SELMER GROUPS AND DESCENT

MICHAEL STOLL

In these lectures we will discuss Selmer sets and Selmer groups, how to use them to get information on rational points and how to compute them in practice in certain cases.

1. Selmer sets

In the following, we work over a fixed number field k with algebraic closure $\bar{k}$. We consider a *nice* variety X over k, i.e., X is smooth, projective and geometrically irreducible. Our goal is to get some information on its set of k-rational points, $X(k)$.

The first question is whether there are any k-rational points on X at all. One easy way of showing that $X(k)$ is empty is to look at a larger set and show that the larger set is empty. In number theory, the larger sets people like to look at come from considering the various completions of k. So let v be a place of k and k_v the completion of k at v. Since $k \subset k_v$, we have $X(k) \subset X(k_v)$.

Theorem 1.1. *Assume that k and X are explicitly given by equations. Then the statement "$\forall v \colon X(k_v) \neq \emptyset$" is decidable.*

Proof. Here is a rough sketch. First one uses bounds for the number of points on varieties over finite fields and Hensel's Lemma to show that $X(k_v) \neq \emptyset$ for all but a finite set of places v that can be effectively bounded (infinite places, places of bad reduction, "small" finite places). Then one shows that for a single place v, checking whether there are k_v-points is a finite computation (this is basically quantifier elimination for infinite places and Hensel's Lemma again for finite places). □

Definition 1.2. If $X(k_v) \neq \emptyset$ for all places v of k, then we say that X *has points everywhere locally* or is *everywhere locally soluble* (or *ELS* for short).

For certain classes of varieties, "$X(k) \neq \emptyset$" is equivalent to "X has points everywhere locally". One says that the *Hasse Principle* holds for such X. The most well-known examples are quadric hypersurfaces (the original Hasse-Minkowski theorem). For curves of genus $g \geq 1$, the Hasse Principle breaks down, however.

So what can we do when $X(k)$ appears to be empty (we are unable to find any k-rational points despite a lot of effort), but X is ELS?

One possibility is to consider a finite étale covering $\pi \colon Y \to X$ defined over k that is geometrically Galois (meaning that the extension $\bar{k}(Y)/\bar{k}(X)$ is Galois). Let $G(\bar{k})$ denote the geometric Galois group of the covering; this is the group of $\bar{k}$-points on a finite group scheme G over k; this group scheme structure is determined by the action of the absolute Galois group of k on the automorphisms of the covering.

Date: August 31, 2017.

Definition 1.3. A *twist* of $\pi\colon Y \to X$ is another finite étale covering $\pi'\colon Y' \to X$ defined over k, such that both coverings become isomorphic over $\bar{k}$. This means that there is an isomorphism $\varphi\colon Y'_{\bar{k}} \xrightarrow{\simeq} Y_{\bar{k}}$ such that the obvious diagram commutes, i.e., $\pi_{\bar{k}} \circ \varphi = \pi'_{\bar{k}}$.

Two twists $\pi'\colon Y' \to X$ and $\pi''\colon Y'' \to X$ of π are *isomorphic* if there is an isomorphism φ as above, but already defined over k. We write $\operatorname{Twist}(\pi)$ (or $\operatorname{Twist}(Y \to X)$ if π is clear from the context) for the set of isomorphism classes of twists of π.

What is the relation to rational points? Here is an important fact.

Theorem 1.4. *Let $\pi\colon Y \to X$ be as above and let $P \in X(k)$ be a k-rational point. Then there is a unique twist $\pi'\colon Y' \to X$ of π (up to isomorphism) such that $P \in \pi'(Y'(k))$. In particular,*

$$X(k) = \coprod_{(\pi'\colon Y' \to X) \in \operatorname{Twist}(\pi)} \pi'(Y'(k)) .$$

Before we sketch how to prove this, let us try to figure out how to parameterise the set $\operatorname{Twist}(\pi)$ for an étale covering $\pi\colon Y \to X$. Let $\pi'\colon Y' \to X$ be a twist of π. Then there is an isomorphism $\varphi\colon Y'_{\bar{k}} \to Y_{\bar{k}}$ satisfying $\pi_{\bar{k}} \circ \varphi = \pi'_{\bar{k}}$. If $Y' \to X$ is isomorphic to $Y \to X$, then there is such an isomorphism over k. So we can measure in a way how far the given twist is from being trivial (meaning, isomorphic to $Y \to X$) by considering the action of the absolute Galois group Γ_k of k on φ. So let $\sigma \in \Gamma_k$; then ${}^\sigma\varphi$ is another isomorphism $Y'_{\bar{k}} \to Y_{\bar{k}}$ (defined to send ${}^\sigma P$ to ${}^\sigma(\varphi(P))$), with $\pi_{\bar{k}} \circ {}^\sigma\varphi = \pi'_{\bar{k}}$, and so ${}^\sigma\varphi \circ \varphi^{-1}$ is a deck transformation of $\pi_{\bar{k}}$, which means that ${}^\sigma\varphi \circ \varphi^{-1} \in G(\bar{k})$. This gives us a map $\xi\colon \Gamma_k \to G(\bar{k})$. Note that

$${}^{\sigma\tau}\varphi \circ \varphi^{-1} = {}^\sigma({}^\tau\varphi \circ \varphi^{-1}) \circ ({}^\sigma\varphi \circ \varphi^{-1}) ,$$

i.e., $\xi_{\sigma\tau} = {}^\sigma\xi_\tau \xi_\sigma$.

We can replace φ by $\gamma \circ \varphi$ for any $\gamma \in G(\bar{k})$; we have

$${}^\sigma(\gamma \circ \varphi) \circ (\gamma \circ \varphi)^{-1} = {}^\sigma\gamma \circ ({}^\sigma\varphi \circ \varphi^{-1}) \circ \gamma^{-1} .$$

This shows that two cocycles ξ and ξ' describe the same twist (up to isomorphism) if and only if there is $\gamma \in G(\bar{k})$ such that $\xi'_\sigma = {}^\sigma\gamma \xi_\sigma \gamma^{-1}$ for all $\sigma \in \Gamma_k$.

Definition 1.5.

(1) A map $\xi\colon \Gamma_k \to G(\bar{k})$ such that $\xi_{\sigma\tau} = {}^\sigma\xi_\tau \xi_\sigma$ for all $\sigma, \tau \in \Gamma_k$ is called a *1-cocycle with values in* G; the set of all such maps is denoted $Z^1(k, G)$.

(2) Two cocycles $\xi, \xi' \in Z^1(k, G)$ such that there is some $\gamma \in G(\bar{k})$ with $\xi'_\sigma = {}^\sigma\gamma \xi_\sigma \gamma^{-1}$ for all $\sigma \in \Gamma_k$ are *cohomologous*; this is an equivalence relation on $Z^1(k, G)$.

(3) The quotient set of $Z^1(k, G)$ by this equivalence relation is the *first Galois cohomology set with values in* G, denoted $H^1(k, G)$.

So we get an injective map $\operatorname{Twist}(\pi) \to H^1(k, G)$. The map is actually bijective: given a 1-cocycle ξ with values in G, one can construct a suitable twist (one "twists" the Galois action on $Y(\bar{k})$ by ξ to construct Y'; more precisely, we define the new action by $\sigma \in \Gamma_k$ to be $\sigma \cdot P = \xi_\sigma^{-1}({}^\sigma P))$, so $H^1(k, G)$ classifies the twists of π.

In general, $H^1(k, G)$ is just a *pointed set* (a set with a distinguished element, which in this case is the class of the trivial cocycle $\sigma \to 1_G$, corresponding to π itself). If G is abelian, however, it is easy to see that $Z^1(k, G)$ is actually an abelian group as well; also, the set of 1-cocycles that are cohomologous to the trivial cocycle form a subgroup $B^1(k, G)$ (of "1-coboundaries"), and two cocycles are cohomologous if and only if they are in the same coset. So for abelian G, we can write $H^1(k,G) = Z^1(k,G)/B^1(k,G)$, and $H^1(k,G)$ is an abelian group.

Proof of Theorem 1.4. Let $P \in X(k)$. Fix any point $Q \in Y(\bar{k})$ with $\pi(Q) = P$. For $\sigma \in \Gamma_k$ we define $\xi_\sigma \in G(\bar{k})$ to be the unique deck transformation that sends Q to ${}^\sigma Q$. Then ξ is a 1-cocycle (note that the effect of ${}^\sigma\xi_\tau\xi_\sigma$ on Q is to send it first to ${}^\sigma Q$ and then to ${}^{\sigma\tau}Q$), and we let $\pi' \colon Y' \to X$ be the corresponding twist. This twist is constructed in such a way that $Q \in Y'(\bar{k}) = Y(\bar{k})$ is fixed by the Galois action, so $Q \in Y'(k)$. Conversely, if $\pi'' \colon Y'' \to X$ is another twist lifting P to a k-rational point Q' on Y'', then there is a unique isomorphism φ (over $\bar{k}$) of coverings between Y'' and Y' sending Q' to Q. The uniqueness together with the fact that φ sends one k-rational point to another k-rational point imply that φ is already defined over k and hence that the two twists are isomorphic. □

The statement of the theorem remains valid for ramified (but still geometrically Galois) coverings, as long as we stay away from the branch points. (The existence statement still holds there, but uniqueness fails.)

Theorem 1.4 provides us with a map $X(k) \to \mathrm{Twist}(\pi) = H^1(k,G)$.

So if we get some control on the twists (and their rational points), then we may get information on $X(k)$ as well. For example, if we could show that for every twist $Y' \to X$, the set $Y'(k)$ is actually empty, then it would follow that $X(k) = \emptyset$ as well. One way of doing this is to check if Y' is ELS. So we make the following definition.

Definition 1.6. Let $\pi \colon Y \to X$ be as above. We define the *π-Selmer set of X* to be the subset $\mathrm{Sel}^\pi(X)$ of $\mathrm{Twist}(\pi)$ consisting of twists $Y' \to X$ such that Y' is ELS.

Corollary 1.7. *If* $\mathrm{Sel}^\pi(X)$ *is empty, then* $X(k) = \emptyset$.

Now here is another important fact.

Theorem 1.8. *The Selmer set* $\mathrm{Sel}^\pi(X)$ *is finite. If π is given explicitly, then the Selmer set is effectively computable (at least in principle).*

Proof. For all but finitely many places v of k, both X and Y will have good reduction, and the reduction of π will still be étale. This implies that the fibre above a point in $X(k_v)$ will consist of points defined over an unramified extension of k_v. Now assume that the twist Y' has a k_v-point Q. Then its image $\pi'(Q)$ is a k_v-point P on X, and the fibre above P in Y consists of unramified points. If k_v^{unr} denotes the maximal unramified extension of k_v, then the fibres above P in both Y and Y' consist entirely of k_v^{unr}-points. This implies that Y and Y' are isomorphic over k_v^{unr}, i.e., the cocycle class in $H^1(k,G)$ corresponding to π' maps to the trivial element of $H^1(k_v^{\mathrm{unr}},G)$ under the canonical map (which is restriction of cocycles or base change to k_v^{unr}, depending on the interpretation). If S is the finite set of places that are either infinite or such that X, Y or π has bad reduction, then the cocycle classes corresponding to twists with Y' ELS are contained in

$$H^1(k,G;S) = \{\xi \in H^1(k,G) : \forall v \notin S \colon \rho_v(\xi) = 0\}\,,$$

where $\rho_v \colon H^1(k,G) \to H^1(k_v^{\mathrm{unr}},G)$ is the map mentioned above and we have used 0 to denote the trivial element of $H^1(K,G)$ for any field extension K of k. It is now a fundamental fact that the set $H^1(k,G;S)$ is finite. (This comes down to the statement that there are only finitely many extensions of k of bounded degree that are unramified outside S.)

We will see how Selmer sets can be computed in some special cases later in this lecture series. □

Note that for Theorem 1.8 it is essential that the covering is étale! The statement is false when π is ramified.

See [Sto07] for a detailed discussion of "descent obstructions" related to Selmer sets.

Exercises. Exercise (1) is quite instructive, but I would recommend doing Exercises (2) and (3) if your time is limited. The first part of Exercise (4) can be done by hand, but the second part will require the use of Magma or SAGE (or a similar system) and some experience with working with such a system.

(1) Work out an explicit proof of Theorem 1.1 in the case when X is a hyperelliptic curve, i.e., X is the smooth projective model of an affine plane curve of the form $y^2 = f(x)$, where $f \in k[x]$ is squarefree.

(2) Let $f_1, f_2 \in \mathbb{Z}[x]$ with f_1 of even degree. We take $k = \mathbb{Q}$. Let X be the nice curve associated to $y^2 = f_1(x)f_2(x)$ and let Y be the nice curve associated to $y_1^2 = f_1(x)$, $y_2^2 = f_2(x)$. Show that $\pi\colon (x, y_1, y_2) \mapsto (x, y_1y_2)$ defines an étale double cover $Y \to X$. Show that $\operatorname{Twist}(\pi)$ is in bijection with the set of squarefree integers, with an integer d corresponding to $Y_d\colon dy_1^2 = f_1(x), dy_2^2 = f_2(x)$ and $\pi_d\colon (x, y_1, y_2) \mapsto (x, dy_1y_2)$.

(3) Continuing the previous exercise, show that Y_d is not ELS if d is divisible by a prime p that does not divide the resultant of f_1 and f_2 (or the leading coefficient of f_1 when f_2 has odd degree).

(4) [Computational] Check that $X\colon y^2 = (-x^2 - x + 1)(x^4 + x^3 + x^2 + x + 2)$ is ELS, but its Selmer set with respect to the double cover constructed as in Exercise (2) is empty. Try to produce more examples of hyperelliptic curves $X\colon y^2 = f(x)$ over $\mathbb{Q}$ with these properties!.

2. Selmer groups

We now consider the case when X is a group variety. Since we assume that X is projective, this means that X is an *abelian variety*. We therefore write A instead of X in this section.

If A is an abelian variety over k, then there exist natural finite étale coverings of A coming from the structure of A as an abelian group: for each positive integer n, there is the multiplication-by-n map $A \xrightarrow{\cdot n} A$. This covering is geometrically Galois, with Galois group scheme $A[n]$, the n-torsion subgroup of A, acting by translations. Twists of the multiplication-by-n map are called *n-coverings* of A. In this case, the corresponding Selmer set is actually an abelian group, the *n-Selmer group* $\operatorname{Sel}^{(n)}(A)$ of A.

We remark that these coverings are basically the whole story in this case: any finite étale covering of A will (at least geometrically) be a morphism $B \to A$ of abelian varieties, surjective with finite fibres. Up to a translation on the target (which corresponds to a twist), this is an isogeny. Precomposing with the dual isogeny $A \to B$, we obtain a multiplication-by-n map that (up to twist) factors through the original covering, and so provides at least the same information.

This is related to the fact that the multiplication-by-n map fits into an exact sequence of k-Galois modules:

$$0 \longrightarrow A[n](\bar{k}) \longrightarrow A(\bar{k}) \xrightarrow{\cdot n} A(\bar{k}) \longrightarrow 0\,,$$

which induces an exact sequence in Galois cohomology

$$0 \longrightarrow A[n](k) \longrightarrow A(k) \xrightarrow{\cdot n} A(k) \xrightarrow{\delta} H^1(k, A[n]) \longrightarrow H^1(k, A) \xrightarrow{\cdot n} H^1(k, A)$$

giving rise to a short exact sequence

$$0 \longrightarrow \frac{A(k)}{nA(k)} \longrightarrow H^1(k, A[n]) \longrightarrow H^1(k, A)[n] \longrightarrow 0\,.$$

The middle group $H^1(k, A[n])$ classifies the twists of the multiplication-by-n map; a twist has k-rational points if and only if it is in the image of $A(k)$: the map $\delta \colon A(k) \to H^1(k, A[n])$ maps a point $P \in A(k)$ to the n-covering $A \to A$, $Q \mapsto nQ + P$, which is the n-covering lifting the point P. (By definition, $\delta(P)$ is the class of the cocycle $\sigma \mapsto {}^{\sigma}Q - Q$ for any point $Q \in A(\bar{k})$ such that $nQ = P$. Under the twisted action, we have $\sigma \cdot Q = \xi_\sigma^{-1}({}^{\sigma}Q) = {}^{\sigma}Q - ({}^{\sigma}Q - Q) = Q$, so that Q becomes a k-rational point on the corresponding twist, hence P lifts to a k-rational point on this twist.) Conversely, if an n-covering has a k-rational point Q, then it lifts some k-point of A, namely the image of Q.

The same argument works over any field of characteristic not dividing n; in particular, we can use it over k_v for each place v of k. Considering all places simultaneously, we obtain a commutative diagram with exact rows:

$$\begin{tikzcd}
0 \arrow[r] & \dfrac{A(k)}{nA(k)} \arrow[r] \arrow[d] & H^1(k, A[n]) \arrow[r] \arrow[d] \arrow[dr, "\alpha"] & H^1(k, A)[n] \arrow[r] \arrow[d, "\rho"] & 0 \\
0 \arrow[r] & \prod_v \dfrac{A(k_v)}{nA(k_v)} \arrow[r] & \prod_v H^1(k_v, A[n]) \arrow[r] & \prod_v H^1(k_v, A)[n] \arrow[r] & 0
\end{tikzcd}$$

The n-Selmer group consists of those twists that have points everywhere locally, which translates into the subgroup of $H^1(k, A[n])$ consisting of those elements whose image under the vertical map is contained in the image of the horizontal map into the product of the $H^1(k_v, A[n])$'s. This is equivalent to the statement

$$\mathrm{Sel}^{(n)}(A) = \ker \alpha\,.$$

Definition 2.1. We define the *Shafarevich-Tate group* of A to be

$$Ш(A) = \ker\Big(H^1(k, A) \longrightarrow \prod_v H^1(k_v, A)\Big)\,.$$

We then have that $\ker \rho = Ш(A)[n]$, and we obtain the short exact sequence

$$0 \longrightarrow \frac{A(k)}{nA(k)} \longrightarrow \mathrm{Sel}^{(n)}(A) \longrightarrow Ш(A)[n] \longrightarrow 0\,.$$

The Shafarevich-Tate group has a geometric interpretation: its elements correspond to the *principal homogeneous spaces* X for A over k that are ELS, up to k-isomorphism. Every n-covering of A is a principal homogeneous space for A in a natural and unique way; the map $H^1(k, A[n]) \to H^1(k, A)$ and its restriction $\mathrm{Sel}^{(n)}(A) \to Ш(A)[n]$ is in this interpretation just the forgetful map that forgets the n-covering structure and only retains the principal homogeneous space structure.

Now we have the following well-known result due to Mordell (for elliptic curves over $\mathbb{Q}$; [Mor22]) and Weil (in full generality; [Wei29]).

Theorem 2.2. *If A is an abelian variety over a number field k, then the group $A(k)$ of k-rational points on A is a finitely generated abelian group.*

In fact, the finiteness of the Selmer group (for any $n \geq 2$; see Theorem 1.8) is an important ingredient in the proof, since it shows that $A(k)/nA(k)$ is finite ("weak Mordell-Weil Theorem"), which is a necessary condition for $A(k)$ to be finitely generated. (The other important ingredient is the theory of heights.) Compare Adam Morgan's first lecture.

By the classification theorem for finitely generated abelian groups, we can therefore write $A(k) \simeq A(k)_{\text{tors}} \oplus \mathbb{Z}^r$, where $A(k)_{\text{tors}} \subset A(k)$ is the finite torsion subgroup of $A(k)$ and r is a nonnegative integer, the *rank* of $A(k)$. So we obtain an embedding

$$\frac{A(k)_{\text{tors}}}{nA(k)_{\text{tors}}} \oplus \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^r \hookrightarrow \operatorname{Sel}^{(n)}(A)\,.$$

In particular, the size of the n-Selmer group (for $n \geq 2$) gives us an *upper bound* on the rank r. (If we know $A(k)_{\text{tors}}/nA(k)_{\text{tors}}$, which is often easy to figure out, then the bound has a chance to be sharp). The n-torsion of $Ш(A)$ measures how far this upper bound is from the truth.

There is the following important conjecture.

Conjecture 2.3. *The Shafarevich-Tate group $Ш(A)$ is finite.*

Note that the finiteness of the Selmer groups together with the exact sequence above show that for all n, the n-torsion subgroup of $Ш(A)$ is finite. It is also known that $H^1(k, A)$ and therefore its subgroup $Ш(A)$ is a torsion group, i.e., all its elements have finite order. The conjecture is wide open in general; it is known for elliptic curves over $\mathbb{Q}$ of analytic rank 0 or 1 (a famous result due to Kolyvagin) and, more generally, for certain "modular" abelian varieties over $\mathbb{Q}$ with a similar restriction on the analytic rank (due to Kolyvagin and Logachëv).

Assuming Conjecture 2.3, we obtain an algorithm for determining the rank r of $A(k)$:

By day, compute $\operatorname{Sel}^{(p)}(A)$ for successive prime numbers p and set

$$R(p) = \min\{\dim_{\mathbb{F}_q} \operatorname{Sel}^{(q)}(A) : q \leq p\}\,;$$

this is an upper bound for r.

By night, search for points in $A(k)$ up to increasing height h and set $r(h)$ to be the rank of the subgroup generated by the points found up to this height; this is a lower bound for r. The conjecture guarantees that after finitely many days and nights we will have that $r(h) = R(p)$; this number is the rank.

In practice (at least when $\dim A \geq 2$), we often can compute only one Selmer group; we then hope that the relevant torsion of $Ш$ vanishes, so that the upper bound on the rank we can deduce gives the actual rank. We then need to find sufficiently many independent points in $A(k)$ to actually reach this bound. This is the standard way of determining the rank unconditionally (or sometimes conditional on the Generalised Riemann Hypothesis to make certain number field computations feasible), and it often works.

If we can compute several Selmer groups (for example, when A is an elliptic curve over $\mathbb{Q}$ and the coefficients in its defining equation are reasonably small), then we can also obtain information on $Ш$. For example, if we know that $A(k)_{\text{tors}}$ is trivial, we know one nontrivial point in $A(k)$, and we can show that $\dim_{\mathbb{F}_2} \operatorname{Sel}^{(2)}(A) = 3$ and $\dim_{\mathbb{F}_3} \operatorname{Sel}^{(3)}(A) = 1$, then we can conclude that $A(k) \simeq \mathbb{Z}$ and that $Ш(A)[2] \simeq (\mathbb{Z}/2\mathbb{Z})^2$ and $Ш(A)[3] = 0$.

For computational purposes, the following facts are relevant.

Proposition 2.4. *Let A be an abelian variety over k and let p be a prime number.*

(1) *Let v be a finite place of k. Then*
$$\dim_{\mathbb{F}_p} \frac{A(k_v)}{pA(k_v)} = \dim_{\mathbb{F}_p} A(k_v)[p] + \begin{cases} [k_v : \mathbb{Q}_p] \dim A & \text{if } v \text{ is above } p, \\ 0 & \text{else.} \end{cases}$$
If v is an infinite place of k and p is odd or v is complex, then $A(k_v)/pA(k_v) = 0$. If v is real, then
$$\dim_{\mathbb{F}_2} \frac{A(k_v)}{2A(k_v)} = \dim_{\mathbb{F}_2} A(k_v)[2] - \dim A\,.$$
(2) *If v is a finite place of k such that $v \nmid p$ and such that A has good reduction at v, then the image of $A(k_v)$ in $H^1(k_v, A[p])$ is exactly the unramified subgroup, i.e., the kernel of $H^1(k_v, A[p]) \to H^1(k_v^{\mathrm{unr}}, A[p])$.*

(3) *Let S be the set of places above p and the places of bad reduction for A, together with the real infinite places of k when $p = 2$ (then S is finite). Then*
$$\mathrm{Sel}^{(p)}(A) = \{\xi \in H^1(k, A[p]; S) : \forall v \in S \colon \operatorname{res}_v(\xi) \in \operatorname{im}(\delta_v)\}\,,$$
where $\delta_v \colon A(k_v) \to H^1(k_v, A[p])$ and $\operatorname{res}_v \colon H^1(k, A[p]) \to H^1(k_v, A[p])$ are the canonical maps.

The last statement reduces the computation of $\mathrm{Sel}^{(p)}(A)$ to that of (a suitable representation of) $H^1(k, A[p]; S)$ together with the determination of the image of δ_v for the finitely many places in S. Since the first statement tells us how large the image is, we can just find the images of (randomly or systematically generated) points in $A(k_v)$ until these images generate a subspace of the correct dimension. Assuming that we have a computable description of the maps res_v, this reduces the task to linear algebra over $\mathbb{F}_p$.

Proof.

(1) First assume that v is finite, of residue characteristic q. We use the fact that $A(k_v)$ contains a finite-index subgroup isomorphic to $\mathbb{Z}_q^{[k_v:\mathbb{Q}_q]\dim A}$. Consider the Snake Lemma diagram
$$\begin{tikzcd} 0 \arrow[r] & \mathbb{Z}_q^{[k_v:\mathbb{Q}_q]\dim A} \arrow[r] \arrow[d, "\cdot p"] & A(k_v) \arrow[r] \arrow[d, "\cdot p"] & T \arrow[r] \arrow[d, "\cdot p"] & 0 \\ 0 \arrow[r] & \mathbb{Z}_q^{[k_v:\mathbb{Q}_q]\dim A} \arrow[r] & A(k_v) \arrow[r] & T \arrow[r] & 0 \end{tikzcd}$$
(where T is the finite quotient). We obtain an exact sequence of $\mathbb{F}_p$-vector spaces
$$0 \longrightarrow A(k_v)[p] \longrightarrow T[p] \longrightarrow \Bigl(\frac{\mathbb{Z}_q}{p\mathbb{Z}_q}\Bigr)^{[k_v:\mathbb{Q}_q]\dim A} \longrightarrow \frac{A(k_v)}{pA(k_v)} \longrightarrow \frac{T}{pT} \longrightarrow 0\,.$$
This gives us (taking into account that $\dim T[p] = \dim T/pT$)
$$\dim \frac{A(k_v)}{pA(k_v)} = \dim A(k_v)[p] + [k_v : \mathbb{Q}_q](\dim A) \dim \frac{\mathbb{Z}_q}{p\mathbb{Z}_q}\,.$$
If $v \nmid p$, then $\mathbb{Z}_q/p\mathbb{Z}_q = 0$, and we obtain the desired result. If $v \mid p$, then $\mathbb{Z}_q/p\mathbb{Z}_q \simeq \mathbb{F}_p$, and we get the stated correction term.

If v is a complex infinite place, then the multiplication-by-p map is surjective on $A(k_v)$.

The same is true for real places when p is odd, since the preimage of any k_v-point has an odd number of geometric points, so at least one point must be real. In the case v real and $p = 2$, we use that $A(k_v)$ has a finite-index subgroup isomorphic to $(\mathbb{R}/\mathbb{Z})^{\dim A}$. We then use the Snake Lemma in a similar way as before.

(2) This follows from (1) and the fact that the dimension of the unramified subgroup is also $\dim A(k_v)[p]$, together with the statement already used earlier that under the assumptions made the image of δ_v is contained in the unramified subgroup of $H^1(k_v, A[p])$.

(3) Statement (2) implies that

$$H^1(k, A[p]; S) = \{\xi \in H^1(k, A[p]) : \forall v \notin S\colon\ \mathrm{res}_v(\xi) \in \mathrm{im}(\delta_v)\}\,.$$

So to get the Selmer group, we just have to impose the remaining conditions at the places $v \in S$. □

Exercises. Exercise (5) is a standard fact on Selmer groups. Exercise (6) is perhaps more interesting, since it provides a possible way how one can improve the upper bound on the rank obtained from a Selmer group computation.

(5) Let A be an abelian variety over k and let m and n be two coprime integers ≥ 1. Show that

$$\mathrm{Sel}^{(mn)}(A) \simeq \mathrm{Sel}^{(m)}(A) \oplus \mathrm{Sel}^{(n)}(A)\,.$$

(This means that it is usually sufficient to restrict n to be a prime power.)

(6) It is well possible that the upper bound on the rank obtained from a Selmer group is not tight. Assume that $A = E$ is an elliptic curve $y^2 = f(x)$ over $\mathbb{Q}$. Let $d \neq 1$ be a squarefree integer; then we can define the *quadratic twist* of E by d to be the elliptic curve $E^{(d)}\colon y^2 = df(x)$. It is known that

$$\mathrm{rank}\, E(\mathbb{Q}) + \mathrm{rank}\, E^{(d)}(\mathbb{Q}) = \mathrm{rank}\, E(\mathbb{Q}(\sqrt{d}))\,.$$

Assume also that you can compute the 2-Selmer groups of E over $\mathbb{Q}$ and over $\mathbb{Q}(\sqrt{d})$, and that you know the rank of $E^{(d)}(\mathbb{Q})$. How could you (in favourable circumstances) deduce a better upper bound for $\mathrm{rank}\, E(\mathbb{Q})$ from this information?

(This works in the same way for Jacobians of hyperelliptic curves.)

3. Selmer groups of elliptic curves

Let A be an abelian variety over k and fix a prime number p. Recall the description of the p-Selmer group from the last lecture:

$$\mathrm{Sel}^{(p)}(A) = \{\xi \in H^1(k, A[p]; S) : \forall v \in S\colon\ \mathrm{res}_v(\xi) \in \mathrm{im}(\delta_v)\}\,,$$

where S is the set of places of k containing the places dividing p, the places of bad reduction for A and, if $p = 2$, the real infinite places of k. So if we want to compute this p-Selmer group, we have to do several things:

1. We need a sufficiently explicit representation of $H^1(k, A[p])$ and of $H^1(k_v, A[p])$ together with the maps res_v.
2. We have to be able to determine the finite subgroup $H^1(k, A[p]; S)$ of $H^1(k, A[p])$.
3. We need an explicit way of evaluating the maps δ_v on points of $A(k_v)$ (in terms of the representation of $H^1(k_v, A[p])$).

In this section, we will look at the case when $A = E$ is an elliptic curve, which we will assume to be given by a Weierstrass equation $y^2 = f(x)$ with $f \in \mathcal{O}_k[x]$, where $\mathcal{O}_k$ is the ring of integers of k. We will consider the case $p = 2$ first. The elements of $E[2]$ are the origin O of the group law on E (which is the point at infinity in the given model) together with the three points $(\theta, 0)$ with θ a root of f. The action of Γ_k on $E[2]$ fixes O and permutes the three nontrivial elements in the same way as it permutes the roots of f. Let $L = k[x]/\langle f \rangle$; this is an étale algebra over k, which is the coordinate ring of the k-scheme whose geometric points are the three nontrivial 2-torsion points on E. Put differently, the elements of L correspond to Γ_k-equivariant maps $E[2] \setminus \{O\} \to \bar{k}$. Note that L splits as a product of finite field extensions of k, corresponding to the irreducible factors of f in $k[x]$ (by the Chinese Remainder Theorem).

Using the Weil pairing, a 2-torsion point T gives rise to a map $w_T \colon E[2] \setminus \{O\} \to \mu_2(\bar{k})$, $T' \mapsto e_2(T, T')$; such maps are given by the elements of $\mu_2(\bar{L})$, where $\bar{L} = L \otimes_k \bar{k}$, and the association $T \mapsto w_T$ is Γ_k-equivariant. An element w of $\mu_2(\bar{L})$ is of the form w_T for some $T \in E[2]$ if and only if $\prod_{T' \in E[2] \setminus \{O\}} w(T') = 1$ (this is because the Weil pairing is a perfect pairing). In other words, the norm of w with respect to the extension $\bar{L}/\bar{k}$ is 1. This leads to a short exact sequence of k-Galois modules

$$0 \longrightarrow E[2] \longrightarrow \mu_2(\bar{L}) \xrightarrow{N} \mu_2(\bar{k}) \longrightarrow 0\,.$$

This sequence is actually split; the inclusion $\mu_2(\bar{k}) \to \mu_2(\bar{L})$ provides a section. Applying Galois cohomology, we obtain a representation of $H^1(k, E[2])$ in the form

$$H^1(k, E[2]) \simeq \ker\Bigl(\frac{L^\times}{L^{\times 2}} \xrightarrow{N} \frac{k^\times}{k^{\times 2}}\Bigr)\,.$$

Here N denotes the map induced by the norm map from L to k. Note that we have used the Kummer isomorphisms $H^1(k, \mu_2(\bar{k})) = k^\times/k^{\times 2}$ and $H^1(k, \mu_2(\bar{L})) = L^\times/L^{\times 2}$, which can be deduced from the short exact sequence

$$0 \longrightarrow \mu_2(\bar{k}) \longrightarrow \bar{k}^\times \xrightarrow{\cdot^2} \bar{k}^\times \longrightarrow 0$$

(and the corresponding sequence for $\bar{L}$) together with “Hilbert's Theorem 90” $H^1(k, \bar{k}^\times) = 0$ and its easy extension $H^1(k, \bar{L}^\times) = 0$. This description works over any field of characteristic $\neq 2$ in place of k, in particular for the completions k_v.

This takes case of the first point in our list of tasks. Note that the restriction maps res_v in this representation are simply induced by the inclusions $L \hookrightarrow L_v$.

An element of $H^1(k, E[2])$, represented by some $\alpha \in L^\times$, is unramified at some finite place v of k if and only if its image in $H^1(k_v^{\mathrm{unr}}, E[2])$ is trivial. In terms of our representation, this means that α becomes a square in $L \otimes_k k_v^{\mathrm{unr}}$. If v is odd, then this is equivalent to saying that the valuation of α is even at each place above v in each component of L (regarding L as a product of finite field extensions of k).

Definition 3.1. If k is a number field, S is a finite set of places of k and L is an étale k-algebra, then we define

$$L(S, 2) = \{\alpha \in L^\times/L^{\times 2} : \forall v \notin S\ \forall w \mid v \colon w(\alpha) \in 2\mathbb{Z}\}\,,$$

where v runs through the finite places of k not in S, w runs through the places of L (more precisely, of the components of L) above v, and we abuse notation by writing $w(\alpha)$ for the normalised additive valuation of α associated to w.

Then $L(S,2)$ is a finite-dimensional $\mathbb{F}_2$-vector space (sometimes called the 2-*Selmer group of* $\mathcal{O}_{L,S}$, the ring of S-integers of L), which can be computed; this computation requires information on the class groups of the components of L and on their unit groups. If the number fields involved have large degree or the coefficients of f get large, one can reduce the computation time considerably by assuming the Generalised Riemann Hypothesis. Note that k itself is an étale k-algebra, so $k(S,2)$ is defined as well.

If S is the set of "bad" places for 2-descent on E (so S consists of the real infinite places, the places above 2 and the places of bad reduction for E), then these considerations imply that

$$H^1(k, E[2]; S) \simeq \ker\bigl(N\colon L(S,2) \to k(S,2)\bigr) .$$

This takes care of the second point in our list of tasks.

One can check that the connecting homomorphism $\delta\colon E(k) \to H^1(k, E[2])$ is given by sending a point $P = (\xi, \eta)$ to the class of $\xi - \theta$ in $L^\times/L^{\times 2}$, where θ is the image of x in L (θ is "the generic root of f"). The origin $P = O$ clearly goes to the trivial class. If $P = (\xi, 0)$ is a 2-torsion point, then the image of P would be zero in the component of L corresponding to $\theta = \xi$; this can be patched by using that the norm of the image has to be a square. We will abuse notation and write δ and δ_v for the compositions

$$E(k) \to H^1(k, E[2]) \to L^\times/L^{\times 2} \qquad \text{and} \qquad E(k_v) \to H^1(k_v, E[2]) \to L_v^\times/L_v^{\times 2} ,$$

where $L_v = L \otimes_k k_v$. Similarly, we write res_v for the canonical map $L^\times/L^{\times 2} \to L_v^\times/L_v^{\times 2}$. Note that (a standard fact) $L_v^\times/L_v^{\times 2}$ is a finite-dimensional $\mathbb{F}_2$-vector space, with which we can compute reasonably easily.

So we can also deal with the last point in our list.

We obtain the following computable description of the 2-Selmer group of E:

$$\mathrm{Sel}^{(2)}(E) \simeq \bigl\{\alpha \in L(S,2) : N(\alpha) = 1, \forall v \in S\colon \mathrm{res}_v(\alpha) \in \mathrm{im}(\delta_v)\bigr\} .$$

As mentioned at the end of the previous lecture, we can determine the dimension of $\mathrm{im}(\delta_v)$ beforehand. We then just have to find enough points in $E(k_v)$ to generate a subspace of $\mathrm{im}(\delta_v)$ of the correct dimension. (For odd places v, it usually suffices to consider the 2-torsion points in $E(k_v)$.) Given explicit $\mathbb{F}_2$-bases of $L(S,2)$, $k(S,2)$ and the $L_v^\times/L_v^{\times 2}$ for the places $v \in S$, we can represent the norm map and the maps res_v by matrices over $\mathbb{F}_2$, and we can describe the images of the maps δ_v by generators. This reduces the determination of the Selmer group to simple linear algebra over $\mathbb{F}_2$.

We remark that a very similar approach works when $A = J$ is the Jacobian variety of a hyperelliptic curve

$$C\colon y^2 = f(x)$$

with a squarefree polynomial $f \in k[x]$ of *odd* degree. (The even degree case is a little bit more involved. For details, see [Sto01].)

Before we try to extend this to p-Selmer groups with $p \geq 3$, we should stop for a moment and think about what was essential for our approach to work. The main point was that we could represent $E[2]$ as a submodule of a Galois module of the form $\mu_2(\bar{L})$ with an étale k-algebra L. We obtained this representation by using the Weil pairing on $E[2]$; L was the coordinate ring of a finite k-scheme X whose geometric points form a (Galois-stable) generating set of $E[2]$.

So we now choose a k-subscheme X of $E[p]$ that generates $E[p]$ and let L be the corresponding étale algebra. (Usually the Galois action will be transitive on $E[p] \setminus \{O\}$; then

L is a field extension of k of degree $p^2 - 1$.) In the same way as before, this gives us an injective homomorphism of Galois modules

$$w \colon E[p] \longrightarrow \mu_p(\bar{L}), \qquad T \longmapsto \bigl(T' \mapsto e_p(T, T')\bigr)\,,$$

where we have again identified the elements of $\mu_p(\bar{L})$ with maps $X \to \mu_p(\bar{k})$. We obtain an exact sequence

$$Q(k) \longrightarrow H^1(k, E[p]) \longrightarrow \frac{L^\times}{L^{\times p}}\,,$$

where Q is the quotient of $\mu_p(\bar{L})$ by the image of w. It can be shown that the left map is zero when the size of X (i.e., the degree of L) is not divisible by p, which applies in particular in the generic case when $X = E[p] \setminus \{O\}$. This also applies over k_v for any place v of k. So we have an embedding of $H^1(k, E[p])$ into $L^\times/L^{\times p}$ (and similarly for the local versions). It remains to describe the image of this embedding as a kernel of a further map. This can be done. For $p = 3$, we obtain the following description.

Proposition 3.2. *Let E be an elliptic curve over k. Let L be the étale algebra corresponding to the nonzero elements of $E[3]$, and let L' be the étale algebra corresponding to the nonzero elements of* $\operatorname{Hom}(E[3], \mathbb{Z}/3\mathbb{Z})$. *There is a subalgebra L^+ of L, which corresponds to the unordered pairs $\{P, -P\}$ of nonzero elements of $E[3]$. Then*

$$H^1(k, E[3]) \simeq \{\alpha \in L^\times/L^{\times 3} : N_{L/L^+}(\alpha) = 1, u(\alpha) = 1\}\,,$$

where $u \colon L^\times/L^{\times 3} \to L'^\times/L'^{\times 3}$ is induced by a certain group homomorphism $L^\times \to L'^\times$.

(The homomorphism $L^\times \to L'^\times$ is defined in the following way. Let M be the étale algebra corresponding to the subset $Y = \{(P, \phi) : \phi(P) = 1\}$ of $(E[3]\setminus\{O\}) \times (\operatorname{Hom}(E[3], \mathbb{Z}/3\mathbb{Z}) \setminus \{0\})$. The projections to the first and second components induce inclusions $i_{M/L} \colon L \to M$ and $L' \to M$. The homomorphism is then given as $N_{M/L'} \circ i_{M/L}$. The background for this is the following. Let p be an odd prime, and let V be a two-dimensional $\mathbb{F}_p$-vector space. Then a map $\phi \colon V \to \mathbb{F}_p$ is a homomorphism if and only if ϕ is homogeneous of degree 1 (i.e., $\phi(\lambda v) = \lambda\phi(v)$ for $\lambda \in \mathbb{F}_p$ and $v \in V$) and has the property that $\sum_{v \in \ell} \phi(v) = 0$ for every affine line $0 \notin \ell \subset V$. The first condition translates into $N_{L/L^+}(\alpha) = 1$ and the second into $u(\alpha) = 1$. This generalises to larger odd p; the first condition gets a bit more involved, though. In the general case, L^+ corresponds to the set of cyclic subgroups of order p of $E[p]$.)

This description can then be used in an analogous way as before for $p = 2$ to compute $\operatorname{Sel}^{(3)}(E)$. When $k = \mathbb{Q}$, this involves number fields of degree 8 and their class and unit groups. These computations are quite feasible when the coefficients in the defining equation of E are not too large; Magma has an implementation.

For details, see [SS04].

Exercises. I recommend doing Exercise (7) to get a feeling of how the computation of a Selmer groups works in a fairly simple case. For Exercise (8), you probably need to use a suitable computer algebra system again.

(7) Consider the curves $E_p \colon y^2 = x^3 - p^2 x$ with a prime p. Try to determine the $\mathbb{F}_2$-dimension of $\operatorname{Sel}^{(2)}(E_p)$.

(8) [Computational] Produce an example where the approach of Problem (6) actually gives a better bound!

4. Selmer sets of hyperelliptic curves

Let $C\colon y^2 = f(x)$ be a hyperelliptic curve over k, where $f \in k[x]$ is a squarefree polynomial of odd degree $2g+1$ or even degree $2g+2$; then g is the genus of the curve. In the exercises to the first lecture, you have seen that if f factors as $f = f_1 f_2$ with at least one of the factors of even degree, then there is an étale double cover $\pi\colon D \to C$, which one can use to define and compute a Selmer set of C. In general, however, the polynomial f will not factor in this way (generically, f will even be irreducible), and so we need to come up with another way of constructing an étale covering of C.

We consider the odd degree case first. By scaling x and y suitably, we can arrange for f to be *monic* and to have coefficients in the ring of integers of k. Let J denote the Jacobian variety of C; this is an abelian variety of dimension g (the genus of C). The smooth projective model of C has a unique point "at infinity" (which is not a point on the affine model given above); it is k-rational (because it is unique), and we will denote it by ∞. Then there is a canonical embedding i of C into J, given by sending $P \in C$ to the divisor class $[P - \infty]$. Now the multiplication-by-2 map $J \to J$ is étale, and we can pull it back to C along i. This gives a Cartesian diagram

$$\begin{tikzcd}
D \arrow[r, hook] \arrow[d, "\pi"] & J \arrow[d, "\cdot 2"] \\
C \arrow[r, hook, "i"] & J
\end{tikzcd}$$

with an étale covering $\pi\colon D \to C$, which is geometrically Galois with Galois group scheme $J[2]$. As already hinted at in the previous lecture, we can represent $H^1(k, J[2])$ in a way analogous to $H^1(k, E[2])$ for an elliptic curve E. We describe this in more detail. Let again $L = k[x]/\langle f \rangle$. The 2-torsion subgroup $J[2]$ is generated by the divisor classes $T_\theta = [(\theta, 0) - \infty]$, where θ runs through the roots of f; the only relation between these generators is that their sum vanishes (the divisor $\sum_\theta (\theta, 0) - (2g+1)\cdot\infty$ is the principal divisor of the function y). We can again define a homomorphism

$$w\colon J[2] \longrightarrow \mu_2(\bar{L}), \qquad w(T) = \bigl(\theta \mapsto e_2(T, T_\theta)\bigr)\,,$$

which sits in a split exact sequence

$$0 \longrightarrow J[2] \xrightarrow{w} \mu_2(\bar{L}) \xrightarrow{N} \mu_2(\bar{k}) \longrightarrow 0$$

as before. In the same way as for elliptic curves, this results in

$$H^1(k, J[2]) \simeq \ker\Bigl(N\colon \frac{L^\times}{L^{\times 2}} \longrightarrow \frac{k^\times}{k^{\times 2}}\Bigr)\,.$$

Since k_v-points on C map via i to k_v-points of J, we get a natural inclusion of $\operatorname{Sel}^\pi(C)$ into the 2-Selmer group $\operatorname{Sel}^{(2)}(J)$ of J; in particular, $\operatorname{Sel}^\pi(C) \subset H^1(k, J[2]; S)$, where S is the finite set containing the infinite places of k, the places above 2 and the places of bad reduction for J (the latter subset is contained in the set of places of bad reduction for C, which is in turn contained in the set of prime divisors of twice the discriminant of f). However, it is no longer true that for each place v outside S, the image of $C(k_v)$ in $H^1(k_v, J[2])$ is the full kernel of the restriction homomorphism to $H^1(k_v^{\mathrm{unr}}, J[2])$. We now assume that S contains all places of bad reduction for C (not just for J). We can prove that we get the full kernel in general only when v is sufficiently large, in the sense that the residue class field of v is sufficiently large. The point is that when the residue class field κ_v is large, then the Weil bounds guarantee that $D_\xi(\kappa_v) \neq \emptyset$ (recall that D_ξ has good reduction at places $v \notin S$, so it makes sense to consider $D(\kappa_v)$) for any unramified twist $\xi \in H^1(k_v, J[2])$, and Hensel's Lemma will then produce k_v-points on D_ξ; the image on C of any such point will map to ξ.

So how large has κ_v to be for this argument to work? The Weil bounds imply that $D_\xi(\kappa_v)$ is non-empty when $p + 1 > 2g'\sqrt{p}$, where g' is the genus of D (which is also the genus of D_ξ). This will be the case when $p \ge 4{g'}^2$ (then $p + 1 > 2g'\sqrt{p+1} > 2g'\sqrt{p}$; the best bound is only slightly better). Now, by the Riemann-Hurwitz formula, we have that

$$g' - 1 = (\deg \pi)(g - 1) = \#J[2] \cdot (g - 1) = 4^g(g - 1)\,.$$

For $g = 2$, this gives $g' = 17$, and our lower bound above for p is $4 \cdot 17^2 = 1156$, and the smallest prime for which the Weil lower bound is positive is $p = 1163$ (it is still negative for the preceding prime 1153). For $g = 3$, the largest prime for which the bound is negative is $p = 66553$.

So, taking $S' = S \cup \{v \text{ finite} : \#\kappa_v < 4(4^g(g - 1))^2\}$ and

$$\delta_{C,v} \colon C(k_v) \longrightarrow \frac{L_v^\times}{L_v^{\times 2}}, \qquad (\xi, \eta) \longmapsto (\xi - \theta) \cdot L_v^{\times 2}$$

(with some patching for points with $\eta = 0$), where θ is again the image of x in L_v, we have the following explicit description of the π-Selmer set of C (which is usually called the 2-*Selmer set* of C, since the covering is induced by the multiplication-by-2 map on the Jacobian):

$$\operatorname{Sel}^{(2)}(C) = \operatorname{Sel}^\pi(C) = \bigl\{\alpha \in L(S, 2) : N(\alpha) = 1, \forall v \in S' \colon \operatorname{res}_v(\alpha) \in \operatorname{im}(\delta_{C,v})\bigr\}\,.$$

In practice (at least when $g \ge 3$), it takes too long to compute the image of $\delta_{C,v}$ for all the places in $S' \setminus S$: this is basically equivalent to enumerating all κ_v-points on C, so will take time at least proportional to $\#\kappa_v$. Also, it is fairly rare that the image of $\delta_{C,v}$ is *not* the full unramified subgroup of $H^1(k_v, J[2])$ when κ_v is moderately large, so that these larger places almost never make a difference. So what one does is to use a smaller set S' that includes S and all places up to some bound for κ_v that is quite a bit smaller than the theoretical bound. This may not give $\operatorname{Sel}^\pi(C)$, but in any case it will result in a set that contains $\operatorname{Sel}^\pi(C)$. If we can find enough k-rational points on C so that their images under δ_C cover the full set we have computed, then we know that we actually have computed $\operatorname{Sel}^\pi(C)$. Note that for f of odd degree, there is always the point $\infty \in C(k)$, so that $\operatorname{Sel}^\pi(C)$ always contains the neutral element of $H^1(k, J[2])$.

We now discuss what changes when f has even degree. The main complication is that there is no longer the nice split exact sequence that exhibits $J[2]$ as a submodule of $\mu_2(\bar{L})$. In the odd degree case, we could use the point at infinity as a kind of base-point. We can try to do something similar, but with fixing one of the ramification points $(\theta_0, 0)$ as a base-point. This gives a map

$$w_{\theta_0} \colon J[2] \longrightarrow \mu_2(\bar{L}), \qquad T \longmapsto \bigl(\theta \mapsto e_2([(\theta, 0) - (\theta_0, 0)], T)\bigr)\,.$$

However, this map is no longer a homomorphism of Galois modules (unless $\theta_0 \in k$, but then we can transform our equation for C into one of odd degree). If we replace θ_0 by θ_1, then we find that

$$w_{\theta_1}(T) = w_{\theta_0}(T) \cdot e_2\bigl([(\theta_0, 0) - (\theta_1, 0)], T\bigr) \in w_{\theta_0}(T) \cdot \mu_2(\bar{k})\,.$$

This shows that we do obtain a homomorphism of Galois modules (which can be checked to be injective)

$$w \colon J[2] \longrightarrow \frac{\mu_2(\bar{L})}{\mu_2(\bar{k})}, \qquad T \longmapsto w_{\theta_0}(T) \cdot \mu_2(\bar{k})$$

for any θ_0 that is a root of f. The image of w is again the subgroup of elements whose norm is 1 (note that here both elements of $\mu_2(\bar{k})$ have norm 1, so that the norm map descends to the quotient). We obtain a commutative diagram with exact rows and columns:

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & & \\
 & \mu_2(\bar{k}) \arrow[r, equal] \arrow[d, hook] & \mu_2(\bar{k}) \arrow[d, hook] & & \\
0 \arrow[r] & \mu_2(\bar{L})^0 \arrow[r, hook] \arrow[d] & \mu_2(\bar{L}) \arrow[r, "N"] \arrow[d] & \mu_2(\bar{k}) \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & J[2] \arrow[r, "w"] \arrow[d] & \dfrac{\mu_2(\bar{L})}{\mu_2(\bar{k})} \arrow[r, "N"] \arrow[d] & \mu_2(\bar{k}) \arrow[r] & 0 \\
 & 0 & 0 & &
\end{tikzcd}$$

Here $\mu_2(\bar{L})^0$ denotes the kernel of the norm map on $\mu_2(\bar{L})$. This gives a diagram in cohomology:

$$\begin{tikzcd}
 & & \dfrac{L^\times}{k^\times L^{\times 2}} \arrow[d, hook] & \\
\mu_2(k) \arrow[r, "\partial"] & H^1(k, J[2]) \arrow[r, "w_*"] & H^1\Big(k, \dfrac{\mu_2(\bar{L})}{\mu_2(\bar{k})}\Big) \arrow[r, "N_*"] \arrow[d] & \dfrac{k^\times}{k^{\times 2}} \\
 & & \mathrm{Br}(k)[2] &
\end{tikzcd}$$

It can be shown that the image of the 2-Selmer group of J under w_* is contained in the image of the upper vertical map (one can write down an explicit map $J(k_v) \to L_v^\times/(k_v^\times L_v^{\times 2})$ that is compatible with w_*, so the image in $\mathrm{Br}(k_v)$ is trivial; one then uses the local-global principle for the Brauer group of k) so that we obtain an inclusion

$$w_*\big(\mathrm{Sel}^{(2)}(J)\big) \subset \ker\Big(N\colon \frac{L^\times}{k^\times L^{\times 2}} \to \frac{k^\times}{k^{\times 2}}\Big)\,.$$

It is also true that the image of ∂ is contained in the Selmer group. The map ∂ is nontrivial if and only if there is an element of norm -1 in $H^0(k, \mu_2(\bar{L})/\mu_2(\bar{k}))$, which is the case if and only if either f splits off a factor of odd degree over k or else f is a constant times the product of two conjugate factors of odd degree defined over a quadratic extension of k. Generically, ∂ is nontrivial and so the "fake 2-Selmer group"

$$\mathrm{Sel}^{(2)}_{\mathrm{fake}}(J) = w_*\big(\mathrm{Sel}^{(2)}(J)\big) \subset \frac{L^\times}{k^\times L^{\times 2}}$$

has $\mathbb{F}_2$-dimension one less than the Selmer group itself. The fake 2-Selmer group is what can be computed (at least when g is even or C has points everywhere locally), which is done in a way similar to the odd degree case. For details, we refer to [PS97] and [Sto01]. For the general theory of "true" and "fake descents", see [BPS16].

Even though in the even degree case there is no canonical embedding of C into J (maybe even none at all that is defined over k!), we can still define a "fake 2-Selmer set" of C in a very similar way as before:

$$\mathrm{Sel}^{(2)}_{\mathrm{fake}}(C) = \left\{\alpha \in \frac{L^\times}{k^\times L^{\times 2}} : N(\alpha) = ck^{\times 2}, \forall v\colon\ \mathrm{res}_v(\alpha) \in \mathrm{im}(\delta_{C,v})\right\},$$

where $\delta_{C,v}$ evaluates to $(\xi - \theta) \cdot k_v^\times L_v^{\times 2}$ at a point $(\xi, \eta) \in C(k_v)$ (with the usual patches when $\eta = 0$ or the point is at infinity) and c is the leading coefficient of f. We can again reduce to (the image of) $L(S, 2)$, but we now have to include the places dividing c in S. As before, we compute in practice a superset of the fake Selmer set, which we can show to be the fake Selmer set if we find enough points to cover it. In contrast to the odd degree case, where there is always the rational point at infinity, now it is quite possible that the fake 2-Selmer set is empty (which follows if the superset we compute is empty), which then proves that C has no k-rational points.

For details on computing 2-Selmer sets of hyperelliptic curves, see [BS09]. In [Bha13], Bhargava uses 2-Selmer sets together with statistical information that comes out of his "geometry of numbers" approach to Selmer group sizes and other data to show that (as the genus gets large), "almost no" hyperelliptic curves over $\mathbb{Q}$ have $\mathbb{Q}$-rational points. In [PS14], a similar approach is used to show that (again as the genus gets large), most odd degree hyperelliptic curves over $\mathbb{Q}$ have the point at infinity as their only rational point.

Exercises. Exercise (10) is similar to Exercise (9), which already contains most of the relevant considerations.

(9) Let $C\colon y^2 = f(x)$ be hyperelliptic of odd degree. Consider an element of $\mathrm{Sel}^{(2)}(C)$, represented by some $\alpha \in L^\times$. Work out how one can obtain explicit equations for the corresponding twist $D_\alpha \to C$!

Hint. Consider the equation $\alpha z^2 = x - \theta$ for $x \in k$ and $z \in L$. Write z in terms of a k-basis of L. You should get an intersection of quadrics in a suitable projective space.

(10) Do the same in the even degree case. How is the fact that an element of the fake 2-Selmer group can represent two different twists reflected in the construction?

Acknowledgments

I would like to thank Tim and Vladimir Dokchitser for organising the *Advanced School and Workshop on Arithmetic of hyperelliptic Curves* at the ICTP in Trieste, where this lecture course was held. I also would like to thank Alexander Betts for pointing out a few mistakes in an earlier version of these notes and for helping with the exercise sessions.

References

[Bha13] Manjul Bhargava, *Most hyperelliptic curves over $\mathbb{Q}$ have no rational points*, 2013. Preprint, `arXiv:1308.0395`. ↑4

[BPS16] Nils Bruin, Bjorn Poonen, and Michael Stoll, *Generalized explicit descent and its application to curves of genus 3*, Forum Math. Sigma **4** (2016), e6, 80, DOI 10.1017/fms.2016.1. MR3482281 ↑4

[BS09] Nils Bruin and Michael Stoll, *Two-cover descent on hyperelliptic curves*, Math. Comp. **78** (2009), no. 268, 2347–2370, DOI 10.1090/S0025-5718-09-02255-8. MR2521292 (2010e:11059) ↑4

[Mor22] Louis J. Mordell, *On the rational solutions of the indeterminate equation of the third and fourth degrees*, Proc. Cambridge Philos. Soc. **21** (1922), 179–192. ↑2

[PS97] Bjorn Poonen and Edward F. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*, J. Reine Angew. Math. **488** (1997), 141–188. MR1465369 (98k:11087) ↑4

[PS14] Bjorn Poonen and Michael Stoll, *Most odd degree hyperelliptic curves have only one rational point*, Ann. of Math. (2) **180** (2014), no. 3, 1137–1166, DOI 10.4007/annals.2014.180.3.7. MR3245014 ↑4

[Sto01] Michael Stoll, *Implementing 2-descent for Jacobians of hyperelliptic curves*, Acta Arith. **98** (2001), no. 3, 245–277, DOI 10.4064/aa98-3-4. MR1829626 ↑3, 4

[SS04] Edward F. Schaefer and Michael Stoll, *How to do a p-descent on an elliptic curve*, Trans. Amer. Math. Soc. **356** (2004), no. 3, 1209–1231, DOI 10.1090/S0002-9947-03-03366-X. MR2021618 ↑3

[Sto01] Michael Stoll, *Implementing 2-descent for Jacobians of hyperelliptic curves*, Acta Arith. **98** (2001), no. 3, 245–277, DOI 10.4064/aa98-3-4. MR1829626 ↑3, 4

[Sto07] ———, *Finite descent obstructions and rational points on curves*, Algebra Number Theory **1** (2007), no. 4, 349–391, DOI 10.2140/ant.2007.1.349. MR2368954 (2008i:11086) ↑1

[Wei29] A. Weil, *L'arithmétique sur les courbes algébriques*, Acta Math. **52** (1929), 281–315. ↑2

Universität Bayreuth, 95440 Bayreuth, Germany