q}(\mu_p)$, $\Delta=\operatorname{Gal}(K/\boldsymbol{Q})$. For each $\chi=\omega^i\in\operatorname{Hom}(\Delta,\boldsymbol{Z}_p^\times)$ with i odd, there is a $\boldsymbol{Z}_p$-extension K_∞^χ/K such that $K_\infty^\chi/\boldsymbol{Q}$ is Galois and Δ acts on $\operatorname{Gal}(K_\infty^\chi/K)$ by χ. We let L_χ denote the first layer in K_∞^χ. Then $\operatorname{Gal}(L_\chi/K)\cong\mu_p^i$ as Δ-modules. Using the fact that p $(=691)$ is properly irregular, one can verify that L_χ is the unique extension of K with this property. One then finds that the representation of $G_{\boldsymbol{Q}}$ on $\alpha'(1-k)$ must factor through $G=\operatorname{Gal}(L_{\omega^{-11}}/\boldsymbol{Q})$. The restriction $\sigma_0|G_{L_{\omega^{-11}}}$ (which one verifies still must have order p) determines an extension $M=M_{\sigma_0}$ of $L_{\omega^{-11}}$ and an injective G-homomorphism $\rho_{\sigma_0}: H\to\alpha'(1-k)$, where $H=\operatorname{Gal}(M/L_{\omega^{-11}})$. The extension M/K must be unramified outside the place over p. Also, ρ_{σ_0} must be surjective. Otherwise, $\operatorname{Im}(\rho_{\sigma_0})=\mu_p^{1-k}$, since (73) does not split. If $k=1$, this would imply $\sigma|_{\boldsymbol{Q}_\infty}$ is trivial. For $3\leq k\leq 11$, one would get an extension K' of K with $\operatorname{Gal}(K'/K)\cong\mu_p^{1-k}$, K'/K unramified outside p. But such an extension (for odd k) exists only for $k=-11$, by the spiegelungsatz. (The only nontrivial component $\mathrm{Cl}_p(K)_\chi$ in the p-primary subgroup of the ideal class group of K occurs for $\chi=\omega^{-11}$.) Now the local condition at p which the cocycle σ satisfies implies that the ramification index for any place over p in the extension

$M/L_{\omega-11}$ is at most p. Note that $L_{\omega-11}/K$ is unramified ($L_{\omega-11}$ is the p-Hilbert class field of K). Let $\chi=\omega^{12-k}$. Then M contains L_χ and L_χ/K is ramified at p. It follows that M/L_χ is an unramified, abelian extension of degree p^2. Also $\mathrm{Gal}(M/L_\chi)$ is an extension of μ_p^{1-k} by μ_p^{-11} as a $\mathrm{Gal}(L_\chi/\boldsymbol{Q})$-module. The class number of L_χ must be divisible by p^2.

Conversely, if p^2 divides the class number of L_χ, one would obtain an extension M/L_χ with precisely the above properties (using a genus theory type argument). Reversing the above considerations, one would find that $S_{A'_p(1-k)}(\boldsymbol{Q}_\infty)$ is nontrivial. Assuming, as we expect, that this is not the case we conclude that the fields L_χ ($\chi=\omega^{12-k}$, $1\leq k\leq 11$ and odd) have class number divisible by p, but not by p^2. (Unfortunately, these fields are probably too large for one to verify this prediction.) Consider the natural map of ideal class groups $\mathrm{Cl}(K)\to\mathrm{Cl}(L_\chi)$. If this map were injective, genus theory would imply that p^{e_k+1} divides $|\mathrm{Cl}(L_\chi)|$, where e_k is the order of the character χ. Our prediction would force the "capitulation" of $\mathrm{Cl}_p(K)$ (which has order p) in L_χ and hence in K_∞^χ.

Consider a $\boldsymbol{Z}_p^d$-extension K_∞ of K (i.e. $\Gamma=\mathrm{Gal}(K_\infty/K)\cong\boldsymbol{Z}_p^d$, $d\geq 1$). Let $\mathrm{Iw}(K_\infty)$ denote the classical Iwasawa module for K_∞: $\mathrm{Iw}(K_\infty)=\mathrm{Gal}(L_\infty/K_\infty)$, where L_∞ is the maximal, abelian, unramified, pro-p extension of K_∞. It is a Λ-module, where $\Lambda=\boldsymbol{Z}_p[[\Gamma]]$ (which is isomorphic to the formal power series ring $\boldsymbol{Z}_p[[T_1, T_2, \cdots, T_d]]$). Assuming (76) and using standard arguments in Iwasawa theory (see [5], [6], and [20]; one is helped by the fact that the unique place of K over p is totally ramified in K_∞^χ), we come to the following (conjectural) conclusions: Let $p=691$, $\chi=\omega^{12-k}$, $1\leq k\leq 11$ and odd. Then $\mathrm{Iw}(K_\infty^\chi)$ should be finite. If K_∞ is any $\boldsymbol{Z}_p^d$-extension of K containing K_∞^χ for one of the above k's (in particular the compositum of all $\boldsymbol{Z}_p$-extensions of K, for which $d=(p+1)/2$), then the Λ-module $\mathrm{Iw}(K_\infty)$ should be pseudo-null.

References

[1] J. Coates, R. Greenberg, Iwasawa theory for abelian varieties, in preparation.

[2] J. Coates, B. Perrin-Riou, On p-adic L-functions attached to motives over $\boldsymbol{Q}$, this volume.

[3] J. Coates and C. G. Schmidt, Iwasawa theory for the symmetric square of an elliptic curve, J. Reine Angew. Math., **375** (1987), 104–156.

[4] P. D. Deligne, Valeurs de fonctions L et périodes d'intégrales, Automorphic Forms, Representations and L-functions, Proc. Symp. Pure Math., **33** (1979), 313–346.

[5] R. Greenberg, The Iwasawa invariants of Γ-extensions of a fixed number field, Amer. J. Math., **95** (1973), 204–214.

[6] ——, On the Iwasawa invariants of totally real number fields, Amer. J. Math., **98** (1976), 263–284.

[7] ——, On p-adic L-functions and cyclotomic fields II, Nagoya Math. J., **67** (1977), 139–158.

[8] ——, Trivial zeros of p-adic L-functions, in preparation.

[9] K. Haberland, Galois cohomology of algebraic number fields, Deutscher Verlag der Wissenschaften, Berlin (1978).
[10] G. Hochschild and J. P. Serre, Cohomology of group extensions, Trans. Amer. Math. Soc., **74** (1953), 110–134.
[11] K. Iwasawa, Lectures on p-adic L-functions, Ann. Math. Studies **74**, Princeton University Press (1972).
[12] ——, On Z_l-extensions of algebraic number fields, Ann. of Math., **98** (1973), 246–326.
[13] J. Jones, Iwasawa theory at multiplicative primes, Thesis (1987), Harvard University.
[14] J. Manin, Periods of parabolic forms and p-adic Hecke series, Math. Sbornik, **92** (1973), 371–393.
[15] ——, The values of p-adic Hecke series at integer points of the critical strip, Math. Sbornik, **93** (1974), 631–637.
[16] B. Mazur, Rational points of abelian varieties with values in towers of number fields, Invent. Math., **18** (1972), 183–266.
[17] B. Mazur and P. Swinnerton-Dyer, Arithmetic of Weil Curves, Invent. Math., **25** (1974), 1–61.
[18] B. Mazur, J. Tate and J. Teitelbaum, On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer, Invent. Math., **84** (1986), 1–48.
[19] B. Mazur and A Wiles, Class fields of abelian extensions of $\boldsymbol{Q}$, Invent. Math., **76** (1984), 179–330.
[20] J. Minardi, Iwasawa modules for Z_p^d-extensions of algebraic number fields, Thesis (1986), University of Washington.
[21] B. Perrin-Riou, Variation de la fonction L p-adique par isogénie, this volume.
[22] D. Rohrlich, On L-functions of elliptic curves and cyclotomic towers, Invent. Math., **75** (1984), 409–423.
[23] K. Rubin, On the main conjecture of Iwasawa theory for imaginary quadratic fields, Invent. Math., **93** (1988), 701–713.
[24] C. G. Schmidt, p-Adic L-functions attached to automorphic representations of $GL(3)$, Invent. Math., **92** (1988), 597–631.
[25] P. Schneider, Motivic Iwasawa theory, this volume.
[26] J. P. Serre, Facteurs locaux des fonctions zeta des variétés algébriques (définitions et conjectures), Sem. Delange-Pisot-Poitou, (1969/70), exp. 19.
[27] ——, Cohomologie galoisienne, Lecture Notes in Math., **5**, Springer (1964).
[28] G. Stevens, Stickelberger elements and modular parametrizations of elliptic curves, to appear.
[29] J. Tate, Duality theorems in Galois cohomology over number fields, Proc. Inter. Congress 1962, 288–295.
[30] ——, p-Divisible groups, Proceedings of a conference on local fields, Springer-Verlag (1967), 158–183.
[31] A. Wiles, On ordinary λ-adic representations associated to modular forms, Invent. Math., **94** (1988), 529–573.
[32] K. Wingberg, Duality theorems for Γ-extensions of algebraic number fields, Compositio Math., **55** (1985), 333–381.

Department of Mathematics
Brandeis University
Waltham, MA 02154
U.S.A.