Part 1. Around Selmer

For a very short and neat intro to Selmer groups of abelian varieties in classical vocabulary, see Karl Rubin’s Introduction to Selmer Groups https://www.math.uci.edu/~krubin/lectures/msri1.pdf

1. The basic mapping

To begin simply, consider $\Gamma = \Gamma_K$ an (étale) finite group scheme over a local or global number field $K$. In effect, this is just a finite group (but not necessarily abelian) together with an action of $G_K$. And now, working over $K$, consider a finite flat étale cover of a connected curve $Y \to X$ with ‘Galois group’ $\Gamma$—i.e., there is a principal action of the group scheme $\Gamma$ on $Y$ with quotient scheme $X$. If $x \in X(K)$, the fiber $Y_x$ is then a $K$-torsor for $\Gamma$, and so gives us a class—in the usual way—in the pointed set $H^1(G_K; \Gamma)$.

This gives us a natural (and fundamental) mapping:

$$(1.1) \quad X(K) \xrightarrow{\alpha_{X/Y,\Gamma}} H^1(G_K; \Gamma).$$

defined by the rule: $x \mapsto \alpha(x) :=$ the class in $H^1(G_K; \Gamma)$ that represents the $\Gamma$-torsor $Y_x$.

\textit{1} For that matter, one could work with more general connected schemes

\textit{2} If $T$ is a $K$-torsor for $\Gamma$, let $t \in T(\bar{K})$ be a $\bar{K}$-valued point of $T$, and the class ‘classifying’ the $K$-torsor $T$ is represented y the 1-cocycle $[g \mapsto \gamma_g]$ where $\gamma_g \in \Gamma(\bar{K})$ is the unique element such that $\gamma_g \cdot t = g(t)$. Here, the ‘dot’ in the LHS indicates the natural action of $\Gamma$ on $T$ and the parenthesis in the RHS indicates the action of Galois.
Moreover, we may take \( Y \to X \) to be \( \text{pro-finite} \) \( \text{étale} \)—and, correspondingly, we may take \( \Gamma \) too to be \( \text{pro-finite} \)—and get the same mapping \([1.1]\).

- This mapping \([1.1]\) is the basis for the \textit{Kummer map} when \( X \) is a connected abelian group scheme (e.g., an abelian variety) taking \( Y \to X \) to be

\[
X \xrightarrow{N} X,
\]

i.e., multiplication by a positive integer \( N \) so that \( \Gamma := X[N] \) and (since \([1.2]\) is a faithfully flat morphism) we have the short exact sequence

\[
0 \to X[N] \to X \xrightarrow{N} X \to 0.
\]

The mapping \([1.1]\) is the classical Kummer map; i.e., the (first) coboundary homomorphism attached to \([1.3]^{3}\).

- It is also the basis of the natural mapping in the anabelian context related to the \( K \)-scheme \( X \) (where \( \Gamma \) is some chosen quotient of the \( \text{étale} \) pro-finite fundamental group (scheme) of \( X \)). For this, let the \( K \)-scheme \( X \) be given with a \( K \)-rational base point \( x_o = \text{Spec}(K) \) in \( X \).

Let

- \( \bar{K}/K \) be an algebraic closure,
- \( \bar{X} := X \times_{\text{Spec}(K)} \text{Spec}(\bar{K}) \),
- \( \bar{x}_o = \text{Spec}(\bar{K}) \) which we view as a ‘geometric point’ of both \( X \) and \( x_o \) leading to the exact sequence (and diagram):

\[
1 \longrightarrow \pi_1(\bar{X}, \bar{x}_o)^{\text{geom}} \longrightarrow \pi_1(X, \bar{x}_o) \longrightarrow \text{Gal}(\bar{K}/K) \longrightarrow 0
\]

\[
\pi_1(x_0, \bar{x}_o) \approx
\]

\[\text{(1.5)}\]

\[\text{This is a straightforward exercise: consider the long exact sequence attached to the short exact sequence } [1.3] \]

\[\text{(1.4)}\]

\[\ldots \longrightarrow X(K) \xrightarrow{N} X(K) \longrightarrow H^1(\text{Gal}(K); \Gamma) \longrightarrow \ldots\]

For a \( K \)-rational \( x \) in \( X(K) \) find \( y \in X(\bar{K}) \) such that \( N \cdot y = x \). The coboundary \( \partial x \) is just given by the class represented by the cocycle \([g \mapsto g(y) - y]\) which also classifies the fiber of \( x \) (with respect to the morphism \([1.2]\)) when viewed as \( X[N]\)-torsor.
The basic features of Galois Theory hold here: any connected finite (or profinite) étale cover of $X$ is given (is ‘classified’), up to isomorphism, by a closed subgroup of $\pi_1(X, \bar{x}_o)$, and the converse is also true.

Examples:

- Let $Y \rightarrow X$ be the profinite étale cover of $X$ ‘classified’ by the image of $\pi_1(x_0, \bar{x}_o)$ in $\pi_1(X, \bar{x}_o)$ under the upper left morphism of diagram 1.5. Alternatively, $Y \rightarrow X$ can be viewed as the maximal (connected) profinite étale cover that has a $K$-rational point mapping to $x_0$. This cover $Y/X$ is not Galois, but its base change $\bar{Y}/\bar{X}$ is Galois with Galois group equal to $\pi_1(\bar{X}, \bar{x}_o)^{\text{geom}}$.

So $\Gamma := \pi_1(\bar{X}, \bar{x}_o)^{\text{geom}}$ is an étale pro-finite group with its natural $G_K$-action. We can view this $\Gamma$ as a profinite group scheme over $K$ that admits a $K$-action on $Y$ such that the quotient is $X$. The corresponding mapping 1.1 is the natural map that plays a principal role in the anabelian theory.

- Taking $\Gamma$ to be the pro-unipotent, the pro-$p$-unipotent, or the abelian, or pro-$p$ abelian quotient of the previous bullet, we get corresponding examples of 1.1.

- More specifically, Put $U^{(0)} := \pi_1(X, x_o)$, and consider, inductively, the lower central series $U^{(n+1)} := [U^{(0)}, U^{(n)}]$, and the corresponding quotients,

$$U(n) := \pi_1(X, x_o)/U^{(n)}.$$

Now take, as our $\Gamma$, $\Gamma := U(n)$ for some positive integer $n$. For $n = 1$, we have that

$$U(1) = \pi_1(\bar{X}, \bar{x}_o)^{\text{ab}} = H_1(\bar{X}, \hat{\mathbb{Z}})$$

and we are in the abelian situation, so the mapping 1.1 is closely related to the Kummer mapping composed with the natural mapping of $X$ to its Albanese variety. Taking $n = 2$ we find ourselves in the context of Chabauty-Coleman-Kim, as we shall see.
More to the point, one can fix some prime \( p \) and work with \( U_p^{[0]} := \text{the pro-}p\text{-completion of } \pi_1(X, x_0) \). One then defines \( U_p^{[n]} \) and \( U_p(n) \) in the analogous way.

In the literature one finds that people like to go even further, taking the \( \mathbb{Q}_p \)-Malcev extensions of these groups \( U_p(n) \).

2. IMPOSING LOCAL CONDITIONS

The mapping

\[
\begin{align*}
X(K) & \quad \xrightarrow{\alpha} \quad H^1(G_K; \Gamma) \\
\end{align*}
\]

is not necessarily an injection. Nevertheless it may help in our understanding of \( X(K) \) if one could put constraints on its image. The constraints we have in mind are obtained by local considerations and there are, at least, two possible ways of imposing them:

- By considering a priori *local cohomological properties* that the image of \( X(K) \) must have.
- By ‘push-out;’ i.e., by considering the relation between local and global rational points.

Both are reasonable procedures, the former more naturally when \( \Gamma \) is abelian, but we will be discussing the latter here.

Let \( K \) be a global number field, \( v \) a place of \( K \) and \( K_v \) the completion of \( K \) at \( v \).

For \( X/K \), and \( x_0 \in X(K) \) we have the commutative diagram

\[
\begin{array}{ccc}
X(K) & \xrightarrow{\alpha} & X(K_v) \\
\downarrow \alpha & & \downarrow \alpha_v \\
H^1(G_K, \pi_1(X, x_0)^{\text{geom}}) & \xrightarrow{\iota_v} & H^1(G_{K_v}, \pi_1(X, x_0)^{\text{geom}})
\end{array}
\]

where the vertical arrows \( \alpha \) and \( \alpha_v \) are given by (1.1) Taking \( \Gamma \) as one of the groups above, we have the induced diagram

\[
\begin{array}{ccc}
X(K) & \xrightarrow{\iota_v} & X(K_v) \\
\downarrow \alpha & & \downarrow \alpha_v \\
H^1(G_K, \Gamma) & \xrightarrow{\iota_v} & H^1(G_{K_v}, \Gamma)
\end{array}
\]
Definition 1. With \( X_{/K}, x_o, \text{ and } \Gamma \) as above, the \( \Gamma \)-Selmer space of \((X, x_o)\) is the (pro-finite) subset:

\[
\Sigma(X, \Gamma) \subset H^1(G_K, \Gamma)
\]

defined to be:

\[
\Sigma(X, \Gamma) := \bigcap_v \iota_v^{-1} \cdot \alpha_v (X(\mathbb{K}_v)) \subset H^1(G_K, \Gamma),
\]

where the intersection is over all places \( v \) of \( \mathbb{K} \).

Since \( \iota_v^{-1} \cdot \alpha_v (X(\mathbb{K}_v)) \) for any \( v \)---and therefore since \( \Sigma(X, \Gamma) \) also---contains the image of \( X(K) \) in \( H^1(G_K, \Gamma) \), Diagram 2.2 can be shaved down to:

\[
(2.3) \quad X(K) \longrightarrow X(K_v) \quad \downarrow \alpha \quad \Sigma(X, \Gamma) \longrightarrow H^1(G_{K_v}, \Gamma),
\]

for any place \( v \).

3. Further structure on the Selmer space

In the case where our \( \Gamma \) is \( U_p(n) \) for some \( n \) (as above), it is a pro-\( p \) group.

Proposition 3.1. Let \( \Gamma := U_p(n) \) for some \( n \). The profinite space \( H^1(G_{K_v}, \Gamma) \) has the (natural) structure of \( p \)-adic (locally) analytic manifold, and for any place \( v \) dividing \( p \), the mapping \( X(K_v) \to H^1(G_{K_v}, \Gamma) \) is \( p \)-adic (locally) analytic\(^4\).

Proof: ???

---

\(^4\) In practice, our “locally analytic” functions on \( X(K_v) \) will be expressible as power series on each residue disc of \( X(K_v) \).
4. A strategy: Chabauty-Coleman-Kim

Letting, as above, $\Gamma := \mathcal{U}_p(n)$ for some $n$, fixing a place $v$, return to the diagram:

\[
\begin{array}{ccc}
X(K) & \longrightarrow & X(K_v) \\
\downarrow & & \downarrow \alpha \\
\Sigma(X, \Gamma) & \longrightarrow & H^1(G_{K_v}, \Gamma),
\end{array}
\]

Can one find a $p$-adic (locally) analytic function $\phi$ on $H^1(G_{K_v}, \Gamma)$ that has the following two properties?

- The analytic function $\phi$ vanishes on the image of $\Sigma(X, \Gamma)$ in $H^1(G_{K_v}, \Gamma)$.
- The composite function $\Phi := \phi \cdot \alpha$ on $X(K_v)$ is expressible as a nonvanishing power series on every residue disc of $X(K_v)$.

**A simple observation:** If $X$ is a curve, and the answer to the above question is yes, then the set of zeroes in $X(K_v)$ of the function $\Phi$ is finite, and this set contains the set of rational points $X(K)$.

5. The abelian case

Here let $\Gamma := \mathcal{U}[1] = [\mathcal{U}\{0\}, \mathcal{U}\{0\}] = \pi_1(\hat{X}, x_o)^{ab}$ (using the notation introduced in Section 1). So,

$$\Gamma \simeq H_1(\hat{X}; \hat{\mathbb{Z}}).$$

For any prime $p$, we might then pass to the $p$-component:

$$\Gamma_p := \Gamma \otimes_{\hat{\mathbb{Z}}} \mathbb{Z}_p \simeq H_1(\hat{X}; \mathbb{Z}_p)$$

giving us the fundamental mapping:

\[
(5.1) \quad X(K) \rightarrow \Sigma(X, H_1(\hat{X}; \mathbb{Z}_p)) \subset H^1(G_K; H_1(\hat{X}; \mathbb{Z}_p)).
\]

When $X$ is a smooth projective curve, we have a canonical $G_K$-equivariant isomorphism $H_1(\hat{X}; \mathbb{Z}_p) \simeq T_pJ$, where $J$ is the jacobian of $X$ and $T_pJ$ is its corresponding $p$-adic Tate module. We assume that there is a $K$-rational point $x_o$ of $X$ that we use to embed $X$ in $J$ in the usual way: $x \mapsto [x - x_o]$. If $S$ is a finite set of primes of $K$ containing those of bad reduction for $X$ as well as those dividing $p$, let $G_{K,S}$ be the maximal quotient of $G_K$ unramified outside $S$. For a prime $v$ of $K$
(especially a prime dividing $p$), Equation 5.1 can be written as the top line of:

$$
\begin{align*}
X(K) \xrightarrow{\subset} J(K) \xrightarrow{} \Sigma(X, T_p J) \xrightarrow{\subset} H^1(G_{K, S} ; T_p J) \\
X(K_v) \xrightarrow{\subset} J(K_v) \xrightarrow{} H^1(G_{K_v} , T_p J) \\
H^0(J_{K_v} , \Omega^1) \xrightarrow{\text{log}_v} H^0(X_{K_v} , \Omega^1)^* 
\end{align*}
$$

Notes:

(i) Only for simplicity of notation, assume that $v$ divides $p$ and is of degree 1, so that $K_v = \mathbb{Q}_p$.

(ii) So $J(K_v) = J(\mathbb{Q}_p)$ is an abelian $p$-adic analytic group of dimension $g := \text{the genus of } X$ with its tangent space at the origin canonically equal to

$$
H^1(X/K_v, \mathcal{O}_X) \simeq H^0(X_{K_v}, \Omega^1)^* \simeq H^0(J_{K_v}, \Omega^1)^*,
$$

the left isomorphism coming from duality.

(iii) Recall the definition of “log$_v$”:

$$
(5.3) \quad J(K_v) \longrightarrow J(K_v)/\text{torsion} \xrightarrow{\text{log}_v} H^0(X_{K_v}, \Omega^1)^*.
$$

Here, $J(K_v)/\text{torsion}$ is an open $p$-adic analytic subgroup of $H^0(X_{K_v}, \Omega^1)^*$, which is itself a locally compact $p$-adic analytic group of dimension $g$. The mapping 5.3 comes from the mapping:

$$
(5.4) \quad J(K_v) \times H^0(X_{K_v}, \Omega^1) \rightarrow K_v
$$
given by the “integral”

$$
(z, \omega) \mapsto \int_0^z \omega,
$$

for $z \in J(K_v)$ and $\omega \in H^0(X_{K_v}, \Omega^1)$. The scare-quotes around the word “integral” is to remind us that it is defined as a coherent anti-derivative. Also, since the differential $\omega$ is translation invariant on $J$, this is indeed a bilinear (bi-analytic) pairing.

(iv) **Intro to the Chabauty-Coleman Method** Consider:
In the case where \( r < g \) the topological closure of the image of the mapping \( \phi : \mathbb{Z}^r \to \mathbb{Z}_p^g \) is a \( \mathbb{Z}_p \)-submodule of \( \mathbb{Z}_p^g \) of smaller rank, so there is a nontrivial differential \( \eta \in H^0(X_{K_v}, \Omega^1) \) such that the image of \( J(K) \) in \( J(K_v) \) lies in the kernel of the composite mapping:

\[
J(K_v) \to H^0(X_{K_v}, \Omega^1)^* \xrightarrow{\eta} K_v.
\]

Restricting, now to \( X(K_v) \) we have the nontrivial analytic function \( \Phi \) given by \( x \mapsto \Phi(x) := \int_{x_o}^x \eta \) (expressible as a coherent anti-derivative on \( X(K_v) \)) or, equivalently, by the composition

\[
X(K_v) \to J(K_v) \xrightarrow{\log} H^0(X_{K_v}, \Omega^1)^* \xrightarrow{\eta} K_v.
\]

Visibly, the zeroes of \( \Phi \) (are finite in number, and) contain the \( K \)-rational points of \( X \). The advantage of this formulation (due to Coleman) is that it can lead to fairly effective procedures on occasions.