Selmer groups are finite

Xiaomin Chu

Nov 2023

Setup K a number field, E an ellipic curve over K. Fix an algebraic closure $\overline{K}$ of K, and algebraic extensions of K means a subfield of $\overline{K}$. $\operatorname{Specm}\mathcal{O}_K$ denotes the set of finite places of K. For each $v \in \operatorname{Specm}\mathcal{O}_K$, choose a place $\overline{v} \in \operatorname{Specm}\mathcal{O}_{\overline{K}}$ extending v, and identify the absolute Galois group of K_v with the decomposition group of $\overline{v}/v$. Fix $n \geq 2$ a positive integer.

Recall that in order to prove the weak Mordell-Weil conjecture, we intruduced the Selmer groups

$$\mathrm{Sel}^{(n)}(E) = \ker H^1(K, E[n]) \to \prod_{v \in \operatorname{Specm}\mathcal{O}_K} H^1(K_v, E(\overline{K_v}))$$

and wished that it's finite.

1 For $\mathbb{G}_m$

We start with something much simpler than an elliptic curve, i.e. $\mathbb{G}_m$. Note that $\mathbb{G}_m(K) = K^\times$ is of course not finitely generated.

Consider the short exact sequence

$$0 \to \mu_n \to \overline{K}^\times \xrightarrow{n} \overline{K}^\times \to 0$$

We may extract the following exact sequence from the cohomological long exact sequence

$$0 \to K^\times/(K^\times)^n \to H^1(K, \mu_n) \to H^1(K, \overline{K}^\times))[n] \to 0$$

But Hilbert 90 says that $H^1(K, \overline{K}^\times) = 0$, so actually $K^\times/(K^\times)^n = H^1(K, \mu_n)$.

$K^\times/(K^\times)^n$ is approximately $\bigoplus_{v \in \operatorname{Specm}\mathcal{O}_K} \mathbb{Z}v$. To make it precise, we use the celebrated exact sequence in algebraic number theory

$$0 \to \mathcal{O}_K^\times \to K^\times \to \bigoplus_{v \in \operatorname{Specm}\mathcal{O}_K} \mathbb{Z}v \to \mathrm{Cl}(K) \to 0$$

where $\mathrm{Cl}(K)$, the ideal class group of K, is finite. Applying the snake lemma to

$$\begin{array}{ccccccc} & & K^\times & \longrightarrow & \bigoplus_{v\in \mathrm{Specm}\,\mathcal{O}_K} \mathbb{Z}v & \longrightarrow & \mathrm{Cl}(K) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle n} & & \downarrow{\scriptstyle n} & & \downarrow{\scriptstyle n} & & \\ 0 & \longrightarrow & K^\times/\mathcal{O}_K^\times & \longrightarrow & \bigoplus_{v\in \mathrm{Specm}\,\mathcal{O}_K} \mathbb{Z}v & \longrightarrow & \mathrm{Cl}(K) & & \end{array}$$

gives us the exact sequence

$$\mathrm{Cl}(K)[n] \to K^\times/(\mathcal{O}_K^\times(K^\times)^n) \to \bigoplus_{v\in \mathrm{Specm}\,\mathcal{O}_K} (\mathbb{Z}/n\mathbb{Z})v \to \mathrm{Cl}(K)/n\mathrm{Cl}(K)$$

But Dirichlet's unit theorem says that $\mathcal{O}_K^\times$ is a finitely generated abelian group, so $K^\times/(K^\times)^n$ isn't much different from $K^\times/(\mathcal{O}_K^\times(K^\times)^n)$. To be more precise, we have the following exact sequence

$$0 \to \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^n \to K^\times/(K^\times)^n \to K^\times/(\mathcal{O}_K^\times(K^\times)^n) \to 0$$

To summurize the discussion above, we have

Theorem 1. *There are two finite groups $R_1(K,n), R_2(K,n)$ such that*

$$R_1(K,n) \to K^\times/(K^\times)^n \to \bigoplus_{v\in \mathrm{Specm}\,\mathcal{O}_K} (\mathbb{Z}/n\mathbb{Z})v \to R_2(K,n)$$

is exact.

In particular,

Corollary 2. *If S is a subgroup of $K^\times/(K^\times)^n$ whose image in $\bigoplus_{v\in \mathrm{Specm}\,\mathcal{O}_K} (\mathbb{Z}/n\mathbb{Z})v$ is finite, then S is finite.*

Proof. S is an extension of its image in $\bigoplus_{v\in \mathrm{Specm}\,\mathcal{O}_K} (\mathbb{Z}/n\mathbb{Z})v$ and a subgroup of $R_1(K,n)$. □

2 Reducing to $E[n] \subset E(K)$

In general E is very different from $\mathbb{G}_m \times \mathbb{G}_m$. But we can compare their H^1 somehow forcefully. Suppose that $E[n] \subset E(K)$, then G_K acts trivially on $E[n]$. Then $H^1(K, E[n]) \cong \mathrm{Hom}(G_K, \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})$ by choosing a basis (a, b) of $E[n]$. In this case, Weil pairing implies that $\mu_n \subset K^\times$. So we have

$$H^1(K, E[n]) \cong \mathrm{Hom}(G_K, \mathbb{Z}/n\mathbb{Z}) \times \mathrm{Hom}(G_K, \mathbb{Z}/n\mathbb{Z}) \cong H^1(K, \mu_n) \times H^1(K, \mu_n)$$

Which then equals $K^\times/(K^\times)^n \times K^\times/(K^\times)^n$. This is very nice.

Now we reduce to this situation.

Proposition 3. *Suppose L/K is a finite Galois extension. If $\mathrm{Sel}^n(E/L)$ is finite, then $\mathrm{Sel}^n(E/K)$ is also finite.*

Proof. We have the inflation-restriction exact sequence

$$0 \to H^1(G_{L/K}, E[n](L)) \xrightarrow{\text{Inf}} H^1(K, E[n]) \xrightarrow{\text{Res}} H^1(L, E[n])$$

and $H^1(G_{L/K}, E[n](L))$ is clearly finite. So $\text{res} : \text{Sel}^n(E/K) \to \text{Sel}^n(E/L)^{G_{L/K}}$ has finite kernel. □

So if we can prove that $\text{Sel}^n(E/K(E[n]))$ is finite, then we have $\text{Sel}^n(E/K)$ is finite. From now on we assume that $E[n] \subset E(K)$.

Remark 4. *If you don't like Weil pairing, you can take $\mu_n \subset K^\times$ as an additional assumption that doesn't hurt.*

3 Proof