Selmer Groups and Kummer Theory for Elliptic Curves

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 :

$$
\begin{tikzcd}
0 \arrow[r] & E(K)[m] \arrow[r] & E(K) \arrow[r, "m"] & E(K) \arrow[dll] \\
& H^1(G, E(\bar{K})[m]) \arrow[r] & H^1(G, E(\bar{K})) \arrow[r, "m"] & H^1(G, E(\bar{K})),
\end{tikzcd}
$$

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

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

where the connecting homomorphism δ is induced by the following pairing :

Definition 0.2.1. *Kummer Pairing*

$$
\begin{aligned}
k : & E(K) \times G_K \to E[m] \\
& (P, \sigma) \mapsto Q^\sigma - Q
\end{aligned}
$$

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 $G_{\bar{K}/L}$ where

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

is the composium 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

$$S = \{v \in M_K^0 | E \textit{ has bad reduction at } v\} \cup \{v \in M_K^0 | v(m) \neq 0\} \cup M_K^\infty$$

In term of Galois cohomology, this translates into the following statement :
$Im(E(K)) \subset H^1(G_K, E[m])$ consists of cohomology classes that are unramified outside of S.
One completes the proof by showing that extensions such as L/K above are necessarly 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 $E(K)/mE(K) \subset H^1(G_K, E[m]) = Hom(G_K, E[m])$. It remains to identify elements of $Hom(G_K, E[m])$ that are coming from $E(K)/mE(K)$.

Remark 0.2.2. *$H^1(G_K, E(\bar{K}))$ is isomorphic to the Weil-Chatelet group of E/K : $WC(E/K)$. Therefore, identifying elements in $ker(\phi)$ is the same as deciding wether 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 $\bar{K}$ which fixes an embedding $\bar{K} \subset \bar{K}_v$ and a decomposition group $G_v \subset G_K$.
G_v acts on $E(K_v)$, hence we obtain :

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

Gathering all places of K gives the following commutative diagram :

$$\begin{tikzcd}
0 \arrow[r] & E(K)/mE(K) \arrow[r, "k"] \arrow[d, "res_v"] & H^1(G_K, E(\bar{K})[m]) \arrow[r] \arrow[d, "res_v"] & H^1(G_K, E(\bar{K}))[m] \arrow[r] \arrow[d, "res_v"] & 0 \\
0 \arrow[r] & E(K_v)/mE(K_v) \arrow[r] & \prod_{v \in M_K} H^1(G_v, E(\bar{K})[m]) \arrow[r] & \prod_{v \in M_K} H^1(G_v, E(\bar{K}))[m] \arrow[r] & 0
\end{tikzcd}$$

where 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 :*

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

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

$$Ш(E/K) := ker\{H^1(G_K, E(\bar{K})) \to \prod_{v \in M_K} H^1(G_v, E(\bar{K}))\}$$

To sum up, we have the following exact sequence :

$$0 \longrightarrow E(K)/mE(K) \longrightarrow S^{(m)}(E/K) \longrightarrow Ш(E/K)[m] \longrightarrow 0$$

0.3 The Selmer group of E/K

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

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

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

$$\begin{aligned} k :& E(K) \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z}) \to H^1(G_K, E_{tors}) \\ & P \otimes (\frac{1}{n} + \mathbb{Z}) \mapsto [\zeta] \end{aligned}$$

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

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

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

where K_v denotes the completion of K at v.

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

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

which exists for all $v \in M_K$.

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

Definition 0.3.1. *Selmer Group* $Sel_E(K)$

$$Sel_E(K) := ker\{H^1(G_K, E_{tors}) \to \prod_{v \in M_K} H^1(G_v, E_{tors})/Im(k_v)\}$$

Definition 0.3.2. *Shafarevich-Tate Group* $Ш_E(K)$

$$Ш_E(K) := Sel_E(K)/im(k)$$

In order to study $Sel_E(K)$, 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 $Sel_E(K)$:

Definition 0.3.3. *The p-primary subgroup* $Sel_E(K)p$ *is given by :*

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

We can now distinguish two cases :

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

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

2. v is non archimedian and the residue field of K at v has characteristic $l = p$:

   In this case, referring to $Chris_w$' talk on p-adic Hodge Theory, recall that

   $$H^1_f(G_v, V_pE) = ker\{H^1(G_v, V_pE) \to H^1(K_v, V_pE \otimes B_{crys})\}$$

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