The class group pairing and p-descent on elliptic curves

Jean Gillibert   Christian Wuthrich[*]

October 19, 2011

Abstract

We give explicit formulae for the logarithmic class group pairing on an elliptic curve defined over a number field. Then we relate it to the descent relative to a suitable cyclic isogeny. This allows us to connect the resulting Selmer group with the logarithmic class group of the base. These constructions are explicit and suitable for computer experimentation. From a conceptual point of view, the questions that arise here are analogues of "visibility" questions in the sense of Cremona and Mazur.

1   Introduction

The class-invariant homomorphism has been introduced by Martin Taylor [30] in order to study the Galois module structure of extensions obtained when dividing points by isogenies between abelian varieties. For instance, let p be an odd prime and let $\varphi\colon E \to E'$ be an isogeny of degree p between elliptic curves over a number field K. Suppose that the kernel of φ is isomorphic to μ_p as a Galois module. For $Q \in E'(K)$ consider the extension $K(\varphi^{-1}(Q))/K$ obtained by adjoining the coordinates of the preimages of Q under φ. It is a Kummer extension, and we may ask for the arithmetic properties of this extension. It is easy to prove that this extension defines a μ_p-torsor $\varphi^{-1}(Q)$ over the ring $\mathcal{O}_{K,S}$ of S-integers of K where S is the set of all bad places for E and of all places above p. We have an exact sequence

$$0 \longrightarrow \mathcal{O}_{K,S}^\times/p \longrightarrow H^1_{\mathrm{fl}}(\mathcal{O}_{K,S}, \mu_p) \longrightarrow \mathrm{Cl}(\mathcal{O}_{K,S})[p] \longrightarrow 0$$

where the right-hand side map can be interpreted as measuring the Galois module structure of μ_p-torsors. The class-invariant homomorphism $\psi^{\mathrm{cl}} : E'(K)/\varphi(E(K)) \to \mathrm{Cl}(\mathcal{O}_{K,S})[p]$ is obtained by sending a point $Q \in E'(K)$ to the Galois module structure of the torsor $\varphi^{-1}(Q)$. It has been conjectured by Taylor, and proved by Taylor et al. that torsion points belong to the kernel of ψ^{cl} (see [24]). In other words, if Q is torsion, then $K(\varphi^{-1}(Q)) = K(\sqrt[p]{\alpha})$ for some $\alpha \in \mathcal{O}_{K,S}^\times$. However, the behaviour of ψ^{cl} on points of infinite order is not fully understood.

It has been proved by Agboola [1] that ψ^{cl} has an alternative "geometric" description. Namely, if we let $P \in E'(K)$ be the generator of the kernel of the dual isogeny $\hat{\varphi}$, then

$$\psi^{\mathrm{cl}}(Q) = \langle P, Q \rangle_S^{\mathrm{cl}}$$

where $\langle \cdot, \cdot \rangle_S^{\mathrm{cl}}$ is the so-called class group pairing introduced by Mazur and Tate [20]. Therefore our Galois structure problem can now be reformulated in terms of the intersection theory on the Néron model of E' over $\mathcal{O}_{K,S}$.

In order to study the Galois module structure of $\varphi^{-1}(Q)$ over the full ring of integers, one needs to handle bad places. The first author has been investigating this. Let $\mathcal{E}$ (resp. $\mathcal{E}'$) be the Néron

model of E (resp. E') over $X = \text{Spec}(\mathcal{O}_K)$, and let $\mathcal{E}^0(X)$ (resp. $\mathcal{E}'^0(X)$) be the subgroup of points that have everywhere good reduction. Again, we have a class-invariant homomorphism

$$\psi^0 : \mathcal{E}'^0(X)/\varphi(\mathcal{E}^0(X)) \longrightarrow \text{Cl}(K)[p]$$

that can also be described using the class group pairing. It is proved in [13] that torsion points belong to the kernel of ψ^0, but it is not possible in general to extend this morphism ψ^0 to all of $E'(K)/\varphi(E(K))$. To overcome this, the first author introduced a more general pairing, called the logarithmic class group pairing, that has values in the so-called logarithmic class group $\text{LogPic}(X,S)$. This pairing combines the class group pairing by Mazur and Tate with Grothendieck's monodromy pairing (see [14]). As a result, we get a class-invariant homomorphism

$$\psi : E'(K)/\varphi(E(K)) \longrightarrow \text{LogPic}(X,S)[p]$$

which generalises both ψ^{cl} and ψ^0. Of course, this new morphism is no longer expected to vanish on torsion points, because the monodromy pairing is known to be non degenerate.

In this paper, we give explicit formulae for the logarithmic class group pairing on elliptic curves, which are suited for implementation in a computer algebra system. (See section 4.4, in particular Lemma 4.4, Lemma 4.5 and the sections 4.4.1 and 4.4.2.) This allows us to conduct numerical experimentations on these objects that, up to now, have been considered from a purely conceptual point of view. Our derivation of the formulae leads us to study the intersection property of certain divisors on the minimal regular model of E as cubic logarithmic line bundles, similar to what was done in [5] for the monodromy pairing.

Under some additional hypotheses (see below in section 1.1) on E and φ, we perform a descent via the isogeny φ. We explicitly describe the Selmer group $\text{Sel}^\varphi(E/K)$ as a subgroup of the fppf cohomology group $H^1_{\text{fl}}(U_1, \mu_p)$ where U_1 is obtained by removing from X a certain subset S_1 of the set of places where E has split multiplicative reduction (see section 3 for details). At another small set S_2 of places of K, we have to impose local conditions. Theorem 3.1 shows that we have an exact sequence

$$0 \longrightarrow \text{Sel}^\varphi(E/K) \longrightarrow H^1_{\text{fl}}(U_1, \mu_p) \longrightarrow \bigoplus_{v \in S_2} H^1_{\text{fl}}(\mathcal{O}_v, \mu_p)$$

and Theorem 3.2 describes the cokernel on the right in terms of the Selmer group $\text{Sel}^{\hat{\varphi}}(E'/K)$ for the dual isogeny. The methods for the descent are very much inspired by [21] except that we use fppf cohomology.

Our interest then focuses on the link between the logarithmic class-invariant homomorphism and the Selmer group. Using Kummer theory in log flat topology, we get an exact sequence

$$0 \longrightarrow \mathcal{O}_K^\times/p \longrightarrow H^1_{\text{fl}}(U_1, \mu_p) \longrightarrow \text{LogPic}(X, S_1)[p] \longrightarrow 0.$$

Let $\psi_{\text{Sel}} : \text{Sel}^\varphi(E/K) \to \text{LogPic}(X, S_1)[p]$ be the restriction of the map on the right to the subgroup $\text{Sel}^\varphi(E/K)$. As our main ingredient to the following investigation, we prove in Theorem 5.1 that the class-invariant homomorphism ψ is equal to the composition of the Kummer map and the map ψ_{Sel}, in other words the following diagram commutes:

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & E'(K)/\varphi(E(K)) & \overset{\kappa}{\longrightarrow} & \text{Sel}^\varphi(E/K) & \longrightarrow & \text{III}(E/K)[\varphi] & \longrightarrow & 0 \\
& & & {\scriptstyle\psi}\searrow & \downarrow{\scriptstyle\psi_{\text{Sel}}} & & & & \\
& & & & \text{LogPic}(X, S_1)[p] & & & &
\end{array}
$$

where $\text{III}(E/K)$ is the Tate-Shafarevich group of E/K, and the horizontal line is exact. This links the logarithmic class group pairing to the descent data.

By the kernel-cokernel sequence, we get an exact sequence

$$0 \longrightarrow \ker(\psi) \longrightarrow \ker(\psi_{\text{Sel}}) \longrightarrow \text{III}(E/K)[\varphi] \longrightarrow \text{coker}(\psi) \longrightarrow \text{coker}(\psi_{\text{Sel}}) \longrightarrow 0$$

Understanding this sequence can be viewed in terms of the notion of "visibility" in the sense of Cremona and Mazur [8]: Instead of comparing the descent maps for two isogenies, we compare φ-descent with Kummer theory in log flat topology. For instance when $\mathrm{coker}(\psi) = 0$, one could say, by analogy with the terminology in [8], that all elements in $\text{Ш}(E/K)[\varphi]$ are *explained* by units.

In the special case when the set S_2 is empty, then $\ker(\psi_{\mathrm{Sel}}) = \mathcal{O}_K^\times/p$ and $\mathrm{coker}(\psi_{\mathrm{Sel}}) = 0$. Hence $\text{Ш}(E/K)[\varphi]$ is completely determined by the kernel and the cokernel of ψ. In particular, this happens if E has everywhere good reduction, in which case these relations have been pointed out previously (see [7] for a survey).

The behaviour of ψ on points of infinite order has to be explored. In Theorem 6.1 we prove that, given a curve E' over $\mathbb{Q}$ with a p-torsion point $P \in E'(\mathbb{Q})$, there exists an infinity of imaginary quadratic fields K and a point $Q \in E'(K)$ of infinite order such that $\langle P, Q \rangle_S^{\mathrm{cl}} \neq 0$. We also remark that ψ is injective when K is a quadratic imaginary field. Finally, we compute some examples of points of infinite order defined over real quadratic fields that lie or do not lie in the kernel of ψ.

Let us review briefly the contents of this paper. At the end of the introduction, we give general hypotheses and notations. In section 2 and 3, we perform the descent. In section 4, which is independent of the rest of the paper, we give explicit formulae for the logarithmic class group pairing on an elliptic curve. In section 5, we describe the connection between Selmer groups and logarithmic class groups via the pairing. In section 6, we focus on quadratic fields, and in final section 7 we give examples over fields of higher degree.

1.1 Hypotheses

Let K be a number field and E/K an elliptic curve. Throughout this paper, except for section 4, we will assume the following hypotheses.

(Hyp 1). p is an odd prime.

(Hyp 2). E admits an isogeny $\varphi\colon E \to E'$ of degree p defined over K.

(Hyp 3). The kernel of the dual isogeny $\hat{\varphi}\colon E' \to E$ is generated by a p-torsion point $P \in E'(K)[p]$.

(Hyp 4). If $p = 3$, none of the bad fibres of E nor of E' is of type IV or IV*.

(Hyp 5'). $K/\mathbb{Q}$ is not ramified at p.

The last condition (Hyp 5') can be weakened quite a bit once some additional notation is introduced. All conclusions in this article hold with condition (Hyp 5') replaced by hypothesis (Hyp 5) in section 2.6. For instance for semistable curves we will only need that the ramification e_v index at all places v above p satisfies $e_v < p - 1$.

While the first three hypotheses are just the setting in which we have placed ourselves, the fourth is merely to exclude that p might divide the order of the group of components at additive places.

1.2 Notations

If v is a place of the number field K, we write K_v, $\mathcal{O}_v$, $\mathfrak{m}_v$, and k_v for the completion at v, its ring of integers, its maximal ideal and its residue field respectively.

We will write $\mathcal{E}$ for the Néron model of E over the ring of integers $\mathcal{O}_K$. Let $\mathcal{E}^0$ be the connected component of the identity and let Φ be the groups of components. So we obtain an exact sequence of sheaves on the fppf site

$$0 \longrightarrow \mathcal{E}^0 \longrightarrow \mathcal{E} \longrightarrow \Phi \longrightarrow 0. \tag{1}$$

For all finite places v of K, we denote by Φ_v the group of components of the fibre of $\mathcal{E}$ at v. Of course, the sheaf Φ can be decomposed as

$$\Phi = \bigoplus_v \Phi_v$$

where v runs through the set of places of bad reduction of $\mathcal{E}$. The number of components of the fibre of $\mathcal{E}$ at v, i.e. the rank of the Φ_v, will be denoted by m_v, while the number of k_v-rational points $\#\Phi_v(k_v)$, the so-called Tamagawa number, is written c_v. We fix a choice of a Néron differential, denoted by ω. Similarly $\mathcal{E}'$, $\mathcal{E}'^0$, Φ', m_v', c_v' and ω' denote the corresponding objects for the elliptic curve E'. By abuse of notation, we also denote by $\varphi\colon \mathcal{E} \to \mathcal{E}'$ the unique morphism between the Néron models extending the isogeny φ. Note that φ induces a map $\varphi\colon \mathcal{E}^0 \to \mathcal{E}'^0$ and another on the components $\varphi\colon \Phi \to \Phi'$.

For any ring R, we will denote the quotient of the unit group $R^\times$ by its p-th powers, simply by $R^\times/p$.

All cohomology groups are computed with respect to the fppf site. We will write $H^1(\mathcal{O}_K, \cdot)$ as a short hand for $H^1(\mathrm{Spec}(\mathcal{O}_K), \cdot)$, similarly for $H^1(\mathcal{O}_v, \cdot)$.

2 Local information on the isogeny

In this section v will be a finite place of K. (Since p is odd, we never have to worry about infinite places.) We wish to describe the isogeny φ locally at the level of Néron models.

If v is not above p, it follows immediately that $\mathcal{E}'[\hat\varphi]$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ as a group scheme over the ring of integers $\mathcal{O}_v$ of K_v and hence, by Cartier duality, $\mathcal{E}[\varphi]$ is μ_p. This is not necessarily the case for places above p as we will see later.

Lemma 2.1. *For any $v \nmid p$, the curves E and E' have semistable reduction at v.*

Proof. Suppose the reduction is additive at v. There is a point P of order p on the curve E' defined over K_v. By assumption (Hyp 1) and (Hyp 4), the group of components Φ' of $\mathcal{E}'$ has order prime to p, so P reduces to a point in $\mathcal{E}'^0$. Since the reduction map is injective on points of order p as $v \nmid p$, the reduced point has order p, too. But the additive group has no p-torsion over k_v, so we reached a contradiction. $\qquad\square$

We will first describe the cases of multiplicative reduction, both for v above p and away from p. There are four cases to consider, depending on whether the reduction is split or non-split multiplicative and depending on which of the two isogenous curves has more connected components. We choose to denominate the latter property by saying the place is "forward" or "backward" for φ.

2.1 The forward split case

In this case, the reduction is **split** multiplicative and $\mathcal{E}$ has **less** components than $\mathcal{E}'$.

The elliptic curves are isomorphic to Tate curves over K_v for certain parameters q and q', respectively. We have $E(K_v) = K_v^\times/q^\mathbb{Z}$ and $E'(K_v) = K_v^\times/(q')^\mathbb{Z}$. Since the number of components is given by the valuation of the parameters, we find that $q' = q^p$ and that the isogeny $\varphi\colon E(K_v) \to E'(K_v)$ is induced by the map $x \mapsto x^p$ on $K_v^\times$. We conclude that $\Phi'/\varphi(\Phi) = \mathbb{Z}/p\mathbb{Z}$ and the cokernel $E'(K_v)/\varphi(E(K_v))$ is isomorphic to $K_v^\times/p$. Also we see that $\mathcal{E}[\varphi]$ is contained in $\mathcal{E}^0$.

The dual map $\hat\varphi_{K_v}$ is then induced by $x \mapsto x$. It follows that $\mathcal{E}'[\hat\varphi] = \Phi'[\hat\varphi] = \mathbb{Z}/p\mathbb{Z}$, in other words the point P reduces to the singular point at v. However, $\hat\varphi\colon E'(K_v) \to E(K_v)$ and hence $\hat\varphi\colon \Phi' \to \Phi$ are surjective. Furthermore, we also see that $\varphi^*(\omega') = p\omega$ and $\hat\varphi^*(\omega) = \omega'$ for the Néron differentials.

2.2 The backward split case

Here the reduction is still **split** multiplicative, but $\mathcal{E}$ has **more** components than $\mathcal{E}'$.

The situation is as above except that E and E' switch their places. This time, we have $q = (q')^p$ and the map φ_{K_v} identifies with $x \mapsto x$ and its dual with $x \mapsto x^p$. So $\mathcal{E}^0[\varphi]$ is trivial and $\mathcal{E}[\varphi] = \Phi[\varphi]$. Since Φ is a constant group scheme, we find that $\mu_p = \mathbb{Z}/p\mathbb{Z}$ over $\mathcal{O}_v$, which implies that $\#k_v \equiv 1 \pmod{p}$. In particular, this case can not occur for a place above p. This time φ_{K_v} is surjective onto $E'(K_v)$, but the cokernel of $\hat{\varphi}_{K_v}$ is isomorphic to $K_v^\times/p$.

For the dual isogeny, we get $\mathcal{E}'[\hat{\varphi}] \subset \mathcal{E}'^0$ and so $\Phi'[\hat{\varphi}] = 0$ and $\Phi/\hat{\varphi}(\Phi') = \mathbb{Z}/p\mathbb{Z}$.

2.3 The backward non-split case

Now, the reduction is **non-split** multiplicative and $\mathcal{E}$ has **more** components than $\mathcal{E}'$.

Let L_w/K_v be the quadratic unramified extension. Over L_w the reduction becomes split, yet the Néron model stays the same. In particular, over L_w we are in the backward split case.

We start by proving that this case can not occur when v is above p. The Tamagawa number c'_v is coprime to p by assumption, so the point $P \in E'(K_v)$ must lie on the identity component. Since the group of non-singular point on the reduction has order coprime to p, the point P must lie in the formal group. Since $\hat{\varphi}$ has a non-trivial kernel in the formal group we must have that $\hat{\varphi}^*(\omega) = \omega'$. This will still be the same over the quadratic extension L_w since the Néron model does not change. But this is in contradiction with what we found in the backward split case. Hence $v \nmid p$.

Let $E^\dagger/K_v$ be the twist of E corresponding to L_w/K_v. Then $E^\dagger$ admits an isogeny $\varphi^\dagger$ of degree p, for which the place is also backward split. So $\mathcal{E}[\varphi] = \mu_p$ becomes $\mathbb{Z}/p\mathbb{Z}$ over $\mathcal{O}_w$, but they are not isomorphic yet over $\mathcal{O}_v$. In fact $\mathcal{E}[\varphi]$ is the twist of $\mathcal{E}^\dagger[\varphi^\dagger]$, which is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. Hence $\mathcal{E}[\varphi] = \mu_p$ is a quadratic twist of $\mathbb{Z}/p\mathbb{Z}$. This implies that $\#k$ must be congruent to -1 modulo p.

We obtain all information about φ by comparing the corresponding information for $E^\dagger$ and $E \times L_w$. For instance, $\mathcal{E}[\varphi] = \Phi[\varphi]$ and $\Phi'/\varphi(\Phi) = 0$. Similarly $\mathcal{E}'[\hat{\varphi}] \subset \mathcal{E}'^0$ and $\Psi[\hat{\varphi}] = 0$ and $\Phi/\hat{\varphi}(\Phi') = \mu_p$.

The cokernel of $\hat{\varphi} \colon E(K_v) \to E'(K_v)$ is the quotient of $L_w^\times/p$ by $K_v^\times/p$. This is equal to $\mathbb{Z}/p\mathbb{Z}$, because L_w contains μ_p, but K_v does not. The cokernel of φ_{K_v} is trivial.

2.4 The forward non-split case

Finally, we have **non-split** multiplicative reduction, but $\mathcal{E}$ has **less** components than $\mathcal{E}'$.

This case is impossible in fact. Since Φ is of order strictly smaller than Φ', the induced map $\hat{\varphi} \colon \Phi' \to \Phi$ can not be injective. Hence the point P can not reduce to the connected component. But this is impossible because $c'_v = \#\Phi'(k_v)$ is coprime to p if the reduction is non-split multiplicative.

2.5 Summary

Table 1 summarises all results so far in the section.

2.6 Places above p

Let v be a place above p. We have seen so far that the reduction at v is either good, forward split multiplicative or additive. Since the Tamagawa numbers at additive places are coprime to p, the point $P \in E'(K_v)[\hat{\varphi}]$ will reduce to a singular point only in the forward split case.

Recall that we fixed Néron differentials ω and ω' for E and E' respectively. If z is such that $\varphi^*(\omega') = z \cdot \omega$ then we call its valuation $a_v(\varphi) = v(z)$ the *Néron scaling* of φ at v. Similar, we define $a_v(\hat{\varphi})$ and we have $a_v(\varphi) + a_v(\hat{\varphi}) = e_v = v(p)$. It can be computed easily from the power series expansion of the isogeny restricted to the formal group; in fact, it is simply the valuation of the leading term.

Case	forward	backward	backward
Reduction	split	split	non-split
Components	$pm_v = m'_v$	$m_v = pm'_v$	$m_v = pm'_v$
Tamagawas	$c'_v = pc_v$	$c_v = pc'_v$	$c_v = c'_v = 1$ or 2
$\mathcal{E}^0[\varphi]$	μ_p	0	0
$\Phi[\varphi]$	0	$\mu_p = \mathbb{Z}/p\mathbb{Z}$	μ_p
$\Phi'/\varphi(\Phi)$	$\mathbb{Z}/p\mathbb{Z}$	0	0
$E'(K_v)/\varphi$	$K_v^\times/p$	0	0
$\mathcal{E}'^0[\hat{\varphi}]$	0	$\mathbb{Z}/p\mathbb{Z}$	$\mathbb{Z}/p\mathbb{Z}$
$\Phi'[\hat{\varphi}]$	$\mathbb{Z}/p\mathbb{Z}$	0	0
$\Phi/\hat{\varphi}(\Phi')$	0	$\mathbb{Z}/p\mathbb{Z}$	μ_p
$E(K_v)/\hat{\varphi}$	0	$K_v^\times/p$	$\mathbb{Z}/p\mathbb{Z}$
$\#k_v$	any	$\equiv 1 \pmod{p}$	$\equiv -1 \pmod{p}$

Table 1: Summary on multiplicative cases

We can now make precise how we can weaken the condition (Hyp 5') in the introduction. A place v is called *forward* if $a_v(\hat{\varphi}) = 0$ and *backward* if $a_v(\varphi) = 0$. Note that forward split places above p are indeed forward, so there is no contradition with the previous definition.

(Hyp 5). All places above p are either forward or backward for φ. Moreover, if a place $v \mid p$ is backward, then we impose that $\mu_p(K_v) = 1$.

Of course, if p is unramified in $K/\mathbb{Q}$ then this condition is automatically satisfied, in other words hypothesis (Hyp 5) implies hypothesis (Hyp 5'). We will see that this new hypothesis may only restrict the situation in the presence of places of good supersingular reduction above p or additive places with potential supersingular reduction. The former can only arise when the ramification index at the place is larger than $p - 1$.

Lemma 2.2. *If the reduction is good ordinary or potentially good ordinary at a place v above p then either $a_v(\varphi) = 0$ or $a_v(\hat{\varphi}) = 0$.*

Proof. We treat first the case when E has good ordinary reduction. Since the formal group is of height 1, either φ or $\hat{\varphi}$ induces on the reduction a separable isogeny. A separable isogeny between elliptic curves induces an injection on differential forms, so the Néron scaling for this isogeny has to be zero.

More precisely, if P reduces to a non-zero point in the reduction, then $\hat{\varphi}$ is separable on the reduction. Hence $a_v(\hat{\varphi}) = 0$ and so the place is forward.

Otherwise, if P reduces to the zero point in the reduction, then $\hat{\varphi}$ induces a purely inseparable isogeny on the reduction, so φ has to induce a separable isogeny. Hence $a_v(\varphi) = 0$ and the place is backward. In this case, P belongs to the formal group and by [28, Theorem IV.6.1] this implies that $e_v > p - 1$.

The cases of multiplicative reduction have already been treated, so we may pass to the case when E has additive, potentially good or multiplicative reduction at v. So the Kodaira type is I_n^* for some $n \geqslant 0$ and there is a quadratic ramified extension L_w/K_v such that $E \times L_w$ has semistable reduction. Write w for its normalised valuation. Fix a minimal equation of E/K_v. Let u be coefficient needed in the transformation of the Weierstrass equation to become minimal over L_w: More precisely u will be such that $u \cdot \omega_{E/L_w} = \omega_{E/K_v}$ holds for the corresponding Néron differentials. Therefore the minimal discriminants satisfy $\Delta_{E/K_v} = u^{12} \cdot \Delta_{E/L_w}$. From [27, p. 365] we find that $v(\Delta_{E/K_v}) = 6 + n$.

The type over L_w will be I_{2n} and so $w(\Delta_{E/L_w}) = 2n$. Hence we get $2 \cdot (6 + n) = 12 \cdot w(u) + 2n$ and we conclude that u is a uniformiser of L_w. The same argument will apply to the corresponding coefficient u' for E'. Write z_w for the constant such that $\varphi^*(\omega_{E'/L_w}) = z_w \cdot \omega_{E/L_w}$ whose valuation is the Néron scaling of φ over L_w. Now

$$\varphi^*(\omega_{E'/K_v}) = \varphi^*(u' \cdot \omega_{E'/L_w}) = u' \cdot z_w \cdot \omega_{E/L_w} = \frac{u'}{u} \cdot z_w \cdot \omega_{E/K_v}$$

shows that if the Néron scaling of φ over L_w is zero, then $a_v(\varphi) = 0$. By the same argument, if the Néron scaling of $\hat\varphi$ over L_w is zero, then $a_v(\hat\varphi) = 0$. So the previous treated semistable ordinary cases imply the result for the additive potentially ordinary case. $\qquad\square$

If instead the reduction is good and supersingular, then both $a_v(\varphi)$ and $a_v(\hat\varphi)$ are positive as $[p]$ is purely inseparable. It follows as before that this can only occur when $e_v > p - 1$. For instance, if E' is the curve 37a1 and K is the field $\mathbb{Q}(P)$ over which it admits a point P of order 3, then $a_v(\varphi) = 6$ and $a_v(\hat\varphi) = 2$ for one of the places above 3. At the supersingular places above p the special fibre of the group schemes $\mathcal{E}[\varphi]$ and $\mathcal{E}'[\hat\varphi]$ are both equal to the group scheme α_p.

Lemma 2.3. *Let v be a place above p. If $e_v < p - 1$ and E is semistable, then v is forward.*

Proof. We have seen in the proof of the previous Lemma that all good places are forward if $e_v < p-1$. The same is true for split multiplicative places and there are no non-split multiplicative places above p. $\qquad\square$

Note that the semistability condition is necessary: The example of the elliptic curve labeled 126a1 in Cremona's tables shows that there are curves even defined over $\mathbb{Q}$ with additive backwards places.

Lemma 3.8 in [25] says that for an isogeny $\psi\colon A \to A'$ between elliptic curves, we have

$$\#A'(K_v)/\psi\big(A(K_v)\big) = (\#k_v)^{a_v(\psi)} \cdot \#A(K_v)[\psi] \cdot \frac{c_v(A')}{c_v(A)}$$

where the last is the ratio of Tamagawa numbers. Let n_v be the degree of K_v over $\mathbb{Q}_p$. Taking into account that $\#E(K_v)[\varphi] = \#\mu_p(K_v) = 1$ for all backward places above p, we deduce from it the following.

$$\#E'(K_v)/\varphi(E(K_v)) = \begin{cases} p^{n_v+1} & \text{if } v \text{ is forward split multiplicative} \\ p^{n_v} & \text{otherwise} \\ 1 & \text{if } v \text{ is backward} \end{cases} \qquad (2)$$

and similarly that

$$\#E(K_v)/\hat\varphi(E'(K_v)) = \begin{cases} 1 & \text{if } v \text{ is backward} \\ p & \text{otherwise} \\ p^{n_v+1} & \text{if } v \text{ is forward split multiplicative} \end{cases} \qquad (3)$$

Note that forward places above p where E does not have multiplicative reduction appear in the middle terms labeled "otherwise".

Lemma 2.4. *Let v be a place above p which is forward. Then $\mathcal{E}'[\hat\varphi] = {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$ as (finite flat) group schemes over $\mathcal{O}_v$. If moreover the reduction is not additive, then $\mathcal{E}[\varphi] = \mu_p$.*

Proof. If the reduction is multiplicative, we know the result already. Assume that the reduction is not multiplicative, so P reduces to a non-singular point.

Let t be a parameter of the formal group of E' with respect to a minimal Weierstrass model. We must have that the formal expansion of $\hat{\varphi}$ is of the form t times a unit power series in t with coefficients in $\mathcal{O}_v$. It induces therefore an isomorphism on the formal groups. Hence the point P in the kernel of $\hat{\varphi}$ can not lie in the formal group and so it reduces to a non-zero, non-singular point in the reduction, i.e. it meets the special fibre of $\mathcal{E}'$ at a non-zero point of the connected component. Hence $\mathcal{E}'[\hat{\varphi}]$ is indeed isomorphic to $\mathbb{Z}/_{p\mathbb{Z}}$ over $\mathcal{O}_v$.

If the reduction is good, then the kernel of φ is the Cartier dual of the kernel of $\hat{\varphi}$ and hence it is equal to μ_p. $\qquad\square$

We note that we can not say that $\mathcal{E}[\varphi] = \mu_p$ if the reduction is additive. In fact the kernel may well not be quasi-finite and hence not flat either. As an example, we can take the curve $E/\mathbb{Q}$ with label 50b4 in Cremona's tables. It admits an isogeny φ of degree 5 to 50b2 satisfying our hypothesis, but the reduction at $v = 5$ is additive (of type II*). The type of φ is forward. It is easy to see that the reduction of the isogeny on the connected component of $\mathcal{E}$ is the zero map and hence we get that the fibre of $\mathcal{E}[\varphi]$ over $\mathbb{F}_5$ is equal to $\mathbf{G}_a$.

2.7 The image of the local Kummer map

For each place v, there are Kummer maps

$$\kappa_v \colon E'(K_v)/\varphi(E(K_v)) \to H^1\big(K_v, E[\varphi]\big) \cong H^1\big(K_v, \mu_p\big) \cong K_v^\times/p$$
$$\kappa'_v \colon E(K_v)/\hat{\varphi}(E'(K_v)) \to H^1\big(K_v, E'[\hat{\varphi}]\big) \cong H^1\big(K_v, \mathbb{Z}/_{p\mathbb{Z}}\big) \cong \mathrm{Hom}\big(K_v^\times/p, \mathbb{Z}/_{p\mathbb{Z}}\big)$$

The very last isomorphism is given by the local reciprocity map. Our aim is to compare the image of κ_v with the natural subgroup $H^1(\mathcal{O}_v, \mu_p) = \mathcal{O}_v^\times/p$.

We now define two finite sets of places. First

$$S_1 = \Big\{ \text{ all forward split multiplicative places}\Big\}. \tag{4}$$

In other words, it is the set of all places (above p or outside p) where E has split multiplicative reduction and the Tamagawa number of E' is larger than the one of E. The second set is defined as

$$S_2 = \Big\{\text{all backward places}\Big\}. \tag{5}$$

So this set S_2 contains the places (outside p) where E has non-split multiplicative reduction or split multiplicative reduction for which the Tamagawa number of E is larger than the one of E', and it contains the places above p for which we have $\varphi^*(\omega') \in \mathcal{O}_v^\times \omega$. The two sets are disjoint.

Proposition 2.5. *For all finite places v*

$$\mathrm{Im}(\kappa_v) = \begin{cases} K_v^\times/p & \text{if } v \in S_1 \\ \mathcal{O}_v^\times/p & \text{otherwise} \\ 0 & \text{if } v \in S_2 \end{cases}$$

$$\mathrm{Im}(\kappa'_v) = \begin{cases} H^1(K_v, \mathbb{Z}/_{p\mathbb{Z}}) & \text{if } v \in S_2 \\ H^1(\mathcal{O}_v, \mathbb{Z}/_{p\mathbb{Z}}) \cong \mathbb{Z}/_{p\mathbb{Z}} & \text{otherwise} \\ 0 & \text{if } v \in S_1 \end{cases}$$

Proof. Our computations in (2) and (3) for places above p and our local computations for multiplicative places, summarised in section 2.5, show that at least all of the above groups that should be equal have the same size. It remains to prove that $\text{Im}(\kappa_v)$ lies in $H^1(\mathcal{O}_v, \mu_p) = \mathcal{O}_v^\times/p$ and that $\text{Im}(\kappa_v')$ lies in $H^1(\mathcal{O}_v, \mathbb{Z}/p\mathbb{Z})$ if $v \notin S_1 \cup S_2$, i.e. if the reduction is neither forward split multiplicative nor backward.

The image of κ_v is equal to the image from $\mathcal{E}'^0(\mathcal{O}_v)/\varphi(\mathcal{E}^0(\mathcal{O}_v))$ if the reduction is not split multiplicative as the Tamagawa numbers are coprime to p. For places $v \nmid p$, we can invoke Lemma 3.1 in [26], which shows that the image of κ_v lies in the unramified part of the local cohomology, i.e. in $H^1(\mathcal{O}_v, \mathcal{E}[\varphi]) = H^1(\mathcal{O}_v, \mu_p)$. Similar for κ_v'.

So we are reduced to the case of good or additive reduction at a place above p not in S_1 or S_2. Otherwise, we can use Lemma 2.4 as follows. We have the corresponding Kummer map for the exact sequence

$$0 \longrightarrow \mathcal{E}'^0[\hat{\varphi}] \longrightarrow \mathcal{E}'^0 \longrightarrow \mathcal{E}^0 \longrightarrow 0$$

of sheaves on the fppf site, giving us

$$
\begin{array}{ccc}
E(K_v)/\hat{\varphi}(E'(K_v)) & == & \mathcal{E}'^0(\mathcal{O}_v)/\hat{\varphi}(\mathcal{E}^0(\mathcal{O}_v)) \\
& & \downarrow \\
& & H^1(\mathcal{O}_v, \mathcal{E}'^0[\hat{\varphi}]) == H^1(\mathcal{O}_v, \mathcal{E}'[\hat{\varphi}]) == H^1(\mathcal{O}_v, \mathbb{Z}/p\mathbb{Z}).
\end{array}
$$

This shows the equality for $\text{Im}(\kappa_v')$. By Lemma 2.4 in [12], $\text{Im}(\kappa_v)$ is the exact orthogonal to $\text{Im}(\kappa_v')$ under the non-degenerate pairing $H^1(K_v, \mu_p) \cup H^1(K_v, \mathbb{Z}/p\mathbb{Z}) \to \mathbb{Z}/p\mathbb{Z}$. Hence, by local duality $\text{Im}(\kappa_v)$ is equal to $H^1(\mathcal{O}_v, \mu_p)$. $\square$

3 Descent via p-isogeny

There are many good and very readable accounts on descent on elliptic curves, see for instance [26, 9, 10]. We are here in the special case of an isogeny with kernel μ_p and wish to rely fully on this assumption. However, we are only interested in the φ-Selmer group rather than the p-Selmer group and hence we won't perform a full descent. Note that for $p = 5$ and $p = 7$, Fisher's thesis [11] contains much more for the case $K = \mathbb{Q}$. In our approach, we follow and generalise [21] for computing the Selmer groups $\text{Sel}^\varphi(E/K)$ and $\text{Sel}^{\hat{\varphi}}(E'/K)$. However, we will reformulate their results in flat cohomology for μ_p and $\mathbb{Z}/p\mathbb{Z}$.

By local duality, see Lemma III.1.1 and Theorem III.1.3 in [22], we have the short exact sequence

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & H^1(\mathcal{O}_v, \mu_p) & \longrightarrow & H^1(K_v, \mu_p) & \longrightarrow & H^1(\mathcal{O}_v, \mathbb{Z}/p\mathbb{Z})^\vee & \longrightarrow & 0 \\
& & \| & & \| & & \downarrow \cong & & \\
0 & \longrightarrow & \mathcal{O}_v^\times/p & \longrightarrow & K_v^\times/p & \xrightarrow{v} & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & 0
\end{array}
$$

where $A^\vee = \text{Hom}(A, \mathbb{Q}/\mathbb{Z})$ denotes the Pontryagin dual of A. The middle term is also dual to $H^1(K_v, \mathbb{Z}/p\mathbb{Z})$.

For any open U in $\text{Spec}(\mathcal{O}_K)$, we have an explicit description of the flat cohomology of μ_p and $\mathbb{Z}/p\mathbb{Z}$. On the one hand, we have

$$
\begin{aligned}
H^1(U, \mu_p) &= \ker\Big(H^1(K, \mu_p) \to \bigoplus_{v \in U} H^1(\mathcal{O}_v, \mathbb{Z}/p\mathbb{Z})^\vee \Big) \\
&= \big\{ x \in K^\times/p \mid v(x) \equiv 0 \pmod{p} \ \forall\, v \in U \big\},
\end{aligned}
$$

9

saying that the local conditions at places in U is that the image should lie in the subgroup $H^1(\mathcal{O}_v, \mu_p)$. Furthermore this fits into the exact sequence

$$0 \longrightarrow \mathcal{O}_{K,S}^\times/p \longrightarrow H^1(U, \mu_p) \longrightarrow \mathrm{Cl}(\mathcal{O}_{K,S})[p] \longrightarrow 0,$$

where S is the complement of U.

On the other hand,

$$H^1(U, \mathbb{Z}/p\mathbb{Z}) = \ker\Big(H^1(K, \mathbb{Z}/p\mathbb{Z}) \to \bigoplus_{v \in U} H^1(\mathcal{O}_v, \mu_p)^\vee \Big).$$

This group classifies cyclic extensions of K of degree p which are unramified at all places in U. So by global class field theory, we have $H^1(\mathcal{O}_K, \mathbb{Z}/p\mathbb{Z}) \cong \mathrm{Hom}(\mathrm{Cl}(K), \mathbb{Z}/p\mathbb{Z})$.

The Selmer group $\mathrm{Sel}^\varphi(E/K)$ is defined to be the subgroup of $H^1(K, E[\varphi])$ whose restriction to $H^1(K_v, E[\varphi])$ lie in the image of the local Kummer map

$$\kappa_v \colon E'(K_v)/\varphi(E(K_v)) \to H^1(K_v, E[\varphi]).$$

Since $E[\varphi] = \mu_p$ over K and over $\mathcal{O}_v$ at all places v outside p, it is natural to compare this Selmer group to the corresponding "Selmer group" $H^1(\mathcal{O}_K, \mu_p)$ for μ_p. In other words, we will compare the images of the first two terms of the following two exact sequences.

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & E'(K_v)/\varphi(E(K_v)) & \xrightarrow{\ \kappa_v\ } & H^1(K_v, E[\varphi]) & \longrightarrow & H^1(K_v, E)[\varphi] & \longrightarrow & 0 \\
 & & & & \big\| & & & & \\
0 & \longrightarrow & H^1(\mathcal{O}_v, \mu_p) & \xrightarrow{\ \lambda_v\ } & H^1(K_v, \mu_p) & \longrightarrow & H^1(\mathcal{O}_v, \mathbb{Z}/p\mathbb{Z})^\vee & \longrightarrow & 0
\end{array}
$$

The image of $H^1(\mathcal{O}_v, \mu_p)$ can also be described as the unramified cocycles in $H^1(K_v, \mu_p)$.

Recall that we have defined in (4) and (5) two disjoint finite sets of places S_1 and S_2. For $i = 1$ or 2, let U_i be the complement of S_i in $\mathrm{Spec}(\mathcal{O}_K)$.

Theorem 3.1. *Let E/K be an elliptic curve satisfying the hypotheses (Hyp 1) – (Hyp 5) in the introduction. Then we have exact sequences*

$$0 \longrightarrow \mathrm{Sel}^\varphi(E/K) \longrightarrow H^1(U_1, \mu_p) \longrightarrow \bigoplus_{v \in S_2} H^1(\mathcal{O}_v, \mu_p)$$

and

$$0 \longrightarrow \mathrm{Sel}^{\hat\varphi}(E'/K) \longrightarrow H^1(U_2, \mathbb{Z}/p\mathbb{Z}) \longrightarrow \bigoplus_{v \in S_1} H^1(\mathcal{O}_v, \mathbb{Z}/p\mathbb{Z}).$$

Proof. Using Proposition 3.2 in [26], we immediately see that the local conditions for an element in $H^1(K, \mu_p)$ to be in $\mathrm{Sel}^\varphi(E/K)$ are equal to the local conditions to be in $H^1(\mathcal{O}_K, \mu_p)$ for all places where the reduction is not split multiplicative. Proposition 2.5 tells us how to compare the images in the cases when v belongs to either S_1 or S_2 or to none. We have to relax the condition at places in S_1 and we have to impose more stringent conditions at places in S_2. The same argument applies to $\mathrm{Sel}^{\hat\varphi}(E'/K)$ with the roles of S_1 and S_2 interchanged. $\qquad\square$

3.1 Global duality

Theorem 3.2. *Let E/K be an elliptic curve satisfying the hypotheses (Hyp 1) – (Hyp 5) in the introduction. Then we have the following exact sequence*

$$
\begin{array}{cccccc}
0 & \longrightarrow & \mathrm{Sel}^\varphi(E/K) & \longrightarrow & H^1(U_1, \mu_p) & \longrightarrow & \bigoplus_{v \in S_2} H^1(\mathcal{O}_v, \mu_p) \\
\end{array}
\tag{6}
$$

$$
\longrightarrow \mathrm{Sel}^{\hat\varphi}(E'/K)^\vee \longrightarrow \mathrm{Cl}\big(\mathcal{O}_{K,S_1}\big)/p \longrightarrow 0
$$

This is of course a version of the exact sequence found by Cassels, Poitou and Tate.

Proof. Let U_{12} be the intersection of U_1 and U_2. Global duality in flat cohomology (see Corollary III.3.2 and Proposition III.0.4.c in [22]) gives that the image A of $H^1(U_{12}, \mu_p)$ under the localisation maps in $\oplus_{v \in S_1 \cup S_2} H^1(K_v, \mu_p)$ and the image B of $H^1(U_{12}, \mathbb{Z}/p\mathbb{Z})$ in $\oplus_{v \in S_1 \cup S_2} H^1(K_v, \mu_p)$ fit into the short exact sequence

$$0 \longrightarrow A \longrightarrow \bigoplus_{v \in S_1 \cup S_2} H^1(K_v, \mu_p) \longrightarrow B^\vee \longrightarrow 0.$$

If we wish to remove the places in S_1 from the middle term, and replace A by the image A' of $H^1(U_{12}, \mu_p)$ in $\oplus_{v \in S_2} H^1(K_v, \mu_p)$, then we have to replace $B^\vee$ by $B'^\vee$, where B' is the subgroup of B of elements that are trivial in $\oplus_{v \in S_1} H^1(K_v, \mathbb{Z}/p\mathbb{Z})$. Now we have

$$0 \longrightarrow A' \longrightarrow \bigoplus_{v \in S_2} H^1(K_v, \mu_p) \longrightarrow B'^\vee \longrightarrow 0.$$

From Theorem 3.1, we deduce the following two exact sequences

$$0 \longrightarrow \mathrm{Sel}^\varphi(E/K) \longrightarrow H^1(U_{12}, \mu_p) \longrightarrow \bigoplus_{v \in S_2} H^1(K_v, \mu_p),$$

$$0 \longrightarrow \mathrm{Sel}^{\hat{\varphi}}(E'/K) \longrightarrow H^1(U_{12}, \mathbb{Z}/p\mathbb{Z}) \longrightarrow \bigoplus_{v \in S_1} H^1(K_v, \mathbb{Z}/p\mathbb{Z}).$$

This proves that A' is the image of the right hand map in the top exact sequence. Also, it shows that B' is the image of $\mathrm{Sel}^{\hat{\varphi}}(E'/K)$ in $\oplus_{v \in S_2} H^1(K_v, \mathbb{Z}/p\mathbb{Z})$. Gathering the information found so far, we get that

$$0 \longrightarrow \mathrm{Sel}^\varphi(E/K) \longrightarrow H^1(U_{12}, \mu_p) \longrightarrow \bigoplus_{v \in S_2} H^1(K_v, \mu_p) \longrightarrow \mathrm{Sel}^{\hat{\varphi}}(E'/K)^\vee$$

is exact. We compare now this sequence with the one we are aiming to prove:

$$
\begin{array}{ccccccc}
0 \longrightarrow \mathrm{Sel}^\varphi(E/K) & \longrightarrow & H^1(U_{12}, \mu_p) & \longrightarrow & \bigoplus_{v \in S_2} H^1(K_v, \mu_p) & \longrightarrow & \mathrm{Sel}^{\hat{\varphi}}(E'/K)^\vee \\
\| & & \alpha \uparrow & & \beta \uparrow & & \gamma \uparrow \\
0 \longrightarrow \mathrm{Sel}^\varphi(E/K) & \longrightarrow & H^1(U_1, \mu_p) & \xrightarrow{\delta} & \bigoplus_{v \in S_2} H^1(\mathcal{O}_v, \mu_p) & \longrightarrow & \mathrm{coker}\,\delta \longrightarrow 0.
\end{array}
$$

The injectivity of α and β gives an exact sequence

$$0 \longrightarrow \ker \gamma \longrightarrow \mathrm{coker}\,\alpha \longrightarrow \mathrm{coker}\,\beta.$$

By definition, the cokernel of α is a subgroup of the group $\oplus_{v \in S_2} H^1(\mathcal{O}_v, \mathbb{Z}/p\mathbb{Z})^\vee$ which is equal to the cokernel of β. Hence $\ker \gamma = 0$ and we shown the exactness of the first four non-zero terms of the exact sequence (6). It remains to find the kernel of the map

$$\mathrm{Sel}^{\hat{\varphi}}(E'/K) \longrightarrow \bigoplus_{v \in S_2} H^1(\mathcal{O}_v, \mu_p)^\vee. \tag{7}$$

This is given by elements of $H^1(U_{12}, \mathbb{Z}/p\mathbb{Z})$ that map to zero in $H^1(K_v, \mathbb{Z}/p\mathbb{Z})$ for $v \in S_1$ and to elements in $H^1(\mathcal{O}_v, \mathbb{Z}/p\mathbb{Z})$ for $v \in S_2$. In other words it is equal to the kernel of

$$H^1(U_1, \mathbb{Z}/p\mathbb{Z}) \longrightarrow \bigoplus_{v \in S_1} H^1(K_v, \mathbb{Z}/p\mathbb{Z})$$

which, again by global duality, is dual to the kernel of $H^2(U_1, \mu_p) \to \oplus_{v \in S_1} H^2(K_v, \mu_p)$. The latter is simply the Brauer group $\mathrm{Br}(K_v)[p]$, while the first sits in an exact sequence

$$0 \longrightarrow \mathrm{Pic}(U_1)/p \longrightarrow H^2(U_1, \mu_p) \longrightarrow \mathrm{Br}(U_1)[p] \longrightarrow 0.$$

By global class field theory, the localisation map on the Brauer groups is injective and so we find that the kernel of (7) is dual to $\mathrm{Pic}(U_1)/p = \mathrm{Cl}(\mathcal{O}_{K,S_1})/p$. $\qquad\square$

Corollary 3.3. *With the same assumption as in Theorem 3.2, we have*

$$\dim_{\mathbb{F}_p} \mathrm{Sel}^{\varphi}(E/K) - \dim_{\mathbb{F}_p} \mathrm{Sel}^{\hat{\varphi}}(E'/K) = \#S_1 + \#\{v \mid \infty\} - \sum_{v \in S_2} n_v + \dim_{\mathbb{F}_p}(\mu_p(K)) - 1$$

where $n_v = [K_v : \mathbb{Q}_p]$ if $v \mid p$ and $n_v = 1$ otherwise.

Proof. Note first that $\#H^1(U_1, \mu_p) = \# \mathrm{Cl}(U_1)[p] \cdot \#\mathcal{O}_{K,S_1}^{\times}/p$. Then the local term $H^1(\mathcal{O}_v, \mu_p) = \mathcal{O}_v^{\times}/p$ is of order p for all places in S_2 outside p because $\mathcal{O}_v$ contains μ_p as we discovered in section 2.2. For all places in S_2 above p, we have $\#\mathcal{O}_v^{\times}/p = p^{n_v}$ as by assumption (Hyp 5) the p-th roots of unity are not contained in K_v. Finally the dimension of $\mathcal{O}_{K,S_1}^{\times}/p$ is $\#S_1 + \#\{v \mid \infty\} + \dim_{\mathbb{F}_p}(\mu_p(K)) - 1$ by Dirichlet's units Theorem. $\qquad\square$

Analogous to Theorem 3.2, we could show that

$$0 \longrightarrow \mathrm{Sel}^{\hat{\varphi}}(E'/K) \longrightarrow H^1(U_2, \mathbb{Z}/p\mathbb{Z}) \longrightarrow \bigoplus_{v \in S_1} H^1(\mathcal{O}_v, \mathbb{Z}/p\mathbb{Z})$$
$$\longrightarrow \mathrm{Sel}^{\varphi}(E/K)^{\vee} \longrightarrow H^2(U_2, \mathbb{Z}/p\mathbb{Z}) \longrightarrow 0.$$

Remark 3.4. One can deduce from these computations some upper and lower bounds on the size of the groups involved. For example, with the same assumption as in Theorem 3.2, we have, using the notations from the previous Corollary,

$$\dim_{\mathbb{F}_p}(\mathrm{Cl}(\mathcal{O}_{K,S_1})/p) \leqslant \dim_{\mathbb{F}_p} \mathrm{Sel}^{\hat{\varphi}}(E'/K) \leqslant \dim_{\mathbb{F}_p}(\mathrm{Cl}(\mathcal{O}_{K,S_1})/p) + \sum_{v \in S_2} n_v$$

and a similar inequality for $\mathrm{Sel}^{\varphi}(E/K)$ can be deduced via Corollary 3.3.

A particular case, in which we can say more is when we have $S_2 = \emptyset$. This is the case, for example, when p does not divide the product $\prod c_v$ of Tamagawa numbers of E and E has semistable reduction at all places above p. Write $\mathrm{Sel}^p(E/K)$ for the p-Selmer group in $H^1(K, E[p])$.

Corollary 3.5. *If $S_2 = \emptyset$, then we have*

$$\mathrm{Sel}^{\varphi}(E/K) = H^1(U_1, \mu_p) \quad and \quad \mathrm{Sel}^{\hat{\varphi}}(E'/K) = (\mathrm{Cl}(\mathcal{O}_{K,S_1})/p)^{\vee}$$

If in addition $S_1 \neq \emptyset$ and $\dim_{\mathbb{F}_p}(\mathrm{Cl}(\mathcal{O}_{K,S_1})/p) \leqslant 1$, then

$$\dim_{\mathbb{F}_p} \mathrm{Sel}^p(E/K) = 2 \cdot \dim_{\mathbb{F}_p}(\mathrm{Cl}(\mathcal{O}_{K,S_1})/p) + \#S_1 + \#\{v \mid \infty\} - 2$$

Proof. The first point follows immediately from Theorem 3.2. Now, we have an exact sequence

$$E'(K)[\hat{\varphi}] \longrightarrow \mathrm{Sel}^\varphi(E/K) \longrightarrow \mathrm{Sel}^p(E/K) \longrightarrow \mathrm{Sel}^{\hat{\varphi}}(E'/K) \longrightarrow T \longrightarrow 0$$

where T is an abelian group whose order is a square by the Cassels-Tate pairing as shown in Corollary 17 in [32] for instance. If we assume that $\mathrm{Cl}(\mathcal{O}_{K,S_1})/p$ is trivial or a group of order p, then $T = 0$. If we also assume that $S_1 \neq \emptyset$, then the first map in the sequence is injective, because of Lemma 5.5. The result follows. □

4 Class group pairings

Recall that in this section, we do not have to make the hypotheses (Hyp 1) – (Hyp 5). Instead they will hold for any elliptic curve over a number field. To see the duality better, we formulate the first part in general for abelian varieties.

4.1 Classical case

Let A be an abelian variety defined over K, and let $\mathcal{A}$ be its Néron model over $X = \mathrm{Spec}(\mathcal{O}_K)$. We denote by $\Phi = \mathcal{A}/\mathcal{A}^0 = \bigoplus_v \Phi_v$ the group of components of $\mathcal{A}$. Let $Z \subset X$ denotes the set of places of bad reduction of $\mathcal{A}$.

If Γ is some (open) subgroup of Φ, we denote by $\mathcal{A}^\Gamma$ the inverse image of Γ by the canonical projection. Thus, $\mathcal{A}^\Gamma$ is an open subgroup scheme of $\mathcal{A}$ having the same generic fibre and whose component group is Γ.

Let A^t be the dual abelian variety of A, and let $\mathcal{A}^t$ be its Néron model. Let us recall briefly that the duality between A and A^t is encoded in the Poincaré line bundle, which has a canonical structure of a biextension. We call this biextension the Weil biextension, denoted by W_K.

We may ask if there is a biextension of $(\mathcal{A}, \mathcal{A}^t)$ by $\mathbf{G}_m$ extending W_K. In [17, exposé VIII, théorème 7.1, b)] Grothendieck defined the so-called monodromy pairing, which is an obstruction to the existence of such a biextension.

More precisely, let Φ^t be the group of components of $\mathcal{A}^t$. The monodromy pairing is a bilinear map of group schemes

$$\Phi \times \Phi^t \longrightarrow \bigoplus_{v \in Z} {}^{\mathbb{Q}}\!/_{\mathbb{Z}} \cdot v$$

In *loc. cit.*, Grothendieck proved the following: If Γ and Γ' are subgroups that are orthogonal under the monodromy pairing, then there exists a unique biextension of $(\mathcal{A}^\Gamma, \mathcal{A}^{t,\Gamma'})$ by $\mathbf{G}_m$ extending W_K, which we denote by $W^{\Gamma,\Gamma'}$. The main tool we will need is not $W^{\Gamma,\Gamma'}$ itself, but rather its underlying $\mathbf{G}_m$-torsor on $\mathcal{A}^\Gamma \times_S \mathcal{A}^{t,\Gamma'}$, which we will denote by $t(W^{\Gamma,\Gamma'})$.

We now recall the definition of the class group pairing introduced by Mazur and Tate in [20, Remark 3.5.3], but going back to earlier work by Manin, Néron and Tate. Suppose again that Γ and Γ' are orthogonal under the monodromy pairing. The class group pairing associated to the couple (Γ, Γ') is the bilinear map defined by

$$\mathcal{A}^\Gamma(X) \times \mathcal{A}^{t,\Gamma'}(X) \longrightarrow \mathrm{Pic}(X)$$
$$(Q, R) \longmapsto \langle Q, R \rangle^{\mathrm{cl}} := (Q \times R)^* \Big(t\big(W^{\Gamma,\Gamma'}\big) \Big).$$

It is also possible to refine this pairing as follows. Let $S \subset X$ be a finite set of finite primes of K, and let $V \subseteq X$ be the complement of S. Then we define the S-class group pairing as

$$\mathcal{A}^\Gamma(V) \times \mathcal{A}^{t,\Gamma'}(V) \longrightarrow \mathrm{Pic}(V)$$
$$(Q, R) \longmapsto \langle Q, R \rangle^{\mathrm{cl}}_S := (Q \times R)^* \Big(t\big(W^{\Gamma,\Gamma'}\big) \Big)$$

where Γ and Γ' are as before. In short, the pairing $\langle \cdot, \cdot \rangle_S^{cl}$ is defined on a bigger group that $\langle \cdot, \cdot \rangle^{cl}$ and has values in $\mathrm{Cl}(\mathcal{O}_{K,S})$. If we take $S = Z$, then $\mathcal{A}^\Gamma(V) = A(K)$ so the pairing $\langle Q, R \rangle_Z^{cl}$ is defined without any restriction on the points P and Q.

4.2 Logarithmic case

Let us recall here some results from [14]. We refer to this article for definitions and conventions concerning log schemes.

Let $U \subseteq X$ be the complement of Z. We denote by $X(\log Z)$ the scheme X endowed with the log structure induced by U, see Definition 2.1.1. in [14]. First, we recall Proposition 4.2.1 in [14].

Proposition 4.1. *There exists a unique biextension $W^{\log}$ of $(\mathcal{A}, \mathcal{A}^t)$ by $\mathbf{G}_m$ for the log flat topology on $X(\log Z)$ extending Weil's biextension W_K.*

We denote by $\mathrm{LogPic}(X, Z)$ the group $H^1_{\mathrm{kpl}}(X(\log Z), \mathbf{G}_m)$ of $\mathbf{G}_m$-torsors for the Kummer log flat topology. From the existence of $W^{\log}$, we deduce a pairing

$$
\begin{aligned}
\mathcal{A}(X) \times \mathcal{A}^t(X) &\longrightarrow \mathrm{LogPic}(X, Z) \\
(Q, R) &\longmapsto \langle Q, R \rangle^{\log} := (Q \times R)^* \left(t(W^{\log}) \right)
\end{aligned}
$$

that we call the logarithmic class group pairing.

The group $\mathrm{LogPic}(X, Z)$ has the following description (see [14, 3.1.3])

$$
\mathrm{LogPic}(X, Z) = \left(\mathrm{Div}(U) \oplus \bigoplus_{v \in Z} \mathbb{Q} \cdot v \right) / \mathrm{DivPrinc}(X),
$$

where $\mathrm{DivPrinc}(X)$ denotes the subgroup of (usual) principal divisors on X. In other words, $\mathrm{LogPic}(X, Z)$ is the group of divisors on X with rational coefficients above Z modulo principal divisors. Of course, if $Z' \subseteq Z$ is a subset of Z, then $\mathrm{LogPic}(X, Z')$ is a subgroup of $\mathrm{LogPic}(X, Z)$. In particular, the group $\mathrm{Pic}(X)$ is a subgroup of $\mathrm{LogPic}(X, Z)$, and we have an exact sequence

$$
0 \longrightarrow \mathrm{Pic}(X) \longrightarrow \mathrm{LogPic}(X, Z) \overset{\nu}{\longrightarrow} \bigoplus_{v \in Z} \mathbb{Q}/\mathbb{Z} \cdot v \longrightarrow 0. \tag{8}
$$

The following Proposition explains how the logarithmic class group pairing is linked to the class group pairing and the monodromy pairing. We recall Proposition 4.3.2 in [14].

Proposition 4.2.   *1. Let Γ and Γ' be orthogonal subgroups as before. Then the restriction of $\langle \cdot, \cdot \rangle^{\log}$ to $\mathcal{A}^\Gamma(X) \times \mathcal{A}^{t, \Gamma'}(X)$ is equal to $\langle \cdot, \cdot \rangle^{cl}$.*

2. We have a commutative diagram

$$
\begin{array}{ccc}
\mathcal{A}(X) \times \mathcal{A}^t(X) & \overset{\langle \cdot, \cdot \rangle^{\log}}{\longrightarrow} & \mathrm{LogPic}(X, Z) \\
\downarrow & & \downarrow{\scriptstyle \nu} \\
\Phi(X) \times \Phi'(X) & \longrightarrow & \bigoplus_{v \in Z} \mathbb{Q}/\mathbb{Z} \cdot v
\end{array}
$$

where the horizontal lower arrow is induced by the monodromy pairing, and the vertical arrow on the left is the reduction map.

We also have a natural surjection

$$
\mathrm{LogPic}(X, Z) \longrightarrow \mathrm{Pic}(U)
$$

whose kernel is the subgroup generated by classes with support in Z. When composing the logarithmic class group pairing with this map, we recover the Z-class group pairing defined at the end of section 4.1.

4.3 A remark on metrics

Let us denote by $\widehat{\mathrm{Pic}}(\mathcal{O}_{K,Z})$ the group of locally free $\mathcal{O}_{K,Z}$-modules of rank one endowed with metrics at all places in Z. Then, using the description of $\widehat{\mathrm{Pic}}(\mathcal{O}_{K,Z})$ in terms of idèles, it is easy to check that

$$\widehat{\mathrm{Pic}}(\mathcal{O}_{K,Z})_{\mathrm{tors}} \simeq \mathrm{LogPic}(X, Z). \tag{9}$$

It is to note that elements in $\widehat{\mathrm{Pic}}(\mathcal{O}_{K,Z})$ have no metrics at infinite places. If we add metrics at infinite places, then we get the so-called Arakelov class group of $\mathcal{O}_{K,Z}$. More precisely, $\widehat{\mathrm{Pic}}(\mathcal{O}_{K,Z})$ is a quotient of the Arakelov class group by the natural subgroup isomorphic to $\mathbb{R} \times (\mathbb{R}/\mathbb{Z})^{\#\{v|\infty\}-1}$.

However, it is possible to endow the Poincaré line bundle on $\mathcal{E}_U \times \mathcal{E}_U$ with natural metrics at places in Z. As a result, we get a metrised class group pairing

$$\mathcal{E}(U) \times \mathcal{E}(U) \to \widehat{\mathrm{Pic}}(\mathcal{O}_{K,Z})$$

and it is easy to check that this metrised pairing is equal to the logarithmic class group pairing via (9). Thus, the logarithmic techniques we use here are closely related to the techniques of Agboola and Pappas in [3]. The main difference is that we do not put metrics at infinite places.

4.4 The explicit computation of the pairing

Here we explain how we are able to compute numerically values of the logarithmic class group pairing on an elliptic curve. Via the Proposition 4.2, this will also give an explicit formula for the class group pairing

$$\langle \cdot, \cdot \rangle^{\mathrm{cl}} : \mathcal{E}(\mathcal{O}_K) \times \mathcal{E}^0(\mathcal{O}_K) \longrightarrow \mathrm{Pic}(X) = \mathrm{Cl}(K)$$

and we recover the monodromy pairing as described in [5, Example 5.8].

The first step is to give an alternative description of our pairing. Let us denote by $f : \mathcal{E} \to X = \mathrm{Spec}(\mathcal{O}_K)$ the structural morphism and by O the unit section of $\mathcal{E}$. If $Q : X \to \mathcal{E}$ is a section of $\mathcal{E}$, then the image of Q is a divisor on $\mathcal{E}$, and we will denote by $[Q]$ the class of this divisor in $\mathrm{Pic}(\mathcal{E})$, just as we write $[D]$ for the class of any divisor D in $\mathrm{Pic}(\mathcal{E})$ and $\mathrm{LogPic}(\mathcal{E}, Z)$. If $\mathcal{L}$ is a line bundle on $\mathcal{E}$, we define the rigidified line bundle associated to $\mathcal{L}$ by the formula

$$\mathcal{L}^{\mathrm{rig}} := \mathcal{L} - f^* O^* \mathcal{L}$$

Note that, for any point $R \in \mathcal{E}(\mathcal{O}_K)$ we get $R^* \mathcal{L}^{\mathrm{rig}} = R^* \mathcal{L} - O^* \mathcal{L}$.

Proposition 4.3. *Let $Q \in \mathcal{E}(\mathcal{O}_K)$. Then there exists a fibral divisor F_Q with rational coefficients such that the element*

$$\mathcal{L}_Q := ([Q] - [O])^{\mathrm{rig}} + [F_Q]$$

of $\mathrm{LogPic}(\mathcal{E}, Z)$, satisfies the Theorem of the cube. Moreover:

(i). For all $R \in \mathcal{E}(\mathcal{O}_K)$ we have

$$\langle Q, R \rangle^{\log} = (-R)^* \mathcal{L}_Q = O^* ([Q + R] - [Q] - [R] + [O]) + (-R)^* [F_Q]$$

(ii). The logarithmic line bundle $(-R)^* [F_Q]$ has integral coefficients if and only if (the reductions of) Q and R are orthogonal under the monodromy pairing.

15

(iii). If R belongs to $\mathcal{E}^0(\mathcal{O}_K)$, then $(-R)^*[F_Q] = 0$.

Proof. The existence of F_Q, and the equality $\langle Q, R \rangle^{\log} = -R^*\mathcal{L}_Q$ are rather standard (see [23, chap. III, 1.4] and [14, 4.3]); note that the minus sign is coming from the fact that the generic fibre of the line bundle $\mathcal{L}_Q$ is equal to the inverse of the line bundle attached to Q via the canonical isomorphism $E(K) \simeq \mathrm{Pic}^0(E)$. Thus, we have

$$\langle Q, R \rangle^{\log} = (-R)^*\mathcal{L}_Q = (-R)^*([Q] - [O]) - O^*([Q] - [O]) + (-R)^*[F_Q]$$

Now, let $T_R \colon \mathcal{E} \to \mathcal{E}$ be the translation by R map. For any line bundle $\mathcal{N}$ on $\mathcal{E}$ we have $(-R)^*\mathcal{N} = O^*T_{-R}^*\mathcal{N}$, and for $Q \in \mathcal{E}(S)$ we get $T_{-R}^*[Q] = [Q + R]$. Now, we can write

$$\begin{aligned}
\langle Q, R \rangle^{\log} &= (-R)^*([Q] - [O]) - O^*([Q] - [O]) + (-R)^*[F_Q] \\
&= O^*([Q + R] - [R]) - O^*([Q] - [O]) + (-R)^*[F_Q] \\
&= O^*([Q + R] - [Q] - [R] + [O]) + (-R)^*[F_Q]
\end{aligned}$$

which proves (i). By Proposition 4.2 and the exactness of (8), we see that $\langle Q, R \rangle^{\log}$ belongs to the usual class group if and only if Q and R are orthogonal to each other under Grothendieck's monodromy pairing. By the formula above, this happens if and only if $(-R)^*[F_Q]$ is a divisor with integral coefficients, so (ii) is proved. Finally, if R belongs to $\mathcal{E}^0(\mathcal{O}_K)$, then $T_{-R}^*[F_Q] = [F_Q]$, because F_Q is fibral. Moreover, $\mathcal{L}_Q$ being cubic, it is rigidified, and this immediately implies that $O^*[F_Q] = 0$. Putting that together, we get

$$(-R)^*[F_Q] = O^*T_{-R}^*[F_Q] = O^*[F_Q] = 0$$

which proves (iii). □

We now recall the notion of denominator ideal of a point of E, see [33]. Let $Q \in \mathcal{E}(\mathcal{O}_K) = E(K)$. Given a finite place v in $\mathcal{O}_K$, we choose a minimal Weierstrass equation for E with coefficients in $\mathcal{O}_v$. We set

$$e_v(Q) = -\tfrac{1}{2}\min\big(v(x(Q)), \, 0\big)$$

where $x(Q)$ is the x-coordinate of Q in our chosen equation. On the one hand, if $Q \neq O$, then one defines the divisor (or ideal) $e(Q)$ on $X = \mathrm{Spec}(\mathcal{O}_K)$ by

$$e(Q) := \sum_v e_v(Q) \cdot v.$$

If E admits a global minimal Weierstrass equation, then the ideal $x(Q)\mathcal{O}_K$ can be written as $a(Q) \cdot e(Q)^{-2}$ for some ideals $a(Q)$ and $e(Q)$ in $\mathcal{O}_K$ coprime to each other.

On the other hand, we set $e(O)$ to be the ideal $O^*\mathcal{O}_{\mathcal{E}}(O)$, where $\mathcal{O}_{\mathcal{E}}(O)$ is the sheaf of ideals attached to the divisor defined by O. Now, $e(Q)$ is well defined for any $Q \in \mathcal{E}(\mathcal{O}_K)$ and, using this ideal, we can now compute the first part of $\langle Q, R \rangle^{\log}$.

Lemma 4.4. *Let $Q, R \in \mathcal{E}(\mathcal{O}_K)$. Then*

$$\langle Q, R \rangle^{\log} = [e(Q + R) - e(Q) - e(R) + e(O)] + (-R)^*[F_Q]$$

in the group $\mathrm{LogPic}(X, Z)$.

Proof. When $Q \neq O$, one proves, using intersection theory, that the class $[e(Q)]$ is equal to the pull-back $O^*[Q]$, see [27, p. 250]. Therefore, the formula follows from Proposition 4.3, (i). □

16

Now we choose a Weierstrass equation with coefficients in $\mathcal{O}_K$, corresponding to a choice of an invariant differential ω over K. Then for any finite place v, there is an element $u_v \in \mathcal{O}_v$ such that the equation becomes minimal after a change of variables that makes $u_v^{-1}\omega$ a Néron differential on $\mathcal{E}/\mathcal{O}_v$.

Lemma 4.5. *If we set $e_v(O) = v(u_v)$, then we have $e(O) = \sum_v e_v(O) \cdot v \in \mathrm{Cl}(K)$.*

Proof. From Liu's book [19, §9.4.4, Lemma 4.29] we can extract

$$e(O) = O^*\mathcal{O}_\mathcal{E}(O) = R^1 f_* \mathcal{O}_\mathcal{E}.$$

By Grothendieck duality, we get $e(O) \simeq (f_*\omega_{\mathcal{E}/X})^{-1}$ where $\omega_{\mathcal{E}/X}$ denotes the canonical sheaf. Now ω is a global section of $\omega_{\mathcal{E}/X}$ and, at all place v, the Néron differential $u_v^{-1}\omega$ is a generator of $H^0(\mathcal{O}_v, f_*\omega_{\mathcal{E}/\mathcal{O}_v})$.

Finally, it is to note that the divisor class $\sum_v e_v(O) \cdot v$ does not depend on the choice of ω. If we multiplied ω by an element $\alpha \in K^\times$, then the sum would get changed by adding the term $\sum_v v(\alpha^{-1}) \cdot v$ which is a principal divisor. $\qquad\square$

Remark 4.6. The values of $v(u_v)$ can easily be computed using Tate's algorithm. They also appear as correcting factors to the Tamagawa numbers in the Birch and Swinnerton-Dyer conjecture over K. A consequence of this Lemma, we note that the expression $e(Q) - e(O)$ behaves well under base change.

It is a standard fact (see [19, §9.4, Exercise 4.14]) that

$$\Delta^{-1} \simeq (f_*\omega_{\mathcal{E}/X})^{12}$$

where Δ is the minimal discriminant of E, which is an ideal in $\mathcal{O}_K$. Hence the correction factor $\frac{1}{12}v(\Delta)$ in the local height formula appears as in Theorem VI.4.1 in [27].

Remark 4.7. From the Lemma, we also deduce that $e(O)$ is trivial if and only if there exists a global minimal equation over $\mathcal{O}_K$. Moreover, in this case, it is possible to compute all the $e_v(Q)$ using the same coordinates.

Suppose E/K is an elliptic curve which is coming by base change from an elliptic curve defined over $\mathbb{Q}$. Then, in the case that no place of additive reduction ramifies in $K/\mathbb{Q}$, the global minimal equation over $\mathbb{Q}$ will still be a global minimal equation over K. See Proposition V.1 and Remark V.1.1 in [28].

We now turn to the computation of the divisor F_Q, which will allow us to compute $\langle Q, R \rangle^{\log}$ completely. Let $Q \in \mathcal{E}(\mathcal{O}_K)$. By (iii) of Proposition 4.3, the support of F_Q can not contain the connected component of the fibre at any place v. So F_Q is supported in the bad fibres and we can look individually at each type of bad reduction. So we will fix the place v now and suppose that $\mathcal{E}/\mathcal{O}_v$ has bad reduction.

Let $\mathcal{X}/\mathcal{O}_v$ be the minimal regular model of E/K_v so that $\mathcal{E}$ is the open subscheme of $\mathcal{X}$ obtained by removing multiple components in the special fibre.

Lemma 4.8. *Let $Q \in \mathcal{E}(\mathcal{O}_v)$. There exists a unique fibral divisor G_Q on $\mathcal{X}$ such that the intersection $\Gamma.([Q] - [O] + [G_Q])$ is trivial for all fibral divisors Γ on $\mathcal{X}$ and such that G_Q intersects the connected component $\mathcal{E}^0$ trivially. Moreover, F_Q is the intersection of G_Q with $\mathcal{E}$.*

Proof. Recall that F_Q is a fibral divisor (with rational coefficients) such that

$$\mathcal{L}_Q = [Q] - [O] + [F_Q]$$

17

satisfies the Theorem of the cube. Moreover, such an F_Q is unique up to addition of an integral multiple of the special fibre of $\mathcal{E}$ (which is a principal divisor). Therefore, there exists a unique such F_Q whose support does not contains the connected component Γ_0. Let n be the exponent of the group of components of $\mathcal{E}$. As nQ falls into the connected component of $\mathcal{E}$, we have

$$\mathcal{L}_{nQ} = [nQ] - [O]$$

that is, $[F_{nQ}] = 0$. On the other hand, we have $\mathcal{L}_{nQ} = n\mathcal{L}_Q$ because the map $Q \mapsto \mathcal{L}_Q$ is a morphism of groups. Let f be a meromorphic section of the generic fibre of $\mathcal{L}$, then $f^{\otimes n}$ is a meromorphic section of the generic fibre of $\mathcal{L}_{nQ}$, and this meromorphic section can be extended into a meromorphic section $\overline{f^{\otimes n}}$ of $\mathcal{L}_{nQ}$. Moreover,

$$\mathcal{L}_Q = \left[\tfrac{1}{n} \operatorname{div}(\overline{f^{\otimes n}}) \right]$$

because the right hand side is cubic and has the same generic fibre than $\mathcal{L}_Q$ (this argument is given in [23, Chap. 3, 1.4]).

On the other hand, we can also consider $\mathcal{L}_{nQ} = [nQ] - [O]$ as a divisor class on $\mathcal{X}$, and choose a meromorphic section g extending $\overline{f^{\otimes n}}$. Let us denote by G_Q the unique fibral divisor on $\mathcal{X}$ whose support does not contains Γ_0, and such that

$$\left[\tfrac{1}{n} \operatorname{div}(g) \right] = [Q] - [O] + [G_Q]$$

holds in $\operatorname{LogPic}(\mathcal{X}, \{v\})$. Then the restriction of G_Q to $\mathcal{E}$ is equal to F_Q. Moreover, if Γ is an irreducible component of the special fibre of $\mathcal{X}$, then we have

$$\Gamma.([Q] - [O] + [G_Q]) = \Gamma.\left[\tfrac{1}{n} \operatorname{div}(g) \right] = \tfrac{1}{n} \cdot \Gamma.[\operatorname{div}(g)]$$

and, on the other hand,

$$\Gamma.\operatorname{div}(g) = \Gamma.([nQ] - [O]) = 0$$

because nQ and O both reduce in the component Γ_0 of $\mathcal{X}$. Therefore, our G_Q satisfies the intersection property. On the other hand, the uniqueness of such a G_Q is proved in Silverman [27, Proposition 8.3], hence the result. $\qquad\square$

The following list gives the unique divisor G_Q for each type of reduction. We fix the point $Q \in \mathcal{E}(\mathcal{O}_v)$ of which we can assume that it does not belong to the connected component $\mathcal{E}^0(\mathcal{O}_v)$ as otherwise $G_Q = F_Q = 0$. Let $\mathcal{E}^0 = \Gamma_0, \Gamma_1, \ldots, \Gamma_m$ be the irreducible components of the special fibre of $\mathcal{X}$. We will determine the coefficients a_j of the divisor $G_Q = a_0\Gamma_0 + \cdots + a_m\Gamma_m$. As remarked before, we must have $a_0 = 0$. By the above Lemma, the intersection with an irreducible component Γ must yield

$$\Gamma.G_Q = \Gamma.([O] - [Q]) = \begin{cases} +1 & \text{if } \Gamma = \Gamma_0, \\ -1 & \text{if } Q \in \Gamma, \text{ and} \\ 0 & \text{otherwise.} \end{cases} \tag{10}$$

These can be expressed in terms of linear equations for the coefficients a_i. For all properties of the intersection pairing on $\mathcal{X}$ we refer to chapter IV in [27].

4.4.1 Multiplicative case

Suppose E has split multiplicative reduction over $\mathcal{O}_v$. Say, there are n connected components to $\mathcal{E}(\mathcal{O}_v)$; hence the Kodaira type is I_n. Fix a Tate parametrisation $u \colon E(K_v) \to K_v^\times / q^{\mathbb{Z}}$ and label the components by $\{\Gamma_j\}_{0 \leqslant j < n}$ where $v(u(R)) \equiv j \pmod{n}$ if and only if R is on Γ_j. (This is well-defined up to reversing the order as u can be composed with $[-1]$.) The special fibre is then the polygon $\Gamma_0 + \Gamma_1 + \cdots + \Gamma_{n-1}$.

Lemma 4.9. *Suppose Q belongs to the component Γ_k with $0 < k < n$. Then*

$$F_Q = G_Q = \sum_{i=1}^{k} \frac{i(n-k)}{n}\Gamma_i + \sum_{i=k+1}^{n-1} \frac{(n-i)k}{n}\Gamma_i.$$

Proof. Once the formula above is known it is a straight forward verification that the equations (10) hold. We use that Γ_j intersects Γ_i if $j - i \equiv \pm 1 \pmod{n}$ and that the multiplicity is 1 in this case and that $\Gamma_j.\Gamma_j = -2$ for all j. For instance for $j = k$, we get only contributions from the terms with $i = k - 1$, k and $k + 1$.

$$G_Q.\Gamma_k = \frac{(k-1)(n-k)}{n}\,\Gamma_{k-1}.\Gamma_k + \frac{k(n-k)}{n}\,\Gamma_k.\Gamma_k + \frac{(n-k-1)k}{n}\,\Gamma_{k+1}.\Gamma_k$$
$$= \frac{(k-1)(n-k)}{n} + (-2)\frac{k(n-k)}{n} + \frac{(n-k-1)k}{n} = -1. \qquad \square$$

The monodromy pairing between Q and R in $E(K_v)$ with values in $\mathbb{Q}/\mathbb{Z}$ is given by the degree of $-R^*[F_Q]$ by Proposition 4.2. If Q belongs to Γ_k and R belongs to Γ_j, then this is equal to

$$-R^*[F_Q] = \begin{cases} -\frac{j(n-k)}{n} & \text{if } j \leqslant k \\ -\frac{(n-j)k}{n} & \text{if } j > k \end{cases}$$

and in both cases this gives that the monodromy pairing between Q and R is jk/n modulo $\mathbb{Z}$. In the non-split multiplicative case, the situation is identical to the split multiplicative case except that $\Phi(k)$ is either trivial (when n is odd) or contains only $\{\Gamma_0, \Gamma_{n/2}\}$ if n is even.

4.4.2 Additive case

Type II and II* : Φ is trivial, so there is nothing to do.

Type III : Φ has order 2 and it is obtained from two line intersecting with multiplicity 2. So $F_Q = G_Q = \frac{1}{2}\Gamma_1$ will do if Q belongs to Γ_1.

Type III* : Again Φ has order 2, but there are now 8 components in the special fibre of $\mathcal{X}$. The connected components of $\mathcal{E}$ are denoted by Γ_0 and Γ_1. Then Γ_0, Γ_2, Γ_4, Γ_6, Γ_5, Γ_3, Γ_1 form a chain and Γ_7 only intersects Γ_6. Then, if $Q \in \Gamma_1$, we have

$$G_Q = \tfrac{3}{2}\Gamma_1 + \Gamma_2 + 2\Gamma_3 + 2\Gamma_4 + \tfrac{5}{2}\Gamma_5 + 3\Gamma_6 + \tfrac{3}{2}\Gamma_7$$

and hence $F_Q = \frac{3}{2}\Gamma_1$.

Type IV : Φ has order 3 and it is obtained from three transversely intersecting lines. We find

$$F_Q = G_Q = \begin{cases} \tfrac{2}{3}\Gamma_1 + \tfrac{1}{3}\Gamma_2 & \text{if } Q \in \Gamma_1, \\ \tfrac{1}{3}\Gamma_1 + \tfrac{2}{3}\Gamma_2 & \text{if } Q \in \Gamma_2. \end{cases}$$

Type IV* : Still Φ has order 3, but there are 7 components. Denote by Γ_6 the unique component of multiplicity 3. Write Γ_0, Γ_1 and Γ_2 for the elements of Φ. Finally for $i = 3, 4, 5$, let Γ_i be the double line connecting Γ_{i-3} and Γ_6. Then

$$G_Q = \begin{cases} \tfrac{4}{3}\Gamma_1 + \tfrac{2}{3}\Gamma_2 + \Gamma_3 + \tfrac{5}{3}\Gamma_4 + \tfrac{4}{3}\Gamma_5 + 2\Gamma_6 & \text{if } Q \in \Gamma_1, \\ \tfrac{2}{3}\Gamma_1 + \tfrac{4}{3}\Gamma_2 + \Gamma_3 + \tfrac{4}{3}\Gamma_4 + \tfrac{5}{3}\Gamma_5 + 2\Gamma_6 & \text{if } Q \in \Gamma_2, \end{cases}$$

and hence $F_Q = \frac{4}{3}\Gamma_1 + \frac{2}{3}\Gamma_2$ or $\frac{2}{3}\Gamma_1 + \frac{4}{3}\Gamma_2$ depending on whether Q is in Γ_1 or Γ_2. Note that the contribution for IV and IV* differ by an integer.

19

Type I_n^* : Label the four components of Φ by $\Gamma_0, \Gamma_1, \Gamma_2, \Gamma_3$. Write Γ_4 for the double line connecting Γ_0 and Γ_1. Then $\Gamma_5, \Gamma_6, \ldots, \Gamma_{4+n}$ forms the chain of double line that links up to Γ_2 and Γ_3. We find

$$
G_Q = \begin{cases}
\Gamma_1 + \frac{1}{2}\Gamma_2 + \frac{1}{2}\Gamma_3 + \Gamma_4 + \Gamma_5 + \cdots + \Gamma_{4+n} & \text{if } Q \in \Gamma_1, \\
\frac{1}{2}\Gamma_1 + \frac{n+4}{4}\Gamma_2 + \frac{n+2}{4}\Gamma_3 + \Gamma_4 + \frac{3}{2}\Gamma_5 + 2\Gamma_6 + \cdots + \frac{n+2}{2}\Gamma_{4+n} & \text{if } Q \in \Gamma_2, \\
\frac{1}{2}\Gamma_1 + \frac{n+2}{4}\Gamma_2 + \frac{n+4}{4}\Gamma_3 + \Gamma_4 + \frac{3}{2}\Gamma_5 + 2\Gamma_6 + \cdots + \frac{n+2}{2}\Gamma_{4+n} & \text{if } Q \in \Gamma_3,
\end{cases}
$$

which gives that

$$
F_Q = \begin{cases}
\Gamma_1 + \frac{1}{2}\Gamma_2 + \frac{1}{2}\Gamma_3 & \text{if } Q \in \Gamma_1, \\
\frac{1}{2}\Gamma_1 + \frac{n+4}{4}\Gamma_2 + \frac{n+2}{4}\Gamma_3 & \text{if } Q \in \Gamma_2, \\
\frac{1}{2}\Gamma_1 + \frac{n+2}{4}\Gamma_2 + \frac{n+4}{4}\Gamma_3 & \text{if } Q \in \Gamma_3.
\end{cases}
$$

4.5 Example

Let E be the elliptic curve 158c1, which has a rational point $P = (13, -15)$ of order 5. Let $K = \mathbb{Q}(\sqrt{-79})$, which has class group of order $h_K = 5$ generated by the ideal $\mathfrak{p} = (2, (1 + \sqrt{-79})/2)$ above 2. The curve E has split multiplicative reduction of type I_{20} above $\mathfrak{p}$ and its conjugate $\bar{\mathfrak{p}}$, while the reduction over the unique place $(\sqrt{-79})$ above 79 is non-split multiplicative of type I_2. The set of bad places is $Z = \{\mathfrak{p}, \bar{\mathfrak{p}}, (\sqrt{-79})\}$ and note that the exact sequence (8) for $\text{LogPic}(\text{Spec}(\mathcal{O}_K), Z)$ does not split. The point

$$
Q = \left(\frac{101}{9}, -\frac{55}{9} + \frac{16}{27}\sqrt{-79} \right)
$$

belongs to $E(K)$ and is of infinite order. Both points P and Q have good reduction at $(\sqrt{-79})$, but bad reduction over $\mathfrak{p}$ and $\bar{\mathfrak{p}}$.

While P has order 5 in the group of components $\Phi_\mathfrak{p}$, the point Q has order 4 and hence they are orthogonal under the monodromy pairing. The value of the logarithmic class group pairing must lie in the class group and we find indeed that

$$
\langle P, Q \rangle^{\log} = [\mathfrak{p}]^2 \in \text{Cl}(\mathcal{O}_K).
$$

Note however that the denominator ideals of P, Q, O and

$$
P + Q = \left(-14 + 3\sqrt{-79}, -186 + 3\sqrt{-79} \right)
$$

are all principal, so the above is the class of the integral ideal $-P^*[F_Q] = -\mathfrak{p} - 3\bar{\mathfrak{p}}$. Furthermore, we find

$$
\langle P, P \rangle^{\log} = \frac{4}{5}\mathfrak{p} + \frac{4}{5}\bar{\mathfrak{p}} \qquad \text{and} \qquad \langle Q, Q \rangle^{\log} = \frac{1}{4}\mathfrak{p} + \frac{1}{4}\bar{\mathfrak{p}}.
$$

5 Tate-Shafarevich groups and Class groups

5.1 The basic connection

Let $S \subseteq X$ be a finite set of finite primes. We have the Kummer exact sequence for the log flat topology, see [14],

$$
0 \longrightarrow \mathcal{O}_K^\times / p \longrightarrow H^1_{\text{kpl}}(X(\log S), \mu_p) \longrightarrow \text{LogPic}(X, S)[p] \longrightarrow 0
$$

and a canonical isomorphism

$$
H^1_{\text{kpl}}(X(\log S), \mu_p) \simeq H^1(U, \mu_p)
$$

We can now use these maps to formulate the central result linking the logarithmic class group pairing to the p-descent. This gives a direct connection between Selmer groups (or Tate-Shafarevich groups) and class groups.

Theorem 5.1. *Assume E/K satisfies the hypotheses in the introduction. Let ψ be the morphism defined by composing the maps*

$$\psi: \quad E'(K)/\varphi(E(K)) \xrightarrow{\kappa} \mathrm{Sel}^\varphi(E/K) \longrightarrow H^1(U_1, \mu_p) \xrightarrow{\rho} \mathrm{LogPic}(X, S_1)[p].$$

Then for all Q in $E'(K)$, we have

$$\psi(Q) = \langle P, Q \rangle^{\log}$$

where $\langle \cdot, \cdot \rangle^{\log}$ is the logarithmic class group pairing.

Proof. By the same arguments as in [13, Lemme 3.2], the morphism ψ can be expressed in terms of the restriction of the canonical biextension $W^{\log}$ on $\mathcal{E}' \times_X \mathcal{E}'$. Namely, for all $Q \in \mathcal{E}'(X)$, we have

$$\psi(Q) = (Q \times P)^*(t(W^{\log}))$$

with notations of section 4.2. This is exactly the definition of the logarithmic class group pairing. $\quad\square$

Remark 5.2. We say that the map ψ defined above is the (logarithmic) class-invariant homomorphism associated to the subgroup $\mathcal{E}[\varphi] \subseteq \mathcal{E}$. This homomorphism has been introduced in a more general setting. It computes the (logarithmic) Galois module structure of $\mathcal{E}[\varphi]$-torsors obtained using the coboundary map κ attached to the isogeny φ. For further discussion about ψ, see [15].

Let us split up the map ψ into

$$\psi: \quad E'(K)/\varphi(E(K)) \xrightarrow{\kappa} \mathrm{Sel}^\varphi(E/K) \xrightarrow{\psi_{\mathrm{Sel}}} \mathrm{LogPic}(X, S_1)[p]$$

Proposition 5.3. *Assume E/K satisfies the hypotheses in the introduction. Then we have an exact sequence*

$$0 \longrightarrow \ker(\psi) \longrightarrow \ker(\psi_{\mathrm{Sel}}) \longrightarrow \mathrm{III}(E/K)[\varphi] \longrightarrow \mathrm{coker}(\psi) \longrightarrow \mathrm{coker}(\psi_{\mathrm{Sel}}) \longrightarrow 0.$$

If we assume moreover that $S_2 = \emptyset$, we get the exact sequence

$$0 \longrightarrow \ker(\psi) \longrightarrow \mathcal{O}_K^\times/p \longrightarrow \mathrm{III}(E/K)[\varphi] \longrightarrow \mathrm{coker}(\psi) \longrightarrow 0.$$

Proof. The exact sequence is simply the kernel-cokernel sequence for the composition $\psi = \psi_{\mathrm{Sel}} \circ \kappa$. If $S_2 = \emptyset$, then $\mathrm{Sel}^\varphi(E/K) = H^1(U_1, \mu_p)$ because the cokernel would lie in $\oplus_{v \in S_2} H^1(\mathcal{O}_v, \mu_p)$ by Theorem 3.1. So kernel and cokernel of ψ_{Sel} identify with the ones of ρ. $\quad\square$

Remark 5.4. In general, one expects that points of infinite order should not belong to the kernel of ψ. Let us describe more precise meanings of this statement.

1). Starting from our point $P \in E'(K)[p]$ as usual, we believe there should exist an infinity of quadratic extensions F/K together with a point $Q \in E'(F)$ of infinite order, such that $\langle P, Q \rangle^{\log} \neq 0$. When $K = \mathbb{Q}$ and E' is semistable, we prove that in Theorem 6.1 below (in fact, we prove a stronger statement).

2). Given a point Q of infinite order on E', we believe there should exist a number field F and a torsion point $R \in E(F)$ such that $\langle Q, R \rangle^{\log} \neq 0$.

We note that 1) is strongly linked with the question asked by Agboola and Pappas in [2]. A variant of 2) has been explored in [4], namely that given Q of infinite order and a fixed prime number p, there should exist a torsion point $R \in E(F)[p^n]$ such that $\langle Q, R \rangle^{\log} \neq 0$. The answer to this question is negative, as shown in [4].

Lemma 5.5. *If $S_1 \neq \emptyset$, then $\kappa(P) \neq 0$ in the Selmer group.*

Proof. By construction, the point P does not reduces in the connected component at places in S_1. Therefore, if $S_1 \neq \emptyset$, the monodromy pairing being non degenerate, $\langle P, P \rangle^{\mathrm{mono}} \neq 0$. By Proposition 4.2, we deduce that $\langle P, P \rangle^{\log} \neq 0$. In other words, $\psi(P) \neq 0$ and, by definition, this implies that $\kappa(P) \neq 0$ in the Selmer group. This also implies that $E(K)[\varphi] = E(K)[p]$. $\qquad \square$

5.2 Splitting ψ into pieces

We denote by $\mathrm{Cl}(\langle S_1 \rangle)$ the subgroup of $\mathrm{Cl}(K)$ generated by ideals with support in S_1.

It follows from the description of $\mathrm{LogPic}(X, S_1)$ and the sequence (8) that we have an exact sequence

$$0 \longrightarrow \mathrm{Cl}(K)[p] \longrightarrow \mathrm{LogPic}(X, S_1)[p] \longrightarrow \bigoplus_{v \in S_1} (\mathbb{Z}/p\mathbb{Z}) \cdot v \tag{11}$$
$$\xrightarrow{\quad\quad\quad} \mathrm{Cl}(K)/p \longrightarrow \mathrm{Cl}(\mathcal{O}_{K,S_1})/p$$

with θ below.

where the map θ is sending $\sum_{v \in S_1} \overline{n_v} \cdot v$ to the class of $\sum_{v \in S_1} n_v \cdot v$. We note that, if $\mathrm{Cl}(\langle S_1 \rangle)[p] = 0$ then $\theta = 0$.

According to Proposition 4.2, when composing the map ψ with the second map of (11), we get the map

$$\psi^{\mathrm{mono}} : E'(K)/\varphi(E(K)) \longrightarrow \bigoplus_{v \in S_1} (\mathbb{Z}/p\mathbb{Z}) \cdot v$$
$$Q \longmapsto \langle P, Q \rangle^{\mathrm{mono}}$$

induced by the monodromy pairing.

We have an exact sequence

$$0 \longrightarrow \bigoplus_{v \in S_1} (\mathbb{Z}/p\mathbb{Z}) \cdot v \longrightarrow \mathrm{LogPic}(X, S_1)[p] \longrightarrow \mathrm{Cl}(\mathcal{O}_{K,S_1})[p] \longrightarrow 0. \tag{12}$$

When composing the map ψ with the right hand side of this sequence, we get the map

$$\psi^{\mathrm{cl}}_{S_1} : E'(K)/\varphi(E(K)) \longrightarrow \mathrm{Cl}(\mathcal{O}_{K,S_1})[p]$$
$$Q \longmapsto \langle P, Q \rangle^{\mathrm{cl}}_{S_1}$$

where $\langle P, Q \rangle^{\mathrm{cl}}_{S_1}$ is the S_1-class group pairing defined at the end of section 4.1.

We note that, when composing the first map of (11) with the right hand side map of sequence (12), we get the natural map $\mathrm{Cl}(K)[p] \to \mathrm{Cl}(\mathcal{O}_{K,S_1})[p]$.

Remark 5.6. When $\mathrm{Cl}(\langle S_1 \rangle)[p] = 0$, then $\mathrm{Cl}(K)[p] \simeq \mathrm{Cl}(\mathcal{O}_{K,S_1})[p]$, so the sequence (11) and (12) split, and we get an isomorphism

$$\mathrm{LogPic}(X, S)[p] \simeq \mathrm{Cl}(\mathcal{O}_{K,S_1})[p] \oplus \bigoplus_{v \in S_1} (\mathbb{Z}/p\mathbb{Z}) \cdot v.$$

Moreover, via this isomorphism, ψ can be identified with the map $(\psi^{\mathrm{cl}}_{S_1}, \psi^{\mathrm{mono}})$.

6 Quadratic fields

6.1 Points of infinite order and the class group pairing

Let S be a finite set of prime numbers. For any number field K, ee will denote by $\mathcal{O}_{K,S}$ the ring of S'-integers of K, where S' is the set of finite places of K lying above elements of S. We will denote by $\langle \cdot, \cdot \rangle_S^{\mathrm{cl}}$ the S'-class group pairing defined in section 4.1.

The pairing $\langle \cdot, \cdot \rangle_S^{\mathrm{cl}}$ has the advantage that, given two points Q and R on E, there always exists a set S such that the pairing $\langle Q, R \rangle_S^{\mathrm{cl}}$ makes sense. For example, we may take S to be the set of primes of bad reduction of E.

We now state a result inspired by the paper [16]. For the convenience of the reader, we give a complete proof, following the method of [16]. Unlike with our previous conventions, $p = 2$ is allowed in this section.

Theorem 6.1. *Let E' be an elliptic curve defined over $\mathbb{Q}$, and let $P \in E'(\mathbb{Q})$ be a point of prime order p. Let $S = \{\ell_1, \ldots, \ell_r\}$ be a set of prime numbers such that P reduces in the connected component of the Néron model of E' at all primes outside S. Then there exists infinitely many quadratic imaginary fields K with a point $Q \in E'(K)$ of infinite order, such that the class group pairing $\langle P, Q \rangle_S^{\mathrm{cl}}$ is non-zero in the group $\mathrm{Cl}(\mathcal{O}_{K,S})[p]$.*

Proof. Let E be the quotient of E' by the cyclic subgroup generated by P, and let $\varphi \colon E \to E'$ be the dual isogeny, that we now consider as a μ_p-torsor. Because E is an elliptic curve, there exists a degree 2 morphism $\theta \colon E \to \mathbb{P}^1$ from E to the projective line. Applying Hilbert's irreducibility Theorem to $\theta \circ \varphi$, we get an infinity of points Q in E', defined over quadratic fields, such that $\varphi^{-1}(Q)$ is a non-trivial μ_p-torsor. More precisely, there exists an infinity of quadratic imaginary fields K together with a point $Q \in E'(K)$ for which the torsor $\varphi^{-1}(Q)$ is non-trivial. According to the proof of [16, Corollary 3.1], we may assume that the primes in S are totally ramified in these quadratic imaginary fields.

Let K be such a field, and let $Q \in E'(K)$ be such a point. Of course, $\varphi^{-1}(Q)$ is just $\kappa(Q)$, where κ is the coboundary map $\kappa \colon E'(K) \to H^1(K, \mu_p)$ associated to the isogeny φ. Let $U = \mathrm{Spec}(\mathcal{O}_{K,S})$. Then P falls into the connected component of the Néron model of E' over U, from which it follows, by [13], that the map κ factorises as

$$E'(K) \xrightarrow{\ \kappa_U\ } H^1(U, \mu_p) \longrightarrow H^1(K, \mu_p).$$

Let F be the field such that $\kappa(Q) = \mathrm{Spec}(F)$, and let $L = \mathbb{Q}[\sqrt[p]{u} \mid u \in \mathbb{Z}_S^\times]$. By a variant of Hilbert's irreducibility Theorem, it is possible to ensure that F is linearly disjoint from L. Then K is linearly disjoint from $\mathbb{Q}[\zeta_p]$, which is a subfield of L. Combining this with the fact that the primes in S are totally ramified in K, we have $\mathcal{O}_{K,S}^\times / p = \mathbb{Z}_S^\times / p$. Therefore, the Kummer exact sequence over U reads

$$0 \longrightarrow \mathbb{Z}_S^\times / p \longrightarrow H^1(U, \mu_p) \xrightarrow{\ \rho_S\ } \mathrm{Cl}(\mathcal{O}_{K,S})[p] \longrightarrow 0.$$

Moreover, because F is linearly disjoint from L, the torsor $\kappa_U(Q)$ does not belong to the subgroup $\mathbb{Z}_S^\times / p$, that is, $\rho_S(\kappa_U(Q)) \neq 0$. On the other hand, we have the relation

$$\rho_S(z) = \rho_S(\kappa_U(Q)) = \langle P, Q \rangle_S^{\mathrm{cl}}$$

which is similar to that observed in Theorem 5.1. This completes the proof of the first part of the statement.

We now have to prove that Q is of infinite order. Suppose Q is a torsion point, then, κ being a morphism, we may suppose that the order of Q is a power of p. Moreover, we may ask by the same arguments as before, that K is linearly disjoint from the field $\mathbb{Q}(E'[p^2])$. This implies that

the p-part of $E'(K)$ is equal to the p-part of $E'(\mathbb{Q})$, in other words Q belongs to $E'(\mathbb{Q})$. This is not possible because in this case the pairing $\langle P, Q \rangle_S^{\mathrm{cl}}$ comes by base change from a class in $\mathrm{Cl}(\mathbb{Z}_S)$, and therefore is trivial. So the point Q is of infinite order. $\qquad\square$

Example 6.2. Let E be the curve labeled 11a2 in Cremona's tables and let E' be 11a1. Since the same curves will appear in further examples, we describe the situation in detail here. The curve E' has a rational point $P = (5, 5)$ of order 5 giving our isogeny $\hat{\varphi}$. The torsion point P does not reduces into the connected component at the only bad prime 11. The isogeny is forward at the split multiplicative place 11 and the reduction is good ordinary at 5. Therefore our hypotheses will be satisfied for any number field K. The set S_2 will be the empty set for all K and S_1 will consist of all places above 11. By Lemma 5.5, there are no non-trivial 5-torsion points in $E(K)$. Since $S_2 = \emptyset$, we get $\mathrm{Sel}^\varphi(E/K) = H^1(\mathcal{O}_{K,\{11\}}, \mu_5)$.

According to Theorem 6.1, there exist infinitely many imaginary quadratic fields K with a point $Q \in E'(K)$ of infinite order such that $\langle P, Q \rangle_{\{11\}}^{\mathrm{cl}}$ is non-zero in the group $\mathrm{Cl}(\mathcal{O}_{K,\{11\}})[5]$. Using Lemma 5.5, we know that P is non-trivial in $\mathrm{Sel}^\varphi(E/K)$, however, since P is defined over $\mathbb{Q}$, we have $\langle P, P \rangle_{\{11\}}^{\mathrm{cl}} = 0$. We deduce that the sequence

$$0 \longrightarrow \mathbb{Z}/_{5\mathbb{Z}} \, P \longrightarrow \mathrm{Sel}^\varphi(E/K) \longrightarrow \mathrm{Cl}(\mathcal{O}_{K,\{11\}})[5] \longrightarrow 0$$

is exact. Hence we conclude that in this case $\dim_{\mathbb{F}_5} \mathrm{III}(E/K)[\varphi]$ is less than $\dim_{\mathbb{F}_5} \mathrm{Cl}(\mathcal{O}_{K,\{11\}})[5]$.

As a concrete example, we may consider $K = \mathbb{Q}(\sqrt{-47})$ whose $\{11\}$-class group has 5 elements. The Mordell-Weil group has rank 2, generated by

$$Q_1 = \left(4, -\tfrac{1}{2} + \tfrac{1}{2}\sqrt{-47} \right) \qquad \text{and} \qquad Q_2 = \left(-2, -\tfrac{1}{2} + \tfrac{1}{2}\sqrt{-47} \right)$$

While $\psi(Q_1) = 0$ and $\langle P, Q_1 \rangle_{\{11\}}^{\mathrm{cl}} = 0$, both $\psi(Q_2)$ and $\langle P, Q_2 \rangle_{\{11\}}^{\mathrm{cl}}$ are the non-trivial class containing the ideal $(7, \tfrac{11}{2} + \tfrac{1}{2}\sqrt{-47})$.

6.2 Comparison to the quadratic twists

Let us suppose that E is defined over $\mathbb{Q}$ and consider E over a quadratic field K. As usual, we can relate all the properties of E/K to $E/\mathbb{Q}$ and to $E^\dagger/\mathbb{Q}$ where $E^\dagger$ is the quadratic twist of E by the fundamental discriminant of K. Now, the twist admits also an isogeny $\varphi^\dagger \colon E^\dagger \to E'^\dagger$.

Since p is odd, all the pieces in the p-descent split up into a part on which $\mathrm{Gal}(K/\mathbb{Q})$ acts trivially and a part on which its non-trivial element acts as -1. We denote $()^-$ the latter subspaces. Since the class group of $\mathbb{Q}$ is trivial, the p-primary part of the class group of K does not have any non-trivial subgroup on which $\mathrm{Gal}(K/\mathbb{Q})$ acts trivial.

For $i = 1$ and 2, let T_i be the subset of S_i of places in $\mathbb{Q}$ which decompose in $K/\mathbb{Q}$. Write $U_{K,1}$ for the complement of the places above S_1 in $\mathcal{O}_K$. The class group of $U_{K,1}$ is denoted by $\mathrm{Cl}(\mathcal{O}_{K,S_1})$.

From (6), we deduce the exact sequence

$$0 \longrightarrow \mathrm{Sel}^{\varphi^\dagger}(E^\dagger/\mathbb{Q}) \longrightarrow H^1(U_{K,1}, \mu_p)^- \longrightarrow \bigoplus_{v \in T_2} H^1(\mathbb{Z}_v, \mu_p)$$
$$\longrightarrow \mathrm{Sel}^{\hat{\varphi}^\dagger}(E'^\dagger/\mathbb{Q})^\vee \longrightarrow \mathrm{Cl}(\mathcal{O}_{K,S_1})/p \longrightarrow 0.$$

Moreover, the second term can be computed as

$$0 \longrightarrow \bigoplus_{v \in T_1} \mathbb{Z}/_{p\mathbb{Z}} \, v \oplus F \longrightarrow H^1(U_{K,1}, \mu_p)^- \longrightarrow \mathrm{Cl}(\mathcal{O}_{K,S_1})[p] \longrightarrow 0$$

where $F = 0$ if K is imaginary and $F = \mathbb{Z}/_{p\mathbb{Z}} \, \eta$ if K is real and η is a fundamental unit.

Note that the kernel of $\varphi^\dagger$ is not isomorphic to μ_p, rather it is of the form $\mu_p \otimes \chi$ over K with χ being the quadratic character corresponding to K. Hence the above can be viewed as an extension of our techniques of the p-descent to isogenies that do not satisfy our hypothesis (Hyp 3), but do satisfy it after a quadratic extension. One could generalise this to arbitrary isogenies if one is willing to pass to a larger extension and to consider particular eigen-spaces as it is done in [21].

6.3   The kernel of the class-invariant homomorphism

Lemma 6.3. *Suppose K is a imaginary quadratic field with $\mu_p \not\subset K$. Then ψ_{Sel} and ψ are injective and*

$$0 \longrightarrow \text{Ш}(E/K)[\varphi] \longrightarrow \operatorname{coker}(\psi) \longrightarrow \operatorname{coker}(\psi_{\mathrm{Sel}}) \longrightarrow 0$$

is exact.

Proof. The map ψ_{Sel} factors as

$$\psi_{\mathrm{Sel}} \colon \operatorname{Sel}^{\varphi}(E/K) \longrightarrow H^1(U_1, \mu_p) \xrightarrow{\ \rho\ } \operatorname{LogPic}(X, S_1)[p]$$

The first map is injective. The kernel of the second map ρ is $\mathcal{O}_K^{\times}/p$, which is trivial if K is an imaginary quadratic field unless $p = 3$ and $K = \mathbb{Q}(\mu_3)$. The rest follows from Proposition 5.3. $\square$

If we are in the case the S_2 is empty, then we deduce further an isomorphism $\text{Ш}(E/K)[\varphi] = \operatorname{coker}(\psi)$. Furthermore, the map ψ_{Sel} is an isomorphism from $\operatorname{Sel}^{\varphi}(E/K)$ to $\operatorname{LogPic}(X, S_1)[p]$. Hence one could proceed to do the p-descent in the logarithmic class group avoiding completely the explicit Kummer map κ.

If instead K is real quadratic, the kernel may be non-trivial, but it will have at most p elements. In fact, it is the intersection of $\mathcal{O}_K^{\times}/p \cong \mathbb{Z}/p\mathbb{Z}$ and $\operatorname{Sel}^{\varphi}(E/K)$ inside $H^1(U_1, \mu_p)$. Two examples are given in section 7.2 below.

7   Numerical Examples

All numerical examples in this paper were computed using Sage [29]. Underlying to it, PARI/GP [31] was heavily used. Furthermore some calculations involved the use of Magma [6]. The algorithms, implemented to be used in Sage, for computing the Selmer groups and the logarithmic class group pairing are available on the authors web pages.

7.1   An imaginary quadratic example

Let us consider the example 6.2 of the curves $E = 11a2$ and $E' = 11a1$ and the point $P = (5, 5)$ over an imaginary quadratic field K. There are now two cases. Either the order of the places above 11 in the class group is divisible by $p = 5$ or not, in other words either θ in sequence (11) is trivial or has an image of order 5. Write $t \in \{0, 1\}$ for the dimension of the image of θ and write h_5 for the dimension of $\operatorname{Cl}(\mathcal{O}_K)[5]$ as $\mathbb{F}_5$-vector spaces. In particular if 11 is inert or ramified in K, then $t = 0$. We find that

$$\dim_{\mathbb{F}_5} \operatorname{Sel}^{\varphi}(E/K) = \dim_{\mathbb{F}_5} \operatorname{LogPic}(X, S_1)[5] = h_5 + \#S_1 - t \text{ and}$$
$$\dim_{\mathbb{F}_5} \operatorname{Sel}^{\hat{\varphi}}(E'/K) = h_5.$$

If we assume that $h_5 \leqslant 1$, then, by Corollary 3.5, we get

$$\dim_{\mathbb{F}_5} \operatorname{Sel}^5(E/K) = 2h_5 + \#S_1 - t - 1.$$

7.2   Real quadratic examples

In the case, when K is a real quadratic field, the map ψ may or may not be injective. First we explain a case, when ψ is *not* injective. Let $K = \mathbb{Q}(\sqrt{2})$ and take again the isogeny φ from 11a2 to 11a1 of example 6.2. The class group of K is trivial. The Mordell-Weil group $E'(K)$ is generated by our 5-torsion point P and the point $Q = \left(\frac{9}{2}, -\frac{1}{2} + \frac{7}{4}\sqrt{2}\right)$ of infinite order. Since S_1 is not empty $\psi(P) \neq 0$ by Lemma 5.5. Since Q has good reduction at (11), we have $\psi(Q) = \langle P, Q\rangle^{\log} = 0$. Note that Q is not in the image of φ as $E(K) = \mathbb{Z}\,\hat{\varphi}(Q)$. It follows that the kernel of $\psi\colon E'(K)/\varphi(E(K)) \to \mathrm{LogPic}(X, S_1)[p]$ is generated by the image of Q. In other words, the image of Q under $E'(K)/\varphi(E(K)) \to \mathrm{Sel}^\varphi(E/K) \to H^1(U_1, \mu_p)$ lands in the image of the global units $\mathcal{O}_K^\times/p$.

If we consider instead the isogeny φ from 35a2 to 35a1 of degree 3, still over $K = \mathbb{Q}(\sqrt{2})$, we find that ψ is injective. The rank of $E'(K)$ is again 1, generated by a point $Q = \left(\frac{9}{2}, -\frac{1}{2} + \frac{35}{4}\sqrt{2}\right)$. But this time

$$\psi(Q) = \frac{2}{3} \cdot (1 + 2\sqrt{2}) + \frac{1}{3} \cdot (1 - 2\sqrt{2}).$$

7.3   A cubic example

We consider our example 6.2 of the curve 11a2 and 11a1 over the cubic field $K = \mathbb{Q}(\mu_7)^+$ obtained by adjoining the root α of $x^3 + x^2 - 2x - 1 = 0$.

The class group of K is trivial and $E(K)$ does not contain any torsion points. The group $\mathrm{Sel}^\varphi(E/K) = H^1(U_1, \mu_5)$ has the explicit basis 11, $\alpha + 1$, $\alpha^2 - 1$ as a $\mathbb{F}_5$-vector space in $K^\times/p$. We have $\mathrm{Sel}^{\hat{\varphi}}(E'/K) = 0$. We deduce that the dimension of $\mathrm{Sel}^5(E/K)$ is 2 and that the dimension of $\mathrm{Sel}^5(E'/K)$ is at most 3 because it is a subspace of $\mathrm{Sel}^\varphi(E/K)$.

As $K/\mathbb{Q}$ is abelian and E is defined over $\mathbb{Q}$, we can apply Kato's Theorem [18]. Firstly, the Tate-Shafarevich groups are finite and, secondly, the computation of the algebraic value of the L-series of E over K using modular symbols reveals that the rank of $E(K)$ is 0. The Birch and Swinnerton-Dyer conjecture asserts that $\mathrm{III}(E/K)$ has 5^4 elements and $\mathrm{III}(E'/K)$ has 5^2. Kato's result and a 2-descent also show that no prime other than 5 can divide the order of these Tate-Shafarevich groups.

From our 5-descent information, we conclude that $\mathrm{III}(E/K)[5] = \left(\mathbb{Z}/5\mathbb{Z}\right)^2$. Doing a further 5-descent with the isogeny from $E' = 11a1$ to $E'' = 11a3$ (whose kernel contains a point of order 5), we find that $\mathrm{III}(E'/K)[5] = \left(\mathbb{Z}/5\mathbb{Z}\right)^2$, too. However, our descents will not reveal if $\mathrm{III}(E''/K)[5]$ is trivial (as BSD predicts) or not. Using the invariance of the BSD formula under isogenies, we see that $\mathrm{III}(E/K)$ will either have 5^4 or 5^6 elements.

We conclude that

$$E(K) = 0 \qquad\qquad E'(K) = \mathbb{Z}/5\mathbb{Z}\,P$$
$$\mathrm{Sel}^5(E/K) = \left(\mathbb{Z}/5\mathbb{Z}\right)^2 \qquad\qquad \mathrm{Sel}^5(E'/K) = \left(\mathbb{Z}/5\mathbb{Z}\right)^3$$
$$\mathrm{III}(E/K) = \left(\mathbb{Z}/25\mathbb{Z}\right)^2 \text{ or } \left(\mathbb{Z}/125\mathbb{Z}\right)^2 \qquad\qquad \mathrm{III}(E'/K) = \left(\mathbb{Z}/5\mathbb{Z}\right)^2 \text{ or } \left(\mathbb{Z}/25\mathbb{Z}\right)^2.$$

7.4   A more complicated cubic example

We take the curve $E = 294b1$ given by the equation

$$y^2 + x\,y = x^3 - x - 1$$

which admits an isogeny φ of degree 7 to the curve $E' = 294b2$. The kernel of the dual is generated by a point $P = (6, 3)$ on E'. We consider this curve over the cubic extension generated by α which satisfies $\alpha^3 + \alpha^2 - 104\,\alpha + 371 = 0$. This is an abelian extension of conductor 313. Its class number is 7.

The set S_1 consists of the two forward split multiplicative places (2) and (3). The set S_2 instead contains the three places above 7, namely $(7, \alpha)$, $(7, \alpha + 3)$ and, $(7, \alpha - 2)$. As an explicit basis for $H^1(U_1, \mu_7)$, we can take $\{2, 3, \alpha - 5, \alpha - 6, 8\alpha^2 + 53\alpha - 513\}$ where the last represents the generator of the seven power of a non-principal ideal. The localisation map $H^1(U_1, \mu_7) \to \oplus_{v \in S_2} H^1(\mathcal{O}_v, \mu_7)$ is a linear map from a vector space of dimension 5 to a space of dimension 3. It can be checked that this map is not surjective, rather its cokernel has dimension 1. We conclude that

$$\dim_{\mathbb{F}_7} \mathrm{Sel}^{\varphi}(E/K) = 3 \qquad \text{and} \qquad \dim_{\mathbb{F}_7} \mathrm{Sel}^{\hat{\varphi}}(E'/K) = 2.$$

With some luck, we are able to find a point of infinite order on $E'(K)$, namely $Q = (2\alpha^2 - 25\alpha + 69, 50\alpha^2 - 625\alpha + 1921)$ and a point $R = (\alpha^2 - 10\alpha + 29, 17\alpha^2 - 170\alpha + 415)$ on $E(K)$ of infinite order. It is possible to show using the Néron-Tate height pairing, that P, $\sigma(P)$, $\varphi(R)$, and $\sigma(\varphi(R))$ are linearly independent in $E'(K)$. From our descent computations, we conclude that $\text{Ш}(E/K)[7] = \text{Ш}(E'/K)[7] = 0$ and that $E'(K)/\varphi(E(K)) = \mathrm{Sel}^{\varphi}(E/K)$ has dimension 3, while $E(K)/\hat{\varphi}(E'(K)) = \mathrm{Sel}^{\hat{\varphi}}(E'/K)$ has dimension 2. It is not difficult to see that the subgroup of points we found has index coprime to 7 in the full Mordell-Weil group. In fact, the Birch and Swinnerton-Dyer conjecture asserts that the index is equal to the order of $\text{Ш}(E'/K)$. We get that P, Q and $\sigma(Q)$ generate $E'(K)/\varphi(E(K))$ while R and $\sigma(R)$ generate $E(K)$ modulo the image of $\hat{\varphi}$.

We now analyse the class-invariant homomorphism

$$\psi \colon E'(K)/\varphi(E(K)) \to \mathrm{LogPic}(X, S_1)[7].$$

The source is a $\mathbb{F}_7$-vector space of dimension 3 generated by P, Q and $\sigma(Q)$. Since the only two places in $S_1 = \{(2), (3)\}$ are principal ideals, we get

$$0 \longrightarrow \mathrm{Cl}(K)[7] \longrightarrow \mathrm{LogPic}(X, S_1)[7] \longrightarrow \mathbb{Z}/_{7\mathbb{Z}}(2) \oplus \mathbb{Z}/_{7\mathbb{Z}}(3) \longrightarrow 0.$$

Hence the target is also a three dimensional space, generated by $\frac{1}{7}(2)$, $\frac{1}{7}(3)$, and $\mathfrak{c} = (7, \alpha)$. It is easy to compute the images of the basis by computing the logarithmic class group pairing. We have

$$\psi(P) = \langle P, P \rangle^{\log} = \tfrac{1}{7}(3) + \tfrac{4}{7}(2),$$
$$\psi(Q) = \langle P, Q \rangle^{\log} = \mathfrak{c}^2,$$
$$\psi(\sigma(Q)) = \langle P, \sigma(Q) \rangle^{\log} = \mathfrak{c}^4$$

and hence $Q + 3\,\sigma(Q)$ is in the kernel of ψ. In fact both kernel and cokernel of ψ are of dimension 1.

7.5 A quintic example

We return to our isogeny $\varphi \colon E \to E'$ with $E = 11a2$ and $E' = 11a1$ from example 6.2. But now over the abelian quintic field K of conductor 61. A simple element α for K is given by a root of $x^5 + x^4 - 24\,x^3 - 17\,x^2 + 41\,x - 13 = 0$. Its class group is trivial. We deduce that the dimension of $\mathrm{Sel}^{\varphi}(E/K)$ is 9 and $\mathrm{Sel}^{\hat{\varphi}}(E'/K)$ is trivial. It follows from the fact that $E(K)$ is finite (again shown using modular symbols) that $\text{Ш}(E/K)[5] = \text{Ш}(E/K)[\varphi]$ is of dimension 8. The Birch and Swinnerton-Dyer conjecture asserts that the order of $\text{Ш}(E/K)$ is $5^8 \cdot 19^2$.

Acknowledgements

References

[1] Adebisi Agboola, *A geometric description of the class invariant homomorphism*, J. Théor. Nombres Bordeaux **6** (1994), no. 2, 273–280.

[2] Adebisi Agboola and George Pappas, *Line bundles, rational points and ideal classes*, Math. Res. Letters **7** (2000), 1–9.

[3] _____ , *On arithmetic class invariants*, Math. Annalen **320** (2001), 339–365.

[4] Adebisi Agboola and Martin J. Taylor, *Class invariants of Mordell-Weil groups*, J. Reine Angew. Math. **447** (1994), 23–61.

[5] Siegfried Bosch and Dino Lorenzini, *Grothendieck's pairing on component groups of Jacobians*, Invent. Math. **148** (2002), no. 2, 353–396.

[6] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993).

[7] Philippe Cassou-Noguès and Martin J. Taylor, *Structures galoisiennes et courbes elliptiques*, J. Théor. Nombres Bordeaux **7** (1995), no. 1, 307–331.

[8] John Cremona and Barry Mazur, *Visualizing elements in the Shafarevich-Tate group*, Experimental Math. **9** (2000), 13–28.

[9] Z. Djabri, Edward F. Schaefer, and N. P. Smart, *Computing the p-Selmer group of an elliptic curve*, Trans. Amer. Math. Soc. **352** (2000), no. 12, 5583–5597.

[10] Tim Dokchitser, *Deformations of p-divisible groups and p-descent on elliptic curves*, Ph.D. thesis, Proefschrift Universiteit Utrecht, 2000.

[11] Tom Fisher, *On 5 and 7 descents for elliptic curves*, Ph.D. thesis, Cambridge University, UK, 2000.

[12] _____ , *The Cassels-Tate pairing and the Platonic solids*, J. Number Theory **98** (2003), no. 1, 105–155.

[13] Jean Gillibert, *Invariants de classes : le cas semi-stable*, Compos. Math. **141** (2005), no. 4, 887–901.

[14] _____ , *Prolongement de biextensions et accouplements en cohomologie log plate*, Int. Math. Res. Not. IMRN (2009), no. 18, 3417–3444.

[15] _____ , *Cohomologie log plate, actions modérées et structures galoisiennes*, J. Reine Angew. Math. (2011), no. ??, ??

[16] Jean Gillibert and Aaron Levin, *Pulling back torsion line bundles to ideal classes*, Preprint, 2011.

[17] Alexandre Grothendieck, *Groupes de monodromie en géométrie algébrique. I*, Lecture Notes in Mathematics, Vol. 288, Springer-Verlag, Berlin, 1972, Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I), Dirigé par A. Grothendieck. Avec la collaboration de M. Raynaud et D. S. Rim.

[18] Kazuya Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Cohomologies p-adiques et application arithmétiques. III, Astérisque, vol. 295, Société Mathématique de France, Paris, 2004.

[19] Qing Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, vol. 6, Oxford University Press, Oxford, 2002, Translated from the French by Reinie Erné, Oxford Science Publications.

[20] Barry Mazur and John Tate, *Canonical height pairings via biextensions*, Arithmetic and geometry, Vol. I, Progr. Math., vol. 35, Birkhäuser Boston, Boston, MA, 1983, pp. 195–237.

[21] Robert Miller and Michael Stoll, *Explicit isogeny descent on elliptic curves*, `http://arxiv.org/abs/1010.3334`, 2010.

[22] James S. Milne, *Arithmetic duality theorems*, second ed., BookSurge, LLC, Charleston, SC, 2006.

[23] Laurent Moret-Bailly, *Pinceaux de variétés abéliennes*, Astérisque (1985), no. 129, 266.

[24] George Pappas, *On torsion line bundles and torsion points on abelian varieties*, Duke Math. J. **91** (1998), no. 2, 215–224.

[25] Edward F. Schaefer, *Class groups and Selmer groups*, J. Number Theory **56** (1996), no. 1, 79–114.

[26] Edward F. Schaefer and Michael Stoll, *How to do a p-descent on an elliptic curve*, Trans. Amer. Math. Soc. **356** (2004), no. 3, 1209–1231.

[27] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994.

[28] _____ , *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.

[29] W. A. Stein et al., *Sage Mathematics Software (Version 4.7.1)*, The Sage Development Team, 2011, available from `http://www.sagemath.org`.

[30] Martin J. Taylor, *Mordell-Weil groups and the Galois module structure of rings of integers*, Illinois J. Math. **32** (1988), no. 3, 428–452.

[31] The PARI Group, Bordeaux, *PARI/GP, version* `2.4.3`, 2011, available from `http://pari.math.u-bordeaux.fr/`.

[32] Fabien Trihan and Christian Wuthrich, *Parity conjectures for elliptic curves over global fields of positive charactersitic*, Compositio Math. **147** (2011), no. 4, 1105–1128.

[33] Christian Wuthrich, *On p-adic heights in families of elliptic curves*, J. London Math. Soc. (2) **70** (2004), no. 1, 23–40.