PRINCIPAL HOMOGENEOUS SPACES. SELMER GROUP AND SHAFAREVICH-TATE GROUP.

DIMITAR P. JETCHEV

Abstract. A proof of the finiteness of the weak Mordell-Weil groups is presented as a motivation for the definitions of Selmer and Shafarevich-Tate groups. The two groups are interpreted geometrically in terms of principal homogeneous spaces. We prove the finiteness of the Selmer group and then explain how to compute it for the case of elliptic curves. For higher genus curves, it is difficult to describe explicitly the homogeneous spaces in terms of equation and so we present a slightly different method for computing Selmer groups in terms of functions on the Jacobian of the curve. Several specific examples are considered at the end.

Introduction

The goal of the paper is to introduce the Selmer group and Shafarevich-Tate group by using the proof of the weak Mordell-Weil theorem as a motivation. This approach allows us to present a more geometric interpretation of the two groups in terms of principal homogeneous spaces and their relation to Galois cohomology.

In section 1, we introduce the Kummer pairing and prove its main properties. We compute the left and right kernels and then view the pairing in terms of the coboundary map in a long exact sequence in Galois cohomology. In section 2, we study in details the properties of the right kernel of the pairing, which turns out to be a finite index subgroup of the Galois group $\mathrm{Gal}(\overline{K}/K)$. Several classical results from algebraic number theory are assumed, such as the Dirichlet's S-unit theorem and standard facts about unramified field extensions of a number field.

Section 3 is devoted to the classical techniques for computing the weak Mordell-Weil by constructing a pairing $b : E(K)/mE(K) \times E[m] \to K^*/K^{*m}$ out of the Weil pairing and using explicit description of principal homogeneous spaces. In section 4, we illustrate these techniques for the case $m = 2$, which is known as complete 2-descent.

In section 5, we define Selmer group and Shafarevich-Tate group using Galois cohomology and then interpret the two groups geometrically, in terms of rational points on homogeneous spaces. We state one of the big open problems in number theory - the conjecture about the finiteness of Ш. In section 6, we prove the finiteness of the Selmer group and explain the main techniques for computing this group for elliptic curves. In the next section, we illustrate these techniques for the case of 2-isogenies.

In the last section, we introduce another method for computing the Selmer group which works in a greater generality and uses rational functions on the Jacobian of the curve.

1. Weak Mordell-Weil Group and Kummer Pairing via Galois Cohomology

Suppose that E/K is an elliptic curve over a number field and $m \geq 2$ is an integer, such that $E[m] \subseteq E(k)$. We define the weak Mordell-Weil group for E/K to be the quotient group $E(K)/mE(K)$, where $E(K)$ is the group of rational points on the elliptic curve E. This group is an interesting object to study for each m, since it contains a lot of information about the full Mordell-Weil group $E(K)$. In fact,

Define a pairing

$$\kappa : E(K) \times \mathrm{Gal}(\overline{K}/K) \to E[m],$$

in the following way: for each $P \in E(K)$ choose $Q \in E$, such that $[m]Q = P$ and let $\kappa(P, \sigma) := Q^\sigma - Q$.

First of all, this pairing is well-defined. Indeed, suppose that Q' is another point, such that $[m]Q = [m]Q' = P$. We need to check that $Q'^\sigma - Q' = Q^\sigma - Q$. But $[m](Q' - Q) = 0$, i.e. $Q - Q' \in E[m] \subseteq E(K)$, which means that $Q' - Q$ is fixed by the action of $\mathrm{Gal}(\overline{K}/K)$. Hence, $(Q' - Q)^\sigma = Q' - Q$, or $Q'^\sigma - Q' = Q^\sigma - Q$. We often call the pairing κ the Kummer pairing.

The basic properties of κ are summarized in the following proposition:

Proposition 1.1. *The pairing κ is bilinear, with left kernel equal to $mE(K)$ and right kernel equal to $Gal(\overline{K}/L)$, where L is a field extension of K obtained by adjoining the coordinates of all points in $[m]^{-1}E(K)$ (or $L = K([m]^{-1}E(K))$). In particular, κ induces a perfect bilinear pairing*

$$E(K)/mE(K) \times Gal(L/K) \to E[m].$$

`Proof:` Bilinearity of κ is obvious from the definition. Suppose that $P \in E(K)$ is in the left kernel of κ. Choose $Q \in E(\overline{K})$, such that $[m]Q = P$. We will show that $Q \in E(K)$ and thus, it will follow that $P \in mE(K)$. But this is clear from the definition, since $\kappa(P, \sigma) = 0$ means precisely that Q is fixed by σ. Conversely, any $P \in mE(K)$ is in the left kernel of κ.

Let $\sigma \in \mathrm{Gal}(\overline{K}/K)(K)$ be in the right kernel. In this case it suffices to show that σ fixes the field extension L/K. Let $P \in E(K)$ and Q be a point, such that $[m]Q = P$. Then $\kappa(P, \sigma) = 0$ implies $Q^\sigma = Q$. Since this is true for any point in $[m]^{-1}E(K)$, then L is fixed by σ, i.e. $\sigma \in \mathrm{Gal}(\overline{K}/L)$. Conversely, any $\sigma \in \mathrm{Gal}(\overline{K}/L)$ is in the right kernel, because it fixes the points in $[m]^{-1}E(K)$.

We obtain the perfect bilinear pairing by moding out by the left and right kernels of κ. □

Next, our goal is to describe the Kummer pairing in terms of Galois cohomology. To begin with, consider the short exact sequence of $\mathrm{Gal}(\overline{K}/K)$-modules for a fixed integer $m > 1$

$$0 \to E[m] \longrightarrow E(\overline{K}) \xrightarrow{[m]} E(\overline{K}) \to 0.$$

This short exact sequence gives a long exact sequence on cohomology

$$\begin{aligned} 0 &\longrightarrow H^0(\mathrm{Gal}(\overline{K}/K), E[m]) \longrightarrow H^0(\mathrm{Gal}(\overline{K}/K), E(\overline{K})) \xrightarrow{[m]} H^0(\mathrm{Gal}(\overline{K}/K), E(\overline{K})) \\ &\xrightarrow{\delta} H^1(\mathrm{Gal}(\overline{K}/K), E[m]) \longrightarrow H^1(\mathrm{Gal}(\overline{K}/K), E(\overline{K})) \xrightarrow{[m]} H^1(\mathrm{Gal}(\overline{K}/K), E(\overline{K})). \end{aligned}$$

But $H^0(G, M) = M^G$ for any group G and a G-module M, so we rewrite the above sequence as

$$\begin{aligned} 0 &\longrightarrow E(K)[m] \longrightarrow E(K) \xrightarrow{[m]} E(K) \\ &\xrightarrow{\delta} H^1(\mathrm{Gal}(\overline{K}/K), E[m]) \longrightarrow H^1(\mathrm{Gal}(\overline{K}/K), E(\overline{K})) \xrightarrow{[m]} H^1(\mathrm{Gal}(\overline{K}/K), E(\overline{K})). \end{aligned}$$

Next, we obtain a short exact sequence out of this long exact sequence, using the fact that $\ker \delta = mE(K)$. We call this short exact sequence the *Kummer sequence*:

$$0 \to E(K)/mE(K) \xrightarrow{\delta} H^1(\mathrm{Gal}(\overline{K}/K), E[m]) \longrightarrow H^1(\mathrm{Gal}(\overline{K}/K), E(\overline{K}))[m] \to 0.$$

Since the left kernel of the pairing κ is $mE(K)$, then κ induces a homomorphism

$$\delta_E : E(K)/mE(K) \to \mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), E[m]).$$

Using the Galois cohomology discussion from above, the homomorphism δ_E is precisely the connecting homomorphism δ for the long exact sequence, constructed above.

2. Properties of the Field Extension $L = K([m]^{-1}E(K))/K$

After introducing the Kummer pairing in the previous section, we will to study in a more detail the field extension $L = K([m]^{-1}E(K))$, which appeared in proposition 1.1 in the previous section. The main result that we prove is that this extension is abelian of exponent m, which is unramified outside of a finite set of places ν. Then, using a general result from algebraic number theory, we prove that L/K is a finite extension.

The main properties of the field extension L/K are summarized in the following

Proposition 2.1. *(i) The field extension L/K is an abelian extension of exponent m. In other words, the Galois group $Gal(L/K)$ is abelian and every element has order dividing m.*
(ii) If S is the finite set of places, at which E has bad reduction, together with the infinite places and the places ν, for which $\nu(m) \neq 0$, then L/K is unramified at each $\nu \notin S$.

The following lemma will be used in the proof of the proposition:

Lemma 2.2. *Suppose that ν is a discrete valuation, such that $\nu(m) = 0$ and E/K has a good reduction at ν. Then the reduction map $E(K)[m] \to \tilde{E}_\nu(k_\nu)$ is injective.*

`Proof:` This is proved in [Sil-1, VIII.§1]. □

We are now ready to prove the proposition:

`Proof of proposition 2.1:` (i) This is a consequence of proposition 1.1. Indeed, the map $\sigma \mapsto \kappa(\sigma, \cdot)$ is an injection $\mathrm{Gal}(L/K) \to \mathrm{Hom}(E(K), E[m])$. Therefore every element of $\mathrm{Gal}(L/K)$ is abelian and of order dividing m, since every homomorphism of $\mathrm{Hom}(E(K), E[m])$ has order dividing m.
(ii) Take a point $Q \in [m]^{-1}E(K)$ and let $P = [m]Q$. Consider the extension $L = K(Q)$ over K. It suffices to show that this extension is unramified at each $\nu \notin S$. Let ν' be an extension of ν in $K(Q)$ and $D_{\nu'/\nu}$ and $I_{\nu'/\nu}$ be the inertia and the decomposition groups, respectively. We will be done if we show that each element of $I_{\nu'/\nu}$ acts trivially on $K(Q)$. Indeed, every element of $I_{\nu'/\nu}$ acts trivially on $\tilde{E}_\nu(k'_{\nu'})$, where $k'_{\nu'}$ denote the reduction of $K(Q)$ at ν'. Therefore $(Q^\sigma - Q)^\sim = \tilde{Q}^\sigma - \tilde{Q} = \tilde{0}$ for all $\sigma \in I_{\nu'/\nu}$. But $Q^\sigma - Q \in E[m]$, because $Q \in [m]^{-1}E(K)$. Thus, lemma 2.2 implies that $Q^\sigma = Q$, so $I_{\nu'/\nu}$ acts trivially on $K(Q)/K$, which means that the field extension is unramified. This proves the proposition. □

Our goal in this section is to show that L/K is a finite extension. So far, we concluded that L/K is abelian extension of exponent m which is unramified outside of a finite set of primes. It turns out that these conditions are enough to claim the finiteness of L/K. The next theorem establishes precisely this statement. In the proof, we assume several nontrivial results from algebraic number theory.

Theorem 2.3. *Let K be a number field, $m \geq 2$ be an integer, and S - a finite set of places, containing all infinite places in K and all finite places ν, such that $\nu(m) \neq 0$. Consider the maximal abelian extension L/K which has exponent m and which is unramified at all places outside of S. Then L/K is a finite extension.*

`Proof:` If the proposition is true for a finite extension K'/K, then it is certainly true for K. Indeed, if L/K is the maximal abelian extension of exponent m, which is unramified outside of the finite set S, then LK'/K' is a maximal abelian extension of exponent m, unramified outside of a set S' of extensions of the places in S to LK'. Therefore, LK'/K' is finite, and so L/K would also be finite. Thus, we can assume that K contains the m-th roots of unity μ_m.

We define *the ring of S-integers*

$$R_S = \{a \in K : \nu(a) \geq \text{ for all } \nu \notin S\}.$$

First, it follows from [La, V] that we can add finitely many places to S, so that R_S becomes a Dedekind domain with class number 1 (i.e. a principal ideal domain). Making S bigger increases L and so we can assume that R_S is a PID.

Next, we use another auxiliary result:

Lemma 2.4. *Let K be a number field (more generally, any field of characteristic 0), containing the m-th roots of unity μ_m. Then the maximal abelian extension of K of exponent m is obtained by adjoining m-th roots of the elements of K. In other words, $L = K(a^{1/m} : a \in K)$ is the maximal abelian extension of K of degree m.*

`Proof:` *** LATER *** □

According to the lemma 2.4, L is the largest extension of K, contained in $K(a^{1/m} : a \in K)$, which is unramified outside of S.

Suppose that $\nu \notin S$. Then $a^{1/m} \in L$ for some $a \in K$ if and only if $K_\nu(a^{1/m})/K_\nu$ is unramified. But since $\nu(m) = 0$, then this condition is satisfied precisely when $\nu(a) \equiv 0 \pmod m$. Finally, we conclude that $L = K(a^{1/m} : a \in T_S)$, where

$$T_S = \{a \in K^*/{K^*}^m : \nu(a) \equiv 0 (\text{mod } m) \text{ for all } \nu \notin S\}$$

We will be done if we prove that T_S is finite. The idea is to consider the natural map $R_S^* \to T_S$. We claim that this map is surjective. Indeed, the valuations $\nu \notin S$ correspond precisely to the prime ideals of R_S. Thus, if $a \in K^*$ represents an element of T_S, then the ideal aR_S is the m-th power of an ideal of R_S (by the definition of T_S). Since R_S is a principal ideal domain, then $aR_S = b^m R_S$ for some $b \in K^*$. Hence, $a = ub^m$ for some $u \in R_S^*$. But then the images of a and u in T_S are the same and therefore the map $R_S^* \to T_S$ is surjective. Since its kernel contains $(R_S^*)^m$ then we obtain a surjective map $R_S^*/(R_S^*)^m \to T_S$. Finally, using Dirichlet's S-unit theorem [La, V], it follows that R_S^* is finitely generated and therefore $R_S^*/(R_S^*)^m$ is finite. Thus, T_S is finite and L/K is a finite extension. □

We finally proved that L/K is a finite extension, which is enough to conclude that $E(K)/mE(K)$ is finite, because of the perfect pairing $E(K)/mE(K) \times \text{Gal}(L/K) \to E[m]$ induced by κ in section 1.

3. Computation of the Weak Mordell-Weil Group and Principal Homogeneous Spaces

Recall that we assumed in the very beginning that $E[m] \subset E(K)$. This assumption implies that $\mu_m \subset K^*$. It follows from Hilbert 90 Satz theorem [Jac] that each homomorphism $\text{Gal}(\overline{K}/K) \to \mu_m$ has the form $\sigma \mapsto \sigma(\beta)/\beta$ for some $\beta \in \overline{K}^*$ and $\beta^m \in K^*$. Therefore, we have an isomorphism $\delta_K : K^*/{K^*}^m \to \text{Hom}(\text{Gal}(\overline{K}/K), \mu_m)$.

The main idea for the computation of the weak Mordell-Weil group $E(K)/mE(K)$ is to use the homomorphisms δ_E (from section 1) and δ_K in order to construct a pairing

$$b : E(K)/mE(K) \times E[m] \to K^*/{K^*}^m,$$

which is computable.

For the construction of this pairing, we use the Weil pairing $e_m : E[m] \times E[m] \to \mu_m$, defined in [Sil1-III.§8]. Define

$$b(P, Q) = \delta_K^{-1}(e_m(\delta_E(P)(\cdot), Q)).$$

The pairing is well-defined, because δ_K is an isomorphism. It is also not hard to check that the pairing is bilinear and nondegenerate on the left. Indeed, if δ_K were degenerate on the left, then for all $Q \in E[m]$ and all $\sigma \in \text{Gal}(\overline{K}/K)$ it will follow that $e_m(\kappa(P, \sigma), Q) = 1$. Since the Weil pairing is nondegenerate, then $\kappa(P, \sigma) = 0$, which means that $P \in mE(K)$ by proposition 1.1.

The pairing b is easily computable. The next proposition discusses how one can compute the pairing b.

Proposition 3.1. *Let S be the finite set of places ν, at which E has a bad reduction, the infinite places and the primes dividing m. Then the image of the pairing b lies in the subgroup*

$$K(S,m) = \{b \in K^*/K^{*m} : \nu(b) \equiv 0 (mod\ m) \text{ for all } \nu \notin S\}$$

Moreover, for a point $Q \in E[m]$ if f_Q and g_Q are functions, satisfying $div(F_Q) = m(Q) - m(0)$ and $f_Q \circ [m] = g_Q^m$ and $P \neq Q$ then $b(P,Q) \equiv f_Q(P) (mod\ K^{*m})$. In the case $P = Q$ one can consider any point $P' \in E(K)$, such that $f_Q(-P') \neq 0$ and use bilinearity of the pairing to obtain $b(P,P) = f_Q(P+P')/f_Q(P')$.

Before presenting the proof, we will mention that the above proposition might be helpful for computing the weak Mordell-Weil group (and therefore the full Mordell-Weil group) for the elliptic curve E/K. Indeed, the functions f_Q can be computed from the equation of the curve. Once we do this, it suffices to take generating points for $E[m]$ (call them Q_1 and Q_2) and consider all pairs $(b_1, b_2) \in K(S,m)$ (which are finitely many). Using the non-degeneracy of the pairing b, we notice that if the equations $b_1 z_1^m = f_{Q_1}(P)$ and $b_2 z_2^m = f_{Q_2}(P)$ have a solution (P, z_1, z_2), such that $P \in E(K)$, $z_1, z_2 \in K^*$, then any other such solution has the same K-rational point P. Therefore, the question computing Mordell-Weil group reduces to the existence of a point $(x, y, z_1, z_2) \in K \times K \times K^* \times K^*$ on an auxiliary curve, defined by the equations $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, $b_1 z_1^m = f_{Q_1}(x,y)$ and $b_2 z_2^m = f_{Q_2}(x,y)$. We call this auxiliary curve a *homogeneous space* for E/K. In the following sections we will develop the theory of homogeneous spaces in terms of Galois cohomology.

`Proof of Proposition 1.2:` Consider the element $\beta = b(P,Q)^{1/m}$ and the field extension $K(\beta)/K$. The proof of the first part is based on two observations. First, the element β is contained in the finite extension $L = K([m]^{-1}E(K))$, as defined in proposition 1.1. Since L/K is unramified outside of S by theorem 2.3, then $K(\beta)/K$ is unramified as well. But we get from algebraic number theory that $K(\beta/K)$ is unramified at ν if and only if $\nu(\beta^m) \equiv 0 \pmod m$. This proves that the image of b is contained in $K(S,m)$.

For the second part of the proposition, recall [Sil-1, III.§8] that f_Q and g_Q are used for defining the Weil pairing. In other words, $e_m(P,Q) := \dfrac{g_Q(X+P)}{g_Q(X)}$ (the last fraction is the same for all X). Choose a point $P' \in E(\overline{K})$, such that $[m]P' = P$. Then by the definition of b and e_m for $X = P'$, we have

$$\frac{\beta^\sigma}{\beta} = e_m(P'^\sigma - P', Q) = \frac{g_Q(P'^\sigma)}{g_Q(P')} = \frac{g_Q(P')^\sigma}{g_Q(P')}.$$

By raising to the m-th power and using the fact that δ_K is an isomorphism, we conclude that $g_Q(P')^m \equiv \beta^m \pmod{K^{*m}}$. Hence, $f_Q(P) = f_Q([m]P') = g_Q(P')^m \equiv b(P,Q) \pmod{K^{*m}}$, which completes the proof of the proposition. □

4. Applications and Complete 2-descent

Our discussion in section 3 will not be complete without an explicit example, for which we compute the weak Mordell-Weil group, using the described techniques. Since the main technical difficulties arise from the group law on the elliptic curve, derived out of the Weierstrass equation, we restrict ourselves to the case $m = 2$, which can be made explicit using the formulas for the group law on the elliptic curve, out of the Weierstrass equations.

First, take a Weierstrass equation for E of the form

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

The 2-torsion point in E are 0 and $Q_i = (e_i, 0)$ for $i = 1, 2, 3$. The first step is to determine the functions f_{Q_i} and g_{Q_i}. In this case, the explicit formulas for the group law on the curve [Sil1-III] makes this quite easy. We check that the function $f_{Q_i} = x - e_i$ satisfies $\mathrm{div}(f_{Q_i}) = 2(Q_i) - 2(0)$.

Moreover,

$$x \circ [2] - e_i = (x^2 - 2e_i x - 2e_i^2 + 2(e_1+e_2+e_3)e_i - (e_1e_2+e_1e_3+e_2e_3))^2/(2y)^2,$$

so we can set $g_{Q_i} = \dfrac{(x^2 - 2e_i x - 2e_i^2 + 2(e_1+e_2+e_3)e_i - (e_1e_2+e_1e_3+e_2e_3))}{2y}$. Recall that knowing f_{Q_i} means knowing explicitely the equations for the principal homogeneous spaces.

Fix $(b_1, b_2) \in K(S,2) \times K(S,2)$. To check whether (b_1, b_2) is in the image of the pairing b means to check whether the system of equations $y^2 = (x-e_1)(x-e_2)(x-e_3)$, $b_1 z_1^2 = x - e_1$ and $b_2 z_2^2 = x - e_2$ has a solution $(x, y, z_1, z_2) \in K \times K \times K^* \times K^*$ (we are using the fact that Q_1 and Q_2 are generators for $E[2]$). By substituting the second and the third equation into the first one, one obtains $y^2 = (x-e_3) b_1 b_2 z_1^2 z_2^2$. Since b_1, b_2, z_1, z_2 are non-zero, we consider $z_3 = \dfrac{y}{b_1 b_2 z_1 z_2}$. Then the new set of equations is $b_1 b_2 z_3^2 = x - e_3$, $b_1 z_1^2 = x - e_1$ and $b_2 z_2^2 = x - e_2$. By eliminating x from these equations, we obtain two equations for z_1, z_2, z_3, namely $b_1 z_1^2 - b_2 z_2^2 = e_2 - e_1$ and $b_1 z_1^2 - b_1 b_2 z_3^2 = e_3 - e_1$. There are standard techniques to determine whether these equations have a solution $(z_1, z_2, z_3) \in K^* \times K^* \times K$. In case we find such a solution, the point P is given by $x(P) = b_1 z_1^2 + e_1$ and $y(P) = b_1 b_2 z_1 z_2 z_3$.

There is one more case which needs to be considered. If $P = Q$, then the above argument does not hold. In other words, we have to worry about the pairs $(b(Q_1,Q_1), b(Q_1,Q_2))$ and $(b(Q_2,Q_1), b(Q_2,Q_2))$. But it is not hard to compute that $b(Q_1,Q_1) = (e_1 - e_3)/(e_2 - e_1)$ and $b(Q_2,Q_2) = (e_2 - e_3)/(e_2 - e_1)$.

We can summarize the whole argument in the following

Theorem 4.1 (Complete 2-descent)**.** *Suppose that E/K is an elliptic curve, given by a Weierstrass equation*

$$y^2 = (x-e_1)(x-e_2)(x-e_3), \quad e_i \in K$$

Let S be the set of places at which E has bad reduction, the places dividing 2 and the infinite places. Then there exists an injective homomorphism

$$E(K)/2E(K) \to K(S,2) \times K(S,2),$$

which is given explicitly (by proposition 3.1) as

$$P \mapsto \begin{cases} (x(P)-e_1, x(P)-e_2) & \text{if } x(P) \neq e_1, e_2, \\ ((e_1-e_3)/(e_1-e_2), e_1-e_2) & \text{if } x(P) = e_1, \\ (e_2-e_1, (e_2-e_3)/(e_2-e_1)) & \text{if } x(P) = e_2, \\ (1,1) & \text{if } P = O. \end{cases}$$

If $(b_1, b_2) \in K(S,2) \times K(S,2)$ is not in the image of the three points O, $(e_1, 0)$ and $(e_2, 0)$, then (b_1, b_2) is the image of a point $P \in K$ if and only if the equations $b_1 z_1^2 - b_2 z_2^2 = e_2 - e_1$ and $b_1 z_1^2 - b_1 b_2 z_3^2 = e_3 - e_1$ have a solution $(z_1, z_2, z_3) \in K^* \times K^* \times K$. If such a solution exists, then a representative for the element of $E(K)/mE(K)$ is given by $x(P) = b_1 z_1^2 + e_1$ and $y(P) = b_1 b_2 z_1 z_2 z_3$.

Finally, let us illustrate the technique of 2-descent with a specific example:

Example: The goal is to compute the weak Mordell-Weil group $E(\mathbb{Q})/2E(\mathbb{Q})$ for the curve

$$E : y^2 = x^3 - 7x^2 + 5x = x(x-2)(x-5).$$

First of all, the discriminant is $\Delta = 2^6 \cdot 3^5 \cdot 5^2$.

5. Definition of Selmer and Shafarevich-Tate Groups

As in the previous section, we are led by the motivation to effectively compute the Mordell-Weil group. The main step is to find generators for the weak Mordell-Weil group $E(K)/mE(K)$.

In the previous section, we obtained the Kummer sequence out of the long exact sequence on group cohomology. Now, we consider a slightly more general setting: suppose that $\phi : E \to E'$ is a non-zero isogeny of elliptic curves over K. Then one has a short exact sequence

$$0 \to E[\phi] \longrightarrow E \xrightarrow{\phi} E' \to 0.$$

In precisely the same way as for the case $E' = E$ and $\phi = [m]$ from the previous section, we obtain a short exact sequence

$$0 \to E'(K)/E(K) \xrightarrow{\delta} H^1(\mathrm{Gal}(\overline{K}/K), E[\phi]) \longrightarrow H^1(\mathrm{Gal}(\overline{K}/K), E(\overline{K}))[\phi] \to 0$$

Next, we consider a place ν for the number field K. Extend ν to a place in the algebraic closure $\overline{K}$. This gives us an embedding $\overline{K} \subset \overline{K}_\nu$ and a decomposition group, which we denote by $D_\nu \subset \mathrm{Gal}(\overline{K}/K)$. By the definition of a decomposition group and of the completion $\overline{K}_\nu$, it follows that D_ν acts on $E(\overline{K}_\nu)$ and $E'(\overline{K}_\nu)$. Repeating the same argument as the one in the previous section, we obtain similar Kummer sequences

$$0 \to E'(K_\nu)/\phi(E(K_\nu)) \to H^1(D_\nu, E[\phi]) \to H^1(D_\nu, E(\overline{K}))[\phi] \to 0.$$

Notice that $D_\nu \subset \mathrm{Gal}(\overline{K}/K)$ and $E(\overline{K}) \subset E(\overline{K}_\nu)$. But recall from the basic properties of Galois cohomology that these inclusions induce restriction maps on cohomology. We do the same for each place ν and use these restriction maps to obtain the following commutative diagram

$$\begin{array}{ccccccc}
0 \to & E'(K)/\phi(E(K)) & \xrightarrow{\delta} & H^1(\mathrm{Gal}(\overline{K}/K), E[\phi]) & \longrightarrow & H^1(\mathrm{Gal}(\overline{K}/K), E(K))[\phi] & \to 0 \\
& \downarrow & & \downarrow & & \downarrow & \\
0 \to & \prod_\nu E'(K_\nu)/\phi(E(K_\nu)) & \xrightarrow{\delta} & \prod_\nu H^1(D_\nu, E[\phi]) & \longrightarrow & \prod_\nu H^1(D_\nu, E(K_\nu))[\phi] & \to 0
\end{array}$$

But in the previous section, we identified the group of equivalence classes of principle homogeneous spaces $WC(E/K)$ with the cohomology group $H^1(\mathrm{Gal}(\overline{K}/K), E)$. Thus, we can change the upper and lower last terms by $WC(E/K)$ and $WC(E/K_\nu)$ respectively.

Our ultimate goal is computing the image of $E'(K)/\phi(E(K))$ in $H^1(\mathrm{Gal}(\overline{K}/K), E[\phi])$, which is the same as computing the kernel of the map $H^1(\mathrm{Gal}(\overline{K}/K), E)[\phi]) \to WC(E/K)[\varphi]$. But the following proposition provides a way of testing whether an element is in the kernel, in terms of K-rational points on the homogeneous spaces of $WC(E/K)$.

Proposition 5.1. *Suppose that C/K is a homogeneous space for E/K. Then C/K represents a trivial element of $WC(E/K)$ if and only if C has at least one K-rational point.*

`Proof:` One of the directions is easy. Suppose that C/K represents a trivial element of $WC(E/K)$. Then there is a K-isomorphism $\varphi : E \to C$. Then $\varphi(0) \in C(K)$, so in particular $C(K)$ is non-empty.

Conversely, suppose that $C(K)$ is non-empty, i.e. $P_0 \in C(K)$. Define a morphism $\theta : E \to C$ by $\theta(Q) = P_0 + Q$. We first show that the morphism θ is defined over K. Suppose $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Then

$$\theta(Q)^\sigma = (P_0 + Q)^\sigma = P_0^\sigma + Q^\sigma = P_0 + Q^\sigma = \theta(Q^\sigma).$$

Thus, the morphism is defined over K. We will prove that θ is an isomorphism. Indeed, since E acts simply transitively on C, then for each $P \in C$ there is a unique $Q \in E$, such that $\theta(Q) = P$ and so θ has degree 1. This means that the induced map on function fields $\theta^* : \overline{K}(C) \to \overline{K}(E)$ is an isomorphism of fields. In other words $\theta^*\overline{K}(C) = \overline{K}(E)$. Therefore, θ has an inverse, which we denote by $\theta^{-1} : \overline{K}(E) \to \overline{K}(C)$. This isomorphism gives rise to a rational function $\psi : C \to E$. We will be done if we show that ψ is a morphism, i.e. is defined at every point. But this follows from [Sil-1, II.2.1] (***LATER***). □

Although we obtained a simple criteria to check if a principal homogeneous space represents the trivial element in the Weil-Chatelet group, it is still a hard question to determine whether a curve C has a K-rational point. In such cases, it is always easier to work over complete local fields,

because we can use Hensel's lemma to reduce the problem to checking whether the curve has a point over a finite ring.

To illustrate more precisely the above idea, consider a place ν and the complete local field K_ν. By proposition 2.1, computing

$$\ker\{H^1(D_\nu, E[\phi])\} \to WC(E/K_\nu)[\phi]$$

reduces to the question of determining whether a homogeneous space C has a K_ν-rational point. *** EXPLAIN WHY THIS REDUCES TO A FINITE AMOUNT OF COMPUTATION *** The idea of localization gives rise to the following definitions:

Definition 5.2. For an isogeny $\phi : E \to E'$ defined over K, consider the ϕ-Selmer group $S^{(\phi)}(E/K)$ to be the subgroup of $H^1(\mathrm{Gal}(\overline{K}/K), E[\phi])$, defined as

$$S^{(\phi)}(E/K) := \ker\left\{ H^1(\mathrm{Gal}(\overline{K}/K), E[\phi]) \to \prod_\nu WC(E/K_\nu) \right\}.$$

We also consider the Shafarevich-Tate group of E/K to be the subgroup of $WC(E/K)$ defined as

$$Ш(E/K) := \ker\left\{ WC(E/K) \to \prod_\nu WC(E/K_\nu) \right\}.$$

One might think *a priori* that the above definitions depend on the extension of each place ν to the algebraic closure $\overline{K}$, since for constructing the Kummer sequence, we fixed an extension of each place ν (and thus a decomposition group D_ν). However, if we use the more geometric interpretation of homogeneous spaces, it follows immediately that both $S^{(\phi)}$ and Ш depend only on E and K. Indeed, recall that a homogeneous space C represents a trivial element in $WC(E/K_\nu)$ if and only if it has a K_ν-rational point, a condition which is certainly independent of the choice of extension of the places ν. Therefore, both $S^{(\phi)}$ and Ш depend only on E and K.

A famous conjecture about $Ш(E/K)$ for an elliptic is that it is always finite and has order a perfect square.

Conjecture: If E/K is an elliptic curve, then $Ш(E/K)$ is finite and $\#Ш(E/K) = \square^2$.

Remark: Another interesting observation for Ш is that it measures the failure of the "local-to-global principle", since the elements in Ш are equivalence classes of homogeneous spaces which have a rational point for every local field K_ν, but do not have a K-rational point. For instance, for quadratic forms we have the Hasse-Minkowski principle, according to which existence of $\mathbb{Q}_\nu$-rational point for each ν-adic field implies existence of $\mathbb{Q}$-rational point. This is not always true for arbitrary curves. The Shafarevich-Tate groups measures the failure of the local-to-global principle. Notice that the above conjecture implies that for all, but finitely many equivalence classes of homogeneous spaces the local-to-global principle still holds.

6. Computing the Selmer Group for Elliptic Curves

Unlike Ш, it is not hard to prove that $S^{(\phi)}$ is finite and effectively computable. The main goal of the section is to prove finiteness of $S^{(\phi)}$ for arbitrary isogeny ϕ and then to explain why $S^{(\phi)}$ is **effectively computable**.

To begin with, let $\phi : E \to E'$ be an isogeny defined over the number field K. Using only the cohomological definition of the Selmer group and Shafarevich-Tate group and the commutative diagram from the previous section, we obtain the following short exact sequence

$$0 \to E'(K)/\phi(E(K)) \to S^{(\phi)}(E/K) \to Ш(E/K)[\phi] \to 0.$$

This is going to be helpful for proving the first main result of the section

Theorem 6.1. *The ϕ-Selmer group $S^{(\phi)}(E/K)$ is finite. In particular, if one chooses ϕ to be the m-isogeny of E to itself, then the weak Mordell-Weil group $E(K)/mE(K)$ is finite.*

The key idea for the proof of the finiteness of the Selmer group is the nontrivial observation that it consists of cohomology classes of cocycles which are *unramified* outside of finite set of places S. Before proceeding, we give a precise definition for a cocycle to be unramified.

Definition 6.2. Suppose that M is a $\mathrm{Gal}(\overline{K}/K)$-module, ν is a discrete valuation for the number field K and $I_\nu \subset \mathrm{Gal}(\overline{K}/K)$ be the inertia group for ν. A cohomology class $\zeta \in H^p(\mathrm{Gal}(\overline{K}/K), M)$ is defined to be *unramified at ν* if has a trivial image in $H^p(I_\nu, M)$ under the restriction map $H^p(\mathrm{Gal}(\overline{K}/K), M) \to H^p(I_\nu, M)$.

First of all, we make one clarification about the above definition. Since we have already fixed a decomposition group D_ν for ν, the inertial group I_ν is determined by the decomposition group as the kernel of the map $D_\nu \to \mathrm{Gal}(\bar{k}_\nu/k_\nu)$, where ν' is the extension of ν to the algebraic closure of K and $\overline{k}_\nu$ and k_ν are the two residue fields for the complete local fields K_ν and $\overline{K}_\nu$ respectively.

With the above definition and explanation, we are ready to begin the proof of theorem 3.1.

`Proof of theorem 3.1:` Suppose that $\zeta \in S^{(\phi)}(E/K)$ and ν is a finite place of K which does not divide the degree of the isogeny ϕ and that E' has a good reduction at ν. We will prove that ζ is unramified at ν. Using the definition of $S^{(\phi)}$, we obtain that ζ has a trivial image in $WC(E/K_\nu)$. But $WC(E/K_\nu)$ is identified with $H^1(D_\nu, E)$, so $\zeta(\sigma) = P^\sigma - P$ is a coboundary, where $P \in E(\overline{K}_\nu)$ for all $\sigma \in D_\nu$. Furthermore, the definition implies that $P^\sigma - P \in E[\phi]$. But $E[\phi] \subset E[m]$ and we can use lemma 2.2 to show that $E(K)[m]$ injects into $\tilde{E}_\nu$. But the reduction (mod ν) maps sends $P^\sigma - P \to (P^\sigma - P)^\sim = \tilde{P}^\sigma - \tilde{P}$. The last point is $\tilde{0}$ for any $\sigma \in I_\nu$ by the definition of the inertia group. Therefore $P^\sigma = P$ for every $\sigma \in I_\nu$ and hence the restriction of ζ to $H^1(I_\nu, E[\phi])$ is trivial, i.e. ζ is unramified at ν.

Finally, the theorem will follow from the next proposition:

Proposition 6.3. *For any finite, abelian $Gal(\overline{K}/K)$-module M the group of cohomology classes which are unramified outside a finite set of primes is finite. In other words, the group*

$$H^1(Gal(\overline{K}/K), M; S) := \{\zeta \in H^1(Gal(\overline{K}/K), M) : \zeta \text{ is unramified outside of } S\}$$

is finite.

`Proof:` Using the definition of the profinite topology and the finiteness of M, we deduce that there must be a finite index subgroup of $\mathrm{Gal}(\overline{K}/K)$ which acts trivially on M. Therefore, we can assume that $\mathrm{Gal}(\overline{K}/K)$ acts trivially on M by changing K with a finite extension (because the inflation-restriction sequence on Galois cohomology implies that it suffices to prove the statement for the extension of K). This in turn implies that $H^1(\mathrm{Gal}(\overline{K}/K), M; S) = \mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), M; S)$. To complete the proof, denote by m the exponent of M (i.e. the smallest m, such that $mx = 0$ for all $x \in M$). Denote by L the maximal abelian extension of exponent m, which is unramified outside of S. Then the natural map $\mathrm{Hom}(\mathrm{Gal}(L/K), M) \to \mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), M; S)$ is clearly an isomorphism. But theorem 2.3 implies that L is finite, i.e. $H^1(\mathrm{Gal}(\overline{K}/K), M; S)$ is a finite extension. □

7. Computing Selmer Group for Isogenies of Degree 2

The techniques from the previous two sections are illustrated with several specific examples.

First, let E/K be an elliptic curve, $E' = E$ and ϕ be the m-isogeny. Suppose also that $E[m] \subset E(K)$. Our goal will be to compute the cohomology group $H^1(\mathrm{Gal}(\overline{K}/K), E[m]; S)$ of elements, which are unramified outside the finite set of places S. Since $E[m] \simeq \mu_m \times \mu_m$, then

$$H^1(\mathrm{Gal}(\overline{K}/K), E[m]) \simeq H^1(\mathrm{Gal}(\overline{K}/K), \mu_m \times \mu_m) \simeq H^1(\mathrm{Gal}(\overline{K}/K), \mu_m) \times H^1(\mathrm{Gal}(\overline{K}/K), \mu_m).$$

By Hilbert Satz 90, $H^1(\mathrm{Gal}(\overline{K}/K), \mu_m) \simeq K^*/(K^*)^m$. Moreover, $H^1(\mathrm{Gal}(\overline{K}/K), \mu_m; S) \cong K(S, m)$. Since each unramified cocycle for $H^1(\mathrm{Gal}(\overline{K}/K), \mu_m \times \mu_m)$ gives rise to a pair of unramified cocycles for the two $H^1(\mathrm{Gal}(\overline{K}/K), \mu_m)$ components, then $H^1(\mathrm{Gal}(\overline{K}/K), E[m]; S) \simeq K(S, 2) \times K(S, 2)$.

Isogenies of Degree 2: The goal is to analyze the Selmer group for all isogenies $\varphi : E \to E'$ of degree 2. First, $E[\phi]$ consists of two points $\{0, T\}$. By translation, we can assume that $T = (0, 0)$ and then the Weierstrass equation of the curve E is

$$E : y^2 = x^3 + ax^2 + bx.$$

Since $E[\phi] \cong \mu_2$ as $\mathrm{Gal}(\overline{K}/K)$-modules, then Hilbert Satz 90 implies that $H^1(\mathrm{Gal}(\overline{K}/K), E[\phi]; S) \cong K(S, 2)$. Take arbitrary $d \in K(S, 2)$. Using the above identification, a cocycle ζ, representing the class, corresponding to d is precisely

$$\zeta : \sigma \mapsto \begin{cases} O & \text{if } \sqrt{d}^\sigma = \sqrt{d} \\ T & \text{if } \sqrt{d}^\sigma = -\sqrt{d} \end{cases}$$

Next, we have to compute explicitly the principal homogeneous space, corresponding to the cohomology class of ζ. This is not hard, if we consider the

8. Computing the Selmer Group of a Jacobian Using Functions On the Curve

The purpose of this section is to introduce a slightly different method for computing the Selmer group, than the classical approach discussed so far, which is based on a choice of a Galois invariant system of divisors on curves. We should note that the described method works in much greater generality.

Let J be the Jacobian of a curve C. Suppose that $\phi : A \to J$ is an isogeny of degree $q = p^r$ for a prime p, where A is an abelian variety. Let $\breve{\phi} : \breve{J} \to \breve{A}$ be the dual isogeny. Since J is the Jacobian of a curve, there must be at least one principal polarization $\lambda : J \to \breve{J}$ (the canonical one) [C-Sil, V]. Let $\Phi = \lambda^{-1}(\breve{J}[\breve{\phi}])$. In particular, $\Phi \subset J[q]$.

We describe the main steps of an algorithm for computing the ϕ-Selmer group $S^\phi(A/K)$. The basic idea is to find a finitely generated K-algebra L and a map F, derived from functions on C, so that F maps $J(K)/\phi A(K)$ to L^*/L^{*q}. Next, we find a map $\iota : H^1(\mathrm{Gal}(\overline{K}/K), A[\phi]) \to L^*/L^{*q}$ so that $F = \iota \circ \delta$ (recall that δ is the connecting homomorphism in the long exact sequence in Galois cohomology). The map ι will be induced from a Weil pairing and the Kummer pairing. Let $L_s = L \otimes_K K_s$. We will similarly be able to define maps F_s and ι_s so that $F_s = \iota_s \circ \delta_s$. We will make an assumption, under which ι and ι_s and hence F and F_s are injective. Finally, we show how to use the maps F and F_s to compute the Selmer group.

Similarly to the case of elliptic curves, let S denote the finite set of places of bad reduction for A, the places that lie over p and the infinite places. We first state the assumptions that we will be used later on.

Assumption I: Every element of $J(K)/\phi A(K)$ is represented by a divisor class, containing an element of $\mathrm{Div}^0(C)(K)$. For each $s \notin S$, every element of $J(K_s)/\phi A(K_s)$ is represented by a divisor class, containing an element of $\mathrm{Div}^0(C)(K_s)$.

The next assumption will guarantee the injectivity of F and F_s. Let $\mu_q(L')$ be the qth roots of unity in L'. We have

$$\mu_q(L') \cong \mu_q(\overline{K_1}) \times \ldots \times \mu_q(\overline{K_n}).$$

Let $e_\phi(P, Q)$ denote the ϕ-Weil pairing of $P \in A[\phi]$ and $Q \in \breve{J}[\breve{\phi}]$. Define $w : A[\phi] \to \mu_q(L')$ by

$$w(P) = (e_\phi(P, \lambda[D_1]), \ldots, e_\phi(P, \lambda[D_n])).$$

Consider the induced map $w : H^1(\mathrm{Gal}(\overline{K}/K), A[\phi]) \to H^1(\mathrm{Gal}(\overline{K}/K), \mu_q(L'))$ (by abuse of notation, we denote it by w as well). It follows from [Se, p.152] that $H^1(\mathrm{Gal}(\overline{K}/K), \mu_q(L')) \cong L^*/L^{*q}$ by a map k, which sends the cohomology class of the cocycle $\sigma \mapsto \sqrt{l}^{\sigma}/\sqrt{l}$ to $l \in L^*$.

Proposition 8.1. *The map $w : A[\phi] \to \mu_q(L')$ is injective and defined over K.*

`Proof:` This is done in [Shae, Prop. 2.2].

Assumption II: The map $w : H^1(\mathrm{Gal}(\overline{K}/K), A[\phi]) \to H^1(\mathrm{Gal}(\overline{K}/K), \mu_q(L'))$ and the maps $w_s : H^1(\mathrm{Gal}(\overline{K}_s/K_s), A[\phi]) \to H^1(\mathrm{Gal}(\overline{K}_s/K_s), \mu_q(L'))$ for every $s \notin S$ are injective.

As we will see later, this assumption will guarantee that the maps F and F_s are injective. We are now ready to describe the steps of the algorithm for computing $S^{(\phi)}(A/K)$, under the above assumptions.

Step 1: Determine the subgroup of $J[q]$, which corresponds to Φ.

Step 2: Choose a nontrivial set of divisors $D_1, D_2, \ldots, D_n$, which is $\mathrm{Gal}(\overline{K}/K)$-invariant and whose divisor classes in Div^0 span Φ.

Step 3: Constructing the K-algebra L and a map $F : J(K)/\phi A(K) \to L^*/L^{*q}$.

We describe the way of constructing the algebra L. Consider the algebra

$$L' = \prod_{i=1}^{n} \overline{K}_i,$$

where $K_i = K$. Let $D_1, \ldots, D_n$ be the divisors from step 2. For each $\sigma \in \mathrm{Gal}(\overline{K}/K)$, let $\tilde{\sigma} \in S_n$ denote a permutation, such that $\tilde{\sigma}(i)$ is the index j, for which $D_i^{\sigma} = D_j$. Define an action of $\mathrm{Gal}(\overline{K}/K)$ on L by the rule

$$(a_1, \ldots, a_n)^{\sigma} = (a^{\sigma}_{\tilde{\sigma}^{-1}(1)}, \ldots, a^{\sigma}_{\tilde{\sigma}^{-1}(n)}).$$

Then we can define the K-algebra L to be the algebra of $\mathrm{Gal}(\overline{K}/K)$-invariants of L'.

There is an equivalent and more practical description of L. Look at the $\mathrm{Gal}(\overline{K}/K)$-orbits of $\{D_1, \ldots, D_n\}$ and let $\Lambda \subset \{1, 2, \ldots, n\}$ be a set of indices, such that $\{D_j\}_{j\in\Lambda}$ is a set of representatives for these orbits. It is not hard to show that

$$L \cong \prod_{j\in\Lambda} L_j,$$

where $L_j := K(D_j)$ denotes the field of definition of D_j. We will prove this explicitly in the case of $|\Lambda| = 1$, but in general the same argument extends. If $\mathrm{Gal}(\overline{K}/K)$ acts transitively on $\{D_i\}$, then

$$l \in L_1 \mapsto (\sigma_1(l), \sigma_2(l), \ldots, \sigma_n(l)) \in \prod_{i=1}^{n} \overline{K}_i$$

gives the desired isomorphism.

Finally, we construct the map $F : J(K)/\phi A(K) \to L^*/L^{*q}$ show how it related to the cohomological maps.

Let $qD_i = (f_i)$, where f_i is defined over $K(D_i)$ (the fiel of definition of the divisor D_i). First, we consider a map $f : C \to L'$ given by $f(P) = (f_1(P), \ldots, f_n(P))$. We will show how f induces a map $F : J(K)/\phi A(K) \to L^*/L^{*q}$.

First, we need two definitions:

Definition 8.2. The **avoidance set** is the set of points of $C(\overline{K})$ which is $\bigcup_{s\in S} \mathrm{Supp}(D_i)$.

Definition 8.3. A **good divisor** is a divisor of C of degree 0, defined over K (or K_s), whose support does not intersect the avoidance set.

From Assumption I, every element of $J(K)/\phi A(K)$ is represented by a divisor class containing a divisor of degree 0, defined over K. Moreover, every divisor class has a representative that does not intersect any given finite set, in particular, the avoidance set. Therefore, every element of $J(K)/\phi A(K)$ is represented by a good divisor.

The construction of F follows from

Lemma 8.4. *The map F induces a homomorphism from the subgroup of $J(K)/qJ(K)$, represented by divisor classes containing good divisors, to L^*/L^{*q}.*

`Proof:` This is done in [Shae, Lemma 2.1]. □

Finally, the next theorem, which is proved in [Shae, Theorem 2.3] establishes the relation between w and F.

Theorem 8.5. *The maps F and $k \circ w \circ \delta$ are the same maps from $J(K)/\phi A(K)$ to L^*/L^{*q}. In particular, if w is injective, then F is injective.*

Step 4: Computing the set of places S.

The finite places over p and the infinite places are easy to compute. The primes of bad reduction for A are precisely those, dividing the conductor of A, which is the same as the conductor of J. The conductor of J in general might be difficult to compute. Notice, however, that the primes, dividing the conductor of J are contained in the set of primes of singular reduction for C (which is easy to compute). By an earlier observation, we are allowed to make S bigger, so S is computable.

Step 5: Determine the image of $H^1(\mathrm{Gal}(\overline{K}/K), A[\phi], S)$ in $L^*/L^{*q} \cong \prod_{j\in\Lambda} L_j^*/L_j^{*q}$. and find generators of that image.

Definition 8.6. Let $L_j(S,q)$ be the subgroup of L_j^*/L_j^{*q} of elements with the property that if we adjoin the q-th root of a representative to L_j, that we get an extension unramified outside of primes over primes of S. Let $\mathbf{L(S,q)} = \prod_{j\in\Lambda} L_j(S,q)$.

Since we are making Assumption II, we have

$$H^1(\mathrm{Gal}(\overline{K}/K), A[\phi]) \cong \ker : H^1(\mathrm{Gal}(\overline{K}/K), \mu_q(L')) \to H^1(\mathrm{Gal}(\overline{K}/K), \mathrm{coker})$$

and

$$H^1(\mathrm{Gal}(\overline{K}/K), A[\phi]; S) \cong \ker : H^1(\mathrm{Gal}(\overline{K}/K), \mu_q(L'); S) \to H^1(\mathrm{Gal}(\overline{K}/K), \mathrm{coker})$$

But the last kernel is isomorphic to $\ker : L(S,q) \to H^1(\mathrm{Gal}(\overline{K}/K), \mathrm{coker})$ (notice the similarity with the case of elliptic curves), so $H^1(\mathrm{Gal}(\overline{K}/K), A[\phi]; S)$ is computable.

By abuse of notation, we refer to the subgroup of $L(S,q)$ above as $H^1(\mathrm{Gal}(\overline{K}/K), A[\phi]; S)$. Let β_s be the natural map from L^*/L^{*q} to L_s^*/L_s^{*q}. Then we can write

$$\begin{array}{ccc} J(K)/\phi A(K) & \overset{F}{\hookrightarrow} & H^1(K, A[\phi]; S) \\ \downarrow & & \downarrow \prod \beta_s \\ \prod\limits_{s\in S} J(K_s)/\phi A(K_s) & \overset{\prod F_s}{\hookrightarrow} & \prod\limits_{s\in S} L_s^*/L_s^{*q}. \end{array}$$

Step 6: Find generators for $J(K_s)/\phi A(K_s)$ and their images under F_s in L_s^*/L_s^{*q}.

Step 7: Using the maps F and F_s, we compute the ϕ-Selmer group $S^{(\phi)}(A/K)$. Note that using the following commutative diagram

$$\begin{array}{ccccc} J(K)/\phi A(K) & \overset{\delta}{\hookrightarrow} & H^1(\mathrm{Gal}(\overline{K}/K), A[\phi]; S) & \overset{\iota}{\hookrightarrow} & L^*/L^{*q} \\ \downarrow & & \downarrow \prod \alpha_s & & \downarrow \prod \beta_s \\ \prod_{s\in S} J(K_s)/\phi A(K_s) & \overset{\prod \delta_s}{\hookrightarrow} & \prod_{s\in S} H^1(\mathrm{Gal}(\overline{K}_s/K_s, A[\phi]) & \overset{\prod \iota_s}{\hookrightarrow} & \prod_{s\in S} L_s^*/L_s^{*q}, \end{array}$$

it suffices to compute the intersection of $\beta_s^{-1}(F_s(J(K_s)/\phi A(K_s)))$ over $s \notin S$.

Harvard University
E-mail address: jetchev@fas.harvard.edu