Derived heights and generalized Mazur-Tate regulators

Massimo Bertolini
Henri Darmon

September 9, 2007

Contents

1 Introduction

Let E be an elliptic curve defined over a number field K, and let L/K be an abelian extension with Galois group G. In [MT1] and [MT2], B. Mazur and J. Tate have defined a height pairing

$$\langle\ ,\ \rangle_{MT} : E_L(K) \times E(K) \longrightarrow G,$$

where $E_L(K)$ is a subgroup of finite index of $E(K)$, consisting of the points of $E(K)$ that are local norms from $E(L)$. Let I denote the augmentation ideal in the integral group ring $\mathbf{Z}[G]$. There is a canonical identification $G = I/I^2$, allowing us to view the Mazur-Tate pairing as taking values in I/I^2. Let $P_1, \ldots, P_r$, (resp. $Q_1, \ldots, Q_r$) denote integral bases for $E_L(K)$ (resp. $E(K)$) modulo torsion. The matrix $(\langle P_i, Q_j \rangle_{MT})$ is an $r \times r$ matrix with entries in I/I^2, and its determinant gives an element of I^r/I^{r+1}. Let Λ_{MT} denote this element; it is the Mazur-Tate regulator associated to $(E, L/K)$.

The goal of this paper is to define (under certain conditions) a lift $\tilde{\Lambda}$ of Λ_{MT} to I^r. This lift depends on some choices, but the following are independent of the choices:

1. The order of vanishing of $\tilde{\Lambda}$, defined to be the least ρ (possibly ∞) such that $\tilde{\Lambda}$ belongs to I^ρ but not to $I^{\rho+1}$.

2. The image Λ of $\tilde{\Lambda}$ in $I^\rho/I^{\rho+1}$.

We call Λ the generalized Mazur-Tate regulator associated to $(E, L/K)$. It is equal to the Mazur-Tate regulator when $\rho = r$, but provides extra information when $\Lambda_{MT} = 0$. In particular, it can be used to formulate a refined conjecture in the spirit of [MT2].

The conjecture of [MT2] relates the Mazur-Tate regulator to the leading coefficient of a θ-element interpolating special values of the Hasse-Weil L-function of E/K. In particular, it predicts that the order of vanishing of this element is at least r, but that some extra vanishing may arise from degeneracies in the Mazur-Tate height (i.e., when $\Lambda_{MT} = 0$). We formulate a conjecture predicting the precise order of vanishing of the element θ, and expressing the value of its leading coefficient in terms of our generalized regulator Λ. In certain cases, we show that our refinement of the Mazur-Tate conjecture follows from the classical conjecture of Birch and Swinnerton-Dyer.

A particularly interesting special case (which partly motivated the present study) arises when K is a quadratic field and L/K is an extension of K of dihedral type. In this case, degeneracies in the Mazur-Tate height seem to be the rule rather than the exception. This case is discussed in section 4.3.

2 Algebraic preliminaries

2.1 Notations and conventions

Given a global field F, and v a place of F, let F_v denote the completion of F at v, and let $F(v)$ denote the residue field. Similarly, if F'/F is a finite extension of F, let $F'_v := \oplus_{w|v} F'_w$, and $F'(v) := \oplus_{w|v} F'(w)$, where the direct sums are taken over all places w of F above v. If F'/F is Galois with group G, then F'_v is similarly equipped with a G-action.

If $\mathcal{E}$ denotes a group scheme over F, then the Galois cohomology groups $H^i(F, \mathcal{E})$ are defined in the usual way, and $H^i(F_v, \mathcal{E})$ is the local counterpart. By convention we write $H^i(F'_v, \mathcal{E}) := \oplus_{w|v} H^i(F'_w, \mathcal{E})$. The group $H^i(F'_v, \mathcal{E})$ is a G-module in a natural way, and is canonically isomorphic as a G-module to the induced module $\mathrm{ind}_{G_w}^{G} H^i(F'_w, \mathcal{E})$, where G_w denotes the decomposition group at w. There is a natural localization map at v (arising from the restriction map)

$$\mathrm{res}_v : H^i(F', \mathcal{E}) \longrightarrow H^i(F'_v, \mathcal{E})$$

which is G-equivariant.

Let E be an elliptic curve defined over F. In this paper, $\mathcal{E}$ will be either the group scheme E_n of n-torsion points on E, or E itself.

Let $\mathbf{A}_F$ denote the ring of adèles of F. We will be particularly interested in the following cohomology groups:

$$\begin{aligned} H^1(\mathbf{A}_F, E_n) &:= \coprod_v H^1(F_v, E_n), \\ H^1(\mathbf{A}_F, E) &:= \oplus_v H^1(F_v, E). \end{aligned}$$

The symbol $\coprod$ denotes restricted direct product with respect to the subgroups $E(F_v)/nE(F_v)$ of $H^1(F_v, E_n)$ (with the inclusions arising from the local n-descent exact sequence). Using this notation, we can combine the local and

global n-descent exact sequences into a commutative diagram:

$$\begin{array}{ccccccccc} & & & & & & 0 & & \\ & & & & & & \downarrow & & \\ 0 & \longrightarrow & E(F)/nE(F) & \longrightarrow & \mathrm{Sel}_n(E/F) & \longrightarrow & \underline{Ш}_n(E/F) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & E(F)/nE(F) & \longrightarrow & H^1(F, E_n) & \longrightarrow & H^1(F, E)_n & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & E(\mathbf{A}_F)/nE(\mathbf{A}_F) & \longrightarrow & H^1(\mathbf{A}_F, E_n) & \longrightarrow & H^1(\mathbf{A}_F, E)_n & \longrightarrow & 0, \end{array}$$

in which the horizontal sequences and the rightmost vertical one are exact.

2.2 Duality

2.2.1 Local Duality

Reference: [Mi], [Ta].

This section summarizes the local Tate duality. Let E be an elliptic curve defined over a local field K.

Proposition 2.1 *The cup product induces a perfect, symmetric, Galois-equivariant pairing*

$$\langle\ ,\ \rangle_{K,n} : H^1(K, E_n) \times H^1(K, E_n) \longrightarrow \mathbf{Z}/n\mathbf{Z}.$$

Let a and b be classes in $H^1(K, E_n)$ and let $a \cup b \in H^2(K, E_n \otimes E_n)$ be their cup-product. The alternating Weil pairing $E_n \otimes E_n \longrightarrow \mu_n$ gives rise to a map $w : H^2(K, E_n \otimes E_n) \longrightarrow H^2(K, \mu_n) = \mathbf{Z}/n\mathbf{Z}$. We define

$$\langle a, b\rangle_{K,n} = w(a \cup b).$$

Recall the local descent exact sequence

$$0 \longrightarrow E(K)/nE(K) \longrightarrow H^1(K, E_n) \longrightarrow H^1(K, E)_n \longrightarrow 0.$$

Proposition 2.2 *The image of $E(K)/nE(K)$ in $H^1(K, E_n)$ is the exact annihilator of itself under the pairing $\langle\ ,\ \rangle_{K,n}$. Hence, there is a perfect pairing*

$$[\ ,\ ]_{K,n} : E(K)/nE(K) \times H^1(K, E)_n \longrightarrow \mathbf{Z}/n\mathbf{Z}.$$

In fact, the duality between $E(K)/nE(K)$ and $H^1(K,E)_n$ comes from a perfect pairing

$$[\ ,\ ]_K : E(K) \times H^1(K,E) \longrightarrow \mathbf{Q}/\mathbf{Z}.$$

Let L/K be a finite Galois extension, with Galois group G.

Proposition 2.3 *The pairing $[\ ,\ ]_K$ induces a perfect duality between the groups $\hat{H}^0(G,E(L))$ and $\hat{H}^1(G,E(L))$.*

The compatibility of the cup product under norms gives:

Proposition 2.4 .

1. *If a belongs to $H^1(L,E_n)$ and b belongs to $H^1(K,E_n)$, then*

$$\langle a, \mathrm{res}_{L/K}(b)\rangle_{L,n} = \langle \mathrm{Cores}_{L/K}(a), b\rangle_{K,n}.$$

2. *If a belongs to $E(L)/nE(L)$ and b belongs to $H^1(K,E)_n$, then*

$$[a, \mathrm{res}_{L/K}(b)]_{L,n} = [\mathrm{Cores}_{L/K}(a), b]_{K,n}.$$

2.2.2 Global Duality

Let E be an elliptic curve defined over a number field K. The sum of the local pairings of prop. 2.1 gives a perfect, symmetric, Galois-equivariant pairing

$$\langle\ ,\ \rangle_{K,n} : H^1(\mathbf{A}_K, E_n) \times H^1(\mathbf{A}_K, E_n) \longrightarrow \mathbf{Z}/n\mathbf{Z}.$$

Similarly we have a perfect pairing

$$[\ ,\ ]_{K,n} : E(\mathbf{A}_K)/nE(\mathbf{A}_K) \times H^1(\mathbf{A}_K, E)_n \longrightarrow \mathbf{Z}/n\mathbf{Z}.$$

Proposition 2.5 *The image of $H^1(K,E_n)$ in $H^1(\mathbf{A}_K,E_n)$ is isotropic with respect to $\langle\ ,\ \rangle_{K,n}$.*

Proof: Let a and b be classes in $H^1(K,E_n)$, and let a_v and b_v denote their localisations in $H^1(K_v,E_n)$, for v a place of K. Then

$$\langle a,b\rangle_{K,n} = \sum_v \langle a_v, b_v\rangle_{K_v,n} = \sum_v \mathrm{res}_v(w(a\cup b)) = 0,$$

where the last equality follows from the global reciprocity law of class field theory.

Proposition 2.6 *A class $a \in H^1(\mathbf{A}_K, E_n)$ annihilates $\mathrm{Sel}_n(E/K)$ under the pairing $\langle\ ,\ \rangle_{K,n}$ if and only if one can write $a = a_1 + a_2$, where a_1 belongs to the image of $H^1(K, E_n)$ in $H^1(\mathbf{A}_K, E_n)$ and a_2 belongs to the image of $E(\mathbf{A}_K)/nE(\mathbf{A}_K)$ in $H^1(\mathbf{A}_K, E_n)$.*

Proof: See [Mi], lemma 6.15, p. 105. (Note that a part of prop. 2.6 follows from props 2.2 and 2.5.)

Corollary 2.7 *There is an exact sequence*

$$0 \longrightarrow \mathrm{Sel}_n(E/K) \longrightarrow H^1(K, E_n) \longrightarrow H^1(\mathbf{A}_K, E)_n \longrightarrow \mathrm{Sel}_n(E/K)^*,$$

where $\mathrm{Sel}_n(E/K)^*$ denotes the Pontryagin dual of $\mathrm{Sel}_n(E/K)$.

Let L/K be a finite Galois extension with Galois group G.

Proposition 2.8 .

1. *If a belongs to $H^1(\mathbf{A}_L, E_n)$ and b belongs to $H^1(\mathbf{A}_K, E_n)$, then*

$$\langle a, \mathrm{res}_{L/K}(b)\rangle_{L,n} = \langle \mathrm{Cores}_{L/K}(a), b\rangle_{K,n}.$$

2. *If a belongs to $E(\mathbf{A}_L)/nE(\mathbf{A}_L)$ and b belongs to $H^1(\mathbf{A}_K, E)_n$, then*

$$[a, \mathrm{res}_{L/K}(b)]_{L,n} = [\mathrm{Cores}_{L/K}(a), b]_{K,n}.$$

Proof: This follows imediately from prop. 2.4.

Let R denote the group ring $\mathbf{Z}/n\mathbf{Z}[G]$.

Definition 2.9 *We define the R-valued pairing*

$$\langle\ ,\ \rangle_{L/K,n} : H^1(\mathbf{A}_L, E_n) \times H^1(\mathbf{A}_L, E_n) \longrightarrow R$$

by

$$\langle a, b\rangle_{L/K,n} := -\sum_{\sigma \in G} \langle a, b^\sigma\rangle_{L,n} \cdot \sigma.$$

Let $\gamma \mapsto \gamma^*$ be the involution in the group ring R which sends every group element σ to σ^{-1}. Let $\epsilon : R \longrightarrow \mathbf{Z}/n\mathbf{Z}$ denote the augmentation map, defined by

$$\epsilon(\sum n_\sigma \cdot \sigma) = \sum n_\sigma.$$

Proposition 2.10 .

1. *The pairing* $\langle\ ,\ \rangle_{L/K,n}$ *is a perfect pairing. It is* R*-linear in the first variable and* $*$*-linear in the second, i.e., for all* $\gamma \in R$*,*

$$\langle \gamma a, b\rangle_{L/K,n} = \gamma\langle a, b\rangle_{L/K,n}, \quad \langle a, \gamma b\rangle_{L/K,n} = \gamma^*\langle a, b\rangle_{L/K,n}.$$

2. *For all* $a, b \in H^1(\mathbf{A}_L, E_n)$*, we have* $\langle a, b\rangle_{L/K,n} = \langle b, a\rangle^*_{L/K,n}$*.*

3. $\epsilon(\langle a, b\rangle_{L/K,n}) = -\langle \mathrm{Cores}_{L/K}(a), \mathrm{Cores}_{L/K}(b)\rangle_{K,n}$*.*

4. *The image of* $E(\mathbf{A}_L)/nE(\mathbf{A}_L)$ *in* $H^1(\mathbf{A}_L, E_n)$ *is isotropic for the pairing* $\langle\ ,\ \rangle_{L/K,n}$*.*

5. *The image of* $H^1(L, E_n)$ *in* $H^1(\mathbf{A}_L, E_n)$ *is isotropic for the pairing* $\langle\ ,\ \rangle_{L/K,n}$*.*

Proof:
1. follows from the fact that $\langle\ ,\ \rangle_{L,n}$ is perfect and G-equivariant (prop. 2.1).
2. follows from the symmetry of $\langle\ ,\ \rangle_{L,n}$ by a formal computation.
3. follows from prop. 2.8.
4. follows from prop. 2.2.
5. follows from prop. 2.5.

2.3 Assumptions

Let E be an elliptic curve over a number field K.

Let E/E^0 be the group of connected components in the Néron model of E over $\mathrm{Spec}\mathcal{O}_K$. Let p be a prime which satisfies the following assumptions:

Assumption 2.11 *Assume that*

1. *The prime* p *does not divide* $2\#E/E^0$*.*

2. *The curve* E/K *has good reduction at all primes above* p*.*

3. *The image of* $Gal(\bar{K}/K)$ *in* $\mathrm{Aut}\,(E_p)$ *contains a Cartan subgroup of* $\mathrm{Aut}\,(E_p) \simeq \mathbf{GL}_2(\mathbf{F}_p)$*.*

Conditions 1 and 2 exclude only a finite set of primes, and so does condition 3 by a result of Serre [Se] and by the theory of complex multiplication.

Let L be an abelian extension of K of degree a power of p. Let G be its Galois group. The assumptions 2.11 have the following consequences:

Lemma 2.12 *The group $E_p(L)$ is trivial.*

Proof: The image of $\mathrm{Gal}(L(E_p)/L)$ in $\mathrm{Aut}\,(E_p)$ also contains a Cartan subgroup of $\mathrm{Aut}\,(E_p)$.

Lemma 2.13 *The group $H^i(Gal(L(E_{p^m})/L), E_{p^m})$ is trivial for all i.*

Proof: Identify $\mathrm{Gal}(L(E_{p^m})/L)$ with a subgroup of $\mathbf{GL}_2(\mathbf{Z}/p^m\mathbf{Z})$; the scalar matrix -1 belongs to $\mathrm{Gal}(L(E_{p^m})/L)$, since this is true for $m = 1$ and p is odd. Let $Z = \{\pm 1\}$ be the group generated by this element. Every term in the Hochschild-Serre spectral sequence

$$H^i(\mathrm{Gal}(L(E_{p^m})/L)/Z, H^j(Z, E_{p^m})) \Rightarrow H^{i+j}(\mathrm{Gal}(L(E_{p^m})/L), E_{p^m})$$

is 0, since $H^j(Z, E_{p^m}) = 0$. (For $j = 0$, this follows from the fact that Z does not fix any non-trivial vector in E_p, and for $j > 0$, it follows from the fact that p does not divide the order of Z.)

Corollary 2.14 *The restriction map $H^1(K, E_{p^m}) \longrightarrow H^1(L(E_{p^m}), E_{p^m})$ is injective.*

Proof: The restriction map $H^1(K, E_{p^m}) \longrightarrow H^1(L, E_{p^m})$ is injective. (Its kernel is $H^1(G, E_{p^m}(L))$ which is zero, by lemma 2.12.) Likewise the restriction map $H^1(L, E_{p^m}) \longrightarrow H^1(L(E_{p^m}), E_{p^m})$ is injective by lemma 2.13. The corollary follows.

For all places v of K, there is the local norm map

$$\mathrm{norm}_v : E(L_v) \longrightarrow E(K_v).$$

Throughout the paper we make the following crucial assumption on L:

Assumption 2.15 *The local maps $norm_v$ are surjective for all v.*

When the local norm maps fail to be surjective, the Mazur-Tate height may fail to be defined on the full Mordell-Weil group $E(K)$, and the theory of derived heights and generalized regulators becomes considerably more complicated.

We hasten to reassure the reader that there are sufficiently many pairs $(E, L/K)$ for which this assumption is satisfied, so that our theory is not vacuous! Let $\mathrm{ram}_{L/K}$ be the set of primes of K which ramify in L, and consider the finite product

$$\Pi(E, L/K) = \prod_{v \in \mathrm{ram}_{L/K}} \#E(K(v)).$$

Then we have:

Proposition 2.16 (Mazur) *If $v \in ram_{L/K}$ is a prime of residue characteristic p, assume that E is ordinary at v. Then assumption 2.15 is satisfied if and only if p does not divide $\Pi(E, L/K)$.*

Proof: See [Ma], §4.

Thus, consider the set of places v of K such that the image of Frob_v in $\mathrm{Gal}(K(E_p)/K) = \mathbf{GL}_2(\mathbf{F}_p)$ does not fix any non-trivial point in E_p. There are infinitely many such v's (in fact, they form a set of positive density) by Chebotarev's theorem. Any extension L which is ramified only at these primes is such that p does not divide $\Pi(E, L/K)$.

2.4 Preliminary calculations

Lemma 2.17 *For all v, the module $E(L_v)$ is a cohomologically trivial G-module.*

Proof: By assumption 2.15, $\hat{H}^0(G, E(L_v)) = 0$. Therefore the cohomology group $\hat{H}^1(G, E(L_v))$ also vanishes, by prop. 2.3. The result then follows from theorem 9, p. 113 of [CF].

Lemma 2.18 *For all v, the restriction map $H^1(K_v, E) \longrightarrow H^1(L_v, E)^G$ is an isomorphism.*

Proof: The kernel and cokernel of this map are the groups $H^1(G, E(L_v))$ and $H^2(G, E(L_v))$ respectively. The result follows from lemma 2.17.

Fix a power p^m of p.

Lemma 2.19 *The restriction maps*

$$H^1(K, E_{p^m}) \longrightarrow H^1(L, E_{p^m})^G, \qquad \mathrm{Sel}_{p^m}(E/K) \longrightarrow \mathrm{Sel}_{p^m}(E/L)^G$$

are isomorphisms.

Proof: The analysis of the spectral sequence

$$H^i(G, H^j(L, E_{p^m})) \Rightarrow H^{i+j}(K, E_{p^m})$$

together with the fact (lemma 2.12) that $E_{p^m}(L) = 0$ reveals that the restriction map $H^1(K, E_{p^m}) \longrightarrow H^1(L, E_{p^m})^G$ is an isomorphism. Hence, the restriction is injective on $\mathrm{Sel}_{p^m}(E/K)$. To show that res : $\mathrm{Sel}_{p^m}(E/K) \longrightarrow \mathrm{Sel}_{p^m}(E/L)^G$ is surjective, let s_L be an element of $\mathrm{Sel}_{p^m}(E/L)^G$. Then there exists a class $s_K \in H^1(K, E_{p^m})$ such that $\mathrm{res}(s_K) = s_L$. But s_K actually belongs to $\mathrm{Sel}_{p^m}(E/K)$, by lemma 2.18.

Definition 2.20 *A prime v of K is said to be admissible for $(E, L/K, p^m)$ if*

1. *E has good reduction at v.*
2. *v does not divide p.*
3. *v splits completely in L/K.*
4. *The group $H^1(K_v, E)_{p^m}$ (or, equivalently, $E(K_v)/p^m E(K_v)$, by prop. 2.2) is isomorphic to $(\mathbf{Z}/p^m\mathbf{Z})^2$.*

Often we will content ourselves with saying that a prime v, (or, later, a set of primes) is admissible, keeping the dependence on $(E, L/K, p^m)$ implicit when there is no danger of confusion.

Lemma 2.21 *For all $s \in \mathrm{Sel}_{p^m}(E/K)$, there exist infinitely many admissible primes v such that the map*

$$\langle s \rangle \longrightarrow E(K_v)/p^m E(K_v)$$

is injective. (Here $\langle s \rangle$ denotes the subgroup of $\mathrm{Sel}_{p^m}(E/K)$ generated by s.)

Proof: We can identify s with a homomorphism from $\mathrm{Gal}(\bar{K}/L(E_{p^m}))$ into E_{p^m}, by cor. 2.14. Let S be the non-trivial extension $L(E_{p^m})$ cut out by this homomorphism. Consider now the following diagram of field extensions:

$$\begin{array}{c} S \\ | \\ L(E_{p^m}) \\ | \\ K. \end{array}$$

By the Chebotarev density theorem we can choose infinitely many places v of K such that $\mathrm{Frob}_v(S/K)$ belongs to $\mathrm{Gal}(S/L(E_{p^m})$, and such that the order of $\mathrm{Frob}_v(S/K)$ is the same as the order of s in $\mathrm{Sel}_{p^m}(E/K)$. In particular, we can choose such v satisfying condition 1 and 2 in the definition of admissible prime. That condition 3 is satisfied is immediate from the choice of v, and condition 4 is satisfied because $E(K_v)_{p^m}$, and hence $E(K_v)/p^mE(K_v)$, are isomorphic to $(\mathbf{Z}/p^m\mathbf{Z})^2$ as abstract groups. This completes the proof, since $\langle s \rangle$ injects in $E(K_v)/p^mE(K_v)$.

Definition 2.22 *A set S of primes is said to be admissible for $(E, L/K, p^m)$ if*

1. *All $v \in S$ are admissible for $(E, L/K, p^m)$.*
2. *The map $\mathrm{Sel}_{p^m}(E/K) \longrightarrow \prod_{v \in S} E(K_v)/p^mE(K_v)$ is an injection.*

Lemma 2.23 *Admissible sets exist.*

Proof: This follows from lemma 2.21.

Choose once and for all an admissible set S.

Let F be a field extension intermediate between K and L.

Definition 2.24 *A cohomology class c belonging to the group $H^1(F, E)_{p^m}$ or $H^1(\mathbf{A}_F, E)_{p^m}$ is said to be admissible for $(E, L/F, p^m)$ if its localisation to $H^1(F_v, E)$ is 0, for all v not in S. Likewise,a cohomology class in the group $H^1(F, E_{p^m})$ or $H^1(\mathbf{A}_F, E_{p^m})$ is called admissible if it maps to an admissible class in $H^1(F, E)_{p^m}$ or $H^1(\mathbf{A}_F, E)_{p^m}$ respectively. Denote by $H^1_S(-, E)_{p^m}$ (resp. $H^1_S(-, E_{p^m})$) the group of admissible classes in $H^1(-, E)_{p^m}$ (resp. $H^1(-, E_{p^m})$).*

Lemma 2.25 *The map* $\mathrm{Sel}_{p^m}(E/F) \longrightarrow \oplus_{v\in S} E(F_v)/p^m E(F_v)$ *is injective, i.e., the set of primes of* F *lying above the places in* S *is admissible for* $(E, L/F, p^m)$.

Proof: Let $\mathcal{K}$ denote the kernel of the map

$$\mathrm{Sel}_{p^m}(E/F) \longrightarrow \oplus_{v\in S} E(F_v)/p^m E(F_v).$$

If $\mathcal{K}$ is non-trivial, then there exists a non-trivial vector in $\mathcal{K}$ invariant under the action of G. By lemma 2.19, this vector gives a non-trivial element in $\mathrm{Sel}_{p^m}(E/K)$ which maps to 0 in $\oplus_{v\in S} E(K_v)/p^m E(K_v)$, a contradiction, since S was assumed admissible for $(E, L/K, p^m)$.

Lemma 2.26 *The map* $H^1_S(\mathbf{A}_F, E)_{p^m} \longrightarrow \mathrm{Hom}(\mathrm{Sel}_{p^m}(E/F), \mathbf{Z}/p^m\mathbf{Z})$ *is surjective.*

Proof: This is simply dual to property 2 in the definition 2.22 of an admissible set, and hence follows from lemma 2.25.

Lemma 2.27 *The restriction map* $H^1_S(K, E_{p^m}) \longrightarrow H^1_S(L, E_{p^m})^G$ *is an isomorphism.*

Proof: As in the proof of lemma 2.19.

3 The generalized regulator

3.1 The modules A_S and B_S

Let A_S and B_S be the following modules:

$$A_S := \oplus_{v\in S} E(L_v)/p^m E(L_v),$$

$$B_S := H^1_S(L, E_{p^m}).$$

Lemma 3.1 *Let* F *be a subextension of* L/K. *We have the exact sequence*

$$\begin{aligned} 0 \longrightarrow\ & \mathrm{Sel}_{p^m}(E/F) \longrightarrow H^1_S(F, E_{p^m}) \longrightarrow H^1_S(\mathbf{A}_F, E)_{p^m} \longrightarrow \\ \longrightarrow\ & \mathrm{Sel}_{p^m}(E/F)^* \longrightarrow 0. \end{aligned}$$

Proof: The surjectivity of the last arrow in this sequence is lemma 2.26. The exactness for the rest of the sequence is stated in cor. 2.7, and does not depend on the assumption that S is admissible.

Let R denote the group ring $\mathbf{Z}/p^m\mathbf{Z}[G]$. The modules A_S and B_S are equipped with a natural R-module structure. Let $t = 2\#S$.

It follows immediately from the definition of an admissible set that the module A_S is a free R-module of rank t. The following theorem states that the same is true for B_S:

Theorem 3.2 *The module B_S is isomorphic to R^t as an R-module.*

Proof: We will prove this in three steps.
Step 1: Assume $m = 1$, $G \simeq \mathbf{Z}/p\mathbf{Z}$. The exact sequence of lemma 3.1 with $F = K$, combined with lemma 2.27, shows that

$$\dim_{\mathbf{F}_p} B_S^G = \dim_{\mathbf{F}_p} \oplus_{v\in S} H^1(K_v, E)_p.$$

By the definition of admissible prime, is follows that $\dim_{\mathbf{F}_p} B_S^G = t$.

When $m = 1$ and $G = \mathbf{Z}/p\mathbf{Z}$, the group ring R has a particularly simple structure: it is isomorphic to the local ring $\mathbf{F}_p[\epsilon]/(\epsilon^p)$, where $\epsilon = (\sigma - 1)$ and σ is a generator of G. Every finitely generated R-module M can be written as a direct sum of cyclic R-modules, and the number of summands is $\dim_{\mathbf{F}_p} M^G$. Hence, we can write

$$B_S = V_1 \oplus \cdots \oplus V_t,$$

where the V_i are cyclic modules over R. Let $n_i = \dim_{\mathbf{F}_p} V_i$. By lemma 3.1 with $F = L$, we find

$$pt = \dim_{\mathbf{F}_p} H_S^1(\mathbf{A}_L, E)_p = \dim_{\mathbf{F}_p} B_S = \sum_{i=1}^{t} n_i.$$

Since $n_i \leq p$ for all i, we have $n_i = p$ for all i, and hence B_S is isomorphic to R^t.

Step 2: Assume $m = 1$, G arbitrary abelian p-group. Since $\dim_{\mathbf{F}_p} B_S^G = t$, it is enough to show that B_S is a free $\mathbf{F}_p[G]$-module. By [CF], theorem 6, p. 112, it suffices to prove that $\hat{H}^0(G, B_S) = 0$. We prove this by induction

on the order of G. When $\#G = p$, this follows from step 1. In general, let F be a subextension of L/K with $\mathrm{Gal}(L/F) \simeq \mathbf{Z}/p\mathbf{Z}$. Note that the set of primes of F above the primes of S is admissible for $(E, L/F, p)$, by lemma 2.25. Hence by step 1, $\hat{H}^0(\mathrm{Gal}(L/F), B_S) = 0$. By the inductive hypothesis, $\hat{H}^0(\mathrm{Gal}(F/K), H^1_S(F, E_p)) = 0$. This completes step 2.

Step 3: General case; m and G are arbitrary.

Lemma 3.3 *Let $B_S[p]$ denote the p-torsion submodule of B_S. Then*

$$B_S[p] \simeq \mathbf{Z}/p\mathbf{Z}[G]^t.$$

Proof: It is a direct consequence of lemma 2.12 that $B_S[p] = H^1_S(L, E_p)$. The result now follows from step 2 applied to $H^1_S(L, E_p)$.

Lemma 3.4 *The module B_S is free as a $\mathbf{Z}/p^m\mathbf{Z}$-module.*

Proof: Let d denote the degree of L over K. By lemma 3.3,

$$B_S \simeq \oplus_{i=1}^{td} \mathbf{Z}/p^{n_i}\mathbf{Z}, \quad n_i \leq m.$$

By lemma 3.1 with $F = L$,

$$\#(B_S) = \#(\oplus_{v \in S} H^1(L_v, E)_{p^m}) = p^{tdm}.$$

Hence, $n_i = m$ for all i.

Step 3 is a consequence of lemmas 3.3 and 3.4, combined with the following module-theoretic observation:

Lemma 3.5 *Let M be an R module such that*

1. *The p-torsion submodule M_p is isomorphic to $\mathbf{Z}/p\mathbf{Z}[G]^t$,*
2. *The module M is $\mathbf{Z}/p^m\mathbf{Z}$-free.*

Then $M \simeq R^t$.

Proof: Let $\omega_1, \ldots, \omega_t$ be a basis for M_p over $\mathbf{Z}/p\mathbf{Z}[G]$. By 2, there exists $\tilde{\omega}_1, \ldots \tilde{\omega}_t$ such that $p^{m-1}\tilde{\omega}_i = \omega_i$ for all i. Define a map $\phi : R^t \longrightarrow M$ by $\phi(\alpha_1, \ldots, \alpha_t) = \sum_{i=1}^t \alpha_i \tilde{\omega}_i$. It induces an isomorphism on p-torsion, hence it is injective. Surjectivity follows by comparing the orders of R^t and M.

Let Ω_S be the R-module $\oplus_{v \in S} H^1(L_v, E_{p^m})$.

Lemma 3.6 *The module Ω_S is a free R-module of rank $2t$.*

Proof: This follows from the descent exact sequence

$$0 \longrightarrow E(L_v)/p^m E(L_v) \longrightarrow H^1(L_v, E_{p^m}) \longrightarrow H^1(L_v, E)_{p^m} \longrightarrow 0,$$

since the modules on both sides of this exact sequence are free when $v \in S$, by properties 3 and 4 in definition 2.20 of admissible primes.

Lemma 3.7 *The natural maps $A_S \longrightarrow \Omega_S$ and $B_S \longrightarrow \Omega_S$ are injective. The intersection of the images of A_S and B_S is the image of $\mathrm{Sel}_{p^m}(E/L)$ in Ω_S.*

Proof: The injectivity of $B_S \longrightarrow \Omega_S$ follows from property 2 in the definition 2.22 of an admissible set. The other facts are clear.

By lemma 3.7 one can view A_S, B_S, and $\mathrm{Sel}_{p^m}(E/L)$ as R-submodules of Ω_S. Abusing notation, we will do this identification when necessary; for example, we will write $A_S \cap B_S = \mathrm{Sel}_{p^m}(E/L)$.

3.2 The regulator in R/R^*

One can view Ω_S as a submodule of $H^1(\mathbf{A}_L, E_{p^m})$; let

$$\langle\ ,\ \rangle : \Omega_S \times \Omega_S \longrightarrow R$$

denote the restriction of the pairing $\langle\ ,\ \rangle_{L/K,p^m}$ to Ω_S. Now, let $\Gamma_A = (a_1, \cdots a_t)$, $\Gamma_B = (b_1, \cdots, b_t)$ denote R-module bases for A_S and B_S respectively. We view Γ_A and Γ_B as either row or column vectors with entries in A_S and B_S, when appropriate. The matrix

$$\Theta(\Gamma_A, \Gamma_B) = (\langle a_i, b_j \rangle)_{1 \le i,j \le t}$$

is a $t \times t$ matrix with entries in R. Let $\Lambda(\Gamma_A, \Gamma_B) \in R$ be its determinant.

Let R^* denote the group of units in R. Let I denote the augmentation ideal of R, i.e., $I = \ker(\epsilon)$.

Lemma 3.8 *R^* consists exactly of the elements $\alpha \in R$ such that $\epsilon(\alpha)$ belongs to $(\mathbf{Z}/p^m\mathbf{Z})^*$.*

Proof: If α is a unit, then so is $\epsilon(\alpha)$. Conversely, if $\epsilon(\alpha) = u \in (\mathbf{Z}/p^m\mathbf{Z})^*$, then we may write $\alpha = u + \alpha_0$, where α_0 belongs to I. But α_0 is nilpotent, and it follows that α is invertible. (A sum of a unit and a nilpotent element is invertible.)

Proposition 3.9 *The value of $\Lambda(\Gamma_A, \Gamma_B)$ is independent of the choice of Γ_A and Γ_B, and on the choice of the admissible set S, up to multiplication by a unit in R^*.*

Proof: First, given a fixed S, we study how $\Lambda(\Gamma_A, \Gamma_B)$ varies with the choice of bases Γ_A and Γ_B for A_S and B_S. Let $\mathbf{GL}_t(R)$ denote the group of invertible $t \times t$ matrices with entries in R. Any two bases Γ_A and $\Gamma_A^{'}$ for A_S differ by multiplication by an element of $\mathbf{GL}_t(R)$, and similarly for bases Γ_B and $\Gamma_B^{'}$ of B_S. Thus, we can write:

$$\Gamma_A^{'} = M\Gamma_A, \qquad \Gamma_B^{'} = \Gamma_B N,$$

for appropriate matrices M and N in $\mathbf{GL}_t(R)$. Hence, we have:

$$\Theta(\Gamma_A^{'}, \Gamma_B^{'}) = M\Theta(\Gamma_A, \Gamma_B)N^*,$$

where N^* denotes the matrix obtained by applying the involution $*$ to the entries of N. Since the determinants of M and N are units in R, it follows that $\Lambda(\Gamma_A, \Gamma_B)$ is well-defined, up to multiplication by an element of R^*.

Now, we study what happens when one enlarges the set S. Let $T = S \cup \{w\}$, where w is an admissible prime. Clearly, T is an admissible set. By definition, $E(K_w)/p^m E(K_w)$ is isomorphic to $(\mathbf{Z}/p^m\mathbf{Z})^2$. Hence $r(A_T) = r(A_S) + 2$, and $r(B_T) = r(B_S) + 2$. Let $\Gamma_A = \{a_1, \ldots, a_t\}$ and $\Gamma_B = \{b_1, \ldots, b_t\}$ be bases for A_S and B_S respectively. Let a_{t+1}, a_{t+2} be an R-basis for $E(L_w)/p^m E(L_w)$, viewed as a subspace of A_T in the obvious way. Then $(a_1, \ldots, a_{t+2})$ is an R-basis for A_T. Choose any elements b_{t+1}, b_{t+2} in B_T such that $(b_1, \ldots, b_{t+2})$ form an R-basis for B_T. Let $\tilde{\Gamma}_A$ and $\tilde{\Gamma}_B$ be the bases for A_T and B_T thus obtained. Setting $\theta_{ij} = \langle a_i, b_j \rangle$, the matrix $\Theta(\tilde{\Gamma}_A, \tilde{\Gamma}_B)$ looks like this:

$$\Theta(\tilde{\Gamma}_A, \tilde{\Gamma}_B) = \left(\begin{array}{c|cc} \Theta(\Gamma_A, \Gamma_B) & \vdots & \vdots \\ \hline & & \\ 0 \ldots 0 & \theta_{t+1,t+1} & \theta_{t+1,t+2} \\ 0 \ldots 0 & \theta_{t+2,t+1} & \theta_{t+2,t+2} \end{array}\right).$$

Hence

$$\Lambda(\tilde{\Gamma}_A, \tilde{\Gamma}_B) = \Lambda(\Gamma_A, \Gamma_B) \det \begin{pmatrix} \theta_{t+1,t+1} & \theta_{t+1,t+2} \\ \theta_{t+2,t+1} & \theta_{t+2,t+2} \end{pmatrix}.$$

Now, the submodule of Ω_S generated by b_{t+1}, b_{t+2} surjects onto $H^1(L_w, E)_{p^m}$, since it generates $B_T/B_S \simeq R^2$ which injects into $H^1(L_w, E)_{p^m} \simeq R^2$. Hence the last determinant in the formula above is a unit, by the non- degeneracy of the local Tate pairing $[\ ,\ ]_{K,p^m}$ (prop. 2.2).

The group R^* acts on R, viewed as a monoid under multiplication. Let R/R^* denote the quotient monoid.

Definition 3.10 *The image* Λ *of* $\Lambda(\Gamma_A, \Gamma_B)$ *in* R/R^* *is called the* weak generalized regulator *associated to* $(E, L/K, p^m)$.

The order of vanishing of an element λ in R is defined to be the least ρ such that λ belongs to I^ρ, but not to $I^{\rho+1}$. The order of vanishing is well-defined on R/R^*. Hence the element Λ has a well-defined order of vanishing. More generally, the ideal in R generated by Λ is canonical, and is related to the Fitting ideal of the Selmer group $\mathrm{Sel}_{p^m}(E/L)$ viewed as an R-module.

3.3 The regulator in R/R_1^*

For the purpose of this section, we will suppose that the Shafarevich-Tate group $\underline{III}(E/K)$ is finite, satisfying

$$\#\underline{III}(E/K) = u \cdot p^s,$$

where u is not divisible by p. Let R_1^* be the subgroup of R^* defined by

$$\begin{aligned} R_1^* &= R^* \text{ if } s \geq m, \\ R_1^* &= \{\alpha \in R^*, \epsilon(\alpha) \equiv 1 \pmod{p^{m-s}}\} \text{ otherwise.} \end{aligned}$$

We will now show how, using the concept of a compatible basis for A_S and B_S, we can define a canonical element in R/R_1^* which refines the weak generalized regulator Λ.

The group $E(K)/p^m E(K)$ injects into both $A_S^G = \oplus_{v \in S} E(K_v)/p^m E(K_v)$ and $B_S^G = H_S^1(K, E_{p^m})$. Let $P_1, \ldots, P_r$ denote an *integral* basis for $E(K)$

modulo torsion. Write $\bar{a}_i$, resp $\bar{b}_i$, for the image of P_i in A_S^G, resp B_S^G. Complete these elements to bases $(\bar{a}_1, \ldots, \bar{a}_t)$, resp. $(\bar{b}_1, \ldots, \bar{b}_t)$ for A_S^G, resp. B_S^G. Let $(a_1^{'}, \ldots, a_t^{'})$, resp. $(b_1^{'}, \ldots, b_t^{'})$ be any basis for A_S, resp. B_S, as an R-module. Denote $\bar{a}_i^{'} = \mathrm{Cores}_{L/K}(a_i^{'})$, $\bar{b}_i^{'} = \mathrm{Cores}_{L/K}(b_i^{'})$. There exist matrices $\bar{M}$ and $\bar{N}$ in $\mathbf{GL}_t(\mathbf{Z}/p^m\mathbf{Z})$ transforming $(\bar{a}_1^{'}, \ldots, \bar{a}_t^{'})$, resp. $(\bar{b}_1^{'}, \ldots, \bar{b}_t^{'})$ into $(\bar{a}_1, \ldots, \bar{a}_t)$, resp. $(\bar{b}_1, \ldots, \bar{b}_t)$. Let M and N be any lifts of $\bar{M}$ and $\bar{N}$ to $\mathbf{GL}_t(R)$, satisfying $\epsilon(M) = \bar{M}$, and $\epsilon(N) = \bar{N}$. Then M, resp. N, transforms $(a_1^{'}, \ldots, a_t^{'})$, resp. $(b_1^{'}, \ldots, b_t^{'})$ into a basis $\Gamma_A = (a_1, \ldots, a_t)$, resp. $\Gamma_B = (b_1, \ldots, b_t)$ for A_S, resp B_S, such that $\mathrm{Cores}_{L/K}(a_i) = \bar{a}_i$ and $\mathrm{Cores}_{L/K}(b_i) = \bar{b}_i$.

Consider the $(t-r) \times (t-r)$-matrix with entries in R:

$$U = (\langle a_i, b_j \rangle)_{r+1 \leq i,j \leq t}.$$

Lemma 3.11 *$\epsilon(\det U) = \alpha \#\underline{Ш}(E/K)$, for some $\alpha \in (\mathbf{Z}/p^m\mathbf{Z})^*$.*

Proof: Let $\tilde{B}_S^G$ be the submodule of B_S^G generated by $\bar{b}_{r+1}, \ldots, \bar{b}_t$. Since the elements $\bar{b}_1, \ldots \bar{b}_r$ generate the image of $E(K)/p^m E(K)$ in B_S^G, and together the elements $\bar{b}_1, \ldots \bar{b}_t$ generate B_S^G, we find that the natural surjective map $B_S^G \longrightarrow H_S^1(K, E)_{p^m}$ induces an isomorphism

$$\tilde{B}_S^G \longrightarrow H_S^1(K, E)_{p^m}.$$

On the other hand there is an exact sequence

$$0 \longrightarrow \underline{Ш}(E/K)_{p^m} \longrightarrow H_S^1(K, E)_{p^m} \longrightarrow \oplus_{v \in S} H^1(K_v, E)_{p^m}.$$

Let $\tilde{H}$ denote the image of $H_S^1(K, E)_{p^m}$ in $\oplus_{v \in S} H^1(K_v, E)_{p^m}$. We may write

$$\underline{Ш}_{p^m}(E/K) \simeq (Z/p^{s_1}\mathbf{Z}) \times \cdots \times (\mathbf{Z}/p^{s_k}\mathbf{Z}),$$

and

$$\tilde{H} \simeq p^{s_1}(\mathbf{Z}/p^m\mathbf{Z}) \times \cdots \times p^{s_k}(\mathbf{Z}/p^m\mathbf{Z}) \times (\mathbf{Z}/p^m\mathbf{Z})^{t-r-k},$$

with some of the s_i possibly equal to m. We may thus suppose that $\bar{a}_{r+1}, \ldots \bar{a}_t$ and $\bar{b}_{r+1}, \ldots, \bar{b}_t$ have been chosen such that $\langle \bar{a}_i, \bar{b}_j \rangle_{K,p^m} = \delta_{ij} p^{s_i}$. The result follows from part 3 of prop. 2.10.

Definition 3.12 *If the bases Γ_A and Γ_B chosen above satisfy*

$$\epsilon(\det U) = \#\underline{Ш}(E/K) \quad \textit{in } \mathbf{Z}/p^m\mathbf{Z},$$

then the bases Γ_A and Γ_B are said to be compatible.

Theorem 3.13 *The element $\Lambda(\Gamma_A, \Gamma_B)$, where Γ_A and Γ_B are compatible bases for A_S and B_S, is well-defined up to multiplication by an element in R_1^*.*

Proof: Let (Γ_A, Γ_B) and $(\Gamma_A^{'}, \Gamma_B^{'})$ denote two sets of compatible bases for A_S and B_S. Write

$$\Gamma_A^{'} = (a_1^{'}, \ldots, a_t^{'}), \quad \Gamma_B^{'} = (b_1^{'}, \ldots, b_t^{'}),$$

and

$$\mathrm{Cores}_{L/K} a_i^{'} = \bar{a}_i^{'}, \mathrm{Cores}_{L/K} b_i^{'} = \bar{b}_i^{'}.$$

We already noted that there exist matrices M and N in $\mathbf{GL}_t(R)$ such that $\Gamma_A = M\Gamma_A^{'}$ and $\Gamma_B = \Gamma_B^{'} N$. From the definition of compatible bases, one sees that M and N must satisfy:

$$\epsilon(M) = \begin{pmatrix} X & 0 \\ \cdots & V \end{pmatrix}, \quad \epsilon(N) = \begin{pmatrix} X^t & \cdots \\ 0 & W \end{pmatrix},$$

where X is a matrix in $\mathbf{GL}_r(\mathbf{Z}/p^m\mathbf{Z})$ and X^t is the transposed matrix. Because X transforms $\{\bar{a}_1, \ldots, \bar{a}_r\}$ into $\{\bar{a}_1^{'}, \ldots, \bar{a}_r^{'}\}$, and because these are images of an integral basis for $E(K)$, it follows that X is the reduction (mod p^m) of a matrix in $\mathbf{GL}_r(\mathbf{Z})$. Hence

$$\det X = \pm 1.$$

Moreover, if U is the matrix defined before, and $U^{'}$ is the corresponding matrix for $(\Gamma_A^{'}, \Gamma_B^{'})$, then $V\epsilon(U^{'})W = \epsilon(U)$, and hence

$$\det V \det W \equiv 1 \pmod{p^{m-s}}.$$

But now we have $\Theta(\Gamma_A, \Gamma_B) = M\Theta(\Gamma_A^{'}, \Gamma_B^{'})N^*$, hence

$$\Lambda(\Gamma_A, \Gamma_B) = \det M \det N^* \Lambda(\Gamma_A^{'}, \Gamma_B^{'}).$$

This completes the proof, since

$$\epsilon(\det M \det N) = (\det X)^2 \det V \det W \equiv 1 \pmod{p^{m-s}}.$$

Finally, following the proof of prop. 3.9, one shows that enlarging the admissible set S only changes the regulator by an element of R_1^*.

Definition 3.14 *The image Λ of $\Lambda(\Gamma_A, \Gamma_B)$ in R/R_1^*, where (Γ_A, Γ_B) are compatible bases for A_S and B_S, is called the* generalized Mazur-Tate regulator *associated to $(E, L/K, p^m)$.*

3.4 Remarks on the generalized regulator

3.4.1 Relationship with the Mazur-Tate regulator

Let P, Q be points in $E(K)$, and let $\bar{a}$ and $\bar{b}$ be the images of P and Q in A_S^G and B_S^G respectively. Choose $a \in A_S$ and $b \in B_S$ such that $\mathrm{Cores}_{L/K}(a) = \bar{a}$ and $\mathrm{Cores}_{L/K}(b) = \bar{b}$. The element $\langle a, b\rangle \in R$ belongs to I, since

$$\epsilon(\langle a, b\rangle) = \langle \bar{a}, \bar{b}\rangle_{K,p^m} = 0,$$

by applying either prop. 2.2 or 2.5.

Proposition 3.15 *The image of $\langle a, b\rangle$ in I/I^2 depends only on P and Q.*

Proof: Let $a' \in A_S$ and $b' \in B_S$ be such that $\mathrm{Cores}_{L/K}(a') = \bar{a}$, and $\mathrm{Cores}_{L/K}(b') = \bar{b}$. We can write

$$a - a' = \sum_{i=1}^{k} \gamma_i a_i, \text{ where } \gamma_i \in I \text{ and } a_i \in A_S,$$

since $\hat{H}^{-1}(G, A_S) = 0$. Hence,

$$\langle a - a', b\rangle = \sum_{i=1}^{k} \gamma_i \langle a_i, b\rangle.$$

But

$$\epsilon(\langle a_i, b\rangle) = \langle \mathrm{Cores}_{L/K} a_i, \bar{b}\rangle_{K,p^m} = 0,$$

by prop. 2.2. Hence $\langle a_i, b\rangle \in I$, so that $\langle a, b\rangle - \langle a', b\rangle$ belongs to I^2.

Similarly, we may write $b - b' = \sum_{i=1}^{h} \lambda_i b_i$, where the λ_i belong to I and the b_i belong to B_S, since $\hat{H}^{-1}(G, B_S) = 0$. Hence,

$$\langle a, b - b'\rangle = \sum_{i=1}^{h} \lambda_i \langle a, b_i\rangle.$$

But

$$\epsilon(\langle a, b_i\rangle) = \langle \bar{a}, \mathrm{Cores}_{L/K}(b_i)\rangle_{K,p^m} = 0,$$

by prop. 2.5. Hence $\langle a, b_i\rangle \in I$, so that $\langle a, b\rangle - \langle a, b'\rangle$ belongs to I^2.

Prop. 3.15 allows us to define a canonical pairing

$$\langle\ ,\ \rangle_1 : E(K) \times E(K) \longrightarrow I/I^2 = G.$$

In [MT1] and [MT2], Mazur and Tate define a pairing

$$\langle\ ,\ \rangle_{MT} : E(K) \times E(K) \longrightarrow I/I^2.$$

The work of K-S. Tan [T2] can be used to show that the two pairings are equal. (See the more detailed discussion in [BD].) Let Λ_{MT} denote the Mazur-Tate regulator, defined to be the determinant of the $r \times r$ matrix $(\langle P_i, P_j \rangle_{MT})$ with entries in I/I^2, where $P_1, \ldots P_r$ is an integral basis for $E(K)$ modulo torsion. It is a canonical element in I^r/I^{r+1}.

Proposition 3.16 *The generalized Mazur-Tate regulator Λ belongs to I^r, and*

$$\Lambda \equiv \#\underline{Ш}(E/K)\Lambda_{MT} \pmod{I^{r+1}}.$$

We point out that our generalized regulator should really be called a leading coefficient - it incorporates both the order of the Shafarevich-Tate group, and the regulator term of the refined Birch-Swinnerton Dyer formulas. It seems unnatural in the context of our refinement to attempt to separate these two terms.

3.4.2 Behavior under norms

Let $K \subset L_1 \subset L_2$ be a tower of abelian extensions of K satisfying the hypotheses of section 2.3. Let $G_1 = \mathrm{Gal}(L_1/K)$ and $G_2 = \mathrm{Gal}(L_2/K)$. Let $\nu : G_2 \longrightarrow G_1$ be the natural homomorphism, and let it be extended to a homomorphism of the group rings R_1 and R_2 of G_1 and G_2. Since ν maps $(R_2)_1^*$ to $(R_1)_1^*$, it gives rise to a well defined map

$$R_2/(R_2)_1^* \longrightarrow R_1/(R_1)_1^*.$$

Let Λ_1 and Λ_2 denote the corresponding generalized regulators. We have the following compatibility formula for these:

$$\nu(\Lambda_2) = \Lambda_1,$$

which follows immediately from the corresponding compatibility for the R-valued pairing $\langle\ ,\ \rangle$ (prop. 2.10).

3.5 Generalized regulators for cyclic groups: derived heights

In this section we concentrate on the case where $G = \mathbf{Z}/p\mathbf{Z}$ is cyclic, with a generator σ. In this case we give an alternate approach to the generalized Mazur-Tate regulator, involving the notion of a *derived height*. This approach has several advantages:

1. The approach via derived heights gives a particularly satisfying and elegant construction of the generalized regulator when $G = \mathbf{Z}/p\mathbf{Z}$.

2. We will prove that the derived heights "of odd order" are symmetric, and that those "of even order" are alternating. This will enable us to predict that ρ (the order of vanishing of the regulator) has the same parity as r_p, the p-rank of $\mathrm{Sel}_p(E/K)$.

3. We will use our explicit understanding of the situation for cyclic groups of prime order to prove theorem 4.8. It asserts that our conjecture 4.4 which refines a Birch Swinnerton-Dyer type conjecture of Mazur and Tate and predicts the precise order of vanishing of their θ-element in many cases, is implied by the classical Birch and Swinnerton-Dyer conjecture over number fields.

Let us choose a set S of primes which is admissible for $(E, L/K, p)$ and let A, B and Ω denote the modules A_S, B_S, and Ω_S of the previous section. Since $m = 1$, these modules are $\mathbf{F}_p$ vector spaces, equipped with G-action - i.e., they are modules over the group ring $R = \mathbf{F}_p[G]$. This group ring is a local ring, isomorphic to $\mathbf{F}_p[\epsilon]/(\epsilon^p)$, where $\epsilon = \sigma - 1$ and σ is an arbitrarily chosen generator of G.

We define a decreasing filtration on $\mathrm{Sel}_p(E/K)$,

$$\mathrm{Sel}_p(E/K) = \mathrm{Sel}^{(1)} \supset \mathrm{Sel}^{(2)} \supset \ldots \supset \mathrm{Sel}^{(p)}$$

by

$$\mathrm{Sel}^{(k)} = \{s \in \mathrm{Sel}_p(E/K) \text{ such that } \exists \tilde{s} \in \mathrm{Sel}_p(E/L) \text{ with } (\sigma - 1)^{k-1}\tilde{s} = s\},$$

for $2 \leq k \leq p$.

Because the norm element $1 + \sigma + \cdots + \sigma^{p-1}$ in the group ring $\mathbf{F}_p[G]$ is equal to $(\sigma - 1)^{p-1}$, we have

Lemma 3.17 *The space* $\mathrm{Sel}^{(p)}$ *is the subspace of elements in* $\mathrm{Sel}_p(E/K)$ *which are norms from* $\mathrm{Sel}_p(E/L)$. *Hence the filtration above terminates in the trivial space, if and only if the space of global norms from* L *in* $\mathrm{Sel}_p(E/K)$ *is trivial.*

Our approach to the generalized regulator in this section is to define a sequence of "derived" height pairings on the $\mathbf{F}_p$-vector space $\mathrm{Sel}^{(k)}$. Each of these pairings is defined canonically on the null-space of the previous one.

More precisely, the main theorem of this section is the following:

Theorem 3.18 *There exists a sequence of canonical pairings*

$$\begin{array}{lll}
\langle\ ,\ \rangle_1 : & \mathrm{Sel}^{(1)} \times \mathrm{Sel}^{(1)} & \longrightarrow\ I/I^2, \\
\langle\ ,\ \rangle_2 : & \mathrm{Sel}^{(2)} \times \mathrm{Sel}^{(2)} & \longrightarrow\ I^2/I^3, \\
\langle\ ,\ \rangle_3 : & \mathrm{Sel}^{(3)} \times \mathrm{Sel}^{(3)} & \longrightarrow\ I^3/I^4, \\
\vdots & \vdots & \vdots\quad\ \vdots \\
\langle\ ,\ \rangle_{p-1} : & \mathrm{Sel}^{(p-1)} \times \mathrm{Sel}^{(p-1)} & \longrightarrow\ I^{p-1}/I^p,
\end{array}$$

such that

1. *For* $s_1, s_2 \in \mathrm{Sel}^{(k)}$, *we have*

$$\langle s_1, s_2\rangle_k = (-1)^{k+1}\langle s_2, s_1\rangle_k.$$

2. *For* $1 \le k \le p-1$, *the space* $\mathrm{Sel}^{(k+1)}$ *is precisely the null-space of* $\langle\ ,\ \rangle_k$.

Proof:
Definition of $\langle\ ,\ \rangle_k$: Let s_1 ands_2 be elements of $\mathrm{Sel}^{(k)}$. Let $\tilde{s}_1$ and $\tilde{s}_2$ be classes in $\mathrm{Sel}_p(E/L)$ such that

$$(\sigma - 1)^{k-1}\tilde{s}_i = s_i, \quad i = 1, 2,$$

and let $a_1 \in A$ and $b_2 \in B$ be classes such that

$$(\sigma - 1)^{p-k}a_1 = \tilde{s}_1, \quad (\sigma - 1)^{p-k}b_2 = \tilde{s}_2.$$

Since $(\sigma - 1)^{p-1} = 1 + \sigma + \cdots + \sigma^{p-1} \pmod p$, we have

$$\mathrm{Cores}_{L/K}a_1 = s_1, \quad \mathrm{Cores}_{L/K}b_2 = s_2.$$

Now consider the element $\langle a_1, b_2\rangle \in R$. This element belongs to I^k. In fact,

$$\langle a_1, \beta\rangle \in I^k, \quad \forall \beta \in B,$$

$$\langle \alpha, b_2\rangle \in I^k, \quad \forall \alpha \in A,$$

since

$$(\sigma - 1)^{p-k}\langle a_1, \beta\rangle = \langle \tilde{s}_1, \beta\rangle = 0,$$

by prop. 2.10, part 5, and

$$(\sigma^{-1} - 1)^{p-k}\langle \alpha, b_2\rangle = \langle \alpha, \tilde{s}_2\rangle = 0,$$

by prop. 2.10, part 4.

Moreover, the image of $\langle a_1, b_2\rangle$ in I^k/I^{k+1} depends only on s_1 and s_2 and not on the choices of $\tilde{s}_1, \tilde{s}_2, a_1$, and b_2. For let $a_1^{'}$ be another element of A satisfying

$$\mathrm{Cores}_{L/K} a_1^{'} = s_1.$$

Then since A is free, there exists $\alpha \in A$ with $a_1 - a_1^{'} = (\sigma - 1)\alpha$. Hence

$$\langle a_1, b_2\rangle - \langle a_1^{'}, b_2\rangle = (\sigma - 1)\langle \alpha, b_2\rangle \in I^{k+1}.$$

The proof that $\langle a_1, b_2\rangle \pmod{I^{k+1}}$ does not depend on the choice of b_2 is similar. Define

$$\langle s_1, s_2\rangle_k := \langle a_1, b_2\rangle \pmod{I^{k+1}}.$$

Proof of part 1: Let $a_1, a_2 \in A$, $b_1, b_2 \in B$ satisfy

$$(\sigma - 1)^{p-k} a_i = \tilde{s}_i, \quad (\sigma - 1)^{p-k} b_i = \tilde{s}_i.$$

Since Ω is a free R-module, we have $a_i - b_i = (\sigma - 1)^k \omega_i$ for some $\omega_i \in \Omega$. One then has

$$\langle a_1 - b_1, a_2 - b_2\rangle = (\sigma - 1)^k (\sigma^{-1} - 1)^k \langle \omega_1, \omega_2\rangle \in I^{k+1}.$$

Hence by prop. 2.10,

$$\langle a_1, b_2\rangle + \langle a_2, b_1\rangle^* = 0 \pmod{I^{k+1}}.$$

Since the involution $*$ acts by $(-1)^k$ on I^k/I^{k+1}, it follows that

$$\langle s_1, s_2\rangle_k = (-1)^{k+1}\langle s_2, s_1\rangle,$$

as was to be shown.

Proof of part 2: For $0 \leq k \leq p$, let

$$B^{(k)} := \{b \in B \text{ such that } (\sigma - 1)^{p-k} b \in \mathrm{Sel}_p(E/L)\}.$$

There is a natural map $h : B^{(k)} \longrightarrow \mathrm{Hom}(\mathrm{Sel}^{(1)}/\mathrm{Sel}^{(k+1)}, I^k/I^{k+1})$ defined by the rule

$$h(b)(s) := \langle a, b\rangle \pmod{I^{k+1}},$$

where $a \in A$ is any class such that $\mathrm{Cores}_{L/K}(a) = s$.

Statement 2 follows from the following more precise formulation:

Lemma 3.19 *For $1 \leq k \leq p-1$,*

1. *the space $\mathrm{Sel}^{(k+1)}$ is precisely the null-space of $\langle\ ,\ \rangle_k$;*
2. *the natural map $h : B^{(k)} \longrightarrow \mathrm{Hom}(\mathrm{Sel}^{(1)}/\mathrm{Sel}^{(k+1)}, I^k/I^{k+1})$ is surjective.*

Proof: By induction on k. Let $N^{(k)} \subset \mathrm{Sel}^{(k)}$ be the nullspace of the pairing $\langle\ ,\ \rangle_k$. The inclusion

$$\mathrm{Sel}^{(k+1)} \subset N^{(k)}$$

follows immediately from the definitions. Suppose that $s \in \mathrm{Sel}^{(k)}$ is an element of $N^{(k)}$. Choose $b \in B$ such that

$$\mathrm{Cores}_{L/K} b = s, \qquad (\sigma - 1)^{p-k} b = \tilde{s}, \text{ with } \tilde{s} \in \mathrm{Sel}_p(E/L).$$

As observed earlier, the element b gives rise, via h, to an element

$$f \in \mathrm{Hom}(\mathrm{Sel}^{(1)}/\mathrm{Sel}^{(k+1)}, I^k/I^{k+1})$$

which is trivial on $\mathrm{Sel}^{(k)}$. When $k = 1$, the homomorphism f is thus trivial on all of $\mathrm{Sel}^{(1)}$. For $k \geq 1$, apply part 2 of the induction hypothesis for $k-1$, to obtain an element $b_0 \in B^{(k-1)}$ such that:

$$\langle a, b - (\sigma - 1)b_0\rangle \in I^{k+1}, \text{ for all } a \in A \text{ with } \mathrm{Cores}_{L/K}(a) \in \mathrm{Sel}^{(1)}.$$

Let $b' = b - (\sigma - 1)b_0$, and consider the class $\beta = (\sigma - 1)^{p-k-1} b' \in B$. Since $(\sigma - 1)^{p-k} b'$ belongs to $\mathrm{Sel}_p(E/L)$, it follows that the image $\bar{\beta}$ of β in

$H^1_S(\mathbf{A}_L, E)_p$ is fixed under the action of G, hence, it belongs to the subspace $H^1_S(\mathbf{A}_K, E)_p$, by lemma 2.18. On the other hand,

$$0 = (\sigma - 1)^{p-k-1}\langle a, b^{'}\rangle = [\mathrm{Cores}_{L/K}(a), \bar{\beta}]_{K,p}.$$

Since $\mathrm{Cores}_{L/K}(a)$ ranges over all the elements of $\mathrm{Sel}^{(1)}$, we can apply cor. 2.7 to conclude that there exists a class $\beta_0 \in H^1(K, E_p)$ with $\tilde{s}^{'} = \beta - \beta_0$ belonging to $\mathrm{Sel}_p(E/L)$. But

$$(\sigma - 1)^k \tilde{s}^{'} = s,$$

and hence, it follows that s belongs to $\mathrm{Sel}^{(k+1)}$, as was to be shown.

Part 2 of the lemma follows immediately upon noting that the natural map $IB^{(k-1)} \longrightarrow \mathrm{Hom}(\mathrm{Sel}^{(1)}/\mathrm{Sel}^{(k)}, I^k/I^{k+1})$ is surjective by the induction hypothesis, and that the map $B^{(k)} \longrightarrow \mathrm{Hom}(\mathrm{Sel}^{(k)}/\mathrm{Sel}^{(k+1)}, I^k/I^{k+1})$ is surjective, by part 1 of the lemma.

This completes step 2, and the proof of thm. 3.18.

Let

$$\rho_p = \dim_{\mathbf{F}_p} \mathrm{Sel}^{(1)} + \cdots + \dim_{\mathbf{F}_p} \mathrm{Sel}^{(p)} = \rho_p^{(1)} + \cdots + \rho_p^{(p)}.$$

We have the following interpretation of ρ_p which will be useful later on:

Proposition 3.20 $\rho_p = \dim_{\mathbf{F}_p} \mathrm{Sel}_p(E/L)$.

We now outline a procedure for expressing the generalized regulator associated to $(E, L/K)$ in terms of partial regulators formed from the derived heights. Choose a basis $s_1, \ldots, s_r$ of $\mathrm{Sel}^{(1)}$ which is compatible with the decreasing filtration on $\mathrm{Sel}_p(E/K)$ (i.e., each quotient $\mathrm{Sel}^{(k)}/\mathrm{Sel}^{(k+1)}$ is generated by a subset of the s_i). In addition, when $\underline{III}_p(E/K) = 0$, so that $E(K)/pE(K) = \mathrm{Sel}_p(E/K)$, assume that the basis $s_1, \ldots, s_r$ is the image of an integral basis of $E(K)$ modulo torsion. For each quotient $\mathrm{Sel}^{(k)}/\mathrm{Sel}^{(k+1)}$, let $d_k = \rho_p^{(k)} - \rho_p^{(k+1)}$ be its dimension over $\mathbf{F}_p$, and let $s^{(1)}, \ldots s^{(d_k)}$ be a basis for this quotient, taken from among the images of the basis vectors s_i. For $1 \leq k \leq p-1$, let $\Theta^{(k)}$ denote the partial regulator matrix:

$$\Theta^{(k)} = (\langle s^{(i)}, s^{(j)}\rangle_k)_{1 \leq i,j \leq d_k},$$

and let

$$\Lambda^{(k)} = \det(\Theta^{(k)}).$$

This is the determinant of a square matrix of dimension $d_k = \rho_p^{(k)} - \rho_p^{(k+1)}$, with entries in I^k/I^{k+1}, and hence

$$\Lambda^{(k)} \in I^{kd_k}/I^{kd_k+1}.$$

It is non-zero when $kd_k < p$, since $\mathrm{Sel}^{(k+1)}$ is precisely the nullspace of $\langle\ ,\ \rangle_k$. Set $\Lambda_{\mathrm{der}} = 0$ when $\mathrm{Sel}^{(p)}$ is non-trivial, and otherwise put

$$\Lambda_{\mathrm{der}} = \Lambda^{(1)}\Lambda^{(2)}\cdots\Lambda^{(p-1)}.$$

By a straightforward computation, one sees that Λ_{der} belongs to I^{ρ_p}, and is non-zero in I^{ρ_p}/I^{ρ_p+1} if and only if $\rho_p < p$. The following theorem relates the generalized regulator to the partial regulators coming from the derived height pairings.

Theorem 3.21 *Let $\underline{Ш}_{(p)}$ denote the quotient of $\underline{Ш}_p(E/K)$ by its Sylow p-subgroup, and let Λ denote the generalized Mazur-Tate regulator associated to $(E, L/K)$. Then*

$$\Lambda = \#\underline{Ш}_{(p)}\Lambda_{\mathrm{der}} \pmod{R_1^*}.$$

Proof: Choose compatible bases $\Gamma_A = (a_1, \ldots, a_t)$ and $\Gamma_B = (b_1, \ldots, b_t)$ for A and B respectively, and write $\bar{a}_i = \mathrm{Cores}_{L/K}a_i$, $\bar{b}_i = \mathrm{Cores}_{L/K}b_i$. The elements $(\bar{a}_1, \ldots, \bar{a}_t)$ and $(\bar{b}_1, \ldots \bar{b}_t)$ are $\mathbf{F}_p$ bases for A^G and B^G respectively. Suppose that the a_i and b_i have been chosen to be compatible with the following filtrations on A and B:

$$\mathrm{Sel}^{(p)} \subset \mathrm{Sel}^{(p-1)} \subset \cdots \subset \mathrm{Sel}^{(1)} \subset A^G,$$

$$\mathrm{Sel}^{(p)} \subset \mathrm{Sel}^{(p-1)} \subset \cdots \subset \mathrm{Sel}^{(1)} \subset B^G,$$

and that in addition whenever $\bar{a}_i$ or $\bar{b}_i$ belongs to $\mathrm{Sel}^{(k)}$, then $(\sigma-1)^{p-k}a_i$ and $(\sigma-1)^{p-k}b_i$ belong to $\mathrm{Sel}_p(E/L)$. With such a choice, the matrix $\Theta(\Gamma_A, \Gamma_B)$ looks like this:

$$\Theta(\Gamma_A, \Gamma_B) = \begin{pmatrix} \Theta_{pp} & \cdots & \Theta_{p1} & \Theta_{p0} \\ \vdots & & \vdots & \vdots \\ \Theta_{1p} & \cdots & \Theta_{11} & \Theta_{10} \\ \Theta_{0p} & \cdots & \Theta_{01} & \Theta_{00} \end{pmatrix},$$

where:
1. The Θ_{ij}'s are $d_i \times d_j$ matrices with entries in $I^{\max(i,j)}$.
2. When $1 \leq k \leq p-1$, we have $\Theta_{kk} \equiv \Theta^{(k)} \pmod{I^{k+1}}$.

Hence one has $\Lambda(\Gamma_A, \Gamma_B) = 0$ if $\mathrm{Sel}^{(p)} \neq 0$. Otherwise, by a straigtforward manipulation of determinants,

$$\begin{aligned} \Lambda(\Gamma_A, \Gamma_B) &= \det \Theta_{p-1,p-1} \cdots \det \Theta_{11} \cdot \det \Theta_{00} \\ &= \Lambda^{(p-1)} \cdots \Lambda^{(1)} \cdot \#\underline{Ш}_{(p)} = \Lambda_{\mathrm{der}} \cdot \#\underline{Ш}_{(p)} \pmod{R_1^*}, \end{aligned}$$

and this concludes the proof.

Remarks:
1. From the discussion in sec. 3.4.1, one sees in particular that the first derived pairing $\langle\ ,\ \rangle_1$ is the usual Mazur-Tate pairing, extended to the p-Selmer group.

2. When $\underline{Ш}_p(E/K)$ is non-trivial, we have $R_1^* = R^*$, and thm. 3.21 simply states that Λ and Λ_{der} have the same order of vanishing.

Proposition 3.22 *The order of vanishing of Λ, when it is $< \infty$, has the same parity as the p-rank of $\mathrm{Sel}_p(E/K)$.*

Proof: We can write

$$\dim_{\mathbf{F}_p} \mathrm{Sel}_p(E/K) = d_1 + \cdots + d_{p-1} + d_p,$$

where

$$d_k = \rho_p^{(k)} - \rho_p^{(k+1)} = \dim_{\mathbf{F}_p}(\mathrm{Sel}^{(k)}/\mathrm{Sel}^{(k+1)}), \quad 1 \leq k \leq p-1,$$

and $d_p = \dim_{\mathbf{F}_p} \mathrm{Sel}^{(p)}$. When k is even, the pairing $\langle\ ,\ \rangle_k$ defines a non-degenerate, alternating pairing on $\mathrm{Sel}^{(k)}/\mathrm{Sel}^{(k+1)}$; hence, d_k is even, and

$$\dim_{\mathbf{F}_p} \mathrm{Sel}_p(E/K) \equiv d_1 + d_3 + \cdots + d_p \pmod 2.$$

On the other hand, the order of vanishing of Λ is

$$d_1 + 2d_2 + 3d_3 + \cdots + pd_p \equiv d_1 + d_3 + \cdots + d_p \pmod 2,$$

and the result follows.

4 The Mazur-Tate conjectures

In this section we refine the conjecture of [MT2] using our generalized regulator. We start by formulating these conjectures in a general framework, and then concentrate on two special cases – the first special case is the one that was considered originally in [MT2]. The second case, that of an abelian extension of dihedral type of a quadratic field, partly motivated the present study, because it provides a setting where degeneracies in the Mazur-Tate height pairing are the rule rather than the exception.

4.1 The general case

For each character χ of $G = \mathrm{Gal}(L/K)$, we can consider the twisted L-function $L(E/K, \chi, s)$. It is defined by an Euler product which is absolutely convergent in the right-hand plane $\Re s > \frac{3}{2}$.

Under standard conjectures (eg., if E arises from an automorphic form on $\mathbf{GL}_2$) these L-functions can be analytically continued to the entire complex plane, and the special values $L(E/K, \chi, 1)$ can be considered.

Definition 4.1 *The Galois L-function attached to $(E, L/K)$ is a complex-valued measure μ on G such that*

$$\int_G \chi d\mu = L(E/K, \chi, 1)$$

for all characters χ of G.

The element μ can simply be thought of as an element in the complex group ring $\mathbf{C}[G]$:

$$\mu = \sum_{\chi \in \hat{G}} L(E/K, \chi, 1) e_\chi,$$

where $e_\chi = 1/\#G \sum_{\sigma \in G} \chi(\sigma)\sigma^{-1}$ is the idempotent in the group ring corresponding to χ.

For the purpose of the Mazur-Tate conjectures, such an element in the complex group ring is not enough: we desire an element belonging to an *integral* group ring, and having similar interpolation properties.

Let E_0 be the connected component in the Néron model for E over K, and let ω be a Néron differential. For every place v of K, define the local factor m_v by

$$m_v = \begin{cases} \#E/E_0(K_v) & \text{if } v \text{ is non-archimedean,} \\ \int_{E(\mathbf{R})} \omega & \text{if } v \text{ is real,} \\ \int_{E(\mathbf{C})} \omega \wedge \bar{\omega} & \text{if } v \text{ is complex.} \end{cases}$$

Let Z be the ring $\mathbf{Z}[\frac{1}{2\#E(L)_{\text{tor}}}]$. Given a character χ of $G = \text{Gal}(L/K)$, let c_χ be the Artin conductor associated to χ, and let $f_\chi = \text{norm}_{K/\mathbf{Q}} c_\chi$. Let $\tau(\chi)$ be the global Gauss sum attached to χ, as in [Fr], pp. 32-35.

Conjecture 4.2 (Rationality and integrality conjecture) *Suppose that L and K are totally real. There exists a Z-valued measure θ on G such that*

$$\int_G \chi d\theta = f_\chi \tau(\chi) L(E/K, \bar{\chi}, 1) \prod_{v \text{ real}} m_v^{-1},$$

for all characters $\chi : G \longrightarrow \mathbf{C}^*$.

The element θ belongs to the integral group ring $Z[G]$. This group ring is equipped with a decreasing filtration by powers of the augmentation ideal I:

$$Z[G] \supset I \supset I^2 \supset \cdots I^k \supset \cdots$$

The first quotient in this filtration is isomorphic to Z

$$Z[G]/I = Z,$$

but the quotients that appear after that are torsion. More precisely, the group $Z \otimes \text{Sym}^k(G)$ maps surjectively to I^k/I^{k+1}, with a small kernel. When the order of G is not invertible in Z, it becomes an interesting question to ask about the position of the element θ in this filtration. This issue is addressed by the vanishing conjecture of Mazur and Tate:

Conjecture 4.3 (Vanishing conjecture) *Let r be the rank of the Mordell-Weil group $E(K)$. The element θ belongs to I^r.*

Remark: This conjecture is written down in [MT2] only in the case $K = \mathbf{Q}$, where the conjectural element θ can be constructed explicitly using modular symbols (cf. sec. 4.2). Any inaccuracy in the conjecture for general K should be blamed only on the authors of this paper!

Assume that the extension L/K satisfies the assumptions of section 2.3, so that the generalized regulator Λ is defined. Let ρ be the order of vanishing of Λ. We make the following conjecture:

Conjecture 4.4 (Refined vanishing conjecture) *The element θ belongs to I^ρ.*

In fact, it should be possible to formulate a more precise conjecture relating the image of θ in $I^\rho/I^{\rho+1}$ to the generalized regulator Λ in $I^\rho/I^{\rho+1}$. We will content ourselves with such a precise statement only in certain special cases which we proceed to outline.

Suppose from now on that the elliptic curve E is *modular*, i.e., there is a non-constant rational map $X_0(N) \longrightarrow E$ defined over $\mathbf{Q}$. By the Shimura-Taniyama-Weil conjecture this is true for all E which are defined over $\mathbf{Q}$, and N is the arithmetic conductor of E.

Conj. 4.2 is then known in the following cases:

1. When $K = \mathbf{Q}$ and $L/\mathbf{Q}$ is a totally real extension of $\mathbf{Q}$, a construction of Birch and Manin (modular symbols) can be used to construct the element θ. See [MT2], for example.

2. When K is a real quadratic field such that all the primes dividing N are split in $K/\mathbf{Q}$, and when L is a ring class field of K, then the element θ can be constructed using homology cycles analogous to modular symbols. (For a construction of these cycles, see for example [Sh].) These "real-quadratic modular symbols" are also studied in the context of the refined conjectures in [D2].

3. When K is an *imaginary* quadratic field such that all the primes dividing N are split in $K/\mathbf{Q}$, and when L is a ring class field of K, an analogue of θ which interpolates special values of *derivatives* of L-series can be formulated, by replacing the modular symbols by Heegner points.

Although this element does not fit into the context of conj. 4.2, still one can formulate a refined conjecture for it, which is partly proved in [D1]. The refined conjecture stated there can only be formulated adequately with the notion of the generalized regulator, which was not available at that time. Thus the generalized regulator and the derived pairings are an important tool in understanding (at least conjecturally) the behaviour of Heegner points over ring class fields of a quadratic field K when the rank of $E(K)$ is > 1. We will formulate a conjecture relating the module of Heegner points in $E(L)$ to the derived height pairings when $G = \mathrm{Gal}(L/K)$ is cyclic of prime order.

4.2 Modular symbols

In this section, the ground field $K = \mathbf{Q}$. Let f be an integer prime to N, and assume for simplicity that f is square-free. Let $Q(\mu_f)^+$ denote the maximal real subfield of $\mathbf{Q}(\mu_f)$. Let G_f be the Galois group of this extension. A complex-valued character of $G_f = (\mathbf{Z}/f\mathbf{Z})^*/\langle \pm 1 \rangle$ can be viewed as an even Dirichlet character with conductor dividing f. Let $g_\chi = f/\mathrm{cond}(\chi)$. Let $L_f(E/\mathbf{Q}, \chi, 1)$ be the L-function of E over $\mathbf{Q}$ with the Euler factors above the primes dividing f removed.

Theorem 4.5 (Birch, Manin) *There exists an element $\theta_f \in \mathbf{Z}[G_f]$ such that*

$$\chi(\theta_f) = g_\chi \cdot \frac{\tau(\chi) L_f(E/\mathbf{Q}, \bar{\chi}, 1)}{2m_\infty},$$

where $\tau(\chi) = \sum_{a=1}^{f} \chi(a) \exp(2\pi i a/f)$ is the (slightly modified) Gauss sum associated to χ.

This element can be constructed using modular symbols – see for example [MT2]. The reader must be warned that the element $\theta_{A,f}$ defined on page 716 of [MT2] is not quite the same as our element θ_f - it satisfies the interpolation property above only for *primitive* characters χ. To make it hold for all characters, one needs to modify the definition of θ_f somewhat. This modification is explained in [D3], sec. 2.3.

Let $L/\mathbf{Q}$ be any subfield of $\mathbf{Q}(\mu_f)^+$ which is not contained in any $\mathbf{Q}(\mu_g)^+$ for g a proper divisor of f. Let $G = \mathrm{Gal}(L/\mathbf{Q})$, and let θ be the image of θ_f by the natural homomorphism from $Z[G_f] \longrightarrow Z[G]$.

Suppose that G is a p-group, and that $L/\mathbf{Q}$ satisfies the conditions of section 2.3 relative to p. The regulator Λ in the group ring $R = \mathbf{Z}/p^m\mathbf{Z}[G]$ is well-defined modulo R_1^*. Let $\underline{\theta}$ be the natural image of θ in R, and let

$$J_f = \prod_v m_v \prod_{v|f} \#E(\mathbf{F}_v),$$

where the product of the m_v is taken over all non-archimedean places of $\mathbf{Q}$.

Conjecture 4.6

$$\underline{\theta} = J_f \Lambda \pmod{R_1^*}.$$

Remarks:
1. We are assuming that p does not divide any of the m_v. Also, because of our assumptions on the surjectivity of the local norms, the $\#E(\mathbf{F}_v)$ for $v|f$ have order prime to p, by prop. 2.16. Hence the extra factor J_f appearing in the above formula is a unit at p. This conjecture gives us a clue about why the assumption on surjectivity of local norms is crucial: when it is not satisfied, one expects to have some extra vanishing caused by the presence of "bad" Euler factors. In order to study the extra vanishing caused by degeneracies in the Mazur-Tate height, it seemed judicious to isolate this phenomenon and avoid the situations where the terms $\#E(\mathbf{F}_v)$ might bring about still further extra vanishing.

2. Conj. 4.6 implies the conjecture of Mazur-Tate in [MT2]. This follows from the comparison between the generalized regulator and the Mazur-Tate regulator.

Evidence when $G = \mathbf{Z}/p\mathbf{Z}$. We now proceed to give a reformulation of our conjecture on θ in the special case when G is cyclic of prime order, using the derived height formalism of section 3.5. In this case we obtain a prediction for the precise order of vanishing of $\underline{\theta}$, and we show that in many cases this prediction follows from the conjecture of Birch and Swinnerton-Dyer.

Let I denote as before the augmentation ideal in the group ring $R = \mathbf{F}_p[G]$, and let Sel be the $\mathbf{F}_p$-vector space $\mathrm{Sel}_p(E/\mathbf{Q})$. The derived heights

$$\langle\ ,\ \rangle_k : \mathrm{Sel}^{(k)} \times \mathrm{Sel}^{(k)} \longrightarrow I^k/I^{k+1}, \quad 1 \leq k \leq p-1$$

define a decreasing filtration of the vector space Sel,

$$\mathrm{Sel}^{(1)} \supset \mathrm{Sel}^{(2)} \supset \cdots \supset \mathrm{Sel}^{(p)},$$

where $\mathrm{Sel}^{(k)}$ is the null-space of $\langle\ ,\ \rangle_{k-1}$. The last step in this filtration, $\mathrm{Sel}^{(p)}$, is trivial if and only if the sub-space of norms from $\mathrm{Sel}_p(E/L)$ is trivial.

As before, let

$$\rho_p = \dim_{\mathbf{F}_p} \mathrm{Sel}^{(1)} + \dim_{\mathbf{F}_p} \mathrm{Sel}^{(2)} + \cdots + \dim_{\mathbf{F}_p} \mathrm{Sel}^{(p)}.$$

Note that the first term in this sum is $r_p = \dim_{\mathbf{F}_p}(\mathrm{Sel}_p(E/\mathbf{Q})) \geq r$, where $r = \mathrm{rank}(E(\mathbf{Q}))$. Thus $\rho_p \geq r_p$, with equality occuring precisely when the canonical pairing $\langle\ ,\ \rangle_1$ is non-degenerate on $\mathrm{Sel}^{(1)}$.

The following conjecture predicts the exact order of vanishing of $\underline{\theta}$:

Conjecture 4.7 *The element $\underline{\theta}$ vanishes to order* exactly *ρ_p. More precisely,*

1. *If $\rho_p \geq p$, then $\underline{\theta} = 0$,*
2. *If $\rho_p < p$ then $\underline{\theta}$ belongs to $I^{\rho_p} - I^{\rho_p+1}$.*

We propose the following evidence for this conjecture:

Theorem 4.8 *Suppose that $\underline{Ш}_p(E/\mathbf{Q})$ is trivial. Then conjecture 4.7 follows from the classical Birch and Swinnerton-Dyer conjecture over L and $\mathbf{Q}$.*

Proof: The rest of this section will be devoted to the proof of theorem 4.8. To begin with, we observe that when the rank r of $E(\mathbf{Q})$ is 0 (and hence, $r_p = \dim_{\mathbf{F}_p}(\mathrm{Sel}_p(E/\mathbf{Q})) = 0$) then the refined conjecture of Mazur and Tate follows immediately from the usual conjecture of Birch and Swinnerton-Dyer (see, for example, the discussion in [MT2], p. 744). Hence, we will assume that $r > 0$ in what follows.

Before tackling the proof, we will need a few lemmas:

Lemma 4.9 *Let Ω be a finitely generated torsion $\mathbf{Z}_p$-module equipped with a G-action, and let Ω_p denote the p-torsion submodule of Ω. If Ω is killed by the norm element in the group ring, and $\dim_{\mathbf{F}_p} \Omega_p < p-1$, then $\Omega = \Omega_p$, i.e., Ω is in fact an $\mathbf{F}_p$-vector space.*

Proof: Choose a generator σ of G and and let Ω^i denote the set of all elements $\omega \in \Omega$ such that $(\sigma - 1)^i \omega = 0$. The endomorphism $(\sigma - 1)$ in $\mathbf{Z}_p[G]$ is topologically nilpotent, and hence the increasing filtration

$$\Omega^1 \subset \Omega^2 \subset \cdots \subset \Omega^k \subset \cdots$$

satisfies $\cup \Omega^k = \Omega$. Moreover, if $\Omega^i = \Omega^{i+1}$, then $\Omega^k = \Omega^i$ for all $k > i$, clearly. Now we observe that Ω^{p-1} is in fact an $\mathbf{F}_p$ vector space. For, it is killed by the norm element N_G, and by $(\sigma - 1)^{p-1}$. But it is not hard to show that

$$N_G - (\sigma - 1)^{p-1} = u \cdot p,$$

where u is a unit in the group ring $\mathbf{Z}_p[G]$. Hence, every element of Ω^{p-1} is killed by p. Since Ω^{p-1} injects into Ω_p, it follows that

$$\dim_{\mathbf{F}_p}(\Omega^{p-1}) < p - 1,$$

and hence $\Omega^{p-1} = \Omega^{p-2}$. Therefore, $\Omega^{p-1} = \Omega$, and Ω is killed by p as was to be shown.

We will apply lemma 4.9 above to the case where $\Omega = \underline{Ш}(E/L) \otimes \mathbf{Z}_p$.

Corollary 4.10 *If $\underline{Ш}_p(E/\mathbf{Q}) = 1$, and if $\rho_p < p$, then $\underline{Ш}(E/L) \otimes \mathbf{Z}_p$ is an $\mathbf{F}_p$ vector space. In particular, $\underline{Ш}(E/L) \otimes \mathbf{Z}_p$ is finite, and $\#\underline{Ш}(E/L) \otimes \mathbf{Z}_p = \#\underline{Ш}_p(E/L)$.*

Proof: By prop. 3.20, we have

$$\dim_{\mathbf{F}_p} \mathrm{Sel}_p(E/L) < p.$$

We may assume without loss of generality that $\dim_{\mathbf{F}_p} E(\mathbf{Q})/pE(\mathbf{Q}) \geq 1$, and hence

$$\dim_{\mathbf{F}_p} \underline{Ш}_p(E/L) < p - 1.$$

Furthermore, the norm maps $\underline{Ш}(E/L)$ to $\underline{Ш}(E/K)$, and hence our assumption that $\underline{Ш}_p(E/K)$ is trivial shows that the norm element kills $\underline{Ш}(E/L) \otimes \mathbf{Z}_p$. The result now follows from lemma 4.9.

Lemma 4.11 (Gross) *Let $\mathrm{ord}_p : \mathbf{Z}_p \longrightarrow \mathbf{Z}$ be the valuation homomorphism. The order of vanishing of $\underline{\theta}$ (if it is finite) is equal to*

$$\mathrm{ord}_p(\prod_{\chi \neq 1} \chi(\theta)),$$

where the product is taken over the $p - 1$ non-trivial characters of G.

Proof: A direct computation. (Or, see [Gr1].)

Proof of thm. 4.8: If the rank of $E(L)$ is strictly greater than the rank of $E(\mathbf{Q})$, then the vector space $E(L)\otimes\mathbf{Q}$ is a non-trivial rational representation of $G \simeq \mathbf{Z}/p\mathbf{Z}$. Hence,

$$\dim_{\mathbf{C}}(E(L)\otimes\mathbf{C})^{\chi} \geq 1,$$

for all complex valued characters $\chi : G \longrightarrow \mathbf{C}^*$, where $(E(L)\otimes\mathbf{C})^{\chi}$ denotes the χ-eigenspace for G acting on $E(L)\otimes\mathbf{C}$. The Birch Swinnerton-Dyer conjectures then predict that $L(E/\mathbf{Q},\chi,1) = 0$ for all characters χ of $G = \mathrm{Gal}(L/\mathbf{Q})$, and hence $\underline{\theta} = 0$. Likewise,

$$\rho_p = \dim_{\mathbf{F}_p}(\mathrm{Sel}_p(E/L)) \geq \dim_{\mathbf{F}_p} E(L)/pE(L) \geq p,$$

and hence $\Lambda = 0$.

Hence, assume from now on that $E(\mathbf{Q})$ and $E(L)$ have the same rank. Let ρ_{an} be the order of vanishing of θ. By lemma 4.11 we have

$$\rho_{\mathrm{an}} = \mathrm{ord}_p(\prod_{\chi\neq 1}\chi(\theta)).$$

But by thm. 4.5, we know that

$$\prod_{\chi\neq 1}\chi(\theta) = \prod_{\chi\neq 1}(\tau(\chi)L(E/\mathbf{Q},\chi,1))(2m_\infty)^{1-p}.$$

On the other hand,

$$\prod_{\chi} L(E/\mathbf{Q},\chi,s) = L(E/L,s).$$

Since we are assuming that $E(L)$ and $E(\mathbf{Q})$ have the same rank, the Birch and Swinnerton-Dyer conjectures predict that the L-functions $L(E/\mathbf{Q},s)$ and $L(E/L,s)$ have the same order of vanishing, r, at $s = 1$. Hence

$$\prod_{\chi\neq 1} L(E/\mathbf{Q},\chi,1) = \lim_{s\longrightarrow 1} L(E/L,s)/L(E/\mathbf{Q},s).$$

By the Birch and Swinnerton-Dyer conjectures over L and $\mathbf{Q}$, this limit is equal to

$$\frac{\#\underline{Ш}(E/L)}{\#\underline{Ш}(E/\mathbf{Q})}\frac{R(E/L)}{R(E/\mathbf{Q})}\frac{\#E(\mathbf{Q})^2_{\mathrm{tor}}}{\#E(L)^2_{\mathrm{tor}}}(m_\infty^{p-1})\mathrm{Disc}(L)^{-\frac{1}{2}},$$

where $R(E/L)$ and $R(E/\mathbf{Q})$ denote the Néron-Tate regulators of E over L and $\mathbf{Q}$. Hence,

$$\rho_{\text{an}} = ord_p \left\{ \frac{\#\underline{III}(E/L)}{\#\underline{III}(E/\mathbf{Q})} \frac{R(E/L)}{R(E/\mathbf{Q})} \frac{\#E(\mathbf{Q})^2_{\text{tor}}}{\#E(L)^2_{\text{tor}}} \right\}.$$

By lemma 2.12, the factor $\frac{\#E(\mathbf{Q})^2_{\text{tor}}}{\#E(L)^2_{\text{tor}}}$ is a unit at p. So is $\#\underline{III}(E/\mathbf{Q})$. Also, the inclusion $E(\mathbf{Q}) \longrightarrow E(L)$ is an isomorphism on the Mordell-Weil groups modulo torsion; since the Néron-Tate heights over $\mathbf{Q}$ and over L differ by a factor of $p = [L : \mathbf{Q}]$, it follows that $R(E/L)/R(E/\mathbf{Q})$ is a rational number and is equal to p^r. Hence,

$$\rho_{\text{an}} = \text{ord}_p(\#\underline{III}(E/L) \otimes \mathbf{Z}_p) + r.$$

By corollary 4.10 we have

$$\text{ord}_p(\#\underline{III}(E/L) \otimes \mathbf{Z}_p) = \dim_{\mathbf{F}_p}(\underline{III}_p(E/L)),$$

and hence

$$\rho_{\text{an}} = \dim_{\mathbf{F}_p}(\underline{III}_p(E/L)) + \dim_{\mathbf{F}_p} E(L)/pE(L) = \dim_{\mathbf{F}_p} \text{Sel}_p(E/L) = \rho_p,$$

as was to be shown.

We note that the strategy used to prove thm. 4.8 is the same as the one used by Gross in [Gr1] and by Ki-Seng Tan in his Harvard Ph.D. thesis [T1]. (There, Tan showed that order of vanishing statement of the Mazur-Tate conjectures follows from the usual Birch Swinnerton-Dyer conjectures over abelian number fields.)

4.3 Conjectures over quadratic fields

In this section, we suppose that E is still defined over $\mathbf{Q}$, but let the ground field K be a quadratic extension of $\mathbf{Q}$. Let $Z = \mathbf{Z}[\frac{1}{2\#E(K)_{\text{tor}}}]$. The Mordell-Weil group $E(K)$ is then equipped with an action of $\text{Gal}(K/\mathbf{Q})$, and we can decompose $E(K) \otimes Z$ into a direct sum of $+$ and $-$ eigenspaces for this action:

$$E(K) \otimes Z = E(K)^+ \oplus E(K)^-.$$

Let r^+ and r^- denote the ranks of these modules. Then $r = r^+ + r^-$, and r^+ and r^- can also be interpreted individually as the ranks of certain elliptic

curves over $\mathbf{Q}$. The integer r^+ is the rank of $E(\mathbf{Q})$, and r^- is the rank of $E_D(\mathbf{Q})$, where E_D is the curve over $\mathbf{Q}$ obtained from E by twisting by the quadratic character corresponding to $K/\mathbf{Q}$.

Let L/K be an extension of dihedral type of odd degree, i.e., $G = \mathrm{Gal}(L/K)$ is an abelian group of odd order, $L/\mathbf{Q}$ is Galois, and the involution τ in $\mathrm{Gal}(K/\mathbf{Q})$ acts on G by

$$\tau\sigma\tau^{-1} = \sigma^{-1}.$$

Let $\langle\ ,\ \rangle_1$ be the first height pairing with values in I/I^2. (It is defined for an arbitrary abelian group G, using prop. 3.15.) Under the above assumptions we have:

Proposition 4.12 *The canonical pairing $\langle\ ,\ \rangle_1$ with values in I/I^2 is trivial on the spaces $E(K)^+$ and $E(K)^-$.*

Proof: A straightforward manipulation, using the definition of $\langle\ ,\ \rangle_{L/K}$ and the Galois equivariance of the pairing $\langle\ ,\ \rangle_L$, shows that

$$\langle \tau a, \tau b\rangle_{L/K} = \tau\langle a, b\rangle_{L/K}\tau^{-1}.$$

Hence we have:

$$\langle \tau P, \tau Q\rangle_1 = \langle P, Q\rangle_1^{\tau} = \langle P, Q\rangle_1^{*},$$

since conjugation by τ acts like the involution $*$ on the group ring $\mathbf{Z}[G]$. Hence if P and Q belong to the same eigenspace, we have

$$\langle P, Q\rangle_1 = \langle P, Q\rangle_1^{*}.$$

Since $*$ acts by -1 on on I/I^2 and I/I^2 is a group of odd order, it follows that $\langle P, Q\rangle_1 = 0$.

Let $\delta = |r^+ - r^-|$. Suppose that the extension L/K has Galois group $G \simeq \mathbf{Z}/p\mathbf{Z} \times \cdots \times \mathbf{Z}/p\mathbf{Z}$ and that the prime p, in addition to satisfying the assumptions of sec. 2.3, has been chosen large enough so that $p > r + \delta$. Under these conditions the generalized Mazur-Tate regulator $\Lambda \in R/R_1^*$ is defined, where R denotes the group ring $\mathbf{F}_p[G]$.

Proposition 4.13 *Under the above assumptions, the generalized regulator Λ belongs to $I^{r+\delta}$.*

Proof: Suppose first that $G \simeq \mathbf{Z}/p\mathbf{Z}$ is cyclic. Let $r_p^{\pm}$ denote the ranks of the plus and minus eigencomponents of the Selmer group $\mathrm{Sel}_p(E/K)$, and let $\delta_p = |r_p^+ - r_p^-|$. By thm. 3.21, Λ vanishes to order at least

$$\rho_p = \dim \mathrm{Sel}^{(1)} + \dim \mathrm{Sel}^{(2)} + \cdot + \dim \mathrm{Sel}^{(p)}.$$

But $\dim \mathrm{Sel}^{(1)} = r_p$, and the nullspace $\mathrm{Sel}^{(2)}$ of $\langle\ ,\ \rangle_1$ has dimension at least δ_p by prop. 4.12, so that

$$\rho_p \geq r_p + \delta_p = 2\max(r_p^+, r_p^-) \geq 2\max(r^+, r^-) = r + \delta,$$

and hence the result follows for $G = \mathbf{Z}/p\mathbf{Z}$. When $G \simeq (\mathbf{Z}/p\mathbf{Z})^t$, let k be the order of vanishing of Λ. We may assume without loss of generality that $k < p$, for otherwise, we are done, as $p > r + \delta$. The image of Λ in I^k/I^{k+1} is then non-zero. This image can be described by a homogenous polynomial $\phi(x_1, \ldots, x_t)$ of degree k in t variables with entries in $\mathbf{F}_p$, by replacing the expressions $(\sigma_j - 1)$, where $\sigma_1, \ldots, \sigma_t$ are a system of generators for G, with variables $x_1, \ldots, x_t$. An induction on t shows that there exists $(a_1, \ldots, a_t)$ such that $\phi(a_1, \ldots, a_t) \neq 0$. Hence, the homomorphism $\Psi : G \longrightarrow H = \mathbf{Z}/p\mathbf{Z}$ defined by $\Psi(\sigma_j) = a_j$ has the property that $\Psi(\Lambda)$ is non-zero in $\underline{I}^k/\underline{I}^{k+1}$, where $\underline{I}$ denotes the augmentation ideal in the group ring $\mathbf{F}_p[H]$. By the compatibility of the generalized regulators under norms discussed in sec. 3.4.2, the element $\Psi(\Lambda)$ is just the generalized regulator associated to $(E, \underline{L}/K)$, where $\underline{L}$ is the fixed field of $\ker(\Psi)$. Since $\mathrm{Gal}(\underline{L}/K) = H$ is cyclic, it follows that $k \geq r + \delta$ from the proof for cyclic groups.

4.3.1 Real quadratic fields and Heegner cycles

We specialize now to the case where K is a real quadratic field such that all $p|N$ are split in $K/\mathbf{Q}$, and let L/K be an abelian extension of dihedral type and satisfying the assumptions of sec. 2.3 as before. In this case, an element θ satisfying an interpolation property for the special values of $L(E/K, \chi, 1)$ can be constructed using certain geodesic cycles. This construction is explained in [D2]. (The element that we call θ is called L_D in the paper [D2].) In sec. 3.1 of [D2], we were led to make the following conjecture on the order of vanishing of θ:

Conjecture 4.14 *θ belongs to $I^{r+\delta}$, where $\delta = |r^+ - r^-|$.*

This conjecture agrees well with prop. 4.13; in fact, one can predict the value of the leading coefficient of θ, in terms of the generalized regulator Λ associated to $(E, L/K)$. As before, let

$$J = \prod \#E(K(v)) \cdot \#E/E_0,$$

where the product is taken over all places v of K which are ramified in L/K.

Conjecture 4.15 $\theta = J\Lambda \pmod{R_1^*}$.

4.3.2 Imaginary quadratic fields and Heegner points

Let K be an imaginary quadratic field such that all $p|N$ are split in $K/\mathbf{Q}$, and let L/K be an abelian extension of dihedral type and of odd degree.

In this case, the sign in the functional equation for $L(E/K, \chi, s)$ is -1. In addition, $L(E/K, \chi, s) = L(E/K, \bar{\chi}, s)$ because E is defined over $\mathbf{Q}$ and χ factors through an extension of dihedral type. Therefore, $L(E/K, \chi, 1) = 0$ for all characters χ of $G = \mathrm{Gal}(L/K)$. However, an element θ' satisfying an interpolation property for the special values of *derivatives* of the L-function, $L'(E/K, \chi, 1)$, can be constructed using Heegner points. This construction is explained in [D1], but we recall it briefly here.

Let f be the conductor of the smallest ring class field containing L, and let L_d, for $d|f$, be the ring class field of K of conductor d. Let $\alpha_d \in E(L_d)$ be the Heegner point defined over the ring class field L_d, defined by the usual construction of Heegner (cf. [Gr2].) For simplicity, assume that these points are obtained from a strong Weil parametrization, with Manin constant equal to 1. Let μ be the Möbius function, and let ω be the odd quadratic Dirichlet character corresponding to $K/\mathbf{Q}$. Let β_1 and β_2 be the following integral combinations of Heegner points,

$$\beta_1 = \sum_{d|f} \mu(d)\alpha_d,$$

$$\beta_2 = \sum_{d|f} \mu(d)\omega(d)\alpha_d,$$

and let γ_1 and γ_2 be the images of β_1 and β_2 in $E(L)$ under the norm map. Finally, define θ' as a kind of resolvent element made from the Heegner points γ_1 and γ_2:

$$\theta' = \sum_{\sigma,\tau \in G} \gamma_1^\sigma \otimes \gamma_2^\tau \otimes \sigma\tau^{-1} \in E(L)^{\otimes 2} \otimes \mathbf{Z}[G],$$

where all tensor products are taken over $\mathbf{Z}$.

The motivation for the definition of β_1 and β_2 is that under norms they are better behaved than the "naive" Heegner points α_d. For details, see [D1], prop. 3.13.

Under certain mildly restrictive assumptions on E and L/K, we were able to show (thm. 2.4 of [D1]) that the element θ' vanishes to order at least $(r-1)+(\delta-1)$, i.e.,

$$\theta' \in E(L)^{\otimes 2} \otimes I^{(r-1)+(\delta-1)}.$$

A refined conjecture of Mazur-Tate type was then formulated in this setting. In particular, we were able to formulate a conjecture (conj. 2.3 of [D1]) on the value of the leading coefficient $\tilde{\theta}'$ of θ', defined to be the image of θ' in $E(L)^{\otimes 2} \otimes I^{r-1}/I^r$. When $\delta > 1$, this leading coefficient was zero, and a stronger conjecture about the leading coefficient in $E(L) \otimes I^{(r-1)+(\delta-1)}/I^{(r+\delta-1)}$, which would have been more natural, eluded us.

We will now formulate such a conjecture, but only in the simplest case where $G = \mathbf{Z}/p\mathbf{Z}$, and where L satisfies the assumptions of 2.3, so that we have at our disposal the construction of the generalized regulator in terms of derived heights. In particular, one has the canonical filtration $\mathrm{Sel}^{(1)} \supset \ldots \supset \mathrm{Sel}^{(p)}$ by the nullspaces of the successive derived pairings. We make the following assumptions:

Assumption 4.16 .

1. *The group $\underline{III}_p(E/K)$ is trivial.*
2. *The rank of $E(L)$ is strictly greater than the rank of $E(K)$.*

Assumption 2 follows from the Birch and Swinnerton-Dyer conjecture, since $L(E/K, \chi, 1) = 0$ for all characters χ of G.

The assumptions above have the following consequences for the Galois module structure of the Mordell-Weil group $E(L)$:

Lemma 4.17 *Under assumptions 4.16, $H^1(G, E(L)) = 0$.*

Proof: Inflation gives an injective map $H^1(G, E(L)) \longrightarrow H^1(K, E)_p$. Because $H^1(G, E(L_v))$ is trivial for all places v of K (by lemma 2.17) it follows that $H^1(G, E(L))$ injects into $\underline{III}_p(E/K)$. But this group is trivial by assumption.

Proposition 4.18 *Under assumption 4.16, the space* $\mathrm{Sel}^{(p)}$ *(consisting of the norms in* $\mathrm{Sel}_p(E/K)$ *from* $\mathrm{Sel}_p(E/L)$*) is non-trivial.*

Proof: Let α be a point in $E(L)$ which does not belong to $E(K) + E(L)_{\mathrm{tor}}$. Such an α exists, by assumption 4.16. Assume without loss of generality that the image of α in $E(L)/pE(L)$ is non-trivial - otherwise, divide α by p as much as is necessary. If $\mathrm{norm}(\alpha)$ is non-trivial in $E(K)/pE(K)$, then it gives a non-zero element in $\mathrm{Sel}^{(p)}$, and we are done. Otherwise, we can choose α of norm 0. Let T be the $\mathbf{Z}[G]$-submodule of $E(L)$ generated by α. The image of T in $E(L)/pE(L)$ is non-trivial, and hence there exists $\beta \in T$ whose image in $E(L)/pE(L)$ is non-zero and invariant under G. But the map $E(K)/pE(K) \longrightarrow (E(L)/pE(L))^G$ is an isomorphism, because its cokernel is $H^1(G, E(L))$ which is trivial by lemma 4.17. Hence, there exists a point P in $E(K)$ such that

$$P = \beta + p\gamma, \quad \gamma \in E(L).$$

Since the image of the point β in $E(L)/pE(L)$ is non-trivial, the image of P in $E(K)/pE(K)$ is non-trivial as well. But β is a combination of the conjugates of α, which are of norm 0; it follows from taking norms in the above equality that

$$pP = p\mathrm{norm}\gamma,$$

and since $E(K)$ is uniquely divisible by p, the point P is a norm of a point γ in $E(L)$. Hence the image of P in $E(K)/pE(K) \subset \mathrm{Sel}_p(E/K)$ gives the desired non-trivial element in $\mathrm{Sel}^{(p)}$.

The proposition just proved shows that the generalized regulator Λ associated to $(E, L/K)$ is always zero under assumptions 4.16, because of the presence of non-trivial global norms. Still, one can use the derived heights to construct a modified regulator term Λ' in this situation. If the space $\mathrm{Sel}^{(p)}$ has dimension strictly greater than 1, set $\Lambda' = 0$. Otherwise, let $s_1, \ldots, s_r$ be an $\mathbf{F}_p$-basis for Sel which is compatible with the filtration on Sel, and arises as the image of an integral basis for $E(K)$. In particular, the element s_r comes from a point $P \in E(K)$ which is a norm from $\mathrm{Sel}_p(E/L)$. Let $\Lambda^{(i)}$, for $1 \leq i \leq p-1$ be the partial regulators formed from the derived height pairing $\langle\ ,\ \rangle_i$ restricted to $\mathrm{Sel}^{(i)}/\mathrm{Sel}^{(i+1)}$, as in section 3.5. Then set

$$\Lambda' = P^{\otimes 2} \cdot \Lambda^{(1)} \cdots \Lambda^{(p-1)}.$$

Let

$$\rho_p^{'} = (\dim_{\mathbf{F}_p} \mathrm{Sel}^{(1)} - 1) + \cdots + (\dim_{\mathbf{F}_p} \mathrm{Sel}^{(p-1)} - 1).$$

One can check that $\Lambda^{'}$ belongs to $E(K)^{\otimes 2} \otimes I^{\rho_p^{'}}/I^{\rho_p^{'}+1}$. By prop. 4.12, $\rho_p^{'}$ is greater or equal to $(r-1)+(\delta-1)$.

Let $\underline{\theta^{'}}$ be the image of $\theta^{'}$ in $E(L)^{\otimes 2} \otimes R$. Let J be the same product of Euler factors as was defined in section 4.3.1. One can now formulate the conjecture on Heegner points:

Conjecture 4.19

$$\underline{\theta^{'}} = \#\underline{Ш}(E/K) J \Lambda^{'}.$$

We now formulate a weaker form of the conjecture (still under the assumptions 4.16), which has the merit of being more explicit. Let $\mathcal{E}(L)$ denote the module generated by the Heegner point γ_1 (or γ_2) in $E(L)$, and let $\mathcal{E}(L)_p$ denote the image of $\mathcal{E}(L)$ in $E(L) \otimes \mathbf{F}_p$.

Conjecture 4.20 *If $\rho_p^{'} > 2p$, then $\mathcal{E}(L)_p = 0$. Otherwise,*

$$\dim_{\mathbf{F}_p}(\mathcal{E}(L)_p) = p - \frac{1}{2}\rho_p^{'}.$$

This conjecture gives a more precise estimate on the size of the module $\mathcal{E}(L)_p$ than was given in th. 2.6 of [D1]. It is likely that the methods there could be applied to prove conjecture 4.20 in certain cases, with the equality replaced by a $\leq$ sign; this would strengthen the estimate provided by th. 2.6 of [D1]. To prove the equality, and not just an upper bound on the size of the module $\mathcal{E}(L)_p$, would seem to require new ideas.

An analogue of conj. 4.20 when L/K is the anticyclotomic $\mathbf{Z}_p$-extension was formulated by B. Perrin-Riou in [PR]. Results in this direction are obtained in [B]. In a forthcoming paper [BD] we extend the formalism of derived heights and generalized regulators to $\mathbf{Z}_p$-extensions, in a more general setting.

References

[B] M. Bertolini, Iwasawa theory, L-functions and Heegner points, PhD Thesis, Columbia University, 1992.

[BD] M. Bertolini and H. Darmon, *Derived p-adic heights*, to appear.

[C1] J.W.S. Cassels, *Arithmetic on curves of genus 1 III. The Tate-Šafarevič and Selmer groups*, Proc. London Math. Soc. (3), 46 (1962), 259-296.

[C2] J.W.S. Cassels, *Arithmetic on curves of genus* 1 *IV. Proof of the Hauptvermutung* J. reine angew. Math., 211 (1962), 95-112.

[CF] Algebraic number theory, edited by J.W.S. Cassels and A. Frölich, Academic Press, 1967.

[D1] H. Darmon, *A refined conjecture of Mazur-Tate type for Heegner points*, Inv. Math. 110, 123-146 (1992)

[D2] H. Darmon, *Heegner points, Heegner Cycles, and Congruences*, Proceedings of a conference on elliptic curves and related topics, Ste-Adèle, Québec, 1992.

[D3] H. Darmon, *Euler systems and refined conjectures of Birch Swinnerton-Dyer type*, proceedings of a conference on p-adic monodromy and the Birch Swinnerton-Dyer conjecture, Boston University, August 1991, to appear.

[Fr] Fröhlich, A., Galois module structure of algebraic integers, Springer-Verlag, 1983.

[Gr1] B.H. Gross, *On the values of abelian L-functions at* $s = 0$, J. Fac. Sci. Univ. Tokyo, Sect. IA, Math. 35 (1988), 177-197.

[Gr2] B.H. Gross, *Heegner points on* $X_0(N)$, in Modular Forms, R.A. Rankin ed., p. 87-107, Ellis Horwood Ltd., 1984.

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

[MT1] B. Mazur and J. Tate, *Canonical height pairings via biextensions*, in Arithmetic and Geometry, Volume I, Michael Artin and John Tate, editors, Progress in Mathematics, Birkhauser, Boston, pp. 195-238.

[MT2] B. Mazur and J. Tate, *Refined conjectures of the "Birch and Swinnerton-Dyer type"*, Duke Math Journal, Vol. 54, No. 2, 1987, p. 711-750.

[Mi] J.S. Milne, Arithmetic duality theorems, Perspectives in Mathematics, Vol. 1, J. Coates, S. Helgason, eds., Academic Press 1986.

[PR] B. Perrin-Riou, *Fonctions L p-adiques, Théorie d'Iwasawa et points de Heegner*, Bull. Soc. Math. de France 115, 1987, 455-510.

[Sc1] P. Schneider, *Iwasawa L-functions of algebraic varieties over algebraic number fields*, Inv. Math. 71, 251-293, 1983.

[Sc2] P. Schneider, *p-adic height pairings II*, Inv. Math. 79, 329-374, 1985.

[Se] J-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. Invent. Math. 15 (1972), 259-331.

[Sh] T. Shintani, On construction of holomorphic cusp forms of half integral weight, Nagoya Math. J., vol. 58 (1975), 83-126.

[T1] K.-S. Tan, Harvard PhD. Thesis, 1991.

[T2] K.-S. Tan, p-adic pairings, proceedings of a conference on p-adic monodromy and the Birch Swinnerton-Dyer conjecture, Boston University, August 1991, to appear.

[Ta] J. Tate, *Duality theorems in Galois cohomology over number fields*, Proc. Intern. Congress Math., Stockholm, pp. 234-241.