J. DIFFERENTIAL GEOMETRY
70 (2005) 1-22

FINDING LARGE SELMER GROUPS

Barry Mazur & Karl Rubin

Abstract

In this paper, we show how to use a recent theorem of Nekovář [12] to produce families of examples of elliptic curves over number fields whose p-power Selmer groups grow systematically in $\mathbf{Z}_p^d$-extensions. We give a somewhat different exposition and proof of Nekovář's theorem, and we show in many cases how to replace the fundamental requirement that the elliptic curve has odd p-Selmer rank by a root number calculation.

1. Introduction

Raoul Bott has inspired many of us by the magnificence of his ideas, by the way he approaches and explains mathematics, and by his warmth, friendship, and humor. In celebration of Raoul's eightieth birthday, we offer this brief article in which we will give an exposition of a theorem of Jan Nekovář. We will explain how the recent cohomological ideas of Nekovář [12] imply (under mild hypotheses plus the Shafarevich–Tate conjecture) systematic growth of the ranks of the group of rational points on certain elliptic curves as one ascends the finite layers of appropriate towers of number fields.

Let K/k be a quadratic extension of number fields, and denote by σ the non-trivial automorphism of K/k. Let p be an odd prime number.

By a $\mathbf{Z}_p$-power extension of K, we mean an abelian extension L/K with Galois group $\mathbf{Z}_p^d$ for some d. If L/K is a $\mathbf{Z}_p$-power extension and L/k is Galois, then σ acts on $\mathrm{Gal}(L/K)$ and we will say that L/K is *k-positive* (resp. *k-negative*) if σ acts trivially (resp. by the scalar -1) on $\mathrm{Gal}(L/K)$. Thus L/k is abelian if L/K is k-positive, and $\mathrm{Gal}(L/k)$ is a generalized dihedral group if L/K is k-negative.

For any such K/k, there is a *maximal* k-positive $\mathbf{Z}_p$-power extension $\mathcal{K}^+$, and a *maximal* k-negative one $\mathcal{K}^-$. The extension $\mathcal{K}^+/K$ is always

The authors are supported by NSF grants DMS-0403374 and DMS-0140378, respectively.
Received 03/15/2005.

non-trivial because $\mathcal{K}^+$ contains the cyclotomic $\mathbf{Z}_p$-extension of K. The extension $\mathcal{K}^-/K$ is non-trivial if K is not totally real (see Lemma 3.2).

If E is an elliptic curve defined over K and L is a (possibly infinite) extension of K, say that E has *Mordell–Weil growth relative to* L/K if for every finite extension F of K in L, the rank of the Mordell–Weil group $E(F)$ is at least $[F : K]$. In particular, if $[L : K]$ is infinite, this property will imply that the Mordell–Weil rank of E over L is infinite. Say that E has *p-Selmer growth relative to* L/K if the pro-p-Selmer rank of E over F is at least $[F : K]$ for all finite extensions F of K in L.

Recent work of Nekovář ([**12**], especially Section 10.7; note that this is unpublished, but available on the indicated website) shows that under extremely mild hypotheses, if E is an elliptic curve over k that has odd pro-p-Selmer rank over K and that is of good ordinary reduction at the primes above p, then E has p-Selmer growth relative to $\mathcal{K}^-/K$. Assuming the Shafarevich–Tate conjecture, this is equivalent to the statement that (under the same hypotheses) if E has odd Mordell–Weil rank over K, then it has Mordell–Weil growth relative to $\mathcal{K}^-/K$.

In this paper we do two things. First, we give a somewhat different exposition of Nekovář's theorem, in the hope of making this important result more accessible and widely known. Namely, we will show how to derive Nekovář's theorem (Theorem 3.1 below) from the main result of [**10**] (which in turn relies crucially on [**12**]) using a pair of functional equations satisfied by an "algebraic" p-adic L-function attached to E over K.

Second, we describe some conditions (Corollary 3.6) under which we can prove that the pro-p-Selmer rank and/or the Mordell–Weil rank of E over K are necessarily odd, so that we can apply Theorem 3.1. This enables us to give families of examples (see Section 5) of $\mathbf{Z}_p^d$-extensions with p-Selmer growth.

An important instance of the above setup is when K is an imaginary quadratic field, $k = \mathbf{Q}$, and σ is complex conjugation. In this case, $\mathcal{K}^+$ is the cyclotomic $\mathbf{Z}_p$-extension of K and $\mathcal{K}^-$ is the anti-cyclotomic $\mathbf{Z}_p$-extension of K. The results of Cornut, Vatsal, and Nekovář [**2**, **17**, **11**] show that if E is defined over $\mathbf{Q}$, E has good ordinary reduction at p, and the pro-p Selmer rank of E over K is odd, then E has Selmer growth relative to $\mathcal{K}^-/K$. (See also the recent preprint [**3**] of Cornut and Vatsal generalizing their work to CM-fields.)

There are other prior results that unconditionally imply p-Selmer growth or positive p-Selmer rank. Greenberg proved in [**5**] that if E is an elliptic curve over $\mathbf{Q}$ with complex multiplication by K, $p > 3$ is a prime of good ordinary reduction for E, and $\operatorname{ord}_{s=1} L(E/\mathbf{Q}, s)$ is

odd, then E has p-Selmer growth relative to $\mathcal{K}^-/K$. Skinner and Urban prove in a recent preprint [16] that given a p-ordinary classical newform of arbitrary weight at least 2 and of odd analytic rank over an imaginary quadratic field K, and satisfying some mild conditions, its p-Selmer rank over K is positive.

Most of the work in this article is on the "algebraic," rather than the "analytic," aspect of the arithmetic. However, the motivation for our work is analytic, in the sense that our main result would follow fairly directly from a generalized version of the Parity conjecture. Namely, if F is a finite extension of K in $\mathcal{K}^-$ and ψ is a character of $\mathrm{Gal}(F/K)$, the Parity conjecture gives the first and last congruences

$$\begin{aligned}\mathrm{rank}(E(K)) &\equiv \mathrm{ord}_{s=1}L(E/K,s) \equiv \mathrm{ord}_{s=1}L(E/K,\psi,s)\\ &\equiv \text{multiplicity of } \psi \text{ in } E(F)\otimes\mathbf{C} \pmod 2\end{aligned}$$

and the middle one is a root number calculation. Our result (if we assume the Shafarevich–Tate conjecture) is the weaker implication that for every such ψ

$$\mathrm{rank}(E(K)) \text{ is odd} \Rightarrow \text{the multiplicity of } \psi \text{ in } E(F)\otimes\mathbf{C} \text{ is positive.}$$

See Corollary 3.6 for special cases in which we can replace our "odd rank" assumption by a root number assumption (i.e., a congruence condition on the conductor of $E/\mathbf{Q}$).

We conclude this introduction with two potential generalizations of the results of this paper.

First, in general $L(E/K,s)$ will factor into a product of L-functions. It is possible that $\mathrm{ord}_{s=1}L(E/K,s)$ is even because an even number of the factors have odd-order vanishing. In this case, we expect that $\mathrm{rank}(E(K))$ is even, so the results of this paper would not apply. However, we expect that the individual factors of $L(E/K,s)$ that vanish will contribute $\mathbf{Z}_p$-power extensions of L/K where E has p-Selmer growth. This should lead to examples in which the pro-p-Selmer rank of E over F is at least $r[F:K]$ for every finite extension F of K in L, with $r>1$.

Second, the results of this paper for Selmer groups of elliptic curves should also apply to Selmer groups of (classical) p-ordinary newforms of arbitrary even weight $k\geq 2$.

We hope to deal with these generalizations in a future paper, by refining the results of [10] and combining those refined results with the methods of this paper.

2. The setting

Fix an elliptic curve E defined over a number field k, and a rational prime $p > 2$. For every finite extension F of k, we have the p-power Selmer group

$$\mathrm{Sel}_p(E,F) := \ker\biggl(H^1(F, E[p^\infty]) \longrightarrow \prod_v H^1(F_v, E)\biggr),$$

where $E[p^\infty]$ is the Galois module of p-power torsion on E, and the product is over all places v of F. This Selmer group sits in an exact sequence

$$0 \longrightarrow E(F) \otimes \mathbf{Q}_p/\mathbf{Z}_p \longrightarrow \mathrm{Sel}_p(E,F) \longrightarrow Ш(E,F)[p^\infty] \longrightarrow 0$$

where $Ш(E,F)[p^\infty]$ is the p-primary part of the Shafarevich–Tate group of E over F. If F is an arbitrary algebraic extension of $\mathbf{Q}$, we define

$$\mathrm{Sel}_p(E,F) := \varinjlim \mathrm{Sel}_p(E,F'),$$

direct limit (with respect to restriction maps on Galois cohomology) over finite extensions F' of k in F, and the Pontrjagin dual

$$\mathcal{S}_p(E,F) := \mathrm{Hom}(\mathrm{Sel}_p(E,F), \mathbf{Q}_p/\mathbf{Z}_p).$$

Throughout this paper, if M is a module over an integral domain R, the R-rank of M will be defined by

$$\mathrm{rank}_R(M) := \dim_{\mathrm{Frac}(R)} M \otimes_R \mathrm{Frac}(R),$$

where $\mathrm{Frac}(R)$ is the field of fractions of R.

Fix a quadratic extension K of k and let σ denote the non-trivial automorphism of K/k. Let $\mathcal{K}$ denote the maximal $\mathbf{Z}_p$-power extension of K (the compositum of all $\mathbf{Z}_p$-extensions of K) and $\Gamma := \mathrm{Gal}(\mathcal{K}/K)$. Then $\mathcal{K}$ is Galois over k, and so σ acts on Γ. We let $\Gamma^\pm$ denote the subgroup of Γ on which σ acts by ± 1, and let $\mathcal{K}^\pm$ be the fixed field of $\Gamma^\mp$, so that $\mathrm{Gal}(\mathcal{K}^\pm/K) \cong \Gamma^\pm$. Then $\mathcal{K}^+$ is the maximal k-positive $\mathbf{Z}_p$-power extension of K, and $\mathcal{K}^-$ is the maximal k-negative one, as discussed in the introduction. Putting $d_\pm := \mathrm{rank}_{\mathbf{Z}_p}(\Gamma^\pm)$, Leopoldt's conjecture for K implies that $d_+ = r_2(k) + 1$ and $d_- = r_2(K) - r_2(k)$, where r_2 denotes the number of conjugate pairs of complex embeddings of a number field.

For example, if K is an imaginary quadratic field, then $k = \mathbf{Q}$, Leopoldt's conjecture trivially holds for K, $d_+ = d_- = 1$ and $\mathcal{K}^+$ and $\mathcal{K}^-$ are the usual cyclotomic and anticyclotomic $\mathbf{Z}_p$-extensions of K.

If K_v is the completion of K at a prime v, we denote by $E_0(K_v)$ the subgroup consisting of points of $E(K_v)$ with non-singular reduction,

so $[E(K_v) : E_0(K_v)]$ is the Tamagawa number at v in the Birch and Swinnerton–Dyer conjecture for E/K.

We will assume the following throughout this paper:

Assumptions 2.1. (i) $p > 2$ and E has good ordinary reduction at all primes of K above p,
(ii) $E(K)$ has no p-torsion,
(iii) for every prime v of K of bad reduction, $[E(K_v) : E_0(K_v)]$ is prime to p.

3. Results

The following theorem is essentially Nekovář's Theorem 10.7.17 [12].

Theorem 3.1.
Suppose that Assumptions 2.1 hold. If $\mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E,K))$ *is odd, then*

(i) $\mathcal{S}_p(E,\mathcal{K}^-)$ *is not a torsion* $\mathbf{Z}_p[[\Gamma^-]]$*-module,*
(ii) *for every finite extension* F *of* K *in* $\mathcal{K}^-$ *the Selmer module* $\mathcal{S}_p(E,F)$ *has a submodule isomorphic to* $\mathbf{Z}_p[\mathrm{Gal}(F/K)]$*, and in particular*

$$\mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E,F)) \geq [F:K].$$

In fact, Theorem 10.7.17 of [12] asserts that the $\mathbf{Z}_p[[\Gamma^-]]$-rank of $\mathcal{S}_p(E,\mathcal{K}^-)$ is odd, while Theorem 3.1 only says that the rank is positive.

We will give a proof of Theorem 3.1 in Section 11. Our method is to show that there is an "algebraic p-adic L-function" satisfying two different functional equations (see Corollary 10.2), and taken together, these functional equations imply the theorem.

See Proposition 4.1 below for an explanation of why one would expect a result like Theorem 3.1 to hold.

Theorem 3.1(ii) says that E has p-Selmer growth relative to $\mathcal{K}^-/K$, using the terminology of the introduction. The following lemma shows that this statement is often non-trivial.

Lemma 3.2. *If* K *is not totally real, then* $[\mathcal{K}^- : K]$ *is infinite.*

Proof. We need to show that d_- is positive. Class field theory shows that $d_- \geq r_2(K) - r_2(k)$ (with equality if Leopoldt's conjecture holds), and we have $r_2(K) \geq 2r_2(k)$ since each complex place of k splits in K. Therefore, if K is not totally real, then $r_2(K) > r_2(k)$ and $d_- > 0$. q.e.d.

Before providing a corollary of Theorem 3.1, we recall two well-known conjectures. Let $\mathbf{Q}_\infty$ denote the (cyclotomic) $\mathbf{Z}_p$-extension of $\mathbf{Q}$.

p-primary Shafarevich–Tate Conjecture. *For every finite extension F of K in $\mathcal{K}$, the p-part $Ш(E,F)[p^\infty]$ of the Shafarevich–Tate group of E over F is finite.*

Torsion Conjecture ([8]). *The Selmer module $\mathcal{S}_p(E, K\mathbf{Q}_\infty)$ is a torsion $\mathbf{Z}_p[[\mathrm{Gal}(K\mathbf{Q}_\infty/K)]]$-module.*

Remark 3.3. If $Ш(E,F)[p^\infty]$ is finite, then there is a canonical identification $\mathcal{S}_p(E,F) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p = E(F) \otimes_{\mathbf{Z}} \mathbf{Q}_p$. Thus, if the p-primary Shafarevich–Tate conjecture holds, then in Theorem 3.1 and the corollaries below we can replace the Selmer groups $\mathcal{S}_p(E,K)$ and $\mathcal{S}_p(E,F)$ by the Mordell–Weil groups $E(K)$ and $E(F)$ (and replace $\mathrm{rank}_{\mathbf{Z}_p}$ by $\mathrm{rank}_{\mathbf{Z}}$).

Remark 3.4. If the Torsion conjecture holds, then Theorem 3.1 cannot hold with $\mathcal{K}^-$ replaced by either $\mathcal{K}^+$ or $\mathcal{K}$ (see Corollary 6.5).

Corollary 3.5.
Suppose that Assumptions 2.1 hold and $\mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E,K))$ is odd.

(i) *If K is not totally real then $\mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E,F))$ is unbounded as F runs through finite extensions of K in $\mathcal{K}$.*

(ii) *More generally, if L is a $\mathbf{Z}_p^d$-extension of K that is Galois but not abelian over k, then $\mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E,F))$ is unbounded as F runs through finite extensions of K in L.*

Proof. Assertion (i) is immediate from Theorem 3.1 and Lemma 3.2. For (ii), we have that σ acts on $\mathrm{Gal}(L/K)$ with (at least one) eigenvalue -1, so $L \cap \mathcal{K}^-$ has infinite degree over K. Thus assertion (ii) follows directly from Theorem 3.1(ii). q.e.d.

The following corollary applies when the elliptic curve E is defined over $\mathbf{Q}$, and K is Galois over $\mathbf{Q}$. It replaces the condition "$\mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E,K))$ is odd" by group-theoretic conditions on $\mathrm{Gal}(K/\mathbf{Q})$ and congruence conditions on the conductor of E. We will deduce this corollary from Theorem 3.1 in Section 11, by showing that its hypotheses imply that $\mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E,K))$ is odd.

Corollary 3.6. *Suppose that Assumptions 2.1 hold, and that*

(a) *E is defined over $\mathbf{Q}$ and K is a Galois extension of $\mathbf{Q}$ whose discriminant is relatively prime to the conductor N_E of E,*

(b) *$\mathrm{Gal}(K/\mathbf{Q})$ is the semidirect product of a (normal) subgroup of odd order with a non-trivial cyclic 2-group,*

(c) *either the p-primary Shafarevich–Tate conjecture holds, or every irreducible $\mathbf{Q}_p$-representation of $\mathrm{Gal}(K/\mathbf{Q})$ not factoring through the unique quotient of order 2 has even dimension,*

(d) *the Dirichlet character χ corresponding to the (unique) quadratic field contained in K satisfies $\chi(-N_E) = -1$.*

Then for every subfield k of K with $[K : k] = 2$, if $\mathcal{K}^-$ is the maximal k-negative $\mathbf{Z}_p$-power extension of K,

(i) *$\mathcal{S}_p(E, \mathcal{K}^-)$ is not a torsion $\mathbf{Z}_p[[\Gamma^-]]$-module,*

(ii) *for every finite extension F of K in $\mathcal{K}^-$, $\mathcal{S}_p(E, F)$ has a submodule isomorphic to $\mathbf{Z}_p[\mathrm{Gal}(F/K)]$, and in particular,*

$$\mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E, F)) \geq [F : K].$$

Remark 3.7. Under hypothesis (b) of Corollary 3.6, all elements of order 2 are conjugate in $\mathrm{Gal}(K/\mathbf{Q})$, and hence the different possible $\mathcal{K}^-/K$ are conjugate.

4. Aside on root numbers

Although we will not need it, the following proposition on root numbers explains why Theorem 3.1 and Corollary 3.6 are consistent with standard conjectures.

If ψ is a character of $\mathrm{Gal}(\bar{K}/K)$, we denote by $W(E/K, \psi)$ the root number corresponding to the L-function $L(E/K, \psi, s)$, as defined (for example) in [4] or [15]. When ψ is the trivial character, we write simply $W(E/K)$. Note that although the analytic continuation and functional equation of $L(E/K, \psi, s)$ are known only in very special cases, the root number is always defined.

Proposition 4.1. *Suppose that $p > 2$, E has good reduction at all primes above p and all primes ramified in $K/\mathbf{Q}$, and*

$$\psi \in \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\mathcal{K}^-/K), \mathbf{C}^\times).$$

(i) *The induced representation $\mathrm{Ind}_k^K \psi$ is real valued and the root number $W(E/K, \psi)$ is independent of ψ, and hence equal to $W(E/K)$.*

(ii) *Suppose that hypotheses* (a), (b), *and* (d) *of Corollary 3.6 are satisfied. Then, $\mathrm{Ind}_{\mathbf{Q}}^K \psi$ is real valued and $W(E/K, \psi) = -1$.*

Proposition 4.1 is essentially proved in [9] Section 2.2. We will recall the proof in Section 12.

Remark 4.2. If F is a finite Galois extension of K and ψ is a complex character of $\mathrm{Gal}(F/K)$, then a suitably general version of the Birch and Swinnerton–Dyer conjecture would predict that the multiplicity of ψ in the representation $E(F) \otimes \mathbf{C}$ is the order of vanishing of $L(E/K, \psi, s)$ at $s = 1$. When $\mathrm{Ind}_{\mathbf{Q}}^K \psi$ is real valued, the conjectured functional equation relates $L(E/K, \psi, s)$ to $L(E/K, \psi, 2 - s)$ and implies that this order of vanishing is even if $W(E/K, \psi) = 1$, and odd if $W(E/K, \psi) = -1$.

Thus (using Proposition 4.1) under the hypotheses of Theorem 3.1 and Corollary 3.6 one expects that for every finite extension F of K in $\mathcal{K}^-$ and every character ψ of $\mathrm{Gal}(F/K)$, ψ occurs in $E(F) \otimes \mathbf{C}$. Theorem 3.1 and Corollary 3.6 show that this expectation is correct, at least if we replace assume that $Ш(E,F)[p^\infty]$ is finite for all such F.

Remark 4.3. There is a partial converse to Proposition 4.1. Namely, suppose that ψ is a character of finite order of $\Gamma := \mathrm{Gal}(\mathcal{K}/K)$. Suppose further that ψ is generic, in the sense that ψ is not the restriction to K of a character of a $\mathbf{Z}_p$-extension of a proper subfield of K. Then the induced representation $\mathrm{Ind}_{\mathbf{Q}}^K \psi$ is real-valued if and only if there is an involution σ of K such that $\psi^\sigma = \psi^{-1}$ (see Proposition 2.5 of [**9**]).

Now suppose in addition that E is defined over $\mathbf{Q}$, the discriminant of K is relatively prime to the conductor E, and K is Galois over $\mathbf{Q}$. Then $W(E/K,\psi) = -1$ if and only if hypotheses (b) and (d) of Corollary 3.6 are satisfied (this is Theorem 2.8 and Proposition 2.9 of [**9**]).

When K is not Galois over $\mathbf{Q}$ the situation is more complicated. We plan to discuss this, and the further implications for p-Selmer growth related to odd parity functional equations, in a future paper.

5. Examples

Example 5.1. Let K be an abelian extension of $\mathbf{Q}$ containing a unique quadratic field (i.e., $\Delta := \mathrm{Gal}(K/\mathbf{Q})$ is an abelian group with non-trivial cyclic 2-part). Then Δ satisfies hypothesis (b) of Corollary 3.6. Let σ be the unique element of order 2 in Δ, and k the fixed field of σ. We will assume that K is imaginary, for if K is real, then the cyclotomic $\mathbf{Z}_p$-extension is the only $\mathbf{Z}_p$-extension of K. Thus σ is complex conjugation and k is the real subfield of K. Let χ be the quadratic character of Δ.

Since Leopoldt's conjecture holds for K, we have $\mathcal{K}^+ = K\mathbf{Q}_\infty$, so $d_+ = 1$, and $\mathcal{K}^-/K$ is a $\mathbf{Z}_p^{d_-}$-extension with $d_- = r_2(K) = [K:\mathbf{Q}]/2$.

Let E be an elliptic curve over $\mathbf{Q}$ with good ordinary reduction at p, satisfying Assumptions 2.1, with conductor N_E prime to the discriminant of K, and such that $\chi(-N_E) = -1$.

By Corollary 3.6, if the p-primary Shafarevich–Tate conjecture holds, then we have that the Selmer module $\mathcal{S}_p(E,\mathcal{K}^-)$ is a non-torsion $\mathbf{Z}_p[[\Gamma^-]]$-module and $\mathrm{rank}_{\mathbf{Z}}(E(F)) \geq [F:K]$ for all finite extensions F of K in $\mathcal{K}^-$.

Now suppose further that p has even order in $(\mathbf{Z}/\ell\mathbf{Z})^\times$ for every odd prime ℓ dividing $[K:\mathbf{Q}]$, and either $p \equiv 3 \pmod 4$ or 4 does not divide $[K:\mathbf{Q}]$. Then, hypothesis (c) of Corollary 3.6 holds even without the assumption that the p-primary Shafarevich–Tate conjecture

holds. Thus, in this case, we conclude unconditionally that $\mathcal{S}_p(E, \mathcal{K}^-)$ is a non-torsion $\mathbf{Z}_p[[\Gamma^-]]$-module and $\mathrm{rank}_{\mathbf{Z}}(\mathcal{S}_p(E, F)) \geq [F : K]$ for all finite extensions F of K in $\mathcal{K}^-$.

If K is an imaginary quadratic field, then $\mathcal{K}^-$ is the anticyclotomic $\mathbf{Z}_p$-extension of K and the conclusions of Corollary 3.6 were already known by work of Vatsal [17] and Cornut [2].

Example 5.2. Suppose K is a complex Galois extension of $\mathbf{Q}$ with

$$\Delta := \mathrm{Gal}(K/\mathbf{Q}) \cong S_3.$$

Note that Δ satisfies hypotheses (b) and (c) of Corollary 3.6. Let M denote the (imaginary) quadratic extension of $\mathbf{Q}$ in K, and χ the Dirichlet character corresponding to $M/\mathbf{Q}$. Leopoldt's conjecture holds for K (for group-theoretic reasons), so $\Gamma := \mathrm{Gal}(\mathcal{K}/K) \cong \mathbf{Z}_p^4$.

Let $\sigma \in \Delta$ be one of the elements of order 2 and k_σ its fixed field. The (non-Galois) cubic field k_σ has one pair of complex embeddings, so $d_- = r_2(K) - r_2(k_\sigma) = 2$. Hence for each such σ there is a (unique) $\mathbf{Z}_p^2$-extension $\mathcal{K}_\sigma^-$ of K, each containing the anticyclotomic $\mathbf{Z}_p$-extension of M.

Let E be an elliptic curve over $\mathbf{Q}$ with good ordinary reduction at p, satisfying Assumptions 2.1, with conductor N_E prime to the discriminant of K, and such that $\chi(-N_E) = -1$.

We conclude by Corollary 3.6 that for each of the three elements $\sigma \in \Delta$ of order 2, the Selmer module $\mathcal{S}_p(E, \mathcal{K}_\sigma^-)$ is not $\mathbf{Z}_p[[\mathrm{Gal}(\mathcal{K}_\sigma^-/K)]]$-torsion, and for every finite extension F of K in $\mathcal{K}_\sigma^-$ we have

$$\mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E, F)) \geq [F : K].$$

(Note that the three $\mathbf{Z}_p^2$-extensions $\mathcal{K}_\sigma^-$ are isomorphic over K, and hence the three Selmer modules $\mathcal{S}_p(E, \mathcal{K}_\sigma^-)$ are isomorphic as well.)

Example 5.3. Suppose K' is a complex Galois extension of $\mathbf{Q}$ with

$$\Delta := \mathrm{Gal}(K'/\mathbf{Q}) \cong S_4.$$

Note that Δ does *not* satisfy hypothesis (b) of Corollary 3.6. Let H be a subgroup of order 2 in Δ, generated by a 2-cycle (so, $H \not\subset A_4$) and let K be the fixed field of H in K'. Let $\sigma \in \Delta - H$ be an element in the normalizer of H, so σ is an automorphism of K of order 2, and let k be the fixed field of σ. One can check that K has 5 pairs of complex embeddings if the complex conjugations in Δ are 2-cycles, and 6 otherwise; k has 2 pairs of complex embeddings in either case.

Assume that Leopoldt's conjecture holds for K. The discussion above shows that $\Gamma := \mathrm{Gal}(\mathcal{K}/K) \cong \mathbf{Z}_p^n$ where n is 6 or 7, and $\Gamma^- := \mathrm{Gal}(\mathcal{K}^-/K)$ has $\mathbf{Z}_p$-rank 3 or 4.

Let E be an elliptic curve over $\mathbf{Q}$, with good ordinary reduction at p, satisfying Assumptions 2.1, with conductor N_E prime to the discriminant of K. It follows from Theorem 2.8 of [9] (or see the proof of Proposition 4.1) that the root number of $L(E/K, s)$ is $\chi(-N_E)$, where χ is the quadratic Dirichlet character corresponding to the fixed field of A_4 in K.

Assume now $\chi(-N_E) = -1$. Then conjecturally $\operatorname{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E, K))$ is odd, and if so, we can use Theorem 3.1 to conclude that the Selmer module $\mathcal{S}_p(E, \mathcal{K}^-)$ is not $\mathbf{Z}_p[[\Gamma^-]]$-torsion, and that for every finite extension F of K in $\mathcal{K}^-$, we have $\operatorname{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E, F)) \geq [F : K]$.

Unfortunately, unlike the situation of Corollary 3.6, we have no general way to show that $\operatorname{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E, K))$ is odd. We do know (using Nekovář's parity theorem [11]) that $\operatorname{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E, M))$ is odd, where M is the (quadratic) fixed field of A_4 in K, but $M \not\subset K$ so there is no apparent way to relate the parity of $\operatorname{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E, K))$ to that of $\operatorname{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E, M))$.

6. The control theorem

Define the Iwasawa algebra

$$\Lambda := \mathbf{Z}_p[[\Gamma]].$$

If $K \subset F \subset \mathcal{K}$, we let $\Lambda_F := \mathbf{Z}_p[[\mathrm{Gal}(F/K)]]$ denote the corresponding quotient of Λ, and $I_F \subset \Lambda$ the corresponding augmentation ideal:

$$0 \longrightarrow I_F \longrightarrow \Lambda \longrightarrow \Lambda_F \longrightarrow 0.$$

Thus I_F is generated by $\{\gamma - 1 : \gamma \in \mathrm{Gal}(\mathcal{K}/F)\}$.

Suppose that either

(i) F is a $\mathbf{Z}_p^d$-extension of K in $\mathcal{K}$ and $R := \Lambda_F$, or
(ii) F is an arbitrary extension of K in $\mathcal{K}$ and $R := \Lambda_F \otimes \mathbf{Q}_p$.

In case (i) R is an integrally closed noetherian domain, and in case (ii) R is a direct sum of integrally closed noetherian domains. If M is a finitely generated torsion R-module, we let $\operatorname{char}_R(M)$ denote the characteristic ideal of M, called the divisor of M in [1] Chapter VII, Section 4.5. (In case (ii), we make this definition component-by-component.) If (some component of) M is not torsion, we set (that component of) $\operatorname{char}_R(M)$ equal to zero. Then M has a submodule isomorphic to R if and only if $\operatorname{char}_R(M) = 0$.

The following "control theorem" is due to Greenberg ([6] Theorem 2).

Theorem 6.1. *Suppose that $K \subset F \subset L \subset \mathcal{K}$, and F/K is finite. Then the natural map*

$$\mathcal{S}_p(E, L) \otimes_{\Lambda_L} \Lambda_F \longrightarrow \mathcal{S}_p(E, F)$$

(*induced by the restriction map* $\mathrm{Sel}_p(E,F) \to \mathrm{Sel}_p(E,L)^{\mathrm{Gal}(L/F)}$) *has finite kernel and cokernel. In particular*

$$\mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E,F)) = \mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E,\mathcal{K}) \otimes_\Lambda \Lambda_F).$$

Corollary 6.2. *The Λ-module $\mathcal{S}_p(E,\mathcal{K})$ is finitely generated.*

Proof. Since $\mathcal{S}_p(E,K)$ is finitely generated over $\mathbf{Z}_p$, this is immediate from Theorem 6.1 and Nakayama's Lemma. q.e.d.

Lemma 6.3. *Suppose $K \subset F \subset L \subset \mathcal{K}$, L/K is a $\mathbf{Z}_p$-power extension, and M is a finitely generated Λ_L-module. Let $M_F := M \otimes_{\Lambda_L} \Lambda_F$.*

(i) *M_F is a finitely generated Λ_F-module.*
(ii) $\mathrm{char}_{\Lambda_F \otimes \mathbf{Q}_p}(M_F \otimes \mathbf{Q}_p) \subset \mathrm{char}_{\Lambda_L}(M)(\Lambda_F \otimes \mathbf{Q}_p)$.
(iii) *If $\mathrm{char}_{\Lambda_L}(M) \subset I_F\Lambda_L$, then M_F has a submodule isomorphic to Λ_F.*

Proof. The first assertion is clear.

For (ii), since $\mathrm{char}_{\Lambda_L \otimes \mathbf{Q}_p}(M \otimes \mathbf{Q}_p) = \mathrm{char}_{\Lambda_L}(M) \otimes \mathbf{Q}_p$, we can reduce by induction to the case that L/F is a $\mathbf{Z}_p$-extension. In that case, (ii) follows from Lemmas 2 and 4 of Section I.1 of [**13**].

If $\mathrm{char}_{\Lambda_L}(M) \subset I_F\Lambda_L$, then by (ii), $\mathrm{char}_{\Lambda_F \otimes \mathbf{Q}_p}(M_F \otimes \mathbf{Q}_p) = 0$. Hence $M_F \otimes \mathbf{Q}_p$ has a submodule isomorphic to $\Lambda_F \otimes \mathbf{Q}_p$, and (iii) follows. q.e.d.

Proposition 6.4. *Suppose that $K \subset F \subset L \subset \mathcal{K}$, L/K is a $\mathbf{Z}_p$-power extension, and $\mathrm{char}_{\Lambda_L}(\mathcal{S}_p(E,L)) \subset I_F\Lambda_L$.*

(i) *If F/K is finite, then $\mathcal{S}_p(E,F)$ has a submodule isomorphic to Λ_F.*
(ii) *If F/K is a $\mathbf{Z}_p$-power extension, then $\mathcal{S}_p(E,F)$ is not a torsion Λ_F-module.*

Proof. Suppose first that F/K is finite. By Lemma 6.3(iii) applied with $M := \mathcal{S}_p(E,L)$, the Λ_F-module $\mathcal{S}_p(E,L) \otimes_{\Lambda_L} \Lambda_F$ has a submodule isomorphic to Λ_F. Now (i) follows from Theorem 6.1.

Now suppose F is a $\mathbf{Z}_p$-power extension of K and $\mathrm{char}_\Lambda(\mathcal{S}_p(E,L)) \subset I_F\Lambda_L$. If F' is a finite extension of K in F, then $I_F \subset I_{F'}$ so assertion (i) shows that $\mathcal{S}_p(E,F')$ has a submodule isomorphic to $\Lambda_{F'}$. Thus by Theorem 6.1, $\mathcal{S}_p(E,F) \otimes \Lambda_{F'}$ has a submodule isomorphic to $\Lambda_{F'}$. Since this holds for every finite extension F' of K in F, it follows that $\mathcal{S}_p(E,F)$ cannot be a torsion Λ_F-module. q.e.d.

Corollary 6.5. *If the Torsion conjecture holds, then $\mathcal{S}_p(E,\mathcal{K})$ is a torsion Λ-module and $\mathcal{S}_p(E,\mathcal{K}^+)$ is a torsion $\Lambda_{\mathcal{K}^+}$-module.*

Proof. If $\mathcal{S}_p(E,\mathcal{K})$ is not a torsion Λ-module, then $\mathrm{char}_\Lambda(\mathcal{S}_p(E,\mathcal{K})) = 0$, and so Proposition 6.4(ii) (with $L = \mathcal{K}$ and $F = K\mathbf{Q}_\infty$) would contradict the Torsion conjecture.

The proof for $\mathcal{K}^+$ is the same. q.e.d.

7. Involutions and functional equations

Suppose that τ is a $\mathbf{Z}_p$-linear involution of Γ. Then, τ induces an involution of Λ (which we will also denote simply by τ, or by $\lambda \mapsto \lambda^\tau$). If M is a Λ-module, we let M^τ be the Λ-module with the same underlying abelian group as M, but with Λ-module structure obtained from that of M by composition with τ.

We will be especially interested in the following two involutions.

Example 7.1. Let ι denote the involution $\gamma \mapsto \gamma^{-1}$ of Γ, and also the induced involution of Λ.

Example 7.2. Let σ be the non-trivial automorphism of K/k as in Section 2. The natural action of σ induces an involution of Γ, and hence of Λ, which we will also denote simply by σ.

Lemma 7.3. *Suppose that T is a (commutative) group of involutions of Γ. Then the natural inclusion $\{\pm 1\} \hookrightarrow \Lambda^\times$ induces an isomorphism*

$$\mathrm{Hom}(T,\{\pm 1\}) \xrightarrow{\sim} H^1(T,\Lambda^\times).$$

Proof. We have a direct sum decomposition $\Lambda^\times \cong \mathbf{F}_p^\times \oplus \Lambda'$ where Λ' is the kernel of the reduction map $\Lambda^\times \to \mathbf{F}_p^\times$. Since Λ' is a pro-p group and $p > 2$, $H^1(T,\Lambda') = 0$ and so

$$H^1(T,\Lambda^\times) = H^1(T,\mathbf{F}_p^\times) = \mathrm{Hom}(T,\mathbf{F}_p^\times) = \mathrm{Hom}(T,\{\pm 1\}).$$

q.e.d.

Proposition 7.4. *Suppose that T is a (commutative) group of involutions of Γ, and $\mathcal{A} \subset \Lambda$ is a principal ideal that is stable under every involution in T. Then there is a homomorphism $\epsilon : T \to \{\pm 1\}$ and a generator $\mathcal{L}$ of $\mathcal{A}$ such that*

$$\mathcal{L}^\tau = \epsilon(\tau)\mathcal{L} \quad \textit{for every } \tau \in T.$$

Further, for each $\tau \in T$, $\epsilon(\tau)$ is uniquely determined by τ and $\mathcal{A}$ (i.e., it does not depend on T or $\mathcal{L}$) and is characterized by the fact that every *generator α of $\mathcal{A}$ satisfies $\alpha^\tau/\alpha \equiv \epsilon(\tau) \pmod{I}$ where I is the augmentation ideal I_K of Λ.*

Proof. Let α be a generator of $\mathcal{A}$. Since $\mathcal{A}$ is stable under involutions in T, the map $c(\tau) := \alpha^\tau/\alpha$ is a 1-cocycle from T to $\Lambda^\times$. By Lemma 7.3, there is a homomorphism $\epsilon : T \to \{\pm 1\}$ that is equivalent in $H^1(T, \Lambda^\times)$ to c. In other words, there is a $u \in \Lambda^\times$ such that $(u^\tau/u)c(\tau) = \epsilon(\tau)$ for every $\tau \in T$. Put $\mathcal{L} := u\alpha$. Then $\mathcal{L}$ is a generator of $\mathcal{A}$ and $\mathcal{L}^\tau = \epsilon(\tau)\mathcal{L}$ for every $\tau \in T$.

For every $\tau \in T$ (with notation as above), we have $\alpha^\tau/\alpha = \epsilon(\tau)u/u^\tau$. Since τ acts trivially on Λ/I, we have $u^\tau \equiv u \pmod{I}$ for every u, and so $\alpha^\tau/\alpha \equiv \epsilon(\tau) \pmod{I}$. q.e.d.

If τ is an involution of Γ, we let $\Gamma_\tau^\pm$ be the submodule of Γ on which τ acts via ± 1, and $\mathcal{K}_\tau^\pm$ the fixed field of $\Gamma_\tau^\mp$. (If σ is the non-trivial automorphism of a quadratic extension K/k, then $\mathcal{K}_\sigma^\pm$ is what we previously denoted simply $\mathcal{K}^\pm$, the maximal k-negative $\mathbf{Z}_p$-power extension of K.)

Proposition 7.5. *Suppose that τ is an involution of Γ, and $\mathcal{L} \in \Lambda$ satisfies $\mathcal{L}^\tau = -\mathcal{L}$. Then $\mathcal{L}$ lies in the augmentation ideal $I_{\mathcal{K}_\tau^+}$.*

Proof. In the exact sequence

$$0 \longrightarrow I_{\mathcal{K}_\tau^+} \longrightarrow \Lambda \longrightarrow \Lambda_{\mathcal{K}_\tau^+} \longrightarrow 0,$$

$I_{\mathcal{K}_\tau^+}$ is stable under τ, and τ induces the identity map on $\Lambda_{\mathcal{K}_\tau^+}$. Since $\mathcal{L}^\tau = -\mathcal{L}$, the image of $\mathcal{L}$ in $\Lambda_{\mathcal{K}_\tau^+}$ must be zero, and the proposition follows. q.e.d.

8. Nekovář's Selmer complex

Definition 8.1. By a *complex* of Λ-modules we mean an infinite *co-complex*, i.e., a sequence of Λ-modules and Λ-homomorphisms

$$C^\bullet : \quad \cdots \longrightarrow C^n \longrightarrow C^{n+1} \longrightarrow \cdots,$$

with (co-)boundary operators raising degrees by 1 and such that the composition of any two successive coboundaries vanishes. We construct other complexes from $C^\bullet$ as follows: the shifted complex, for $k \in \mathbf{Z}$

$$C^\bullet[k] : \quad \cdots \longrightarrow C^{n+k} \longrightarrow (C')^{n+1+k} \longrightarrow \cdots,$$

the Λ-dual complex

$$\mathrm{Hom}_\Lambda(C^\bullet, \Lambda) : \quad \cdots \longrightarrow \mathrm{Hom}_\Lambda(C^{-n}, \Lambda) \longrightarrow \mathrm{Hom}_\Lambda(C^{-n-1}, \Lambda) \longrightarrow \cdots,$$

and, if τ is an involution of Λ

$$(C^\bullet)^\tau : \quad \cdots \longrightarrow (C^n)^\tau \longrightarrow (C^{n+1})^\tau \longrightarrow \cdots.$$

Let $\mathcal{C}$ denote the category of complexes of Λ-modules and let $\mathcal{D}$ be the derived category.

Suppose now that $\mathcal{S}_p(E,\mathcal{K})$ is a torsion Λ-module. Let $C^\bullet_{\mathrm{Nek}}$ be Nekovář's "Selmer complex", the complex in $\mathcal{D}$ that is denoted by $\widetilde{\mathbf{R}\Gamma}_{f,\mathrm{Iw}}(\mathcal{K}/K,\, T_p(E))$ in [12] Section 9.7.1, where $T_p(E) := \varprojlim E[p^n]$ is the p-adic Tate module of E. Nekovář shows that $C^\bullet_{\mathrm{Nek}}$ has the following properties.

Theorem 8.2.

(i) $H^2(C^\bullet_{\mathrm{Nek}}) = \mathcal{S}_p(E,\mathcal{K})$,

(ii) $C^\bullet_{\mathrm{Nek}}$ *has a canonical skew-Hermitian (with respect to the involution ι of Example 7.1) self-duality in the derived category $\mathcal{D}$*

$$C^\bullet_{\mathrm{Nek}} \cong \mathbf{R}\mathrm{Hom}_\Lambda(C^\bullet_{\mathrm{Nek}},\Lambda)^\iota[-3],$$

(iii) *there is an isomorphism of complexes $\varphi : C^\bullet_{\mathrm{Nek}} \xrightarrow{\sim} (C^\bullet_{\mathrm{Nek}})^\sigma$ in $\mathcal{D}$ (where σ is the involution of Example 7.2) such that*

$$\varphi^\sigma \circ \varphi : C^\bullet_{\mathrm{Nek}} \to C^\bullet_{\mathrm{Nek}}$$

is the identity in $\mathcal{D}$ and the following diagram of isomorphisms in $\mathcal{D}$ commutes

$$\begin{array}{ccc} C^\bullet_{\mathrm{Nek}} & \xrightarrow{\sim} & \mathbf{R}\mathrm{Hom}_\Lambda(C^\bullet_{\mathrm{Nek}},\Lambda)^\iota[-3] \\ \downarrow{\scriptstyle\varphi} & & \uparrow{\scriptstyle\varphi^*} \\ (C^\bullet_{\mathrm{Nek}})^\sigma & \xrightarrow{\sim} & \mathbf{R}\mathrm{Hom}_\Lambda((C^\bullet_{\mathrm{Nek}})^\sigma,\Lambda)^\iota[-3] \end{array}$$

where φ^* is the morphism of complexes (in $\mathcal{D}$) induced by φ and the horizontal isomorphisms are the canonical ones from (ii).

Proof. For (i), see [12] Section 9.6.7 and Section 9.7, and for (ii), see [12] Proposition 9.7.3. Assertion (iii) follows from the functoriality of $C^\bullet_{\mathrm{Nek}}$ and its self-duality (ii); see [12] Proposition 6.4.2 and Corollary 6.4.3. q.e.d.

We next recall some notation from [10].

Definition 8.3. A *basic skew-Hermitian Λ-module* is a free Λ-module Φ of finite rank with a non-degenerate skew-Hermitian pairing

$$h : \Phi \otimes_\Lambda \Phi^\iota \longrightarrow \mathfrak{m}$$

where $\mathfrak{m}$ is the maximal ideal of Λ and by skew-Hermitian we mean that $h(b\otimes a) = -h(a\otimes b)^\iota$.

Suppose Φ is a basic skew-Hermitian module. We define a complex $\Phi^\bullet$ concentrated in degrees 1 and 2 by setting $\Phi^1 := \Phi$ and $\Phi^2 := \mathrm{Hom}_\Lambda(\Phi^\iota,\Lambda)$, with coboundary map induced by h. Let

$$N^\bullet := \mathrm{Hom}(\Phi^\bullet,\Lambda)^\iota[-3].$$

We have canonical identifications

$$N^1 = \mathrm{Hom}(\mathrm{Hom}(\Phi^\iota, \Lambda), \Lambda)^\iota = \Phi = \Phi^1,$$
$$N^2 = \mathrm{Hom}(\Phi, \Lambda)^\iota = \mathrm{Hom}(\Phi^\iota, \Lambda) = \Phi^2$$

with coboundary $-h : N^1 \to N^2$ (because h is skew-Hermitian). We fix an isomorphism $j : \Phi^\bullet \to \mathrm{Hom}(\Phi^\bullet, \Lambda)^\iota[-3]$ by setting $j^1 := -1$ and $j^2 := +1$.

Under our Assumptions 2.1, we have the following result from [**10**] (Theorem 7.5).

Theorem 8.4. *Suppose that $\mathcal{S}_p(E, \mathcal{K})$ is a torsion Λ-module. Then there is a basic skew-Hermitian Λ-module Φ such that*

(i) *there is an isomorphism $\psi : \Phi^\bullet \xrightarrow{\sim} C^\bullet_{\mathrm{Nek}}$ in the derived category $\mathcal{D}$ where $\Phi^\bullet$ is the complex of Definition 8.3,*
(ii) *there is a commutative diagram of isomorphisms in $\mathcal{D}$*

$$\begin{array}{ccc} \Phi^\bullet & \xrightarrow{\sim} & \mathrm{Hom}_\Lambda(\Phi^\bullet, \Lambda)^\iota[-3] \\ \downarrow{\scriptstyle \psi} & & \uparrow{\scriptstyle \psi^*} \\ C^\bullet_{\mathrm{Nek}} & \xrightarrow{\sim} & \mathbf{R}\mathrm{Hom}_\Lambda(C^\bullet_{\mathrm{Nek}}, \Lambda)^\iota[-3] \end{array}$$

where ψ^* is the isomorphism induced by ψ, and the horizontal isomorphisms are from Definition 8.3 and Theorem 8.2(ii)*, respectively.*

Corollary 8.5. *If Φ is as in Theorem 8.4, then there is a short exact sequence of Λ-modules*

$$0 \longrightarrow \Phi \longrightarrow \mathrm{Hom}(\Phi^\iota, \Lambda) \longrightarrow \mathcal{S}_p(E, \mathcal{K}) \longrightarrow 0.$$

Proof. By Theorems 8.4(i) and 8.2(i), $H^2(\Phi^\bullet) = H^2(C^\bullet_{\mathrm{Nek}}) = \mathcal{S}_p(E, \mathcal{K})$ and the corollary follows. q.e.d.

9. The inversion involution

Let ι be the inversion involution on Γ, i.e., $\iota(\gamma) = \gamma^{-1}$, as in Example 7.1. Suppose that $\mathcal{S}_p(E, \mathcal{K})$ is a torsion Λ-module, so we can apply the results of Section 8.

Proposition 9.1. *With Φ as in Theorem 8.4, we have*

$$\mathrm{rank}_\Lambda(\Phi) \equiv \mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E, K)) \pmod 2.$$

Proof. Let $I := I_K$ denote the augmentation ideal of Λ, so $\Lambda/I = \Lambda_K \cong \mathbf{Z}_p$. Tensoring the exact sequence of Corollary 8.5 with Λ/I gives

$$\Phi/I\Phi \xrightarrow{\bar{h}} \mathrm{Hom}(\Phi^\iota/I\Phi^\iota, \mathbf{Z}_p) \longrightarrow \mathcal{S}_p(E,\mathcal{K}) \otimes_\Lambda \mathbf{Z}_p \longrightarrow 0.$$

Since ι acts trivially on Λ/I, the map $\bar{h}$ is represented by a skew symmetric matrix with entries in $\mathbf{Z}_p$. Such a matrix has even rank (that is, the non-degeneracy rank of the matrix, which is the $\mathbf{Z}_p$-rank of the image), and it follows that

$$\mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E,\mathcal{K}) \otimes_\Lambda \mathbf{Z}_p) \equiv \mathrm{rank}_{\mathbf{Z}_p}(\Phi/I\Phi) = \mathrm{rank}_\Lambda(\Phi) \pmod 2.$$

On the other hand, Theorem 6.1 shows that

$$\mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E,K)) = \mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E,\mathcal{K}) \otimes_\Lambda \mathbf{Z}_p),$$

and the proposition follows. q.e.d.

Corollary 9.2. *Suppose that $\mathcal{S}_p(E,\mathcal{K})$ is a torsion Λ-module. Let H be the matrix giving the skew-Hermitian pairing of Theorem 8.4 with respect to some Λ-basis of Φ, and $\mathcal{L} := \det(H) \in \Lambda$. Then $\mathcal{L}$ is a generator of $\mathrm{char}(\mathcal{S}_p(E,\mathcal{K}))$ and $\mathcal{L}^\iota = (-1)^r\mathcal{L}$, where $r := \mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E,K))$.*

Proof. By Corollary 8.5, $\det(H)$ is a generator of $\mathrm{char}(\mathcal{S}_p(E,\mathcal{K}))$. On the other hand, H is a skew-Hermitian matrix (i.e., the transpose of H is $-H^\iota$), so

$$\det(H)^\iota = \det(H^\iota) = \det(-H) = (-1)^{\mathrm{rank}_\Lambda(\Phi)} \det(H) = (-1)^r \det(H)$$

the final equality by Proposition 9.1. q.e.d.

10. The involution σ

Let σ be the non-trivial automorphism of K/k as in Section 2, and let σ also denote the corresponding involutions of Γ and Λ as in Example 7.2. The following theorem is one of the keys to the proof of Theorem 3.1. Let $I := I_K \subset \Lambda$ denote the augmentation ideal.

Theorem 10.1. *Suppose $\mathcal{L}$ is a generator of $\mathrm{char}(\mathcal{S}_p(E,\mathcal{K}))$. Then there is a unit $u \in \Lambda^\times$, $u \equiv 1 \pmod I$, such that $\mathcal{L}^\sigma = u\mathcal{L}$.*

Proof. We may suppose $\mathcal{S}_p(E,\mathcal{K})$ is a torsion Λ-module, or else we have $\mathrm{char}(\mathcal{S}_p(E,\mathcal{K})) = 0$ and there is nothing to prove. Let $\Phi^\bullet$ be the complex of Definition 8.3.

Combining Theorems 8.2(iii) and 8.4, we get an isomorphism $\eta : \Phi^\bullet \to (\Phi^\bullet)^\sigma$ in the derived category $\mathcal{D}$ and a commutative diagram

$$\begin{array}{ccc} \Phi^\bullet & \xrightarrow{\sim} & \mathrm{Hom}_\Lambda(\Phi^\bullet, \Lambda)^\iota[-3] \\ {\scriptstyle\eta}\big\downarrow\big\uparrow{\scriptstyle\eta^\sigma} & & \big\uparrow{\scriptstyle\eta^*} \\ (\Phi^\bullet)^\sigma & \xrightarrow{\sim} & \mathrm{Hom}_\Lambda((\Phi^\bullet)^\sigma, \Lambda)^\iota[-3]. \end{array} \tag{10.1}$$

By Corollary 5.6 of [**10**], there is an isomorphism of complexes (in the category $\mathcal{C}$) $f : \Phi^\bullet \to (\Phi^\bullet)^\sigma$ that gives rise to η. Let $\Phi^* := \mathrm{Hom}_\Lambda(\Phi^\iota, \Lambda)$, the degree-2 module of $\Phi^\bullet$. Then f is given by isomorphisms of Λ-modules

$$f^1 : \Phi \xrightarrow{\sim} \Phi^\sigma, \qquad f^2 : \Phi^* \xrightarrow{\sim} (\Phi^*)^\sigma.$$

Let $f^\sigma : (\Phi^\bullet)^\sigma \to \Phi^\bullet$ be the morphism of complexes given by

$$(f^1)^\sigma : \Phi^\sigma \to (\Phi^\sigma)^\sigma = \Phi, \qquad (f^2)^\sigma : (\Phi^*)^\sigma \to ((\Phi^*)^\sigma)^\sigma = \Phi^*.$$

Applying the functor $\mathrm{Hom}_\Lambda(\,\cdot\,, \Lambda)^\iota$ to f^1 and f^2 gives isomorphisms

$$(f^2)^* : \Phi^\sigma \to \Phi, \qquad (f^1)^* : (\Phi^*)^\sigma \to \Phi^*.$$

These Λ-isomorphisms give a morphism of complexes $f^* : (\Phi^\bullet)^\sigma \to \Phi^\bullet$, and the commutativity of (10.1) says $f^* = f^\sigma$ as morphisms $\Phi^\bullet \to \Phi^\bullet$ in the derived category $\mathcal{D}$. By Corollary 5.6 of [**10**], we conclude that f^* is homotopic to f^σ. By our definition of basic skew-Hermitian module (Definition 8.3), the coboundary map $\Phi \to \Phi^*$ of $\Phi^\bullet$ is zero modulo the maximal ideal $\mathfrak{m}$ of Λ. Therefore every homotopy must be congruent to the identity modulo $\mathfrak{m}$, and in particular

$$(f^2)^* = (f^1)^\sigma \text{ on } \Phi \otimes (\Lambda/\mathfrak{m}). \tag{10.2}$$

Consider the diagram

$$\begin{array}{ccc} \Phi & \xrightarrow{h} & \Phi^* \\ {\scriptstyle f^1}\big\downarrow & & \big\downarrow{\scriptstyle f^2} \\ \Phi^\sigma & \xrightarrow{h^\sigma} & (\Phi^*)^\sigma \end{array} \tag{10.3}$$

where h is the coboundary map in the complex $\Phi^\bullet$. Fix a Λ-basis of Φ, use the dual basis for Φ^*, and the corresponding bases for Φ^σ and $(\Phi^*)^\sigma$. With these bases, if we let $d := \mathrm{rank}_\Lambda(\Phi)$, (10.3) becomes

$$\begin{array}{ccc} \Lambda^d & \xrightarrow{H} & \Lambda^d \\ {\scriptstyle F^1}\big\downarrow & & \big\downarrow{\scriptstyle F^2} \\ \Lambda^d & \xrightarrow{H^\sigma} & \Lambda^d \end{array}$$

where H is a $d \times d$ matrix with entries in Λ, and $F^1, F^2 \in \mathrm{GL}_d(\Lambda)$. By (10.2), we see that $(F^1)^{\iota\sigma}$ is congruent modulo $\mathfrak{m}$ to the transpose of F^2. As in the proof of Corollary 9.2, it follows from Corollary 8.5 that $\det(H)$ is a generator of $\mathrm{char}(\mathcal{S}_p(E,\mathcal{K}))$, and we see that $\det(H)^\sigma = u\det(H)$, where

$$u := \det(F^2)/\det(F^1) \equiv \det(F^1)^{\iota\sigma}/\det(F_1) \equiv 1 \pmod{\mathfrak{m}}.$$

Now the theorem follows from Proposition 7.4. q.e.d.

Corollary 10.2. *Suppose that $\mathcal{S}_p(E,\mathcal{K})$ is a torsion Λ-module. Then there is a generator $\mathcal{L}$ of $\mathrm{char}(\mathcal{S}_p(E,\mathcal{K}))$ such that*

$$\mathcal{L}^\iota = (-1)^r\mathcal{L}, \quad \mathcal{L}^\sigma = \mathcal{L}$$

where $r := \mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E,K))$.

Proof. Let T be the group generated by the (commuting) involutions ι and σ of Γ. By Corollary 9.2 and Theorem 10.1, the ideal $\mathrm{char}(\mathcal{S}_p(E,\mathcal{K}))$ is stable under every element of T. Now the corollary follows from Proposition 7.4, Corollary 9.2, and Theorem 10.1. q.e.d.

11. Proofs of Theorem 3.1 and Corollary 3.6

Proof of Theorem 3.1. If $\mathcal{S}_p(E,\mathcal{K})$ is not a torsion Λ-module, then Theorem 3.1 holds by Proposition 6.4 (with $L = \mathcal{K}$ and $F \subset \mathcal{K}^-$). So we may assume that $\mathcal{S}_p(E,\mathcal{K})$ is a torsion Λ-module.

Let $\mathcal{L}$ be a generator of $\mathrm{char}_\Lambda(\mathcal{S}_p(E,\mathcal{K}))$ satisfying Corollary 10.2. Since we assume that $\mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E,K))$ is odd, we have $\mathcal{L}^{\iota\sigma} = -\mathcal{L}$. Note that (in the notation of Section 7) $\Gamma^+_{\iota\sigma} = \Gamma^-$ and $\mathcal{K}^+_{\iota\sigma} = \mathcal{K}^-$. By Proposition 7.5, we have $\mathcal{L} \in I_{\mathcal{K}^+_{\iota\sigma}} = I_{\mathcal{K}^-}$, so Theorem 3.1 follows from Proposition 6.4 (with $L = \mathcal{K}$ and $F \subset \mathcal{K}^-$). q.e.d.

Corollary 3.6 will follow immediately from Theorem 3.1 once we show that (under the hypotheses of Corollary 3.6) $\mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E,K))$ is odd. We will deduce this from Nekovář's parity theorem [**11**] for Selmer groups over $\mathbf{Q}$.

Lemma 11.1. *Suppose G is a finite group of odd order. If V is a non-trivial irreducible representation of $\mathbf{R}[G]$, then $\dim_{\mathbf{R}}(V)$ is even.*

Proof. We will prove this by induction on the order of G. If G is cyclic, then the lemma is clear. If not, then by the Feit–Thompson theorem, G has a proper normal subgroup H. If H acts trivially on V, then we are done by induction (applied to G/H), so we may assume that H acts non-trivially on V.

Decompose $V = \oplus_i V_i$ where each V_i is an irreducible representation of $\mathbf{R}[H]$. If some V_j is the trivial representation then (since H is normal) H acts trivially on the G-span of V_j. But the G-span of V_j is non-zero and G-stable, hence equal to V. This contradicts our assumption that H acts non-trivially on V.

Thus, by induction each $\dim_{\mathbf{R}}(V_i)$ is even, and so $\dim_{\mathbf{R}}(V)$ is even. q.e.d.

Lemma 11.2. *Suppose Δ is the semidirect product of a (normal) subgroup of odd order with a non-trivial cyclic 2-group. If ρ is an irreducible representation of $\mathbf{R}[\Delta]$, not equal to either the trivial representation or the unique quadratic one-dimensional character, then $\dim(\rho)$ is even.*

Proof. Let H denote the (normal) odd-order subgroup of Δ with cyclic 2-power quotient. If ρ is trivial on H, then the proposition is clear.

Decompose $\rho|_H = \oplus_i \rho_i$ into irreducible representations of $\mathbf{R}[H]$. Arguing exactly as in the proof of Lemma 11.1, we conclude that each ρ_i is non-trivial, and then by Lemma 11.1, each $\dim(\rho_i)$ is even. q.e.d.

Proposition 11.3. *Suppose that K is Galois over $\mathbf{Q}$ and $\mathrm{Gal}(K/\mathbf{Q})$ satisfies hypothesis* (b) *of Corollary 3.6. Let M denote the (unique) quadratic field contained in K.*

(i) $\mathrm{rank}_{\mathbf{Z}}(E(K)) \equiv \mathrm{rank}_{\mathbf{Z}}(E(M)) \pmod 2$.
(ii) *If in addition $\mathrm{Gal}(K/\mathbf{Q})$ satisfies hypothesis* (c) *of Corollary 3.6, then $\mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E,K)) \equiv \mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E,M)) \pmod 2$.*

Proof. Let $V := (E(K)\otimes\mathbf{R})/(E(M)\otimes\mathbf{R})$ and $\Delta := \mathrm{Gal}(K/\mathbf{Q})$. Then

$$\mathrm{rank}_{\mathbf{Z}}(E(K)) - \mathrm{rank}_{\mathbf{Z}}(E(M)) = \dim_{\mathbf{R}}(V).$$

The $\mathbf{R}[\Delta]$-module V contains no copies of either of the two one-dimensional real representations of Δ, so Lemma 11.2 shows that $\dim_{\mathbf{R}}(V)$ is even. This proves (i).

If the p-primary Tate–Shafarevich conjecture holds, then (ii) follows immediately from (i). If every irreducible $\mathbf{Q}_p$-representation of Δ not factoring through $\mathrm{Gal}(M/\mathbf{Q})$ has even dimension, then exactly as above the $\mathbf{Q}_p$-dimension of $(\mathcal{S}_p(E,K)\otimes\mathbf{Q}_p)/(\mathcal{S}_p(E,M)\otimes\mathbf{Q}_p)$ is even. q.e.d.

Theorem 11.4. *Suppose that hypotheses* (a), (b), (c), *and* (d) *of Corollary 3.6 are satisfied. Then $\mathrm{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E,K))$ is odd.*

Proof. Let M denote the quadratic extension of $\mathbf{Q}$ inside K, and let E' denote the quadratic twist of E by M. Then $L(E/M,s) = L(E/\mathbf{Q},s)L(E'/\mathbf{Q},s)$ and $\mathcal{S}_p(E,M) \cong \mathcal{S}_p(E,\mathbf{Q}) \oplus \mathcal{S}_p(E',\mathbf{Q})$. Nekovář [11] proved that

$$\operatorname{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E,\mathbf{Q})) \equiv \operatorname{ord}_{s=1} L(E/\mathbf{Q},s) \pmod 2$$

and similarly for E'. We deduce that

$$\operatorname{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E,M)) \equiv \operatorname{ord}_{s=1} L(E/M,s) \pmod 2.$$

By (for example) Proposition 4.1(ii) applied with K replaced by M, the root number $W(E/M) = -1$, so $\operatorname{ord}_{s=1}L(E/M,s)$ is odd and we conclude that $\operatorname{rank}_{\mathbf{Z}_p}(\mathcal{S}_p(E,M))$ is odd.

It now follows from Proposition 11.3(ii) that $\operatorname{rank}_{\mathbf{Z}_p}\mathcal{S}_p(E,K)$ is odd. q.e.d.

Proof of Corollary 3.6. Corollary 3.6 follows immediately from Theorem 3.1, using Theorem 11.4. q.e.d.

12. Proof of Proposition 4.1

Proposition 4.1 is essentially proved in [9] Section 2.2. For completeness, we sketch the proof here.

Proof of Proposition 4.1. Suppose $\psi \in \operatorname{Hom}_{\text{cont}}(\operatorname{Gal}(\mathcal{K}^-/K), \mathbf{C}^\times)$. Since σ acts as -1 on $\operatorname{Gal}(\mathcal{K}^-/K)$, we have $\psi^\sigma = \psi^{-1} = \bar\psi$. Therefore $\operatorname{Ind}_k^K\psi = \operatorname{Ind}_k^K\bar\psi$, so $\operatorname{Ind}_k^K\psi$ is real valued in part (i), and similarly for $\operatorname{Ind}_{\mathbf{Q}}^K\psi$ in part (ii).

In Proposition 10 of [15], Rohrlich gives a formula for the root number $W(E/K,\psi) = W(E/k,\operatorname{Ind}_k^K\psi)$ that depends only on E and $\det(\operatorname{Ind}_k^K\psi)$, and does not otherwise depend on ψ. To complete the proof of (i), we need only show that $\det(\operatorname{Ind}_k^K\psi)$ does not depend on ψ.

Let $\mathfrak{p}$ be a prime of $\bar{\mathbf{Q}}$ above p. Since ψ has p-power order, $\psi \equiv \mathbf{1} \pmod{\mathfrak{p}}$ where $\mathbf{1}$ is the trivial character, and so

$$\det(\operatorname{Ind}_k^K\psi) \equiv \det(\operatorname{Ind}_k^K\mathbf{1}) \pmod{\mathfrak{p}}.$$

Since p is odd and both sides of this congruence are characters taking only the values ±1, it follows that the congruence must be an equality. This proves (i).

For (ii), we use Rohrlich's Proposition 10 [15] again to conclude that

$$W(E/K,\psi) = W(E/\mathbf{Q},\operatorname{Ind}_{\mathbf{Q}}^K\psi) = \chi(-N_E)$$

where $\chi := \det(\mathrm{Ind}_{\mathbf{Q}}^{K}\psi)$. Exactly as above, we have $\det(\mathrm{Ind}_{\mathbf{Q}}^{K}\psi) = \det(\mathrm{Ind}_{\mathbf{Q}}^{K}\mathbf{1})$, and by Proposition 2.9 of [9], hypothesis (b) of Corollary 3.6 ensures that $\det(\mathrm{Ind}_{\mathbf{Q}}^{K}\mathbf{1})$ is the unique quadratic character of $\mathrm{Gal}(K/\mathbf{Q})$. Now the hypothesis (d) of Corollary 3.6 completes the proof of (ii). q.e.d.

13. Acknowledgments

We would like to thank Jay Pottharst for reading a preliminary version of this paper and for providing us with a simpler version of Lemma 6.3.

References

[1] N. Bourbaki, *Éléments de mathématique. Fasc.* XXXI. *Algèbre commutative. Chapitre* 7 : *Diviseurs*, Actualités Scientifiques et Industrielles, **1314**, Paris, Hermann, 1965, MR 0260715, Zbl 0547.13002.

[2] C. Cornut, *Mazur's conjecture on higher Heegner points*, Invent. Math. **148** (2002) 495–523, MR 1908058.

[3] C. Cornut & V. Vatsal, *CM points and quaternion algebras*, preprint, 2004.

[4] P. Deligne, *Les constantes des équations fonctionnelles des fonctions L*, in 'Modular Functions of One Variable II', Lect. Notes in Math., **349**, Springer, New York, 1973, 501–595, MR 0349635, Zbl 0271.14011.

[5] R. Greenberg, *On the Birch and Swinnerton-Dyer conjecture*, Invent. Math. **72** (1983) 241–265, MR 0700770, Zbl 0546.14015.

[6] R. Greenberg, *Galois theory for the Selmer group of an abelian variety*, Compositio Math. **136** (2003) 255–297, MR 1977007.

[7] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms. Cohomologies p-adiques et applications arithmétiques*, III, Astérisque **295** (2004) 117–290, MR 2104361.

[8] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972) 183–266, MR 0444670, Zbl 0258.14009.

[9] B. Mazur & K. Rubin, *Studying the growth of Mordell–Weil*, Documenta Math., extra volume (2003) 585–607, MR 2046609.

[10] B. Mazur & K. Rubin, *Organizing the arithmetic of elliptic curves*, to appear in Advances in Math.

[11] J. Nekovář, *On the parity of ranks of Selmer groups*, II, C.R. Acad. Sci. Paris Sér. I Math. **332** (2001) 99–104, MR 1813764.

[12] J. Nekovář, *Selmer complexes* (Second version, November 2003), preprint available at http://www.math.jussieu.fr/∼nekovar/pu/.

[13] B. Perrin-Riou, *Arithmétique des courbes elliptiques et théorie d'Iwasawa*, Bull. Soc. Math. Suppl., Mémoire, **17** (1984), MR 0799673, Zbl 0599.14020.

[14] B. Perrin-Riou, *Groupes de Selmer et accouplements: cas particulier des courbes elliptiques*, Documenta Math., extra volume (2003) 725–760, MR 2046613.

[15] D. Rohrlich, *Galois theory, elliptic curves, and root numbers*, Compositio Math. **100** (1996) 311–349, MR 1387669, Zbl 0860.11033.

[16] C. Skinner & E. Urban, *Sur les déformations p-adiques de certaines représentations automorphes*, to appear in Journal de l'Institut de Mathématiques de Jussieu.

[17] V. Vatsal, *Uniform distribution of Heegner points*, Invent. Math. **148** (2002) 1–46, MR 1892842.

Department of Mathematics
Harvard University
Cambridge, MA 02138

Department of Mathematics
University of California Irvine
Irvine, CA 92697