DERIVED P-ADIC HEIGHTS

By Massimo Bertolini and Henri Darmon

Introduction. Let E be an elliptic curve defined over a number field K, and let K_∞/K be a $\mathbb{Z}_p$-extension. Denote by Λ the Iwasawa algebra $\mathbb{Z}_p[[\Gamma]]$, with $\Gamma = \mathrm{Gal}\,(K_\infty/K)$. Given any topological generator γ of Γ, write I for the ideal $(\gamma - 1)\Lambda$ of Λ. Let $E(K)_p = \lim_{\overleftarrow{n}} E(K)/p^n E(K)$ denote the p-adic completion of $E(K)$. When E has good ordinary reduction at the primes above p which are ramified in K_∞/K, there is a canonical symmetric pairing

$$\langle\ ,\ \rangle : E(K)_p \times E(K)_p \to I/I^2,$$

called the *p-adic height pairing* (for a definition, see for instance [MT1] or [Sc1]).

Unlike the Néron-Tate canonical height, the p-adic height pairing can be degenerate in certain cases, and the phenomena associated to this degeneracy are poorly understood. This paper is devoted to the study of these questions.

One of the main results of this paper, Theorem 2.18, states the existence, for $1 \le k \le p-1$, of a sequence of canonical pairings, called *derived p-adic heights*,

$$\langle\langle\ ,\ \rangle\rangle_k : \bar{S}_p^{(k)} \times \bar{S}_p^{(k)} \to I^k/I^{k+1} \otimes \mathbb{Q},$$

where $\bar{S}_p^{(1)} = \lim_{\overleftarrow{n}} \mathrm{Sel}_{p^n}(E/K)$ is the inverse limit of the p^n-Selmer groups with respect to the multiplication by p maps, and for $k \ge 2$ $\bar{S}_p^{(k)}$ denotes the null-space of $\langle\langle\ ,\ \rangle\rangle_{k-1}$.

We show that these pairings are either symmetric or alternating, depending on whether k is odd or even, and the space of universal norms of $\bar{S}_p^{(1)}$ is contained in their null-space. We also show that the restriction of $\langle\langle\ ,\ \rangle\rangle_1$ to $E(K)_p$ is equal to $\langle\ ,\ \rangle$. We give an alternate description of the null-spaces $\bar{S}_p^{(k)}$ in terms of the Λ-module structure of the Selmer group of E/K_∞. See Theorem 2.18 and Theorem 2.7.

The product of the discriminants of the above pairings (viewed as defined on $(\bar{S}_p^{(k)}/\bar{S}_p^{(k+1)})$) provides a generalization of the notion of p-adic regulator. This

Manuscript received May 27, 1994.

Research of the first author supported in part by M.U.R.S.T. of Italy and by Consiglio Nazionale delle Ricerche.

Research of the second author supported in part by an NSF grant and by NSERC.

American Journal of Mathematics 117 (1995), 1517–1554.

derived regulator is useful in all instances where the p-adic height $\langle\langle\ ,\ \rangle\rangle_1$ is degenerate (i.e. the classical p-adic regulator vanishes) as a way of describing in a convenient manner the leading coefficient of the p-adic (algebraic) L-function associated to the data $(E, K_\infty/K)$. See Theorem 2.23 for the precise statement.

When E is defined over $\mathbb{Q}$, the anticyclotomic $\mathbb{Z}_p$-extension of an imaginary quadratic field K provides a prototypical example of the above situation, since the Galois equivariance of $\langle\langle\ ,\ \rangle\rangle_1$ forces degeneracy if the "plus" and "minus" part of $\bar{S}_p^{(1)}$ under the action of complex conjugation have different ranks. This case is analyzed in detail in the third part of the paper where, inspired by conjectures of Mazur ([Ma2], [Ma3]), we predict that the null-space of the second derived height consists exactly of the subspace of universal norms (cf. §3.2). We also explain how this fits into a (partly conjectural) picture describing the behavior of Heegner points over the anticyclotomic tower.

1. Preliminary results.

1.1. Notations and assumptions. We keep the notations of the introduction. For $n \geq 1$, let K_n/K denote the subextension of K_∞ of degree p^n. Given a place v of K, let K_v be the completion of K at v. If F is any finite extension of K, we write

$$F_v = \bigoplus\nolimits_{w|v} F_w,$$

where the sum is taken over all places of F above v. Functors on abelian categories will always be additive, e.g.,

$$H^i(F_v, M) := \bigoplus\nolimits_{w|v} H^i(F_w, M),$$

if M is any Gal$(\bar{K}/K)$-module.

Throughout the paper we make the following assumptions on $(E, p, K_\infty/K)$.

(1) $p \nmid 2\#(E/E^0)$, where E/E^0 denotes the group of connected components of the Néron model of E over Spec$(\mathcal{O}_K)$.

(2) E has good reduction above p.

(3) The image of the Galois representation ρ_p : Gal$(\bar{K}/K) \longrightarrow$ Aut(E_p) contains a Cartan subgroup of Aut$(E_p) \simeq GL_2(\mathbb{F}_p)$.

(4) The local norm mappings Norm$_v$: $E((K_n)_v) \longrightarrow E(K_v)$ are surjective for all primes v of K and for all finite subextensions K_n of K_∞/K.

Proposition 1.1. *Assume that for all primes v ramified in K_∞/K, $p \nmid \#E(\mathbb{F}_v)$ and v is ordinary for E. Then assumption 4 is satisfied.*

Proof. This is proved in [Ma1], §4. □

Conversely, observe that assumption 4 implies that all the primes above p which are ramified in K_∞/K are ordinary primes for E.

Using Proposition 1.1, it is easy to construct $\mathbb{Z}_p$-extensions satisfying conditions 1-4, once E/K is fixed. First, almost all primes p of $\mathbb{Q}$ satisfy conditions 1-3, by Serre's "open image theorem" [Se] and the theory of complex multiplication. Given a prime v of K above p where E has good reduction, let α_v and β_v denote the eigenvalues of the Frobenius at v. Assume for simplicity that E does not have complex multiplications, and that K_v has residue field $\mathbb{F}_p$ (the set of such v's has density 1). The conditions that E be ordinary at v and $p \nmid \#E(\mathbb{F}_v)$ translate into $a_v \not\equiv 0, 1 \pmod p$, where a_v is the rational integer $a_v = \alpha_v + \beta_v$. If $p \geq 7$, this is equivalent to $a_v \neq 0, 1$ in $\mathbb{Z}$ by the Hasse bound $a_v \leq 2\sqrt{p}$. Now choose a rational prime $l \neq p$ lying below primes of good reduction for E. The integer a_v is equal to the trace of $Frob_v$ acting on the Tate module T_lE. By [Se], we may assume that $\mathrm{Gal}(K(E_{l^n})/K)$ is isomorphic to $GL_2(\mathbb{Z}/l^n\mathbb{Z})$ for all $n \geq 1$. The Chebotarev density theorem applied to the extensions $K(E_{l^n})/K$ for $n \to \infty$ implies that the set of v as above such that $a_v \neq 0, 1$ has density 1.

In conclusion, any $\mathbb{Z}_p$-extension K_∞/K such that p lies below the primes v considered above satisfies conditions 1–4.

1.2. The duality formalism. In this section let L/K denote any finite subextension of K_∞/K. We review some duality theorems for the Galois cohomology of an elliptic curve, together with results of [BD] built on them. (In effect, these results hold more generally for finite abelian p-extensions.)

1.2.1. Duality (Reference: [Mi], chapter 1). Let v be a finite prime of K and m be a positive integer. Recall the local Tate pairing

$$\langle\ ,\ \rangle_{L_v,m} : H^1(L_v, E_m) \times H^1(L_v, E_m) \to \mathbb{Z}/m\mathbb{Z},$$

defined by composing the cup product with the Weil pairing. (In view of our conventions, $H^1(L_v, E_m) = \bigoplus_{w|v} H^1(L_w, E_m)$, thus $\langle\ ,\ \rangle_{L_v,m}$ is actually a sum over the primes of L dividing v of the local Tate pairings.) The local Tate pairing is nondegenerate, symmetric and Galois-equivariant. The submodule of local points $E(L_v)/mE(L_v)$ is the orthogonal complement of itself under $\langle\ ,\ \rangle_{L_v,m}$. Hence there is also an induced nondegenerate pairing

$$[\ ,\ ]_{L_v,m} : E(L_v)/mE(L_v) \times H^1(L_v, E)_m \to \mathbb{Z}/m\mathbb{Z}.$$

Later we shall need the following compatibility formulae for the local Tate pairings, which are consequences of standard properties of the cup product.

$$(1) \qquad \langle \mathrm{cores}_{L_v/K_v}(a), b\rangle_{K_v,m} = \langle a, \mathrm{res}_{L_v/K_v}(b)\rangle_{L_v,m}, \quad \forall a \in H^1(L_v, E_m), \forall b \in H^1(K_v, E_m).$$

$$(2) \qquad [\mathrm{cores}_{L_v/K_v}(a), b]_{K_v,m} = [a, \mathrm{res}_{L_v/K_v}(b)]_{L_v,m}, \quad \forall a \in E(L_v)/mE(L_v), \forall b \in H^1(K_v, E)_m.$$

Let Σ be a finite, possibly empty, set of nonarchimedean primes of K. The local Tate pairing gives rise in the obvious way to nondegenerate Galois-equivariant pairings

$$\langle\ ,\ \rangle_{L,m} : \bigoplus_{v\in\Sigma} H^1(L_v, E_m) \times \bigoplus_{v\in\Sigma} H^1(L_v, E_m) \to \mathbb{Z}/m\mathbb{Z}.$$
$$[\ ,\ ]_{L,m} : \bigoplus_{v\in\Sigma} E(L_v)/mE(L_v) \times \bigoplus_{v\in\Sigma} H^1(L_v, E)_m \to \mathbb{Z}/m\mathbb{Z}.$$

Define the Σ-Selmer group of E/L to be

$$\mathrm{Sel}_m^{\Sigma}(E/L) = \{s \in H^1(L, E_m) : \mathrm{res}_w(s) \in E(L_w)/mE(L_w)\ \forall w \mid v,\ v \notin \Sigma\}.$$

When Σ is the empty set, one finds the usual Selmer group $\mathrm{Sel}_m(E/L)$. By definition, there is a map

$$\mathrm{Sel}_m(E/L) \to \bigoplus_{v\in\Sigma} E(L_v)/mE(L_v).$$

By passing to the Pontryagin dual, we obtain a map

$$\delta = \delta_\Sigma : \bigoplus_{v\in\Sigma} H^1(L_v, E)_m \to \mathrm{Sel}_m(E/L)^{dual},$$

where $H^1(L_v, E)_m$ is identified with $(E(L_v)/mE(L_v))^{dual}$ via the local Tate duality. The following, known as the Cassels dual exact sequence, plays a key role in our construction.

Proposition 1.2. *There is an exact sequence*

$$0 \to \mathrm{Sel}_m(E/L) \to \mathrm{Sel}_m^{\Sigma}(E/L) \to \oplus_{v\in\Sigma} H^1(L_v, E)_m \xrightarrow{\delta} \mathrm{Sel}_m(E/L)^{dual},$$

where the first map is the canonical inclusion and the second one is induced by the natural map $H^1(L, E_m) \to H^1(L, E)_m$ followed by localization.

Proof. [Mi], Lemma 6.15, p. 105. □

The nontrivial point in the proof of 1.2 is to show the exactness at the third term of the sequence. Rephrased, this means that a $\#\Sigma$-tuple of local classes of $\oplus_{v\in\Sigma} H^1(L_v, E)_m$ pairs to zero with all the elements of the Selmer group $\mathrm{Sel}_m(E/L)$ under the local Tate pairing if and only if it comes from a global class of $\mathrm{Sel}_m^{\Sigma}(E/L)$.

Half of this statement, namely, that the image of $\mathrm{Sel}_m^{\Sigma}(E/L)$ in $\mathrm{Sel}_m(E/L)^{dual}$ is zero, follows from the global reciprocity law of class field theory. (More precisely, given global classes α and β of $H^1(L, E_m)$, their cup product composed with the Weil pairing gives an element $\alpha \cdot \beta$ in the m-torsion $Br(L)_m$ of the Brauer group of L. The local invariant at v of $\alpha \cdot \beta$ is equal to the local Tate pairing $\langle \mathrm{res}_v(\alpha), \mathrm{res}_v(\beta)\rangle_{L_v,m}$. But the sum of the local invariants is zero by class field theory.) The other half follows from Tate's global duality theorem [Mi], ch. I, Theorem 4.10. Write G for the Galois group of the extension L/K. The $\mathbb{Z}/m\mathbb{Z}[G]$-valued pairing we introduce next will be an ingredient in the construction of the derived heights. Define

$$\langle\ ,\ \rangle : \bigoplus_{v\in\Sigma} H^1(L_v, E_m) \times \bigoplus_{v\in\Sigma} H^1(L_v, E_m) \to \mathbb{Z}/m\mathbb{Z}[G]$$

by the rule

$$\langle x, y\rangle := \sum_{g\in G} \langle x, y^g\rangle_{L,m} \cdot g^{-1}.$$

Write $\epsilon : \mathbb{Z}/m\mathbb{Z}[G] \to \mathbb{Z}/m\mathbb{Z}$ for the augmentation map. Let $\lambda \mapsto \lambda^*$ denote the involution of $\mathbb{Z}/m\mathbb{Z}[G]$ defined on group-like elements by $g \mapsto g^{-1}$.

PROPOSITION 1.3.

(1) *The pairing $\langle\ ,\ \rangle$ is nondegenerate. It is $\mathbb{Z}/m\mathbb{Z}[G]$-linear in the first variable and $*$-linear in the second variable, i.e. for all $\lambda \in \mathbb{Z}/m\mathbb{Z}[G]$ we have $\langle \lambda a, b\rangle = \lambda\langle a, b\rangle$, $\langle a, \lambda b\rangle = \lambda^*\langle a, b\rangle$.*

(2) $\langle a, b\rangle = \langle b, a\rangle^*$.

(3) $\epsilon\langle a, b\rangle = -\langle \mathrm{cores}_{L/K}(a), \mathrm{cores}_{L/K}(b)\rangle_{K,m}$.

(4) *The image of $\bigoplus_{v\in\Sigma} E(L_v)/mE(L_v)$ in $\bigoplus_{v\in\Sigma} H^1(L_v, E_m)$ is isotropic for $\langle\ ,\ \rangle$.*

(5) *The image of $\mathrm{Sel}_m^\Sigma(E/L)$ in $\bigoplus_{v\in\Sigma} H^1(L_v, E_m)$ is isotropic for $\langle\ ,\ \rangle$.*

Proof.

(1) follows from the fact that $\langle\ ,\ \rangle_{L,m}$ is nondegenerate and G-equivariant.

(2) follows from the symmetry and G-equivariance of $\langle\ ,\ \rangle_{L,m}$.

(3) is a consequence of formula (1) above.

(4) follows from the isotropy of the local points with respect to the local Tate pairing.

(5) follows from the global reciprocity law of class field theory. □

1.2.2. Descent theory. From now on, we shall work with p-groups (notationwise, replace the positive integer m with p^m).

LEMMA 1.4. *For any choice of Σ, the restriction map induces an isomorphism*

$$\mathrm{res} : \mathrm{Sel}_{p^m}^\Sigma(E/K) \to \mathrm{Sel}_{p^m}^\Sigma(E/L)^G.$$

Proof. The Hochschild-Serre spectral sequence gives

$$H^1(G,H^0(L,E_{p^m})) \to H^1(K,E_{p^m}) \to H^1(L,E_{p^m})^G \to H^2(G,H^0(L,E_{p^m})).$$

By assumption 3 of §1.1, $E_p(L) = 0$. Hence we get an isomorphism $H^1(K,E_{p^m}) \to H^1(L,E_{p^m})^G$. It follows that $\mathrm{Sel}^{\Sigma}_{p^m}(E/K)$ injects into $\mathrm{Sel}^{\Sigma}_{p^m}(E/L)^G$. Let s be an element of this last group. Then s is a class of $H^1(K,E_{p^m})$ whose image in $H^1(L_v,E)^G$ is trivial for all v not in Σ. To conclude the proof, observe that restriction induces an isomorphism $H^1(K_v,E) \to H^1(L_v,E)^G$ for all v. For this, by the Hochschild-Serre spectral sequence, it suffices to check that $\hat{H}^1(G,E(L_v))$ and $\hat{H}^2(G,E(L_v))$ are both trivial. This is equivalent to $\hat{H}^0(G,E(L_v)) = \hat{H}^1(G,E(L_v)) = 0$ ([CF], Theorem 9, p. 113). The first group is trivial by our assumption on the local norms. As for the second group, it is dual of the first by the compatibility formula (2) of §1.2.1, combined with the nondegeneracy of the local Tate pairing. □

Definition 1.5. An *admissible set* for $(E,L/K,p^m)$ is any finite set Σ of primes of K such that for all v in Σ:

(1) res char$(v) \neq p$ and v is a prime of good reduction for E;

(2) v is split in L;

(3) $E(K_v)/p^mE(K_v) \simeq (\mathbb{Z}/p^m\mathbb{Z})^2$;

(4) $\mathrm{Sel}_{p^m}(E/K)$ injects into $\bigoplus_{v\in\Sigma}E(K_v)/p^mE(K_v)$ under the natural restriction map.

The existence of admissible sets of primes for $(E,L/K,p^m)$ (infinitely many, indeed) is proved in [BD], Lemma 2.23. It follows from a standard argument based on the Chebotarev density theorem applied to M/K, M being the extension of $L(E_{p^m})$ cut out by the elements of the Selmer group $\mathrm{Sel}_{p^m}(E/K)$. The same argument shows that one can assume that the cardinality of Σ is equal to $dim_{\mathbb{F}_p}(\mathrm{Sel}_{p^m}(E/K)\otimes\mathbb{F}_p)$.

PROPOSITION 1.6. *Let Σ be an admissible set for $(E,L/K,p^m)$. Then there is an exact sequence*

$$0 \to \mathrm{Sel}_{p^m}(E/L) \to \mathrm{Sel}^{\Sigma}_{p^m}(E/L) \to \bigoplus_{v\in\Sigma}H^1(L_v,E)_{p^m} \xrightarrow{\delta} \mathrm{Sel}_{p^m}(E/L)^{dual} \to 0.$$

Proof. By Proposition 1.2 and duality, we only need to show that the map $\mathrm{Sel}_{p^m}(E/L) \to \bigoplus_{v\in\Sigma}E(L_v)/p^mE(L_v)$ is injective. Assume the contrary, and denote by s a nonzero element of the kernel. Then we can find a nonzero element s' of the $\mathbb{Z}/p^m\mathbb{Z}[G]$-module $\mathbb{Z}/p^m\mathbb{Z}[G]s$ fixed under the action of G. s' is in the kernel of the above map. Since by Lemma 1.5 s' comes from $\mathrm{Sel}_{p^m}(E/K)$, this contradicts the hypothesis that Σ is admissible. □

LEMMA 1.7. *Let Σ be an admissible set for $(E, L/K, p^m)$.*

(1) *The modules $\bigoplus_{v\in\Sigma} E(L_v)/p^m E(L_v)$, $\bigoplus_{v\in\Sigma} H^1(L_v, E)_{p^m}$ and $\bigoplus_{v\in\Sigma} H^1(L_v, E_{p^m})$ are free $\mathbb{Z}/p^m\mathbb{Z}[G]$-modules of ranks $2\#\Sigma$, $2\#\Sigma$ and $4\#\Sigma$, respectively.*

(2) *We can identify $\bigoplus_{v\in\Sigma} E(L_v)/p^m E(L_v)$ and $\mathrm{Sel}^{\Sigma}_{p^m}(E/L)$ with submodules of $\bigoplus_{v\in\Sigma} H^1(L_v, E_{p^m})$ via the natural maps. Then, their intersection is equal to $\mathrm{Sel}_{p^m}(E/L)$.*

Proof. (1) follows immediately from the definition of admissible set and the local Tate duality. As for (2), the only non-obvious thing is to show that the natural map $\mathrm{Sel}^{\Sigma}_{p^m}(E/L) \to \bigoplus_{v\in\Sigma} H^1(L_v, E_{p^m})$ is injective. Its kernel contains the elements of $\mathrm{Sel}_{p^m}(E/L)$ mapping to zero in $\bigoplus_{v\in\Sigma} E(L_v)/p^m E(L_v)$. Since Σ is admissible, the kernel is 0. □

When Σ is an admissible set, the descent module $\mathrm{Sel}_{p^m}(E/L)$ has a simple and "predictable" Galois structure. This fact will play an important role in the construction of the derived heights.

PROPOSITION 1.8. *Let Σ be admissible for $(E, L/K, p^m)$. Then $\mathrm{Sel}^{\Sigma}_{p^m}(E/L)$ is a free $\mathbb{Z}/p^m\mathbb{Z}[G]$-module of rank $2\#\Sigma$.*

Proposition 1.8 is proved in [BD], Theorem 3.2. The proof consists in a counting argument, which exploits the exact sequence of Proposition 1.6 and the information on the $\mathbb{Z}/p^m\mathbb{Z}[G]$-module structure of $\bigoplus_{v\in\Sigma} H^1(L_v, E)_{p^m}$ contained in Lemma 1.7.

2. Derived p-adic heights.

2.1. Derived heights for cyclic groups. In this section we define a sequence of canonical pairings associated with finite cyclic p-extensions. The first pairing turns out to be equal, when restricted to the points, to the pairing of [Sc1] (adapted to finite extensions as in [T]) and of [MT1]: See §2.2. The successive pairings are each defined on the null-space of the previous. This generalizes results obtained in [BD] for cyclic extensions of prime degree. The notations are as follows. Let $L = K_n$ for some $n \geq 1$, and $G = \mathrm{Gal}(L/K) \simeq \mathbb{Z}/p^n\mathbb{Z}$. Fix any generator γ of G. Write Λ for the group ring $\mathbb{Z}/p^n\mathbb{Z}[G]$ and $I = (\gamma - 1)\Lambda$ for its augmentation ideal. (Note: The order of G is the same as the order of the ring of coefficients $\mathbb{Z}/p^n\mathbb{Z}$.) Given a Λ-module M, let

$$N : M \to M^G$$

denote the norm operator. We identify N with the element $\sum_{g\in G} g$ of Λ.

LEMMA 2.1. *There exist operators* $D^{(0)}, \ldots, D^{(p-1)} \in \Lambda$ *such that:*

(1) $D^{(0)} = N$;

(2) $(\gamma - 1)D^{(k)} = D^{(k-1)}$ *for* $1 \leq k \leq p - 1$.

In particular $(\gamma - 1)^k D^{(k)} = N$ *for* $0 \leq k \leq p - 1$.

Proof. Let

$$D^{(k)} := (-1)^k \gamma^{-k} \sum_{i=0}^{p^n-1} \binom{i}{k} \gamma^i.$$

The claim follows from a direct computation (cf. also [D], §3.1). □

LEMMA 2.2. *For* $0 \leq k \leq p - 1$, *the module* I^k/I^{k+1} *is isomorphic to* $\mathbb{Z}/p^n\mathbb{Z}$ *equipped with the trivial G-action.*

Proof. By induction on k, the case $k = 0$ being trivial. Let $1 \leq k \leq p - 1$. Consider the exact sequence

$$0 \to C_k \to I^{k-1}/I^k \xrightarrow{\gamma-1} I^k/I^{k+1} \to 0.$$

Given $\alpha \in C_k$, let x be any lift of α to I^{k-1}. Then there exists $y \in \Lambda$ such that

$$(\gamma - 1)x = (\gamma - 1)^{k+1} y,$$

i.e. $x = (\gamma - 1)^k y + z$, where $z \in \Lambda^G$. Since $\Lambda^G = N\Lambda$, there exists $w \in \Lambda$ such that $Nw = z$. By Lemma 2.1, we may write $N = (\gamma - 1)^k D^{(k)}$. Thus

$$x = (\gamma - 1)^k (y + D^{(k)} w).$$

We have proved that $C_k = 0$ for $1 \leq k \leq p - 1$. By the induction hypothesis, $I^{k-1}/I^k \simeq \mathbb{Z}/p^n\mathbb{Z}$. This proves Lemma 2.2. □

LEMMA 2.3. *Let M be a free* Λ*-module of finite rank. For* $0 \leq k \leq p - 1$, *we have* $\ker((\gamma - 1)^{k+1}) = D^{(k)}M$, *where we identify* $(\gamma - 1)^{k+1}$ *with the operator on M defined by left multiplication by* $(\gamma - 1)^{k+1}$.

Proof. We may reduce to prove the lemma for $M = \Lambda$. We reason by induction on k. Note that by Lemma 2.1

$$D^{(k)}\Lambda \subset \ker((\gamma - 1)^{k+1}).$$

We have the exact sequence

$$0 \to \ker((\gamma - 1)^{k+1}) \to \Lambda \xrightarrow{(\gamma-1)^{k+1}} I^{k+1} \to 0.$$

By Lemma 2.2, $I^{k+1} \simeq (\mathbb{Z}/p^n\mathbb{Z})^{p^n-k-1}$ as an abelian group. Thus

$$\ker((\gamma - 1)^{k+1}) \simeq (\mathbb{Z}/p^n\mathbb{Z})^{k+1}.$$

For $k = 0$, $D^{(0)}\Lambda = N\Lambda = \Lambda^G$ is isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$, hence the claim is true. In general, there is an exact sequence

$$0 \to \Omega_k \to D^{(k)}\Lambda \xrightarrow{(\gamma-1)} D^{(k-1)}\Lambda \to 0.$$

By the induction hypothesis, $D^{(k-1)}\Lambda \simeq (\mathbb{Z}/p^n\mathbb{Z})^k$. Since $\Lambda^G = N\Lambda \subset D^{(k)}\Lambda$ by Lemma 2.1, we deduce $\Omega_k = \Lambda^G$ and $D^{(k)}\Lambda \simeq (\mathbb{Z}/p^n\mathbb{Z})^{k+1}$. This concludes the proof of Lemma 2.3. □

COROLLARY 2.4. *Let M be a free Λ-module of finite rank. Given $x \in M^G$, assume that there exists $y \in M$ such that $(\gamma - 1)^k y = x$, with $0 \le k \le p - 1$. Then there exists $z \in M$ such that $D^{(k)}z = y$. In particular, $Nz = x$.*

Proof. y belongs to $\ker((\gamma - 1)^{k+1})$. □

COROLLARY 2.5. *Let M be a free Λ-module of finite rank. For $0 \le k \le p - 1$ we have $\ker D^{(k)} = I^{k+1}M$, where $D^{(k)}$ operates on M by left multiplication.*

Proof. We may assume $M = \Lambda$. By Lemma 2.1, $I^{k+1} \subset \ker D^{(k)}$. The exact sequence

$$0 \to D^{(k)}\Lambda \to \Lambda \xrightarrow{(\gamma-1)^{k+1}} I^{k+1} \to 0,$$

which is a consequence of Lemma 2.3, gives $\#(D^{(k)}\Lambda)\#(I^{k+1}) = \#(\Lambda)$. By combining this with the exact sequence

$$0 \to \ker D^{(k)} \to \Lambda \to D^{(k)}\Lambda \to 0,$$

we get $\#(\ker D^{(k)}) = \#(I^{k+1})$. The corollary follows. □

Recall the involution $* : \Lambda \to \Lambda$ defined on group-like elements by $g^* = g^{-1}$.

COROLLARY 2.6. *For $0 \le k \le p - 1$, $(D^{(k)})^* = uD^{(k)}$, where u is a unit of Λ.*

Proof. We have $(D^{(k)})^*\Lambda \subset \ker(\gamma - 1)^{k+1} = D^{(k)}\Lambda$, since $(\gamma - 1)^{k+1}D^{(k)} = 0$ implies $((\gamma - 1)^*)^{k+1}(D^{(k)})^* = 0$, and $(\gamma - 1)^* = -\gamma^{-1}(\gamma - 1)$. But $\#((D^{(k)})^*\Lambda) = \#(D^{(k)}\Lambda)$, since $*$ is an automorphism of Λ. Hence $(D^{(k)})^*\Lambda = D^{(k)}\Lambda$. The corollary follows. □

Let Sel := $\mathrm{Sel}_{p^n}(E/K)$. By Lemma 1.4 (applied to the empty set) the restriction map

$$\mathrm{Sel} \to \ Sel_{p^n}(E/L)^G$$

is an isomorphism. Hence we may abuse notation somewhat and identify Sel with its image in $\mathrm{Sel}_{p^n}(E/L)$ under restriction. We define a filtration on Sel

$$\mathrm{Sel} = \mathrm{Sel}^{(1)} \supset \mathrm{Sel}^{(2)} \supset \cdots \supset \mathrm{Sel}^{(k)} \supset \cdots$$

by letting

$$\begin{aligned}\mathrm{Sel}^{(k)} &:= \{s \in \mathrm{Sel} : \exists \tilde{s} \in \mathrm{Sel}_{p^n}(E/L) \ s.t.\ (\gamma - 1)^{k-1}\tilde{s} = s\} \\ &:= \mathrm{Sel} \cap (\gamma - 1)^{k-1}\mathrm{Sel}_{p^n}(E/L).\end{aligned}$$

Since the operator $\gamma - 1$ is nilpotent, $\mathrm{Sel}^{(k)} = 0$ for k sufficiently large.

THEOREM 2.7. *For $1 \le k \le p-1$, there exists a sequence of canonical pairings*

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

such that:

(1) $\langle s_1, s_2\rangle_k = (-1)^{k+1}\langle s_2, s_1\rangle_k$ *for all* $s_1, s_2 \in \mathrm{Sel}^{(k)}$,

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

(3) *the norm space* $\mathrm{cores}_{L/K}\mathrm{Sel}_{p^n}(E/L)$ *is contained in the null-space of all the pairings.*

Proof.

Definition of $\langle\ ,\ \rangle_k$. Let Σ be an admissible set for $(E, L/K, p^n)$. Let $X = X_\Sigma$, $Y = Y_\Sigma$ denote the free Λ-modules of Lemma 1.7 $\bigoplus_{v\in\Sigma} E(L_v)/p^nE(L_v)$ and $\mathrm{Sel}^{\Sigma}_{p^n}(E/L)$, respectively. Given $s_i \in \mathrm{Sel}^{(k)}$, $i = 1, 2$, let $\tilde{s}_i \in \mathrm{Sel}_{p^n}(E/L)$ be such that $(\gamma - 1)^{k-1}\tilde{s}_i = s_i$. Lemma 1.7, 2. allows us to view $\tilde{s}_1$, respectively $\tilde{s}_2$ as an element of X, respectively Y. By Corollary 2.4 we can find $x_1 \in X$, $y_2 \in Y$ such that

$$\begin{aligned} D^{(k-1)}x_1 &= \tilde{s}_1, \\ D^{(k-1)}y_2 &= \tilde{s}_2. \end{aligned}$$

In particular, $\mathrm{cores}_{L/K}x_1 = s_1$, $\mathrm{cores}_{L/K}y_2 = s_2$. Let

$$\langle\ ,\ \rangle : \bigoplus_{v\in\Sigma} H^1(L_v, E_{p^n}) \times \bigoplus_{v\in\Sigma} H^1(L_v, E_{p^n}) \longrightarrow \Lambda$$

be the Λ-valued pairing defined in §1.2. Recall that $\langle\ ,\ \rangle$ is Λ-linear in the first variable and $*$-linear in the second (Proposition 1.3, (1)). We have $\langle x_1, y_2\rangle \in I^k$. This follows from Corollary 2.5 (applied to $M = \Lambda$) and Corollary 2.6, as

$$\begin{aligned} (D^{(k-1)})^*\langle x_1, y_2\rangle &= \langle x_1, D^{(k-1)}y_2\rangle \\ &= \langle x_1, \tilde{s}_2\rangle = 0, \end{aligned}$$

where the last equality comes from Proposition 1.3, (4). We define

$$\langle s_1, s_2 \rangle_k := \langle x_1, y_2 \rangle \pmod{I^{k+1}}.$$

We have to check that $\langle\ ,\ \rangle_k$ is well-defined. To this end, let $x_1' \in X$ and $y_2' \in Y$ be such that

$$D^{(k-1)}x_1' = \tilde{s}_1', \qquad \mathrm{cores}_{L/K}x_1' = s_1,$$
$$D^{(k-1)}y_2' = \tilde{s}_2', \qquad \mathrm{cores}_{L/K}y_2' = s_2,$$

with $\tilde{s}_1'$ and $\tilde{s}_2'$ elements of $\mathrm{Sel}_{p^n}(E/L)$. Then,

$$\mathrm{cores}_{L/K}(x_1 - x_1') = 0, \ \mathrm{cores}_{L/K}(y_1 - y_1') = 0.$$

Since X and Y are free Λ-modules, there exist $\xi \in X$ and $\eta \in Y$ such that $x_1 - x_1' = (\gamma - 1)^*\xi$ and $y_1 - y_1' = (\gamma - 1)^*\eta$. It is enough to show that $\langle x_1 - x_1', y_2\rangle \in I^{k+1}$ and $\langle x_1, y_2 - y_2'\rangle \in I^{k+1}$. We have

$$\begin{aligned}(D^{(k)})^*\langle x_1 - x_1', y_2\rangle &= \langle \xi, (\gamma-1)D^{(k)}y_2\rangle \\ &= \langle \xi, \tilde{s}_2\rangle = 0\end{aligned}$$

by Proposition 1.3, (4), and

$$\begin{aligned}D^{(k)}\langle x_1, y_2 - y_2'\rangle &= \langle (\gamma-1)D^{(k)}x_1, \eta\rangle \\ &= \langle \tilde{s}_1, \eta\rangle = 0,\end{aligned}$$

the last equality being a consequence of 1.3, (5).

The pairing $\langle\ ,\ \rangle_k$ is also independent of the admissible set Σ. For, if Σ' is another admissible set, $\Sigma \cup \Sigma'$ is also admissible. The modules X_Σ and $X_{\Sigma'}$ inject into $X_{\Sigma\cup\Sigma'}$, and similarly for Y. Moreover, the restriction of the Λ-valued pairing on $\bigoplus_{v\in\Sigma\cup\Sigma'}H^1(L_v, E_{p^n})$ to $\bigoplus_{v\in\Sigma}H^1(L_v, E_{p^n})$ coincides with the Λ-valued pairing on $\bigoplus_{v\in\Sigma}H^1(L_v, E_{p^n})$. Thus, the above calculations also show that $\langle\ ,\ \rangle_k$ is independent of Σ. Finally, $\langle\ ,\ \rangle_k$ is visibly independent of the choice of the generator γ of G.

Proof of (1). Let $s_1, s_2 \in \mathrm{Sel}^{(k)}$. There are $\tilde{s}_1, \tilde{s}_2 \in \mathrm{Sel}_{p^n}(E/L)$ such that $(\gamma - 1)^{k-1}\tilde{s}_i = s_i$, $i = 1, 2$. As above, we can find $x_i \in X$, $y_i \in Y$ for $i = 1, 2$ such that

$$D^{(k-1)}x_i = \tilde{s}_i, \ \ D^{(k-1)}y_i = \tilde{s}_i.$$

Hence

$$D^{(k-1)}(x_i - y_i) = 0, \quad i = 1, 2.$$

By Lemma 1.7, $Z = \bigoplus_{v \in \Sigma} H^1(L_v, E_{p^n})$ is a free Λ-module and we can view X and Y as submodules of Z. Then, Corollary 2.5 implies the existence of $z_i \in Z$ such that

$$(\gamma - 1)^k z_i = x_i - y_i.$$

It follows from Corollary 2.5, applied to $M = \Lambda$, that $\langle x_1 - y_1, x_2 - y_2 \rangle$ belongs to I^{k+1}. By the isotropy of X and Y with respect to $\langle\ ,\ \rangle$ (Proposition 1.3) we find

$$\langle x_1, y_2 \rangle = -\langle y_1, x_2 \rangle \pmod{I^{k+1}}.$$

Since the involution $*$ acts as $(-1)^k$ on I^k/I^{k+1}, Proposition 1.3, (2) gives

$$\langle x_1, y_2 \rangle = (-1)^{k+1} \langle x_2, y_1 \rangle \pmod{I^{k+1}}.$$

In view of the definition of our pairings, this concludes the proof of 1.

Proof of (2). By induction on k. By (1), it is enough to prove that the right null-space of $\langle\ ,\ \rangle_k$ is equal to $\mathrm{Sel}^{(k+1)}$, for $1 \leq k \leq p-1$.

Case $k = 1$. Let s_2 be in the (right) null-space of $\langle\ ,\ \rangle_1$. Let $y_2 \in Y$ such that $\mathrm{cores}_{L/K} y_2 = s_2$. Then $\langle x_1, y_2 \rangle$ belongs to I^2 for all $x_1 \in X$ mapping by corestriction to Sel. By Corollary 2.5 and 2.6, we get

$$0 = (D^{(1)})^* \langle x_1, y_2 \rangle = \langle x_1, D^{(1)} y_2 \rangle.$$

Let β be the image of $D^{(1)} y_2$ in $\bigoplus_{v \in \Sigma} H^1(L_v, E)_{p^n}$ under the natural map. Since, by Lemma 2.1, $(\gamma - 1) D^{(1)} y_2 = s_2$, then β belongs to $(\bigoplus_{v \in \Sigma} H^1(L_v, E)_{p^n})^G = \bigoplus_{v \in \Sigma} H^1(K_v, E)_{p^n}$. By the compatibility formula (2) of §1.2.1 we find immediately

$$\langle x_1, D^{(1)} y_2 \rangle = -[s_1, \beta]_{K,p^n} \cdot N$$

for all s_1 in the Selmer group Sel, where $[\ ,\ ]_{K,p^n}$ is the local pairing introduced in §1.2.1 and $N = D^{(0)}$ denotes the norm operator. Hence $[s_1, \beta]_{K,p^n} = 0$ for all $s_1 \in \mathrm{Sel}$. By Proposition 1.2, there exists a global class α in $\mathrm{Sel}^{\Sigma}_{p^n}(E/K)$ mapping to β under the natural map. Thus, $D^{(1)} y_2 - \alpha$ belongs to $\mathrm{Sel}_{p^n}(E/L)$, and

$$(\gamma - 1)(D^{(1)} y_2 - \alpha) = (\gamma - 1) D^{(1)} y_2 = s_2.$$

In other words, s_2 belongs to $\mathrm{Sel}^{(2)}$, and this concludes the proof of the case $k = 1$.

Claim.

1. Let $y_2 \in Y$ be such that $D^{(k-1)}y_2$ belongs to $\mathrm{Sel}_{p^n}(E/L)$. Then y_2 induces a homomorphism ϕ in $\mathrm{Hom}(\mathrm{Sel}, I^k/I^{k+1})$ by the rule

$$\phi(s_1) = \langle x_1, y_2\rangle \pmod{I^{k+1}}$$

where, given $s_1 \in \mathrm{Sel}$, x_1 denotes any element of X such that $\mathrm{cores}_{L/K}x_1 = s_1$.

2. If the element $s_2 = \mathrm{cores}_{L/K}y_2 \in \mathrm{Sel}^{(k)}$ belongs to the right null-space of $\langle\ ,\ \rangle_k$, then we can view ϕ as a homomorphism in $\mathrm{Hom}(\mathrm{Sel}/\mathrm{Sel}^{(k)}, I^k/I^{k+1})$.

Proof of the Claim. $\langle x_1, y_2\rangle$ belongs to I^k. For, in view of Corollary 2.5,

$$(D^{(k-1)})^*\langle x_1, y_2\rangle = \langle x_1, D^{(k-1)}y_2\rangle = 0.$$

The last equality follows from Proposition 1.3, (5). Note that ϕ does not depend on the choice of x_1. For, given another $x_1' \in X$ such that $\mathrm{cores}_{L/K}x_1' = s_1$, by the freeness of X we can find $\xi \in X$ such that $x_1 - x_1' = (\gamma - 1)^*\xi$. Then

$$(D^{(k)})^*\langle x_1 - x_1', y_2\rangle = \langle \xi, D^{(k-1)}y_2\rangle = 0.$$

Hence $\langle x_1, y_2\rangle \equiv \langle x_1', y_2\rangle \pmod{I^{k+1}}$. Finally, if s_2 is in the null-space of $\langle\ ,\ \rangle_k$, then $\phi(\mathrm{Sel}^{(k)}) \subset I^{k+1}$. This concludes the proof of the claim.

Now let k be at least 2. By the induction hypothesis, for $1 \le i \le k-1$ the pairings $\langle\ ,\ \rangle_i$ induce identifications

$$\mathrm{Sel}^{(i)}/\mathrm{Sel}^{(i+1)} = \mathrm{Hom}(\mathrm{Sel}^{(i)}/\mathrm{Sel}^{(i+1)}, I^i/I^{i+1}).$$

By Lemma 2.2, multiplication by $(\gamma-1)^{k-i}$ identifies $\mathrm{Hom}(\mathrm{Sel}^{(i)}/\mathrm{Sel}^{(i+1)}, I^i/I^{i+1})$ with $\mathrm{Hom}(\mathrm{Sel}^{(i)}/\mathrm{Sel}^{(i+1)}, I^k/I^{k+1})$. Thus, we can find $y^{(1)}, \dots, y^{(k-1)}$ in Y such that:

(1) $\mathrm{cores}_{L/K}y^{(i)} = s^{(i)} \in \mathrm{Sel}^{(i)}$,

(2) $D^{(i-1)}y^{(i)} = \tilde{s}^{(i)} \in \mathrm{Sel}_{p^n}(E/L)$,

(3) $\langle x_1, y_2\rangle = \langle x_1, (\gamma-1)^{k-1}y^{(1)}\rangle + \cdots + \langle x_1, (\gamma-1)y^{(k-1)}\rangle \pmod{I^{k+1}}$ for all x_1 as above.

Let $y_2' = y_2 - (\gamma-1)^{k-1}y^{(1)} - \cdots - (\gamma-1)y^{(k-1)}$. By Lemma 2.1,

(i) $\mathrm{cores}_{L/K}y_2' = s_2$,

(ii) $D^{(k-1)}y_2' = D^{(k-1)}y_2 - \tilde{s}^{(1)} - \cdots - \tilde{s}^{(k-1)} \in \mathrm{Sel}_{p^n}(E/L)$.

By definition of y_2', $\langle x_1, y_2'\rangle = 0 \pmod{I^{k+1}}$ for all $x_1 \in X$ such that $\mathrm{cores}_{L/K}x_1$ belongs to Sel. Hence, by Corollary 2.5 and 2.6,

$$0 = (D^{(k)})^*\langle x_1, y_2'\rangle = \langle x_1, D^{(k)}y_2'\rangle.$$

Let β be the image of $D^{(k)}y_2'$ in $\bigoplus_{v\in\Sigma}H^1(L_v,E)_{p^n}$ under the natural map. Since $(\gamma-1)D^{(k)}y_2'=D^{(k-1)}y_2'$ belongs to $\mathrm{Sel}_{p^n}(E/L)$, then β belongs to

$$\Big(\bigoplus_{v\in\Sigma}H^1(L_v,E)_{p^n}\Big)^G=\bigoplus_{v\in\Sigma}H^1(K_v,E)_{p^n}.$$

By formula (2) of §1.2.1, we find $\langle x_1,D^{(k)}y_2'\rangle=-[s_1,\beta]_{K,p^n}\cdot N$ for all s_1 in the Selmer group Sel. It follows

$$[s_1,\beta]_{K,p^n}=0$$

for all s_1 in Sel. Then, by Proposition 1.2 there exists $\alpha\in\mathrm{Sel}_{p^n}^{\Sigma}(E/K)$ mapping to β under the natural map. Hence $D^{(k)}y_2'-\alpha$ belongs to $\mathrm{Sel}_{p^n}(E/L)$. Moreover,

$$(\gamma-1)^k(D^{(k)}y_2'-\alpha)=s_2,$$

i.e. s_2 belongs to $\mathrm{Sel}^{(k+1)}$. This concludes the proof of (2).

Proof of (3). It follows from the factorization in Λ of $\mathrm{cores}_{L/K}$ as $(\gamma-1)^kD^{(k)}$ for $1\le k\le p-1$ (Lemma 2.1).

2.2. Comparison of pairings. We keep the notations of §2.1. The first pairing of Theorem 2.7 induces on points a pairing

$$E(K)\times E(K)\to I/I^2,$$

which, by an abuse of notation, we still denote by $\langle\ ,\ \rangle_1$. We show that it is equal to the "analytic" height pairings of Schneider [Sc1] (as formulated by K.-S. Tan [T] for finite extensions) and of [MT1].

For the convenience of the reader, we recall the definition of $\langle\ ,\ \rangle_1$. Fix an admissible set Σ for $(E,L/K,p^n)$, and denote by X, respectively Y the free Λ-modules $\bigoplus_{v\in\Sigma}E(L_v)/p^nE(L_v)$, respectively $\mathrm{Sel}_{p^n}^{\Sigma}(E/L)$. Given P, respectively Q in $E(K)$, we write $\bar a$, respectively $\bar b$ for its image in X^G, respectively Y^G. Choose $a\in X$, $b\in Y$ such that $\mathrm{cores}_{L/K}(a)=\bar a$, $\mathrm{cores}_{L/K}(b)=\bar b$. Recall the Λ-valued pairing $\langle\ ,\ \rangle$ of §1.2.1. The element $\langle a,b\rangle$ belongs to I. Equivalently by Lemma 2.5, $D^{(0)}\langle a,b\rangle=0$. But $D^{(0)}\langle a,b\rangle=\langle a,\bar b\rangle$, and this is zero by Proposition 1.3, (4). The image of $\langle a,b\rangle$ in I/I^2 depends only on P and Q: This is proved, in greater generality, in the course of constructing the pairings $\langle\ ,\ \rangle_k$ in the proof of Theorem 2.7. By definition

$$\langle P,Q\rangle_1:=\langle a,b\rangle\ (\mathrm{mod}\ I^2).$$

In [T] an "algebraic" definition of height is introduced, and shown to be equal to the analytic pairings of Mazur-Tate and Schneider. Hence it suffices to show that $\langle\ ,\ \rangle_1$ is equal to the algebraic pairing of [T], whose definition we now recall.

Tan defines a homomorphism

$$\Phi_{L/K} : E(K) \otimes E(K) \otimes \mathrm{Hom}(G, \mathbb{Z}/p^n\mathbb{Z}) \to \mathbb{Z}/p^n\mathbb{Z}$$

as follows. Let $P, Q \in E(K) = H^0(G, E(L))$, and $\psi \in \mathrm{Hom}(G, \mathbb{Z}/p^n\mathbb{Z}) = H^2(G, \mathbb{Z})$. The cup product of P and ψ gives an element $P \cup \psi \in H^2(G, E(L))$. We have $H^2(K, E) = 0$ by [Mi], Corollary I.6.24, p.111, since p is odd. Then the Hochschild-Serre spectral sequence defines a surjective homomorphism (transgression)

$$H^1(L, E)^G \xrightarrow{trg} H^2(G, E(L)) \to 0.$$

Let $\gamma \in H^1(L, E)^G$ be such that $trg(\gamma) = P \cup \psi$. For all v, since restriction induces an isomorphism $H^1(K_v, E) \simeq H^1(L_v, E)^G$ (see the proof of Lemma 1.4), there exists $\alpha_v \in H^1(K_v, E)$ which maps in $H^1(L_v, E)^G$ to the localization at v of γ. Let $[\ \ ,\ \ ]_{K_v,p^n} : E(K_v)/p^nE(K_v) \times H^1(K_v, E)_{p^n} \to \mathbb{Z}/p^n\mathbb{Z}$ denote the local Tate duality of §1.2.1. Define

$$\Phi_{L/K}(P \otimes Q \otimes \psi) = \sum_v [Q_v, \alpha_v]_{K_v,p^n}.$$

One can check that this is independent of the choices made. Identify I/I^2 with G and G with its bi-dual, in the usual way. Then $\Phi_{L/K}$ defines a pairing

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

THEOREM 2.8. *We have $\langle P, Q\rangle_1 = \langle P, Q\rangle_{KS}$ for all $P, Q \in E(K)$.*

Proof. By definition

$$\begin{aligned}
\langle P, Q\rangle_1 &= \sum_{i=0}^{p^n-1} \langle a, b^{\gamma^{-i}}\rangle_{L,p^n} \cdot \gamma^i \pmod{I^2} \\
&= -\sum_{i=0}^{p^n-1} \langle a, b^{\gamma^i}\rangle_{L,p^n} \cdot i(\gamma - 1) \pmod{I^2} \\
&= \langle a, D^{(1)}b\rangle_{L,p^n} \cdot (\gamma - 1) \pmod{I^2}\ ,
\end{aligned}$$

where $\langle\ ,\ \rangle_{L,p^n}$ denotes the local pairing of §1.2.1, a and b are chosen as above and $D^{(1)} = -\sum_{i=0}^{p^n-1} i\gamma^i$ is the derivative operator of Lemma 2.1. Let η be the image of $D^{(1)}b$ in $H^1(L, E)$. Since $(\gamma - 1)D^{(1)} = D^{(0)}$ is the norm operator, η belongs to $H^1(L, E)^G$. Let $\psi \in \mathrm{Hom}(G, \mathbb{Z}/p^n\mathbb{Z})$ be the homomorphism such that $\psi(\gamma) = 1 \pmod{p^n\mathbb{Z}}$.

LEMMA 2.9. *We have* $trg(\eta) = Q \cup \psi$.

Clearly $\langle a, D^{(1)}b\rangle_{L,p^n} = \sum_v [P_v, \eta_v]_{K_v,p^n}$, where $\eta_v \in H^1(K_v, E)$ corresponds to the localization of η under the isomorphism $H^1(K_v, E) \simeq H^1(L_v, E)^G$. Then, in view of the definition of the height pairings, Lemma 2.9 implies that $\langle P, Q\rangle_1 = \langle Q, P\rangle_{KS}$ for all $P, Q \in E(K)$. Theorem 2.8 follows from the symmetry of $\langle\ ,\ \rangle_1$ (Theorem 2.7, (1)). □

Proof of Lemma 2.9. We make use of the explicit formula for computing the transgression homomorphism on cocycles given in [T], proof of Lemma 3.2. Let $G_K = \mathrm{Gal}(\bar{K}/K)$, $G_L = \mathrm{Gal}(\bar{K}/L)$. Let $f : G_L \longrightarrow E(\bar{K})$ be a 1-cocycle representing η. Then

$$\tau f(\tau^{-1}\sigma\tau) - f(\sigma) = \sigma l(\tau) - l(\tau) \qquad \forall\sigma \in G_L,\ \forall\tau \in G_K,$$

for some $l(\tau) \in E(\bar{K})$. The point $l(\tau)$ is determined modulo elements in $E(L)$. Fix $R \in E(\bar{K})$ such that $p^nR = Q$. It is easy to see that we can choose $l(\tau) = iR + e(\tau)$, where $e(\tau) \in E_{p^n}$ and $0 \le i \le p^n - 1$ is an integer such that τ maps to γ^i in G. With this choice of $l(\tau)$ we have

(1) $l(\sigma) = f(\sigma)$ for all $\sigma \in G_L$,

(2) $l(\tau\sigma) = l(\tau) + \tau l(\sigma)$ for all $\sigma \in G_L$, $\tau \in G_K$.

This follows from an explicit computation, observing that $E_{p^n}(L) = 0$ by assumption 3 of §1.1. Then a well-defined 2-cocycle $g : G \times G \longrightarrow E(L)$ representing $tr(\eta)$ is given by the formula

$$g(\gamma^{i_1}, \gamma^{i_2}) = l(\tau_1) + \tau_1 l(\tau_2) - l(\tau_1\tau_2) \qquad 0 \le i_1, i_2 \le p^n - 1,$$

where τ_j, $j = 1, 2$ is chosen so that it maps in G to γ^{i_j}. We find

$$g(\gamma^{i_1}, \gamma^{i_2}) = \begin{cases} 0 & \text{for } i_1 + i_2 \le p^n - 1 \\ Q & \text{for } i_1 + i_2 > p^n - 1. \end{cases}$$

But this is precisely a representative for $Q \cup \psi$, as one can see by describing explicitly on cochains the cup product ([CF], pp.106-7) and the identification via coboundary $\mathrm{Hom}(G, \mathbb{Z}/p^n\mathbb{Z}) = H^2(G, \mathbb{Z})$. This concludes the proof of Lemma 2.9. □

Remark 2.10. The definition of the pairings $\langle\ ,\ \rangle_1$ and $\langle\ ,\ \rangle_{KS}$ works equally well when L/K is a finite abelian p-extension, not necessarily cyclic. The two pairings still coincide in this more general setting, as a consequence of their norm-compatibility (combined with Theorem 2.8). More precisely, given a tower $K \subset L_1 \subset L$, write $\nu : I/I^2 \longrightarrow I_1/I_1^2$ for the natural projection, I_1 being the augmentation ideal of $\mathbb{Z}/p^n\mathbb{Z}[\mathrm{Gal}(L_1/K)]$. Then a computation gives the identities

(where we use the obvious notations)

(1) $\nu(\langle P, Q\rangle_{1,L/K}) = \langle P, Q\rangle_{1,L_1/K}$ for all $P, Q \in E(K)$,

(2) $\nu(\langle P, Q\rangle_{KS,L/K}) = \langle P, Q\rangle_{KS,L_1/K}$ for all $P, Q \in E(K)$.

2.3. Compatibility of the derived heights. We shall define the p-adic derived heights by compiling the derived heights corresponding to the finite layers of the $\mathbb{Z}_p$-extension K_∞/K. To do this, we need to study the compatibility of the derived heights for finite cyclic groups under change of extension, and this is the goal of this section.

Recall that K_n denotes the subextension of K_∞/K of degree p^n. Write G_n for the Galois group $\mathrm{Gal}\,(K_n/K)$, Λ_n for the group ring $\mathbb{Z}/p^n\mathbb{Z}[G_n]$, and I_n for its augmentation ideal. Let $\mathrm{Sel}_n := \mathrm{Sel}_{p^n}(E/K)$. Let

$$\mathrm{Sel}_n = \mathrm{Sel}_n^{(1)} \supset \mathrm{Sel}_n^{(2)} \supset \cdots \supset \mathrm{Sel}_n^{(k)} \supset \cdots$$

denote the filtration of Sel_n defined by

$$\begin{aligned} \mathrm{Sel}_n^{(k)} \ : &= \{s \in \mathrm{Sel}_n : \exists \tilde{s} \in \mathrm{Sel}_{p^n}(E/K_n) \ s.t. \ (\gamma_n - 1)^{k-1}\tilde{s} = s\} \\ : &= \mathrm{Sel}_{p^n}(E/K) \cap (\gamma_n - 1)^{k-1}\mathrm{Sel}_{p^n}(E/K_n). \end{aligned}$$

Let

$$\langle\ ,\ \rangle_{k,n} : \mathrm{Sel}_n^{(k)} \times \mathrm{Sel}_n^{(k)} \longrightarrow I_n^k/I_n^{k+1}$$

be the derived height pairings defined in §2.1. By abuse of notation we shall write m_p for any map induced in cohomology by $E_{p^{n+1}} \xrightarrow{p} E_{p^n}$. In particular, we have a map

$$m_p : \mathrm{Sel}_{n+1} \longrightarrow \mathrm{Sel}_n.$$

Since $E_p(K) = 0$ by our assumptions, Sel_n injects into Sel_{n+1} under the natural map, and m_p is induced by the multiplication by p on Sel_{n+1}. The next proposition contains the compatibility result we need. Let

$$\nu_n : \Lambda_{n+1} \longrightarrow \Lambda_n$$

denote the natural projection of group rings, and also, by abusing notation, the induced map $I_{n+1}^k/I_{n+1}^{k+1} \longrightarrow I_n^k/I_n^{k+1}$ for any k.

PROPOSITION 2.11.

(1) *For $1 \leq k \leq p$, the map m_p respects the filtrations on* Sel_{n+1} *and* Sel_n, *i.e.* $m_p(\mathrm{Sel}_{n+1}^{(k)}) \subset \mathrm{Sel}_n^{(k)}$.

(2) *For* $1 \leq k \leq p-1$, *we have*

$$\nu_n \langle s_1, s_2 \rangle_{k,n+1} = \langle m_p s_1, m_p s_2 \rangle_{k,n}$$

for all s_1, s_2 *in* $\mathrm{Sel}_{n+1}^{(k)}$.

Proof of Part 1. Fix any topological generator γ of $\mathrm{Gal}(K_\infty/K)$, and let γ_n be the generator of $\mathrm{Gal}(K_n/K)$ corresponding to γ under the natural projection. Denote by

$$D_n^{(k)} \in \Lambda_n, \ 0 \leq k \leq p-1\text{-}$$

the operators defined in the proof of Lemma 2.1 (with γ_n replacing γ). Write

$$\begin{aligned} q_n &: \mathbb{Z}/p^{n+1}[G_{n+1}] \to \mathbb{Z}/p^{n+1}\mathbb{Z}[G_n], \\ \pi_n &: \mathbb{Z}/p^{n+1}\mathbb{Z}[G_n] \to \mathbb{Z}/p^n\mathbb{Z}[G_n] \end{aligned}$$

for the natural projections. Thus their composite $\pi_n q_n$ is equal to ν_n.

LEMMA 2.12. *For* $0 \leq k \leq p-1$ *there exists* $\mathcal{D}_n^{(k)} \in \mathbb{Z}/p^{n+1}\mathbb{Z}[G_n]$ *such that:*

(1) $q_n D_{n+1}^{(k)} = p\mathcal{D}_n^{(k)}$,

(2) $\pi_n \mathcal{D}_n^{(k)} = D_n^{(k)}$.

Proof. By definition of $D_n^{(k)}$, we reduce to show that for all $0 \leq i \leq p^n - 1$ the equality

$$\sum_{j=0}^{p-1} \binom{i + jp^n}{k} = p\binom{i}{k}, \quad 0 \leq k \leq p-1$$

holds in $\mathbb{Z}/p^{n+1}\mathbb{Z}$. This follows from an easy induction argument. □

We conclude the proof of Part 1.

Let $s \in \mathrm{Sel}_{n+1}^{(k)}$. Let Σ be an admissible set for $(E, K_{n+1}/K, p^{n+1})$. Then by the results of §2.1 there exists $y \in \mathrm{Sel}_{p^{n+1}}^{\Sigma}(E/K_{n+1})$ such that

$$(1) \qquad D_{n+1}^{(k-1)} y := \tilde{s} \in \mathrm{Sel}_{p^{n+1}}(E/K_{n+1}), \quad (\gamma_{n+1} - 1)^{k-1}\tilde{s} = s.$$

Then

$$\begin{aligned} m_p s &= m_p(\mathrm{cores}_{K_{n+1}/K} y) \\ &= \mathrm{cores}_{K_n/K}(m_p \mathrm{cores}_{K_{n+1}/K_n} y) \\ &= (\gamma_n - 1)^{k-1} D_n^{(k-1)}(m_p \mathrm{cores}_{K_{n+1}/K_n} y). \end{aligned}$$

Let $y' := m_p \mathrm{cores}_{K_{n+1}/K_n} y$. We claim that

$$D_n^{(k-1)} y' \in \mathrm{Sel}_{p^n}(E/K_n).$$

For, $D_n^{(k-1)} y' \in \mathrm{Sel}^{\Sigma}_{p^n}(E/K_n)$ since $y' \in \mathrm{Sel}^{\Sigma}_{p^{n+1}}(E/K_n)[p^n] = \mathrm{Sel}^{\Sigma}_{p^n}(E/K_n)$, where the equality follows, for example, from Proposition 1.8 and $E_p(K_n) = 0$. Moreover, by Lemma 2.12

$$\begin{aligned} D_n^{(k-1)} y' &= p\mathcal{D}_n^{(k-1)} \mathrm{cores}_{K_{n+1}/K_n} y \\ &= D_{n+1}^{(k-1)} \mathrm{cores}_{K_{n+1}/K_n} y \\ &= \mathrm{cores}_{K_{n+1}/K_n} D_{n+1}^{(k-1)} y \\ &= \mathrm{cores}_{K_{n+1}/K_n} \tilde{s} \in \mathrm{Sel}_{p^{n+1}}(E/K_n). \end{aligned}$$

Thus, $D_n^{(k-1)} y' \in \mathrm{Sel}_{p^{n+1}}(E/K_n) \cap \mathrm{Sel}^{\Sigma}_{p^n}(E/K_n) = \mathrm{Sel}_{p^n}(E/K_n)$. We find

$$\text{(2)} \qquad D_n^{(k-1)} y' := \tilde{s}' \in \mathrm{Sel}_{p^n}(E/K_n), \quad (\gamma_n - 1)^{k-1} \tilde{s}' = m_p s.$$

In particular, $m_p s$ belongs to $\mathrm{Sel}_n^{(k)}$, as was to be shown.

Proof of Part 2. We begin with a couple of lemmas.

LEMMA 2.13. *Let F be a local field. Let $p_n : \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ be the canonical projection. Then for all x, y in $H^1(F, E_{p^{n+1}})$, the local Tate pairing satifies*

$$p_n(\langle x, y\rangle_{F,p^{n+1}}) = \langle m_p x, m_p y\rangle_{F,p^n}.$$

Proof. Recall that the local Tate pairing is defined by composing the cup product with the Weil pairing $w_n : E_{p^n} \otimes E_{p^n} \to \mu_{p^n}$. The Lemma follows from the explicit definition of the cup product on cocycles ([CF], pp.106-7) combined with the relation $w_{n+1}(\xi \otimes \eta)^p = w_n(p\xi \otimes p\eta)$ for all $\xi, \eta \in E_{p^{n+1}}$. □

Given an admissible set Σ for $(E, K_n/K, p^n)$ we let

$$\langle\ ,\ \rangle_{(n)} : \bigoplus\nolimits_{v\in\Sigma} H^1((K_n)_v, E_{p^n}) \times \bigoplus\nolimits_{v\in\Sigma} H^1((K_n)_v, E_{p^n}) \to \Lambda_n$$

denote the nondegenerate pairing defined in §1.2.1.

LEMMA 2.14. *Let Σ be an admissible set for $(E, K_{n+1}/K, p^{n+1})$. For all $x, y \in \bigoplus_{v\in\Sigma} H^1((K_{n+1})_v, E_{p^{n+1}})$ we have*

$$\nu_n\langle x, y\rangle_{(n+1)} = \langle m_p(\mathrm{cores}_{K_{n+1}/K_n} x), m_p(\mathrm{cores}_{K_{n+1}/K_n} y)\rangle_{(n)}\,.$$

Proof. Note that Σ is also admissible for $(E, K_n/K, p^{n+1})$ and for $(E, K_n/K, p^n)$. The formulae (1) and (2) of §1.2.1 and Lemma 2.13 give

$$\begin{aligned}\nu_n\langle x, y\rangle_{(n+1)} &= \sum_{\sigma\in G_n} \pi_n\langle x, (\mathrm{cores}_{K_{n+1}/K_n} y)^\sigma\rangle_{K_{n+1},p^{n+1}} \cdot \sigma^{-1} \\ &= \sum_{\sigma\in G_n} \pi_n\langle \mathrm{cores}_{K_{n+1}/K_n} x, (\mathrm{cores}_{K_{n+1}/K_n} y)^\sigma\rangle_{K_n,p^{n+1}} \cdot \sigma^{-1} \\ &= \langle m_p(\mathrm{cores}_{K_{n+1}/K_n} x), m_p(\mathrm{cores}_{K_{n+1}/K_n} y)\rangle_{(n)}. \qquad \Box\end{aligned}$$

We conclude the proof of Part 2.

Let Σ be an admissible set for $(E, K_{n+1}/K, p^{n+1})$. Let $s \in \mathrm{Sel}_{n+1}^{(k)}$. Then there exists x belonging to $\bigoplus_{v\in\Sigma} E((K_{n+1})_v)/p^{n+1}E((K_{n+1})_v)$ such that

$$(3) \qquad D_{n+1}^{(k-1)} x := \tilde{s} \in \mathrm{Sel}_{p^{n+1}}(E/K_{n+1}), \quad (\gamma_{n+1} - 1)^{k-1}\tilde{s} = s.$$

Let $x' := m_p \mathrm{cores}_{K_{n+1}/K_n} x$. With the formal argument of the proof of Part 1, we can show that

$$(4) \qquad D_n^{(k-1)} x' := \tilde{s}' \in \mathrm{Sel}_{p^n}(E/K_n), \quad (\gamma_n - 1)^{k-1}\tilde{s}' = m_p s.$$

In view of the definition of our pairings (Theorem 2.7), the claim follows from Lemma 2.14 and the equations (1)–(4). □

2.4. Derived p-adic heights. By Proposition 2.11, we may compile the pairings $\langle\ ,\ \rangle_{k,n}$ via the maps m_p, in order to define pairings on the inverse limit of the modules $\mathrm{Sel}_n^{(k)}$. We may use Theorem 2.7 to obtain the properties of these new pairings, once we know that the modules $\mathrm{Sel}_n^{(k)}$ can be recovered from their inverse limit in the natural way. This is proved in Proposition 2.17, after a few preliminary definitions. The properties of the p-adic pairings we construct are summarized in Theorem 2.18.

Definition 2.15.

1. We define the *pro-p Selmer group* of E/K_n to be

$$S_p(E/K_n) := \varprojlim_m \mathrm{Sel}_{p^m}(E/K_n),$$

where the inverse limit is with respect to the maps m_p.

2. In view of Proposition 2.11, we define a filtration on $S_p(E/K)$

$$S_p(E/K) = S_p^{(1)} \supset S_p^{(2)} \supset \cdots \supset S_p^{(p-1)} \supset S_p^{(p)}$$

by letting $S_p^{(k)} := \lim_{\overleftarrow{n}} \mathrm{Sel}_n^{(k)}$, the limit being taken by means of the maps m_p.

Since $E_p(K_n) = 0$ by our assumptions, we have that $E(K_n)_p$ is equal to $E(K_n) \otimes \mathbb{Z}_p$, and it injects into $S_p(E/K_n)$. They coincide if and only if the p-primary part $\text{Ш}(E/K_n)_{p^\infty}$ of the Shafarevich-Tate group of E/K_n is finite.

Given $s = (s_n)_{n \geq 1}, t = (t_n)_{n \geq 1} \in S_p^{(k)}$ with $1 \leq k \leq p-1$, Proposition 2.11 allows us to define canonical pairings

$$\langle \ , \ \rangle_k : S_p^{(k)} \times S_p^{(k)} \longrightarrow I^k / I^{k+1}$$

by the rule

$$\langle s, t \rangle_k = (\langle s_n, t_n \rangle_{k,n})_{n \geq 1}.$$

Definition 2.16. Let $N \subset M$ be an inclusion of free $\mathbb{Z}_p$-modules of finite rank. Define the *p-adic saturation* $Sat_M(N)$ of N in M to be the maximal submodule of M containing N with finite index.

The theory of elementary divisors guarantees the existence of $Sat_M(N)$. To ease notations, we shall often write $\bar{N}$ instead of $Sat_M(N)$. In particular, we write $\bar{S}_p^{(k)}$ for $Sat_{S_p^{(1)}}(S_p^{(k)})$, $1 \leq k \leq p$. Thus $\bar{S}_p^{(1)} = S_p^{(1)}$. Let

$$US_p(E/K) := \bigcap_{n \geq 1} \text{cores}_{K_n/K}(S_p(E/K_n))$$

denote the universal norm submodule of $S_p(E/K)$.

The next proposition is the key to relate the p-adic pairings $\langle \ , \ \rangle_k$ to the pairings for the finite layers of K_∞/K.

PROPOSITION 2.17. *For $1 \leq k \leq p$ the cokernel of the natural map $S_p^{(k)} \longrightarrow \text{Sel}_n^{(k)}$ is bounded independently of n.*

Proof. By induction on k. For $k = 1$, the cokernel in Sel_n is

$$(\text{Ш}(E/K)/\text{Div}\,(\text{Ш}(E/K)))[p^n],$$

where Div is the functor which to every abelian group associates its divisible part. Assume that $S_p^{(k)} \longrightarrow \text{Sel}_n^{(k)}$ has a cokernel whose order is bounded independently of n. Choosing an identification of I^k/I^{k+1} with $\mathbb{Z}_p$, we may view the pairing $\langle \ , \ \rangle_k$ as taking values in $\mathbb{Z}_p$. By the structure theory of pairings over $\mathbb{Q}_p$, there is a finite index submodule $T_p^{(k)}$ of $S_p^{(k)}$ such that the pairing $\langle \ , \ \rangle_k$ restricted to

$T_p^{(k)}$ has the form

$$\begin{pmatrix} p^{a_1}J & & & & \\ & \ddots & & & \\ & & p^{a_s}J & & \\ & & & \ddots & \\ & & & & 0 \end{pmatrix},$$

relative to a basis $e_1, \dots, e_s, e_{s+1}, \cdots, e_r$, (respectively $e_1, e_1', \dots, e_s, e_s', e_{s+1}, \dots, e_r$), where $J = (1)$ (respectively $J = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$) if $\langle\ ,\ \rangle_k$ is symmetric, i.e., k is odd (respectively $\langle\ ,\ \rangle_k$ is alternating, i.e. k is even). Let x be an element of $\mathrm{Sel}_n^{(k+1)}$. By the induction hypothesis, the cokernel of the natural map $T_p^{(k)} \longrightarrow \mathrm{Sel}_n^{(k)}$ is bounded independently of n, by p^A, say. Then $y = p^A x$ belongs to the image of $T_p^{(k)}$. We have

$$\langle y, \xi \rangle_{k,n} = 0$$

for all ξ in $\mathrm{Sel}_n^{(k)}$, hence for all ξ in the image of $T_p^{(k)}$. Let $\tilde{y}$ be any element of $T_p^{(k)}$ mapping to y, so that, by definition of $\langle\ ,\ \rangle_k$,

$$\langle \tilde{y}, \xi \rangle_k \equiv 0 \bmod p^n$$

for all ξ in $T_p^{(k)}$. This implies that $\tilde{y}$ is of the form

$$\tilde{y} = \lambda_1 p^{n-a_1} e_1 + \cdots + \lambda_s p^{n-a_s} e_s + \lambda_{s+1} e_{s+1} + \cdots + \lambda_r e_r$$

if k is odd, or

$$\tilde{y} = \lambda_1 p^{n-a_1} e_1 + \gamma_1 p^{n-a_1} e_1' + \cdots + \lambda_s p^{n-a_s} e_s + \gamma_s p^{n-a_s} e_s' + \lambda_{s+1} e_{s+1} + \cdots + \lambda_r e_r,$$

where λ_i and γ_i are scalars in $\mathbb{Z}_p$. Let B denote the maximum of the a_i. Write

$$\tilde{z} = p^B(\lambda_{s+1} e_{s+1} + \cdots + \lambda_r e_r).$$

Since $\tilde{z}$ is in the null-space of $\langle\ ,\ \rangle_k$ resricted to $T_p^{(k)}$, it follows that $p^A \tilde{z}$ belongs to the null-space of $\langle\ ,\ \rangle_k$. Hence $p^{A+B}\tilde{z}$ belongs to $S_p^{(k+1)}$. On the other hand, letting z be the image of $\tilde{z}$ in $\mathrm{Sel}_n^{(k+1)}$, we have $z = p^{A+B} x$. Hence $p^{2A+2B} x$ belongs to the image of $S_p^{(k+1)}$. Since A and B do not depend on n, this proves the claim. □

THEOREM 2.18. *For $1 \leq k \leq p-1$, there exists a sequence of canonical pairings*

$$\langle\langle\ ,\ \rangle\rangle_k : \bar{S}_p^{(k)} \times \bar{S}_p^{(k)} \to I^k/I^{k+1} \otimes \mathbb{Q}$$

such that:

(1) $\langle\langle s_1, s_2\rangle\rangle_k = (-1)^{k+1}\langle\langle s_2, s_1\rangle\rangle_k \ \forall s_1, s_2 \in \bar{S}_p^{(k)}$,

(2) $\bar{S}_p^{(k+1)}$ *is the null-space of* $\langle\langle\ ,\ \rangle\rangle_k$,

(3) $US_p(E/K)$ *is contained in the null-space of all the pairings,*

(4) *the restriction of* $\langle\langle\ ,\ \rangle\rangle_1$ *to* $E(K)_p$ *is equal to the p-adic height relative to* $(E, K_\infty/K)$ *(as defined in* [MT1] *or* [Sc1]*),*

(5) $p^{A_k}\langle\langle\ ,\ \rangle\rangle_k$ *takes values in* I^k/I^{k+1}, *where* p^{A_k} *denotes the exponent of the finite group* $\bar{S}_p^{(k)}/S_p^{(k)}$.

Proof. Define $\langle\langle\ ,\ \rangle\rangle_k$ by extending $\langle\ ,\ \rangle_k$ to $\bar{S}_p^{(k)}$ in the natural way.

(1) It follows directly from Theorem 2.7.

(2) Observe that $\bar{S}_p^{(k+1)}$ is contained in the null-space of $\langle\langle\ ,\ \rangle\rangle_k$. As for the reverse inclusion, let y be in the null-space of $\langle\langle\ ,\ \rangle\rangle_k$. Then there exists $A \geq 0$ such that $p^A y$ belongs to the null-space of $\langle\ ,\ \rangle_k$. By Proposition 2.17, there exists $B \geq 0$ such that $p^{A+B}y$ maps to $\mathrm{Sel}_n^{(k+1)}$ for all n, and hence $p^{A+B}y$ belongs to $S_p^{(k+1)}$. This proves (2).

(3) By Theorem 2.7, (3), it suffices to observe that $US_p(E/K)$ is contained in

$$\varprojlim_n (\mathrm{cores}_{K_n/K}\mathrm{Sel}_{p^n}(E/K_n)),$$

where the limit is taken with respect to the maps m_p.

(4) The homomorphisms $\Phi_{K_n/K}$ of §2.2 satisfy the compatibility relation [T]

$$p_m^n \Phi_{K_n/K}(P \otimes Q \otimes \psi) = \Phi_{K_m/K}(P \otimes Q \otimes p_m^n \psi),$$

where, for $n \geq m$, $p_m^n : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ denotes the canonical projection and, given any homomorphism ψ in $\mathrm{Hom}(\mathrm{Gal}(K_n/K), \mathbb{Z}/p^n\mathbb{Z})$, $p_m^n\psi$ is viewed as a homomorphism in $\mathrm{Hom}(\mathrm{Gal}(K_m/K), \mathbb{Z}/p^m\mathbb{Z})$. Tan defines a p-adic height pairing by means of the homomorphism

$$\Phi_{K_\infty/K} = \varprojlim_n \Phi_{K_n/K} : E(K)_p \otimes E(K)_p \otimes \mathrm{Hom}(\Gamma, \mathbb{Z}_p) \to \mathbb{Z}_p,$$

where the tensor products and the homomorphisms are are of $\mathbb{Z}_p$-modules. He shows that this coincides with the p-adic height of Mazur-Tate and Schneider. Statement (4) follows from Theorem 2.8 and the definition of $\langle\langle\ ,\ \rangle\rangle_1$.

(5) We have $\langle\!\langle s,t\rangle\!\rangle_k = p^{-2A_k}\langle p^{A_k}s, p^{A_k}t\rangle_k$ for all $s,t \in \bar{S}_p^{(k)}$. Let $s = (s_n), t = (t_n)$. It is enough to show that $\langle p^{A_k}s_n, p^{A_k}t_n\rangle_{k,n}$ belongs to $p^{A_k}(I_n^k/I_n^{k+1})$ for all n. By the claim in the proof of Theorem 2.7, (2) there exists a homomorphism $\phi : \mathrm{Sel}_n \to I_n^k/I_n^{k+1}$ such that

$$\langle p^{A_k}s_n, p^{A_k}t_n\rangle_{k,n} = \phi(p^{A_k}s_n) = p^{A_k}\phi(s_n).$$

This proves (5). □

Definition 2.19. We call the canonical pairing $\langle\!\langle\ ,\ \rangle\!\rangle_k$ of Theorem 2.18 the *k-th derived p-adic height pairing.*

It is possible to use the derived heights to generalize the notion of p-adic regulator. Choose a basis $s_1,\dots,s_r$ for the free $\mathbb{Z}_p$-module $S_p(E/K)$ compatible with the filtration

$$S_p(E/K) = \bar{S}_p^{(1)} \supset \bar{S}_p^{(2)} \supset \cdots \supset \bar{S}_p^{(p)}.$$

This is possible because, by definition of p-adic saturation, the successive quotients $\bar{S}_p^{(k)}/\bar{S}_p^{(k+1)}$ are free $\mathbb{Z}_p$-modules. Say that the projection of $s_{j_k+1},\dots,s_{j_k+d_k}$ to $\bar{S}_p^{(k)}/\bar{S}_p^{(k+1)}$ is a basis for $\bar{S}_p^{(k)}/\bar{S}_p^{(k+1)}$. Define the *k-th partial regulator*, $1 \le k \le p-1$,

$$R^{(k)} := \det\left(\langle\!\langle s_i, s_j\rangle\!\rangle_k\right)_{j_k+1\le i,j\le j_k+d_k}.$$

Notice that $R^{(k)}$ depends on the choice of the basis, and is well-defined up to multiplication by a p-adic unit. Given $t \ge 0$, we let $(I^t/I^{t+1} \otimes \mathbb{Q})/\mathbb{Z}_p^\times$ denote the quotient of the multiplicative monoid $I^t/I^{t+1} \otimes \mathbb{Q}$ by the action of the group of p-adic units $\mathbb{Z}_p^\times$. Let

$$\rho_p^{(k)} := \mathrm{rank}_{\mathbb{Z}_p}(\bar{S}_p^{(k)}), \quad \rho_p := \sum_{k=1}^{p} \rho_p^{(k)}.$$

Observe that if $\bar{S}_p^{(p)} = 0$ (i.e. by Theorem 2.18, $\langle\!\langle\ ,\ \rangle\!\rangle_{p-1}$ is nondegenerate) then $\rho_p = \sum_{k=1}^{p-1} kd_k$.

Definition 2.20. If $\langle\!\langle\ ,\ \rangle\!\rangle_{p-1}$ is nondegenerate, we define the *derived regulator* $R_{der} \in (I^{\rho_p}/I^{\rho_p+1} \otimes \mathbb{Q})/\mathbb{Z}_p{}^\times$ to be the product of the partial regulators $R^{(1)}\cdots R^{(p-1)}$. Otherwise, we let $R_{der} = 0$.

By Theorem 2.18, R_{der} is nonzero when $\langle\!\langle\ ,\ \rangle\!\rangle_{p-1}$ is nondegenerate. We say in this case that ρ_p is the *order of vanishing* of R_{der}. On the other hand, if $US_p(E/K)$ is nontrivial, then Theorem 2.18 implies $R_{der} = 0$.

Remark 2.21. If $\text{Ш}(E/K)_{p^\infty}$ is finite, then $S_p(E/K) \simeq E(K)\otimes\mathbb{Z}_p$ has a natural basis coming from an integral basis $P_1,\ldots,P_r$ for the Mordell-Weil group $E(K)$. Let $M \in M_n(\mathbb{Z}_p)$ be an endomorphism sending $P_1,\ldots,P_r$ to a basis compatible with the filtration on $S_p(E/K)$. Using this compatible basis, define the partial regulators $R^{(k)}$ as above, and define the generalized regulator by the formula:

$$R_{der} = \det(M)^{-2}R^{(1)}\cdots R^{(p-1)}.$$

This is well-defined in I^{ρ_p}/I^{ρ_p+1} (not just up to a p-adic unit) and does not depend on the choice of M.

In the next section we shall relate R_{der} to the leading coefficient of the characteristic power series of the Pontryagin dual of $\text{Sel}_{p^\infty}(E/K_\infty)$. Here we content ourselves with proving a parity statement for the order of vanishing.

Proposition 2.22. *Assume that $\langle\langle\ ,\ \rangle\rangle_{p-1}$ is nondegenerate. Then the order of vanishing of R_{der} has the same parity as the rank of the pro-p Selmer group $S_p(E/K)$.*

In particular, if $\text{Ш}(E/K)_{p^\infty}$ is finite, then the order of vanishing of R_{der} has the same parity as the rank of the Mordell-Weil group $E(K)$.

Proof. With notations as above, we have

$$\text{rank}_{\mathbb{Z}_p}(S_p(E/K)) = d_1 + \cdots + d_{p-1}.$$

For k even, by Theorem 2.18 $\langle\langle\ ,\ \rangle\rangle_k$ is a nondegenerate alternating pairing on the free $\mathbb{Z}_p$-module of rank d_k $\bar{S}_p^{(k)}/\bar{S}_p^{(k+1)}$. Hence d_k is even and

$$\text{rank}_{\mathbb{Z}_p}(S_p(E/K)) \equiv d_1 + d_3 + \cdots + d_{p-2} \pmod 2.$$

On the other hand, the order of vanishing of R_{der} is equal to

$$d_1 + 2d_2 + 3d_3 + \cdots + (p-1)d_{p-1} \equiv d_1 + d_3 + \cdots + d_{p-2} \pmod 2. \qquad \square$$

2.5. Refined Birch Swinnerton-Dyer formulae. We keep the notations of §2.4. Let

$$\mathcal{X}_\infty = \text{Hom}_{\mathbb{Z}_p}(\text{Sel}_{p^\infty}(E/K_\infty), \mathbb{Q}_p/\mathbb{Z}_p)$$

denote the Pontryagin dual of the Selmer group of E/K_∞. The main result of this section relates the order of vanishing and the leading coefficient of the characteristic ideal of $\mathcal{X}_\infty$ to the derived regulator R_{der} defined before. Assume that $\mathcal{X}_\infty$ is a torsion Λ-module. (Otherwise, both R_{der} and the characteristic ideal vanish, since $US_p(E/K) \neq 0$.) Let $\mathcal{L}_\infty$ denote a characteristic power series of $\mathcal{X}_\infty$. $\mathcal{L}_\infty$ is determined up to a unit of Λ. Let $\sigma_p \geq 0$ be the smallest exponent such that $\mathcal{L}_\infty$ belongs to I^{σ_p}, and let $\bar{\mathcal{L}}_\infty$ denote the image of $\mathcal{L}_\infty$ in $(I^{\sigma_p}/I^{\sigma_p+1})/\mathbb{Z}_p^\times$. Write

$\operatorname{char}(\mathcal{X}_\infty)$ for the characteristic ideal of $\mathcal{X}_\infty$. Clearly σ_p and $\bar{\mathcal{L}}_\infty$ depend only on $\operatorname{char}(\mathcal{X}_\infty)$, and therefore we may call them the *order of vanishing* and the *leading coefficient* of $\operatorname{char}(\mathcal{X}_\infty)$.

THEOREM 2.23. *The order of vanishing σ_p is greater than or equal to ρ_p, and we have:*

$$\bar{\mathcal{L}}_\infty = \# \frac{\text{Ш}(E/K)_{p^\infty}}{\operatorname{Div}(\text{Ш}(E/K)_{p^\infty})} \cdot R_{der}$$

in $(I^{\rho_p}/I^{\rho_p+1} \otimes \mathbb{Q})/\mathbb{Z}_p^\times$, where Div *denotes the divisible part.*

COROLLARY 2.24.

(1) *Assume that $\langle\!\langle\ ,\ \rangle\!\rangle_{p-1}$ is nondegenerate. Then σ_p is equal to ρ_p.*

(2) *Let p^B be the order of the finite group $\text{Ш}(E/K)_{p^\infty}/\operatorname{Div}(\text{Ш}(E/K)_{p^\infty})$.*

Then $p^B R_{der}$ belongs to $(I^{\rho_p}/I^{\rho_p+1})/\mathbb{Z}_p^\times$.

Remark 1. When $\langle\!\langle\ ,\ \rangle\!\rangle_1$ is nondegenerate, then R_{der} is equal to the usual p-adic regulator, and Theorem 2.23 contains as a particular case the Birch Swinnerton-Dyer formulae of Schneider [Sc2], [Sc3] (cf. also [PR1], [PR3]). On the other hand, when $\langle\!\langle\ ,\ \rangle\!\rangle_1$ happens to be degenerate, the order of vanishing of $\operatorname{char}(\mathcal{X}_\infty)$ is strictly greater than the order of vanishing of the classical regulator, and one needs the refined Birch Swinnerton-Dyer formula of Theorem 2.23 to capture the order of vanishing and the leading coefficient of $\operatorname{char}(\mathcal{X}_\infty)$. See ch. 3 for an illustration of this.

Remark 2. If $\langle\!\langle\ ,\ \rangle\!\rangle_{p-1}$ is degenerate, i.e. R_{der} is zero, the order of vanishing of $\operatorname{char}(\mathcal{X}_\infty)$ is stricly greater than ρ_p by Theorem 2.23. It is tempting to hope that the null-space of $\langle\!\langle\ ,\ \rangle\!\rangle_{p-1}$ reduces to the p-adic saturation $\bar{U}S_p(E/K)$ of the universal norms for almost all primes p. It would follow that $\langle\!\langle\ ,\ \rangle\!\rangle_{p-1}$ is nondegenerate if and only if $\mathcal{X}_\infty$ is a torsion Λ-module. In this case, by Corollary 2.24, the order of vanishing is precisely ρ_p. See the next chapter for the formulation of stronger conjectures of this sort, when K_∞/K is the anticyclotomic $\mathbb{Z}_p$-extension of an imaginary quadratic field. In general, however, it appears possible to fabricate examples where the radical of the $(p-1)$-th derived height is larger than the submodule of universal norms. See Remark 3.11 for more details.

Proof of Theorem 2.23. Given $n \geq 0$ fix an admissible set $\Sigma = \Sigma_n$ for $(E, K_n/K, p^n)$. Let $t = 2\#\Sigma$. Fix any bases $(x_1, \dots, x_t)$ and $(y_1, \dots, y_t)$ for the free Λ_n-modules of rank t, $X = \bigoplus_{v\in\Sigma} E((K_n)_v)/p^n E((K_n)_v)$ and $Y = \operatorname{Sel}^{\Sigma}_{p^n}(E/K_n)$, respectively. By Lemma 1.7, we can view X and Y as submodules of the free rank $2t$ Λ_n-module $Z = \bigoplus_{v\in\Sigma} H^1((K_n)_v, E_{p^n})$. Thus, by restricting the pairing

$\langle\ ,\ \rangle = \langle\ ,\ \rangle_{(n)}$ of §2.3 to $X \times Y$ we find a pairing

$$(*) \qquad \langle\ ,\ \rangle : X \times Y \to \Lambda_n$$

(denoted in the same way by abusing notation). The next two lemmas, by relating char $(\mathcal{X}_\infty)$ to $\langle\ ,\ \rangle$, provide a the bridge beween char $(\mathcal{X}_\infty)$ and the derived heights and regulator. The reader may find all the facts about the theory of Fitting ideals we need below in [MW], Appendix.

LEMMA 2.25. *The Fitting ideal* $\mathrm{Fitt}_{\Lambda_n}(\mathrm{Sel}_{p^n}(E/K_n)^{dual})$ *of the Pontryagin dual of* $\mathrm{Sel}_{p^n}(E/K_n)$ *is a principal ideal, generated by the discriminant* $\det(\langle x_i, y_j\rangle_{1\le i,j\le t})$ *of the pairing* $(*)$.

Proof. Let $W = \bigoplus_{v\in\Sigma} H^1((K_n)_v, E)_{p^n}$. By the properties of the local Tate pairing, $\langle\ ,\ \rangle : Z \times Z \to \Lambda_n$ induces a nondegenerate pairing $[\ ,\ ] : X \times W \to \Lambda_n$. Let y_i' be the image of y_i in W, and let $x_i^\vee$ be the basis of W which is dual to x_i with respect to the pairing $[\ ,\ ]$. By Lemma 1.7, the exact sequence of Proposition 1.6 gives a presentation of the Λ_n-module $\mathrm{Sel}_{p^n}(E/K_n)^{dual}$ with t generators and t relations. Hence $\mathrm{Fitt}_{\Lambda_n}(\mathrm{Sel}_{p^n}(E/K_n)^{dual})$ is a principal ideal, generated by $\det(a_{ij})$, where $y_j' = \sum_i a_{ij} x_i^\vee$. Since $a_{ij} = [x_i, y_j'] = \langle x_i, y_j\rangle$, the result follows. □

LEMMA 2.26. *Let* $\mu_n : \Lambda \to \Lambda_n$ *be the canonical projection. Then* $\mu_n(\mathrm{char}(\mathcal{X}_\infty)) = \mathrm{Fitt}_{\Lambda_n}(\mathrm{Sel}_{p^n}(E/K_n)^{dual})$.

Proof.

Step 1. Let J_n be the ideal of Λ $(p^n, (\gamma^{p^n} - 1))$. Then there is a natural identification

$$\mathcal{X}_\infty / J_n \mathcal{X}_\infty = \mathrm{Sel}_{p^n}(E/K_n)^{dual}.$$

For, by combining the argument in the proof of Lemma 1.4 with $E_p(K_\infty) = 0$, one can prove that the restriction map composed with the inclusion $E_{p^n} \subset E_{p^\infty}$ induces a natural isomorphism $\mathrm{Sel}_{p^n}(E/K_n) = \mathrm{Sel}_{p^\infty}(E/K_\infty)^{\Gamma_n}[p^n]$, Γ_n being the Galois group $\mathrm{Gal}(K_\infty/K_n)$. By taking duals, the identification follows.

Step 2. Since $\Lambda_n = \Lambda/J_n$, step 1 and the theory of Fitting ideals give

$$\mu_n(\mathrm{Fitt}_\Lambda(\mathcal{X}_\infty)) = \mathrm{Fitt}_{\Lambda_n}(\mathrm{Sel}_{p^n}(E/K_n)^{dual}).$$

Lemma 2.25 implies that $\mathrm{Fitt}_\Lambda(\mathcal{X}_\infty)$ is a principal ideal. The next step shows that in this case $\mathrm{Fitt}_\Lambda(\mathcal{X}_\infty)$ is equal to the characteristic ideal char $(\mathcal{X}_\infty)$, concluding the proof of Lemma 2.26.

Step 3.

SUBLEMMA. *Let* T *be a torsion* Λ*-module whose Fitting ideal* $\mathrm{Fitt}_\Lambda(T)$ *is principal. Then the characteristic ideal* char (T) *of* T *is equal to* $\mathrm{Fitt}_\Lambda(T)$.

Proof of the Sublemma. We use repeatedly without explicit mention the following fact: Given an exact sequence of finitely generated Λ-modules

$$0 \to M_1 \to M \to M_2 \to 0,$$

then

$$\mathrm{Fitt}_\Lambda(M_1)\,\mathrm{Fitt}_\Lambda(M_2) \subset \mathrm{Fitt}_\Lambda(M) \subset \mathrm{Fitt}_\Lambda(M_2).$$

By the classification theorem of Λ-modules there is an exact sequence

$$0 \to C_1 \to T \to \bigoplus_i \Lambda/\Lambda f_i \to C_2 \to 0,$$

with C_1 and C_2 finite. Since T is torsion, there is also an exact sequence

$$0 \to D_1 \to \bigoplus_i \Lambda/\Lambda f_i \to T \to D_2 \to 0,$$

with D_1 and D_2 finite. The first sequence implies easily

$$\mathrm{Fitt}_\Lambda(T)\,\mathrm{Fitt}_\Lambda(C_2) \subset \mathrm{Fitt}_\Lambda(T/C_1)\,\mathrm{Fitt}_\Lambda(C_2) \subset \mathrm{Fitt}_\Lambda\left(\bigoplus_i \Lambda/\Lambda f_i\right).$$

Similarly, from the second sequence we get

$$\mathrm{Fitt}_\Lambda\left(\bigoplus_i \Lambda/\Lambda f_i\right)\mathrm{Fitt}_\Lambda(D_2) \subset \mathrm{Fitt}_\Lambda\left(\left(\bigoplus_i \Lambda/\Lambda f_i\right)/D_1\right)\mathrm{Fitt}_\Lambda(D_2) \subset \mathrm{Fitt}_\Lambda(T).$$

Since $\mathrm{char}(T) = \mathrm{Fitt}_\Lambda(\bigoplus_i \Lambda/\Lambda f_i)$, by combining the two chains of inclusions we find

$$\mathrm{Fitt}_\Lambda(T)\,\mathrm{Fitt}_\Lambda(C_2)\,\mathrm{Fitt}_\Lambda(D_2) \subset \mathrm{char}(T)\,\mathrm{Fitt}_\Lambda(D_2) \subset \mathrm{Fitt}_\Lambda(T).$$

$\mathrm{Fitt}_\Lambda(C_2)$ and $\mathrm{Fitt}_\Lambda(D_2)$ are finite index ideals in Λ. For C_2 and D_2 are finite Λ-modules, and the Fitting ideal of a finitely generated Λ-module contains a positive power of the annihilator of that module. Hence there is a finite index ideal I (equal to $\mathrm{Fitt}_\Lambda(C_2)\,\mathrm{Fitt}_\Lambda(D_2)$) such that

$$\mathrm{Fitt}_\Lambda(T) \cdot I \subset \mathrm{char}(T)$$

with finite index. By hypothesis, $\mathrm{Fitt}_\Lambda(T) = (\theta)$ is a principal ideal. Let δ_1 and δ_2 be nonzero elements of I with no common irreducible factors. Since $\mathrm{char}(T)$ divides $\delta_1\theta$ and $\delta_2\theta$, we conclude that $\mathrm{char}(T)$ divides θ and $\mathrm{Fitt}_\Lambda(T)$ is contained in $\mathrm{char}(T)$ with finite index. Let $\mathrm{char}(T)\cdot(\alpha) = \mathrm{Fitt}_\Lambda(T)$. Then the finite module $\mathrm{char}(T)/\mathrm{Fitt}_\Lambda(T)$ is isomorphic to $\Lambda/(\alpha)$. Thus α must be a unit of Λ. This finishes the proof of the sublemma, and also of Lemma 2.26. □

Recall the filtration $S_p(E/K) = \bar{S}_p^{(1)} \supset \cdots \supset \bar{S}_p^{(p-1)} \supset \bar{S}_p^{(p)}$ defined in §2.4. It ends with 0, by Theorem 2.18, if and only if the pairing $\langle\!\langle\ ,\ \rangle\!\rangle_{p-1}$ is nondegenerate. For $1 \leq k \leq p$, we let $\bar{\mathrm{Sel}}_n^{(k)}$ denote the image of $\bar{S}_p^{(k)}$ in $\mathrm{Sel}_{p^n}(E/K) = \bar{\mathrm{Sel}}_n^{(1)}$ under the natural map. Since $\bar{S}_p^{(k)}$ is defined as the p-adic saturation in $S_p(E/K)$ of the module $S_p^{(k)}$, the $\bar{\mathrm{Sel}}_n^{(k)}$ give rise to a filtration of $\mathrm{Sel}_{p^n}(E/K)$ such that

$$\bar{\mathrm{Sel}}_n^{(k)}/\bar{\mathrm{Sel}}_n^{(k+1)} \simeq (\mathbb{Z}/p^n\mathbb{Z})^{d_k}, \quad 1 \leq k \leq p-1,$$

$$\bar{\mathrm{Sel}}_n^{(p)} \simeq (\mathbb{Z}/p^n\mathbb{Z})^{d_p},$$

where $d_k = \mathrm{rank}_{\mathbb{Z}_p}(\bar{S}_p^{(k)}/\bar{S}_p^{(k+1)})$ and $d_p = \mathrm{rank}_{\mathbb{Z}_p}\bar{S}_p^{(p)}$. In view of Lemmas 1.7 and 1.4, we can identify $\mathrm{Sel}_{p^n}(E/K)$ with the intersection submodule of the free $\mathbb{Z}/p^n\mathbb{Z}$-modules $X^{G_n} = \bigoplus_{v\in\Sigma} E(K_v)/p^nE(K_v)$ and $Y^{G_n} = \mathrm{Sel}_{p^n}^{\Sigma}(E/K)$. Choose a basis $(\bar{x}_1, \ldots, \bar{x}_t)$, respectively $(\bar{y}_1, \ldots, \bar{y}_t)$ for X^{G_n}, respectively Y^{G_n}, compatible with the above filtration. Assume that for $1 \leq k \leq p-1$ the projection of $(\bar{x}_{j_k+1}, \ldots, \bar{x}_{j_k+d_k})$ to $\bar{\mathrm{Sel}}_n^{(k)}/\bar{\mathrm{Sel}}_n^{(k+1)}$ is a basis for $\bar{\mathrm{Sel}}_n^{(k)}/\bar{\mathrm{Sel}}_n^{(k+1)}$, and that $(\bar{x}_{j_p+1}, \ldots, \bar{x}_{j_p+d_p})$ is a basis for $\bar{\mathrm{Sel}}_n^{(p)}$. And similarly for $(\bar{y}_{j_k+1}, \ldots, \bar{y}_{j_k+d_k})$. Let $(x_1, \ldots, x_t)$, respectively $(y_1, \ldots, y_t)$ be a basis for X, respectively Y such that $\mathrm{cores}_{K_n/K} x_k = \bar{x}_k$ and $\mathrm{cores}_{K_n/K} y_k = \bar{y}_k$. Write r for $\mathrm{rank}_{\mathbb{Z}_p} S_p(E/K)$. Then $r = \sum_{i=1}^{p} d_i$.

Lemma 2.27. *Let $\epsilon : \Lambda_n \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$ be the augmentation map and let $\langle\ ,\ \rangle : X \times Y \longrightarrow \Lambda_n$ be the pairing $(*)$ introduced before. Then for some unit $u \in \mathbb{Z}/p^n\mathbb{Z}$ we have the equality in $\mathbb{Z}/p^n\mathbb{Z}$*

$$\epsilon(\det(\langle x_i, y_j\rangle_{r+1\leq i,j\leq t})) = u \cdot \#\frac{\text{Ш}(E/K)_{p^\infty}}{\mathrm{Div}(\text{Ш}(E/K)_{p^\infty})}.$$

Proof. Of course, $\epsilon(\det(\langle x_i, y_j\rangle_{r+1\leq i,j\leq t}))$ is equal to $\det(\epsilon\langle x_i, y_j\rangle_{r+1\leq i,j\leq t})$. By Proposition 1.3, (3), $\epsilon\langle x_i, y_j\rangle = -\langle \bar{x}_i, \bar{y}_j\rangle_{K,p^n}$ for $1 \leq i, j \leq t$. Since $(\bar{x}_1, \ldots, \bar{x}_r)$ is a basis for $\bar{\mathrm{Sel}}_n^{(1)} \subset \mathrm{Sel}_{p^n}(E/K)$, the global reciprocity law (see Proposition 1.2) gives

$$\text{(a)} \qquad \langle \bar{x}_i, \bar{y}_j\rangle_{K,p^n} = 0, \quad 1 \leq i \leq r, \quad 1 \leq j \leq t.$$

Similarly, since $(\bar{y}_1, \ldots, \bar{y}_r)$ is a basis for $\bar{\mathrm{Sel}}_n^{(1)}$, the isotropy of the local points under the local Tate pairing (§1.2.1) gives

$$\text{(b)} \qquad \langle \bar{x}_i, \bar{y}_j\rangle_{K,p^n} = 0, \quad 1 \leq i \leq t, \quad 1 \leq j \leq r.$$

Suppose that the group $\text{Ш}(E/K)_{p^\infty}/\text{Div}\,(\text{Ш}(E/K)_{p^\infty})$ is isomorphic to

$$\mathbb{Z}/p^{\alpha_1}\mathbb{Z}\bigoplus\cdots\bigoplus\mathbb{Z}/p^{\alpha_s}\mathbb{Z}.$$

We have $s \leq t-r$. Assume, without loss of generality, that $\alpha_i < n$. The image of $\text{Sel}^{\Sigma}_{p^n}(E/K)$ in $\bigoplus_{v\in\Sigma}H^1(K_v,E)_{p^n}$ is generated by the images of $\bar{y}_{r+1},\dots,\bar{y}_t$, and it is isomorphic to the direct sum of $t-r$ summands

$$\mathbb{Z}/p^{n-\alpha_1}\mathbb{Z}\bigoplus\cdots\bigoplus\mathbb{Z}/p^{n-\alpha_s}\bigoplus\mathbb{Z}/p^n\mathbb{Z}\bigoplus\cdots\bigoplus\mathbb{Z}/p^n\mathbb{Z}.$$

Hence, by (a), (b) and the local Tate duality we find

$$\det(\langle\bar{x}_i,\bar{y}_j\rangle_{r+1\leq i,j\leq t}) = u_1\cdot\#\frac{\text{Ш}(E/K)_{p^\infty}}{\text{Div}\,(\text{Ш}(E/K)_{p^\infty})}$$

for a unit u_1 of $\mathbb{Z}/p^n\mathbb{Z}$. The lemma follows. □

Let p^A be the maximum of the exponents of the finite groups $\bar{S}_p^{(k)}/S_p^{(k)}$, $1\leq k\leq p$. Then for all $n\geq 1$ we have $p^A\cdot\bar{\text{Sel}}_n^{(k)}\subset\text{Sel}_n^{(k)}$. Consider the discriminant $\det(\langle p^Ax_i,p^Ay_j\rangle_{1\leq i,j\leq t})$. By Lemma 2.25, it generates $p^{2At}\,\text{Fitt}_{\Lambda_n}(\text{Sel}_{p^n}(E/K_n)^{dual})$. Although the admissible set $\Sigma=\Sigma_n$ depends on n, we may assume that $t=2\#\Sigma$ is independent of n (see the remark after definition 1.5: We may assume that t be equal to $2dim_{\mathbb{F}_p}(\text{Sel}_{p^n}(E/K)\otimes\mathbb{F}_p)$). In particular, $p^{2tA}\,\text{Fitt}_{\Lambda_n}(\text{Sel}_{p^n}(E/K_n)^{dual})$ is nonzero for n sufficiently large. For $1\leq k\leq p$ the elements $(p^A\bar{x}_{j_k+1},\dots,p^A\bar{x}_{j_k+d_k})$, $(p^A\bar{y}_{j_k+1},\dots,p^A\bar{y}_{j_k+d_k})$, belong to $\text{Sel}_n^{(k)}$. Choose $(x'_{j_k+1},\dots,x'_{j_k+d_k})$ in X and $(y'_{j_k+1},\dots,y'_{j_k+d_k})$ in Y such that:

(1) $\text{cores}_{K_n/K}x'_{j_k+i}=p^A\bar{x}_{j_k+i}$, $\text{cores}_{K_n/K}y'_{j_k+i}=p^A\bar{y}_{j_k+i}$;

(2) $D_n^{(k-1)}x'_{j_k+i}$ belongs to $\text{Sel}_{p^n}(E/K_n)$, $D_n^{(k-1)}y'_{j_k+i}$ belongs to $\text{Sel}_{p^n}(E/K_n)$.

For $r+1\leq i\leq t$, let $x'_i=p^Ax_i$ and $y'_i=p^Ay_i$. Let U and V in $M_t(\Lambda_n)$ be $t\times t$ matrices with entries in Λ_n such that $(x_1,\dots,x_t)U=(x'_1,\dots,x'_t)$, and $(y_1,\dots,y_t)V=(y'_1,\dots,y'_t)$. Since $\text{cores}_{K_n/K}x'_i=\text{cores}_{K_n/K}p^Ax_i$ and $\text{cores}_{K_n/K}y'_i=\text{cores}_{K_n/K}p^Ay_i$, we find $\epsilon(U)=\epsilon(V)=p^AI_t$, where I_t is the identity matrix in $M_t(\mathbb{Z}/p^n\mathbb{Z})$. Thus, we may replace $\det(\langle p^Ax_i,p^Ay_j\rangle_{1\leq i,j\leq t})$ by $\det(\langle x'_i,y'_j\rangle_{1\leq i,j\leq t})$ in the computation of the leading coefficient of $p^{2At}\,\text{Fitt}_{\Lambda_n}(\text{Sel}_{p^n}(E/K_n)^{dual})$. Observe that for $j_k+1\leq i\leq j_k+d_k$, $\langle x'_i,y\rangle$ belongs to I_n^k for all $y\in Y$. For, $D_n^{(k-1)}\langle x'_i,y\rangle=0$, by Proposition 1.3, (5). Let $\sigma_p=d_1+2d_2+\cdots+(p-1)d_{p-1}+pd_p$. Then

$$\det(\langle x'_i,y'_j\rangle_{1\leq i,j\leq t})\in I_n^{\sigma_p}.$$

Thus the order of vanishing of $\text{char}(\mathcal{X}_\infty)$ is greater or equal than σ_p. This is enough to prove the theorem when $\langle\!\langle\ ,\ \rangle\!\rangle_{p-1}$ is degenerate, i.e. $d_p\neq 0$. For, $\sigma_p>\rho_p=d_1+2d_2+\cdots+(p-1)d_{p-1}$ and $R_{der}=0$ by definition. From now on assume that $\langle\langle\ ,\ \rangle\rangle_{p-1}$ is nondegenerate, hence $\rho_p = \sigma_p$. By Lemma 2.27 and the above remarks, we find the equality in I^{ρ_p}/I^{ρ_p+1}

$$\det(\langle x'_i, y'_j\rangle_{1\le i,j\le t}) = u_n \cdot p^{2A(t-r)} \cdot \#\frac{\text{III}(E/K)_{p^\infty}}{\text{Div}\,(\text{III}(E/K)_{p^\infty})} \cdot \prod_{k=1}^{p-1} \det(\langle x'_i, y'_j\rangle_{j_k+1\le i,j\le j_k+d_k}),$$

for some unit u_n of $\mathbb{Z}/p^n\mathbb{Z}$. By the definition of the derived heights $\langle\ ,\ \rangle_{k,n}$ we have in $I_n^{\rho_p}/I_n^{\rho_p+1}$

$$\prod_{k=1}^{p-1} \det((\langle p^A\bar{x}_i, p^A\bar{y}_j\rangle_{k,n})_{j_k+1\le i,j\le j_k+d_k}) = \prod_{k=1}^{p-1} \det(\langle x'_i, y'_j\rangle_{j_k+1\le i,j\le j_k+d_k}).$$

But

$$p^{2Ar}\mu_n(R_{der}) = \prod_{k=1}^{p-1} \det((\langle p^A\bar{x}_i, p^A\bar{y}_j\rangle_{k,n})_{j_k+1\le i,j\le j_k+d_k}).$$

Theorem 2.23 follows. □

Remark 2.28. The results of this section and of the previous one are concerned with the study of the degeneracy of the p-adic height. We point out that Schneider [Sc2] has conjectured that the p-adic height attached to the cyclotomic $\mathbb{Z}_p$-extension K_∞ of a number field K is always nondegenerate. Assuming this conjecture, theorem 2.18 implies that $\mathcal{X}_\infty$ is Λ-torsion. In this case the generalized regulator R_{der} coincides with the usual p-adic regulator, and by Theorem 2.23 the characteristic ideal of $\mathcal{X}_\infty$ vanishes to order $r = \text{rank}_{\mathbb{Z}_p} S_p(E/K)$. In particular, $\mathcal{X}_\infty \otimes \mathbb{Q}$ is a semisimple $\mathbb{Q}_p[[\Gamma]]$-module. It also follows that the Mordell-Weil group $E(K_\infty)$ is a finitely generated $\mathbb{Z}$-module, since $E(K_\infty)_{tors}$ is finite under our assumptions by [Ma3], §6. If $K = \mathbb{Q}$ and E has complex multiplications, Rubin [Ru] has shown that $\mathcal{X}_\infty$ is torsion over Λ. If in addition the analytic rank of E is at most one, the results of Kolyvagin [Ko] combined with a theorem of Bertrand [Ber] on values of p-adic theta functions show that the p-adic height is nondegenerate. Much less is known when E does not have complex multiplications. Kato has announced recently a proof that $\mathcal{X}_\infty$ is Λ-torsion, for modular elliptic curves. Nothing is known about the p-adic height.

Now let E be a complex multiplication elliptic curve defined over $\mathbb{Q}$ and let K be its field of complex multiplications. Assuming that the sign of the functional equation of $L(E/\mathbb{Q}, s)$ is -1 and K_∞ is the anticyclotomic $\mathbb{Z}_p$-extension of K, the results of Greenberg [Gr] show that the Λ-rank of $\mathcal{X}_\infty$ is equal to 2, and hence the p-adic height must be degenerate because of the presence of universal norms.

With E and K as above, Brattström [Br] gives examples of $\mathbb{Z}_p$-extensions of K such that the attached p-adic height is degenerate, whereas a variant of $\mathcal{X}_\infty$

is torsion over the Iwasawa algebra. We refer the reader to her paper for more details.

In the next chapter we treat in detail the case of the anticyclotomic $\mathbb{Z}_p$-extension of an imaginary quadratic field K, assuming that E is an elliptic curve over $\mathbb{Q}$ such that K is different from the field of endomorphisms of E.

In general, it is rather common to have degeneracies in the p-adic height. For example, let L_∞ be a $\mathbb{Z}_p^d$-extension of a number field K. (Recall that we can always choose d so that it is equal to $r_2 + 1$, r_2 being the number of complex embeddings of K.) One can show that it is possible to define a p-adic height pairing

$$S_p(E/K) \times S_p(E/K) \to \mathrm{Gal}\,(L_\infty/K) \simeq \mathbb{Z}_p^d$$

by imposing that it be compatible with the p-adic heights relative to the $\mathbb{Z}_p$-extensions K_∞ contained in L_∞ under the natural maps $\mathrm{Gal}\,(L_\infty/K) \to \mathrm{Gal}\,(K_\infty/K)$. Letting r denote the $\mathbb{Z}_p$-rank of $S_p(E/K)$, suppose that $r(r+1) < 2d$. It follows that for at least one of the $\mathbb{Z}_p$-extensions K_∞ the corresponding p-adic height is identically zero. See also the examples in Remark 3.11.

More natural examples of degeneracies in the p-adic height are treated in the next chapter.

3. Elliptic curves and anticyclotomic $\mathbf{Z}_p$-extensions.

In this chapter K_∞ denotes the anticyclotomic $\mathbb{Z}_p$-extension of an imaginary quadratic field K, defined by adjoining to K values of modular functions at complex multiplication points of p-power conductor. It is the only $\mathbb{Z}_p$-extension of K that is dihedral over $\mathbb{Q}$. We require that $(E, p, K_\infty/K)$ satisfy the assumptions of §1.1. We also assume that $\text{Ш}(E/K)_{p^\infty}$ is finite. Thus $S_p(E/K) = E(K)_p$, and we can readily translate standard analytic conjectures into statements on the rank of the pro-p Selmer group $S_p(E/K)$.

The goal of this chapter is to sketch the Iwasawa theory, still largely conjectural, for elliptic curves over $\mathbb{Q}$ with values in the intermediate extensions of K_∞/K. In this situation the degeneracy of the p-adic height pairing tends to be the rule, and the theory of derived heights allows a conceptual formulation of the theory.

3.1. The conjectures of Mazur.

We begin by recalling some conjectures of Mazur (see [Ma3], and also [Ma2]) concerning the null-space of the p-adic height. Let τ denote a fixed complex conjugation. Thus, given $g \in \mathrm{Gal}\,(K_\infty/K)$, we have $g^\tau = g^{-1}$. Write $S_p(E/K)^\pm$ for the submodule of $S_p(E/K)$ on which τ acts as ± 1, and $r_\pm$ for the $\mathbb{Z}_p$-rank of $S_p(E/K)^\pm$. Write $r = r_+ + r_-$ for $\mathrm{rank}_{\mathbb{Z}_p}(S_p(E/K))$. The following Galois equivariance property of the derived p-adic heights holds.

LEMMA 3.1. *For all $s_1, s_2 \in \bar{S}_p^{(k)}$, $\langle\langle \tau s_1, \tau s_2 \rangle\rangle_k = (-1)^k \langle\langle s_1, s_2 \rangle\rangle_k$.*

Proof. The Galois equivariance of the local Tate pairing implies immediately the equality

$$\langle \tau x, \tau y\rangle_{(n)} = \tau\langle x, y\rangle_{(n)}\tau^{-1},$$

where $\langle\ ,\ \rangle_{(n)}$ denotes the Λ_n-valued pairing of §2.3. Hence by definition

$$\langle\!\langle \tau s_1, \tau s_2\rangle\!\rangle_k = \langle\!\langle s_1, s_2\rangle\!\rangle_k^*,$$

where $*$ denotes the involution of Λ given on group-like elements by $g^* = g^{-1}$. The lemma follows from the fact that $*$ acts on $I^k/I^{k+1} \otimes \mathbb{Q}$ as $(-1)^k$. □

In particular, we find that the p-adic height pairing $\langle\!\langle\ ,\ \rangle\!\rangle_1$ is trivial when restricted to $S_p(E/K)^+ \times S_p(E/K)^+$ and $S_p(E/K)^- \times S_p(E/K)^-$. Hence, the null-space of $\langle\!\langle\ ,\ \rangle\!\rangle_1$ has rank at least $|r_+ - r_-|$. Following Mazur's terminology we give:

Definition 3.2. We say that E is in the *generic case* if either E does not have complex multiplications or K is not the complex multiplication field of E.

Conjecture 3.3 (Mazur). Assume that E is in the generic case. Then the null-space of $\langle\!\langle\ ,\ \rangle\!\rangle_1$ has rank $|r_+ - r_-|$, i.e. $\mathrm{rank}_{\mathbb{Z}_p} \bar{S}_p^{(2)} = |r_+ - r_-|$.

In other words, the anticyclotomic p-adic height should be as nondegenerate as possible. We may reformulate Conjecture 3.3 by saying that the pairing

$$\langle\!\langle\ ,\ \rangle\!\rangle_1 : S_p(E/K)^+ \times S_p(E/K)^- \to I/I^2,$$

obtained by restriction of $\langle\!\langle\ ,\ \rangle\!\rangle_1$, is either left or right nondegenerate. Since, by Theorem 2.18, the universal norm submodule $US_p(E/K)$ is contained in the null-space of $\langle\!\langle\ ,\ \rangle\!\rangle_1$, Conjecture 3.3 implies that $US_p(E/K)$ is contained in either $S_p(E/K)^+$ or $S_p(E/K)^-$, whichever has the larger rank. The following "growth number" conjecture gives precise information on the size of $US_p(E/K)$.

Conjecture 3.4 (Mazur). Assume that E is in the generic case. If $\mathrm{rank}_{\mathbb{Z}_p}(S_p(E/K))$ is even, respectively odd then $US_p(E/K) = 0$, respectively $US_p(E/K) \simeq \mathbb{Z}_p$.

Equivalently (see for example [B], §II.1) the Pontryagin dual $\mathcal{X}_\infty$ of $\mathrm{Sel}_{p^\infty}(E/K_\infty)$ is a torsion Λ-module, respectively has rank 1 over Λ when $\mathrm{rank}_{\mathbb{Z}_p}(S_p(E/K))$ is even, respectively odd.

3.2. Applications of the derived p-adic heights. Consider the second derived p-adic height

$$\langle\!\langle\ ,\ \rangle\!\rangle_2 : \bar{S}_p^{(2)} \times \bar{S}_p^{(2)} \to I^2/I^3 \otimes \mathbb{Q}.$$

Assume Conjecture 3.3. Then $\mathrm{rank}_{\mathbb{Z}_p}(\bar{S}_p^{(2)}) = |r_+ - r_-|$ and $\bar{S}_p^{(2)}$ is contained in one of the eigenspaces of τ acting on $S_p(E/K)$. Thus Lemma 3.1 does not force any degeneracy of $\langle\!\langle\ ,\ \rangle\!\rangle_2$. On the other hand, we have the *a priori* information that the universal norms $US_p(E/K)$ are contained in the null-space of $\langle\!\langle\ ,\ \rangle\!\rangle_2$. Conjecture 3.4 indicates that $US_p(E/K)$ need not be trivial (see also §3.2.3 below). Inspired by the philosophy of Conjecture 3.3, we formulate the following:

Conjecture 3.5. Assume that E is in the generic case. Then the null-space of the second derived p-adic height $\langle\!\langle\ ,\ \rangle\!\rangle_2$ is equal to $\bar{U}S_p(E/K)$, the p-adic saturation of $US_p(E/K)$ in $S_p(E/K)$.

For the sake of clarity, let us make two separate discussions according to the parity of the rank of $S_p(E/K)$.

3.2.1. The even rank case. Assume that $\mathrm{rank}_{\mathbb{Z}_p} S_p(E/K)$ is even. Assuming Conjecture 3.4, we may reformulate 3.5 as follows.

Conjecture 3.6. Assume that E is in the generic case, and that $\mathrm{rank}_{\mathbb{Z}_p} S_p(E/K)$ is even. Then the second derived p-adic height pairing is nondegenerate.

By Theorem 2.18, this is equivalent to $\bar{S}_p^{(3)} = 0$. Since we are assuming that $US_p(E/K)$ is trivial, $\mathcal{X}_\infty$ is a torsion Λ-module. By combining Theorem 2.23 with the above conjecture, we obtain a conjectural statement for the order of vanishing of the characteristic ideal of $\mathcal{X}_\infty$.

Conjecture 3.7. Assume that E is in the generic case and that $\mathrm{rank}_{\mathbb{Z}_p}(S_p(E/K))$ is even. Then the characteristic ideal of $\mathcal{X}_\infty$ vanishes to order $r + |r_+ - r_-| = 2\max(r_+, r_-)$.

3.2.2. The odd rank case. Assume that $\mathrm{rank}_{\mathbb{Z}_p} S_p(E/K)$ is odd. Assuming Conjecture 3.4, we reformulate 3.5 as follows.

Conjecture 3.8. Assume that E is in the generic case and that $\mathrm{rank}_{\mathbb{Z}_p} S_p(E/K)$ is odd. Then the null-space of the second derived p-adic height pairing is a free rank one $\mathbb{Z}_p$-module equal to $\bar{U}S_p(E/K)$.

Conjecture 3.8 provides a characterization of the space of universal norms $US_p(E/K)$ (or, rather, its p-adic saturation) in terms of the second derived height. This brings up the challenge of finding a computational definition of the derived heights, in order to have a way of approximating numerically $US_p(E/K)$.

If $\bar{U}S_p(E/K)$ is isomorphic to $\mathbb{Z}_p$, then $\mathcal{X}_\infty$ is a Λ-module of rank 1 and, by definition, the derived regulator R_{der} vanishes. The theory of derived heights may be used to define a *modified derived regulator* R'_{der}, which accounts for this situation. By Theorem 2.18, Conjecture 3.8 amounts to $\bar{S}_p^{(3)} = \bar{U}S_p(E/K)$. Hence, with notations as in §2.3, the partial regulators $R^{(k)}$ vanish for $3 \leq k \leq p-1$. Let $d_i = \operatorname{rank}_{\mathbb{Z}_p} \bar{S}_p^{(i)}/\bar{S}_p^{(i+1)}$, $i = 1, 2$. Then we define

$$R'_{der} := R^{(1)}R^{(2)} \in (I^{d_1+2d_2}/I^{d_1+2d_2+1} \otimes \mathbb{Q})/\mathbb{Z}_p{}^\times.$$

Note that the order of vanishing of R'_{der} is exactly $d_1 + 2d_2$. By the above conjectures, this is equal to $(r-1)+(|r_+ - r_-|-1) = 2(max(r_+, r_-)-1)$. Along the lines of Theorem 2.23, one can prove a theorem connecting the modified regulator R'_{der} to the leading coefficient of the characteristic ideal of the Λ-torsion submodule $(\mathcal{X}_\infty)_{tors}$ of $\mathcal{X}_\infty$. (For reasons of brevity, we do not give details.)

Conjecture 3.9. Assume that E is in the generic case, and that $\operatorname{rank}_{\mathbb{Z}_p}(S_p(E/K))$ is odd. Then the characteristic ideal of $(\mathcal{X}_\infty)_{tors}$ vanishes to order $(r-1)+(|r_+ - r_-|-1)$.

3.2.3. Heegner points (Reference: [B]). Assume that $E/\mathbb{Q}$ is a modular elliptic curve and that K satisfies the Heegner hypothesis, i.e. all rational primes dividing the conductor of E are split in K. Then the analytic rank of $E(K)_p$ is odd. Assuming standard conjectures, so is $\operatorname{rank}_{\mathbb{Z}_p}(S_p(E/K))$. There is a collection of complex multiplication points defined over K_∞, called Heegner points. Let $\mathcal{E}(E/K_n)_p \subset S_p(E/K_n)$ denote the cyclic $\mathbb{Z}_p[\operatorname{Gal}(K_n/K)]$-module generated by any Heegner point of level K_n. Define the Λ-modules

$$\hat{\mathcal{E}}(E/K_\infty)_p := \varprojlim_n \mathcal{E}(E/K_n)_p,$$
$$\hat{S}_p(E/K_\infty) := \varprojlim_n S_p(E/K_n),$$

where the projective limits are with respect to the natural corestriction mappings. Note that $\hat{\mathcal{E}}(E/K_\infty)_p$ is contained in $\hat{S}_p(E/K_\infty)$. One can show that $\hat{S}_p(E/K_\infty)$ is a free Λ-module of finite rank (equal to the $\mathbb{Z}_p$-rank of $US_p(E/K)$) and that $\hat{\mathcal{E}}(E/K_\infty)_p$ is a cyclic Λ-module (cf. [B], ch. II). Thus $\hat{\mathcal{E}}(E/K_\infty)_p$ is either isomorphic to Λ or 0. Analytic evidence combined with a theorem of Gross-Zagier lead to the natural expectation that some of the Heegner points of level K_n have infinite order, i.e., $\hat{\mathcal{E}}(E/K_\infty)_p$ is isomorphic to Λ. Assuming this, it is proved in [B], §III.1 that the conclusion of Conjecture 3.4, i.e. $US_p(E/K) \simeq \mathbb{Z}_p$, holds. This is equivalent to $\hat{S}_p(E/K_\infty)$ being a free Λ-module of rank 1. In this situation, $\hat{S}_p(E/K_\infty)/\hat{\mathcal{E}}(E/K_\infty)_p$ is a cyclic torsion Λ-module. The next conjecture blends a conjecture of B. Perrin-Riou [PR2] with Conjecture 3.9. Let $\operatorname{char}(\hat{S}_p(E/K_\infty)/\hat{\mathcal{E}}(E/K_\infty)_p)$ denote the characteristic ideal of $\hat{S}_p(E/K_\infty)/\hat{\mathcal{E}}(E/K_\infty)_p$.

Conjecture 3.10. $\operatorname{char}(\hat{S}_p(E/K_\infty)/\hat{\mathcal{E}}(E/K_\infty)_p)^2$ vanishes to order $(r-1)+(|r_+-r_-|-1)$.

The results of [B], ch. III, based on the ideas of Kolyvagin [Ko], provide evidence for Conjecture 3.10.

Remark 3.11.

1. We sketch the possible construction of an example where the radical of the $p-1$-th derived height is larger than the space of universal norms. Let $p=3$, and let E denote an elliptic curve subject to our assumptions, whose rank is 1 over $\mathbb{Q}$ and 2 over an imaginary quadratic field K. Write $s_\pm$ for a generator of $S_p(E/K)^\pm$. Denote by K_∞, respectively C_∞ the anticyclotomic, respectively cyclotomic $\mathbb{Z}_p$-extension of K. Thus $L_\infty = C_\infty K_\infty$ is the unique $\mathbb{Z}_p^2$-extension of K. According to our conjectures, the p-adic height pairing $\langle\ ,\ \rangle_a$ attached to K_∞/K should be nondegenerate. Assume this, and let

$$\begin{pmatrix} 0 & A \\ A & 0 \end{pmatrix}$$

be its matrix relative to the basis (s_+, s_-). Similarly, let

$$\begin{pmatrix} B & 0 \\ 0 & C \end{pmatrix}$$

be the matrix of the cyclotomic height $\langle\ ,\ \rangle_c$ relative to (s_+, s_-) . We assume, in agreement with the conjecture of Schneider mentioned in remark 2.28, that this matrix is nondegenerate. For $\lambda \in \mathbb{Z}_p$, define a homomorphism

$$\operatorname{Gal}(L_\infty/K) = \operatorname{Gal}(C_\infty/K) \times \operatorname{Gal}(K_\infty/K) \simeq \mathbb{Z}_p \times \mathbb{Z}_p \to \operatorname{Gal}(M_\infty^{(\lambda)}/K) \simeq \mathbb{Z}_p$$

by the rule $(x,y) \mapsto \lambda x + y$. Thus the p-adic height attached to $M_\infty^{(\lambda)}$ is equal to $\lambda\langle\ ,\ \rangle_c + \langle\ ,\ \rangle_a$, and its p-adic regulator is given by $BC\lambda^2 - A^2$. Now suppose that BC is a square in $\mathbb{Z}_p$. Then the $\mathbb{Z}_p$-extensions $M_\infty^{(\lambda)}$ corresponding to $\lambda = \pm(A/\sqrt{BC})$ are such that the radical $\bar{S}_p^{(2,\lambda)}$ of the associated p-adic height pairing has rank 1. Moreover, they are different from K_∞, since λ is nonzero. Since the second derived height is alternating, it must be zero on $\bar{S}_p^{(2,\lambda)}$. By a conjecture of Mazur (cf. [Ma2] and [Ma3]), the universal norms from $M_\infty^{(\lambda)}$ should be trivial. Thus the above construction would provide the desired example. We remark that the above regulators can actually be computed, by using the analytic definition of p-adic height.

2. Here we construct examples of $\mathbb{Z}_p$-extensions such that $\mathcal{X}_\infty$ is highly nonsemisimple for the action of $\gamma - 1$. By Theorem 2.23 this amounts to show that most derived p-adic heights are degenerate. Let K be an abelian extension of a number field F such that $G := \mathrm{Gal}(K/F)$ is a cyclic group of order $p - 1$. Suppose that K_∞ is a $\mathbb{Z}_p$-extension of K such that G acts on Γ via an odd character $\chi : G \to \mathbb{Z}_p^\times$ of order $p - 1$. For example, consider the case $F = \mathbb{Q}$, $K = \mathbb{Q}(\mu_p)$. The existence of a $\mathbb{Z}_p$-extension as above follows from class field theory combined with standard properties of the local units in cyclotomic fields. Now let E be an elliptic curve over F subject to our assumptions. Moreover, assume that $S_p(E/K) = S_p(E/F)$, so that G acts trivially on $S_p(E/K)$, and that the $\mathbb{Z}_p$-rank of $S_p(E/K)$ is odd. The formula

$$\langle\!\langle gs_1, gs_2 \rangle\!\rangle_k = \chi(g)^{-k} \langle\!\langle s_1, s_2 \rangle\!\rangle_k \quad \forall g \in G, \quad \forall s_1, s_2 \in \bar{S}_p^{(k)}$$

is a generalization of Lemma 3.1 and is proved similarly. It follows that the first $p-2$ derived heights are totally degenerate. Moreover, since the rank of $S_p(E/K)$ is odd, the fact that the $p - 1$-th derived height is alternating implies that it must have nonzero radical. Is it possible that this radical has rank larger than the one of the module of universal norms?

Universita di Pavia, Dipartimento di Matematica, Via Abbiategrasso 209, 27100
Pavia, Italy
Electronic mail: MB61@IPVIAN.BITNET

McGill University, Mathematics Department, 805 Sherbrooke Street, West,
Montreal, QC H3A 2K6, Canada
Electronic mail: DARMON@MATH.MCGILL.CA

REFERENCES

[B] M. Bertolini, Selmer groups and Heegner points in anticyclotomic $\mathbb{Z}_p$-extensions, *Compositio Math.* (to appear).

[BD] M. Bertolini and H. Darmon, Derived heights and generalized Mazur-Tate regulators, *Duke Math. J.* **76** (1994), 75–111.

[Ber] D. Bertrand, Valeurs de fonctions theta et hauteurs p-adiques, Séminaire de Théorie des Nombres, Paris 1980–81, *Progr. Math.* vol. 22, Birkhäuser, Boston, 1982, pp. 1–11.

[Br] G. Brattström, The invariants of the Tate-Shafarevich group in a $\mathbb{Z}_p$-extension can be infinite, *Duke Math. J.* **52** (1985), 149–156.

[CF] J. W. S. Cassels and A. Frölich, *Algebraic Number Theory*, Academic Press, Orlando, FL, 1967.

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

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

[Ko] V. A. Kolyvagin, *Euler Systems*, *The Grothendieck Festschrift*, vol. 2 (P. Cartier et al. eds.), Birkhäuser, Boston, 1990, pp. 435–483.

[Ma1] B. Mazur, Rational points of abelian varieties with values in towers of number fields, *Invent. Math.* **18** (1972), 183–266.

[Ma2] ________, Modular curves and arithmetic, *Proc. Int. Cong. of Math.*, Warszawa, 1983.

[Ma3] ________, Elliptic curves and towers of number fields, preprint.

[MT1] B. Mazur and J. Tate, Canonical height pairings via biextensions, *Arithmetic and Geometry*, vol. 1 (M. Artin and J. Tate, eds.), *Progr. Math.* , Birkhäuser, Boston, 1983, pp. 195–238.

[MT2] ________, Refined conjectures of the "Birch and Swinnerton-Dyer type", *Duke. Math. J.* **54** (1987), 711.

[MW] B. Mazur and A. Wiles, Class fields of abelian extensions of $\mathbb{Q}$, *Invent. Math.* **76** (1984), 179–330.

[Mi] J. S. Milne, Arithmetic duality theorems, *Perspect. Math.*, Academic Press, Boston, 1986.

[PR1] B. Perrin-Riou, Arithmétique des courbes elliptiques et théorie d'Iwasawa, *Bull. Soc. Math. France Suppl.* **17** (1984).

[PR2] ________, Fonctions L p-adiques, Théorie d'Iwasawa et points de Heegner, *Bull. Soc. Math. France* **115** (1987), 399–456.

[PR3] ________, Théorie d'Iwasawa et hauteurs p-adiques, *Invent. Math.* **109** (1992), 137–185.

[Ru] K. Rubin, The "main conjectures" of Iwasawa theory for imaginary quadratic fields, *Invent. Math.* **79** (1985), 25–68.

[Sc1] P. Schneider, p-adic height pairings I, *Invent. Math.* **69** (1982), 401–409.

[Sc2] ________, Iwasawa L-functions of varieties over algebraic number fields. A first approach, *Invent. Math.* **71** (1983), 251–293.

[Sc3] ________, p-adic height pairings II, *Invent. Math.* **79** (1985), 329–374.

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

[T] K-S. Tan, p-adic pairings, Proceedings of the Boston University Workshop on p-adic Monodromy and the Birch Swinnerton-Dyer conjecture, *Contemp. Math.*, American Mathematical Society, Providence, RI, preprint.