PAIRINGS IN THE ARITHMETIC OF ELLIPTIC CURVES

BARRY MAZUR AND KARL RUBIN

Introduction

The recent work of Cornut, Vatsal, Bertolini, Darmon, Nekovár and others on the Mordell-Weil and Shafarevich-Tate groups of elliptic curves over anticyclotomic towers has made it timely to organize, and possibly sharpen, the collection of yet unresolved conjectures regarding the finer structure we expect to be true about this piece of arithmetic. That was the general aim of two of our recent preprints ([MR1], [MR2]) the former being the text of an address given at the International Congress of Mathematicians in Beijing last summer by the second author. It was also the aim of the lecture delivered by the first author at the conference in Barcelona in July. Since there was some overlap in our two lectures (Beijing, Barcelona), we felt it reasonable not to repeat things, but rather, in this write-up for the proceedings of the Barcelona conference, to concentrate only on the following part of the story which was not really covered in any of the other accounts.

In a recent preprint [N2], Nekovár developed a *derived complex* version of the theory of Selmer modules and expressed some of the standard dualities enjoyed by Selmer modules in the language of derived complexes. The advantage of this is its naturality and generality: the cohomological machinery directly yields such a structure, and we are well-advised to keep that structure in view. The disadvantage is the unavoidable largeness of the technique, which makes it slightly inconvenient, for example, to explain it in an hour. Nevertheless, if one is to understand, and build upon, the collection of outstanding unsolved problems regarding our anticyclotomic context, it might be a good idea to hold in one's head all these dualities at the same time. As an expository tool, it occurred to us to hypothesize a certain rigidification of Nekovár's theory (a single skew-Hermitian module) from which one might obtain the Selmer module of interest, and all of its attendant height pairings, and Cassels pairings, and upon which one can impose

Both authors partially supported by the National Science Foundation.

some of the finer structure carried, in some contexts, by Selmer modules (see for example the discussion of Heegner points and L-functions in [MR1]). This hypothesized skew-Hermitian module has the virtue of being very easy to explain, making use of only low-tech methods. The great disadvantage of our theory is that we have no natural way of constructing the relevant skew-Hermitian matrices in any nontrivial case. Our hope that perhaps we may eventually be able to find such natural constructions, at least in some cases, was inspired by the vague analogy it has to Seifert's classical results which express the algebraic topology of abelian covers of knot complements in terms of skew-symmetric matrices with coefficients in an appropriate localization of the group ring of the first homology group of the knot complement. The Cassels pairing in arithmetic has a formal structure similar to the Blanchfield pairing in knot theory. The height pairings, however, which play such a prominent role in arithmetic also have analogues in knot theory, but, to our knowledge, these analogues haven't been explicitly used in either classical knot theory, or in the theory of knots in higher dimensions.

We offer Part 1 of this article as a possibly helpful expository warm-up for any student interested in learning Nekovár's "Selmer complexes." Part 2 discusses the arithmetic of elliptic curves over anticyclotomic towers from the viewpoint sketched in Part 1.

Part 1. **The structure of Selmer modules**

1. Selmer groups of elliptic curves

Consider the structure "carried by" the *p-Selmer group* $S_p(E,K)$ of an elliptic curve E over a number field K. Recall that this Selmer group is the $\mathbf{Z}_p$-module of finite type defined as the Pontrjagin dual of:

$$\ker(H^1(K,E[p^\infty]) \to \prod_v H^1(K_v,E)),$$

where $E[p^\infty]$ is the Galois module of p-power torsion on E, and the product is over all places v of K. We define $S_p(E,K)_{\mathrm{tors}}$ to be the torsion subgroup of $S_p(E,K)$ and $S_p(E,K)_{\mathrm{free}}$ the canonical torsion-free quotient $S_p(E,K)/S_p(E,K)_{\mathrm{tors}}$.

Let the superscripts ${}^{\mathcal{D}}$ and ${}^{\diamond}$ denote Pontrjagin dual and $\mathbf{Z}_p$-dual, respectively, so that $M^{\mathcal{D}} := \mathrm{Hom}(M,\mathbf{Q}/\mathbf{Z})$ and $M^{\diamond} := \mathrm{Hom}(M,\mathbf{Z}_p)$.

For simplicity let us assume the Shafarevich-Tate conjecture, so that $S_p(E,K)_{\mathrm{tors}}$ is canonically isomorphic to the Pontrjagin dual of the p-primary subgroup of the Shafarevich-Tate group of E over K. It follows that there are canonical isomorphisms

$$S_p(E,K)_{\mathrm{free}} \cong E(K)^{\diamond}, \qquad S_p(E,K)_{\mathrm{tors}} \cong Ш(E,K)[p^{\infty}]^{\mathcal{D}},$$

$$(E(K)/E(K)_{\mathrm{tors}}) \otimes \mathbf{Z}_p \cong S_p(E,K)^{\diamond}_{\mathrm{free}}.$$

The Cassels pairing induces a nondegenerate skew-symmetric pairing

$$S_p(E,K)^{\mathcal{D}}_{\mathrm{tors}} \otimes S_p(E,K)^{\mathcal{D}}_{\mathrm{tors}} \longrightarrow \mathbf{Q}_p/\mathbf{Z}_p.$$

Since this pairing is nondegenerate, it induces an isomorphism

$$S_p(E,K)_{\mathrm{tors}} \cong S_p(E,K)^{\mathcal{D}}_{\mathrm{tors}},$$

and hence a nondegenerate skew-symmetric pairing

$$S_p(E,K)_{\mathrm{tors}} \otimes S_p(E,K)_{\mathrm{tors}} \longrightarrow \mathbf{Q}_p/\mathbf{Z}_p. \tag{1'}$$

Assume now that every place v of K of residual characteristic p is a prime of good, ordinary reduction for E. By a $\mathbf{Z}_p$*-power extension* of K let us mean a Galois extensions with Galois group isomorphic to $\mathbf{Z}_p^d$ for some natural number d, and by $\Gamma := \Gamma(K)$ let us mean the Galois group of the maximal $\mathbf{Z}_p$-power extension of K in an algebraic closure of K (assumed chosen and fixed). Recall that we have a canonical symmetric, bilinear, p-adic height pairing

$$S_p(E,K)^{\diamond}_{\mathrm{free}} \otimes S_p(E,K)^{\diamond}_{\mathrm{free}} \longrightarrow \Gamma(K) \otimes \mathbf{Q}_p \tag{2'}$$

and we may even guarantee that the the values of this pairing are nearly integers, in the sense that they are contained in

$$\frac{1}{\delta(E,K)} \cdot \Gamma(K) \subset \Gamma(K) \otimes \mathbf{Q}_p$$

where the denominator $\delta(E,K)$ is a very controllable number, often 1 (cf. [MT]). The p-adic height pairing is conveniently functorial in K, and in particular when $K/\mathbf{Q}$ is Galois the pairing is $\mathrm{Gal}(K/\mathbf{Q})$-equivariant in an evident sense.

We will be studying, later, more machinery than $(1')$ and $(2')$ that Selmer groups are naturally endowed with, but for the moment let us take a step backwards and repeat the algebraic structure discussed so far.

Let A be a discrete valuation ring and a $\mathbf{Z}_p$-algebra (A was simply $\mathbf{Z}_p$ in the previous paragraph). Denote by $\mathcal{K}$ the field of fractions of A. Let Γ be an abelian pro-p-group, and let S be an A-module of finite type. Form the canonical exact sequence of A-modules

$$0 \longrightarrow T \longrightarrow S \longrightarrow F \longrightarrow 0,$$

where T is a torsion A-module and F free. We assume that we have a nondegenerate bilinear skew-symmetric pairing

$$T \otimes_A T \longrightarrow \mathcal{K}/A, \tag{1}$$

and a bilinear symmetric pairing

$$F^\diamond \otimes F^\diamond \to \Gamma \otimes_{\mathbf{Z}_p} \mathcal{K} \tag{2}$$

where the superscript $^\diamond$ now denotes A-duality, i.e., $F^\diamond := \mathrm{Hom}_A(F, A)$. Also, it is good to bear in mind (without formally including this feature in our axiomatic set-up above) that in the prototype, the symmetric pairing (2) takes values in

$$\frac{1}{\delta} \cdot \Gamma \otimes_{\mathbf{Z}_p} A \subset \Gamma \otimes_{\mathbf{Z}_p} \mathcal{K},$$

where δ is something computable.

How might one naturally come across an A-module S above with the two types of pairings as sketched above?

2. Hermitian and Skew-Hermitian modules

Fix a commutative ring R endowed with an involution $\iota : R \to R$.

If M is an R-module, let M^ι denote the R-module having the same underlying abelian group M, but with R-module structure obtained from that of M by composition with ι. Clearly $(M^\iota)^\iota = M$. By a *semi-linear* (R, ι)*-module* we mean an R module W endowed with an involution $i : W \to W$ such that $i(rw) = \iota(r) \cdot i(w)$ for all $r \in R$ and $w \in W$. Equivalently, we may think of the involution i as an R-module isomorphism $i : W \to W^\iota$ such that $i^\iota \cdot i : W \to (W^\iota)^\iota = W$ is the identity. We refer to such a pair (W, i) as a *semi-linear module*, for short. The involution ι of the free R-module R endows that module with a natural semi-linear structure. If M is an R-module and W is a semi-linear R-module, the the R-module $\mathrm{Hom}_R(M, W)$ inherits a semi-linear structure as follows. For $f \in \mathrm{Hom}(M, W)$ let $i(f) \in \mathrm{Hom}_R(M, W)$ be given by $i(f) := i \circ f$. For a free R-module Φ of finite rank, by the *semi-linear* R*-dual* Φ^* of Φ we mean the R-module $\Phi^* := \mathrm{Hom}_R(\Phi^\iota, R)$ with the semi-linear structure as given above.

If $I \subset R$ is an ideal which is stable under the action ι then the quotient R/I inherits an involution compatible with ι; we denote it again ι. Let us call such an ideal I a *switching ideal* if ι induces the identity involution on R/I and the automorphism "multiplication by -1" on I/I^2.

Example 2.1. A principal example for us is the following. Suppose B is a commutative $\mathbf{Z}_p$-algebra and G is a commutative pro-p group.

Let R be the completed group ring $B[[G]]$, and let ι be the involution which operates as the identity on B and by $g \mapsto g^{-1}$ on G.

If $H \subset G$ is a closed subgroup, let $I_H \subset R$ be the closed ideal generated by all elements of the form $h-1 \in R$ for $h \in H$. That is, I_H is the kernel of the natural projection $B[[G]] \to B[[G/H]]$. We have a canonical isomorphism of $B[[G/H]]$-modules

$$H \otimes_{\mathbf{Z}_p} B[[G/H]] \cong I_H/I_H^2$$

characterized by the property that the element $h \otimes 1$ is sent to $h-1$ modulo I_H^2 for all $h \in H$. The augmentation ideal $I_G \subset B[[G]]$ is a switching ideal.

If Φ is an R-module, and W a semi-linear R-module, a pairing

$$\pi : \Phi \otimes_R \Phi^\iota \to W$$

is called *Hermitian* if

$$\pi(a \otimes_R b) = +i(\pi(b \otimes_R a)),$$

and *skew-Hermitian* if

$$\pi(a \otimes_R b) = -i(\pi(b \otimes_R a)).$$

Remark 2.2. When we talk of Hermitian or skew-Hermitian pairings with values in the ring R we will always mean to view the ring R *with semi-linear R-module structure given by its involution ι.* Note however, that if $i : W \to W$ is a semi-linear involution of an R-module W, then so is $-i$, and if we switch to considering $i' = -i$, then Hermitian pairings with values in the semi-linear R-module (W, i) are skew-Hermitian pairings with values in (W, i'), and vice-versa.

3. Derived pairings

Suppose from now on that Φ is free over R of finite rank, and $W = R$. Suppose further that we have a nondegenerate R-valued skew-Hermitian pairing $\Phi \otimes \Phi^\iota \to R$. Such a pairing corresponds to an injective R-homomorphism

$$h : \Phi \longrightarrow \Phi^*$$

and the skew-Hermitian property of the pairing is then equivalent to the fact that the induced map

$$\Phi^\iota = \mathrm{Hom}(\Phi^*, R) \xrightarrow{h^*} \mathrm{Hom}(\Phi, R) = (\Phi^*)^\iota$$

is identified with $-h$ under the canonical isomorphism $\mathrm{Hom}_R(\Phi, \Phi^*) = \mathrm{Hom}_R(\Phi^\iota, (\Phi^*)^\iota)$.

Let S denote the cokernel of h, so that

$$0 \longrightarrow \Phi \xrightarrow{h} \Phi^* \longrightarrow S \longrightarrow 0 \tag{3}$$

is a free resolution of the R-module S, giving, in particular that the A-modules $\mathrm{Tor}^i_R(S,A)$ and $\mathrm{Ext}^i_R(S,A)$ vanish for every R-algebra A and every $i > 1$. If A is an R-algebra put

$$\begin{aligned} M(A) &:= \mathrm{Tor}^1_R(S,A) = \ker(h \otimes_R A), \\ S(A) &:= S \otimes_R A = \mathrm{coker}(h \otimes_R A) \end{aligned}$$

(the letter M is chosen to remind us of *Mordell-Weil*, while the letter S is chosen to remind us of *Selmer*; see §5). These definitions give us an exact sequence of A-modules

$$0 \longrightarrow M(A) \longrightarrow \Phi \otimes_R A \xrightarrow{h \otimes A} \Phi^* \otimes_R A \longrightarrow S(A) \longrightarrow 0. \tag{4}$$

Now let us pass to the special case where A is an R-algebra with involution, compatible with the involution ι of R. We use the same letters ι and i to refer to the involutions of A and of $\Phi^* \otimes_R A$. We have that $h^* \otimes_R A = -h \otimes_R A$, and using this along with (4) (for the upper exact sequence) and (3) (for the lower exact sequence) gives a commutative diagram of A-modules,

$$\begin{tikzcd}
0 \arrow[r] & M(A)^\iota \arrow[r] & \Phi^\iota \otimes A \arrow[r, "-h\otimes A"] \arrow[d, "\cong"] & (\Phi^*)^\iota \otimes A \arrow[r] \arrow[d, "\cong"] & S(A)^\iota \arrow[r] & 0 \\
0 \arrow[r] & \mathrm{Hom}_R(S,A) \arrow[r] & \mathrm{Hom}(\Phi^*,A) \arrow[r, "h^*\otimes A"] & \mathrm{Hom}(\Phi,A) \arrow[r] & \mathrm{Ext}^1_R(S,A) \arrow[r] & 0.
\end{tikzcd}$$

Thus we obtain canonical isomorphisms

$$M(A)^\iota \cong \mathrm{Hom}_R(S,A), \tag{5}$$

$$S(A)^\iota \cong \mathrm{Ext}^1_R(S,A). \tag{6}$$

Assume now that A is a quotient R-algebra with compatible involution, that is, $A = R/I$ where $I \subset R$ is stable under ι. Tensoring the exact sequence

$$0 \longrightarrow I \longrightarrow R \longrightarrow A \longrightarrow 0$$

with S gives a canonical injection

$$0 \longrightarrow \mathrm{Tor}^1_R(S,A) \longrightarrow I \otimes_R S$$

and composing this with the natural pairing

$$(I \otimes_R S) \otimes_R \mathrm{Hom}_R(S,A) \longrightarrow I \otimes_R A = I/I^2$$

we get the pairing

$$\mathrm{Tor}^1_R(S,A) \otimes_A \mathrm{Hom}_R(S,A) \longrightarrow I/I^2.$$

Now, using the definition of $M(A)$ and (5), we obtain the pairing:

$$M(A) \otimes_A M(A)^\iota \longrightarrow I/I^2. \tag{7}$$

Note that if ι induces multiplication by -1 on I/I^2, then (7) is an A-bilinear *symmetric* pairing.

Remark 3.1. Here is a more direct description of the pairing (7). Let $\langle\ ,\ \rangle$ denote the skew-Hermitian pairing corresponding to h, and if $m \in M(A) \subset \Phi/I\Phi$ let $\tilde{m} \in \Phi$ denote any choice of lifting of m. Then, from the definition of $M(A)$, $\langle \tilde{m}, x\rangle \in I \subset R$ for every $x \in \Phi$. If $m_1, m_2 \in M(A)$ we see that the value $\langle \tilde{m}_1, \tilde{m}_2\rangle \in I$, when taken modulo I^2, is dependent only upon the elements $m_1, m_2 \in M(A)$ and independent of the choices of liftings $\tilde{m}_1, \tilde{m}_2 \in \Phi$. Then the A-bilinear pairing (7) is defined by the rule

$$m_1 \otimes m_2 \ \mapsto\ \langle \tilde{m}_1, \tilde{m}_2\rangle \pmod{I^2} \ \in\ I/I^2.$$

Now let us suppose, for simplicity, that A is a principal ideal domain, and denote its field of fractions by $\mathcal{K}$. The natural exact sequence

$$0 \longrightarrow S(A)_{\text{tors}} \longrightarrow S(A) \longrightarrow S(A)_{\text{free}} \longrightarrow 0,$$

decomposing the A-module $S(A)$ into its torsion A-submodule and torsionfree quotient, has a (noncanonical) splitting. Combining this with the natural long exact sequence coming from applying the functor $\operatorname{Hom}_R(S,\ \cdot\ )$ to the exact sequence of R-modules $0 \to A \to \mathcal{K} \to \mathcal{K}/A \to 0$ we obtain an exact sequence

$$0 \longrightarrow \operatorname{Hom}_A(S(A)_{\text{tors}}, \mathcal{K}/A) \longrightarrow \operatorname{Ext}^1_R(S, A) \longrightarrow \operatorname{Ext}^1_R(S, \mathcal{K}),$$

from which we see that the A-torsion submodule of $\operatorname{Ext}^1_R(S, A)$ may be identified with $\operatorname{Hom}_A(S(A)_{\text{tors}}, \mathcal{K}/A)$. Therefore, restricting the isomorphism (6) to $S(A)^\iota_{\text{tors}}$ we obtain a pairing

$$S(A)_{\text{tors}} \otimes_A S(A)^\iota_{\text{tors}} \longrightarrow \mathcal{K}/A \tag{8}$$

which is A-bilinear and nondegenerate.

Remark 3.2. Here is a more direct description of the pairing (8). Suppose $s \in S(A)_{\text{tors}}$, say $as = 0$ with $a \in A$. From the definition (4) of $S(A)$, we can choose $\tilde{s} \in \Phi \otimes A$ and $\tilde{s}^* \in \Phi^* \otimes A$ such that $\tilde{s}^*$ lifts s (under (4)) and $\tilde{s}$ lifts $a\tilde{s}^*$. Similarly, if $t \in S(A)^\iota_{\text{tors}}$ and $bt = 0$ we can lift to $\tilde{t} \in \Phi^\iota \otimes A$ whose image in $(\Phi^*)^\iota \otimes A$ is b times a lift of t.

Let $\langle\ ,\ \rangle_A$ denote the skew-Hermitian pairing $(\Phi \otimes A) \otimes (\Phi^\iota \otimes A) \to A$ induced by h. Then the pairing (8) is given by

$$s \otimes t \mapsto (ab)^{-1}\langle \tilde{s}, \tilde{t}\rangle_A \pmod{A} \ \in (ab)^{-1}A/A \subset \mathcal{K}/A.$$

This is independent of all the choices that were made.

In summary, given a skew-Hermitian module Φ over R, with the hypotheses above, for every ideal $I \subset R$ stable under the action of ι with $A := R/I$ a principal ideal domain, we get an A-bilinear pairing (7) on $M(A)$ with values in I/I^2 and a nondegenerate A-bilinear pairing (8) on $S(A)_{\mathrm{tors}}$ with values in $\mathcal{K}/A$.

In the special case where $I \subset R$ is a switching ideal, the pairing (7) is symmetric and the pairing (8) is skew-symmetric.

4. Discriminants, "L-functions", and regulators

Let Φ be a skew-Hermitian module over R as in §3, and continue to suppose that $A = R/I$ is a principal ideal domain. Denote by $D \in R$ the discriminant of the skew-Hermitian pairing on Φ (well-defined up to an element uu^ι with $u \in R^\times$). Let r denote the rank of the free A-module $M(A)$, and denote by $d \in I^r/I^{r+1}$ the discriminant of the symmetric pairing (7) (well-defined up to an element vv^ι with $v \in A^\times$). Let $s \in A$ denote a generator of the Fitting ideal of the A-torsion module $S(A)_{\mathrm{tors}}$.

Proposition 4.1. *The discriminant D lies in I^r, and if $D^{(r)} \in I^r/I^{r+1}$ denotes the image of D in I^r/I^{r+1} then we have (up to a unit in $A^\times$)*

$$D^{(r)} = d \cdot s.$$

Remark 4.2. One might think of this formula as analogous to the standard (conjectured, or sometimes proved) formulas linking a special value of the r-th derivative of an L-function to the product of a height-pairing regulator times a term which reflects torsion in the Selmer group.

Proof of Proposition 4.1. Form the free A-modules $\Psi := \Phi/I\Phi$ and $\Psi^* := \Phi^*/I\Phi^*$. Then $\Psi^* = \mathrm{Hom}(\Psi^\iota, A)$, and both Ψ and Ψ^* are free over A of rank $g := \mathrm{rank}_R(\Phi)$. The A-module Ψ inherits an A-bilinear skew-Hermitian pairing from the skew-Hermitian pairing on Φ.

Since $M(A)$ is the kernel of $h \otimes A : \Psi \to \Psi^*$, $M(A)$ is a direct summand of Ψ. Fix an R-basis of Φ whose first r elements reduce modulo I to an A-basis of $M(A)$, and let N be the submodule of Ψ generated by the reductions of the last $g - r$ basis elements. Then $\Psi = M(A) \oplus N$, and with respect to this basis the pairing on Φ is given by a matrix

$$B = \begin{pmatrix} B_1 & B_2 \\ B_3 & B_4 \end{pmatrix}$$

where B_1, B_2, and B_3 are $r \times r$, $r \times (g-r)$, and $(g-r) \times r$ matrices with entries in I, and B_4 is a $(g-r) \times (g-r)$ matrix with entries in

R. Thus we see directly that $D = \det(B) \in I^r$ and

$$D^{(r)} \equiv \det(B_1)\det(B_4) \pmod{I^{r+1}}. \tag{9}$$

By Remark 3.1, the matrix giving the pairing (7) on $M(A)$ with respect to our chosen basis is $B_1 \pmod{I^2}$, so $d \equiv \det(B_1) \pmod{I^{r+1}}$.

Let B' and B'_4 be the reductions of B and B_4 modulo I, so their entries lie in A and

$$B' = \begin{pmatrix} 0 & 0 \\ 0 & B'_4 \end{pmatrix}.$$

Then B' is the matrix describing the map $h \otimes A : \Psi \to \Psi^*$. Thus B' has rank $g - r$, so the $(g-r) \times (g-r)$-matrix B'_4 has nonzero determinant in A. Further, we have

$$S(A) = \operatorname{coker}(h \otimes A) = \Psi^*/B'\Psi = M(A)^* \oplus (N^*/B'_4 N)$$

so $S(A)_{\text{tors}} = N^*/B'_4 N$ has Fitting ideal $\det(B'_4)$. Now the proposition follows from (9). □

Part 2. Skew-Hermitian modules and arithmetic

5. The arithmetic of (E, K, p)

Let us fix an elliptic curve E over a number field K, having good ordinary reduction at all primes of K above p. We keep the notation as in §1. Let $\tilde{K}$ be the maximal $\mathbf{Z}_p$-power extension of K, and $\Gamma(K) = \mathrm{Gal}(\tilde{K}/K)$. Let R be a localization of the completed group ring $\mathbf{Z}_p[[\Gamma(K)]]$, viewed as $\mathbf{Z}_p[[\Gamma(K)]]$-algebra, endowed with the (unique) involution $\iota : R \to R$ compatible with the standard involution of $\mathbf{Z}_p[[\Gamma(K)]]$ (given by inversion of group elements). By an *intermediate field extension* L we mean an extension field L of K contained in $\tilde{K}$. Put $H_L := \mathrm{Gal}(\tilde{K}/L) \subset \Gamma(K)$, and note that the ideal I_L of R generated by I_{H_L} is stable under the involution ι and I_K is a switching ideal. Define the quotient R-algebra

$$A_L := R/I_L = R \otimes_{\mathbf{Z}_p[[\Gamma(K)]]} \mathbf{Z}_p[[\mathrm{Gal}(L/K)]].$$

For arbitrary intermediate extensions L define the Selmer A_L-module

$$S(L) = S_p(E, L; R) := \varprojlim_{K'} (S_p(E, K') \otimes_{\mathbf{Z}_p[[\Gamma(K)]]} R),$$

the projective limit being taken over all finite extensions K' of K in L. Denote the R-module $S(\tilde{K})$ simply S.

Assume the following:

Perfect Control axiom. *The natural A_L-homomorphism*

$$S \otimes_R A_L \longrightarrow S(L)$$

is an isomorphism for all intermediate fields L.

Remark 5.1. Although the Perfect Control axiom doesn't universally hold, the homomorphism $S \otimes_R A_L \to S(L)$ usually has rather small kernel and cokernel bounded independent of L (as implied by the "Control Theorem," which holds in a fairly general context) and it is often possible to choose localizations R of $\mathbf{Z}_p[[\Gamma(K)]]$ so as to avoid the support of these kernels and cokernels, and thereby force this axiom to hold (see [M, G]). An alternate strategy is to simply replace the classical Selmer groups $S(L)$ by $S'(L) := S \otimes_R A_L$ relying on the control theorem, when it applies, to guarantee that these $S'(L)$'s are not very different from the $S(L)$'s. In what follows we just assume the Perfect Control axiom.

Put

$$M(L) := \mathrm{Hom}_R(S, A_L)^\iota = \mathrm{Hom}_{A_L}(S(L), A_L)^\iota,$$

the latter equality holding because of the Control axiom. If $L \subset L'$ is an inclusion of intermediate fields, using the first equality above we have a natural induced homomorphism $M(L') \to M(L)$. Moreover, again using the first equality, for any intermediate field L we have

$$M(L) \cong \varprojlim_{K'} M(K')$$

where K' ranges through any increasing sequence of intermediate fields whose union is L. In particular, for any intermediate field L, $M(L)$ can be computed as a projective limit of $M(K')$'s for intermediate fields K' of finite degree over K.

If $L \subset L'$ is an inclusion of intermediate fields of finite degree over K, let $E(L') \to E(L)$ denote the natural trace (also called "norm") mapping on Mordell-Weil groups. For any intermediate field L, of finite degree or not, consider the A_L-module

$$U(L) := \varprojlim_{K'} (E(K')/E(K')_{\mathrm{tors}} \otimes \mathbf{Z}_p) \otimes_{\mathbf{Z}_p[[\Gamma(K)]]} A_L$$

where K' ranges through any increasing sequence of intermediate fields of finite degree over K whose union is L.

Proposition 5.2. *Let L be an intermediate field.*

(i) *If $[L : K]$ is finite and $G = \mathrm{Gal}(L/K)$, then there is a natural isomorphism of A_L-modules*

$$M(L) \cong (E(L)/E(L)_{\mathrm{tors}}) \otimes_{\mathbf{Z}[G]} A_L.$$

(ii) *For arbitrary L there is a natural isomorphism of A_L-modules*

$$M(L) \cong U(L).$$

Proof. We will prove (i), and then (ii) follows by passing to the projective limit. So we assume that L/K is finite. Recall that we have also assumed the Shafarevich-Tate conjecture and the Perfect Control axiom.

We have

$$M(L)^\iota = \mathrm{Hom}_{A_L}(S(L), A_L) = \mathrm{Hom}_{\mathbf{Z}_p[G]}(S_p(E,L), \mathbf{Z}_p[G]) \otimes A_L.$$

The maximal $\mathbf{Z}_p$-torsion-free quotient

$$S_p(E,L)_{\mathrm{free}} := S_p(E,L)/S_p(E,L)_{\mathrm{tors}}$$

of $S_p(E,L)$ satisfies

$$S(L)_{\mathrm{free}} \cong \mathrm{Hom}(E(L), \mathbf{Z}_p).$$

Therefore we get isomorphisms

$$\begin{aligned} \mathrm{Hom}_{\mathbf{Z}_p[G]}(S_p(E,L), \mathbf{Z}_p[G]) &\cong \mathrm{Hom}_{\mathbf{Z}_p[G]}(S_p(E,L)_{\mathrm{free}}, \mathbf{Z}_p[G]) \\ &\cong \mathrm{Hom}_{\mathbf{Z}_p[G]}(\mathrm{Hom}(E(L), \mathbf{Z}_p), \mathbf{Z}_p[G]) \\ &\cong \mathrm{Hom}_{\mathbf{Z}_p}(\mathrm{Hom}(E(L), \mathbf{Z}_p), \mathbf{Z}_p) \\ &\cong (E(L)/E(L)_{\mathrm{tors}}) \otimes \mathbf{Z}_p \end{aligned}$$

using (for example) [Br] Proposition VI.3.4 for the third isomorphism. Tensoring with A_L proves (i). □

Let us now examine whether we have analogues of the two basic isomorphisms (5), (6) of §3. Specifically (assuming the Perfect Control axiom) are there natural isomorphisms of A_L-modules

$$M(L) \overset{?}{\cong} \mathrm{Tor}_R(S, A_L), \qquad S(L)^\iota \overset{?}{\cong} \mathrm{Ext}^1_R(S, A_L) \tag{10}$$

for every intermediate extension L?

In [N2] (cf. §6.6, and passim) Nekovár constructs what he calls the *Selmer complex* of R-modules. Applying his construction to our triple (E, K, p) we get that the associated Selmer complex lies in the derived category of bounded R-modules, and is supplied with a skew-Hermitian self-pairing, which, if one assumes the Perfect Control axiom and the vanishing of what Nekovár calls "error terms," produces the isomorphisms (10). Given a skew-Hermitian R-module Φ let us view the corresponding R-homomorphism $\mathbf{\Phi} = \{\Phi \to \Phi^*\}$ as being a complex in the derived category of bounded R-modules (putting Φ^* in degree 1) and note that the skew-Hermitian pairing gives an isomorphism

$$\eta : \mathbf{\Phi} \xrightarrow{\sim} \mathrm{Hom}_R(\mathbf{\Phi}^\iota, R)[-3].$$

Definition 5.3. Let (E, K, p) be as above,and R a localization of the completed p-adic group ring of $\Gamma(K)$ with involution ι which extends the natural involution on the group ring. Let us say that the skew-Hermitian R-module Φ *organizes the arithmetic of* (E, K, p) if the corresponding R-homomorphism $h : \Phi \to \Phi^*$ is injective, the Perfect Control axiom holds, and the complex $\mathbf{\Phi}$ is quasi-equivalent to Nekovár's Selmer complex, the quasi-equivalence being compatible with skew-Hermitian pairings.

If Φ organizes the arithmetic of (E, K, p), then for every intermediate extension L/K we have an exact sequence of A_L-modules

$$0 \longrightarrow U(L) \longrightarrow \Phi \otimes_R A_L \longrightarrow \Phi^* \otimes_R A_L \longrightarrow S_p(E, L) \otimes A_L \longrightarrow 0.$$

Further, the induced pairing on $U(L)$ described in §3 coincides with the p-adic height pairing on $U(L)$, and if $[L : K]$ is finite and A_L is a principal ideal domain then the induced pairing on $(S_p(E, L) \otimes A_L)_{\mathrm{tors}}$ described in §3 coincides with the Cassels pairing.

6. The classical anticyclotomic setting

In this section we assume all the hypotheses and notation of section 5 and, furthermore, that E is an elliptic curve over $\mathbf{Q}$ without complex multiplication, K is a quadratic imaginary field, and p is an odd prime number. We have that $\Gamma(K)$ is free of rank two over $\mathbf{Z}_p$ and decomposes canonically as the product

$$\Gamma(K) = \Gamma^{\mathrm{anti}} \times \Gamma^{\mathrm{cycl}}$$

where $\Gamma^{\mathrm{anti}} := \mathrm{Gal}(K^{\mathrm{anti}}/K)$ and $\Gamma^{\mathrm{cycl}} := \mathrm{Gal}(K^{\mathrm{cycl}}/K)$. Here K^{anti}/K and K^{cycl}/K are the classical anticyclotomic and cyclotomic $\mathbf{Z}_p$-extensions of K, respectively.

We will be particularly interested in the anticyclotomic $\mathbf{Z}_p$-extension, so put

$$L := K^{\mathrm{anti}}.$$

As in [MR1], [MR2] let us consider the sign of $\chi_K(-N)$ where χ_K is the quadratic Dirichlet character attached to the field K, and N is the conductor of E. Conditional upon the hypotheses that we have made, this sign controls two things. First, thanks to a result of Nekovár [N1], if the sign is "+" then the rank of $E(K)$ is even, and if the sign is "−" then that rank is odd. Thanks also to recent results of Vatsal, Cornut, Kolyvagin and others, if the sign is "+" then $U(L)$ is trivial, while if it is "−" then $U(L)$ is free of rank one over A_L. In the case where the sign is "−" we have the height pairing

$$h_L : U(L) \otimes_{A_L} U(L)^\iota \longrightarrow I_L/I_L^2 = \Gamma^{\mathrm{cycl}} \otimes_{\mathbf{Z}_p} A_L.$$

Under the above hypotheses, in [MR1] we made the following conjecture.

Conjecture 6.1. *If $\chi_K(-N) = -1$ then the height-pairing h_L is an isomorphism of free, rank-one A_L-modules.*

Put another way, Conjecture 6.1 says that the *regulator* of the height pairing h_L on $U(L)$ is a unit.

Now suppose that the skew-Hermitian R-module Φ organizes the arithmetic of (E, K, p), as in Definition 5.3, with $(x, y) \mapsto \langle x, y\rangle$ denoting the R-valued skew-Hermitian pairing on Φ. Choose an element $u \in \Phi$ that projects to a generator of the A_L-module $U(L)$ in $\Phi/I_L\Phi$. Then $\langle u, v\rangle \in I_L$ for all $v \in \Phi$, and Conjecture 6.1 would imply that $\langle u, u\rangle$ is a generator of the ideal $I_L \subset R$.

Under these conditions, the Gram-Schmidt projector $\pi : \Phi \to \Phi$ defined by

$$v \mapsto \pi(v) = v - \frac{\langle v, u\rangle}{\langle u, u\rangle} u$$

splits the skew-Hermitian module Φ into the direct sum of the free, rank-one skew-Hermitian R-module Ru and its orthogonal complement $\pi(\Phi)$.

Remark 6.2. If the Conjecture 6.1 holds, and if there is a skew-Hermitian organizer of the arithmetic of (E, K, p), then under the above conditions when $\chi_K(-N) = -1$ the Selmer complex in the derived category splits as a direct sum of a complex quasi-isomorphic to the complex $R \to R$ (the mapping sending 1 to an "imaginary" generator of I_L) plus another complex. The former complex would account for the universal norms in Mordell-Weil compiled by ascending the anticyclotomic tower; the latter complex cannot vanish if the rank of the Mordell-Weil group of E over K is greater than 1 and indeed the R-rank g of an organizer Φ must be at least equal to the rank of the Mordell-Weil group of E over K.

Remark 6.3. If Φ organizes the arithmetic of (E, K, p), then the characteristic ideal of the Selmer R-module S is the discriminant D of the pairing $h : \Phi \to \Phi^*$. In this situation the "two-variable main conjecture" is equivalent to the following.

Conjecture 6.4. *The discriminant of h is equal, up to a unit in R, to the two-variable p-adic L-function of Haran and Hida* [Ha, Hi, PR1, PR2].

For more about the relation between our setup and other anticyclotomic conjectures, see [MR1].

References

[Br] K. Brown, Cohomology of groups, *Grad. Texts in Math.* **87**, Springer, New York (1982).

[Co] C. Cornut, Mazur's conjecture on higher Heegner points, *Invent. math.* **148** (2002) 495–523.

[G] ———, Galois theory for the Selmer group of an abelian variety. To appear.

[Ha] S. Haran, p-adic L-functions for elliptic curves over CM fields, thesis, MIT 1983.

[Hi] H. Hida, A p-adic measure attached to the zeta functions associated with two elliptic modular forms. I, *Invent. Math.* **79** (1985), 159–195.

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

[MR1] B. Mazur, K. Rubin, Elliptic curves and class field theory. In: *Proceedings of the International Congress of Mathematicians, ICM 2002, Beijing,* Ta Tsien Li, ed., vol II. Beijing: Higher Education Press (2002) 185–195.

[MR2] ———, Studying the growth of Mordell-Weil. To appear in a special issue of *Documenta Math.* dedicated to K. Kato.

[MT] B. Mazur, J. Tate, Canonical height pairings via biextensions. In: *Arithmetic and Geometry*, Progr. Math. **35**, Birkhaüser, Boston (1983) 195–237.

[N1] J. Nekovář, On the parity of ranks of Selmer groups. II, *C. R. Acad. Sci. Paris Sér. I Math.* **332** (2001) 99–104.

[N2] ———, Selmer complexes. Preprint available at `http://www.math.jussieu.fr/∼nekovar/pu/`.

[PR1] B. Perrin-Riou, Fonctions L p-adiques, théorie d'Iwasawa et points de Heegner, *Bull. Soc. Math. France* **115** (1987), 399–456.

[PR2] ———, Points de Heegner et dérivées de fonctions L p-adiques, *Invent. Math.* **89** (1987), 455–510.

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

Department of Mathematics, Harvard University, Cambridge, MA 02138 USA

E-mail address: `mazur@math.harvard.edu`

Department of Mathematics, Stanford University, Stanford, CA 94305 USA

E-mail address: `rubin@math.stanford.edu`