THE SELMER GROUP, THE SHAFAREVICH-TATE GROUP, AND THE WEAK MORDELL-WEIL THEOREM

BJORN POONEN

Abstract. This is an introduction to classical descent theory, in the context of abelian varieties over number fields.

1. Further reading

We begin by suggesting reference for readers who want to see more details than are presented in this article.

Here are some references for group cohomology, roughly in order of increasing depth: Appendix B to [Sil99], the articles by Atiyah & Wall and Gruenberg in [CF86], and the books [Ser79] and [Ser02].

Here are some references for the Mordell-Weil Theorem, and for the Selmer and Shafarevich-Tate groups, again roughly in order of increasing depth: Chapters 8 and 10 of [Sil99], the book [Ser97], the "Abelian varieties" article by Milne in [CS86], and the book [Mil86].

Also, many of these topics are covered in lecture notes of courses given by Milne, available at `www.jmilne.org` at no cost.

2. Group cohomology: H^0

Let G be a profinite group. Let A be a (discrete, left) G-module. This means that A is an abelian group on which G acts, and that the map $G \times A \to A$ is continuous when A is given the discrete topology. Define A^G and $\mathrm{H}^0(G, A)$ by

$$A^G = \mathrm{H}^0(G, A) := \{\, a \in A : ga = a \text{ for all } g \in G \,\}.$$

The subgroup A^G is known as the subgroup of *G-invariants* of A.

The following example demonstrates why this concept is important to us. Let k be a number field. Let $G = G_k := \mathrm{Gal}(\overline{k}/k)$ be the absolute Galois group of k. Let A be an abelian variety[1] over k. Then G_k acts on the abelian group $A(\overline{k})$. The abbreviation $\mathrm{H}^0(k, A)$ is commonly used for $\mathrm{H}^0(G_k, A(\overline{k}))$. By Galois theory, $\mathrm{H}^0(k, A) = A(k)$, where $A(k)$ is the group of k-rational points on A, also known as the *Mordell-Weil group* of A.

Mordell-Weil Theorem. *The group $A(k)$ is a finitely generated abelian group.*

In other words $A(k) \simeq \mathbf{Z}^r \oplus T$, where r is a nonnegative integer, and T is a finite abelian group. The integer r is called the *rank* of A over k. The group T is called the *torsion subgroup*, because it consists of the set of elements of $A(k)$ of finite order. There exists an algorithm for computing T in theory, and this algorithm is practical at least when A is an

Date: February 20, 2002.

The writing of this article was supported by NSF grant DMS-9801104, and a Packard Fellowship. It is based on a series of two lectures given at the Arizona Winter School on March 13–14, 1999.

[1]Readers unfamiliar with abelian varieties can replace "abelian variety" with "elliptic curve" throughout this article. A better solution is to become familiar with abelian varieties by reading Milne's articles in [CS86]!

elliptic curve. There is no such algorithm currently known for computing r, even in theory. More precisely, there is a candidate for an algorithm, based on ideas to be discussed later in this article, but it terminates only if the p-primary part of a certain group $Ш(A)$ is finite for some prime p.

Given an abelian group B and a positive integer m, use the abbreviation B/m for B/mB. The Mordell-Weil Theorem implies the following.

Weak Mordell-Weil Theorem. *If $m \geq 2$, then $A(k)/m$ is finite.*

The only known proof of the Mordell-Weil Theorem involves combining the Weak Mordell-Weil Theorem (one $m \geq 2$ suffices) with the theory of height functions. If one can determine the size of $A(k)/m$ for some integer $m \geq 2$, then one can determine the rank of $A(k)$.

3. Group cohomology: H^i for all $i \geq 0$

Suppose that

$$0 \to A \to B \to C \to 0$$

is an exact sequence of G-modules. This means that the morphisms respect the G-actions, and that it is exact as a sequence of abelian groups. Then there is an exact sequence

$$0 \to A^G \to B^G \to C^G \tag{1}$$

but one cannot always append $\to 0$ to the right end. In other words, the functor $A \mapsto A^G$ is only *left exact*. To help understand what happens past the right end, we have the following:

Theorem 1. *There exists a collection of functors $\mathrm{H}^i(G, -)$ for $i \geq 0$ such that for every exact sequence*

$$0 \to A \to B \to C \to 0$$

of G-modules, the sequence (1) extends to a long exact sequence

$$\begin{aligned} 0 \to &\mathrm{H}^0(G, A) \to \mathrm{H}^0(G, B) \to \mathrm{H}^0(G, C) \to \\ &\mathrm{H}^1(G, A) \to \mathrm{H}^1(G, B) \to \mathrm{H}^1(G, C) \to \\ &\mathrm{H}^2(G, A) \to \cdots, \end{aligned}$$

functorially with respect to the exact sequence.

"Functorially" means that given a morphism of exact sequences, that is, a commutative diagram such as

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0, \end{array}$$

there is a morphism of the associated long exact sequences; that is, the diagram

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & \mathrm{H}^0(G, A) & \longrightarrow & \mathrm{H}^0(G, B) & \longrightarrow & \mathrm{H}^0(G, C) & \longrightarrow & \mathrm{H}^1(G, A) & \longrightarrow & \dots \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathrm{H}^0(G, A') & \longrightarrow & \mathrm{H}^0(G, B') & \longrightarrow & \mathrm{H}^0(G, C') & \longrightarrow & \mathrm{H}^1(G, A') & \longrightarrow & \dots \end{array}$$

commutes.

One way to define $\mathrm{H}^i(G,A)$ is to first define i-cochains, i-cocyles, and i-coboundaries, and then to set

$$\mathrm{H}^i(G,A) = \frac{\{i\text{-cocycles}\}}{\{i\text{-coboundaries}\}}.$$

When $i=1$, a 1-*cocycle* is a continuous function $\xi : G \to A$ such that $\xi_{gh} = \xi_g + g\xi_h$ for all $g,h \in G$. (Here $\xi_g := \xi(g) \in A$.) And a 1-coboundary is a function $G \to A$ of the form $g \mapsto ga - a$ determined by some $a \in A$. For the origins of these funny expressions, their generalizations to $i > 1$, and other constructions of the functors $\mathrm{H}^i(G,-)$ making the theorem true, see the article of Atiyah and Wall in [CF86]. In some sense, however, the characterization given by the theorem is more important than the actual definition.

If G acts trivially on A, then $\mathrm{H}^1(G,A) = \mathrm{Hom}_{\mathrm{conts}}(G,A)$, the group of continuous homomorphisms from G to A. In general, if G is any profinite group, A is any G-module, and $i \geq 1$, then $\mathrm{H}^i(G,A)$ is a *torsion* abelian group, which means that each element has finite order. *Hilbert's Theorem 90* states that if k is a perfect field, then $\mathrm{H}^1(G_k, \overline{k}^*) = 0$. (This holds even if k is not perfect, but then one usually replaces $\overline{k}$ by the separable closure k^s, and writes $G_k = \mathrm{Gal}(k^s/k)$.)

Exercise. Use Hilbert's Theorem 90 to show that if m is an integer not divisible by the characteristic of k, and μ_m denotes the group of m^{th} roots of unity, then $\mathrm{H}^1(G_k, \mu_m) \simeq k^*/k^{*m}$.

4. Restriction

If $H \subseteq G$ is a closed subgroup, and A is a G-module, then A can also be considered as an H-module, and there exist *restriction* homomorphisms

$$\mathrm{H}^i(G,A) \xrightarrow{\mathrm{Res}} \mathrm{H}^i(H,A)$$

for each $i \geq 0$. On H^0, Res is simply the inclusion $A^G \hookrightarrow A^H$. On H^1, Res maps the class of the 1-cocycle $\xi : G \to A$ to the class of $\xi|_H : H \to A$.

For us, the following special case will be important. Let k be a number field. Let k_v denote the completion of k at a place v. If we identify $\overline{k}$ with the algebraic closure of k inside $\overline{k}_v$, then we have an injection

$$\begin{aligned} G_v := \mathrm{Gal}(\overline{k}_v/k_v) &\hookrightarrow G_k := \mathrm{Gal}(\overline{k}/k) \\ \sigma &\mapsto \sigma|_{\overline{k}} \end{aligned}$$

whose image is a decomposition group at v. Let A be an abelian variety over k. The composition

$$\mathrm{H}^1(k,A) := \mathrm{H}^1(G_k, A(\overline{k})) \xrightarrow{\mathrm{Res}} \mathrm{H}^1(G_v, A(\overline{k})) \to \mathrm{H}^1(G_v, A(\overline{k}_v)) =: \mathrm{H}^1(k_v, A)$$

is denoted Res_v.

5. Twists (also known as k-forms)

"Twists of an object over a field are classified by H^1 of its automorphism group over the algebraic closure." This is not a theorem, because we have not and will not make completely precise what we mean by an object. It is only a vague principle, but nevertheless it holds in many common situations in arithmetic geometry.

We now elaborate a little (but still not being completely precise). Let k be a perfect field. Let V be an object over k, for example a variety equipped with some extra structure defined

over k. We assume that the objects form a category, and that there is a notion of base extension: that is, given an object V over k and a field extension L of k, there should be an associated object V_L over L. A *twist* or *k-form* of V is an object W over k such that there exists a (structure-preserving) isomorphism $W_{\overline{k}} \simeq V_{\overline{k}}$ of objects over $\overline{k}$. Then there is an injection

$$\{\text{twists of } V\} \quad \hookrightarrow \quad \mathrm{H}^1(G_k, \mathrm{Aut}(V_{\overline{k}}))$$

that in many situations is a bijection. Where we write "twists of V" we identify two twists if they are isomorphic over k. The group $\mathrm{Aut}(V_{\overline{k}})$ is the group of automorphisms of $V_{\overline{k}}$ as an object over $\overline{k}$. This group may be nonabelian, hence not a G_k-module, but it turns out that the definition of H^1 can be generalized [Ser02, I.§5], to define $\mathrm{H}^1(G_k, \mathrm{Aut}(V_{\overline{k}}))$ not as a group, but as a pointed set (i.e., a set equipped with a special "zero element").

The injection is defined as follows. Suppose that W is a twist of V over k. Fix an isomorphism $\phi : W_{\overline{k}} \to V_{\overline{k}}$. Then for $g \in G_k$, we apply g to obtain another isomorphism ${}^g\phi : W_{\overline{k}} \to V_{\overline{k}}$. Then the 1-cocycle $g \mapsto {}^g\phi \circ \phi^{-1} \in \mathrm{Aut}(V_{\overline{k}})$ represents an element of $\mathrm{H}^1(G_k, \mathrm{Aut}(V_{\overline{k}}))$.

6. Torsors (also known as principal homogeneous spaces)

Let A be an abelian variety over a perfect field k. A *homogeneous space* of A over k is a variety X over k equipped with a transitive action of A, that is, a morphism $A \times X \to X$ for which the induced action of $A(\overline{k})$ on $X(\overline{k})$ is transitive. A *principal homogeneous space* of A over k is a homogeneous space X such that for each $x_1, x_2 \in X(\overline{k})$ there is a *unique* $a \in A(\overline{k})$ mapping x_1 to x_2. Principal homogeneous spaces of A over k are also known as *k-torsors under A*.

Let $\mathbb{A}$ denote the abelian variety A equipped with the additional structure of an A-action given by the group law morphism $A \times \mathbb{A} \to \mathbb{A}$. Then $\mathbb{A}$ is a k-torsor under A. Moreover, the twists of $\mathbb{A}$ *as a k-torsor under A* are exactly the k-torsors under A. Let us apply the vague principle of the previous section. The automorphisms of $\mathbb{A}_{\overline{k}}$ are precisely the translation maps $\mathbb{A}_{\overline{k}} \to \mathbb{A}_{\overline{k}}$ given by $a \mapsto a + b$ associated to each $b \in A(\overline{k})$. It turns out that the injection given by the vague principle for this situation is a bijection, so that we have

$$\{k\text{-torsors under } A\} \quad \longleftrightarrow \quad \mathrm{H}^1(G_k, A(\overline{k})) =: \mathrm{H}^1(k, A).$$

A k-torsor X under A satisfying any of the following equivalent conditions is said to be *trivial*:

(1) $X \simeq \mathbb{A}$ (as torsors)
(2) $X(k)$ is nonempty.
(3) X corresponds to $0 \in \mathrm{H}^1(k, A)$.

It sometimes helps to visualize torsors with the following analogy: abelian varieties are to torsors as vector spaces V are to affine translates of V (in some larger vector space W).

Let X be a smooth, projective, geometrically integral curve of genus 1 over a field k. Let E be its jacobian, which is an elliptic curve over k (that is, a one-dimensional abelian variety over k, or equivalently, a genus 1 curve equipped with a k-rational point). Then X is a k-torsor under E. Thus the classification of genus 1 curves over k reduces to the classification of elliptic curves over k (the easy part) together with an understanding of $\mathrm{H}^1(k, E)$ for each elliptic curve over k (the hard part).

The group $\mathrm{H}^1(k, A)$ classifying torsors under A is understood well for certain types of fields k, and not so well for others:

(1) If k is a finite field, then $\mathrm{H}^1(k, A) = 0$. This is a theorem of Lang, and it holds more generally when A is any connected group variety over a finite field k.
(2) If k_v is a local field (say, the completion of a number field at a place), then $\mathrm{H}^1(k_v, A) \simeq \mathrm{Hom}_{\mathrm{conts}}(A^\vee(k_v), \mathbf{Q}/\mathbf{Z})$, where $A^\vee$ is the dual abelian variety. This fact is known as *Tate local duality*.
(3) If k is a number field, $\mathrm{H}^1(k, A)$ is big and difficult to understand. There is no known algorithm that decides, given a k-torsor X under A, whether X corresponds to $0 \in \mathrm{H}^1(k, A)$ (or equivalently, whether $X(k)$ is nonempty). It has not even been proved yet that there is an algorithm in the case where A is an elliptic curve over $\mathbf{Q}$.

7. The Shafarevich-Tate group

From now on, we assume that k is a number field, and that A is an abelian variety over k. Recall that there is a restriction map $\mathrm{Res}_v : \mathrm{H}^1(k, A) \to \mathrm{H}^1(k_v, A)$ for each place v of k (finite or infinite). If we identify elements of H^1 with torsors, then Res_v takes a k-torsor X under A to the base extension $X \times_k k_v$. Define the *Shafarevich-Tate group* $Ш(k, A)$ of A over k as

$$\ker \left[\mathrm{H}^1(k, A) \xrightarrow{\mathrm{Res}} \prod_{\text{places } v \text{ of } k} \mathrm{H}^1(k_v, A) \right],$$

where $\mathrm{Res} = \prod_v \mathrm{Res}_v$.

Call a k-torsor X under A *locally trivial* if it is in the kernel of every map Res_v, or equivalently if $X(k_v)$ is nonempty for every v. Then one can describe $Ш(k, A)$ geometrically as the set of isomorphism classes of locally trivial k-torsors X under A.

In general, given a smooth, projective, geometrically integral variety X over a number field k, it is possible to compute a finite set S of places of k such that $X(k_v)$ is guaranteed to be nonempty for $v \notin S$. (Sketch of proof: choose a model for X that is smooth over a ring of S-integers in k for some S containing all the archimedean places, and enlarge S by including enough of the small nonarchimedean primes that the Weil conjectures force the mod v reduction to have points over the residue field for each of the large primes $v \notin S$. Then Hensel's Lemma lifts these points to points in $X(k_v)$.) Also, for each $v \in S$, one can decide whether or not $X(k_v)$ is nonempty. (Sketch: for $k_v = \mathbf{C}$, $X(k_v)$ is automatically nonempty. For $k_v = \mathbf{R}$, one can use elimination of quantifiers for semialgebraic sets. For k_v nonarchimedean, write down equations for X and clear denominators so that the coefficients lie in the valuation ring of k_v; search for solutions to the equations modulo higher and higher powers of the maximal ideal; either one will eventually reach a power modulo which there are no solutions, or one will find an approximate point that is so close v-adically that one can use Hensel's Lemma to lift it to an exact solution in k_v.) Applying this to torsors shows that there is an algorithm to test whether a k-torsor X under A is locally trivial. On the other hand, it is not known how to decide whether a k-torsor X under A is trivial.

A variety X over a number field k is said to *violate the Hasse principle* if $X(k_v)$ is nonempty for all v but $X(k)$ is empty. Then a k-torsor X under A violates the Hasse principle if and only if it corresponds to a nonzero element of $Ш(k, A)$. For example, suppose that X is the projective plane curve over $\mathbf{Q}$ defined by the homogeneous equation $3x^3 + 4y^3 + 5z^3 = 0$. The genus of X is $(3-1)(3-2)/2 = 1$. Clearly $X(\mathbf{R})$ is nonempty, and using Hensel's Lemma, it is easy to show that $X(\mathbf{Q}_p)$ is nonempty for each prime p. On the other hand, with some

work one can show that $X(\mathbf{Q})$ is empty, so X violates the Hasse principle. Thus, if E is the jacobian of X, then X represents a nonzero element of $Ш(\mathbf{Q}, E)$.

Conjecture. For every number field k and every abelian variety A over k, the group $Ш(k, A)$ is finite.

This conjecture has been proved in some special cases, for instance if A is an elliptic curve over $\mathbf{Q}$ and the L-function of A over $\mathbf{Q}$ has a zero of order at most 1 at $s = 1$.

Remark. There is an analogy between abelian varieties and unit groups. Let $\mathcal{O}_{\overline{k}}$ denote the ring of algebraic integers in $\overline{k}$. Then $\mathrm{H}^0(k, \mathcal{O}_{\overline{k}}^*)$ is the group of units in the ring of integers of k. Dirichet's Unit Theorem states that this group is finitely generated; this can be viewed as the analogue of the Mordell-Weil Theorem, which states that $\mathrm{H}^0(k, A) = A(k)$ is finitely generated.

For each nonarchimedean place v of k, extend the v-adic absolute value $|\ |_v$ to $\overline{k}_v$, and let $\mathcal{O}_{\overline{k}_v}$ be the (non-discrete) valuation ring $\{\, \alpha \in \overline{k}_v : |\alpha|_v \leq 1 \,\}$. For each archimedean place v of k, let $\mathcal{O}_{\overline{k}_v} = \overline{k}_v$. Then

$$\ker \left[\mathrm{H}^1(k, \mathcal{O}_{\overline{k}}^*) \xrightarrow{\mathrm{Res}} \prod_v \mathrm{H}^1(k_v, \mathcal{O}_{\overline{k}_v}^*) \right] \quad \simeq \quad \mathrm{Cl}(k),$$

the class group of k. This suggests that $Ш(k, A)$ is an analogue of $\mathrm{Cl}(k)$. The finiteness of $\mathrm{Cl}(k)$ can be proved using the geometry of numbers (e.g., Minkowski's theorem on lattice points in convex symmetric regions). Is there a geometry of numbers approach to proving the finiteness of $Ш(k, A)$?

8. The Selmer group

Fix an integer $m \geq 2$. For any abelian group B, let B_m denote the kernel of the multiplication-by-m map $B \to B$. Suppose that A is an abelian variety over a perfect field k. Then the m-torsion subgroup of A is the G_k-module $A_m := A(\overline{k})_m$. The long exact sequence associated to

$$0 \to A_m \to A(\overline{k}) \xrightarrow{m} A(\overline{k}) \to 0$$

is

$$0 \to A(k)_m \to A(k) \xrightarrow{m} A(k) \to \mathrm{H}^1(k, A_m) \to \mathrm{H}^1(k, A) \xrightarrow{m} \mathrm{H}^1(k, A),$$

from which we extract the top row of

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \dfrac{A(k)}{m} & \longrightarrow & \mathrm{H}^1(k, A_m) & \xrightarrow{\rho} & \mathrm{H}^1(k, A)_m & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle \mathrm{Res}} & \searrow^{\tilde{\rho}} & \downarrow{\scriptstyle \mathrm{Res}} & & \\ 0 & \longrightarrow & \displaystyle\prod_v \frac{A(k_v)}{m} & \longrightarrow & \displaystyle\prod_v \mathrm{H}^1(k_v, A_m) & \longrightarrow & \displaystyle\prod_v \mathrm{H}^1(k_v, A)_m & \longrightarrow & 0. \end{array} \tag{2}$$

The bottom row is the product of the analogous sequences over each completion k_v. The first vertical map is induced by the inclusions $A(k) \hookrightarrow A(k_v)$ for each v, and the other vertical maps are restriction maps. The diagonal dotted map $\tilde{\rho}$ is the composition in either direction. The diagram commutes.

If we could prove that $\mathrm{H}^1(k, A_m)$ were finite, then (2) would show that $A(k)/m$ is finite too, and we would have proved the Weak Mordell-Weil Theorem. But unfortunately, it turns

out that $\mathrm{H}^1(k, A_m)$ is infinite whenever A is nonzero. Therefore we must bound the image of $A(k)/m$ in $\mathrm{H}^1(k, A_m)$ by using (2) to see that this image equals $\ker(\rho)$. Unfortunately, it is not known how to decide, given an element of $\mathrm{H}^1(k, A_m)$, whether its image in $\mathrm{H}^1(k, A)_m$ is zero or not, just as it is not known how to decide whether a general element of $\mathrm{H}^1(k, A)$ is zero or not. Therefore we instead bound $\ker(\rho)$ by the larger group $\ker(\tilde{\rho})$: this helps, since given $\xi \in \mathrm{H}^1(k, A_m)$, we can decide whether $\xi \in \ker(\tilde{\rho})$ as follows: compute a torsor X representing its image in $\mathrm{H}^1(k, A)$, and use the method discussed in the previous section to test whether X is locally trivial.

The *m-Selmer group* $\mathrm{Sel}^m(A/k)$ is defined as $\ker(\tilde{\rho})$, or equivalently as the set of $\xi \in \mathrm{H}^1(k, A_m)$ whose restriction $\mathrm{Res}_v \in \mathrm{H}^1(k_v, A_m)$ is in the image of $\frac{A(k_v)}{m} \to \mathrm{H}^1(k_v, A_m)$ for every v. If we apply the Snake Lemma to

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \dfrac{A(k)}{m} & \longrightarrow & \mathrm{H}^1(k, A_m) & \longrightarrow & \mathrm{H}^1(k, A)_m & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle \tilde{\rho}} & & \downarrow{\scriptstyle \mathrm{Res}} & & \\ 0 & \longrightarrow & 0 & \longrightarrow & \displaystyle\prod_v \mathrm{H}^1(k_v, A)_m & = & \displaystyle\prod_v \mathrm{H}^1(k_v, A)_m & \longrightarrow & 0, \end{array}$$

the first half of the snake (i.e., the sequence of kernels of the vertical maps) is the fundamental exact sequence

$$0 \to \frac{A(k)}{m} \to \mathrm{Sel}^m(A/k) \to Ш_m \to 0, \tag{3}$$

where $Ш := Ш(k, A)$. In particular, the image of $A(k)/m$ in $\mathrm{H}^1(k, A_m)$ is contained in $\mathrm{Sel}^m(A/k)$.

9. Computing the Selmer group

Theorem 2. *The group* $\mathrm{Sel}^m(A/k)$ *is finite and computable (in theory).*

This, together with (3), implies both the Weak Mordell-Weil Theorem and the finiteness of the m-torsion in Ш.

Corollary 3. *The groups* $A(k)/m$ *and* $Ш_m$ *are finite (but not necessarily computable).*

The reason that $A(k)/m$ and $Ш_m$ cannot be immediately computed from $\mathrm{Sel}^m(A/k)$ is that one still cannot decide how much of $\mathrm{Sel}^m(A/k)$ in (3) comes from $A(k)/m$, or equivalently how much of $\mathrm{Sel}^m(A/k)$ maps to 0 in $Ш_m$. Knowledge of the size of either $A(k)/m$ or $Ш_m$ could be used to deduce the size of the other, however.

We will sketch the proof of Theorem 2, but first we need a few definitions. Let k_v^{unr} denote the maximal unramified extension of k_v in $\overline{k}_v$. Let $I_v := \mathrm{Gal}(\overline{k}_v/k_v^{\mathrm{unr}}) \subseteq \mathrm{Gal}(\overline{k}_v/k_v)$ be the inertia group at v. An element $\xi \in \mathrm{H}^1(k_v, A_m)$ or $\xi \in \mathrm{H}^1(k, A_m)$ is called *unramified* at v if and only if it restricts to 0 in $\mathrm{H}^1(k_v^{\mathrm{unr}}, A_m) = \mathrm{H}^1(I_v, A_m)$.

Brief sketch of proof of Theorem 2. Let S be a finite set of places of k containing

- the archimedean places,
- the finite primes where A has bad reduction, and
- the finite primes dividing m.

Recall that $\mathrm{Sel}^m(A/k)$ is the subgroup of $\xi \in \mathrm{H}^1(k, A_m)$ satisfying a local condition at each v, namely that ξ should map to 0 in $\mathrm{H}^1(k_v, A)_m$. We will first impose the conditions at the infinitely many $v \notin S$, and then impose the conditions at the finitely many $v \in S$. The proof boils down to the following facts.

(1) For $v \notin S$, an element ξ maps to 0 in $\mathrm{H}^1(k_v, A)_m$ if and only if ξ is unramified at v. Thus if we define

$$\mathrm{H}^1(k, A_m; S) := \{\, \xi \in \mathrm{H}^1(k, A_m) : \xi \text{ is unramified at all } v \notin S \,\},$$

then

$$\mathrm{Sel}^m(A/k) = \{\, \xi \in \mathrm{H}^1(k, A_m; S) : \xi \text{ maps to 0 in } \mathrm{H}^1(k_v, A)_m \text{ for all } v \in S \,\}.$$

(2) The group $\mathrm{H}^1(k, A_m; S)$ is finite and computable. The proof of this involves the Dirichlet Unit Theorem and the finiteness of $\mathrm{Cl}(L)$ for some finite extensions L of k.
(3) Given $\xi \in \mathrm{H}^1(k, A_m; S)$ there exists an algorithm for constructing a torsor X representing the image of ξ in $\mathrm{H}^1(k, A)$. Then, as discussed in earlier sections, we can test whether ξ maps to 0 in $\mathrm{H}^1(k_v, A)_m$, by testing whether $X(k_v)$ is nonempty for each $v \in S$.

□

The process of computing the Selmer group and using it to bound $A(k)/m$ is known as *descent*, because as a very special case it includes Fermat's "infinite descent" method for solving diophantine equations such as $x^4 + y^4 = z^2$. (Integer solutions to this equation give rational points on the genus 1 curve $X^4 + 1 = Z^2$; after choosing a rational point as origin, it becomes an elliptic curve of rank zero, as a Selmer group computation shows.)

10. 2-descent on an elliptic curve with rational 2-torsion

In this section we show how to compute $\mathrm{Sel}^2(A/k)$ in the case where $A = E$ is an elliptic curve over $\mathbf{Q}$ with $E_2 \subseteq E(\mathbf{Q})$. Then E has an equation

$$y^2 = (x - e_1)(x - e_2)(x - e_3)$$

where $e_1, e_2, e_3 \in \mathbf{Z}$ are distinct. Let $P_i = (e_i, 0) \in E(\mathbf{Q})$ and let O denote the identity of E (the point at infinity). Then

$$E_2 = \{O, P_1, P_2, P_3\} \simeq \mathbf{Z}/2 \times \mathbf{Z}/2 \simeq \mu_2 \times \mu_2$$

as $G_{\mathbf{Q}}$-modules, with $P_1 \leftrightarrow (1, -1)$ and $P_2 \leftrightarrow (-1, 1)$. By Kummer Theory (the exercise earlier in these notes, involving Hilbert's Theorem 90), $\mathrm{H}^1(\mathbf{Q}, \mu_2) \simeq \mathbf{Q}^*/\mathbf{Q}^{*2}$, so $\mathrm{H}^1(\mathbf{Q}, E_2) \simeq (\mathbf{Q}^*/\mathbf{Q}^{*2})^{\oplus 2}$. If p is a prime such that e_1, e_2, e_3 are distinct modulo p, then E has good reduction at p. Hence we may take as the set S of "bad places" in the previous section, the set consisting of the archimedean place ∞ and the primes dividing $2(e_1 - e_2)(e_2 - e_3)(e_3 - e_1)$. We then have the following facts (for the proof, see Chapter 10 of [Sil99]):

(1) If $\xi \in \mathrm{H}^1(\mathbf{Q}, E_2)$ corresponds to the image of (a, b) in $(\mathbf{Q}^*/\mathbf{Q}^{*2})^{\oplus 2}$ (where $a, b \in \mathbf{Q}^{*2}$), then ξ is unramified at a prime p if and only if p is unramified in the quadratic extensions $\mathbf{Q}(\sqrt{a})$ and $\mathbf{Q}(\sqrt{b})$ of $\mathbf{Q}$.
(2) The composition

$$E(\mathbf{Q}) \to E(\mathbf{Q})/2 \hookrightarrow \mathrm{H}^1(\mathbf{Q}, E_2) \simeq (\mathbf{Q}^*/\mathbf{Q}^{*2})^{\oplus 2}$$

maps a point (x, y) in $E(\mathbf{Q})$ other than O, P_1, P_2 to $(x - e_1, x - e_2) \in (\mathbf{Q}^*/\mathbf{Q}^{*2})^{\oplus 2}$. (More symmetrically, define a map from $E(\mathbf{Q})$ to the subgroup of $(\mathbf{Q}^*/\mathbf{Q}^{*2})^{\oplus 3}$ where the product of the three coordinates is 1 by sending (x, y) to $(x-e_1, x-e_2, x-e_3)$. This formula makes no sense when (x, y) is one of the P_i, but two of the three coordinates are nonzero, and one can determine what the third should be by the requirement that the product be 1.)

(3) The image of (a, b) under

$$(\mathbf{Q}^*/\mathbf{Q}^{*2})^{\oplus 2} \simeq \mathrm{H}^1(\mathbf{Q}, E_2) \to \mathrm{H}^1(\mathbf{Q}, E)$$

corresponds to a torsor $X_{a,b}$ birational to the curve defined by the equations $x - e_1 = az_1^2$, $x - e_2 = bz_2^2$, $x - e_3 = abz_3^2$ in the variables x, z_1, z_2, z_3. (This comes from the fact that the field extension corresponding the the multiplication-by-2 map $E \to E$ is obtained by adjoining $\sqrt{x - e_1}$ and $\sqrt{x - e_2}$ to the function field of E.)

It follows from (1) that $\xi \in \mathrm{H}^1(\mathbf{Q}, E_2)$ is unramified outside S if and only if ξ is represented by some pair (a, b) of elements in the subgroup $\langle -1, S\rangle$ of $\mathbf{Q}^*/\mathbf{Q}^{*2}$ generated by -1 and the finite primes of S. Thus

$$\mathrm{Sel}^2(E/\mathbf{Q}) \subseteq \mathrm{H}^1(\mathbf{Q}, E_2; S) \simeq \langle -1, S\rangle^{\oplus 2} \subset (\mathbf{Q}^*/\mathbf{Q}^{*2})^{\oplus 2}.$$

To decide which $(a, b) \in \langle -1, S\rangle^{\oplus 2}$ actually belong to $\mathrm{Sel}^2(E/\mathbf{Q})$, check whether $X_{a,b}$ has points over $\mathbf{R}$ and over $\mathbf{Q}_p$ for all finite primes $p \in S$.

11. Example

Let E be the elliptic curve $y^2 = x^3 - x$ over $\mathbf{Q}$. Let r be the rank of $E(\mathbf{Q})$. We will compute r, $\mathrm{Sel}^2(E/\mathbf{Q})$, and $Ш(\mathbf{Q}, E)_2$. Take $e_1 = -1$, $e_2 = 0$, $e_3 = 1$. Then we may take $S = \{\infty, 2\}$. The homomorphism

$$E(\mathbf{Q})/2 \to \mathrm{Sel}^2(E/\mathbf{Q}) \subseteq \mathrm{H}^1(\mathbf{Q}, E_2; S) \simeq \langle -1, 2\rangle^{\oplus 2} \subset (\mathbf{Q}^*/\mathbf{Q}^{*2})^{\oplus 2}$$

maps

$$\begin{aligned} O &\mapsto (1, 1) \\ P_1 = (-1, 0) &\mapsto (2, -1) \\ P_2 = (0, 0) &\mapsto (1, -1) \\ P_3 = (1, 0) &\mapsto (2, 1) \end{aligned}$$

so at least these images are contained in $\mathrm{Sel}^2(E/\mathbf{Q})$.

Now, for the other $(a, b) \in \langle -1, 2\rangle^{\oplus 2}$ we must check whether $X_{a,b}$ has points over $\mathbf{R}$ and $\mathbf{Q}_2$. An affine piece of $X_{a,b}$ is given by the equations

$$x + 1 = az_1^2, \quad x = bz_2^2, \quad x - 1 = abz_3^2,$$

and it will suffice to check this piece for points over $\mathbf{R}$ and $\mathbf{Q}_2$, because when a smooth curve over a local field has a point, the implicit function theorem implies that the curve has an analytic neighborhood of such points.

If $a < 0$ and $X_{a,b}$ has a real point, the first equation shows that it satisfies $x \leq -1$, the second equation shows that $b < 0$, and the third equation yields a sign contradiction. Thus

$$\{(1, 1), (2, -1), (1, -1), (2, 1)\} \subseteq \mathrm{Sel}^2(E/\mathbf{Q}) \subseteq \langle 2\rangle \times \langle -1, 2\rangle.$$

But $\mathrm{Sel}^2(E/\mathbf{Q})$ is a group, so it equals either the group of order 4 on the left, or the group of order 8 on the right. A calculation shows that $X_{1,2}(\mathbf{Q}_2)$ is empty, so $\mathrm{Sel}^2(E/\mathbf{Q}) = \{(1,1),(2,-1),(1,-1),(2,1)\}$, which has order 4. Since $E(\mathbf{Q})/2 \to \mathrm{Sel}^2(E/\mathbf{Q})$ is surjective, $Ш(\mathbf{Q},E)_2 = 0$. Finally, since $E_2 \subseteq E(\mathbf{Q})$, $\#(E(\mathbf{Q})/2) = 2^{2+r}$. On the other hand, $\#(E(\mathbf{Q})/2) \leq 4$, so $r = 0$.

12. Structure of Ш

We return to the situation where A is an abelian variety over a number field k. Let $Ш = Ш(k,A)$. The group $\mathrm{H}^1(k,A) = \mathrm{H}^1(G_k, A(\overline{k}))$ is torsion, as discussed in Section 3, since G_k is a profinite group. Hence the subgroup $Ш \subseteq \mathrm{H}^1(k,A)$ is torsion. In particular, we may write $Ш = \bigoplus_p Ш_{p^\infty}$, where for each prime number p, $Ш_{p^\infty}$ denotes the p-primary part of Ш, that is, the subgroup of elements of Ш whose order is a power of p. By descent, $Ш_m$ is finite for each positive integer m. Therefore, by abelian group theory,

$$Ш_{p^\infty} \simeq \left(\frac{\mathbf{Q}_p}{\mathbf{Z}_p}\right)^{n_p} \oplus T_p$$

where $n_p \in \mathbf{Z}_{\geq 0}$ and T_p is a finite abelian p-group, hence of the form

$$T_p \simeq \frac{\mathbf{Z}}{p^{s_1}} \oplus \ldots \oplus \frac{\mathbf{Z}}{p^{s_\ell}}$$

for some $s_i \in \mathbf{Z}_{>0}$. The group $\bigoplus_p \left(\frac{\mathbf{Q}_p}{\mathbf{Z}_p}\right)^{n_p} \subseteq Ш$ is called the *infinitely divisible* subgroup of Ш. The conjecture that Ш is finite says that the infinitely divisible subgroup should be trivial, and that moreover $T_p = 0$ for all but finitely many primes p.

Let $A^\vee$ denote the dual abelian variety. Then there exists a bilinear *Cassels-Tate pairing*

$$Ш(k,A) \times Ш(k,A^\vee) \to \mathbf{Q}/\mathbf{Z}$$

whose kernel on either side is the infinitely divisible subgroup. See [PS99] for various definitions of this pairing. If $Ш(k,A)$ is finite, then $Ш(k,A^\vee)$ also is finite (this can be deduced from the existence of an isogeny $A \to A^\vee$), and the Cassels-Tate pairing is nondegenerate.

If D is a divisor on A, one can define a homomorphism of abelian varieties $\phi_D : A \to A^\vee$ that maps $a \in A(k)$ to the class of $D_a - D$ in $\mathrm{Pic}^0(A)$, where D_a is obtained by translating the divisor D by $-a$. (We use $-a$ only so that the translation agrees with the operation of t_a^* on the corresponding line sheaves, where $t_a : A \to A$ is the translation-by-a map.) If D is ample, then ϕ_D is an isogeny, and it is then called the polarization associated to D; in general a polarization on A over k is a homomorphism ϕ_D defined over k but possibly coming from an ample divisor D defined only over $\overline{k}$.) The map ϕ_D induces a homomorphism $Ш(k,A) \to Ш(k,A^\vee)$, and composing this with the Cassels-Tate pairing lets one define a pairing

$$Ш(k,A) \times Ш(k,A) \to \mathbf{Q}/\mathbf{Z},$$

which turns out to be alternating if D is defined over k.

A finite abelian group equipped with a nondegenerate alternating pairing always has square order. Thus if ϕ_D is an isomorphism with D defined over k, and if $\#Ш(k,A)$ is finite, then $\#Ш(k,A)$ is a square. In particular, if A is an elliptic curve, and D is the degree 1 divisor

consisting of the origin O, then ϕ_D is an isomorphism; thus for elliptic curves, Ш is of square order whenever it is finite.

See [PS99] for more information, including an example of a principally polarized abelian variety over $\mathbf{Q}$ with $\#Ш = 2$. (This is possible, since the polarization ϕ_D does not come from any D defined over $\mathbf{Q}$. A principal polarization is a polarization that is an isomorphism $A \to A^\vee$.) William Stein found a non-principally polarized example with $\#Ш = 3$.

References

[CF86] J. W. S. Cassels and A. Fröhlich (eds.), *Algebraic number theory*, London, Academic Press Inc. [Harcourt Brace Jovanovich Publishers], 1986, Reprint of the 1967 original.

[CS86] Gary Cornell and Joseph H. Silverman (eds.), *Arithmetic geometry*, Springer-Verlag, New York, 1986, Papers from the conference held at the University of Connecticut, Storrs, Connecticut, July 30–August 10, 1984.

[Mil86] J. S. Milne, *Arithmetic duality theorems*, Academic Press Inc., Boston, MA, 1986.

[PS99] Bjorn Poonen and Michael Stoll, *The Cassels-Tate pairing on polarized abelian varieties*, Ann. of Math. (2) **150** (1999), no. 3, 1109–1149.

[Ser79] Jean-Pierre Serre, *Local fields*, Springer-Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg.

[Ser97] Jean-Pierre Serre, *Lectures on the Mordell-Weil theorem*, third ed., Friedr. Vieweg & Sohn, Braunschweig, 1997, Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt, With a foreword by Brown and Serre.

[Ser02] Jean-Pierre Serre, *Galois cohomology*, english ed., Springer-Verlag, Berlin, 2002, Translated from the French by Patrick Ion and revised by the author.

[Sil99] Joseph H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 199?, Corrected reprint of the 1986 original.

Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA
E-mail address: poonen@math.berkeley.edu