0.1 Introduction

For a given elliptic curve $E/K$ where $K$ is a number field and $m \geq 2$ an integer, we first present the $m$-Selmer group of $E/K$ corresponding to the multiplication by $m$ isogeny. Then, we give a more general definition of the Selmer group of $E/K$ and its $p$-primary subgroups.

0.2 The $m$-Selmer group of $E/K : S^{(m)}(E/K)$

Let $K$ be a number field and $E/K$ an elliptic curve. We propose to follow the proof of the weak Mordell-Weil theorem for $E/K$ to motivate and give the definition of $S^{(m)}(E/K)$.

Theorem 0.2.1. Weak Mordell-Weil Theorem

$$E(K)/mE(K)$$

is a finite group

Remark 0.2.1. It will be enough to assume $E[m] \subset E(K)$ in what follows using the following lemma:

Lemma 0.2.1. Let $L/K$ be a finite Galois extension. If $E(L)/mE(L)$ is finite, then $E(K)/mE(K)$ is also finite.

proof : cf The Arithmetic of Elliptic Curves, VIII,1.1.1

Let $G_K = Gal(\bar{K}/K)$ and consider the short exact sequence of $G_K$-modules induced by the multiplication by $m$ map :

$$0 \longrightarrow E(\bar{K})[m] \longrightarrow E(\bar{K}) \xrightarrow{m} E(\bar{K}) \longrightarrow 0.$$
taking Galois cohomology yields:

\[
0 \longrightarrow E(K)[m] \longrightarrow E(K) \xrightarrow{m} E(K) \xleftarrow{\delta} H^1(G, E(K)[m]) \longrightarrow H^1(G, E(K)) \xrightarrow{\phi} H^1(G, E(K))[m] \longrightarrow 0.
\]

from which we can extract the Kummer sequence for \(E/K\):

\[
0 \longrightarrow E(K)/mE(K) \xrightarrow{\delta} H^1(G_K, E(K)[m]) \xrightarrow{\phi} H^1(G_K, E(K))[m] \longrightarrow 0.
\]

where the connecting homomorphism \(\delta\) is induced by the following pairing:

**Definition 0.2.1. Kummer Pairing**

\[
k : E(K) \times G_K \rightarrow E[m]
\]

\[
(P, \sigma) \mapsto Q^\sigma - Q
\]

where \(Q \in E(\bar{K})\) s.t. \(mQ = P\).

**Proposition 0.2.1.**

1. The Kummer pairing is well defined

2. The Kummer pairing is bilinear

3. The left kernel of \(k\) is \(mE(K)\)
4. The right kernel of \( k \) is \( G_{K/L} \) where

\[
L = K([m]^{-1}E(K))
\]

is the compositum of all fields \( K(Q) \) as \( Q \) ranges over points of \( E(\bar{K}) \) satisfying \([m]Q \in E(K)\).

proof: \( k \) is well defined by Remark 0.2.1. The rest of the proof is given in The Arithmetic of Elliptic Curves, VIII.1.

Using previous proposition, we obtain a perfect bilinear pairing

\[
E(K)/mE(K) \times G_{L/K} \to E[m]
\]

which reduces the problem to proving that \( G_{L/K} \) is finite.

This last step can be achieved by showing that \( L/K \) is unramified outside of

\[
S = \{v \in M^0_K | E \text{ has bad reduction at } v\} \cup \{v \in M^0_K | v(m) \neq 0\} \cup M^\infty_K
\]

In term of Galois cohomology, this translates into the following statement:

\( \text{Im}(E(K)) \subset H^1(G_K, E[m]) \) consists of cohomology classes that are unramified outside of \( S \).

One completes the proof by showing that extensions such as \( L/K \) above are necessarily finite (see The Arithmetic of Elliptic Curves, VIII, Prop 1.6).

We stop here our study of the weak Mordell-Weill theorem and concentrate on locating \( E(K)/mE(K) \) in \( H^1(G_K, E[m]) \).

Since we assumed \( E[m] \subset E(K) \), we have that \( E(K)/mE(K) \subset H^1(G_K, E[m]) = \text{Hom}(G_K, E[m]) \). It remains to identify elements of \( \text{Hom}(G_K, E[m]) \) that are coming from \( E(K)/mE(K) \).
Remark 0.2.2. $H^1(G_K, E(\overline{K}))$ is isomorphic to the Weil-Châtelet group of $E/K : WC(E/K)$. Therefore, identifying elements in $\ker(\phi)$ is the same as deciding whether or not a given homogenous space $C/K$ for $E/K$ has a $K$-rational point.

As this can be done easily locally using Hensel’s lemma, we will reformulate the Kummer sequence from a local point of view:

For $v \in M_K$, fix an extension of $v$ in $\overline{K}$ which fixes an embedding $\overline{K} \subset \overline{K}_v$ and a decomposition group $G_v \subset G_K$.

$G_v$ acts on $E(K_v)$, hence we obtain:

\[
0 \longrightarrow E(K_v)/mE(K_v) \longrightarrow H^1(G_v, E[m]) \longrightarrow H^1(G_v, E(\overline{K}_v))[m] \longrightarrow 0.
\]

Gathering all places of $K$ gives the following commutative diagram:

\[
\begin{array}{cccccc}
0 & \longrightarrow & E(K)/mE(K) & \xrightarrow{k} & H^1(G_K, E(\overline{K})[m]) & \longrightarrow & H^1(G_K, E(\overline{K}))[m] & \longrightarrow & 0 \\
\text{res}_v \downarrow & & \downarrow \text{res}_v & & \downarrow \text{res}_v & & \downarrow \text{res}_v & & \\
0 & \longrightarrow & E(K_v)/mE(K_v) \longrightarrow \prod_{v \in M_K} H^1(G_v, E(\overline{K})[m]) & \longrightarrow & \prod_{v \in M_K} H^1(G_v, E(\overline{K}))[m] & \longrightarrow & 0
\end{array}
\]

where $\text{res}_v$ denotes the restriction homomorphism relative to the inclusion $G_v \subset G_K$.

We finally define the $m$-Selmer group from the above diagram:

**Definition 0.2.2.** The $m$-Selmer group of $E/K$, denoted $S^{(m)}(E/K)$, is the subgroup of $H^1(G_K, E[m])$ defined by:

\[
S^{(m)}(E/K) := \ker \{ H^1(G_K, E[m]) \to \prod_{v \in M_K} H^1(G_v, E(\overline{K})) \}
\]

**Definition 0.2.3.** The Shafarevich-Tate group of $E/K$, denoted $\Sha(E/K)$, is defined as:

\[
\Sha(E/K) := \ker \{ H^1(G_K, E(\overline{K})) \to \prod_{v \in M_K} H^1(G_v, E(\overline{K})) \}
\]
To sum up, we have the following exact sequence:

$$0 \rightarrow E(K)/mE(K) \rightarrow S^{(m)}(E/K) \rightarrow \text{III}(E/K)[m] \rightarrow 0$$

### 0.3 The Selmer group of $E/K$

We now generalize the definitions above by considering the torsion subgroup of $E(\overline{Q})$ and its $p$-primary subgroups.

Fix an embedding of $K \subset \overline{Q}$ and consider $E[p^\infty] \subset E_{\text{tors}} \subset E(\overline{Q})$ where $E[p^\infty]$ is the $p$-primary subgroup of $E_{\text{tors}}$ i.e. the union of all $E[p^n]$.

Consider $G_K = Gal(\overline{Q}/K)$. Its action on $E_{\text{tors}}$ allows us to define the Kummer map:

$$k : E(K) \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z}) \rightarrow H^1(G_K, E_{\text{tors}})$$

$$P \otimes \left( \frac{1}{n} + \mathbb{Z} \right) \mapsto [\zeta]$$

where $[\zeta] : \sigma \mapsto Q^\sigma - Q$, with $Q \in E(\overline{K})$ and $nQ = P$.

Moreover, for $v$ a prime of $K$, we similarly define the $v$-adic Kummer map:

$$k : E(K_v) \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z}) \rightarrow H^1(G_v, E_{\text{tors}})$$

where $K_v$ denotes the completion of $K$ at $v$.

On the cohomology side, by embedding $\overline{Q} \subset \overline{K_v}$, we obtain a restriction map

$$H^1(G_K, E_{\text{tors}}) \rightarrow H^1(G_v, E_{\text{tors}})$$

which exists for all $v \in M_K$.

We can now define the Selmer group of $E/K$:

**Definition 0.3.1.** Selmer Group $Sel_E(K)$
\[ \text{Sel}_E(K) := \ker \{ H^1(G_K, E_{\text{tors}}) \to \prod_{v \in M_K} H^1(G_v, E_{\text{tors}})/\text{Im}(k_v) \} \]

**Definition 0.3.2.** Shafarevich-Tate Group \( \Sha_E(K) \)

\[ \Sha_E(K) := \text{Sel}_E(K)/\text{im}(k) \]

In order to study \( \text{Sel}_E(K) \), one breaks it down into its \( p \)-primary subgroups:

Let \( p \) be a prime, following the construction above, we define the Kummer map at \( p \):

\[ k_{v,p} : E(K_v) \otimes_{\mathbb{Z}} (\mathbb{Q}_p/\mathbb{Z}_p) \to H^1(G_v, E[p^\infty]) \]

which yields the definition of the \( p \)-primary subgroup of \( \text{Sel}_E(K) \):

**Definition 0.3.3.** The \( p \)-primary subgroup \( \text{Sel}_E(K)p \) is given by:

\[ \text{Sel}_E(K)p := \ker \{ H^1(G_K, E[p^\infty]) \to \prod_{v \in M_K} H^1(G_v, E[p^\infty])/\text{Im}(k_{v,p}) \} \]

We can now distinguish two cases:

1. \( v \) is archimedean or \( v \) is non archimedean and the residue field of \( K \) at \( v \) has characteristic \( l \neq p \):

   In this case, \( \text{Im}(k_{v,p}) = 0 \)

2. \( v \) is non archimedean and the residue field of \( K \) at \( v \) has characteristic \( l = p \):

   In this case, referring to Chris’ talk on \( p \)-adic Hodge Theory, recall that

   \[ H^1_f(G_v, V_p E) = \ker \{ H^1(G_v, V_p E) \to H^1(K_v, V_p E \otimes B_{\text{crys}}) \} \]

   Now using \( V_p E/T_p E \simeq E[p^\infty] \), we have that \( \text{Im}(k_{v,p}) = \text{Im}(H^1_f(G_v, V_p E)) \subset H^1(G_v, E[p^\infty]) \)