Functiones et Approximatio
55.1 (2016), 59–81
doi: 10.7169/facm/2016.55.1.5

ARITHMETIC LOCAL CONSTANTS FOR ABELIAN VARIETIES WITH EXTRA ENDOMORPHISMS

Sunil Chetty

Abstract: This work generalizes the theory of arithmetic local constants, introduced by Mazur and Rubin, to better address abelian varieties with a larger endomorphism ring than $\mathbb{Z}$. We then study the growth of the p^∞-Selmer rank of our abelian variety, and we address the problem of extending the results of Mazur and Rubin to dihedral towers $k \subset K \subset F$ in which $[F : K]$ is not a p-power extension.

Keywords: elliptic curve, abelian variety, Selmer rank, complex multiplication.

1. Introduction

In [9], Mazur and Rubin introduce a theory of arithmetic local constants for an elliptic curve E in terms of Selmer structures associated to E. With this theory they study, for an odd prime p, the growth in $\mathbb{Z}_p$-corank of the p^∞-Selmer group $\mathrm{Sel}_{p^\infty}(E/K)$ (see §5) over a dihedral extension of number fields. To be precise, an extension F/k is *dihedral* if $k \subset K \subset F$ is a tower of number fields with K/k quadratic, F/k Galois, F/K p-power abelian, and a lift of the non-trivial element $c \in \mathrm{Gal}(K/k)$ acts on each $\sigma \in \mathrm{Gal}(F/K)$ as $c\sigma c^{-1} = \sigma^{-1}$. They prove (under mild assumptions, see [9, §7]) that the growth in the $\mathbb{Z}_p$-corank of $\mathrm{Sel}_{p^\infty}(E/)$ over F/K must be at least $[F : K]$.

Here, we consider a more general context for the theory of local constants. In particular, we replace the elliptic curve E/k with a pair $(X/k, \lambda)$ of an abelian variety X/k and a polarization $\lambda : X \to X^\vee$ on X of degree prime to p, where $X^\vee$ is the dual abelian variety. We consider the ring of integers $\mathcal{O}$ of a number field $\mathbb{K}$, and assume $\mathcal{O} \subset \mathrm{End}_K(X)$ is contained in the ring of endomorphisms of X defined over K. The case $\mathcal{O} = \mathbb{Z}$ and $\mathbb{K} = \mathbb{Q}$ is that of Mazur and Rubin in [9]. Recent work of Seveso [15] addresses similar questions for abelian varieties with real multiplication.

2010 Mathematics Subject Classification: primary: 11G05, 11G10; secondary: 11G07, 11G15

The condition that X has a polarization degree prime to p implies that many of the constructions of [9] generalize verbatim[1], with E replaced by X. The goal in the present work is, in particular, to generalize Theorem 6.4 of [9] in the case that the endomorphism ring of X is strictly larger than $\mathbb{Z}$.

As a motivating example, consider p an odd rational prime, $X = E$ an elliptic curve defined over $\mathbb{Q}$ with complex multiplication by the ring of integers $\mathcal{O}$ of a quadratic imaginary field $\mathbb{K}$ in which p does not split, and set $K = \mathbb{K}$. The $\mathbb{Z}_p$-corank of $\mathrm{Sel}_{p^\infty}(E/K)$ would be even, so E would not satisfy the hypotheses of Theorem 7.2 of [9] and hence one does not obtain a lower bound for the $\mathbb{Z}_p$-corank of $\mathrm{Sel}_{p^\infty}(E/F)$. One needs to consider $\mathrm{Sel}_{p^\infty}(E/F)$ as a module over $\mathcal{O} \otimes \mathbb{Z}_p$ in order to obtain any useful generalization of the main tool (Theorem 6.4 of [9]) in the proof of Theorem 7.2 of [9].

1.1. Notation and assumptions

Before continuing, we introduce some notation and assumptions that will be used until §6.1, where we will ease the restrictions on F/K.

Fix an odd rational prime p. The tower $k \subset K \subset F$ is as above, with K/k quadratic, F/K an abelian p-extension, and F/k dihedral. Also, X/k and $\mathcal{O} \subset \mathrm{End}_K(X)$ are as above, and we denote the cohomology groups $H^i(\mathrm{Gal}(\bar{K}/K), X(\bar{K}))$ by $H^i(K, X)$. Define a set $\mathfrak{S}_F$ of primes v of K by

$$\mathfrak{S}_F := \{v \mid p, \text{ or } v \text{ ramifies in } F/K, \text{ or where } X/K \text{ has bad reduction}\},$$

and define $\mathfrak{S}_L$ similarly for intermediate fields $K \subset L \subset F$. For a cyclic extension L/K contained in F, define A_L to be the twist of X, in the sense of [10], associated to L/K (see §3 below).

We assume that our prime p is unramified in $\mathcal{O} \subset \mathrm{End}_K(X)$ and we denote $\mathbb{K}_\mathfrak{p}$ and $\mathcal{O}_\mathfrak{p}$ for the local field and ring, respectively, at a prime $\mathfrak{p}$ of $\mathcal{O}$ above p. For each prime v of K we fix an extension of v to $\bar{K}$, which in turn fixes an embedding of $\bar{K}$ into an algebraic closure of K_v and a decomposition subgroup $G_{K_v} = \mathrm{Gal}(\bar{K}_v/K_v) \subset G_K$.

We fix a polarization $\lambda : X \to X^\vee$ on X of degree prime to p, thus fixing an isogeny $\lambda \in \mathrm{Hom}(X, X^\vee)$ which has an inverse in $\lambda^{-1} \in \mathrm{Hom}(X^\vee, X) \otimes \mathbb{Q}$. Associated to λ is the Rosati involution on $\mathrm{End}(X) \otimes \mathbb{Q}$, given by

$$\alpha \mapsto \alpha^\dagger := \lambda^{-1} \circ \alpha^\vee \circ \lambda,$$

where $\alpha^\vee$ is the dual of α. This in particular satisfies,

$$\mathrm{e}_{\ell,\lambda}(\alpha a, a') = \mathrm{e}_{\ell,\lambda}\left(a, \alpha^\dagger a'\right),$$

where $e_{\ell,\lambda}(\cdot,\cdot) = e_\ell(\cdot, \lambda(\cdot))$ is the Weil pairing and $a, a' \in T_\ell(X) \otimes \mathbb{Q}$ (see [11, §16-17]).

We assume that the non-trivial element $c \in \mathrm{Gal}(K/k)$ acts as the Rosati involution on $\mathcal{O} \subset \mathrm{End}_K(X) \otimes \mathbb{Q}$, and that $\mathcal{O}$ is taken to itself by the Rosati involution, i.e. $\mathcal{O}^c = \mathcal{O}^\dagger = \mathcal{O}$.

[1] see subsection "Generalizations" in [9, §1]

Remark 1.1. Suppose $X = E$ is an elliptic curve defined over k with complex multiplication by $\mathcal{O} \subset \mathbb{K}$ and $\mathcal{O} \subset \mathrm{End}_K(E)$. We know that the Rosati involution is the automorphism of $\mathcal{O} \otimes \mathbb{Q} = \mathbb{K}$ of order 2. If $\mathbb{K} \not\subseteq k$, then $k\mathbb{K} = K$ and so the action of the Rosati involution and $c \in \mathrm{Gal}(K/k)$ on $\mathcal{O}$ must coincide.

1.2. Main results

With the above discussion in mind, the goal in the following is to keep track of the extra endomorphisms of the variety X/k. Effectively this amounts to extending the base ring (from $\mathbb{Z}_p$ to $\mathcal{O} \otimes \mathbb{Z}_p$) for the p^∞-Selmer module, and as such the main results address this base extension.

In §2 we address the important properties, for our purposes, of torsion $\mathcal{O}$-modules, noting Proposition 2.8 for those modules equipped with a certain biliear form. In §3 we extend the results of [9] regarding Selmer structures and duality, and in §4 we apply those results to obtain information about the $\mathcal{O}/p\mathcal{O}$-rank of the relevant modules (as in §2 of [9]). This, in particular, motivates a generalized definition (in §6) of the arithmetic local constant δ_v, and combining §2-§4 in §5 leads to our main result, Theorem 6.2.

As an application, in §6.1 we are able to address another generalization mentioned in the introduction of [9]. In particular, we will consider dihedral towers $k \subset K \subset F$ where $[F : K]$ is not a prime power. For example, suppose $[F : K]$ is divisible by two distinct odd primes p, q and L/K is a cyclic extension contained in F. Then we have a p-power extension M/K and a q-power extension M'/K in L (one of these may be trivial) such that $M \cap M' = K$ and $L = MM'$. We can apply Theorem 6.2 for X, A_M, and the (p-power) dihedral extension M/k and then separately for A_M, A_L, and a (q-power) dihedral extension M'/k. Assuming Conjecture 6.6, we can combine this information to compare X and A_L.

In addition to applications to growth in p-Selmer rank, it would be interesting to compare the individual δ_v to a quotient of the local root numbers for the L-function associated to X, as in [3]. We leave this question to future work.

2. Torsion $\mathcal{O}$-modules

In this section we consider various $\mathcal{O}$-modules, and so we prove some general results before applying them to our specific situation. Our abelian variety X and the associated cohomology groups $H^i(K, X)$ are the basic examples of $\mathcal{O}$-modules to keep in mind.

As $\mathcal{O}/p\mathcal{O}$ may not be an integral domain, one does not have a natural definition of the $\mathcal{O}/p\mathcal{O}$-rank of an $\mathcal{O}/p\mathcal{O}$-module via its fraction field (since there would be no such field). However, since $p\mathcal{O} = \prod_i \mathfrak{p}_i$ with $\mathfrak{p}_i \neq \mathfrak{p}_j$ when $i \neq j$, one has

$$\mathcal{O}/p\mathcal{O} \cong \oplus_i (\mathcal{O}/\mathfrak{p}_i)$$

induced by the natural $\mathcal{O} \to \oplus_i(\mathcal{O}/\mathfrak{p}_i)$ maps.[2] Thus, $\mathcal{O}/p\mathcal{O}$ is a direct sum of fields $\mathcal{O}/\mathfrak{p}_i$, and each of these is a finite extension of $\mathbb{F}_p$.

[2] Alternatively, one has $\mathcal{O}/p\mathcal{O} = \mathcal{O} \otimes_{\mathbb{Z}} (\mathbb{Z}/p\mathbb{Z})$ and that $\mathcal{O}$ is a torsion-free, hence flat, $\mathbb{Z}$-module (see [7, §XVI.3]), which yields the same decomposition.

Definition 2.1. Set $R = \mathcal{O}/p\mathcal{O}$ and $R_i = \mathcal{O}/\mathfrak{p}_i$, so $R \cong \oplus_{i=1}^m R_i$. For any R-module M of finite type, define the *R-rank* of M to be

$$\mathrm{rank}_R M := (\ldots, \dim_{R_i} M \otimes_R R_i, \ldots) \in \mathbb{Z}^m.$$

We say $a = (a_1, \ldots, a_m) \in \mathbb{Z}^m$ is *even* if a_i is even for each i.

A first, and most important, property of this definition of R-rank is that it behaves as one expects with respect to short exact sequences. We will exploit this property frequently. The proof of this and the subsequent Lemma are left as exercises for the reader.

Proposition 2.2. *If $0 \to M_1 \to M_2 \to M_3 \to 0$ is a short exact sequence of R-modules then*

$$rank_R M_2 = rank_R M_1 + rank_R M_3.$$

Lemma 2.3. *If M is an $\mathcal{O}/p\mathcal{O}$-module of finite type (i.e. M is p-torsion as an $\mathcal{O}$-module) then $M \otimes_R (\mathcal{O}/\mathfrak{p}) \cong M[\mathfrak{p}]$.*

For any R-module M, we denote $M^\dagger$ for the R-module which has the same underlying set as M, but with R-action given by $rm := r^\dagger m$. Also, for any abelian group Γ, we denote $\mathrm{Hom}(M, \Gamma) := \mathrm{Hom}_{\mathbb{Z}}(M, \Gamma)$ for the R-module of group homomorphisms from M to Γ, with the R-action on $\mathrm{Hom}(M, \Gamma)$ given by $(rf)(x) = f(rx)$.

Lemma 2.4. *Suppose M is an R-module and $\mathfrak{c} : M \xrightarrow{\sim} M$ is an isomorphism of groups with $\mathfrak{c}(rm) = r^\dagger \mathfrak{c}(m)$. Then $M \cong M^\dagger$ as R-modules and in particular $rank_R M = rank_R M^\dagger$.*

Proof. The isomoprhism $\mathfrak{c}$ induces an R-isomorphism, since $\mathfrak{c}(rm) = r^\dagger \mathfrak{c}(m)$. ∎

Lemma 2.5. *$rank_R R_t = rank_R Hom(R_t^\dagger, \mathbb{F}_p)^\dagger$, for each $t \in \{1, \ldots, m\}$.*

Proof. By Definition 2.1,

$$\begin{aligned} \mathrm{rank}_R R_t &= (\ldots, \dim_{R_j} R_t \otimes_R R_j, \ldots) \\ &= (0, \ldots, \dim_{R_t} R_t, \ldots, 0), \\ \mathrm{rank}_R \mathrm{Hom}(R_t, \mathbb{F}_p)^\dagger &= (\ldots, \dim_{R_j} \mathrm{Hom}(R_t, \mathbb{F}_p)^\dagger \otimes_R R_j, \ldots). \end{aligned}$$

Since $\mathrm{Hom}(R, \mathbb{F}_p)^\dagger$ is an $\mathcal{O}/p\mathcal{O}$-module, we can use Lemma 2.3 to obtain

$$\dim_{R_j} \mathrm{Hom}(R_t, \mathbb{F}_p)^\dagger \otimes_R R_j = \dim_{R_j} \mathrm{Hom}(R_t, \mathbb{F}_p)^\dagger[\mathfrak{p}_j], \tag{2.1}$$

and we claim that

$$\dim_{R_j} \mathrm{Hom}(R_t, \mathbb{F}_p)^\dagger[\mathfrak{p}_j] = \left\{ \begin{array}{ll} 0 & \text{when } R_t \neq R_j^\dagger \\ 1 & \text{when } R_t = R_j^\dagger \end{array} \right\} \tag{2.2}$$

Consider $f \in \mathrm{Hom}(R_t, \mathbb{F}_p)^\dagger[\mathfrak{p}_j]$, with $R_t \neq R_j^\dagger$. If $f(r^\dagger x) = 0$ for all $x \in R_t$ and all $r^\dagger \in \mathfrak{p}_j^\dagger$ then f is the zero map, since there exists some $r^\dagger \in \mathfrak{p}_j^\dagger$ such that $r^\dagger \notin \mathfrak{p}_t$ and hence $r^\dagger R_t = R_t$. When $R_t = R_j^\dagger$, we have $r^\dagger x = 0$ for all $x \in R_t$, and so $f(r^\dagger x) = 0$ is satisfied for every $f \in \mathrm{Hom}(R_j^\dagger, \mathbb{F}_p)^\dagger[\mathfrak{p}_j]$, and this set has R_j-dimension 1.

Now consider $R_t \neq R_s$. Then viewing $R_t \otimes_R R_s$ either as $R_t[\mathfrak{p}_s]$ or $R_s[\mathfrak{p}_t]$ shows that $R_t \otimes_R R_s$ is trivial, and hence has rank 0. When $R_t = R_s$, we have $R_t \otimes_R R_t = R_t$. From this and (2.2), we obtain $\dim_R R_t = \dim_R \mathrm{Hom}(R_t^\dagger, \mathbb{F}_p)^\dagger$. ■

Remark 2.6. Alternatively, one can prove Lemma 2.5 as follows. Define a perfect pairing $(\ ,\ ) : R_t \times R_t^\dagger \to \mathbb{F}_p$ via $(x, y) \mapsto \mathrm{Tr}_{R_t/\mathbb{F}_p}(xy^\dagger)$. This pairing satisfies $(rx, y) = (x, r^\dagger y)$ and hence gives an R_t-module isomoprhism $R_t \cong \mathrm{Hom}(R_t^\dagger, \mathbb{F}_p)^\dagger$.

Corollary 2.7. *If M is an R-module of finite type, then*

$$rank_R M = rank_R Hom(M^\dagger, \mathbb{F}_p)^\dagger.$$

Proof. This follows from the Lemma and $M \cong \oplus_t R_t^{n_t}$. ■

The next proposition is analogous to a well-known theorem for alternating pairings on vector spaces. Specifically, if k is a field with $\mathrm{char}(k) \neq 2$ and there is a non-degenerate, skew-symmetric pairing on a finite dimensional k-vector space V, then $\dim_k V$ is even (see [7, §XV.8] or [12, §9.5]).

Proposition 2.8. *Suppose A is a commutative ring, char$(A) \neq 2$, and $A \cong \oplus_{j=1}^n A_j$, where each A_j is a local ring with principal maximal ideal $\mathfrak{m}_j$. Let M, N be A-modules with M finite and $[\ ,\ ] : M \times M \to N$ be a non-degenerate, skew-symmetric pairing which satisfies $[sx, y] = [x, sy]$ for all $x, y \in M$ and $s \in A$. Then there exist A-submodules M', M'' with $M' \cong M''$ and $M \cong M' \oplus M''$.*

Proof. Let $M_j = M \otimes A_j$. We first note that $A \cong \oplus_j A_j$ implies $M \cong \oplus M_j$. Since M is finite, we see that $x \in M_j$ implies $x \in M_j[\mathfrak{m}_j^t]$ for some t. For $i \neq j$, $x \in M_j$ and $y \in M_i$, we have that $[x, y] = 0$. Indeed, there is some $\alpha \in \mathfrak{m}_j$ with $\alpha x = 0$ which acts as a unit on M_i. Thus, there is some $y' \in M_i$ with $\alpha y' = y$ and so

$$0 = [\alpha x, y'] = [x, \alpha y'] = [x, y].$$

Now, suppose $x \in M_j$ is of maximal order, i.e. that $x \in M_j[\mathfrak{m}_j^t]$ but $x \notin M_j[\mathfrak{m}_j^{t-1}]$ and that t is maximal. Let π be a generator of $\mathfrak{m}_j$ in A_j. Since $\pi^{t-1} x \neq 0$ there is some $y \in M_j$ such that $[\pi^{t-1} x, y] \neq 0$. We then have $0 \neq [\pi^{t-1} x, y] = [x, \pi^{t-1} y]$ and so $\pi^{t-1} y \neq 0$. In particular, this implies that $y \notin M_j[\mathfrak{m}_j^{t-1}]$ and $y \in M_j[\mathfrak{m}_j^t]$, since x was chosen to be of maximal order. Moreover, we have that $\mathrm{span}_{A_j} \{x\} \cong \mathrm{span}_{A_j} \{y\}$. We also note that if $w = ax$ for some $a \in A$ then

$$[x, w] = [x, ax] = [ax, x] = [w, x]$$

and so $[x, w] = 0$.

Set $U := \mathrm{span}_{A_j}\{x, y\}$. We claim that $U \cap U^\perp = \{0\}$. Let $z \in U \cap U^\perp$ with $z = ax + by$ for some $a, b \in A_j$, and suppose that $a \neq 0$. Since A_j is a local ring, we have $\pi^t \nmid a$, so $a \mid \pi^{t-1}$. So, we can find $a' \in A_j$ such that $aa' = \pi^{t-1}$. Now, for $w = a'y$ we have

$$[z, w] = [ax + by, a'y] = [ax, a'y] = [(aa')x, y] = [\pi^{t-1}x, y] \neq 0,$$

contradicting $z \in U^\perp$. In the same way we can see that if $\pi^t \nmid b$ then we can find $w \in U$ such that $[z, w] \neq 0$.

We are now left with the case that $\pi^t \mid a$ and $\pi^t \mid b$. Since x was chosen to be of maximal order, this forces $z = 0$ and it follows that $U \cap U^\perp = \{0\}$. Also, the above argument shows that $U \cong A_j x \oplus A_j y$. The finiteness of M (and hence M_j) then implies that we can decompose M_j as $M_j = U \oplus U^\perp$ and by induction we obtain the claim. ∎

Remark 2.9. Recall that $R = \mathcal{O}/p\mathcal{O}$, $R_j = \mathcal{O}/\mathfrak{p}_j$, and set $S = \mathcal{O} \otimes \mathbb{Z}_p$ and $S_j = \mathcal{O}_{\mathfrak{p}_j}$. We have decompositions $R \cong \oplus_j R_j$ and $S \cong \oplus_j S_j$. For $\mathcal{R}_L := R_L \otimes \mathbb{Z}_p$, where R_L is as in §3 of [9] (see also §3 below), we again have a decomposition $\mathcal{O} \otimes \mathcal{R}_L \cong \oplus_j (\mathcal{O}_{\mathfrak{p}_j} \otimes R_L)$. In what follows, these rings will play the role of A in the above proposition.

3. Selmer structures and Tate duality

As our goal is to establish a theorem analogous to Theorem 6.4 of [9], we need to generalize the results of [9] regarding the pairing of Tate's local duality in order to yield information about the Selmer structures of Definition 3.3 as $\mathcal{O}$-modules.

Using Definition 3.3 of [9] (see also Definition 1.1 of [10]), we have the $\mathcal{I}$-twist A of X exactly as in the elliptic curve case $X = E$. Specifically, for a cyclic extension L/K contained in F, let ρ_L denote the unique faithful irreducible rational representation of $\mathrm{Gal}(L/K)$. Define the $\mathcal{I}_L$-twist of X to be $A_L := \mathcal{I}_L \otimes X$, where

$$\mathcal{I}_L := \mathbb{Q}[\mathrm{Gal}(F/K)]_L \cap \mathbb{Z}[\mathrm{Gal}(F/K)]$$

and $\mathbb{Q}[\mathrm{Gal}(F/K)]_L$ is the sum of all (left) ideals of $\mathbb{Q}[\mathrm{Gal}(F/K)]$ isomorphic to ρ_L. We define the ring R_L (mentioned in Remark 2.9) as the maximal order of $\mathbb{Q}[\mathrm{Gal}(F/K)]_L$, and when $[L : K] = p^m$ we have that $R_L \cong \mathbb{Z}[\mu_{p^m}]$ has a unique prime above p.

Remark 3.1. By definition (in [10]), when $\mathcal{I}_L$ is a $\mathbb{Z}$-module, the twist $A_L = \mathcal{I}_L \otimes X$ is a $\mathbb{Z}$-module. However, we may regard it as an $\mathcal{O}$-module, simply by letting $\mathcal{O}$ act on $\mathcal{I}_L \otimes X$ via its action on X. The resulting module coincides with the $\mathcal{O}$-module $\mathcal{I}'_L \otimes X$ obtained by twisting X with the $\mathcal{O}$-module

$$\mathcal{I}'_L := \mathbb{K}[\mathrm{Gal}(F/K)]_L \cap \mathcal{O}[\mathrm{Gal}(F/K)].$$

Proposition 3.2. *For $\hat{p}$ the unique prime above p in $\mathcal{I}_L$, there is a canonical $Gal(\bar{K}/K)$-isomorphism $A_L[\hat{p}] \cong X[p]$.*

Proof. This is exactly as in Proposition 4.1 of [9] (also Remark 4.2 in [9]), where our $\hat{p}$ is their $\mathfrak{p} = \mathfrak{p}_L$. ■

We are concerned with the following Selmer structures, analogous to those of §2 and §4 of [9].

Definition 3.3. Define a Selmer structure $\mathcal{X}$ on $X[p]$ as the collection of $\mathcal{O}$-modules $H^1_{\mathcal{X}}(K_v, X[p])$, defined to be, for each v, the image of

$$X(K_v)/pX(K_v) \hookrightarrow H^1(K_v, X[p]).$$

Fix a generator π of $\hat{p}$, with $\hat{p}$ as in Proposition 3.2. Define a Selmer structure $\mathcal{A}$ on $X[p]$ by setting, for each v, $H^1_{\mathcal{A}}(K_v, X[p])$ to be the image of

$$A_L(K_v)/\pi A_L(K_v) \hookrightarrow H^1(K_v, A_L[\hat{p}]) \cong H^1(K_v, X[p]).$$

We note that the image in $H^1(K_v, X[p])$ is independent of the choice of our generator. As in [9, §1], define

$$H^1_{\mathcal{X}+\mathcal{A}}(K_v, X[p]) := H^1_{\mathcal{X}}(K_v, X[p]) + H^1_{\mathcal{A}}(K_v, X[p])$$
$$H^1_{\mathcal{X}\cap\mathcal{A}}(K_v, X[p]) := H^1_{\mathcal{X}}(K_v, X[p]) \cap H^1_{\mathcal{A}}(K_v, X[p]).$$

Definition 3.4. We say that a Selmer structure $\mathcal{F}$ on $X[p]$ is *self-dual* if for every prime v, $H^1_{\mathcal{F}}(K_v, [X[p])$ is its own orthogonal complement under the pairing of Tate's local duality:

$$\langle\ ,\ \rangle_v : H^1(K_v, X[p]) \times H^1(K_v, X[p]) \to H^2(K_v, \boldsymbol{\mu}_p) = \mathbb{F}_p. \tag{3.1}$$

We note that in Definition 3.4, we are making use of our assumption that X has a polarization of degree prime to p in order to have (3.1) as a *self*-pairing.

Definition 3.5. Given a Selmer structure $\mathcal{F}$ on $X[p]$, define the *Selmer group* to be

$$H^1_{\mathcal{F}}(K, X[p]) := \ker H^1(K, X[p]) \to \prod_v H^1(K_v, X[p])/H^1_{\mathcal{F}}(K_v, X[p]).$$

Thus, $H^1_{\mathcal{F}}(K, X[p])$ is the set of classes whose localizations are in $H^1_{\mathcal{F}}(K_v, X[p])$, or in other words the classes satisfying the local conditions defined by $\mathcal{F}$.

Proposition 3.6. *The Selmer structures $\mathcal{X}$ and $\mathcal{A}$ on $X[p]$ are self-dual.*

Proof. The Tate pairing is the same as that in [9], and Tate local duality holds for a general abelian variety (see [9, §1.4]). This shows that $\mathcal{X}$ is self-dual. For $\mathcal{A}$, the proof is exactly Proposition A.7 of Appendix A of [9], noting that we need only regard A_L as a $\mathbb{Z}$-module here. ■

The pairing (3.1) is not $\mathcal{O}$-linear, but understanding the interplay of the pairing and the map induced by c on the local cohomology groups $H^1(K_v, X[p])$ provides information (see Lemma 4.4 below) about the R-rank of certain Selmer groups.

Now, we fix a lift of the nontrivial element $c \in \mathrm{Gal}(K/k)$ to $\mathrm{Gal}(\bar{K}/k)$, which we also denote c. As $c \in G_k$ with $c(K) = K$, we have that $c : K_v \xrightarrow{\sim} K_{v^c}$. The maps $c : G_K \to G_K : \ s \mapsto c^{-1}sc$ and $c : M \to M : \ a \mapsto c(a)$, for any G_k-module M, are compatible in the sense of [14, §VII.5], and hence induce $c^* : H^*(K, M) \to H^*(K, M)$ on cohomology. Similarly, from $c : G_{K_v} \to G_{K_{v^c}}$ we obtain $c^* : H^*(G_{K_{v^c}}, M) \to H^*(G_{K_v}, M)$.

Lemma 3.7. *For G_k-module M, the map $c^* : H^1(G_K, M) \to H^1(G_K, M)$ induced by the lift $c \in G_k$ of c is independent of the choice of lift.*

Proof. The claim follows from a special case of Proposition 3 of §VII.5 of [14]. ■

Lemma 3.8. *Let M and N be two G_k-modules and $\phi : M \to N$ a G_k-equivariant map. Then for the map $\phi^* : H^*(K, M) \to H^*(K, N)$ induced by ϕ,*

$$\phi^* \circ c^* = c^* \circ \phi^* : H^*(K_{v^c}, M) \to H^*(K_v, N).$$

Proof. Let $G = \mathrm{Gal}(\bar{K}_v/K_v)$ and $G' = \mathrm{Gal}(\bar{K}_{v^c}/K_{v^c})$. We prove the claim on cochains. For each $i \geqslant 0$, let $P_i := \mathbb{Z}[G^{i+1}]$, be the free module generated by elements $(g_0, \ldots, g_i) \in G^{i+1}$, with a G-action by

$$s.(g_0, \ldots, g_i) = (s.g_0, \ldots, s.g_i).$$

These form the standard resolution for $\mathbb{Z}$ (see [14, §VII.3] or [1, §I.5]).

Suppose $f \in \mathrm{Hom}_{G'}(P'_i, M)$. Then

$$\begin{aligned} c^*(f)(g_0, \ldots, g_i) &= c(f(c^{-1}g_0c, \ldots, c^{-1}g_ic)) \\ \phi^*(f)(g_0, \ldots, g_i) &= \phi(f(g_0, \ldots, g_i)), \end{aligned}$$

and it follows that

$$(\phi^* \circ c^*)(f)(g_0, \ldots, g_i) = (c^* \circ \phi^*)(f)(g_0, \ldots, g_i),$$

using the G_k-equivariance of ϕ. ■

Let $W = X[p]$. Denote $e^* : H^*(K, W \otimes W) \to H^*(K, \boldsymbol{\mu}_p)$ for the map induced by the Weil pairing $e_{p,\lambda}$ on W. We will also use e^* for the maps induced by $e_{p,\lambda}$ on G_{K_v}-cohomology and $G_{K_{v^c}}$-cohomology, and context will make the notation clear. We know that $e_{p,\lambda}$ is $\mathrm{Gal}(\bar{K}/k)$-equivariant (see [16, §III.8] or [11, §12]). By Lemma 3.8, we see that

$$e^* \circ c^* = c^* \circ e^* : H^*(K_{v^c}, W \otimes W) \to H^*(K_v, \boldsymbol{\mu}_p).$$

Proposition 3.9. *Suppose S is a finite set of primes v of K such that $v \in S$ if and only if $v^c \in S$. For any a, $b \in \oplus_{v \in S} H^1(K_v, W)$, let $\langle a, b\rangle := \sum_{v \in S} \langle a_v, b_v\rangle_v$. Then*

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

Proof. Recall that $\langle\ ,\ \rangle_v$ is defined via the composition (cf. [13, §1.4])

$$\begin{array}{ccccc} H^1(K_v,W)\otimes H^1(K_v,W) & & & & \\ \downarrow \cup & & & & \\ H^2(K_v,W\otimes W) & \xrightarrow{e^*} & H^2(K_v,\boldsymbol{\mu}_p) & \xrightarrow{\mathrm{inv}_v} & \boldsymbol{\mu}_p. \end{array}$$

The cup product $\cup$ is functorial, so the commutative diagram

$$\begin{array}{ccccc} H^1(K_{v^c},W) & \otimes & H^1(K_{v^c},W) & \xrightarrow{\cup} & H^2(K_{v^c},W\otimes W) \\ \downarrow{\scriptstyle c^*} & & \downarrow{\scriptstyle c^*} & & \downarrow{\scriptstyle c^*} \\ H^1(K_v,W) & \otimes & H^1(K_v,W) & \xrightarrow{\cup} & H^2(K_v,W\otimes W) \end{array}$$

implies $a\cup c^*(b)=c^*c^*(a)\cup c^*(b)=c^*(c^*(a)\cup b)$. Also we can see that, for all $i\geqslant 0$,

$$\begin{array}{ccc} H^i(K,W) & \xrightarrow[c^*]{\sim} & H^i(K,W) \\ \downarrow{\scriptstyle \mathrm{res}_{v^c}} & & \downarrow{\scriptstyle \mathrm{res}_v} \\ H^i(K_{v^c},W) & \xrightarrow[c^*]{\sim} & H^i(K_v,W). \end{array}$$

commutes by recalling that on cochains $\mathrm{res}_v(f)$ is restriction of the map f. Using Lemma 3.8 and the property $\mathrm{inv}_v\circ c^*=\mathrm{inv}_{v^c}$ (see [14, §§XI.1-XI.2], particularly Proposition 1) of the local invariant map, we see $\langle a,c^*(b)\rangle=\langle c^*(a),b\rangle$. ∎

The next proposition shows how the R-action on our cohomology groups interacts with the pairing (3.1).

Proposition 3.10. *For any a, $b\in H^1(K_v,X[p])$ and $r\in R$, $\langle ra,b\rangle_v=\langle a,r^\dagger b\rangle_v$.*

Proof. Let $W=X[p]$ as above, and let $x,y\in W$ and $r\in\mathcal{O}$. The claim is a consequence of the identity $\mathrm{e}_{p,\lambda}(rx,y)=\mathrm{e}_{p,\lambda}\left(x,r^\dagger y\right)$. As $e_{p,\lambda}$ is bilinear, it can be viewed as a map on $W\otimes_{\mathbb{Z}}W$, and the above property becomes $\mathrm{e}_{p,\lambda}(rx\otimes y)=\mathrm{e}_{p,\lambda}\left(x\otimes r^\dagger y\right)$. Now, for $a,b\in H^1(K_v,W)$ we have r and $r^\dagger$ acting by $(ra)(g)=r.a(g)$ and $(r^\dagger b)(g)=r^\dagger.b(g)$. Thus, keeping in mind that $\mathcal{O}\subset\mathrm{End}_K(X)$, it follows that

$$\begin{aligned} e^*((ra)\cup b)(g,h) &= \mathrm{e}_{p,\lambda}\left(((ra)\cup b)(g,h)\right) \\ &= \mathrm{e}_{p,\lambda}\left((a\cup(r^\dagger b))(g,h)\right) \\ &= e^*_{p,\lambda}((a\cup(r^\dagger b))(g,h), \end{aligned}$$

and so

$$\begin{aligned} \langle ra,b\rangle_v &= \mathrm{inv}_v\circ e^*_{p,\lambda}((ra)\cup b) \\ &= \mathrm{inv}_v\circ e^*_{p,\lambda}(a\cup(r^\dagger b))=\langle a,r^\dagger b\rangle_v. \end{aligned}$$

∎

Corollary 3.11. *The orthogonal complement of* $H^1(K_v, X[p])[\mathfrak{p}]$ *under* (3.1) *is* $\oplus_{\mathfrak{q}\neq\mathfrak{p}^\dagger} H^1(K_v, X[p])[\mathfrak{q}]$.

Proof. Set $M = H^1(K_v, X[p])$. Let $a \in M[\mathfrak{p}]$, $b \in M$, and $r \in \mathfrak{p}$. Then

$$0 = \langle 0, b\rangle_v = \langle ra, b\rangle_v = \langle a, r^\dagger b\rangle_v,$$

so $r^\dagger M \subset M[\mathfrak{p}]^\perp$ and in turn $\mathfrak{p}^\dagger M \subset M[\mathfrak{p}]^\perp$. Since $M = \oplus_{\mathfrak{q}|p} M[\mathfrak{q}]$, we see that $\mathfrak{p}^\dagger M = \oplus_{\mathfrak{q}\neq\mathfrak{p}^\dagger} M[\mathfrak{q}] \subset M[\mathfrak{p}]^\perp$, and non-degeneracy finishes the claim. ∎

4. $\mathcal{O}/p\mathcal{O}$-rank

Recall $\mathfrak{S}_L$ is a finite set of primes of K containing those which divide p or are ramified in L/K or where X does not have good reduction. In this section we fix a cyclic extension L/K contained in F.

Lemma 4.1. *For* $v \notin \mathfrak{S}_L$, *the Selmer structures* $\mathcal{X}$ *and* $\mathcal{A}$ *on* $X[p]$ *coincide.*

Proof. This is Corollary 4.6 of [9], which uses Lemma 19.3 of [2]. Specifically, both $\mathcal{X}$ and $\mathcal{A}$ are self-dual (cf §3) and when $v \notin \mathfrak{S}_L$ then both $T_p(X)$ and $T_p(A_L)$ are unramified at v. Thus,

$$H^1_{\mathcal{X}}(K_v, X[p]) = H^1_{\mathcal{A}}(K_v, X[p]) = H^1(K_v^{ur}/K_v, X[p]).$$ ∎

Let $R = \mathcal{O}/p\mathcal{O}$ and $R_i = \mathcal{O}/\mathfrak{p}_i$ be as in the previous section. We now generalize the main results of §1 of [9] regarding self-dual Selmer structures. Later, determining the difference in the $(\mathcal{O}\otimes\mathbb{Z}_p)$-corank of the p^∞-Selmer groups associated to $\mathcal{X}$ and $\mathcal{A}$ will be reduced to determining the difference in the R-corank of the p-Selmer groups, and Theorem 4.5 below describes the latter. We phrase the result specifically in terms of the Selmer structures $\mathcal{X}$ and $\mathcal{A}$, as we make use of the assumption on c introduced in the beginning of §1 to prove Lemma 4.3.

Remark 4.2. The following is an example of an application of Lemma 2.4. Set $W = X[p]$ and

$$B = \bigoplus_{v\in\mathfrak{S}_L} (H^1_{\mathcal{X}+\mathcal{A}}(K_v, W)/H^1_{\mathcal{X}\cap\mathcal{A}}(K_v, W)).$$

We check that $v \in \mathfrak{S}_L$ if and only if $v^c \in \mathfrak{S}_L$. Since $c \in \mathrm{Gal}(K/k)$, we have $v \mid p$ implies $v^c \mid p$. Also, if w witnesses that v is ramified in L/K then w^c witnesses that v^c is ramified in L/K. Lastly, since X is defined over k, X has good reduction at v if and only if X has good reduction at v^c.

The automorphism c induces an isomorphism $X(K_v) \xrightarrow{\sim} X(K_{v^c})$ and in turn $H^1(K_v, W) \xrightarrow{\sim} H^1(K_{v^c}, W)$. This restricts to a group isomorphism

$$H^1_{\mathcal{X}}(K_v, W) \xrightarrow{\sim} H^1_{\mathcal{X}}(K_{v^c}, W).$$

We have analogous isomorphisms for $H^1_{\mathcal{A}}(K_v, W)$. As B is a direct sum taken over all $v \in \mathfrak{S}_L$, we know that $H^1_{\mathcal{X}+\mathcal{A}}(K_v, W)$ and $H^1_{\mathcal{X}+\mathcal{A}}(K_{v^c}, W)$ occur symmetrically in B. Thus,

$$\begin{aligned} B &= \bigoplus_{v \in \mathfrak{S}_L} (H^1_{\mathcal{X}+\mathcal{A}}(K_v, W)/H^1_{\mathcal{X}\cap\mathcal{A}}(K_v, W)) \\ &\cong \bigoplus_{v^c \in \mathfrak{S}_L} (H^1_{\mathcal{X}+\mathcal{A}}(K_{v^c}, W)/H^1_{\mathcal{X}\cap\mathcal{A}}(K_{v^c}, W)) = B \end{aligned}$$

and so $c : B \xrightarrow{\sim} B$. Lemma 2.4 then gives $\mathrm{rank}_R B = \mathrm{rank}_R B^\dagger$.

Recall the definition of a Selmer group, e.g. $H^1_{\mathcal{X}}(K, X[p])$, in Definition 3.5. The following Lemmas generalize Proposition 1.3 of [9].

Lemma 4.3. *Since $\mathcal{X}$ and $\mathcal{A}$ are self-dual,*

$$\begin{aligned} &\mathit{rank}_R H^1_{\mathcal{X}+\mathcal{A}}(K, X[p])/H^1_{\mathcal{X}\cap\mathcal{A}}(K, X[p]) \\ &\qquad = \sum_{v \in S} \mathit{rank}_R(H^1_{\mathcal{X}}(K_v, X[p])/H^1_{\mathcal{X}\cap\mathcal{A}}(K_v, X[p])). \end{aligned}$$

Proof. We follow the ideas of Proposition 1.3 of [9], noting the adjustments needed to address R-rank. Let W and B be as in Remark 4.2. The Tate pairing restricts to $H^1_{\mathcal{X}+\mathcal{A}}(K_v, W)$ for each v, and since $\mathcal{X}$ and $\mathcal{A}$ are self-dual we obtain a pairing $\langle\ ,\ \rangle : B \times B \to \mathbb{F}_p$.

Defining $C_{\mathcal{X}}$ (resp. $C_{\mathcal{A}}$) to be the projection of $\oplus_v H^1_{\mathcal{X}}(K_v, W)$ (resp. $\oplus_v H^1_{\mathcal{A}}(K_v, W)$) in B, the local self-duality of $\mathcal{X}$ (resp. $\mathcal{A}$) implies that $C_{\mathcal{X}}$ (resp. $C_{\mathcal{A}}$) is its own orthogonal complement under $\langle\ ,\ \rangle$. Using these orthogonality relations, we will show

$$\mathrm{rank}_R C = \mathrm{rank}_R C_{\mathcal{X}} = \mathrm{rank}_R C_{\mathcal{A}} = \frac{1}{2}\mathrm{rank}_R B. \tag{4.1}$$

First we note $B = C_{\mathcal{X}} \oplus C_{\mathcal{A}}$, and since $C_{\mathcal{X}}^\perp = C_{\mathcal{X}}$ and $C_{\mathcal{A}}^\perp = C_{\mathcal{A}}$, the pairing $\langle\ ,\ \rangle$ restricts to a non-degenerate pairing on $C_{\mathcal{X}} \times C_{\mathcal{A}}$. From this we obtain in the usual way (see [7, §I.9] or [7, §XIII.5]) an R-isomorphism $C_{\mathcal{X}} \to \mathrm{Hom}(C_{\mathcal{A}}, \mathbb{F}_p)^\dagger$ which implies

$$\mathrm{rank}_R C_{\mathcal{X}} = \mathrm{rank}_R \mathrm{Hom}(C_{\mathcal{A}}, \mathbb{F}_p)^\dagger = \mathrm{rank}_R C_{\mathcal{A}}^\dagger,$$

using Corollary 2.7 for the right-hand equality. Then by Lemma 2.4, as in Remark 4.2, we see

$$\mathrm{rank}_R C_{\mathcal{X}} = \mathrm{rank}_R C_{\mathcal{A}}^\dagger = \mathrm{rank}_R C_{\mathcal{A}}.$$

Thus, we have the middle and right-hand equalities of (4.1).

Similarly, from $B \times B \to \mathbb{F}_p$ and $C = C^\perp$, we obtain $C \times (B/C) \to \mathbb{F}_p$ which gives

$$\mathrm{rank}_R C = \mathrm{rank}_R \mathrm{Hom}(B/C, \mathbb{F}_p)^\dagger = \mathrm{rank}_R (B/C)^\dagger,$$

and in turn, again by Lemma 2.4, we have $\text{rank}_R C = \text{rank}_R B/C$. Now using the exact sequence (of R-modules)

$$0 \to C \to B \to B/C \to 0$$

and Proposition 2.2, we have

$$\text{rank}_R B = \text{rank}_R C + \text{rank}_R(B/C) = 2\text{rank}_R C,$$

and hence the left-hand equality of (4.1). The result now follows from

$$C \cong H^1_{\mathcal{X}+\mathcal{A}}(K_v, W)/H^1_{\mathcal{X}\cap\mathcal{A}}(K_v, W)$$

and

$$C_{\mathcal{X}} \cong \oplus_v H^1_{\mathcal{X}}(K_v, W)/H^1_{\mathcal{X}\cap\mathcal{A}}(K_v, W). \qquad \blacksquare$$

Lemma 4.4. *With the same assumptions and notation of Lemma 4.3,*

$$rank_R H^1_{\mathcal{X}+\mathcal{A}}(K, W) \equiv rank_R(H^1_{\mathcal{X}}(K, W) + H^1_{\mathcal{A}}(K, W)) \mod 2.$$

Proof. Again, we follow Proposition 1.3 of [9]. For $u \in H^1_{\mathcal{X}+\mathcal{A}}(K, W)$, write $u_s \in C$ for the localization of u, and u_x, u_a for the projections of u_s to $C_{\mathcal{X}}$, $C_{\mathcal{A}}$, respectively. Using the symmetry of $\langle\ ,\ \rangle$, the pairing

$$[\ ,\ ] : H^1_{\mathcal{X}+\mathcal{A}}(K, W) \times H^1_{\mathcal{X}+\mathcal{A}}(K, W) \to \mathbb{F}_p :\ [u, w] := \langle u_x, w_a \rangle$$

is skew-symmetric. Also, exactly as in [9], the kernel of $[\ ,\ ]$ is exactly $H^1_{\mathcal{X}}(K, W) + H^1_{\mathcal{A}}(K, W)$, and so $[\ ,\ ]$ induces an $\mathbb{F}_p$-valued, non-degenerate, skew-symmetric pairing on

$$H := H^1_{\mathcal{X}+\mathcal{A}}(K, W)/(H^1_{\mathcal{X}}(K, W) + H^1_{\mathcal{A}}(K, W)).$$

Since $[\ ,\ ]$ is defined in terms of $\sum_{v\in\mathfrak{S}_L}\langle\ ,\ \rangle_v$, we use Propositions 3.10 and 3.9, respectively, to see that

$$[u, rw] = [r^\dagger u, w] \quad \text{and} \quad [u, c^*(w)] = [c^*(u), w].$$

Define $[\ ,\ ]'$ on H by $[u, w]' := [u, c^*(w)]$. The non-degeneracy and skew-symmetry of $[\ ,\ ]$ imply that $[\ ,\ ]'$ is non-degenerate and skew-symmetric also. In addition, the two properties above imply that $[ru, w]' = [u, rw]'$ and with this pairing Proposition 2.8 (with $A = R$) shows that $\text{rank}_R H$ is even. $\blacksquare$

Theorem 4.5. *Since $\mathcal{X}$ and $\mathcal{A}$ are self-dual,*

$$\begin{aligned} rank_R H^1_{\mathcal{X}}(K, X[p]) - rank_R H^1_{\mathcal{A}}(K, X[p]) \\ \equiv \sum_{v\in S} rank_R(H^1_{\mathcal{X}}(K_v, X[p])/H^1_{\mathcal{X}\cap\mathcal{A}}(K_v, X[p])) \mod 2. \end{aligned}$$

Proof. Applying Lemma 4.1, the claim follows from the congruences

$$\begin{aligned}\operatorname{rank}_R H^1_{\mathcal{X}}(K,X[p]) - \operatorname{rank}_R H^1_{\mathcal{A}}(K,X[p])&\\ \equiv \operatorname{rank}_R H^1_{\mathcal{X}}(K,X[p]) + \operatorname{rank}_R H^1_{\mathcal{A}}(K,X[p])&\\ \equiv \operatorname{rank}_R (H^1_{\mathcal{X}}(K,X[p]) + H^1_{\mathcal{A}}(K,X[p])) + \operatorname{rank}_R H^1_{\mathcal{X}\cap\mathcal{A}}(K,X[p])&\\ \equiv \operatorname{rank}_R H^1_{\mathcal{X}+\mathcal{A}}(K,X[p]) - \operatorname{rank}_R H^1_{\mathcal{X}\cap\mathcal{A}}(K,X[p])&\\ \equiv \sum_{v\in S} \operatorname{rank}_R (H^1_{\mathcal{X}}(K_v,X[p])/\dim H^1_{\mathcal{X}\cap\mathcal{A}}(K_v,X[p])) \mod 2.&\end{aligned}$$

The last two steps follow from Lemmas 4.3 and 4.4. ∎

Remark 4.6. The summands in the right-hand side of Theorem 4.5 motivate Definition 6.1 below of the arithmetic local constants δ_v.

5. *p*-Selmer corank

The p-Selmer group $H^1_{\mathcal{X}}(K,X[p]) = \mathrm{Sel}_p(X/K)$ sits in the exact sequence (see for example [16, §X.4])

$$0 \to X(K)\otimes \mathbb{Z}/p^m\mathbb{Z} \to \mathrm{Sel}_{p^m}(X/K) \to Ш(X/K)[p^m] \to 0 \tag{5.1}$$

and passing to the limit $\mathrm{Sel}_{p^\infty}(X/K)$ sits in

$$0 \to X(K)\otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Sel}_{p^\infty}(X/K) \to Ш(X/K)[p^\infty] \to 0. \tag{5.2}$$

We have similar sequences for $H^1_{\mathcal{A}}(K,X[p]) = \mathrm{Sel}_{\hat{p}}(A_L/K)$ and for the associated direct limit $\mathrm{Sel}_{p^\infty}(A_L/K)$.

We next generalize Proposition 2.1 of [9], but in order to do so we need to define a notion of corank over the ring $\mathcal{O}\otimes\mathbb{Z}_p$ (particularly in the case that it is not an integral domain). Again, we have a decomposition

$$\mathcal{O}\otimes\mathbb{Z}_p \cong \oplus_i \mathcal{O}_{\mathfrak{p}_i}.$$

Definition 5.1. Let $S := \mathcal{O}\otimes\mathbb{Z}_p$ and $S_i := \mathcal{O}_{\mathfrak{p}_i}$. For an S-module M, define the S-corank of M to be

$$\operatorname{corank}_S M := (\ldots, \operatorname{corank}_{S_i} M\otimes\mathcal{O}_{\mathfrak{p}_i}, \ldots).$$

Proposition 5.2.

$$\mathit{corank}_S \mathit{Sel}_{p^\infty}(X/K) \equiv \mathit{rank}_R \mathit{Sel}_p(X/K) - \mathit{rank}_R X(K)[p] \mod 2.$$

Proof. We follow the strategy of Proposition 2.1 of [9]. Let

$$\begin{aligned} d &:= \operatorname{rank}_R(\mathrm{Sel}_{p^\infty}(X/K)/\mathrm{Sel}_{p^\infty}(X/K)_{\mathrm{div}})[p]\\ &= \operatorname{rank}_R(Ш(X/K)[p^\infty]/Ш(X/K)[p^\infty]_{\mathrm{div}})[p].\end{aligned}$$

We have

$$\begin{aligned}\operatorname{corank}_S \mathrm{Sel}_{p^\infty}(X/K) &= (\ldots, \operatorname{corank}_{S_i} \mathrm{Sel}_{p^\infty}(X/K) \otimes S_i, \ldots) \\ &= (\ldots, \operatorname{rank}_{R_i} \mathrm{Sel}_{p^\infty}(X/K)_{\mathrm{div}}[p] \otimes R_i, \ldots) \\ &= (\ldots, \operatorname{rank}_{R_i} \mathrm{Sel}_{p^\infty}(X/K)[p] \otimes R_i, \ldots) - d \\ &= \operatorname{rank}_R \mathrm{Sel}_{p^\infty}(X/K)[p] - d,\end{aligned}$$

with the first and last equalities by definition, and the others as in [9]. From (5.2) we obtain another sequence

$$0 \to (X(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p)[p] \to \mathrm{Sel}_{p^\infty}(X/K)[p] \to Ш(X/K)[p] \to 0$$

and then applying Proposition 2.2 we have

$$\operatorname{rank}_R \mathrm{Sel}_{p^\infty}(X/K)[p] = \operatorname{rank}_R (X(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p)[p] + \operatorname{rank}_R Ш(X/K)[p].$$

From (5.1) and Proposition 2.2 we obtain

$$\operatorname{rank}_R \mathrm{Sel}_p(X/K) = \operatorname{rank}_R (X(K)/pX(K)) + \operatorname{rank}_R Ш(X/K)[p].$$

Combining these, we see that

$$\begin{aligned}&\operatorname{corank}_S \mathrm{Sel}_{p^\infty}(X/K) - \operatorname{rank}_R \mathrm{Sel}_p(X/K) \\ &\qquad = \operatorname{rank}_R \mathrm{Sel}_{p^\infty}(X/K)[p] - d - \operatorname{rank}_R \mathrm{Sel}_p(X/K) \\ &\qquad = \operatorname{rank}_R (X(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p)[p] - \operatorname{rank}_R (X(K)/pX(K)) - d \\ &\qquad = -\operatorname{rank}_R X(K)[p] - d.\end{aligned}$$

Here we have cancelled the $Ш(X/K)[p]$ terms in the second equality, and the last equality follows from the exact sequence

$$0 \to X(K)[p] \to X(K) \otimes \mathbb{Z}/p\mathbb{Z} \to (X(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p)[p] \to 0,$$

defined by considering each term as an $\mathcal{O}$-module and decomposing each term as in [12, §11.2], and applying [7, §XVI.2].

It remains to see that d is even, which will show that the above equality implies the desired congruence modulo 2. We prove d is even below in Proposition 5.8. ■

First, we recall some definitions and results of Appendix A of [9]. For a cyclic extension L/K of degree p^n in F we define $\mathcal{R}_L := R_L \otimes \mathbb{Z}_p$, where R_L is as in §3, and consider $\mathcal{R}_L$ as a G_K-module by letting G_K act trivially. Let ζ be a primitive p^n root of unity and denote ι for the involution of R_L induced by $\zeta \mapsto \zeta^{-1}$, and similarly for $\mathcal{R}_L$. Let $\pi := \zeta - \zeta^{-1}$, which is a generator of the unique prime $\hat{p}$ of R_L above p and of the maximal ideal $\mathfrak{P}$ of $\mathcal{R}_L$.

For W an $\mathcal{R}_L$-module and B a $\mathbb{Z}_p$-module, a pairing $\langle\ ,\ \rangle : W \times W \to B$ is *ι-adjoint* if for each $r \in \mathcal{R}_L$ and $x, y \in W$, $\langle rx, y\rangle = \langle x, r^\iota y\rangle$. Also, a pairing $\langle\ ,\ \rangle : W \times W \to \mathcal{R}_L \otimes_{\mathbb{Z}_p} B$ is *$\mathcal{R}_L$-semilinear* if for each $r \in \mathcal{R}_L$ and $x, y \in W$

$$\langle rx, y\rangle = r\langle x, y\rangle = \langle x, r^\iota y\rangle,$$

and is *skew-Hermitian* if it is $\mathcal{R}_L$-semilinear and $\langle y, x\rangle = -\langle x, y\rangle^{\iota\otimes 1}$.

Mazur and Rubin construct a map $\tau : \mathcal{R}_L \to \mathbb{Z}_p$ such that composition with $\tau \otimes 1 : \mathcal{R}_L \otimes_{\mathbb{Z}_p} B \to B$ gives a bijection (Lemma A.3 and Proposition A.4 of [9]) between the set of $\mathcal{R}_L$-semilinear pairings $W \times W \to \mathcal{R}_L \otimes_{\mathbb{Z}_p} B$ and the set of ι-adjoint pairings $W \times W \to B$. Also, if $\langle\ ,\ \rangle_{\mathcal{R}_L}$ corresponds to $\langle\ ,\ \rangle_{\mathbb{Z}_p}$ then $\langle\ ,\ \rangle_{\mathcal{R}_L}$ is perfect (resp. G_K-equivariant) if and only if $\langle\ ,\ \rangle_{\mathbb{Z}_p}$ is perfect (resp. G_K-equivariant).

Definition 5.3 (Definition A.5 of [9])**.** Let $p^n = [L : K]$. Define two pairings: $f : \mathcal{I}_L \times \mathcal{I}_L \to R_L$ by

$$f(\alpha, \beta) := \pi^{-2p^{n-1}} \alpha\beta^\iota,$$

and $\langle\ ,\ \rangle_{\mathcal{R}_L} := f \otimes e_{p,\lambda}$ on $T_p(A_L) = \mathcal{I}_L \otimes T_p(X)$ by

$$\langle \alpha \otimes x, \beta \otimes y \rangle := (\pi^{-2p^{n-1}} \alpha\beta^\iota) \otimes \mathrm{e}_{p,\lambda}(x, y) \in \mathcal{R}_L \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(1). \tag{5.3}$$

In Theorem A.12 of [9], Mazur and Rubin use the pairing (5.3) and arguments of Flach [5] to obtain a perfect, skew-Hermitian, $\mathrm{Gal}(K/k)$-equivariant pairing $[\ ,\ ]_{\mathcal{R}_L}$ on

$$Ш(A_L/K)_{/\mathrm{div}} := Ш(A_L/K)/Ш(A_L/K)_{\mathrm{div}},$$

taking values in $D_p := \mathcal{R}_L \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p$. Using Flach's arguments, we can also obtain the classical Cassels-Tate pairing on $Ш(X/K)_{/\mathrm{div}}$ from the Weil pairing on $X[p]$. We first show that these pairings satisfy $[sx, y] = [x, s^\dagger y]$, for each $s \in \mathcal{O}$.

Proposition 5.4. *Suppose Y/k is an abelian variety with an action of $\mathcal{O}$ and $B = \mathbb{Q}_p/\mathbb{Z}_p$ or $B = D_p$. If $\langle\ ,\ \rangle : T_p(Y) \times T_p(Y) \to B$ induces (via Flach's construction) $[\ ,\ ]$ on $Ш(Y/K)_{/div}$ and $\langle sx, y\rangle = \langle x, s^\dagger y\rangle$ for all $s \in \mathcal{O}$, then $[sx, y] = [x, s^\dagger y]$ for all $s \in \mathcal{O}$.*

Proof. We recall the construction of $[\ ,\ ]$ from p.116 of [5]. Let $V_p(Y) = T_p(Y) \otimes \mathbb{Q}$. From $x, x' \in \mathrm{Sel}_{p^\infty}(Y/K)$, we obtain cocylces $\alpha, \alpha' \in Z^1(K, Y[p^\infty])$. From the exact diagram

$$\begin{array}{ccccc} & & C^1(K, V_p(Y)) & \longrightarrow & C^1(K, Y[p^\infty]) \longrightarrow 0 \\ & & \downarrow d & & \downarrow d \\ C^2(K, T_p(Y)) & \longrightarrow & C^2(K, V_p(Y)) & \longrightarrow & C^2(K, Y[p^\infty]) \end{array}$$

we see that α and α' can be lifted to $\beta, \beta' \in C^1(K, V_p(Y))$, and we have $d\beta, d\beta' \in C^2(K, T_p(Y))$. The pairing $\langle\ ,\ \rangle$ induces a cup-product $\cup$

$$C^i(K, V_p(Y)) \times C^j(K, V_p(Y)) \xrightarrow{\cup} C^{i+j}(K, B).$$

Since $H^3(K, B) = 0$, there is some $\epsilon \in C^2(K, B)$ such that $d\beta \cup \beta' = d\epsilon$. Since α' represents $x \in \mathrm{Sel}_{p^\infty}(Y/K)$, $\mathrm{res}_v(\alpha')$ is the image of some cocycle $\beta'_v \in Z^1(K_v, V_p(Y))$. Define

$$\gamma_v := \mathrm{res}_v(\beta) \cup \beta'_v - \mathrm{res}_v(\epsilon) \in C^2(K_v, B),$$

and then $[x, x'] := \sum_v \mathrm{inv}_v(\gamma_v)$.

Just as in Proposition 3.10, the cup-product $\cup$ satisfies an $\mathcal{O}$-adjoint property, so

$$d(s\beta) \cup \beta' = s(d\beta) \cup \beta' = d\beta \cup s^\dagger \beta',$$

giving the same ϵ for both pairs (sx, x') and $(x, s^\dagger x')$. Also,

$$\mathrm{res}_v(s\beta) \cup \beta'_v = s(\mathrm{res}_v(\beta)) \cup \beta'_v = \mathrm{res}_v(\beta) \cup s^\dagger \beta'_v.$$

Thus the pairs (sx, x') and $(x, s^\dagger x')$ define the same γ_v, for each v, and so $[sx, x'] = [x, s^\dagger x']$. ∎

Corollary 5.5. *If* $[\ ,\ ]$ *is obtained from* $e_{p,\lambda}$ *or* $\langle\ ,\ \rangle_{\mathcal{R}_L}$, *then* $[sx, y] = [x, s^\dagger y]$ *for all* $s \in \mathcal{O}$.

Proof. We have already seen that $\mathrm{e}_{p,\lambda}(sx, y) = \mathrm{e}_{p,\lambda}\left(x, s^\dagger y\right)$. By definition, the $\mathcal{O}$-action on $\mathcal{I}_L \otimes T_p(X)$ is $s(\alpha \otimes x) = \alpha \otimes (sx)$. Therefore,

$$\begin{aligned}
\langle s(\alpha \otimes x), \beta \otimes y\rangle &= \langle \alpha \otimes (sx), \beta \otimes y\rangle \\
&= (\pi^{-2p^{n-1}} \alpha\beta^\iota) \otimes \mathrm{e}_{p,\lambda}(sx, y) \\
&= (\pi^{-2p^{n-1}} \alpha\beta^\iota) \otimes \mathrm{e}_{p,\lambda}\left(x, s^\dagger y\right) \\
&= \langle \alpha \otimes x, \beta \otimes (s^\dagger y)\rangle = \langle \alpha \otimes x, s^\dagger(\beta \otimes y)\rangle,
\end{aligned}$$

and Proposition 5.4 gives the claim. ∎

Proposition 5.6. *Let* $[\ ,\ ]$ *denote the Cassels-Tate pairing*

$$Ш(X/K)_{/div} \times Ш(X/K)_{/div} \to \mathbb{Q}_p/\mathbb{Z}_p.$$

Then $[c^*(x), x'] = [x, c^*(x')]$.

Proof. Recall that $e_{p,\lambda}$ is G_k-equivariant. We keep the notation in the proof of Proposition 5.4. Specifically, let $B = \mathbb{Q}_p/\mathbb{Z}_p$ and let $x, x' \in \mathrm{Sel}_{p^\infty}(X/K)$. Just as in Proposition 3.8 the G_k-equivariance of $e_{p,\lambda}$ implies, for any cochains ω, ω',

$$c^*(c^*(\omega) \cup \omega') = \omega \cup c^*(\omega'). \tag{5.4}$$

Let the pair $c^*(\beta), \beta'$ (resp. $\beta, c^*(\beta')$) define $\epsilon \in C^2(K, B)$ and $\gamma_v \in C^2(K_v, B)$ (resp. ϵ', γ'_v) as in Proposition 5.4. Property (5.4) then implies that $c^*(\epsilon) = \epsilon'$. From $c^* \circ \mathrm{res}_v = \mathrm{res}_{v^c} \circ c^*$, we obtain

$$\begin{aligned}
\gamma'_v &= \mathrm{res}_v(\beta) \cup c^*(\beta'_{v^c}) - \mathrm{res}_v(c^*(\epsilon)) \\
&= c^*(\mathrm{res}_{v^c}(c^*(\beta)) \cup \beta'_{v^c} - \mathrm{res}_{v^c}(\epsilon)) \\
&= c^*(\gamma_{v^c}),
\end{aligned}$$

and so $\sum_v \mathrm{inv}_v(\gamma'_v) = \sum_v \mathrm{inv}_v \circ c^*(\gamma_{v^c}) = \sum_v \mathrm{inv}_{v^c}(\gamma_{v^c})$. Thus, we conclude that $[x, c^*(x')] = [c^*(x), x']$. ∎

Remark 5.7. The proposition also follows from Theorem A.12 of [9]. In particular, Mazur and Rubin show that the G_k-equivariance of $e_{p,\lambda}$ implies $\mathrm{Gal}(K/k)$-equivariance of $[\ ,\ ]$, and $\mathrm{Gal}(K/k)$ acts trivially on $\mathbb{Q}_p/\mathbb{Z}_p$.

The following proposition shows that $d = \mathrm{rank}_R Ш(X/K)_{/\mathrm{div}}[p]$ is even. Theorem 1 of [5] shows that $Ш(X/K)_{/\mathrm{div}}$ is finite, and in particular it is a finite p-group. Thus, for some $t \geqslant 1$

$$Ш(X/K)_{/\mathrm{div}} = Ш(X/K)_{/\mathrm{div}}[p^t] = \oplus_i Ш(X/K)_{/\mathrm{div}}[\mathfrak{p}_i^t].$$

Proposition 5.8. *$d = rank_R(Ш(X/K)[p^\infty]/Ш(X/K)[p^\infty]_{div})[p]$ is even.*

Proof. From Corollary 5.5 and Proposition 5.6 the pairing $[\ ,\ ]$ on $Ш(X/K)_{/\mathrm{div}}$ satisfies $[sx, x'] = [x, s^\dagger x']$ and $[c^*(x), x'] = [x, c^*(x')]$ for all $s \in \mathcal{O}$ and $x, x' \in Ш(X/K)_{/\mathrm{div}}$. Define $[\ ,\ ]'$ by $[x, y]' := [x, c^*(y)]$ as in Lemma 4.4, obtaining a non-degenerate, skew-symmetric, $\mathbb{Z}_p$-bilinear pairing on $Ш(X/K)_{/\mathrm{div}}$ with $[sx, y]' = [x, sy]'$ for all $s \in \mathcal{O}$ and $x, y \in Ш(X/K)_{/\mathrm{div}}$. Since $Ш(X/K)_{/\mathrm{div}}$ is finite, Proposition 2.8 (with $A = \mathcal{O} \otimes \mathbb{Z}_p$) then shows that d is even. ■

We now provide the analogous statement to Proposition 5.2 for A_L. Previously, we noted that the twist A_L is defined over K, but in fact it is essential that A_L have a model over k in order to apply Theorem A.12 of [9]. Again, the results of Appendix A of [9] (Definition A.8 and on, or alternatively [10, §6]) allow us to consider A_L defined over k. Combining Propositions 5.2 and 5.9 in Theorem 6.2 below proves a generalization of Theorem 6.4 of [9]. Recall $\mathcal{R}_L = R_L \otimes \mathbb{Z}_p$.

Proposition 5.9.

$$corank_{\mathcal{O}\otimes\mathcal{R}_L} Sel_{p^\infty}(A_L/K) \equiv rank_R Sel_{\hat{p}}(A_L/K) - rank_R X(K)[p] \mod 2.$$

Proof. The proof is the same as Proposition 5.2, using Proposition 3.2 to identify $A_L(K)[\hat{p}]$ with $E(K)[p]$, and seeing that $d = \mathrm{rank}_R Ш(A_L/K)_{/\mathrm{div}}[\hat{p}]$ is even as follows. Theorem 1 of [5] shows $M = Ш(A_L/K)_{/\mathrm{div}}$ is an $\mathcal{O}\otimes\mathcal{R}_L$-module of finite cardinality. Since

$$\mathcal{O} \otimes \mathcal{R}_L = \mathcal{O} \otimes (\mathbb{Z}_p \otimes R_L) = (\mathcal{O} \otimes \mathbb{Z}_p) \otimes R_L,$$

we have $M = \oplus_j (M \otimes \mathcal{O}'_{\hat{\mathfrak{p}}_j})$, where $\mathcal{O}'_{\hat{\mathfrak{p}}_j} = \mathcal{O}_{\mathfrak{p}_j} \otimes R_L$. As noted above, Theorem A.12 of [9] produces a perfect, skew-Hermitian, $\mathrm{Gal}(K/k)$-equivariant pairing $[\ ,\ ]$. Defining $[x, y]' = [x, c^*(y)]$ as before gives a non-degenerate, skew-symmetric, $\mathcal{R}_L$-bilinear pairing with $[sx, y]' = [x, sy]'$ for all $s \in \mathcal{O}$. We can therefore apply Proposition 2.8 (with $A = \mathcal{O} \otimes \mathcal{R}_L$) to see d is even. ■

6. Main results

We are now in a position to define and make use of the arithmetic local constants for our abelian variety X. Recall $R = \mathcal{O}/p\mathcal{O}$, where $\mathcal{O} \subset \mathrm{End}_K(X)$. Also, recall that for each cyclic L/K, we have a twist A_L of X and rings R_L (see §3) and $\mathcal{R}_L = R_L \otimes \mathbb{Z}_p$.

Definition 6.1. As in Definition 4.5 of [9], for each cyclic L/K contained in F, we define the arithmetic local constant $\delta_v := \delta(v, X, L/K)$ by

$$\delta_v := \mathrm{rank}_R(H^1_{\mathcal{X}}(K_v, X[p])/H^1_{\mathcal{X}\cap\mathcal{A}}(K_v, X[p])) \mod 2.$$

Theorem 6.2. *For $\mathfrak{S}_L$ as in §1.1,*

$$\mathit{corank}_{\mathcal{O}\otimes\mathbb{Z}_p} \mathit{Sel}_{p^\infty}(X/K) - \mathit{corank}_{\mathcal{O}\otimes\mathcal{R}_L} \mathit{Sel}_{p^\infty}(A_L/K) \equiv \sum_{v\in\mathfrak{S}_L} \delta_v \mod 2.$$

Proof. First, Lemma 4.1 and Theorem 4.5 give

$$\mathrm{rank}_R\mathrm{Sel}_p(X/K) - \mathrm{rank}_R\mathrm{Sel}_{\hat{p}}(A_L/K) \equiv \sum_{v\in\mathfrak{S}_L} \delta_v \mod 2.$$

The claim then follows from this, Proposition 5.2 and Proposition 5.9. ∎

Corollary 5.3 of [9] shows that in the elliptic curve case, δ_v can be computed via a completely local formulae, and the same arguments apply in our more general setting. For v a prime of K and w a prime of L above v, if $L_w \neq K_v$, let L'_w be the unique subfield of L_w containing K_v with $[L_w : L'_w] = p$, and otherwise let $L'_w := L_w = K_v$. Proposition 5.2 of [9] provides an $\mathcal{O}$-module isomorphism

$$H^1_{\mathcal{X}\cap\mathcal{A}}(K_v, X[p]) \cong (X(K_v) \cap N_{L_w/L'_w} X(L_w))/pX(K_v). \tag{6.1}$$

Proposition 6.3 (Corollary 5.3 of [9]). *For every prime v of K,* (6.1) *implies*

$$\delta_v \equiv \mathit{rank}_R X(K_v)/(X(K_v) \cap N_{L_w/L'_w} X(L_w)) \mod 2.$$

Corollary 6.4. *Let $\mathfrak{S}^c_L$ be the set of primes v of K such that v ramifies in L/K and $v^c = v$. Then*

$$\mathit{corank}_{\mathcal{O}\otimes\mathbb{Z}_p} \mathit{Sel}_{p^\infty}(X/K) - \mathit{corank}_{\mathcal{O}\otimes\mathcal{R}_L} \mathit{Sel}_{p^\infty}(A_L/K) \equiv \sum_{v\in\mathfrak{S}^c_L} \delta_v \mod 2.$$

Proof. The arguments are as in the proof of Theorem 7.1 of [9]. If $v \notin \mathfrak{S}^c_L$ then $v^c \neq v$ or v is unramified in L/K. If $v^c \neq v$ then Lemma 5.1 of [9] shows that $\delta_v + \delta_{v^c} \equiv 0$. If $v^c = v$ and v is unramified then, Lemma 6.5 of [9] shows that v splits completely in L/K and hence N_{L_w/L'_w} is surjective. Using Proposition 6.3, we see that $\delta_v \equiv 0$. ∎

The following is a first example of a class of abelian varieties for which Proposition 6.2 can be used to produce a lower bound for the growth in p-Selmer $(\mathcal{O}\otimes\mathbb{Z}_p)$-rank.

Corollary 6.5. *Suppose that for every $v \in \mathfrak{S}^c_F$, we have $v \mid p$ and X has good ordinary, non-anomalous reduction at v. If $\mathit{corank}_{\mathcal{O}\otimes\mathbb{Z}_p} \mathit{Sel}_{p^\infty}(X/K)$ is odd then*

$$\mathit{corank}_{\mathcal{O}\otimes\mathbb{Z}_p} \mathit{Sel}_{p^\infty}(X/F) \geqslant ([F : K], \ldots, [F : K]).$$

Proof. Suppose L/K is a cyclic extension contained in F. Theorem 6.2 and Corollary 6.4 show that we need only see that $\delta_v = 0$ for all $v \in \mathfrak{S}_F^c$. Since $v \in \mathfrak{S}_F^c$, we have v is totally ramified in L_w/K_v by Lemma 6.5 of [9].

The assumptions that $v \mid p$ and that X has good ordinary, non-anomalous reduction at v allow us to apply the arguments of Appendix B of [9] to see $\delta_v = 0$. The key ingredients therein are, firstly, the diagram on page 239 of [8], which applies to abelian varieties of any dimension. Secondly, non-anomalous reduction guarantees the relevant norm maps are surjective.

Now, for each cyclic L in F, we have

$$\operatorname{corank}_{\mathcal{O}\otimes\mathbb{Z}_p}\mathrm{Sel}_{p^\infty}(X/K) \equiv \operatorname{corank}_{\mathcal{O}\otimes\mathcal{R}_L}\mathrm{Sel}_{p^\infty}(A_L/K) \mod 2,$$

and by our hypotheses, the left-hand side is odd. As in Theorem 7.1 of [9], the Pontrjagin dual $\mathcal{S}_p(X/F)$ of $\mathrm{Sel}_{p^\infty}(X/F)$ (see for example [9, §3]) decomposes as

$$\mathcal{S}_p(X/F) \cong \oplus_L \mathcal{S}_p(A_L/K),$$

with each $\mathcal{S}_p(A_L/K)$ a $\mathbb{K}[\mathrm{Gal}(F/K)]_L \otimes \mathbb{Q}_p$-module (see §3 and Remark 3.1), and we have just seen each has odd dimension. From $\mathbb{K}[\mathrm{Gal}(F/K)] \cong \oplus_L \mathbb{K}[\mathrm{Gal}(F/K)]_L$, we see that $\mathcal{S}_p(X/F)$ contains a submodule isomorphic to

$$\mathbb{K}_p[\mathrm{Gal}(F/K)] \cong \oplus_L (\mathbb{K}[\mathrm{Gal}(F/K)]_L \otimes \mathbb{Q}_p),$$

and the claim follows. ■

6.1. Composite dihedral extensions

We now consider an abelian extension F/K of odd degree $[F : K] = m$, and a cyclic extension L/K inside F. To ease notation, we fix some ordering of the primes in $[L : K] = \prod_i p_i^{e_i}$, where $e_i > 0$ for each i. For such L/K in F and each i, there exists a p_i-power subextension M_i/K such that L/M_i is of degree prime to p_i.

By Proposition 5.10 of [10], if M and M' are cyclic extensions of K inside L with $[M : K]$ and $[M' : K]$ coprime and $L = MM'$, then the twist A_L of X with respect to L/K may also be realized as a twist of A_M, i.e. $A_L \cong (A_M)_{M'}$. Thus, if we want to compare A_L and X, it suffices to compare X with A_M, and also A_M with $(A_M)_{M'}$. As in the paragraph preceeding Proposition 5.9, we consider A_M and $(A_M)_{M'}$ as defined over k.

In order to inductively apply Theorem 6.2 (see Theorem 6.9 below), we assume the following conjecture.

Conjecture 6.6. *Suppose p is a prime, Y/L is an abelian variety, $B \subset End_L(Y)$ is an integral domain, and $\mathfrak{q}$ and $\mathfrak{q}'$ are primes of B above p. Then*

1. *$corank_{B\otimes\mathbb{Z}_p} Sel_{p^\infty}(Y/L)$ is independent of p,*
2. *$corank_{B_\mathfrak{q}} Sel_{p^\infty}(Y/L) \otimes B_\mathfrak{q} = corank_{B_{\mathfrak{q}'}} Sel_{p^\infty}(Y/L) \otimes B_{\mathfrak{q}'}$,*

Remark 6.7. Both parts of the conjecture follow from the Shafarevich-Tate Conjecture. Indeed, when $\#Ш(Y/L) < \infty$, (5.2) implies

$$\mathrm{corank}_{B\otimes\mathbb{Z}_p}\mathrm{Sel}_{p^\infty}(Y/L) = \mathrm{rank}_{B\otimes\mathbb{Z}_p}(Y(L)\otimes\mathbb{Q}_p/\mathbb{Z}_p) = (\ldots,\mathrm{rank}_B Y(L),\ldots).$$

Each entry in the tuple is identical, giving (2), and independent of p, giving (1).

For the remainder, we let F/K be as at the beginning of §6.1 with F/k dihedral, X/k and $\mathcal{O}\subset\mathrm{End}_K(X)$ as in the previous sections (see §1.1), and assume that each prime dividing $[F:K]$ is unramified in $\mathcal{O}$. For Theorem 6.9 below, we also fix a cyclic extension L/K in F.

For each M/K in L, let R_M denote the maximal order in $\mathbb{Q}[\mathrm{Gal}(F/K)]_M$ (as in §3 for $M=L$) and $\mathcal{O}_M=\mathcal{O}\otimes R_M$.[3] Recall c is the non-trivial element of $\mathrm{Gal}(K/k)$. Let (as in Corollary 6.4)

$$\mathfrak{S}_M^c := \{\text{primes } v \text{ of } K : v^c = v \text{ and } v \text{ ramifies in } M/K\}.$$

Set $M_0=K$ and for each $i>0$ set $M_i\subset L$ to be a p_i-extension of K such that $p_i\nmid[L:M_i]$.

Using Conjecture 6.6 (2), for any p, the tuple defining $\mathrm{corank}_{B\otimes\mathbb{Z}_p}\mathrm{Sel}_{p^\infty}(Y/L)$ may be thought of as a single value, so we define $r_p(Y/L,B)\in\mathbb{Z}$ by

$$r_p(Y/L,B) := \mathrm{corank}_{B_\mathfrak{q}}\mathrm{Sel}_{p^\infty}(Y/L)\otimes B_\mathfrak{q},$$

where $\mathfrak{q}$ is some prime of B above p. In turn, one may interpret the right-hand side of Theorem 6.2 as a single value, so we define $\delta(X,L/K)\in\mathbb{Z}/2\mathbb{Z}$ as

$$\delta(X,L/K) := \text{the first component of } \left(\sum_{v\in\mathfrak{S}_L}\delta(v,X,L/K)\right) \mod 2.$$

Remark 6.8. We emphasize that the *sum* of the local constants $\delta(v,X,L/K)$, for fixed X and L/K, has constant parity across components, by Conjecture 6.6 (2) and Theorem 6.2. It would be interesting to determine under what conditions one can prove that the *individual* $\delta(v,X,L/K)$ have constant parity across components.

Theorem 6.9. *Assume Conjecture 6.6. For $K=M_0,M_1,\cdots,L$ as above and p a prime dividing $[L:K]$,*

$$r_p(A_L/K,\mathcal{O}_L) - r_p(X/K,\mathcal{O}) \equiv \sum_{i\geqslant 1}\delta(A_{M_{i-1}},M_i/K) \mod 2.$$

Proof. Without loss of generality we may assume $p=p_1$. We proceed by induction on the number j of primes dividing $[L:K]$, and the case $j=1$ is that of Theorem 6.2. Suppose now that $j>1$, and let $M=M_1$ and let M' correspond

[3] We note that $\mathcal{O}_L\otimes\mathbb{Z}_p\cong\mathcal{O}\otimes\mathcal{R}_L$, with the latter as in Theorem 6.2. The new notation is more convenient for dealing with more than one prime.

to the compositum of the M_i for $1 < i \leqslant j$. Recall from the discussion above that Proposition 5.10 of [10] shows $A_L \cong (A_M)_{M'}$. Arguments of Howe [6, §2] show that A_M has a polarization degree of p^2, in particular prime to $[L : M]$, and so we can apply Theorem 6.2 in L/M with A_M playing the role of X. For p' any prime dividing $[L : M]$, by induction we have

$$r_{p'}(A_L, \mathcal{O}_L) - r_{p'}(A_M, \mathcal{O}_M) \equiv \sum_{i \geqslant 2} \delta(A_{M_{i-1}}, M_i/M) \mod 2.$$

Using Conjecture 6.6 (1), we have

$$r_p(Y/K, B) \equiv r_{p'}(Y/K, B) \mod 2,$$

for $Y = X$, A_M, A_L, and $B = \mathcal{O}$, $\mathcal{O}_M$, $\mathcal{O}_L$, respectively, and hence

$$\begin{aligned} r_p(A_L/K, \mathcal{O}_L) - r_p(X/K, \mathcal{O}) &\equiv r_{p'}(A_L/K, \mathcal{O}_L) - r_{p'}(A_M/K, \mathcal{O}_M) \\ &\quad + r_p(A_M/K, \mathcal{O}_M) - r_p(X/K, \mathcal{O}) \\ &\equiv \sum_{i \geqslant 2} \delta(A_{M_{i-1}}, M_i/M) \\ &\quad + \delta(X, M/K) \\ &\equiv \sum_{i \geqslant 1} \delta(A_{M_{i-1}}, M_i/K) \mod 2. \end{aligned}$$

We are able to restrict the primes v in the preceeding sums to those in $\mathfrak{S}^c_{M_i}$ just as in Corollary 6.4. ∎

As in Corollary 6.5, the following is a first example of a setting in which Theorem 6.9 can be used to provide a lower bound for growth in the rank of E (i.e. when $X = E$ is an elliptic curve).

Corollary 6.10. *Let E/k be an elliptic curve, $\mathbb{K} \not\subset k$, and assume $\#Ш(E/F) < \infty$. For each cyclic L/K let $M_{L,i} \subset L$ be as in the paragraphs preceeding Theorem 6.9. Suppose that for every prime v of K,*

1. *if $v = v^c$ then v is unramified in $M_{L,i}/K$ for every L and each $i \geqslant 2$,*
2. *if $v = v^c$ and v ramifies in $M_{L,1}/K$ then $v \nmid p_1$ and E has good reduction at v.*

Let m be the number of primes v satisfying (2). If $\mathrm{rank}_{\mathcal{O}} E(K) + m$ is odd, then $\mathrm{rank}_{\mathcal{O}} E(F) \geqslant [F : K]$.

Proof. Fix a cyclic extension L/K inside F, and set $M_i = M_{L,i}$. From $\#Ш(E/F) < \infty$ we have (e.g.) $\mathrm{rank}_{\mathcal{O}} E(K) = r_p(E/K, \mathcal{O})$ and Conjecture 6.6, so we are in the situation of Theorem 6.9. As in Corollary 6.4, if v is unramified or $v \neq v^c$ then $\delta(v, A_{m_{i-1}}, M_i/K) \equiv 0$ or

$$\delta(v, A_{m_{i-1}}, M_i/K) + \delta(v^c, A_{m_{i-1}}, M_i/K) \equiv 0,$$

respectively, for every $i \geqslant 1$. For $v = v^c$, condition (1) gives $\delta(v, A_{m_{i-1}}, M_i/K) \equiv 0$, for every $i \geqslant 2$. Thus $\delta(E, M_i/K) \equiv 0$ for $i \geqslant 2$. By Theorem 2.8 of [4], condition (2) along with $\mathbb{K} \not\subset k$ gives $\delta(v, E, M_1/K) \equiv (1, 1)$, and so $\delta(E, M_1/K) \equiv m$.

Using Theorem 6.9, we combine the calculations to see that

$$r_p(A_L/K, \mathcal{O}_L) \equiv r_p(E/K, \mathcal{O}) + m \mod 2.$$

By assumption, this is forces $r_p(A_L/K, \mathcal{O}_L)$ to be odd and hence at least 1. The claim then follows just as in Corollary 6.5. ■

Acknowledgements. This material is based upon work supported by the National Science Foundation under grant DMS-0457481. The author would like to thank Karl Rubin for his many helpful conversations on this material, and thank Karl Rubin and Jan Nekovář for comments on initial drafts of this paper.

References

[1] K. Brown, *Cohomology of Groups*, volume 87 of *Graduate Texts in Mathematics*, Springer, 1982.
[2] J.W.S. Cassels, *Diophantine equations with special reference to elliptic curves*, J. London Math. **41** (1966), 193–291.
[3] S. Chetty, *Comparing local constants of elliptic curves in dihedral extensions*, submitted, draft: arXiv:1002.2671.
[4] S. Chetty and L. Li, *Computing local constants for cm elliptic curves*, Rocky Mountain J. Math. **44**(3) (2014), 853–863.
[5] M. Flach, *A generalisation of the Cassels-Tate pairing*, J. reine angew. Math. **412** (1990), 113–127.
[6] E. Howe, *Isogeny classes of abelian varieties with no principal polarizations*, in *Moduli of abelian varieties (Texel Island, 1999)*, volume 195 of Progress in Mathematics, pages 203–216. Birkhäuser, 2001.
[7] S. Lang, *Algebra*, volume 211 of *Graduate Texts in Mathematics*, Springer, revised third edition, 2002.
[8] J. Lubin and M. Rosen, *The norm map for ordinary abelian varieties*, Journal of Algebra **52** (1978), 236–240.
[9] B. Mazur and K. Rubin, *Finding large Selmer rank via an arithmetic theory of local constants*, Annals of Mathematics **166**(2) (2007), 581–614.
[10] B. Mazur, K. Rubin, and A. Silverberg, *Twisting Commutative Algebraic Groups*, Journal of Algebra **314**(1) (2007), 419–438.
[11] J.S. Milne, *Abelian Varieties*, in G. Cornell and J. Silverman, editors, *Arithmetic Geometry*, Springer-Verlag, 1986, available at `http://www.jmilne.org/math/`.
[12] J. Rotman, *Advanced Modern Algebra*, Prentice Hall, 2002.
[13] K. Rubin, *Euler Systems*, Hermann Weyl Lectures - The Institute for Advanced Study, Princeton University Press, 2000.

[14] J-P. Serre, *Local Fields*, volume 42 of *Graduate Texts in Mathematics*, Springer, 1977.

[15] M. Seveso, *The arithmetic theory of local constants for abelian varieties*, Rend. Semin. Mat. Univ. Padova **127** (2012), 17–39.

[16] J. Silverman, *Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*, Springer, 1986.

Address: Sunil Chetty: Mathematics Department, College of St. Benedict and St. John's University, USA.

E-mail: schetty@csbsju.edu

Received: 27 October 2015; **revised:** 1 February 2016