

DESCENT ON ELLIPTIC CURVES

MICHAEL STOLL

ABSTRACT. Let E be an elliptic curve over \mathbb{Q} (or, more generally, a number field). Then on the one hand, we have the finitely generated abelian group $E(\mathbb{Q})$, on the other hand, there is the Shafarevich-Tate group $\text{III}(\mathbb{Q}, E)$. *Descent* is a general method of getting information on both of these objects — ideally complete information on the Mordell-Weil group $E(\mathbb{Q})$, and usually partial information on $\text{III}(\mathbb{Q}, E)$.

What descent does is to compute (for a given $n > 1$) the n -Selmer group $\text{Sel}^{(n)}(\mathbb{Q}, E)$; it sits in an exact sequence

$$0 \longrightarrow E(\mathbb{Q})/nE(\mathbb{Q}) \longrightarrow \text{Sel}^{(n)}(\mathbb{Q}, E) \longrightarrow \text{III}(\mathbb{Q}, E)[n] \longrightarrow 0$$

and thus contains combined information on $E(\mathbb{Q})$ and $\text{III}(\mathbb{Q}, E)$.

The main problem I want to discuss in this “short course” is how to actually do this explicitly, with some emphasis on obtaining representations of the elements of the Selmer group as explicit covering spaces of E . These explicit representations are useful in two respects — they allow a search for rational points (if successful, this proves that the element is in the image of the left hand map above), and they provide the starting point for performing “higher” descents (e.g., extending a p -descent computation to a p^2 -descent computation).

Prerequisites: Basic knowledge of elliptic curves (e.g., Silverman’s book [Si1]), some Galois cohomology and algebraic number theory (e.g., Cassels–Fröhlich [CF]).

This chapter contains the notes (with little changes) I wrote for the “short course” with the same title I gave at the Institut Henri Poincaré in the fall of 2004. The purpose of the course was to give an introduction to the topic and at the same time discuss some (then) recent results. Owing to the introductory nature of the text, we give proofs of most theorems, even though some can be found in the literature. Also, in some cases such a proof may be less elegant, but more elementary, than necessary.

The results described in these notes (if not “classical”, i.e., to be found in, e.g., Silverman’s book [Si1]) were obtained in collaboration with John Cremona, Tom Fisher, Cathy O’Neil, Ed Schaefer and Denis Simon. In some respect, the present text is by now fairly obsolete, since everything that is in it can be found in [ScSt, CFOSS1, CFOSS2] (or will be found in [CFOSS3]). However, we think that these notes may still be of some use, since they give a good overview over the ideas, without going too much into technical details. If you want to know more about these, you are welcome to consult the papers mentioned above.

I would like to particularly advertise Theorems 2.4 and 2.7. While it has been known for a long time that n -Selmer groups of elliptic curves can be computed in principle, these results give a rather precise statement on what is required if one really wants to perform such a computation. As it turns out, this is usually less demanding when n is a prime number, but even so, it is rarely feasible (with current technology regarding the computational theory of algebraic number fields) to perform the computation when $n \geq 5$.

1. THE SELMER GROUP

In the following, K will be a number field, and E will be an elliptic curve defined over K . E is an algebraic group over K , and so its set of rational points, $E(K)$, forms a group, the so-called Mordell-Weil group. By the Mordell-Weil theorem, it is a finitely generated abelian group, and one of the big questions is how to determine it (in the sense of, say, giving generators as points in $E(K)$ and relations). Descent is the main tool used for that, both in theory and in practice. Doing an n -descent on E means to compute the n -Selmer group $\text{Sel}^{(n)}(K, E)$, which we will introduce in this section.

Note that saying that $E(K)$ is a finitely generated abelian group amounts to asserting the existence of an exact sequence

$$0 \longrightarrow E(K)_{\text{tors}} \longrightarrow E(K) \longrightarrow \mathbb{Z}^r \longrightarrow 0$$

with $r \geq 0$ an integer and $E(K)_{\text{tors}}$ a finite abelian group; it consists of all elements of $E(K)$ of finite order. Less canonical, but sometimes more convenient, we also have

$$E(K) \cong E(K)_{\text{tors}} \oplus \mathbb{Z}^r .$$

For any concrete curve E , it is fairly straightforward to find $E(K)_{\text{tors}}$, and we will not be concerned with how to do that in these lectures. The hard part is to determine the rank r . This is where descent helps.

1.1. Definition and first properties.

We first set some (fairly standard) notation. If v is a place of K , we write K_v for the completion of K at v and K_v^{unr} for the maximal unramified extension of K_v . If v is a finite place, then k_v denotes the residue class field of K_v . If k is any field, \bar{k} denotes an algebraic closure of k .

Let $n > 1$ be an integer. The usual definition of the n -Selmer group makes use of Galois cohomology. We follow the usual convention in writing $H^j(k, M)$ for the Galois cohomology group $H^j(\text{Gal}(k), M)$, where k is a field, $\text{Gal}(k)$ is the absolute Galois group of k , and M is a $\text{Gal}(k)$ module (with continuous action; the group cohomology also is defined in terms of continuous cocycles).

Consider the short exact sequences of $G_K = \text{Gal}(\bar{K}/K)$ -modules

$$0 \longrightarrow E[n](\bar{K}) \longrightarrow E(\bar{K}) \xrightarrow{n} E(\bar{K}) \longrightarrow 0$$

(which is usually just written

$$0 \longrightarrow E[n] \longrightarrow E \xrightarrow{n} E \longrightarrow 0).$$

Then we have the long exact sequence of cohomology groups

$$0 \longrightarrow E[n](K) \longrightarrow E(K) \xrightarrow{n} E(K) \xrightarrow{\delta} H^1(K, E[n]) \longrightarrow H^1(K, E) \xrightarrow{n} H^1(K, E).$$

We deduce from it another short exact sequence:

$$0 \longrightarrow E(K)/nE(K) \xrightarrow{\delta} H^1(K, E[n]) \longrightarrow H^1(K, E)[n] \longrightarrow 0$$

It turns out that knowing $E(K)$ is essentially equivalent to knowing its free abelian rank $r = \text{rank } E(K)$. (Once we know r , we can look for points until we have found r independent ones. Then we only need to find the K -rational torsion points and “saturate” the subgroup generated by the independent points. All of this can be done effectively.) Now the idea is to use the above exact sequence to at least get an upper bound on r : r can be read off from the size of the group $E(K)/nE(K)$ on the left, and so any bound on that group will provide us with a bound on r . From the exact sequence, we see that $E(K)/nE(K)$ sits inside $H^1(K, E[n])$; however this group is infinite, and so it does not give a bound.

But we can use some additional information. We know (trivially) that any K -rational point on E is also a K_v -rational point, for all places v of K . Now it is possible to compute the image of the local map

$$E(K_v)/nE(K_v) \xrightarrow{\delta_v} H^1(K_v, E[n])$$

for any given v explicitly; and for all but a finite explicitly determinable set of places S , the image just consists of the “unramified part” of $H^1(K_v, E[n])$. This

means that in some sense, we can compute all the necessary “local” conditions and use this information in bounding the “global” group $E(K)/nE(K)$. Formally, we define the n -Selmer group of E , $\text{Sel}^{(n)}(K, E)$, to be the subgroup of $H^1(K, E[n])$ of elements that under all restriction maps res_v are in the image of δ_v in the following diagram.

$$\begin{array}{ccccccc}
0 & \longrightarrow & E(K)/nE(K) & \xrightarrow{\delta} & H^1(K, E[n]) & \longrightarrow & H^1(K, E)[n] \longrightarrow 0 \\
& & \downarrow & & \downarrow \Pi_v \text{res}_v & \searrow \alpha & \downarrow \Pi_v \text{res}_v \\
0 & \longrightarrow & \prod_v E(K_v)/nE(K_v) & \xrightarrow{\prod_v \delta_v} & \prod_v H^1(K_v, E[n]) & \longrightarrow & \prod_v H^1(K_v, E)[n] \longrightarrow 0
\end{array}$$

Equivalently, $\text{Sel}^{(n)}(K, E)$ is the kernel of the map α . The image of $\text{Sel}^{(n)}(K, E)$ in $H^1(K, E)[n]$ is the kernel of the rightmost vertical map in the diagram. More generally, one defines the *Shafarevich-Tate group* of E , $\text{III}(K, E)$ to be

$$\text{III}(K, E) = \ker\left(H^1(K, E) \longrightarrow \prod_v H^1(K_v, E)\right).$$

Then we get another short exact sequence:

$$0 \longrightarrow E(K)/nE(K) \xrightarrow{\delta} \text{Sel}^{(n)}(K, E) \longrightarrow \text{III}(K, E)[n] \longrightarrow 0.$$

This time, one can (and we will) prove that the middle group is finite. And at least in principle, it is computable. In this way, we can compute the product $(\#E(K)/nE(K))(\#\text{III}(K, E)[n])$, and in particular, we obtain a bound on the rank r . The obstruction against this bound being sharp lies in $\text{III}(K, E)$, which is therefore also an interesting object. Of course, its size (conjectured, but not generally proved to be finite) also shows up in the famous Birch and Swinnerton-Dyer conjecture, and there are other reasons to study $\text{III}(K, E)$ for its own sake.

We need some more notions and notation. The *unramified part* of $H^1(K_v, E[n])$ is the kernel of the restriction map $H^1(K_v, E[n]) \longrightarrow H^1(K_v^{\text{unr}}, E[n])$. For any finite set of places S of K containing the infinite places, we define $H^1(K, E[n]; S)$ to be the subgroup of $H^1(K, E[n])$ of elements that map into the unramified part of $H^1(K_v, E[n])$ for all places $v \notin S$.

The finiteness of the Selmer group then follows from the two observations that $\text{Sel}^{(n)}(K, E) \subset H^1(K, E[n]; S)$ for a suitable finite set S , and that $H^1(K, E[n]; S)$ is finite for all finite sets S of places of K .

The latter is a standard fact; in the end it reduces to the two basic finiteness results of algebraic number theory: finiteness of the class group and finite generation of the unit group.

Theorem 1.1. *If S is a finite set of places of K containing the infinite places, then $H^1(K, E[n]; S)$ is finite.*

PROOF: This is a standard result, see for example [Se2, II.6.2] for a more general version. We give a proof tailored to the situation at hand, since it also gives some insight into the computational issues.

There is a finite extension $L = K(E[n])$ of K (the n -division field of E) such that $E[n]$ becomes a trivial L -Galois module. We have the inflation-restriction exact sequence

$$0 \longrightarrow H^1(L/K, E[n](L)) \longrightarrow H^1(K, E[n]) \longrightarrow H^1(L, E[n]),$$

and the group on the left is finite. Taking into account the ramification conditions, we see that $H^1(K, E[n]; S)$ maps into $H^1(L, E[n]; S_L)$ with finite kernel, where S_L is the set of places of L above some place of K in S . Therefore it suffices to show that $H^1(L, E[n]; S_L)$ is finite. Now

$$H^1(L, E[n]) = H^1(L, (\mathbb{Z}/n\mathbb{Z})^2) = \text{Hom}(G_L, (\mathbb{Z}/n\mathbb{Z})^2),$$

and the ramification condition means that the fixed field of the kernel of a homomorphism coming from $H^1(L, E[n]; S_L)$ is unramified outside S_L . On the other hand, this fixed field is an abelian extension of exponent dividing n ; it is therefore contained in the maximal abelian extension M of exponent n that is unramified outside S_L .

By Kummer theory (L contains the n th roots of unity because of the n -Weil pairing), $M = L(\sqrt[n]{U})$ for some subgroup $U \subset L^\times / (L^\times)^n$. Enlarging S_L by including the primes dividing n , the ramification condition translates into

$$U = L(S_L, n) = \{\alpha \in L^\times : n \mid v(\alpha) \text{ for all } v \notin S_L\} / (L^\times)^n$$

(the “ n -Selmer group of \mathcal{O}_{L, S_L} ”). Applying the Snake Lemma to the diagram below then provides us with the exact sequence

$$0 \longrightarrow \mathcal{O}_{L, S_L}^\times / (\mathcal{O}_{L, S_L}^\times)^n \longrightarrow L(S_L, n) \longrightarrow \text{Cl}_{S_L}(L)[n] \longrightarrow 0.$$

Since the S_L -unit group $\mathcal{O}_{L, S_L}^\times$ is finitely generated and the S_L -class group $\text{Cl}_{S_L}(L)$ is finite, $U = L(S_L, n)$ is finite, and hence so is the extension M . We see that all the homomorphisms have to factor through the finite group $\text{Gal}(M/L)$, whence

$H^1(L, E[n]; S_L)$ is finite.

$$\begin{array}{ccccccc}
& & 0 & & 0 & & 0 \\
& & \downarrow & & \downarrow & & \downarrow \\
& & \mathcal{O}_{L,S_L}^\times & \xrightarrow{n} & \mathcal{O}_{L,S_L}^\times & \longrightarrow & L(S_L, n) \dashrightarrow \\
& & \downarrow & & \downarrow & & \downarrow \\
& & L^\times & \xrightarrow{n} & L^\times & \longrightarrow & L^\times / (L^\times)^n \longrightarrow 0 \\
& & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & I_{S_L} & \xrightarrow{n} & I_{S_L} & \longrightarrow & I_{S_L} / nI_{S_L} \longrightarrow 0 \\
& & \downarrow & & \downarrow & & \downarrow \\
& & \text{---} \rightarrow \text{Cl}_{S_L}(L) & \xrightarrow{n} & \text{Cl}_{S_L}(L) & & \\
& & \downarrow & & \downarrow & & \\
& & 0 & & 0 & &
\end{array}$$

□

Before we state the next result, we need some more notation. The definitions can be found in [Si2, Ch. IV]. Let \mathcal{E} be the Néron model of E over \mathcal{O}_{K_v} . We write $\mathcal{E}(\bar{k}_v)^0$ for the connected component of the identity on the special fiber of \mathcal{E} , $E(K_v^{\text{unr}})^0$ for the subgroup of $E(K_v^{\text{unr}})$ consisting of points mapping into $\mathcal{E}(\bar{k}_v)^0$ (these are the points of good reduction on a minimal Weierstrass model at v), and $E(K_v^{\text{unr}})^1$ for the kernel of reduction at v (consisting of the points whose reduction is zero). There is an exact sequence

$$0 \longrightarrow E(K_v^{\text{unr}})^0 \longrightarrow E(K_v^{\text{unr}}) \longrightarrow \Phi_v(\bar{k}_v) \longrightarrow 0,$$

where Φ_v is the component group of the special fiber of \mathcal{E} . This is a finite algebraic group defined over k_v . The order $c_v(E) = \#\Phi_v(k_v)$ of its subgroup of elements defined over k_v is called the *Tamagawa number* of E at v .

The following result implies that $\text{Sel}^{(n)}(K, E)$ is finite.

Theorem 1.2. $\text{Sel}^{(n)}(K, E) \subset H^1(K, E[n]; S)$ where S is any finite set of places of K containing the infinite places, the places dividing n and the finite places v such that $\gcd(c_v(E), n) > 1$.

PROOF: We have to show that for $\xi \in \text{Sel}^{(n)}(K, E) \subset H^1(K, E[n])$ and for $v \notin S$, ξ maps to zero in $H^1(K_v^{\text{unr}}, E[n])$. Consider the exact sequences

$$\begin{array}{ccccccc}
0 & \longrightarrow & E(K_v^{\text{unr}})^0 & \longrightarrow & E(K_v^{\text{unr}}) & \longrightarrow & \Phi_v(\bar{k}_v) \longrightarrow 0 \\
0 & \longrightarrow & E(K_v^{\text{unr}})^1 & \longrightarrow & E(K_v^{\text{unr}})^0 & \longrightarrow & \mathcal{E}(\bar{k}_v)^0 \longrightarrow 0
\end{array}$$

Applying the Snake Lemma to multiplication-by- n on these sequences gives exact sequences of cokernels

$$E(K_v^{\text{unr}})^0/nE(K_v^{\text{unr}})^0 \longrightarrow E(K_v^{\text{unr}})/nE(K_v^{\text{unr}}) \longrightarrow \Phi_v(\bar{k}_v)/n\Phi_v(\bar{k}_v)$$

and

$$E(K_v^{\text{unr}})^1/nE(K_v^{\text{unr}})^1 \longrightarrow E(K_v^{\text{unr}})^0/nE(K_v^{\text{unr}})^0 \longrightarrow \mathcal{E}(\bar{k}_v)^0/n\mathcal{E}(\bar{k}_v)^0.$$

We claim that the image of $E(K_v)$ in $E(K_v^{\text{unr}})$ is divisible by n . Let $P \in E(K_v)$. Then in the first sequence, the image of P in the group furthest on the right is in $\Phi_v(k_v)/(\Phi_v(k_v) \cap n\Phi_v(\bar{k}_v))$, and this group is trivial, since $c_v(E) = \#\Phi_v(k_v)$ is prime to n . Hence the image of P comes from $E(K_v^{\text{unr}})^0/nE(K_v^{\text{unr}})^0$. In the second sequence, the group on the right is trivial, because the \bar{k}_v -points of a connected commutative algebraic group over k_v form a divisible group. The first group is also trivial, because it is a \mathbb{Z}_p -module (with p the residue characteristic of v), and n is invertible in this ring. Hence $E(K_v^{\text{unr}})^0/nE(K_v^{\text{unr}})^0 = 0$, and the image of P must vanish in $E(K_v^{\text{unr}})/nE(K_v^{\text{unr}})$. Now consider the following diagram.

$$\begin{array}{ccc} E(K_v)/nE(K_v) & \xrightarrow{\delta_v} & H^1(K_v, E[n]) \\ \downarrow & & \downarrow \\ E(K_v^{\text{unr}})/nE(K_v^{\text{unr}}) & \xrightarrow{\delta_v^{\text{unr}}} & H^1(K_v^{\text{unr}}, E[n]) \end{array}$$

We have seen that the left vertical arrow is the zero map, therefore the image of δ_v also maps trivially under the right vertical map. This exactly means that the elements of the Selmer group (mapping into the image of $E(K_v)$ in $H^1(K_v, E[n])$) are unramified at v . \square

REMARK: The proof shows that in general, the image of $E(K_v)$ in $H^1(K_v^{\text{unr}}, E[n])$ is isomorphic to $\Phi_v(k_v)/(\Phi_v(k_v) \cap n\Phi_v(\bar{k}_v))$ for all finite places v that do not divide n . In particular, the order of the image divides the Tamagawa number $c_v(E)$.

1.2. Interpretation of Selmer group elements.

The definition of the Selmer group as a subgroup of $H^1(K, E[n])$ is rather abstract, its elements being given by classes of 1-cocycles with values in $E[n]$. However, it is possible to give the Selmer group elements much more concrete interpretations. This is based on the following general fact, see [Se2, III.1].

Proposition 1.3. *Let X be some algebraic or geometric object, defined over K . Then the set of twists of X , i.e., objects Y defined over K such that X and Y are isomorphic over \bar{K} , up to K -isomorphism, is parameterized by $H^1(K, \text{Aut}_{\bar{K}}(X))$. (When the automorphism group of X is abelian, this is an abelian group; otherwise, it is a pointed set with the class of X as its distinguished element.)*

PROOF: This is quite standard (at least in many concrete manifestations, in particular in the cases we need; see [CFOSS1] for details). The map from the twists to $H^1(K, \text{Aut}_{\bar{K}}(X))$ is obtained as follows. Let Y be a twist of X . Then there is an isomorphism $\phi : Y \rightarrow X$, defined over \bar{K} . Then $\xi_\sigma = \phi^\sigma \phi^{-1}$ defines a 1-cocycle with values in $\text{Aut}_{\bar{K}}(X)$, and postcomposing ϕ by an automorphism of X changes ξ into a cohomologous cocycle. To get the map in the reverse direction, one takes the \bar{K} -“points” of X and “twists” the action of G_K by ξ by decreeing that the action of σ on Y (which has the same underlying set of \bar{K} -“points” as X) is given by the action of σ on X , followed by $\xi_{\sigma^{-1}}$. This is the nontrivial direction, and one needs to check that a suitable principle of “Galois descent” holds. \square

Since $\text{Sel}^{(n)}(K, E) \subset H^1(K, E[n])$, this means that we can obtain interpretations of Selmer group elements via interpretations of elements of $H^1(K, E[n])$ as twists. So we have to look for “objects” whose (\bar{K} -)automorphism group is $E[n]$.

Principal homogeneous spaces. Let us first look at a somewhat simpler situation related to $H^1(K, E)$. Consider “objects” of the form $C \xrightarrow{\cong} E$, where the isomorphism is defined over \bar{K} . Two such diagrams are isomorphic if there is an isomorphism $C \xrightarrow{\cong} C'$ and a point $P \in E$ such that the diagram

$$\begin{array}{ccc} C & \xrightarrow{\cong} & E \\ \downarrow & & \downarrow \cdot + P \\ C' & \xrightarrow{\cong} & E \end{array}$$

commutes. Then the automorphisms of the trivial object $E \xrightarrow{\cong} E$ are just the translations, so the automorphism group is $E(\bar{K})$. The objects are called *principal homogeneous spaces* for E , and they are classified (up to K -isomorphisms) by the *Weil-Châtelet group* $\text{WC}(K, E) = H^1(K, E)$.

Given a curve C as above, we can change the isomorphism to E by any translation without changing the isomorphism class of C as a principal homogeneous space. So given C , the only ambiguity in endowing it with a structure as a principal homogeneous space comes from the automorphism group of E as an elliptic curve. Generically, this is just $\{\pm 1\}$, and so there will be at most two structures as a principal homogeneous space for E on C . (The two will coincide when either one has order dividing 2 in $H^1(K, E)$.)

Note also that a principal homogeneous space has an algebraic group action of E on it. If $\phi : C \rightarrow E$ is an isomorphism (over \bar{K}), then

$$C \times E \ni (P, Q) \longmapsto P + Q := \phi^{-1}(\phi(P) + Q) \in C$$

is defined over K , since it is unchanged when ϕ is post-composed with a translation on E . Also, there is a well-defined (over K) “difference morphism”

$$C \times C \ni (P, P') \longmapsto P - P' := \phi(P) - \phi(P') \in E$$

such that, for example, $P + (P' - P) = P'$. Conversely, given morphisms $C \times E \rightarrow C$ and $C \times C \rightarrow E$ satisfying the usual properties, C becomes a principal homogeneous space (in the sense above) by picking any point $P_0 \in C$ and considering the isomorphism $C \ni P \mapsto P - P_0 \in E$. So we could have defined principal homogeneous spaces also through actions of E on curves C . (In fact, this is what is usually done.)

If C has a K -rational point P , then there is a K -defined isomorphism $\phi : C \rightarrow E$ that maps P to O . We obtain a diagram

$$\begin{array}{ccc} C & \xrightarrow{\phi} & E \\ \phi \downarrow & & \parallel \\ E & \xlongequal{\quad} & E \end{array}$$

showing that C is trivial as a principal homogeneous space (i.e., K -isomorphic to $E \xrightarrow{=} E$).

In this context, the elements of $\text{III}(K, E)$ are represented by principal homogeneous spaces with K_v -points for every place v , or with points “everywhere locally”, up to isomorphism over K . Nontrivial elements of $\text{III}(K, E)$ are those that have points everywhere locally, but no global points, i.e., those that “fail the Hasse Principle”.

First interpretation: n -coverings. Here, our object X is the multiplication-by- n map $E \xrightarrow{n} E$. The twists are covering maps $C \xrightarrow{\pi} E$ such that there is an isomorphism $C \rightarrow E$ over \bar{K} such that the following diagram commutes.

$$\begin{array}{ccc} C & \xrightarrow{\pi} & E \\ \downarrow & & \parallel \\ E & \xrightarrow{n} & E \end{array}$$

Such a $C \xrightarrow{\pi} E$ is called an n -covering of E . An isomorphism between two n -coverings $C \xrightarrow{\pi} E$ and $C' \xrightarrow{\pi'} E$ is given by an isomorphism $\phi : C \rightarrow C'$ such that the following diagram commutes.

$$\begin{array}{ccc} C & \xrightarrow{\pi} & E \\ \phi \downarrow & & \parallel \\ C' & \xrightarrow{\pi'} & E \end{array}$$

The automorphisms of $E \xrightarrow{n} E$ are then given by the translations by n -torsion points (acting on the left E), so that we indeed obtain $E[n]$ as the automorphism group.

In this interpretation, the map $E(K)/nE(K) \rightarrow H^1(K, E[n])$ comes about as follows. To a point $P \in E(K)$, we associate the n -covering $E \xrightarrow{\pi} E$ such that

$\pi(Q) = nQ + P$. It is easy to check that the isomorphism class of the covering only depends on $P \bmod nE(K)$. On the other hand, each n -covering $C \xrightarrow{\pi} E$ such that $C(K) \neq \emptyset$ is isomorphic to one of this form: there is an isomorphism between C and E defined over K (mapping a K -rational point on C to $O \in E$); under the composed map $E \xrightarrow{\cong} C \xrightarrow{\pi} E$, the origin O maps to some $P \in E(K)$, and then the map must be $Q \mapsto nQ + P$. Tracing through the definition of the connecting map δ shows that the map defined here coincides with δ under our interpretation.

For the Selmer group elements, this means that they correspond to the n -coverings that have points *everywhere locally*.

Note that the curve C in an n -covering $C \xrightarrow{\pi} E$ carries the structure of a *principal homogeneous space* for E : any \bar{K} -isomorphism $C \rightarrow E$ in the definition above provides such a structure, and since these isomorphisms are all related by translations (by n -torsion points), the isomorphism class of the principal homogeneous space structure is well-defined. This gives us the map $H^1(K, E[n]) \rightarrow H^1(K, E)$ in the coverings interpretation.

Second interpretation: Maps to \mathbb{P}^{n-1} . Here is another interpretation. On E , we can consider the map to \mathbb{P}^{n-1} that is given by the complete linear system associated to $n \cdot O$. Other objects are diagrams

$$\begin{array}{ccc} C & \longrightarrow & S \\ \cong \downarrow & & \downarrow \cong \\ E & \longrightarrow & \mathbb{P}^{n-1} \end{array}$$

with the dashed isomorphisms defined over \bar{K} . Twists of \mathbb{P}^{n-1} like S are called *Severi-Brauer varieties*; they are classified (according to the general principle) by $H^1(K, \mathrm{PGL}_n)$. Since PGL_n is non-abelian, this is just a pointed set; however, applying Galois cohomology to the exact sequence

$$0 \longrightarrow \mathbb{G}_m \longrightarrow \mathrm{GL}_n \longrightarrow \mathrm{PGL}_n \longrightarrow 0,$$

one obtains an injection $H^1(K, \mathrm{PGL}_n) \rightarrow H^2(K, \mathbb{G}_m) = \mathrm{Br}(K)$ identifying $H^1(K, \mathrm{PGL}_n)$ with the n -torsion $\mathrm{Br}(K)[n]$ in the Brauer group of K . (See [Se1, X.5]. Note that we use $H^1(K, \mathrm{GL}_n) = 0$, which is an easy generalization of Hilbert's Theorem 90.)

An isomorphism between two such diagrams is given by a pair of isomorphisms $C \rightarrow C'$ and $S \rightarrow S'$ such that the diagram

$$\begin{array}{ccccc}
 C & \xrightarrow{\quad} & & \xrightarrow{\quad} & S \\
 \downarrow & \dashrightarrow & E & \longrightarrow & \mathbb{P}^{n-1} \\
 & & \downarrow \cdot + P & & \downarrow \\
 & & E & \longrightarrow & \mathbb{P}^{n-1} \\
 \downarrow & \dashrightarrow & & \dashrightarrow & \downarrow \\
 C' & \xrightarrow{\quad} & & \xrightarrow{\quad} & S'
 \end{array}$$

commutes, with some choice of $P \in E$ and some automorphism of \mathbb{P}^{n-1} over \bar{K} . Automorphisms of $E \rightarrow \mathbb{P}^{n-1}$ are therefore given by translations on E that fix the linear system $|n \cdot O|$. Translation by P does this if and only if $n \cdot P \in |n \cdot O|$, i.e., iff $P \in E[n]$. So we obtain again the correct automorphism group, and we see that $H^1(K, E[n])$ also classifies diagrams as above, up to isomorphism over K . The map to $H^1(K, E)$ comes through “forgetting” the right half of the diagram.

In particular, we see that the curve C in both the coverings and the maps to \mathbb{P}^{n-1} interpretation of a given element in $H^1(K, E[n])$ is the same (as a principal homogeneous space for E). So, also in our second interpretation, the elements of the Selmer group are those diagrams such that C has points everywhere locally. This implies that also the Severi-Brauer variety S has points everywhere locally. Now there is the very important local-global principle for the Brauer group:

$$0 \longrightarrow \text{Br}(K) \longrightarrow \bigoplus_v \text{Br}(K_v) \xrightarrow{\sum_v \text{inv}_v} \mathbb{Q}/\mathbb{Z} \longrightarrow 0$$

is exact. In particular, an element of the Brauer group of K that is locally trivial is already (globally) trivial. This implies that S has a K -rational point, and so $S \cong \mathbb{P}^{n-1}$. Whence the following result.

Proposition 1.4. *The elements of $\text{Sel}^{(n)}(K, E)$ are in 1-to-1 correspondence with K -isomorphism classes of diagrams*

$$\begin{array}{ccc}
 C & \longrightarrow & \mathbb{P}^{n-1} \\
 \downarrow & & \downarrow \\
 \cong \downarrow & & \downarrow \cong \\
 E & \longrightarrow & \mathbb{P}^{n-1}
 \end{array}$$

such that C has points everywhere locally.

Let us look at what this means for various small values of n .

$n = 2$: On E , the map to \mathbb{P}^1 given by $|2 \cdot \mathcal{O}|$ is just the x -coordinate. It is a 2-to-1 map ramified in four points (namely, $E[2]$). Any twist $C \rightarrow \mathbb{P}^1$ will have the same geometric properties, which means that C can be realized by a model of the form

$$y^2 = f(x) = ax^4 + bx^3 + cx^2 + dx + e.$$

(This is an affine model; a somewhat better way is to consider

$$y^2 = F(x, z) = ax^4 + bx^3z + cx^2z^2 + dxz^3 + ez^4$$

in a $(1, 2, 1)$ -weighted projective plane.)

$n = 3$: The map $E \rightarrow \mathbb{P}^2$ given by $|3 \cdot \mathcal{O}|$ is an embedding of degree 3, realizing E as a plane cubic curve. Similarly, any element of the 3-Selmer group can be realized as a plane cubic curve, with an action of $E[3]$ on it through linear automorphisms.

$n = 4$: Here we obtain a degree-4 embedding into \mathbb{P}^3 ; its image is given as the intersection of two quadrics.

More generally, for $n \geq 4$, the image in \mathbb{P}^{n-1} is given as the intersection of $n(n-3)/2$ quadrics; for $n \geq 5$, this is no longer a complete intersection. For $n = 5$, there is a nice description by sub-Pfaffians of a 5×5 matrix of linear forms. For general elements of $H^1(K, E[n])$, we obtain another forgetful map. If we forget the left hand side of the diagram, then we obtain a map

$$\text{Ob} : H^1(K, E[n]) \rightarrow H^1(K, \text{PGL}_n) = \text{Br}(K)[n],$$

the ‘‘obstruction’’ against an embedding (or a map) into \mathbb{P}^{n-1} .

Warning. This map is *not* a homomorphism!

1.3. What the Selmer group can be used for.

The most obvious use of the Selmer group is to provide an upper bound for the Mordell-Weil rank r : we have

$$n^r = \frac{\#\text{Sel}^{(n)}(K, E)}{\#(E(K)_{\text{tors}}/nE(K)_{\text{tors}})\#\text{III}(K, E)[n]} \leq \frac{\#\text{Sel}^{(n)}(K, E)}{\#(E(K)_{\text{tors}}/nE(K)_{\text{tors}})}.$$

To get this, it is sufficient to just compute the order of the Selmer group.

Moreover, by computing the sizes of various Selmer groups (for coprime values of n), we can compare the bounds we get, and in some cases deduce lower bounds on the order of $\text{III}(K, E)$. For example, if we get $r \leq 3$ from the 2-Selmer group and $r \leq 1$ from the 3-Selmer group, then we know that $\#\text{III}(K, E)[2] \geq 4$.

On the other hand, in order to show that the rank bound we get is sharp, we need to prove that all elements of the Selmer group come from K -rational points on E . This is rather easy if we find sufficiently many independent points on E . However, in many cases, some of the generators of $E(K)$ can be rather large and will not be

found by a systematic search. Here, it is useful to represent the elements of the Selmer group as n -coverings C . We then have a diagram

$$\begin{array}{ccc} C & \xrightarrow{\text{deg } n} & \mathbb{P}^{n-1} \\ \text{deg } n^2 \downarrow \pi & & \downarrow \text{deg } 2n \\ E & \xrightarrow[x]{\text{deg } 2} & \mathbb{P}^1 \end{array}$$

with a rational map of degree $2n$ on the right hand side.

For example, when $n = 2$, the map $\mathbb{P}^1 \rightarrow \mathbb{P}^1$ on the right hand side is given by two quartic forms (the quartic showing up in the equation of the 2-covering C and its quartic covariant).

From the general theory of heights, we expect the logarithmic height of a point on C , as given by its image in \mathbb{P}^{n-1} , to be smaller by a factor of about $1/2n$ than that of the x -coordinate of its image on E . This will make these points much easier to find on C (in \mathbb{P}^{n-1}) than on E . If we find a K -rational point on C , we know that the corresponding element of the n -Selmer group is in the image of δ , and we can improve the lower bound on the rank. Note that in practice, to really be fairly certain that the points on C are as small as expected, it is necessary to have a “small” model of C , i.e., given by equations with small coefficients.

In case we do not find a K -rational point on C , we can use the curve C as the basis for “higher descents”; in this way we may be able to prove that C does not have any K -rational points, or find points on curves that cover C .

The program for the following will therefore be to first show how one can compute the p -Selmer group for a prime number p (the most important case). Then we will discuss how to obtain from this computation actual covering curves. But first, we will introduce another interpretation of the elements of $H^1(K, E[n])$.

Third interpretation: Theta groups. In the second interpretation, on the morphism $E \rightarrow \mathbb{P}^{n-1}$ there is an action of $E[n]$; in particular, $E[n]$ acts on \mathbb{P}^{n-1} by automorphisms. Thus we obtain a homomorphism $\chi_E : E[n] \rightarrow \text{PGL}_n$. We can then define Θ_E by the following diagram. This works on the level of group schemes or on the level of groups (of \bar{K} -points). For details see [CFOSS1].

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathbb{G}_m & \xrightarrow{\alpha} & \Theta_E & \xrightarrow{\beta} & E[n] \longrightarrow 0 \\ & & \parallel & & \downarrow & & \downarrow \chi_E \\ 0 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \text{GL}_n & \longrightarrow & \text{PGL}_n \longrightarrow 0 \end{array}$$

Proposition 1.5. *In the above, for any $\theta, \theta' \in \Theta_E$, we have*

$$[\theta, \theta'] = \theta\theta'\theta^{-1}\theta'^{-1} = \alpha(e_n(\beta(\theta), \beta(\theta'))),$$

where $e_n : E[n] \times E[n] \rightarrow \mu_n \hookrightarrow \mathbb{G}_m$ is the n -Weil pairing.

PROOF: Let $T, T' \in E[n]$. We have to show that for any two lifts $\theta, \theta' \in \mathrm{GL}_n$ of $\chi_E(T)$ and $\chi_E(T')$, we have

$$[\theta, \theta'] = e_n(T, T') I_n$$

(where I_n is the $n \times n$ identity matrix).

For this, note that \mathbb{P}^{n-1} can be identified with $\mathbb{P}(L(n \cdot O)^*)$. For every $T \in E[n]$, choose $f_T \in \bar{K}(E)^\times$ such that $\mathrm{div}(f_T) = n \cdot T - n \cdot O$. Then the action of T on $\mathbb{P}(L(n \cdot O)^*)$ is induced by

$$L(n \cdot O) \ni f \longmapsto (P \mapsto f_T(P)f(P-T)) \in L(n \cdot O).$$

Note that a choice of θ lifting $\chi_E(T)$ corresponds to a choice of f_T . Now the action of the commutator $[\theta, \theta']$ is given on $L(n \cdot O)$ by

$$f \longmapsto \left(P \mapsto \frac{f_T(P) f_{T'}(P-T)}{f_T(P-T) f_{T'}(P)} f(P) \right).$$

The factor in front of $f(P)$ is constant (where defined) as can be checked by verifying that its divisor is zero, and is equal to $e_n(T, T')$, see for example Exercise 3.16 in [Si1]. \square

The proof shows that Θ_E can be represented as the set

$$\{(T, f_T) : T \in E[n], f_T \in \bar{K}(E)^\times, \mathrm{div}(f_T) = n \cdot T - n \cdot O\}$$

with the group structure given by

$$(T, f_T)(T', f_{T'}) = (T + T', P \mapsto f_T(P)f_{T'}(P-T));$$

also $\alpha(\lambda) = (O, \lambda)$ and $\beta(T, f_T) = T$.

More generally, we define a *theta group* of level n for E to be an exact sequence (of K -group schemes)

$$0 \longrightarrow \mathbb{G}_m \xrightarrow{\alpha} \Theta \xrightarrow{\beta} E[n] \longrightarrow 0$$

such that for $\theta, \theta' \in \Theta$, we have again

$$[\theta, \theta'] = \alpha(e_n(\beta(\theta), \beta(\theta'))).$$

(Note that this implies that Θ is a *central* extension of $E[n]$ by \mathbb{G}_m .) An isomorphism of two such diagrams is given by a G_K -isomorphism $\phi : \Theta \longrightarrow \Theta'$ making the following diagram commutative.

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \Theta & \longrightarrow & E[n] \longrightarrow 0 \\ & & \parallel & & \downarrow \phi & & \parallel \\ 0 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \Theta' & \longrightarrow & E[n] \longrightarrow 0 \end{array}$$

Working out what the automorphisms (in the sense of isomorphisms of theta groups) of Θ_E are, we find that they are of the form $(T, f_T) \longmapsto (T, \varphi(T)f_T)$ for a homomorphism $\varphi : E[n] \longrightarrow \mathbb{G}_m$. Such a φ necessarily takes values in μ_n , and

by the non-degeneracy of the Weil pairing e_n , there is some $T' \in E[n]$ such that $\varphi(T) = e_n(T', T)$. We see that the automorphism group is again $E[n]$. Furthermore, we have the following result.

Proposition 1.6. *All theta groups of level n for E are isomorphic over \bar{K} (i.e., as abstract group extensions).*

PROOF: Short proof: On the level of abstract groups, theta groups are classified by $H^2((\mathbb{Z}/n\mathbb{Z})^2, \bar{K}^\times)$. There is a canonical map

$$H^2((\mathbb{Z}/n\mathbb{Z})^2, \bar{K}^\times) \longrightarrow \bigwedge^2 \text{Hom}((\mathbb{Z}/n\mathbb{Z})^2, \bar{K}^\times)$$

induced by the commutator. Since \bar{K}^\times is divisible by n , this map is an isomorphism by a result from group cohomology. Since theta groups are represented on the left as the elements that map to the Weil pairing e_n in the right hand group, there is only one such extension, up to isomorphism.

Sketch of long, but down-to-earth proof: choosing any set-theoretic section $E[n] \longrightarrow \Theta$ mapping O to the neutral element, the underlying set of Θ can be identified with $\bar{K}^\times \times E[n]$. The group structure is then given by a map

$$f : E[n] \times E[n] \longrightarrow \bar{K}^\times$$

such that

$$(\lambda, T)(\lambda', T') = (\lambda\lambda'f(T, T'), T + T').$$

From the group axioms, we find that f has to satisfy

$$f(O, T) = f(T, O) = 1, \quad f(T, T')f(T + T', T'') = f(T, T' + T'')f(T', T'').$$

(I.e., f is a normalized 2-cocycle.) We also have that

$$f(T, T') = e_n(T, T')f(T', T).$$

If we have two theta groups Θ_1 and Θ_2 , with multiplication given by f_1 and f_2 , then setting $f(T, T') = f_1(T, T')/f_2(T, T')$, f satisfies the cocycle condition, and it is symmetric: $f(T, T') = f(T', T)$. We now construct a map $\varphi : E[n] \longrightarrow \bar{K}^\times$. Set $\varphi(O) = 1$. Pick a basis T, T' for $E[n]$. Set

$$\begin{aligned} \varphi(T) &= (f(T, T)f(T, 2T) \dots f(T, (n-1)T))^{-1/n} \\ \varphi(T') &= (f(T', T')f(T', 2T') \dots f(T', (n-1)T'))^{-1/n} \end{aligned}$$

with any choice of the n th roots (here we need that \bar{K}^\times is divisible by n). Then we continue by defining

$$\begin{aligned} \varphi(mT) &= f(T, T)f(T, 2T) \dots f(T, (m-1)T) \varphi(T)^m \\ \varphi(mT') &= f(T', T')f(T', 2T') \dots f(T', (m-1)T') \varphi(T')^m \\ \varphi(mT + m'T') &= f(mT, m'T') \varphi(mT) \varphi(m'T') \end{aligned}$$

Now we have by an easy induction using the cocycle relation that

$$f(aT, bT) = \frac{\varphi(aT + bT)}{\varphi(aT)\varphi(bT)}, \quad f(aT', bT') = \frac{\varphi(aT' + bT')}{\varphi(aT')\varphi(bT')}$$

$$\text{and } f(aT, bT') = \frac{\varphi(aT + bT')}{\varphi(aT)\varphi(bT')}.$$

Since we can express $f(aT + bT', cT + dT')$ in terms of values like the above, we get that

$$f(P, Q) = \frac{\varphi(P + Q)}{\varphi(P)\varphi(Q)}$$

for all $P, Q \in E[n]$. Then

$$\Theta_2 \ni (\lambda, P) \longmapsto (\varphi(P)\lambda, P) \in \Theta_1$$

is an isomorphism. \square

We deduce that $H^1(K, E[n])$ parameterizes theta groups of level n for E , up to K -isomorphism. These theta groups are not geometric objects like our n -covering curves, but they are quite useful.

If $C \longrightarrow \mathbb{P}^{n-1}$ in our second interpretation represents an element of $\text{Sel}^{(n)}(K, E)$, then we can easily find the corresponding theta group Θ_C . Namely, $E[n]$ acts by automorphisms on this diagram and thus gives us a homomorphism $\chi_C : E[n] \longrightarrow \text{PGL}_n$. As before, we can then define Θ_C to be the pull-back of the image of χ_C under the canonical map $\text{GL}_n \longrightarrow \text{PGL}_n$:

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \Theta_C & \longrightarrow & E[n] \longrightarrow 0 \\ & & \parallel & & \downarrow & & \downarrow \chi_C \\ 0 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \text{GL}_n & \longrightarrow & \text{PGL}_n \longrightarrow 0 \end{array}$$

For more general diagrams $C \longrightarrow S$, GL_n and PGL_n have to be replaced by their twists corresponding to $\text{Ob}(C \rightarrow S) = S$; in this way, we obtain Θ_C as a subgroup of A_S^\times , where A_S is the central simple algebra corresponding to S . (See below.)

2. COMPUTATION OF THE SELMER GROUP AS AN ABSTRACT GROUP

The interpretations given so far are not very well suited for actually *computing* the n -Selmer group. (For $n = 2$, this is not quite true: John Cremona's `mwrnk` program actually enumerates 2-coverings in order to find the 2-Selmer group.) So we will need some other representation of the Selmer group that is more algebraic in nature and yields itself more easily to computation. The main results of this section are Theorems 2.4 and 2.7.

Before we go into this, let me remark that the various Selmer groups are related. From the diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & E[m] & \longrightarrow & E & \xrightarrow{m} & E \longrightarrow 0 \\
& & \downarrow & & \parallel & & \downarrow n \\
0 & \longrightarrow & E[mn] & \longrightarrow & E & \xrightarrow{mn} & E \longrightarrow 0 \\
& & \downarrow m & & \downarrow m & & \parallel \\
0 & \longrightarrow & E[n] & \longrightarrow & E & \xrightarrow{n} & E \longrightarrow 0
\end{array}$$

we can deduce an exact sequence

$$\begin{aligned}
0 &\longrightarrow \frac{E(K)[n]}{mE(K)[mn]} \longrightarrow \mathrm{Sel}^{(m)}(K, E) \longrightarrow \mathrm{Sel}^{(mn)}(K, E) \\
&\longrightarrow \mathrm{Sel}^{(n)}(K, E) \longrightarrow \frac{\mathrm{III}(K, E)[n]}{m\mathrm{III}(K, E)[mn]} \longrightarrow 0.
\end{aligned}$$

Here the map $\mathrm{Sel}^{(m)} \longrightarrow \mathrm{Sel}^{(mn)}$ is induced by the inclusion $E[m] \hookrightarrow E[mn]$, and the map $\mathrm{Sel}^{(mn)} \longrightarrow \mathrm{Sel}^{(n)}$ is induced by multiplication by m $E[mn] \longrightarrow E[n]$. In particular, the composition $\mathrm{Sel}^{(n)} \longrightarrow \mathrm{Sel}^{(mn)} \longrightarrow \mathrm{Sel}^{(n)}$ (the first map coming from the diagram where the roles of m and n are exchanged) is multiplication by m on $\mathrm{Sel}^{(n)}$. Together with the exact sequence above, this implies that

$$\mathrm{Sel}^{(mn)}(K, E) \cong \mathrm{Sel}^{(m)}(K, E) \times \mathrm{Sel}^{(n)}(K, E)$$

whenever m and n are coprime.

Therefore it is sufficient to compute $\mathrm{Sel}^{(n)}(K, E)$ when $n = p^f$ is a prime power. The first step in this is to consider the case $n = p$. The computation of $\mathrm{Sel}^{(p^2)}(K, E)$ (and for higher powers of p) then is most easily done by computing the fibers of the canonical map $\mathrm{Sel}^{(p^2)}(K, E) \longrightarrow \mathrm{Sel}^{(p)}(K, E)$ one by one. (This procedure is sometimes referred to as “second” or “higher descent”.)

Fourth interpretation: via étale algebras.

The goal of the interpretation I will explain now is to ease computation of the Selmer group. So we will consider an algebraic realization of $H^1(K, E[n])$ and not a geometric one.

In what follows, one of the main characters of the play will be the *étale algebra* R of $E[n]$. This is just the affine coordinate algebra of the 0-dimensional scheme $E[n]$. More concretely, we have

$$R = \mathrm{Map}(E[n], \bar{K})^{G_K}, \quad \text{so that} \quad E[n] = \mathrm{Spec} R.$$

The elements of R are the G_K -equivariant maps on $E[n]$ with values in \bar{K} . Note that the action of $\sigma \in G_K$ is

$$f \longmapsto (f^\sigma : T \mapsto f(T^{\sigma^{-1}})^\sigma).$$

For example, any rational function on E defined over K and not having poles in $E[n]$ will give an element of R .

Since $E[n]$ is an étale K -scheme, R is an étale algebra: it is isomorphic to a product of (finite) field extensions of K , one for each G_K -orbit on $E[n]$. If T is a point in one such orbit, then the corresponding field extension is $K(T)$ (i.e., K with the coordinates of the n -torsion point T adjoined). For example, we always have a splitting $R = K \times R_1$, where the K corresponds to the singleton orbit $\{O\}$, and R_1 corresponds to $E[n] \setminus \{O\}$.

We will also use $\bar{R} = R \otimes_K \bar{K} = \text{Map}(E[n], \bar{K})$. As an algebra, this is just $\bar{K}^{E[n]} \cong \bar{K}^{n^2}$, but the action of G_K is “twisted” by its action on $E[n]$, permuting the factors.

In this context, \bar{R}^\times is the multiplicative group of maps from $E[n]$ into \bar{K}^\times , and R^\times is the subgroup of G_K -equivariant such maps. For example, every $T \in E[n]$ gives a map

$$e(T) : E[n] \ni S \mapsto e_n(T, S) \in \mu_n \subset \bar{K}^\times,$$

and so we obtain an injective (because e_n is non-degenerate) homomorphism

$$e : E[n] \longrightarrow \bar{R}^\times.$$

The idea now is to extend this to (the beginning of) a resolution of $E[n]$ as a K -Galois module, in order to get some more or less concrete realization of $H^1(K, E[n])$.

In general, if R_A and R_B are the coordinate rings of two affine K -schemes A and B , then $R_A \otimes_K R_B$ is the coordinate ring of $A \times B$. So $R \otimes_K R$ is the algebra of G_K -equivariant maps from $E[n] \times E[n]$ into \bar{K} , and $\bar{R} \otimes_{\bar{K}} \bar{R} = (R \otimes_K R) \otimes_K \bar{K}$ is the algebra of all such maps.

Now observe that all $e(T)$, for $T \in E[n]$, are not only maps, but homomorphisms $E[n] \longrightarrow \bar{K}^\times$. I.e., $\alpha = e(T)$ satisfies the relations $\alpha(T_1 + T_2) = \alpha(T_1)\alpha(T_2)$. By the non-degeneracy of the Weil pairing, we also know that the $e(T)$ are *all* the homomorphisms. This implies that, if we define

$$\partial : \bar{R}^\times \ni \alpha \longmapsto \left((T_1, T_2) \mapsto \frac{\alpha(T_1)\alpha(T_2)}{\alpha(T_1 + T_2)} \right) \in (\bar{R} \otimes_{\bar{K}} \bar{R})^\times,$$

then

$$0 \longrightarrow E[n] \xrightarrow{e} \bar{R}^\times \xrightarrow{\partial} (\bar{R} \otimes_{\bar{K}} \bar{R})^\times$$

will be exact.

In order to use that to realize $H^1(K, E[n])$, we need to know what the image of the map ∂ is. One obvious property of all $\partial\alpha$ is that they are symmetric:

$\partial\alpha(T_1, T_2) = \partial\alpha(T_2, T_1)$. But there are more conditions they satisfy. Let us define

$$\partial : (\bar{R} \otimes_{\bar{K}} \bar{R})^\times \ni \rho \longmapsto \left((T_1, T_2, T_3) \mapsto \frac{\rho(T_1, T_2)\rho(T_1 + T_2, T_3)}{\rho(T_1, T_2 + T_3)\rho(T_2, T_3)} \right) \in (\bar{R} \otimes_{\bar{K}} \bar{R} \otimes_{\bar{K}} \bar{R})^\times.$$

Then we have the following result. We define $\text{Sym}_{\bar{K}}^2(\bar{R})$ to be the subalgebra of $\bar{R} \otimes_{\bar{K}} \bar{R}$ consisting of symmetric maps (and similarly $\text{Sym}_K^2(R)$ for R and K).

Proposition 2.1. *The following is an exact sequence.*

$$0 \longrightarrow E[n] \xrightarrow{e} \bar{R}^\times \xrightarrow{\partial} (\text{Sym}_{\bar{K}}^2(\bar{R}))^\times \xrightarrow{\partial} (\bar{R} \otimes_{\bar{K}} \bar{R} \otimes_{\bar{K}} \bar{R})^\times$$

PROOF: We only have to show exactness at $(\text{Sym}_{\bar{K}}^2(\bar{R}))^\times$. It is immediately checked that $\partial\partial\alpha = 1$ for $\alpha \in \bar{R}^\times$. On the other hand, if $\rho \in (\text{Sym}_{\bar{K}}^2(\bar{R}))^\times$ such that $\partial\rho = 1$, then as a map $E[n]^2 \longrightarrow \bar{K}^\times$, ρ is a symmetric 2-cocycle, and we have seen in our discussion of theta groups that each such 2-cocycle is a coboundary, which translates into $\rho = \partial\alpha$ for some $\alpha \in \bar{R}^\times$. \square

Corollary 2.2. *There is an isomorphism*

$$H = \frac{\ker(\partial \mid \text{Sym}_K^2(R)^\times)}{\partial R^\times} \xrightarrow{\cong} H^1(K, E[n]).$$

It is defined as follows. Take $\rho \in \text{Sym}_K^2(R)^\times$ such that $\partial\rho = 1$. Then there is some $\gamma \in \bar{R}^\times$ such that $\partial\gamma = \rho$. Now the Galois 1-cocycle $\sigma \mapsto \gamma^\sigma/\gamma$ takes values in the kernel of ∂ , so we can write $\gamma^\sigma/\gamma = e(T_\sigma)$, where $\sigma \mapsto T_\sigma$ is a 1-cocycle with values in $E[n]$ representing the image of ρ in $H^1(K, E[n])$.

PROOF: From the proposition, we get the short exact sequence

$$0 \longrightarrow E[n] \xrightarrow{e} \bar{R}^\times \xrightarrow{\partial} \ker(\partial \mid (\text{Sym}_{\bar{K}}^2(\bar{R}))^\times) \longrightarrow 0.$$

Apply the long exact cohomology sequence to get

$$R^\times \xrightarrow{\partial} \ker(\partial \mid \text{Sym}_K^2(R)^\times) \xrightarrow{\delta} H^1(K, E[n]) \longrightarrow H^1(K, \bar{R}^\times) = 0.$$

(The latter equality is an easy generalization of Hilbert's Theorem 90.) The description of the isomorphism follows the definition of the connecting map δ above. \square

Therefore, we can represent $H^1(K, E[n])$ as a subquotient of $\text{Sym}_K^2(R)^\times / (\text{Sym}_K^2(R)^\times)^n$. Putting in the condition that the elements are unramified outside the set S of places of K described in Thm. 1.2, we see that $\text{Sel}^{(n)}(K, E)$ is contained in a subquotient of the “ n -Selmer group” of the S -integers of $\text{Sym}_K^2(R)$,

$$\text{Sym}_K^2(R)(S, n) = \frac{\{\rho \in \text{Sym}_K^2(R)^\times : \text{Sym}_K^2(R)(\sqrt[n]{\rho}) \text{ unramified outside } S\}}{(\text{Sym}_K^2(R)^\times)^n}.$$

This is a finite group that is effectively computable. However, this computation requires the knowledge of the class and unit groups of the number fields occurring as factors of $\text{Sym}_K^2(R)$. If $n = p$ is an odd prime, we have a splitting

$$\text{Sym}_K^2(R) \cong K \times \prod_j L_j \times L,$$

where K corresponds to $\{(O, O)\}$, L_j corresponds to the set $\{(T, jT) : O \neq T \in E[p]\}$ (where j runs through a set of representatives of \mathbb{F}_p^\times modulo identifying inverses), and L corresponds to the set of unordered bases of $E[p]$. The cardinality of this set, and therefore the degree of L , is $(p-1)^2 p(p+1)/2$. Generically, L is a number field of that relative degree over K , and so even for $p = 3$, this is outside the range of practical applicability of current methods in computational algebraic number theory. So we will need a better, smaller representation. But let us first see how one could use our current representation at least in principle to actually compute the Selmer group.

For this, note that the result of Thm. 1.2 can be extended to show that the Selmer group can be obtained by a finite computation:

$$\text{Sel}^{(n)}(K, E) = \{\xi \in H^1(K, E[n]; S) : \forall v \in S : \text{res}_v(\xi) \in \delta_v(E(K_v)/nE(K_v))\}$$

(For this, one needs to show that the image of $E(K_v)/nE(K_v)$ in $H^1(K_v, E[n])$ is exactly the unramified part, for all $v \notin S$.) In order to turn this into an algorithm, we first need to find the image H_S of $H^1(K, E[n]; S)$ in H . This is obtained through the computation of $\text{Sym}_K^2(R)(S, n)$ and then passing to the relevant subquotient. (For this, we need to find $R(S, n)$ and compute its image under ∂ .) Then we need to have explicit representations of the maps res_v and δ_v , for all $v \in S$. For the restriction maps, we just observe that the result of Cor. 2.2 works over any field K and is functorial. Applying this observation to the field extension $K \subset K_v$, we get

$$\text{res}_v : H \longrightarrow H_v = \frac{\ker(\partial \mid (\text{Sym}_K^2(R) \otimes_K K_v)^\times)}{\partial(R \otimes_K K_v)^\times};$$

this is induced by the canonical map $\text{Sym}_K^2(R) \longrightarrow \text{Sym}_K^2(R) \otimes_K K_v$. Note also that H_v is a finite group. To get a nice representation of δ_v (or δ), we remind ourselves of the usual definition of the Weil pairing.

Let $T \in E[n]$ be an n -torsion point. Then there is a rational function $G_T \in K(T)(E)^\times$ such that

$$\text{div}(G_T) = n^*(T) - n^*(O) = \sum_{P:nP=T} P - \sum_{Q:nQ=O} Q.$$

This divisor is stable under translations by elements of $E[n]$, therefore we have that $G_T(P + S) = c(S)G_T(P)$ for some constant $c(S)$ independent of P , when $S \in E[n]$. This constant is $e_n(S, T)$. We can choose these functions G_T in such a way that $G : T \mapsto G_T$ is Galois-equivariant. Then we can interpret G as an

element of $R(E)^\times$ (where $R(E) = K(E) \otimes_K R$; its elements are G_K -equivariant maps from $E[n]$ into $\bar{K}(E)$), and we have $G(P+T) = e(T)G(P)$ for $P \in E \setminus E[n^2]$ and $T \in E[n]$. Now consider the following diagram.

$$\begin{array}{ccccccc} 0 & \longrightarrow & E[n] & \longrightarrow & E & \xrightarrow{n} & E \longrightarrow 0 \\ & & \parallel & & \downarrow G & & \downarrow r \\ 0 & \longrightarrow & E[n] & \xrightarrow{e} & \bar{R}^\times & \xrightarrow{\partial} & \ker(\partial \mid \mathrm{Sym}_K^2(\bar{R})^\times) \longrightarrow 0 \end{array}$$

The map r is defined as shown: to find $r(P)$, take some $Q \in E$ such that $nQ = P$, then $r(P) = \partial G(Q)$. This is well defined, since another choice Q' in place of Q will differ from Q by addition of an n -torsion point T , so

$$\partial G(Q') = \partial G(Q + T) = \partial(e(T)G(Q)) = \partial G(Q),$$

since $\partial e(T) = 1$. This also shows that r is defined over K , so $r \in \mathrm{Sym}_K^2(R)(E)^\times$. To find out what function $r_{T_1, T_2} \in \bar{K}(E)^\times$ is, let us determine its divisor. By definition,

$$r_{T_1, T_2}(nQ) = \frac{G_{T_1}(Q)G_{T_2}(Q)}{G_{T_1+T_2}(Q)},$$

so

$$n^*(\mathrm{div}(r_{T_1, T_2})) = n^*(T_1) + n^*(T_2) - n^*(T_1 + T_2) - n^*(O).$$

So r_{T_1, T_2} has simple zeros at T_1 and T_2 and simple poles at $T_1 + T_2$ and O : it is the function witnessing that $T_1 + T_2$ is the sum of T_1 and T_2 . So, up to normalizing constants, with respect to a Weierstraß model of E , r_{T_1, T_2} is the equation of the line joining T_1 and T_2 divided by the equation of the (vertical) line joining $T_1 + T_2$ and O . For suitable normalization of the G_T , we can take quite concretely the following. Here, the line joining two points T_1 and T_2 , such that $T_1, T_2, T_1 + T_2 \neq O$ (the tangent line at T of E , when $T_1 = T_2 = T$) is supposed to have equation

$$y = \lambda_{T_1, T_2} x + m_{T_1, T_2}.$$

Take

$$r_{T_1, T_2} = \begin{cases} 1 & \text{if } T_1 = O \text{ or } T_2 = O; \\ x - x(T_1) & \text{if } T_1 + T_2 = O, T_1 \neq O; \\ \frac{y - \lambda_{T_1, T_2} x - m_{T_1, T_2}}{x - x(T_1 + T_2)} & \text{if } T_1, T_2, T_1 + T_2 \neq O. \end{cases}$$

Now, chasing through the definitions of the connecting homomorphisms

$$E(K) \xrightarrow{\delta} H^1(K, E[n]) \quad \text{and} \quad H \xrightarrow{\cong} H^1(K, E[n]),$$

we easily find the following.

Proposition 2.3. *The composition $E(K) \xrightarrow{\delta} H^1(K, E[n]) \longrightarrow H$ is induced by $r : E(K) \setminus E[n] \longrightarrow \mathrm{Sym}_K^2(R)^\times$.*

The “missing” values on $E(K)[n]$ can be obtained by a suitable rescaling and limiting process. This result is again valid for all fields K and functorial in K , so we can use it to compute the local maps $\delta_v : E(K_v)/nE(K_v) \hookrightarrow H_v$. Since we can easily compute the size of the group on the left hand side — say, $n = p$ is a prime, then

$$\dim_{\mathbb{F}_p} E(K_v)/pE(K_v) = \dim_{\mathbb{F}_p} E(K_v)[p] + \begin{cases} 0 & \text{if } v \text{ is finite and } v \nmid p; \\ [K_v : \mathbb{Q}_p] & \text{if } v \mid p; \\ -[K_v : \mathbb{R}] & \text{if } v \text{ is infinite —} \end{cases}$$

we can just pick random points in $E(K_v)$ until their images in H_v generate a subspace of the correct size. Having found all the “local images”

$$J_v = \delta_v(E(K_v)/pE(K_v)) \subset H_v, \quad \text{for } v \in S,$$

the determination of the Selmer group as a subgroup of H_S is reduced to linear algebra over \mathbb{F}_p . *Mutatis mutandis*, this will also work for arbitrary n .

Let us summarize the discussion.

Theorem 2.4. *There is an effective procedure for computing the n -Selmer group of an elliptic curve over a number field K . It requires class group and unit group computations in extensions of K of the form $K(\{T_1, T_2\})$, where $\{T_1, T_2\}$ is an unordered pair of n -torsion points of E .*

As mentioned above, as it stands, this result is rather theoretical, since the number fields that occur are too large for practical computations. However, we can improve the situation. Restricting to n -torsion subgroups in the basic exact sequence

$$0 \longrightarrow E[n] \xrightarrow{e} \bar{R}^\times \xrightarrow{\partial} \ker(\partial \mid (\text{Sym}_K^2(\bar{R}))^\times) \longrightarrow 0,$$

we obtain

$$0 \longrightarrow E[n] \xrightarrow{e} \mu_n(\bar{R}) \xrightarrow{\partial} \partial\mu_n(\bar{R}) \longrightarrow 0.$$

This gives us

$$0 \longrightarrow \frac{(\partial\mu_n(\bar{R}))^{G_K}}{\partial\mu_n(\bar{R})} \longrightarrow H^1(K, E[n]) \longrightarrow H^1(K, \mu_n(\bar{R})) \cong R^\times / (R^\times)^n.$$

The isomorphism comes in the usual way from the fact that $H^1(K, \bar{R}^\times) = 0$.

Now we have the following nice fact (see [DSS, ScSt]).

Proposition 2.5. *If $n = p$ is a prime, then $(\partial\mu_p(\bar{R}))^{G_K} = \partial\mu_p(R)$.*

For the proof, one basically checks all possibilities for the image of G_K in $\text{Aut}(E[p]) \cong \text{GL}_2(\mathbb{F}_p)$, the most interesting case being when the image is a p -Sylow subgroup.

REMARK: The result is not true in general for composite n . For example, taking $n = 4$, there are 20 conjugacy classes (out of 62) of subgroups of $\text{GL}_2(\mathbb{Z}/4\mathbb{Z})$ such

that the kernel above has order 2 or even 4. To give a very concrete example, consider the elliptic curve $y^2 = x^3 + x + 2/13$ over \mathbb{Q} ; then the index of $\partial\mu_4(R)$ in the $G_{\mathbb{Q}}$ -invariants of $\partial\mu_4(\bar{R})$ is 2. (Here the subgroup is the one problematic one of index 2. It occurs generically when the discriminant of the cubic is minus a square.)

In any case, we have a homomorphism

$$H \xrightarrow{\cong} H^1(K, E[n]) \longrightarrow R^\times / (R^\times)^n.$$

By the definition of the Kummer map $R^\times / (R^\times)^n \longrightarrow H^1(K, \mu_n(\bar{R}))$, it is obtained as follows. Take $\rho \in \text{Sym}_K^2(R)^\times$ representing an element of H , so $\partial\rho = 1$. Then there is $\gamma \in \bar{R}^\times$ such that $\partial\gamma = \rho$. Now $\gamma^\sigma / \gamma \in \ker \partial \subset \mu_n(\bar{R})$ for all $\sigma \in G_K$, hence $\gamma^n \in R^\times$. If we change ρ into $\rho \cdot \partial\alpha$ with $\alpha \in R^\times$, then γ^n changes into $\gamma^n \alpha^n$, and we get a well-defined map $H \longrightarrow R^\times / (R^\times)^n$. A somewhat more explicit description is to say that the map is induced by

$$\text{Sym}_K^2(R)^\times \ni \rho \longmapsto \left(T \mapsto \prod_{j=0}^{n-1} \rho(T, jT) \right) \in R^\times.$$

So when $n = p$ is a prime number, then we can use the image of H in $R^\times / (R^\times)^p$ instead of H itself. The advantage of this is obvious: the field extensions of K occurring in R are usually *much* smaller than the ones in $\text{Sym}_K^2(R)$. Generically, $R = K \times R_1$, with R_1 a field extension of K of degree $p^2 - 1$. For $K = \mathbb{Q}$ and $p = 3$, this leads to octic number fields, where computations are feasible.

To make this approach work, we need to know the image \tilde{H} of H in $R^\times / (R^\times)^p$, and we need to realize the map $E[p] \xrightarrow{\delta} H^1(K, E[p]) \longrightarrow \tilde{H}$.

The first question is answered by looking at the map $H \rightarrow \tilde{H}$: given $\alpha \in R^\times$, if $\alpha(R^\times)^p \in \tilde{H}$, then $\alpha = \gamma^p$ such that $\partial\gamma \in \text{Sym}_K^2(R)$. This means that

$$\tilde{H} = \frac{\{\alpha \in R^\times : \partial\alpha \in (\text{Sym}_K^2(R)^\times)^p\}}{(R^\times)^p},$$

and we can compute \tilde{H}_S , the image of H_S , as a subgroup of $R(S, p)$. (There is another description of \tilde{H} that for $p > 3$ uses smaller fields, and it only requires checking for p th powers in fields of degree at most $p^2 - 1$; compare [ScSt].)

Note also that given $\alpha \in R^\times$ representing an element of \tilde{H} , we find ρ representing the corresponding element of H as $\rho = \sqrt[p]{\partial\alpha}$. By the characterization of \tilde{H} , the root exists, and since $H \cong \tilde{H}$, it does not matter which root we take if there is a choice (as long as it is symmetric and a cocycle, i.e., $\partial\rho = 1$); they will all represent the same element of H .

For the realization of δ , consider the following diagram.

$$\begin{array}{ccccccc}
0 & \longrightarrow & E[p] & \longrightarrow & E & \xrightarrow{p} & E \longrightarrow 0 \\
& & \downarrow e & & \downarrow G & & \downarrow F \\
0 & \longrightarrow & \mu_p(\bar{R}) & \longrightarrow & \bar{R}^\times & \xrightarrow{p} & \bar{R}^\times \longrightarrow 0
\end{array}$$

Here, $F \in R(E)^\times$ is the function such that $F_T(pQ) = G_T(Q)^p$ for $T \in E[p]$. We find that the divisor of F_T is $p \cdot T - p \cdot O$, and if $F(pQ) = G(Q)^p$ with $G \in R(E)^\times$, then F induces a well-defined map $F : E(K) \setminus E[p] \longrightarrow R^\times / (R^\times)^p$, independent of the particular choice of F . Tracing through the definitions shows:

Proposition 2.6. *The composition $E(K) \xrightarrow{\delta} H^1(K, E[p]) \longrightarrow R^\times / (R^\times)^p$ is given by F on $E(K) \setminus E[p]$.*

Again, this is functorial in K , and so we can use it for the local maps δ_v . The algorithm for computing $\text{Sel}^{(p)}(K, E)$ then works as before, but now working within R instead of $\text{Sym}_K^2(R)$.

Theorem 2.7. *Let p be a prime number. There is an algorithm that computes $\text{Sel}^{(p)}(K, E)$, which is efficient modulo computation of class and unit groups in the number fields $K(T)$, where T runs through points of order p on E .*

3. CONSTRUCTING GEOMETRIC REPRESENTATIONS OF SELMER GROUP ELEMENTS

Our goal in the following will be to find explicitly the n -coverings corresponding to given elements of the n -Selmer group. We assume that we have realized the Selmer group as a subgroup of

$$H = \frac{\ker(\partial \mid \text{Sym}_K^2(R)^\times)}{\partial R^\times}.$$

In practice, $n = p$, and we will have computed the p -Selmer group as a subgroup of $\tilde{H} \subset R^\times / (R^\times)^p$, but we can easily transfer this to H , by the map $\alpha \mapsto \sqrt[p]{\partial \alpha}$ on representatives.

We first need to explain the connection between our third and fourth interpretations of elements of $H^1(K, E[n])$ in some detail. By the general theory of central group extensions, theta groups are classified by the G_K -equivariant symmetric 2-cocycles in $Z^2(E[n], \bar{K}^\times)$, modulo the coboundaries of G_K -equivariant 1-cochains. The correspondence is as follows. First note that for every theta group

$$0 \longrightarrow \mathbb{G}_m \xrightarrow{\alpha} \Theta \longrightarrow E[n] \longrightarrow 0,$$

there is a K -defined set-theoretic section $E[n](\bar{K}) \longrightarrow \Theta(\bar{K})$ (equivalently, a morphism $E[n] \rightarrow \Theta$ of K -schemes that is a section to $\Theta \rightarrow E[n]$). To see this,

pick any section $s : E[n](\bar{K}) \rightarrow \Theta(\bar{K})$; then for any $\sigma \in G_K$, s^σ/s gives a map $E[n](\bar{K}) \rightarrow \bar{K}^\times$, which (as a function of σ) is a cocycle, hence can be interpreted as an element of $Z^1(K, \bar{K}^\times)$. Now $H^1(K, \bar{K}^\times) = 0$, so there is some map $t : E[n](\bar{K}) \rightarrow \bar{K}^\times$ such that $s^\sigma(T)t^\sigma(T) = s(T)t(T)$; replacing s by st therefore yields a K -defined section.

Given such a section s , we obtain a K -defined 2-cocycle $\phi : E[n](\bar{K})^2 \rightarrow \bar{K}^\times$ by setting $\phi(T_1, T_2) = \alpha^{-1}(s(T_1)s(T_2)s(T_1 + T_2)^{-1})$. Changing the section s amounts to a change of ϕ by the coboundary of a K -defined 1-cochain. The commutator condition translates into $\phi(T_1, T_2) = e_n(T_1, T_2)\phi(T_2, T_1)$.

Now if we fix a K -defined section $\tilde{\chi}_E : E[n](\bar{K}) \rightarrow \Theta_E(\bar{K}) \subset \mathrm{GL}_n(\bar{K})$, then we obtain a 2-cocycle ε in the way described for a general theta group. Then the “difference” ϕ/ε will be a *symmetric* 2-cocycle, since the commutator condition cancels.

If n is odd, then there is a specific way of choosing a lift $\tilde{\chi}_E$ such that ε becomes a power of the Weil pairing e_n ; in fact, $\varepsilon = e_n^k$ such that $2k \equiv 1 \pmod{n}$.

Given a symmetric 2-cocycle ρ , we get from Θ_E to Θ_ρ by “twisting” the multiplication in Θ_E by ρ . Writing (T, λ) for the element $\lambda\tilde{\chi}_E(T)$, the multiplication in Θ_E is

$$(T_1, \lambda_1)(T_2, \lambda_2) = (T_1 + T_2, \lambda_1\lambda_2\varepsilon(T_1, T_2)),$$

whereas the multiplication in Θ_ρ will be

$$(T_1, \lambda_1)(T_2, \lambda_2) = (T_1 + T_2, \lambda_1\lambda_2\rho(T_1, T_2)\varepsilon(T_1, T_2)).$$

Now, our definition of the maps ∂ was exactly such that they correspond to the coboundary maps in the standard cochain complex

$$C^1(E[n], \bar{K}^\times) \xrightarrow{\partial} C^2(E[n], \bar{K}^\times) \xrightarrow{\partial} C^3(E[n], \bar{K}^\times).$$

Therefore, the elements of H represent exactly the K -defined symmetric 2-cocycles modulo the coboundaries of K -defined 1-cochains. Tracing through the definitions, we see that the theta group Θ_ρ corresponds to the same element of $H^1(K, E[n])$ as the image of ρ in H .

Recall the obstruction map

$$\mathrm{Ob} : H^1(K, E[n]) \rightarrow H^1(K, \mathrm{PGL}_n) \cong H^2(K, \mu_n) = \mathrm{Br}(K)[n].$$

In our second interpretation, it was given by mapping $C \rightarrow S$ to the element of $H^1(K, \mathrm{PGL}_n)$ corresponding to the twist S of \mathbb{P}^{n-1} . From this it is obvious that $\mathrm{Ob} = \chi_{E,*}$ is the map induced by $\chi_E : E[n] \rightarrow \mathrm{PGL}_n$ on cohomology. (χ_E was defined in Section 1.3 in the course of discussing the “third interpretation” of the Selmer group elements.)

Now $H^1(K, \mathrm{PGL}_n)$ also classifies K -isomorphism classes of *central simple algebras* of dimension n^2 over K ; these are twists of the matrix algebra $\mathrm{Mat}_n(K)$. Therefore, one possible way of representing the obstruction explicitly is through the

construction of the corresponding central simple algebra. Given a theta group Θ , we obtain this in a very simple way: observe that the set \bar{A}_Θ of all linear combinations of elements of Θ (where we use the scalar multiplication coming from the theta group structure) is in a natural way a \bar{K} -algebra of dimension n^2 carrying an action of G_K (we simply extend the multiplication we have on Θ linearly). We let A_Θ denote the K -algebra of G_K -invariant elements. For Θ_E , we obtain in this way the matrix algebra $\text{Mat}_n(\bar{K})$ with its usual G_K -action; this is because Θ_E naturally sits inside GL_n and spans the matrix algebra. The \bar{K} -isomorphism between Θ_E and Θ extends to a \bar{K} -isomorphism between $\text{Mat}_n(\bar{K})$ and \bar{A}_Θ , showing that A_Θ is indeed a central simple K -algebra. It is then obvious that A_Θ corresponds to $\text{Ob}(\Theta)$.

As an aside, note that there is a completely natural and coordinate-free K -defined isomorphism

$$\langle \Theta_E \rangle \xrightarrow{\cong} \text{End}(L(n \cdot O))$$

given by identifying Θ_E with the set of pairs (T, f_T) as before and using their action on $L(n \cdot O)$.

How do we realize the central simple algebra $\text{Ob}(\xi)$ in terms of $\rho \in \text{Sym}_K^2(R)^\times$ representing $\xi \in H^1(K, E[n])$? Note that once we fix a section $s : E[n] \rightarrow \Theta$, the elements of $A_\Theta = \langle \Theta \rangle^{G_K}$ are identified with K -equivariant maps $E[n] \rightarrow \bar{K}$ and therefore can be viewed as elements of R . The map is

$$A_\Theta \ni \sum_T z(T)s(T) \mapsto (z : T \mapsto z(T)) \in R.$$

Therefore, we can use R as the underlying K -vector space, and we only have to define a new multiplication. Let us do it first with Θ_E . From the definitions, we get that the multiplication on $A = A_{\Theta_E}$ must be defined by

$$z_1 *_{\varepsilon} z_2 = (T \mapsto \sum_{T_1+T_2=T} \varepsilon(T_1, T_2) z_1(T_1) z_2(T_2)).$$

In general, for $A_\rho = A_{\Theta_\rho}$, we define the multiplication as

$$z_1 *_{\varepsilon\rho} z_2 = (T \mapsto \sum_{T_1+T_2=T} \varepsilon(T_1, T_2) \rho(T_1, T_2) z_1(T_1) z_2(T_2)).$$

Proposition 3.1. *Let $\rho = \partial\gamma$ with $\gamma \in \bar{R}^\times$. Then in the realizations given above, a \bar{K} -isomorphism between A_ρ and A is given by*

$$\phi_\gamma : \bar{A}_\rho \ni z \mapsto \gamma z \in \bar{A},$$

where the multiplication is that of $\bar{R}(!)$.

PROOF: We compute

$$\begin{aligned} \phi_\gamma(z_1 *_{\varepsilon\rho} z_2) &= (T \mapsto \gamma(T) \sum_{T_1+T_2=T} \varepsilon(T_1, T_2) \rho(T_1, T_2) z_1(T_1) z_2(T_2)) \\ &= (T \mapsto \sum_{T_1+T_2=T} \varepsilon(T_1, T_2) \gamma(T_1) z_1(T_1) \gamma(T_2) z_2(T_2)) \\ &= \phi_\gamma(z_1) *_{\varepsilon} \phi_\gamma(z_2). \end{aligned}$$

□

REMARK: One can view A and A_ρ as twisted versions of the group algebra of $E[n]$. The group algebra (over \bar{K}) is \bar{R} , with convolution as multiplication:

$$z_1 * z_2 = (T \mapsto \sum_{T_1+T_2=T} z_1(T_1) z_2(T_2)).$$

We can also consider the G_K -invariant subalgebra $(R, *)$. Now it turns out that $(R, *)$ is actually isomorphic to (R, \cdot) (i.e., with point-wise multiplication). This isomorphism is given by “Fourier transform” in the following way. Define

$$\bar{R} \ni \alpha \mapsto \left(\hat{\alpha} : T \mapsto \frac{1}{n^2} \sum_S e_n(T, S) \alpha(S) \right) \in \bar{R}.$$

Then one can easily check that $\widehat{\alpha\beta} = \hat{\alpha} * \hat{\beta}$ and that $\hat{\alpha} = \alpha/n^2$. Furthermore, $\hat{\cdot}$ is defined over K , so it gives an isomorphism $(R, \cdot) \xrightarrow{\cong} (R, *)$.

We get $A = (R, *_{\varepsilon})$ by twisting convolution in such a way that commutators on the image of $E[n]$ evaluate to the Weil pairing.

Now suppose that ρ represents an element ξ in the n -Selmer group. Then we know that the obstruction vanishes, hence there is an isomorphism $\iota : A_\rho \xrightarrow{\cong} \text{Mat}_n(K)$. Given such an isomorphism, we can write the cocycle representing $\text{Ob}(\xi) \in H^1(K, \text{PGL}_n)$ explicitly as a coboundary. In the diagram below, we obtain an automorphism (over \bar{K}) of Mat_n , which must be conjugation by some matrix $M \in \text{GL}_n(\bar{K})$.

$$\begin{array}{ccc} \bar{A}_\rho & \xrightarrow{\iota} & \text{Mat}_n \\ \downarrow \phi_\gamma & & \downarrow M \\ \bar{A} & \xrightarrow{\cong} & \text{Mat}_n \end{array}$$

We can find M (which is well-defined up to a multiplicative constant) from the automorphism by linear algebra.

Proposition 3.2. *We have that for all $\sigma \in G_K$,*

$$\mathbb{P}(M^\sigma M^{-1}) = \chi_E(\xi_\sigma).$$

Here $\mathbb{P}(X)$ denotes the image of $X \in \text{GL}_n$ in PGL_n .

PROOF: The map labeled M in the diagram above is $X \mapsto MXM^{-1}$. Applying σ to the diagram, we see that on the one hand, by the bottom isomorphism,

$$z \frac{\gamma^\sigma}{\gamma} \mapsto \sum_T z(T) \frac{\gamma^\sigma}{\gamma}(T) \tilde{\chi}_E(T) = \sum_T z(T) e_n(\xi_\sigma, T) \tilde{\chi}_E(T).$$

(Recall that in our fourth interpretation, $e(\xi_\sigma) = \gamma^\sigma/\gamma$, where $\partial\gamma = \rho$.) On the other hand, we need to have that

$$z \frac{\gamma^\sigma}{\gamma} \mapsto \sum_T z(T) M^\sigma M^{-1} \tilde{\chi}_E(T) M M^{-\sigma}.$$

Comparing these expressions shows that

$$M^\sigma M^{-1} \tilde{\chi}_E(T) = e_n(\xi_\sigma, T) \tilde{\chi}_E(T) M^\sigma M^{-1}$$

for all $T \in E[n]$. If we write $M^\sigma M^{-1} = X \tilde{\chi}_E(\xi_\sigma)$, then we find that X commutes with all $\tilde{\chi}_E(T)$ and therefore with all of Mat_n . Therefore X must be a scalar matrix, and

$$\mathbb{P}(M^\sigma M^{-1}) = \mathbb{P}(\tilde{\chi}_E(\xi_\sigma)) = \chi_E(\xi_\sigma).$$

□

From this, we can draw the following useful conclusion.

Corollary 3.3. *With the notations above, the second interpretation of an element $\xi \in \text{Sel}^{(n)}(K, E)$ can be realized in the form*

$$\begin{array}{ccc} C & \longrightarrow & \mathbb{P}^{n-1} \\ \downarrow & & \downarrow \\ E & \xrightarrow{|n \cdot O|} & \mathbb{P}^{n-1} \end{array}$$

Note that for $n \geq 3$, the horizontal arrows are embeddings, and so the map on the left is given by restriction of the map on the right.

PROOF: We note that by the previous proposition, the cocycle associated to the diagram is exactly ξ . □

In practical terms, this means that we make the linear change of variables corresponding to M^\top (acting on the right) in the equations of $E \subset \mathbb{P}^{n-1}$ to obtain equations for C .

However, recall that in order to find M , we need to actually *have* an isomorphism between A_ρ and $\text{Mat}_n(K)$. To find such an isomorphism explicitly is a nontrivial problem, even though we already know that such an isomorphism exists. When $n = 2$, this turns out to be equivalent to finding a K -rational point on a conic, knowing that it has points everywhere locally. The problem of “trivializing the algebra” that comes up here can be viewed as a generalization of this very classical problem.

At least in theory, the problem can be reduced to solving a norm equation (over K or some extension of K). In practice, however, the data defining the algebra structure on A_ρ can be very large (they come in the end from elements of $R(S, n)$ and often will involve units of the number fields occurring in R), making this approach impractical. On the other hand, at least when working over \mathbb{Q} , we have a method that seems to work very well in practice (at least when $n = 3$, which is the only case where the first step, the computation of the Selmer group as a group, can be carried out successfully), although we have so far not proved that it really always works. The idea is to first find a maximal order in A_ρ , which we know is isomorphic to $\text{Mat}_n(\mathbb{Z})$. Then we apply a certain reduction procedure with the goal of reducing the structure constants in size until they are small enough to read off an isomorphism.

Even though it is not immediately relevant to what we are doing in these lectures, I would like to mention the following.

Proposition 3.4.

- (1) *The obstruction map is even: $\text{Ob}(-\xi) = \text{Ob}(\xi)$.*
- (2) *The Weil pairing cup-product pairing*

$$\cup_e : H^1(K, E[n]) \times H^1(K, E[n]) \longrightarrow H^2(K, \mu_n)$$

can be expressed in terms of the obstruction map:

$$\xi \cup_e \eta = \text{Ob}(\xi + \eta) - \text{Ob}(\xi) - \text{Ob}(\eta).$$

In particular, Ob is a quadratic map:

$$\text{Ob}(m\xi) = m^2 \text{Ob}(\xi), \quad \text{Ob}(\xi + \eta) + \text{Ob}(\xi - \eta) = 2 \text{Ob}(\xi) + 2 \text{Ob}(\eta).$$

PROOF: (1) We get the diagram corresponding to $-\xi$ from the diagram corresponding to ξ by composing it with inversion on E :

$$\begin{array}{ccc} C & \longrightarrow & S \\ \downarrow & & \downarrow \\ E & \longrightarrow & \mathbb{P}^{n-1} \\ \downarrow -1 & & \downarrow \\ E & \longrightarrow & \mathbb{P}^{n-1} \end{array}$$

In particular, the Brauer-Severi variety for $-\xi$ is the same (namely S) as the one for ξ .

(2) This is a straight-forward, if somewhat tedious, verification using cocycles. \square

REMARK: There is another way of obtaining the model of C in \mathbb{P}^{n-1} (which is the one actually currently used in my 3-descent program). It roughly works as follows.

Instead of mapping $E \xrightarrow{\phi} \mathbb{P}^{n-1}$, we can also map to the dual curve, i.e., we send $P \in E$ to the point in $(\mathbb{P}^{n-1})^\vee$ corresponding to the osculating hyperplane at $\phi(P)$ (for $n = 3$, this is just the tangent line, for $n = 2$, it is $\phi(P) \in (\mathbb{P}^1)^\vee = \mathbb{P}^1$ itself). We can combine ϕ and this morphism $\phi^\vee : E \rightarrow (\mathbb{P}^{n-1})^\vee$ into a single morphism and then follow it by the Segre embedding, where we can identify \mathbb{P}^{n^2-1} with $\mathbb{P}(\text{Mat}_n)$ and the embedding with multiplication of column vectors by row vectors. The image of Segre is therefore the set of rank-1 matrices.

$$E \xrightarrow{(\phi, \phi^\vee)} \mathbb{P}^{n-1} \times (\mathbb{P}^{n-1})^\vee \xrightarrow{\text{Segre}} \mathbb{P}^{n^2-1} = \mathbb{P}(\text{Mat}_n)$$

The image of E in $\mathbb{P}(\text{Mat}_n)$ will also be contained in the hyperplane of trace-zero matrices; this corresponds to the fact that $\phi(P)$ is on the hyperplane $\phi^\vee(P)$.

Now there is a commutative diagram

$$\begin{array}{ccc} E & \xrightarrow{(\phi, \phi^\vee)} & \mathbb{P}^{n-1} \times (\mathbb{P}^{n-1})^\vee & \xrightarrow{\text{Segre}} & \mathbb{P}(\text{Mat}_n) \\ \downarrow G & & & & \uparrow \tilde{\chi}_E \\ \mathbb{P}(\bar{R}) & \dashrightarrow & \text{---} & \xrightarrow{t} & \mathbb{P}(\bar{R}) \end{array}$$

where $t \in R$ is a certain element satisfying $t(O) = 0$, $t(T) \neq 0$ for all $T \neq O$. For example, when $n = 3$ and $\tilde{\chi}_E$ is chosen so as to make $\varepsilon = e_3^2$, then $t(T) = 1/y(T)$ (w.r.t. a Weierstraß model of E).

Twisting by the cocycle represented by $\rho = \partial\gamma$, we obtain a model C_1 of C in $\mathbb{P}(\bar{R})$ as $\gamma^{-1} \cdot G(E)$. This can be computed explicitly in terms of ρ only: applying ∂ , we have

$$z \in C_1 \iff \gamma z \in G(E) \iff \rho \partial z \in r(E),$$

and the latter leads to quadratic equations in z , from which $r(E)$ can be eliminated. Then $t \cdot C_1$ will be contained in the rank-1, trace-0 locus of $\mathbb{P}(\bar{A}_\rho)$ (identifying underlying vector spaces). If we have an isomorphism $A_\rho \xrightarrow{\iota} \text{Mat}_n(K)$, then we obtain C by projecting $\iota(t \cdot C_1) \subset \mathbb{P}(\text{Mat}_n)$ to any nonzero column.

4. MINIMIZATION AND REDUCTION

I would like to come back to the diagram

$$\begin{array}{ccccccc} \mathbb{P}^1 & \xleftarrow{x} & E & \xleftarrow{\pi} & C & \xrightarrow{|D|} & S & \xrightarrow[\cong]{\iota} & \mathbb{P}^{n-1} \\ & & \parallel & & \downarrow \cong & & \downarrow \cong & & \\ & & E & \xleftarrow{n} & E & \xrightarrow{|n \cdot O|} & \mathbb{P}^{n-1} & & \end{array}$$

From this diagram, one can read off that $\pi^*(O) \sim nD$ as divisors on C . Now there is a theory of heights on varieties. For a very ample divisor D , one defines

$$h_D : C \xrightarrow{|D|} \mathbb{P}^N \xrightarrow{h} \mathbb{R}_{\geq 0}$$

via the logarithmic height on \mathbb{P}^N . This is well-defined up to bounded functions. The main facts are that this induces a homomorphism

$$\{\text{divisors on } C\} \longrightarrow \frac{\{\text{functions } C \rightarrow \mathbb{R}_{\geq 0}\}}{\{\text{bounded functions}\}}$$

and that it is compatible with dominant morphisms $C' \xrightarrow{\phi} C$ in the sense that

$$h_{\phi^*D} = h_D \circ \phi + O(1)$$

for divisors D on C .

So if $Q \in C(K)$ and $P = \pi(Q) \in E(K)$, we get that

$$\begin{aligned} h_D(Q) &= \frac{1}{n} h_{\pi^*O}(Q) + O(1) = \frac{1}{n} h_O(P) + O(1) \\ &= \frac{1}{2n} h_{2O}(P) + O(1) = \frac{1}{2n} h(x(P)) + O(1). \end{aligned}$$

So up to something bounded, going from E to C divides logarithmic heights by $2n$. Now, to really make use of this, one needs the “ $O(1)$ ” to be fairly small. How large the error is depends mainly on the size of the coefficients in the equations describing C (and E) — the smaller they are, the better. So we would like to choose coordinates on \mathbb{P}^{n-1} in such a way that C is described by small equations. There are two ways in which the equations can be large. The first is that the model is not minimal, i.e., it has unnecessary prime powers in its discriminant. So in a first step, one will try to remove these and obtain a minimal model. This step, called “minimization”, has been worked out in theory and practice for $n = 2, 3, 4$ and is being worked on for $n = 5$.

Then, assuming now that the model is minimal, we still can make coordinate changes by $\text{SL}_n(\mathbb{Z})$. So we would like to find such a coordinate change that makes the coefficients of our equations small. This step, called “reduction”, has been worked out (for this special case at least) in theory for all n , and is implemented for $n = 2, 3, 4$. For details, see [CFS].

There is an implementation in **MAGMA** (in its current form mostly due to Tom Fisher and Steve Donnelly) that computes the 3-Selmer group $\text{Sel}^{(3)}(\mathbb{Q}, E)$ (inside $R^\times / (R^\times)^3$) of an elliptic curve E over \mathbb{Q} . It then transfers the elements into H , finds the structure constants for the central simple algebras associated to them, computes an isomorphism with $\text{Mat}_3(\mathbb{Q})$, finds the equations for the model in \mathbb{P}^8 and then projects the model into \mathbb{P}^2 ; finally this is minimized and reduced. This program works quite well in practice for curves of moderate size and produces a list of curves corresponding to $(\text{Sel}^{(3)}(\mathbb{Q}, E) \setminus \{0\}) / \{\pm 1\}$. (Note that elements that are negatives of each other give rise to the same curve, which has two different structures as a principal homogeneous space for E .)

REFERENCES

- [CF] J.W.S. CASSELS, A. FRÖHLICH: *Algebraic number theory*, Academic Press, 1993.
- [CFOSS1] J.E. CREMONA, T.A. FISHER, C. O'NEIL, D. SIMON, M. STOLL: *Explicit n -descent on elliptic curves. I. Algebra*, J. reine angew. Math. **615**, 121–155 (2008).
- [CFOSS2] J.E. CREMONA, T.A. FISHER, C. O'NEIL, D. SIMON, M. STOLL: *Explicit n -descent on elliptic curves. II. Geometry*, J. reine angew. Math. **632**, 63–84 (2009).
- [CFOSS3] J.E. CREMONA, T.A. FISHER, C. O'NEIL, D. SIMON, M. STOLL: *Explicit n -descent on elliptic curves. III. Algorithms*, in preparation.
- [CFS] J.E. CREMONA, T.A. FISHER, M. STOLL: *Minimisation and reduction of 2-, 3- and 4-coverings of elliptic curves*, Algebra & Number Theory **4**, No. 6, 763–820 (2010).
- [DSS] Z. DJABRI, E.F. SCHAEFER, N. SMART: *Computing the p -Selmer group of an elliptic curve*, Trans. Amer. Math. Soc. **352**, 5583–5597 (2000).
- [ScSt] E.F. SCHAEFER, M. STOLL: *How to do a p -descent on an elliptic curve*, Trans. Amer. Math. Soc. **356**, 1209–1231 (2004).
- [Se1] J.-P. SERRE: *Local fields*, Springer GTM 67, Springer-Verlag, New York Berlin Heidelberg, 2nd corrected printing, 1995.
- [Se2] J.-P. SERRE: *Galois cohomology*, Springer-Verlag, Berlin Heidelberg, 1997.
- [Si1] J.H. SILVERMAN: *The arithmetic of elliptic curves*, Springer GTM 106, Springer-Verlag, Berlin Heidelberg New York Tokyo, 1986.
- [Si2] J.H. SILVERMAN: *Advanced topics in the arithmetic of elliptic curves*, Springer GTM 151, Springer-Verlag Berlin Heidelberg New York, 1994.

MATHEMATISCHES INSTITUT, UNIVERSITÄT BAYREUTH, 95440 BAYREUTH, GERMANY.

E-mail address: Michael.Stoll@uni-bayreuth.de