Galois Cohomology (Study Group)

1 Selmer Groups and Kummer Theory for Elliptic Curves (by Céline Maistret)

Let K be a number field, E an elliptic curve over K. In order to prove the Mordell - Weil Theorem, one breaks it in to parts, proving $E(K)/mE(K)$ is finite, and then using descent.

Let $G_{\overline{K}/K} = \mathrm{Gal}(\overline{K}/K)$, then we have $G_{\overline{K}/K}$ acts on $E[m]$, $E(\overline{K})$. Consider the multiplication by m-isogeny, we have a short exact sequence: $0 \to E[m] \to E(\overline{K}) \overset{[m]}{\to} 0$. Taking Galois Cohomology:

$$0 \to E(K)[m] \to E(K) \to E(K) \to H^1(G_{\overline{K}/K}, E(\overline{K})[m]) \to H^1(G_{\overline{K}/K}, E(\overline{K})) \to H^1(G_{\overline{K}/K}, E(\overline{K})) \to \dots$$

We can extract the *Kummer Sequence* for E/K:

$$0 \longrightarrow E(K)/mE(K) \overset{k}{\longrightarrow} H^1(G_{\overline{K}/K}, E(\overline{K})[m]) \overset{\phi}{\longrightarrow} H^1(G_{\overline{K}/K}, E(\overline{K}))[m] \longrightarrow 0\ .$$

The connecting homomorphism is the *Kummer map*: $k : E(K) \to H^1(G_{\overline{K}/K}, E\,(K)\,[m])$ defined by $P \mapsto [\xi] : \sigma \mapsto Q^\sigma - Q$, where $Q \in E(\overline{K})$ such that $mQ = P$.

Properties of k:

1. It is well defined
2. The left kernel is $mE(K)$.

Consider $L = K\left([m]^{-1}\,E(K)\right)$, which is the composium of all $K(Q)$, where $Q \in E(\overline{K})$ with $mQ = P$. Define $S = \left\{\nu \in M_K^0 | E \,\text{has bad reduction at}\, \nu\right\} \cup \left\{\nu \in M_K^0 | \nu(m) \neq 0\right\} \cup M_K^\infty$. We have $\mathrm{im}(E(K)) \subset H^1(G_{\overline{K}/K}, E[m])$ consists of unramified classes of cocycles outside of S. So $\mathrm{im}(k) = \ker(\phi : H^1(G_{\overline{K}/K}, E[m]) \to H^1(G_{\overline{K}/K}, E(\overline{K}))[m])$, so let us analyse $H^1(G_{\overline{K}/K}, E(\overline{K})) \cong \mathrm{WC}(E/K)$.

Local consideration: Let $\nu \in M_K$, fix an extension of ν in $\overline{K}$, we get an embedding of $\overline{K} \subset \overline{K}_\nu$, and a decomposition group $G_\nu \subset G_{\overline{K}/K}$. G_ν acts on $E(\overline{K}_\nu)$.

$$0 \longrightarrow E(K_\nu)/mE(K_\nu) \longrightarrow H^1(G_\nu, E[m]) \longrightarrow H^1(G_\nu, E(K_\nu))[m] \longrightarrow 0$$

We get the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K)/mE(K) & \overset{k}{\longrightarrow} & H^1(G_{\overline{K}/K}, E[m]) & \overset{\phi}{\longrightarrow} & H^1(G_{\overline{K}/K}, E(\overline{K}))[m] & \longrightarrow & 0 \\ & & & & & & \downarrow{\scriptstyle \mathrm{res}} & & \\ 0 & \longrightarrow & \prod_\nu E(K_\nu)/mE(K_\nu) & \longrightarrow & \prod_\nu H^1(G_\nu, E[m])) & \longrightarrow & \prod_\nu H^1(G_\nu, E(K_\nu))[m] & \longrightarrow & 0 \end{array}$$

Definition 1.1. The *m-Selmer group* is the subgroup of $H^1(G_{\overline{K}/K}, E(\overline{K})[m])$ given by:

$$S^{(m)}(E/K) = \ker \left\{ H^1(G_{\overline{K}/K}, E[m]) \to \prod_{\nu} H^1(G_\nu, E(\overline{K_\nu})[m] \right\}.$$

The *Tate - Shaferevich group*, Ш(E/K) is defined as $\ker \left\{ H^1(G_{\overline{K}/K}, E(\overline{K})) \to \prod_\nu H^1(G_\nu, E(\overline{K_\nu})) \right\}$.

So we get the commutative diagram:

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

More general construction: Embed $\overline{\mathbb{Q}} \subset \overline{K_\nu}$, get an embedding of $\overline{K} \subset \overline{K_\nu}$, consider $E[p^\infty] \subset E_{\text{tor}} \subset E(\overline{\mathbb{Q}})$.

Definition 1.2. $E[p^\infty]$ is the p-primary subgroup of E_{tor}, i.e., union of $E[p^n]$.

We get a new (more general) Kummer map: $k : E(K) \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z}) \to H^1(G_K, E_{\text{tor}})$ defined by $P \otimes \left(\frac{1}{n} + \mathbb{Z}\right) \mapsto [\xi] : \sigma \mapsto Q^\sigma - Q$, where $Q \in E(\overline{K})$ such that $nQ = P$.

We have a restriction map: $\text{Res} : H^1(G_K, E_{\text{tor}}) \to H^1(G_\nu, E_{\text{tor}})$.

Definition 1.3. $\text{Sel}_E(K) := \ker \left\{ H^1(G_K, E_{\text{tor}}) \to \prod_\nu H^1(G_\nu, E_{\text{tor}}) / \operatorname{im} k_\nu \right\}$.
Ш$_E(K) := \text{Sel}(K) / \operatorname{im} k$.

To study $\text{Sel}_E(K)$, one breaks it down into its p-primary subgroups $\text{Sel}_E(K)_p$, where p is a fixed prime. We define $k_{\nu,p} : E(K_\nu) \otimes_{\mathbb{Z}} (\mathbb{Q}_p/\mathbb{Z}_p) \to H^1(G_K, E[p^\infty])$.

$\text{Sel}_E(K)_p := \ker \left\{ H^1(G_K, E[p^\infty] \to \prod_\nu H^1(G_\nu, E[p^\infty] / \operatorname{im} k_{\nu,p} \right\}$.

Two cases could happen:

1. $\nu \in M_K^0$ with residue field of K at ν of characteristic $l \neq p$. This case can be generalised to $\nu \in M_K^\infty$. In this case $\operatorname{im} k_{\nu,p} = 0$.

2. $\nu \in M_K^0$, with residue field of K at ν of characteristic $l = p$. In this case we use Hodge theory:

   Recall: $H^1_f(G_\nu, V_pE) = \ker \left\{ H^1(G_\nu, V_pE) \to G^1(G_\nu, V_pE \otimes \mathbb{B}_{\text{crys}}) \right\}$. Now $V_pE/T_pE \cong E\,[p^\infty]$. Then $\operatorname{im} k_{\nu,p} = \operatorname{im}(H^1_f(G_\nu, V_pE) \to H^1(G_\nu, E[p^\infty])$.