AN EXPOSITION OF THE 2-DESCENT ON AN ELLIPTIC CURVE

ALAN ZHAO

Abstract. The purpose of this document is to highlight the key ideas behind the process of 2-descent on an elliptic curve E over a field K in the case where (1) E has full K-rational 2-torsion and (2) where E has a 2-isogeny defined over K. We will require some Galois cohomology in both cases, where as in (1) we further require the properties of the Weil pairing and for (2) we further require the theory of homogeneous spaces of E.

1. The Case of Full Rational 2-Torsion

Let E be an elliptic curve over a perfect field K. As the title of the section suggests, we assume that $E[2] \subset E(K)$. With this assumption, we are in a position to begin pulling together numerous concepts from Chapters 2, 3, and 8 from [Sil09] to formulate 2-descent in the case of full rational 2-torsion. The principal goal of this section, then, is to attempt to make sense of how these three chapters dotted throughout this book come together to form this result. And from this attempt will perhaps arise many other questions. So, to begin our ascent, we introduce the following definition.

Definition 1.1. *Define the* ***Kummer pairing*** *as the map*

$$\kappa_2 : E(K) \times Gal(\overline{K}/K) \to E[2], \tag{1.1}$$

where $\kappa_2(P, \sigma) = Q^\sigma - Q$ *where* $Q \in E(\overline{K})$ *satisfies* $2Q = P$.

Now as singularly displayed above, the definition of κ_2 needs some explanation, both conceptual and motivic.

Remark. *Consider the following:*

i. *We assume that the field K is perfect, and so $\overline{K}/K$ is actually Galois.*
ii. *The existence of Q follows from the fact that a morphism of curves is either constant or surjective. It is well-known that the multiplication-by-2 map $[2] : E \to E$ is a morphism due to, for example, the duplication formula of a point $P = (x, y) \in E$, which gives the coordinates of $2P$ in terms of K-rational functions in x and y. Hence, it is either constant or surjective (*[Sil09, Chapter II, Theorem 2.3]*). It is very clearly not constant (e.g., by the finiteness of $E[2]$), and so is surjective.*
iii. *The construction of κ_2 is natural in the following sense: there is a short exact sequence (of which we shall see plenty of in this exposition) of $Gal(\overline{K}/K)$-modules*

$$0 \to E[2] \to E(\overline{K}) \to E(\overline{K}) \to 0, \tag{1.2}$$

with the third arrow from the left being the morphism $[2] : E \to E$. Taking $Gal(\overline{K}/K)$-cohomology yields a long exact sequence with connecting homomorphism $\delta : E(K) \to H^1(Gal(\overline{K}/K), E[2])$. The three characters of this map are those found in κ_2.

Date: September 2020.

*Now, $H^1(Gal(\overline{K}/K), E[2])$ is really just a set of equivalence classes of maps $Gal(\overline{K}/K) \to E[2])$. And so one can reimagine the map $E(K) \to Map(Gal(\overline{K}/K), E[2])$ as a pairing $E(K) \times Gal(\overline{K}/K) \to E[2]$, which is the content of the above definition. But now why define $\kappa_2(P, \sigma)$ as in the definition? The reason is cohomological: in reimagining the map δ, the functions $Gal(\overline{K}/K) \to E[2])$ that we want are called **1-cocyles**. Here, $\kappa_2(P, \sigma)$ provides us with a "simple" 1-cocycle, a **1-coboundary**.*

It turns out that the Kummer pairing has the following four useful properties.

Proposition 1.2. *The following are true:*

i. The Kummer pairing is well-defined.
ii. The Kummer pairing is bilinear.
iii. The kernel of the Kummer pairing on the left is $2E(K)$.
iv. The kernel of the Kummer pairing on the right is $Gal(\overline{K}/L)$, where

$$L = K([2]^{-1}E(K)) \tag{1.3}$$

where the adjoined element runs over all $Q \in E(\overline{K})$ such that $2Q \in E(K)$. Hence, the Kummer pairing induces a perfect bilinear pairing

$$b_2 : E(K)/2E(K) \times G_{L/K} \to E[2]. \tag{1.4}$$

Remark. *The Kummer pairing exists for any positive integer, not just 2. Similarly, the above Proposition works for any positive integer. But because our focus is 2-descent, we only discuss the case $m = 2$.*

Proof. Properties (i)-(iii) and the first part of (iv) may be proven directly from the definition of κ_2. By (ii) and (iii), the induced pairing $\kappa_2' : E(K)/2E(K) \times \mathrm{Gal}(L/K) \to E[2]$ is an isomorphism in each variable, and so the bilinear pairing is perfect. □

Remark. *The extension L/K in the above Proposition is Galois because $G_{\overline{K}/L}$ is the kernel of the map $Gal(\overline{K}/K) \to Hom(E(K), E[2])$ given by $\sigma \mapsto \kappa_2(\cdot, \sigma)$, and so is a normal subgroup. By the Fundamental Theorem of Galois Theory, it follows that L/K is Galois, and $Gal(\overline{K}/K)/Gal(\overline{K}/L) \simeq Gal(L/K)$.*

So, our naïve definition of the Kummer map has worked to provide us with some already interesting relations between $E(K)$, $\mathrm{Gal}(\overline{K}/K)$, and $E[2]$. One will note from remark (iii) following Definition 1.1 that (iii) of the above Proposition is to be expected, while (iv) is a coarse looking assertion due to the sheer size of the extension L/K. But this is actually the content of the proof of the Mordell-Weil Theorem presented in [Sil09, Chapter 8, §1]. But getting back to 2-descent, the above Proposition tells us we have the homomorphism

$$\delta_E : E(K)/2E(K) \to \mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), E[2]), \tag{1.5}$$

where $\delta_E(P)(\sigma) = \kappa_2(P, \sigma)$ (note the similarity to the connecting homomorphism δ in Remark 1). In the same remark, we introduced an exact sequence in Equation 1.2. Using the analogy of elliptic curves as described at the start of [Del07, Section 1], we arrive at an analogous exact sequence

$$1 \to \mu_2 \to \overline{K}^* \to \overline{K}^* \to 1, \tag{1.6}$$

where the third arrow from the left is the map $z \mapsto z^m$. Taking Galois cohomology yields the short exact sequence

$$1 \to (K^*)/(K^*)^2 \to H^1(\mathrm{Gal}(\overline{K}/K), \mu_2) \to H^1(\mathrm{Gal}(\overline{K}/K), \overline{K}^*)[2] \to 0 \tag{1.7}$$

where the second arrow from the left is the connecting homomorphism δ_K. One will now immediately recall the following famous theorem of Hilbert.

Proposition 1.3 (Hilbert's Theorem 90)**.** $H^1(Gal(\overline{K}/K), \overline{K}^*) = 0$.

Proof. [Ser13, Chapter X, Proposition 2]. □

In particular, we have that δ_K is an isomorphism. Explicitly computing δ gives us that $\delta(a)$ is the cohomology class of the map $\sigma \mapsto \sigma(\alpha)/\alpha$, where $\alpha \in \overline{K}^*$ is any element satisfying $\alpha^2 = a$.

But let us not stop here in gathering facts about $E(K)$, $E[2]$, and $\mathrm{Gal}(\overline{K}/K)$, because to make sense better sense of this analogy, we must ask that based on this analogy, if $E[2] \subset E(K)$, does $\mu_2 \subset K^*$? The answer to this is obviously yes, but it in fact holds for 2 replaced by any integer $m > 2$. A reading of [Sil09, Chapter III, §8] will lead one to recall the following:

Definition 1.4. *Let g be as in* [Sil09, p. 93]. *Define the* ***Weil pairing*** *as the map*

$$e_2 : E[2] \times E[2] \to \mu_2 \tag{1.8}$$

where $e_2(S, T) = g(X + S)/g(X)$.

The original goal of this pairing was to generate a pairing on $E[2]$ that was Galois invariant, so as to resolve the problem that the natural determinant pairing is not Galois invariant. We prove this Galois invariance, along with other important properties, in the following proposition.

Proposition 1.5. *The Weil pairing enjoys the following properties:*

i. It is bilinear.
ii. It is alternating: $e_m(T, T) = 1$. In particular, $e_m(S, T) = e_m(T, S)^{-1}$.
iii. It is nondegenerate: if $e_m(S, T) = 1$ for all $S \in E[2]$, then $T = O$.
iv. It is Galois invariant:

$$\sigma(e_2(S, T)) = e_2(\sigma(S), \sigma(T)) \tag{1.9}$$

for any $\sigma \in Gal(\overline{K}/K)$.

Proof. (i): The key ingredient in proving the linearity of the first factor will be the following observation. The map $k : E \to \mathbb{P}^1$ defined by $k(X) = g(X + S)/g(X)$ for a fixed $S \in E[2]$. Then, $k(X)$ is an mth root of unity and takes on finitely many values, and so is not surjective, and hence constant ([Sil09, Chapter 2, Theorem 2.3]). The proof of linearity in the first factor is concluded by working directly with the definition of e_2.

Finally, we sketch the proof of linearity in the second factor. Let g_1, g_2, g_3 be the g's associated to T_1, T_2, and $T_3 = T_1 + T_2$. Then, express g_3 in terms of g_1 and g_2 to bring $g_3(X + S)/g_3(X)$ closer to the desired form.

(ii): An application of bilinearity to the expression $e_m(S + T, S + T)$ reduces the proof to showing that $e_m(T, T) = 1$ for all $T \in E[m]$. The desired expression is then $g(X + T) = g(X)$. Recall that e_2 is well-defined because the function $X \mapsto g(X + T)/g(X)$ is constant. We would like to do the same here: construct a constant function with the desired form. The equation $\div(f) = m(T) - m(O)$ hints that we might be able to construct a function with zero divisor, as it is principal. In this light, we utilize the following trick:

$$\mathrm{div}\,(f(X)f(X + T)) = m(T) - m(O) + m(O) - m(-T). \tag{1.10}$$

And since $-T = T$, this divisor is zero, and so $f(X)f(X + T)$ is constant. Now if we choose $T' \in E$ with $2T' = T$, we know $g(X)g(X + T')$ is also constant since $f \circ [2] = g^2$. So,

$$g(X)g(X + T') = g(X + T')g(X + T' + T') = g(X + T')g(X + T) \tag{1.11}$$

and since $g(X+T') \neq 0$ (true since $f(X)f(X+T) \neq 0$, and $g(X)^m g(X+T')^m = f(X)f(X+T)$), $g(X) = g(X+T)$ as desired.
(iii): Suppose $e_2(S,T) = 1$ for all $S \in E[2]$, and so $g(X+S) = g(X)$. Then, [Sil09, Chapter III, Theorem 4.10(b,c)] tells us that $g \in [2]^*\overline{K}(E)$. Therefore, $g = h \circ [2]$ for some $h \in \overline{K}(E)$. So then, $(h \circ [2])^2 = g^2 = f \circ [2]$, and because $[2] : E \to E$ is surjective, $f = h^2$. Then, $\mathrm{div}(h) = (T) - (O)$, and since $\mathrm{div}(h)$ is principal, $T =)$ by [Sil09, Chapter III, Theorem 3.3]. (iv): Direct verification from the action of $\mathrm{Gal}(\overline{K}/K)$ on f and g. □

Remark. *The Weil pairing exists for any positive integer, not just 2. Similarly, the above Proposition works for any positive integer. But because our focus is 2-descent, we only discuss the case $m = 2$.*

With this remark we consider general e_m ($m \geq 2$) for illustrative purposes and assume $E[m] \subset E(K)$. Now, an element of K is fixed by all elements of $\mathrm{Gal}(\overline{K}/K)$. But for $P = \sigma(P)$ for $P \in E[m]$ and $\sigma \in \mathrm{Gal}(\overline{K}/K)$ because $E[m] \subset E(K)$. So, we actually have that the *image* of e_m is invariant under $\mathrm{Gal}(\overline{K}/K)$. And a bit of group theory and use of (i) and (iii) allows us to deduce that $e_,$ is actually surjective. So we have reached our promise that $\mu_m \subset K^*$!

So now we return to the case of $m = 2$. An interesting question now is: how can we combine all of the above ideas together? We construct a bilinear pairing that meshes all of the others together.

Theorem 1.6. *We have the following:*

i. With notation as above, there is a bilinear pairing

$$\rho : E(K)/2E(K) \times E[2] \to (K^*)/(K^*)^2 \tag{1.12}$$

which satisfies $e_m(\delta_E(P)(\sigma), T) = \delta_K(\rho(P,T))(\sigma)$ for all $\sigma \in Gal(\overline{K}/K)$ (recall the definitions of δ_E and δ_K from Equations 1.5 and 1.7, respectively).

ii. This pairing ρ is non-degenerate on the left.

iii. Let $S \subset M_K$ be the set of infinite places, finite primes at which E has bad reduction, and the set of primes dividing m. Then,

$$im(\rho) \subset K(S,2) = \{b \in (K^*)/(K^*)^2 : ord_v(b) \cong 0 \pmod m \text{ for all } v \notin S\}. \tag{1.13}$$

iv. The pairing in (a) can be computed as follows. For $T \in E[2]$, choose $f_T, g_T \in K(E)$ satisfying

$$div(f_T) = m(T) - m(O) \text{ and } f_T \circ [2] = g_T^2. \tag{1.14}$$

Then for any $T \neq P \in E(K)$, $\rho(P,T) \cong f_T(P) \pmod{(K^*)^2}$. The case of $P = T$ may be handled with exploiting linearity on ρ.

Proof. (i): Proposition 1.3 shows that the property ρ satisfies in fact makes it well-defined. Bilnearity then follows from the bilinearity of κ_2 and e_2.
(ii): Use the isomorphism of Propostion 1.3 combined with the nondegeneracy of e_2 (Proposition 1.5(iii)).
(iii): If we let $\beta = \rho(P,T)^{1/2}$, then $K(\beta) \subset L$ where L is as in Proposition 1.2(iv) (for this, trace through the definition to get back to ρ to get to κ_2). Since L is unramified, over K, so is $K(\beta)$. This is true if and only if $\mathrm{ord}_v(\beta^m) \cong 0 \pmod m$. (iv): Set $\rho(P,T) = \beta^2$ for $\beta \in \overline{K}$. The proof then largely follows from an application of Proposition 1.3. □

So now one must ask: What is the use of this pairing ρ? The key lies in (ii) and (iii) of the above proposition. In the proof of [Sil09, Chapter 8, Proposition 1.6], it is explicitly shown that $K(S,2)$

is finite. Keep this in mind for a moment as we discussion the implications of (ii). Fix generators T_1 and T_2 of $E[2]$, and consider $\rho(P, T_1)$ and $\rho(P, T_2)$ for some $P \in E(K)/2E(K)$. By bilinearity of ρ, quantities of this form will generate all the values the image of ρ. Now consider a point $Q \neq P$. Then, if $\rho(P, T_i) = \rho(Q, T_i)$ for $i = 1, 2$, then by (ii), we must have that $P = Q$ by bilinearity.

The upshot then is that properties (ii) and (iii) give us an injection $\iota : E(K)/2E(K) \to K(S, 2) \times K(S, 2)$. And by the bilinearity of ρ this is actually a homomorphism! Hence, we can deduce the structure of $E(K)/2E(K)$ by the First Isomorphism Theorem. All that remains to do now is to sketch how to find the image of ι. In this case, since $E[2] \subset E(K)$, the function $f_T = x - x(T)$ will satisfy (iv) of the above Theorem for some g_T. Also, our elliptic curve will be of the form $y^2 = (x-e_1)(x-e_2)(x-e_3)$ for some set of $e_i \in K$. Any two non-zero 2-torsion points will generate $E[2]$, say $(e_1, 0)$ and $(e_2, 0)$. So for fixed $b_1, b_2 \in K(S, 2)$, we question if we can solve the system

$$y^2 = (x - e_1)(x - e_2)(x - e_3), b_1 z_1^2 = x - e_1, b_2 z_2^2 = x - e_2. \tag{1.15}$$

By working through the algebra and carefully handling cases of the form $\rho(T_i, T_i)$ (see the last sentence of (iv)), we obtain the following Proposition.

Proposition 1.7. ***[Complete 2-Descent]*** *Let E/K be an elliptic curve given by a Weierstrass equation*

$$y^2 = (x - e_1)(x - e_2)(x - e_3) \tag{1.16}$$

where the $e_i \in K$. Let S be the finite set of places of K containing all archimedean places, all places dividing 2, and all places at which E has bad reduction. Let $K(S, 2)$ be as defined above. Then the mapping

$$\iota_2 : E(K)/2E(K) \to K(S, 2) \times K(S, 2) \tag{1.17}$$

defined by

$$P = (x, y) \mapsto \begin{cases} (x - e_1, x - e_2) & x \neq e_1, e_2 \\ \left(\frac{e_1 - e_3}{e_1 - e_2}, e_1 - e_2\right) & x = e_1 \\ \left(e_2 - e_1, \frac{e_2 - e_3}{e_2 - e_1}\right) & x = e_2 \\ (1, 1) & P = \mathcal{O} \end{cases} \tag{1.18}$$

is an injective homomorphism. Now, let $(b_1, b_2) \in K(S, 2) \times K(S, 2)$ be a pair that is not the image of $\mathcal{O}$, $(e_1, 0)$, or $(e_2, 0)$. Then, this data point has preimage $P = (x, y)$ if and only if the system

$$b_1 z_1^2 - b_2 z_2^2 = e_2 - e_1 \tag{1.19}$$

$$b_1 z_1^2 - b_1 b_2 z_3^2 = e_3 - e_1 \tag{1.20}$$

has a solution with $z_1, z_2 \in K^*$ and $z_3 \in K$. For such a solution, $x = b_1 z_1^2 + e_1$ and $y = b_1 b_2 z_1 z_2 z_3$.

This will conclude the discussion of 2-descent in the case where $E[2] \subset E(K)$. However, such a condition feels quite strong. We now present a version of 2-descent where E has what is called a 2-isogeny: Assume that $E(K)[2]$ has a non-zero point T, and we can then construct an isogeny $\phi : E \to E'$ with kernel $\{\mathcal{O}, T\}$.

2. The Case of a 2-Isogeny

As we are now dealing with a less strict condition, we will need some more technology before advancing. But beyond this theory, what will allow us to construct a version of 2-descent in this case is the isomorphism $\delta_K : (K^*)/(K^*)^2 \to H^1(\mathrm{Gal}(\overline{K}/K), \mu_2)$, as it provides us a bridge from algebra (domain of δ_K, and the content of §1) to cohomology (codomain of δ_K, and the content of

this section). In fact, the beginnings of the construction of 2-descent in this case exactly rely on Theorem 1.6 to get going.

An *isogeny* is a morphism $\alpha : E \to E'$ between two elliptic curves E and E' such that $\alpha(O) = O'$, where O and O' are the base points of E and E', respectively. We will refer to a 2-isogeny in this section as a map of the form ϕ presented in the last sentence of §1. The following result about isogenies will be critical in the coming presentation. It takes statements from [Sil09, Chapter III, Theorem 6.1, Theorem 6.2].

Theorem 2.1. *Fix an isogeny $\alpha : E \to E'$ of degree m (equivalent to the statement that $\#\ker\alpha = m$). Then, there exists a unique isogeny $\hat{\alpha} : E' \to E$ such that $\hat{\alpha} \circ \alpha = [m]$ on E and $\alpha \circ \hat{\alpha} = [m]$ on E'.*

Proof. See the proofs of [Sil09, Chapter III, Theorem 6.1, Theorem 6.2]. □

Although the existence of a unique dual isogeny as demonstrated in this theorem is all we will need in practice, for more context one can turn to [Sil09, Chapter III, §4, 6] as a start.

2.1. **The Build-Up to the Interchange of Algebra and Cohomology.** One will notice that in Theorem 1.7, not only were we able to give a structure to $E(K)/2E(K)$ as a subgroup of $K(S,2) \times K(S,2)$, but in a majority of cases we were able to conclude that we had a point $E(K)/2E(K)$ if and only if it satisfied a system of equations. It turns out we can continue to do this in the context of cohomology.

Remark. *The upshot of the theory we present in this subsection are Proposition 2.8, Theorem 2.9, and the calculation following the proof of this Theorem. Because it is only these three results of what is presented in this subsection that will be quoted in the second subsection, a more cohesive first read might be to skip to these three results instead of getting bogged down in all the technical details that precede them. If one chooses to come back and read these details, pay attention to the natural flow of the build-up. Every object constructed has a motive as to how it precises the theory that precedes it.*

To begin, we first need to establish some definitions (in a more general context) that in a sense allows us to measure the relatedness of two curves. The first one helps form a base measure.

Definition 2.2. *Let C/K be a smooth projective curve. The **automorphism group of** C, denoted $Aut(C)$, is a group of $\overline{K}$-isomorphisms of C.*

We now move to relate C to other curves.

Definition 2.3. *A **twist of** C/K is a smooth curve C'/K that is $\overline{K}$-isomorphic to C. Two twists are equivalent if they are isomorphic over K. Denote this set of equivalences as $Twist(C/K)$.*

Now fix a twist C' of C, and let $\phi : C \to C'$ be the corresponding isomorphism. Now armed with these two definitions, we can now define a measure of the relatedness of C' and C by seeing how far off ϕ is from a K-isomorphism. Consider the map

$$\xi : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(C), \xi(\sigma) = \phi^{\sigma}\phi^{-1}, \tag{2.1}$$

where σ acts on the coefficients of ϕ. Notice that if ϕ is defined over K, $\phi^{\sigma} = \phi$ and so ξ sends everything to the identity — that is, something that is "purely" C.

Next up is to answer the question, "What can we do with all this?"

Theorem 2.4. *Let C, C', ϕ, ξ be as above. Then the following are true.*

i. The map ξ is a 1-cocycle. We denote the corresponding cohomology class by $\{\xi\}$.
ii. $\{\xi\}$ is determined by the K-isomorphism class of C' and is independent of the choice of ϕ. So we obtain a natural map

$$Twist(C/K) \to H^1(Gal(\overline{K}/K), Aut(C)). \tag{2.2}$$

iii. The map in (ii) is a bijection.

Proof. (i): This claim is by definition just checking that $\xi(\sigma \circ \tau) = (\xi_\sigma)^\tau \circ \xi(\tau)$.
(ii): Let C''/K be another twists of C that is K-isomorphic to C'. Now choose a $\overline{K}$-isomorphism $\psi : C'' \to C$. It remains to show that $\phi^\sigma\phi^{-1}$ and $\psi^\sigma\psi^{-1}$ are in the same cohomology class. To do this, we tie together ϕ and ψ with a K-isomorphism $\theta : C'' \to C$. Consider $\alpha = \phi \circ \theta\psi^{-1}$. A quick calculation yields that $\alpha^\sigma \circ \psi^\sigma \circ \psi^{-1} = \phi^\sigma \circ \phi^{-1} \circ \alpha$, which suffices.
(iii): Suppose C' and C'' as defined above yield the same cohomology class in $H^1(\mathrm{Gal}(\overline{K}/K), \mathrm{Aut}(C))$. Let ϕ, ψ, α be as defined above. Now consider the map $\theta : C'' \to C$ where $\theta = \phi^{-1} \circ \alpha \circ \psi$. A quick computation will show that $\theta^\sigma = \theta$, proving that θ is defined over K. So, the natural map in (ii) is injective.

To prove that the natural map is surjective, we start with a 1-cocycle $\xi : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(C)$. Denote the function field twisted by ξ as $\overline{K}(C)_\xi$. It is isomorphic to $\overline{K}(C)$ (say by an isomorphism Z), but the difference is that $Z(f)^\sigma = Z(f^\sigma\xi(\sigma))$. In otherwords, the action of $\mathrm{Gal}(\overline{K}/K)$ on $\overline{K}(C)_\xi$ is twisted by ξ.

Consider now the subfield $\mathcal{F} \subset \overline{K}(C)_\xi$ that is fixed by $\mathrm{Gal}(\overline{K}/K)$. By considering Galois invariance, one can show that $\mathcal{F} \cap \overline{K} = K$.

Next, the fact that $\overline{K}\mathcal{F} = \overline{K}(C)_\xi$ follows immediately from [Sil09, Chapter II, Lemma 5.8.1] applied to the $\overline{K}$-vector space $\overline{K}(C)_\xi$. What this implies is that $\mathcal{F}$ has transcendence degree 1 over K, and so by [Sil09, Chapter II, Theorem 2.4(c)] we have that $\mathcal{F} \simeq K(C')$ for some twists C'. From the above fact, we also have that $\overline{K}(C') \simeq \overline{K}(C)$. Then, [Sil09, Chapter II, Corollary 2.4.1] tells us that C' and C are isomorphic over $\overline{K}$, say by a map $\phi : C \to C'$. It now remains to show that C' gives the desired cohomology class $\{\xi\}$.

For what remains, set $\phi^* = Z$, so that the twisted action $Z(f)^\sigma = Z(f^\sigma \circ \xi(\sigma))$ can be rewritten as $(f \circ \phi)^\sigma = f^\sigma \circ \xi(\sigma) \circ \phi$. This will show that $\phi^\sigma = \xi(\sigma) \circ \phi$, and we're done. □

We now apply this theory to an elliptic curve E/K. Now, in addition to being a curve, E also has a group structure. So we now look for classes in $\mathrm{Twist}(E/K)$ on which we may find a similar addition structure. For that, we turn to the following definition.

Definition 2.5. *A **principal homogeneous space** for E/K is a pair $(C/K, \mu)$, where C is a smooth curve and*

$$\mu : C \times E \to C \tag{2.3}$$

is a morphism defined over K which satisfies the following three properties:

i. $\mu(p, O) = p$ for all $p \in C$
ii. $\mu(\mu(p, P), Q) = \mu(p, P + Q)$ for all $p \in C$ and $P, Q \in E$
iii. For all $p, q \in C$ there is a unique $P \in E$ such that $\mu(p, P) = q$.

Now because we want μ to define an addition structure on C, we shall denote $\mu(p, P) = p +_C P$. Addition on E will just be denoted by "+". With that set, we return to deducing facts from the above definition. Property (iii) highly suggests that we can define a subtraction map $\nu : C \times C \to E$, where

for q, p, P described in (iii), $\nu(q, p) = P$. It turns out that defining $\nu(q, p) = q -_C p$ leads to a notion of addition and subtraction on C that does what we expect it to.

We now prove the tacit claim we skipped over earlier: that this curve C in the pair (C, μ) is actually a twist of E. Some other properties may also be picked up along the way.

Proposition 2.6. *Let E and C be as above, and fix a point $p_0 \in C$ and define a map*

$$\theta : E \to C, P \mapsto p_0 +_C P. \tag{2.4}$$

i. The map θ is an isomorphism defined over $K(p_0)$. In particular, C is a twist of E.
ii. For all $p \in C$ and all $P \in E$,

$$p +_C P = \theta(\theta^{-1}(p) + P). \tag{2.5}$$

iii. For all $p, q \in C$, $q -_C p = \theta^{-1}(q) - \theta^{-1}(p)$.
iv. The subtraction map ν is a morphism and defined over K.

Proof. (i): For $\sigma \in \mathrm{Gal}(\overline{K}/K)$ such that $\sigma(p_0) = p_0$,

$$\sigma(\theta(P)) = \sigma(p_0) +_C \sigma(P) = p_0 +_C \sigma(P) = \theta(\sigma(P)). \tag{2.6}$$

Then, the kernel of this map has cardinality 1, so its degree is 1. Then, [Sil09, Chapter II, Corollary 2.4.1] does the job.
(ii): Follows from computation using the fact that θ is an isomorphism.
(iii): Same proof structure as (ii).
(iv): We use [Sil09, Chapter III, Theorem 3.6] and (iii) to conclude that ν is a morphism. Then, for any $\sigma \in \mathrm{Gal}(\overline{K}/K)$,

$$\sigma((q -_C p)) = \sigma(\theta^{-1}(q) - \theta^{-1}(p)) = \sigma(\theta^{-1}(q)) - \sigma(\theta^{-1}(p)) \tag{2.7}$$

since subtraction on E is defined over K. Then,

$$\sigma(\theta^{-1}(q)) - \sigma(\theta^{-1}(p)) = \sigma(p_0 +_C \theta^{-1}(q)) - \sigma(p_0 +_C \theta^{-1}(p)) \tag{2.8}$$

since μ is defined over K. But of course this last quantity is just $\sigma(q) -_C \sigma(p)$. □

Now as is going with the theme of this section so far, we want to identify those homogeneous spaces, say C and C',which are related by a K-isomorphism $\theta : C \to C'$, then consider the set of homogeneous spaces modulo this equivalence relation. However, *we must also carry over the action of E on C to C'*. So, we add a criterion onto our equivalence relation the compatability condition that $\theta(p +_C P) = \theta(p) +_{C'} P$.

Definition 2.7. *The set of these equivalence classes is called the **Weil-Châtelet group for** E/K and is denoted by $WC(E/K)$. The equivalence class containing E/K is called the **trivial class**.*

Remark. *One will note in our definition we call $WC(E/K)$ a group. The reason for this is presented in Theorem 2.9, and is the connective tissue between this section and the first, for it carries an algebraic concept into cohomology.*

It will be important for us later to talk about the identity element of $WC(E/K)$: the trivial class. We can in fact easily characterize it.

Proposition 2.8. *Let C and E be as in this section so far. Then, C/K is in the trivial class of $WC(E/K)$ if and only if $C(K)$ is not the empty set.*

Proof. If C/K is in the trivial class, there is a K-isomorphism $\theta : E \to C$. Then, $\theta(O) \in C(K)$ since $O \in E(K)$.

Now suppose that $p_0 \in C_K$. Then recall the isomorphism $\theta : E \to C$ given by $\theta(P) = p_0 +_C P$ in Proposition 2.6(i). By this statement, it is an isomorphism defined over $K(p_0) = K$. Finally, the compatability condition on θ is just the (ii) of Definition 2.5. □

The remark discuss preceding the above proposition now deepens, as checking the triviality of a homogeneous space is just answering the fundamental Diophantine question of, "Does this curve have any rational solutions?" It turns out this few thousand year old question can be rephrased in terms of cohomology, as we now present.

Theorem 2.9. *Let E/K be an elliptic curve. There is a bijection*

$$WC(E/K) \longleftrightarrow H^1(Gal(\overline{K}/K), E) \tag{2.9}$$

defined as follows: let C/K be a homogeneous space for E/K and choose any point $p_0 \in C$. Then, $\{C/K\} \mapsto \{\sigma \mapsto \sigma(p_0) - p_0\}$.

Remark. *We use this theorem to define a group structure on $WC(E/K)$, yield a group isomorphism $WC(E/K) \xrightarrow{\sim} H^1(Gal(\overline{K}/K), E)$.*

Proof. We first check that the map is well-defined. Because $\sigma \mapsto \sigma(p_0) - p_0$ is a 1-cocycle. Next, let C and C' be equivalent homogeneous spaces with K-isomorphism $\theta : C \to C'$. We observe that for this equivalence $\theta : C \to C'$ of homogeneous spaces, $\theta(q) -_{C'} \theta(p) = q -_C p$. This is an identity that is just a matter of cleverly grouping together points. This tells us that for $p_0' \in C'$, $\sigma(p_0) - p_0$ differ by the coboundary $\sigma((\theta(p_0) -_{C'} p_0')) -_{C'} (\theta(p_0) -_{C'} p_0')$.

For injectivity, let everything be as in the previous paragraph, and suppose that there exists $P_0 \in E$ satisfying

$$\sigma(p_0) -_C = p_0 = \sigma(p_0') -_{C'} p_0' +_(\sigma(P_0) - P_0). \tag{2.10}$$

Then, it turns out the $\overline{K}$-isomorphism $\theta : C \to C'$ given by $p \mapsto p_0' -_{C'} (p -_C p_0) + P_0$. is actually a K-isomorphism. This suffices to prove injectivity.

For surjectivity, let $\xi : \mathrm{Gal}(\overline{K}/K) \to E$ represent an element in $H^1(\mathrm{Gal}(\overline{K}/K), E)$. We defer Theorem 2.4 and construct an embedding $E \hookrightarrow \mathrm{Aut}(E)$ via $P \mapsto \tau_P$, which is translation by P. So now we consider ξ in the group $H^1(\mathrm{Gal}(\overline{K}/K), \mathrm{Aut}(E))$, from which we may apply Theorem 2.4 to find a twist C/K and a $\overline{K}$-isomorphism $\phi : C \to E$ such that $-\xi(\sigma) = \phi^\sigma \circ \phi^{-1}$. Then, one checks that the map $\mu : C \times E \to C$ where $\mu(p, P) = \phi^{-1}(\phi(p) + P)$ makes the pair (C, μ) a homogeneous space. Then, take $p_0 = \phi^{-1}(O)$. Then, $\sigma(p_0) -_C p_0 = \xi(\sigma)$, and so we're done. □

Let us now apply this theory to our case of 2-descent. We stated at the beginning of the section that we require $E(K)$ have at least 2 points of 2-torsion, say O and T. After translating the curve we may assume that E takes the form

$$E : y^2 = x^3 + ax^2 + bx \tag{2.11}$$

where $T = (0, 0)$.

Now let $K(\sqrt{d})/K$ be a quadratic extension of K, and let T be as above. Then, then homomorphism

$$\xi : \mathrm{Gal}(\overline{K}/K) \to E, \sigma \mapsto \begin{cases} O & \sigma(\sqrt{d}) = \sqrt{d} \\ T & \sigma(\sqrt{d}) = -\sqrt{d} \end{cases} \tag{2.12}$$

is actually a 1-cocycle, and so we construct the homogeneous space corresponding to ξ. Now as in the above Theorem, we embed $E \hookrightarrow \mathrm{Aut}(E)$. Then for a point $P = (x, y)$,

$$\tau_T(P) = \left(\frac{b}{x}, -\frac{by}{x^2}\right). \tag{2.13}$$

Hence the action of a non-trivial automorphism $\sigma \in \mathrm{Gal}(\overline{K}/K)$ on $K(\sqrt{d})$ on $\overline{K}(E)$ is determined by the following:

$$\sigma(\sqrt{d}) = -\sqrt{d} x^\sigma = \frac{b}{x}, y^\sigma = -\frac{by}{x^2} \tag{2.14}$$

as one will recall that $\overline{K}(E) = \overline{K}(x, y)$, where x and y are the Weierstrass coordinate functions for E ([Sil09, Chapter III, Corollary 3.1.1]). As one will recall in the proof of Theorem 2.4, the twist we are looking for is the one whose function field is the subfield of $\overline{K}(E)_\xi$ fixed by $\mathrm{Gal}(\overline{K}/K)$. By considering the fixed functions

$$z = \frac{x\sqrt{d}}{y}, w = \sqrt{d}\left(x - \frac{b}{x}\right)\left(\frac{x}{y}\right)^2 \tag{2.15}$$

one finds the relation $C : dw^2 = d^2 - 2adz^2 + (a^2 - 4b)z^4$. It turns out from some theory presented in [Sil09, Chapter II, Proposition 2.5.2] on hyperelliptic curves that C extends to a smooth projective curve. So, we have found our desired twist C with an isomorphism $\theta : E \to C$ defined over $K(\sqrt{d})$ where $(x, y) \mapsto (z, w)$ (we obtain this by showing that ϕ has an inverse and is hence bijective, and so has only one element in its kernel, after which we may apply [Sil09, Chapter II, Corollary 2.4.1]).

It now remains to compute what element of $H^1(\mathrm{Gal}(\overline{K}/K, E)$ corresponds to C. And luckily, taking any point $p \in C$ and taking the cocycle $\sigma \mapsto \sigma(p) -_C p$ suffices to show that C maps to $\{\xi\}$! Remember this curve C. It will become very useful to us in what follows.

With all of this theory, we have firmly concluded the investigation of twists of an elliptic curve E/K in the sense that we are now able to turn to the Diophantine nature of the task at hand.

2.2. **Formulating 2-Descent: Local to Global Considerations.** Diophantine equations in local fields K_v (with v a place of K) may be solved relatively simply thanks to Hensel's Lemma (see, for instance, [Mil08, Chapter 7, Theorem 7.33]). To summarize: Let $\mathfrak{m} = \{x \in K : v(x) > 0\}$ and $A = \{x \in K : v(x) \geq 0\}$. Then a solution to a polynomial in $A/\mathfrak{m}$ lifts to a solution in A. And since the field $A/\mathfrak{m}$ is finite in our case, we would be looking at only a finite amount of computation.

However, just because a Diophantine equation is solvable in all K_v does not mean it is solvable is K (this unfortunate fact is the infamous failure of the Hasse-Minkowski local-to-global principle for higher degree polynomials). We in fact use this in one of our definitions to come.

With the idea of this subsection set up, we move to establish some concrete theory. Let $\phi : E \to E'$ be a non-zero isogeny. Then we have a short exact sequence of $\mathrm{Gal}(\overline{K}/K)$-modules:

$$0 \longrightarrow E[\phi] \longrightarrow E \xrightarrow{\phi} E' \longrightarrow 0. \tag{2.16}$$

Then we can take Galois cohomology to get a long exact sequence of cohomology groups, from which we may extract the following short exact sequence

$$0 \longrightarrow E'(K)/\phi(E(K)) \xrightarrow{\delta} H^1(\mathrm{Gal}(\overline{K}/K), E[\phi]) \longrightarrow H^1(\mathrm{Gal}(\overline{K}/K), E)[\phi] \longrightarrow 0. \tag{2.17}$$

where δ is the connecting homomorphism. We now turn to local considerations. Choose a place v of K, and extend v to $\overline{K}$ so as to embed $\overline{K} \subset \overline{K}_v$ and a decomposition group $G_v \subset \mathrm{Gal}(\overline{K}/K)$. One

may mimic the above argument to obtain exact sequences

$$0 \longrightarrow E'(K_v)/\phi(E(K_v)) \xrightarrow{\delta_v} H^1(G_v, E[\phi]) \longrightarrow H^1(G_v, E)[\phi] \longrightarrow 0 \tag{2.18}$$

where δ_v is the connecting homomorphism. Now the inclusions $G_v \subset \mathrm{Gal}(\overline{K}/K)$ and $E(\overline{K}) \subset E(\overline{K}_v$ give us restriction maps on cohomology (see [Sil09, Appendix B]). Furthermore, the fourth term in each of the above exact sequences may be replaced by $WC(E/K)[\phi]$ or $WC(E/K_v)[\phi]$ by Theorem 2.9. So, gluing everything together we get the following commutative diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E'(K)/\phi(E(K)) & \xrightarrow{\delta} & H^1(\mathrm{Gal}(\overline{K}/K), E[\phi]) & \longrightarrow & WC(E/K)[\phi] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \prod_v E'(K_v)/\phi(E(K_v)) & \xrightarrow{\delta_v} & \prod_v H^1(G_v, E[\phi]) & \longrightarrow & \prod_v WC(E/K_v)[\phi] & \longrightarrow & 0
\end{array} \tag{2.19}$$

Here, the product is taken over all places of K. Now, we want to focus on the part of the commutative diagram that contains the Weil-Châtelet groups. And one will notice that in the commutative diagram,

$$\ker\left(H^1(\mathrm{Gal}(\overline{K}/K), E[\phi] \to WC(E/K)[\phi]\right) \tag{2.20}$$

will determine the behavior of the mappings in the top row! Of course, this is going to be quite difficult, as determining this kernel is, by Proposition 2.8, determining the existence of K-rational points on homogeneous spaces of E. But the local kernel

$$\ker\left(H^1(G_v, E[\phi]) \to WC(E/K_v)[\phi]\right) \tag{2.21}$$

is easier to determine by the discussion at the start of this section. As also discussed, there is also a failure of the local-to-global principle. This prompts the following two definitions.

Definition 2.10. *Let $\phi : E/K \to E'/K$ be an isogeny. The ϕ-Selmer group of E/K is defined by*

$$S^{\phi}(E/K) = ker\left(H^1(Gal(\overline{K}/K), E[\phi] \to \prod_v WC(E/K_v)[\phi]\right) \tag{2.22}$$

Definition 2.11. *The Shafarevich-Tate group of E/K is given by*

$$Ш(E/K) = ker\left(WC(E/K) \to \prod_v WC(E/K_v)\right). \tag{2.23}$$

The structure of the remainder of this section will be as follows. We present two key results: the first with proof and the second without, as the latter will follow from the definitions. From there, we exit this subsection and formulate 2-descent in this case.

The first result is just the observation that from the way we have defined the Selmer and Shafaverich-Tate groups that an exact sequence is somewhere to be found.

Theorem 2.12. *There is an exact sequence*

$$0 \longrightarrow E'(K)/\phi(E(K)) \longrightarrow S^{\phi}(E/K) \longrightarrow Ш(E/K)[\phi] \longrightarrow 0. \tag{2.24}$$

The second result yields us two finiteness statements.

Theorem 2.13. *Let M be a finite abelian $Gal(\overline{K}/K)$-module, and let $S \subset M_K$ be a finite set of places. Define*

$$H^1(Gal(\overline{K}/K), M; S) = \{\xi \in H^1(Gal(\overline{K}/K), M) : \xi \text{ is unramified outside } S\}. \tag{2.25}$$

Then, we have the following:

i. $H^1(Gal(\overline{K}/K), M; S)$ *is finite.*

ii. Let S *consist of the infinite places of* K*, places where* E *has bad reduction, and places* v *where* $v(\deg \phi) > 0$*. Then,*

$$S^{\phi}(E/K) \subset H^1(Gal(\overline{K}/K), E[\phi]; S). \tag{2.26}$$

In particular, $S^{\phi}(E/K)$ *is finite, since it is a subset of* $H^1(Gal(\overline{K}/K), M; S)$*.*

Proof. (ii): Let $\xi \in S^{\phi}(E/K)$ and let $v \notin S$. From the declaration of ξ we know that it is trivial in $WC(E/K_v)$ for any place v of K. And so in particular by Theorem **??**, there is a point $P \in E(K_v)$ such that $\xi(\sigma) = \{\sigma(P) - P\}$ for all $\sigma \in G_v$. Because I_v acts trivially on the residue field of K_v, $\sigma(P) - P$ is in the kernel of the "reduction modulo v" map $E \to \tilde{E}$ (see [Sil09, Chapter 7, Section 2] for a discussion on this topic).

But now $\sigma(P) - P \in E[\phi] \subset E[m]$ (true since E is defined over K). And since $E(K_v)[m]$ injects into $\tilde{E}_v$, we have that $P = \sigma(P)$. This will complete the proof that ξ is unramified at v. Now, the second claim of (ii) follows directly from (i).

(i): Since $\mathrm{Gal}(\overline{K}/K)$ acts continuously on M. Here, the continuous action is defined with respect to cosets of finite index normal subgroups of $\mathrm{Gal}(\overline{K}/K)$ and the discrete topology on M. This is all equivalent to saying that the stabilizer of the action of $\mathrm{Gal}(\overline{K}/K)$ on an element $m \in M$ is a subgroup of $\mathrm{Gal}(\overline{K}/K)$ of finite index.

Then, using the inflation-restriction sequence ([Sil09, Appendix B, Section 2]), we may prove this lemma for a finite extension of K. Choose one so large that the action of $\mathrm{Gal}(\overline{K}/K)$ on M is trivial, where

$$H^1(\mathrm{Gal}(\overline{K}/K), M; S) = \mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), M; S). \tag{2.27}$$

Note the notation on the right does not need an extra definition as due to the trivial action, any homomorphism $\mathrm{Gal}(\overline{K}/K) \to M$ will also be a 1-cocycle, from which we can apply already supplied definitions.

Now M is finite, and so there exists some smallest positive integer m such that $mM = \{0\}$. Let L/K be the maximal abelian extension of exponent m that is unramified outside S. By [Sil09, Chapter VIII, Proposition 1.6], this extension is finite, and the isomorphic natural map

$$\mathrm{Hom}(\mathrm{Gal}(L/K), M; S) \to \mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), M; S) \tag{2.28}$$

finishes the job. □

Now notice that this Theorem allows us to compute $S^{\phi}(E/K)$. This is because outside of S, E has good reduction at v, and in particular its reduction is an actual elliptic curve E_v/K_v. Then, any homogeneous space of E_v/K_v is $\overline{K}_v$-isomorphic to E_v/K_v. In particular, the genera of both are 1, and by the Hasse-Weil bound, both have a rational point in a finite field. Then, Hensel's lemma allows us to lift this solution to a solution in K_v. So, in such cases, $C(K_v) \neq$ and so C is in the trivial class of $WC(E/K_v)$.

Now let's go back to the exact sequence in Equation 2.24. In an optimal setting where we have a local-tolglobal principle (i.e., $Ш(E/K)[\phi] =$), this means we have an isomorphism $E'(K)/\phi(E(K)) \simeq S^{\phi}(E/K)$. So now we want to be able to take some $\xi \in S^{\phi}(E/K)$, obtain a homogeneous space C_{ξ}, and then somehow go back to $E'(K)/\phi(E(K))$. This turns out to be very easy.

Proposition 2.14. *Let $\phi : E \to E'$ be a K-isogeny, let ξ be a cocycle representing an element of $H^1(Gal(\overline{K}/K), E[\phi])$, and let C_ξ be the corresponding homogeneous space. Choose an $\overline{K}$-isomorphism $\theta : C_\xi \to E$ satisfying*

$$\theta^\sigma \circ \theta^{-1} = (\textit{translation by } \xi_\sigma). \tag{2.29}$$

Then,

i. $\phi \circ \theta$ is defined over K.
ii. Suppose there is a point $P \in C(K)$. Then the point $\phi \circ \theta(P) \in E'(K)$ maps to ξ via the connecting homomorphism δ as in 2.19.

As promised, we now move on to the presentation of 2-descent. We omit calculations in order to focus mainly on the material.

2.3. **2-Descent.** Recall our setup in this case. We have a K-rational 2-torsion point on E at the origin, and so we write $E; y^2 = x^3 + ax^2 + bx$. Denote the origin by T. Now, define $E' : Y^2 = X^3 - 2aX^2 + (a^2 - 4b)X$ and the isogeny $\phi : E \to E'$ given by $(x, y) \mapsto \left(\frac{y^2}{x^2}, \frac{y(b-x^2)}{x^2}\right)$. One can easily verify it has kernel $\{O, T\}$. Let S be the set of infinite places, places where E has bad reduction, and places that divide 2. If we identify $E[\phi]$ with μ_2, we reach the following isomorphism $H^1(\mathrm{Gal}(\overline{K}/K), E[\phi]; S) \simeq K(S, 2)$

Remark. *This uses the isomorphism $(K^*)/(K^*)^2 \simeq H^1(Gal(\overline{K}/K, \mu_2)$. Let $a \in K(S, 2)$. Then, choosing $\alpha \in \overline{K}$ such that $\alpha^2 = a$, $K(\alpha)/K$ is unramified outside S. Next, the inertia group I_v has the largest unramified extension of K as its fixed field. So, restricting the map $Gal(\overline{K}/K) \to \mu_2$ to $I_v \to \mu_2$ would produce a constant mapping to the identity of μ_2. In particular, it is unramified outside S. So, we have the demonstrated the desired isomorphism.*

Tracing through this identification, we reach the cocycle presented in the calculation following Theorem 2.9. Denote the homogeneous space that arises from this calculation by C_d for $d \in K(S, 2)$. So, we may compute the Selmer group $S^\phi(E/K)$ by computing $C_d(K_v)$ for each of the finitely many $d \in K(S, 2)$ and $v \in S$.

Recall the isomorphism θ presented in the aforementioned calculation. It turns out that $\phi \circ \theta$ is a K-isomorphism as described in Proposition 2.14. The connecting homomorphism may be computed explicitly: $\delta(O) = 1$, $\delta(T) = a^2 - 4b$, and $\delta(X, Y) = X$ otherwise. All of this may be summarized in the next Theorem.

Theorem 2.15 (**Descent via 2-Isogeny**). *Let E/K and E'/K be two elliptic curves given by the equations*

$$E : y^2 = x^3 + ax^2 + bx, E' : Y^2 = X^2 - 2aX^2 + (a^2 - 4b)X \tag{2.30}$$

and let

$$\phi : E \to E', \phi(x, y) = \left(\frac{y^2}{x^2}, \frac{y(b - x^2)}{x^2}\right) \tag{2.31}$$

be the isogeny with kernel $\{O, T\}$. Let C_d/K be the homogeneous space given by

$$C_d : dw^2 = d^2 - 2adz^2 + (a^2 - 4b)z^4. \tag{2.32}$$

Then there is an exact sequence

$$0 \longrightarrow E'(K)/\phi(E(K)) \xrightarrow{\delta} K(S, 2) \longrightarrow WC(E/K)[\phi] \tag{2.33}$$

where for $d \in K(S,2)$, we have that $d \mapsto \{C_d/K\}$. Let $\theta : C_d \to E$ be the isomorphism presented in the calculations following Theorem 2.9. Then, the map $\phi \circ \theta$ has the property that if $P \in C_d(K)$, then $\delta \circ \phi \circ \theta(P) = d \pmod{(K^*)^2}$.

Finally,

$$S^{\phi}(E/K) \simeq \{d \in K(S,2) : C_d(K_v) \neq \text{ for all } v \in S\}. \tag{2.34}$$

References

[Del07] Christophe Delaunay, *Heuristics on class groups and on tate-shafarevich groups: the magic of the cohen-lenstra heuristics*, Ranks of elliptic curves and random matrix theory **341** (2007), 323–340.

[Mil08] James S Milne, *Algebraic number theory*, JS Milne, 2008.

[Ser13] Jean-Pierre Serre, *Local fields*, vol. 67, Springer Science & Business Media, 2013.

[Sil09] Joseph H Silverman, *The arithmetic of elliptic curves*, vol. 106, Springer Science & Business Media, 2009.

Email address: asz2115@columbia.edu