CONCRETE SELMER GROUP MANIPULATIONS

BRIAN OSSERMAN

1. A Brief Lemma

We begin with a basic lemma whose proof is short but clever:

**Lemma 1.** Let $G$ be a finite group of order $n$, and $A$ a $G$-module. Then multiplication by $n$ is the 0 map on $H^k(G, A)$ for all $k > 0$.

**Proof:** The key is to make use of the trace map on an injection resolution of $A$ by $G$-modules. Denote by $\text{Tr}_G$ the trace map, defined on any $G$-module, sending an element to the sum of its $G$-conjugates. Fix an injective resolution

$$0 \rightarrow A \rightarrow I_0 \rightarrow I_1 \rightarrow I_2 \rightarrow \ldots$$

Then $H^k(G, A)$ is the cohomology of the complex

$$0 \rightarrow I_0^G \rightarrow I_1^G \rightarrow I_2^G \rightarrow \ldots$$

For $k > 0$, pick any element $x \in I_k^G$ mapping to 0 in $I_{k+1}^G$; by the exactness of the injective resolution, there is a $y \in I_{k-1}$ which maps to $x$. Then $\text{Tr}_G y \in I_{k-1}^G$, and maps to $\text{Tr}_G x$. But $x$ is fixed by $G$, so $\text{Tr}_G x = nx$. Thus, $[x] = 0$ in $H^k(G, A)$, as desired.

This leads immediately to the following corollary:

**Corollary 1.** Let $G$ be a finite group of order $n$, relatively prime to the order of a finite $G$-module $A$. Then $H^k(G, A) = 0$ for all $k > 0$.

**Proof:** Since the order of $A$ is prime to $n$, multiplication by $\frac{1}{n}$ is a well-defined map (of $G$-modules) from $A$ to itself, which means it is also a well-defined map on cocycles. Thus, any cocycle is $n$ times another cocycle, and from the lemma the result follows immediately.

2. A Pairing

In this section we will assume that $p$ is odd, and $\text{Gal}(\mathbb{Q}(E[p])\mathbb{Q}) \cong GL_2(\mathbb{Z}/p\mathbb{Z})$. Write $L = K(E[p])$. We have assumed that $D$ (the discriminant of $K$) is prime to $N$ and to $p$, so the ramification of $\mathbb{Q}(E[p])$ over $\mathbb{Q}$ is disjoint from the ramification of $K$ over $\mathbb{Q}$, and their intersection is therefore just $\mathbb{Q}$. Hence, they are linearly disjoint extensions, so $\text{Gal}(L/K) \cong \text{Gal}(\mathbb{Q}(E[p])\mathbb{Q})$. We write $G$ for $\text{Gal}(L/K)$.

We wish to show:

**Proposition 1.** (Grass 9.1) The restriction map gives an isomorphism:

$$H^1(G_K, E[p]) \rightarrow H^1(G_L, E[p])^G = \text{Hom}_G(G_L, E[p])$$
Proof: Since $G_L$ is normal in $G_K$ (with quotient $\mathcal{G}$), by the Hochschild-Serre spectral sequence, the kernel of the restriction map is $H^1(\mathcal{G}, E[p])$ and the cokernel maps into $H^2(\mathcal{G}, E[p])$, so we wish to show both of these are trivial. In fact, $H^k(\mathcal{G}, E[p]) = 0$ for all $k$, which we shall show via another Hochschild-Serre spectral sequence, using the normal subgroup $Z \subset \mathcal{G}$ given by $Z = \mathbb{Z}/p\mathbb{Z}$; that is, the subgroup which corresponds to the subgroup of $\text{Aut}(E[p])$ that simply multiplies torsion points by integers which are non-zero mod $p$ (equivalently, the scalar matrices of $GL_2(\mathbb{Z}/p\mathbb{Z})$). We have

$$H^n(\mathcal{G}/Z, H^n(Z, E[p])) \Rightarrow H^{n+2}(\mathcal{G}, E[p])$$

Thus, to complete the proof of the proposition, it suffices to note $H^n(Z, E[p]) = 0$ for all $n$. $H^0(Z, E[p]) = 0$ because $p > 2$, while $H^n(Z, E[p]) = 0$ for all $n > 0$ by the corollary to our lemma above, as $Z$ has order $p - 1$ and $E[p]$ has order $p^2$.

The isomorphism of this proposition gives us a pairing

$$[\cdot, \cdot] : H^1(G_K, E[p]) \times G_L \rightarrow E[p]$$

which is nondegenerate on the left in the sense that if $[s, \rho] = 0$ for all $\rho \in G_L$, then $s = 0$. It also satisfies $[\sigma(s), \sigma(\rho)] = [s, \sigma(\rho)] = \sigma([s, \rho])$ for all $\sigma \in \mathcal{G}$.

Suppose $S$ is a finite subgroup of $H^1(G_K, E[p])$. Let $G_S$ be the (normal) subgroup of $G_L$ of $\rho$ such that $[s, \rho] = 0$ for all $s \in S$, and write $L_S$ for the fixed field of $G_S$, a finite Galois extension of $L$. Then:

**Proposition 2.** (Gross 9.3) The induced pairing

$$[\cdot, \cdot] : S \times \text{Gal}(L_S/L) \rightarrow E[p]$$

is nondegenerate, and gives Galois module isomorphisms $\text{Gal}(L_S/L) \cong \text{Hom}(S, E[p])$, $S \cong \text{Hom}_G(\text{Gal}(L_S/L), E[p])$.

Proof: Non-degeneracy of the pairing is immediate: it is nondegenerate on the left side because it is the restriction of a left nondegenerate pairing, and it is non-degenerate on the right because we have modded out by the $\rho$ which pair to 0 with $S$. This means the pairing induces injections $\text{Gal}(L_S/L) \hookrightarrow \text{Hom}(S, E[p])$ and $S \hookrightarrow \text{Hom}_G(\text{Gal}(L_S/L), E[p])$. Now, $S$ is a $\mathbb{Z}/p\mathbb{Z}$ vector space, say of dimension $r$. Then $\text{Hom}(S, E[p]) \cong E[p]^r$ which, since $E[p]$ is a simple Galois module, is semisimple. Thus, $\text{Gal}(L_S/L) \cong E[p]^s$ for some $s \leq r$. But since $\mathcal{G}$ is the full linear group acting on $E[p]$, the only endomorphisms that commute with it are the scalar maps, and $\text{Hom}_G(E[p], E[p]) = \mathbb{Z}/p\mathbb{Z}$, so $\text{Hom}_G(\text{Gal}(L_S/L), E[p]) = \text{Hom}_G(E[p]^s, E[p]) = \mathbb{Z}/p\mathbb{Z}^s$. But we assumed that $S \cong \mathbb{Z}/p\mathbb{Z}^s$, and $S$ injects into $\text{Hom}_G(\text{Gal}(L_S/L), E[p])$, so $r = s$ and in fact $r = s$ and both injections induce isomorphisms.

3. The Selmer Group

We now apply the results of the previous section to $S = \text{Sel}_p(E/K)$. Following Gross' notation, we write $M = L_S$, $H = \text{Gal}(M/L) = \text{Gal}(L_S/L)$. We also assume that $p$ does not divide the Heeger point $y_K$ in $E(K)$, so that its image $\delta y_K$ in $\text{Sel}_p(E/K)$ is non-zero. Since $L$ contains $E[p]$, $L(\frac{1}{p}y_K)$ is a Galois extension of $L$. Moreover, it is a subfield of $M$, since an element $\sigma$ of $G_M$ is, by definition, an element of $G_L$ which pairs to 0 with anything in $\text{Sel}_p(E/K)$, which is to say that any cocycle $f \in \text{Sel}_p(E/K) \subset H^1(G_K, E[p])$ sends $\sigma$ to 0. In particular, $\delta y_K$ defines a cocycle by $\sigma \mapsto \sigma(\frac{1}{p}y_K) - \frac{1}{p}y_K$ for some fixed choice of $\frac{1}{p}y_K$, and since
this maps \( \sigma \) to 0, \( \sigma \) fixes \( L(\frac{1}{p}y_K) \). Thus, \( L(\frac{1}{p}y_K) \) is indeed a subfield of \( M \), and we can write \( I \) for the subgroup of \( H \) fixing it. Note that the Galois action on \( \frac{1}{p}y_K \)

sends it precisely to the other possible choices of \( \frac{1}{p}y_K \), or equivalently, to \( \frac{1}{p}y_K \) plus elements of \( E[p] \), so \( H/I \cong E[p] \). Lastly, let \( \tau \) be a choice of complex conjugation map in \( \text{Gal}(M/\mathbb{Q}) \), and write \( H^+ \) and \( I^+ \) for the subgroups of \( H \) and \( I \) fixed by conjugation by \( \tau \).

**Lemma 2.** We can express \( H^+ = \{ (\tau h)^2 : h \in H \} \), \( I^+ = \{ (\tau i)^2 : i \in I \} \), and \( H^+/I^+ \cong \mathbb{Z}/p\mathbb{Z} \).

**Proof:** Note that by the previous proposition, \( H \cong \text{Hom}(\text{Sel}_p(E/K), E[p]) \), and is in particular a \( \mathbb{Z}/p\mathbb{Z} \) vector space. Then I claim that \( H^+ = H^{\tau+1} = \{ h^\tau h : h \in H \} \):

- certainly \( H^+ \), which is the kernel of \( \tau - 1 \), contains \( H^{\tau+1} \), as \( \tau^2 - 1 = 0 \). On the other hand if \( h \in H^+, h^\tau+1 = h^2 \), and since \( p \) is odd and \( H \) is a \( \mathbb{Z}/p\mathbb{Z} \) vector space, squaring (i.e., multiplication by \( 2 \)) is an automorphism (of Galois modules), so \( h = (h^{1/2})^{\tau+1} \)

and is in \( H^{\tau+1} \), as desired. But \( h^\tau = \tau h^{-1} = \tau h \), so \( h^\tau h = (\tau h)^2 \). The same argument applies to \( I^+ \). Lastly, this implies that \( H^+/I^+ = (H/I)^+ = E[p]^+ \cong \mathbb{Z}/p\mathbb{Z} \).

**Proposition 3.** (Gross 9.5) Let \( s \in \text{Sel}_p(E/K)^\pm \). The following are equivalent:

i) \( [s, \rho] = 0 \) for all \( \rho \in H \)
ii) \( [s, \rho] = 0 \) for all \( \rho \in H^+ \)
iii) \( [s, \rho] = 0 \) for all \( \rho \in H^+ \cap I^+ \)
iv) \( s = 0 \)

**Proof:** The implications iv) \( \Rightarrow i) \Rightarrow ii) \Rightarrow iii) \) are trivial. Moreover, by the nondegeneracy of our pairing, i) \( \Rightarrow iv) \). Thus, it suffices to show that iii) \( \Rightarrow i) \).

Now, \( s \) defines a group homomorphism from \( H^+ \) to \( E[p] \), and by the lemma, \( I^+ \subseteq H^+ \), so a vanishing on \( H^+ \cap I^+ \) means it must vanish on all of \( H^+ \). But we chose \( s \in \text{Sel}_p(E/K)^\pm \), so the homomorphism it induces \( H \rightarrow E[p] \) maps \( H^+ \rightarrow E[p]^\pm \), and \( H^- \rightarrow E[p]^\mp \). Since \( s \) vanishes on \( H^+ \), \( s(H) \subseteq E[p]^\mp \). But \( s(H) \) is a \( G \)-submodule of \( E[p] \), which is simple, so if it is strictly contained inside it, it must be trivial, and \( s(H) = 0 \), as desired.

The last step is to relate the vanishing of the pairing \([,] \) on very particular Galois automorphisms to local vanishing of \( s \), which will, when put together with the previous proposition, allow us to relate local vanishing of \( s \) at enough places to global vanishing. For this part, let \( \lambda \) be a prime of \( K \) not dividing \( N_p \), then it is unramified in \( M/K \). Suppose further that \( \lambda \) splits in \( l/K \), and write \( \lambda_M \) for a prime factor of \( \lambda \) in \( M \). The Frobenius element \( \text{Fr}_{M/K}(\lambda_M) \) in \( \text{Gal}(M/K) \) is actually in \( H \), due to the hypothesis that \( \lambda \) splits in \( L \). Moreover, the \( G \)-orbit of \( \text{Fr}_{M/K}(\lambda_M) \), which we write \( \text{Frob}(\lambda) \), depends, as the notation suggests, only on \( \lambda \).

**Proposition 4.** (Gross 9.6) For \( s \in \text{Sel}_p(E/K) \), the following are equivalent:

i) \( [s, \text{Fr}_{M/K}(\lambda_M)] = 0 \)
ii) \( [s, \rho] = 0 \) for all \( \rho \in \text{Frob}(\lambda) \)
iii) \( s_{\lambda} = 0 \) in \( H^1(G_{K_{\lambda}}, E[p]) \)

**Proof:** The equivalence of i) and ii) follows from the property of \([,] \) that \( [s, \sigma(\rho)] = \sigma([s, \rho]) \), as all the elements of \( \text{Frob}(\lambda) \) are conjugate to \( \text{Fr}_{M/K}(\lambda_M) \). Since the Shafarevich-Tate group of \( E \) is locally trivial by definition, we have an isomorphism between \( E(K_{\lambda})/pE(K_{\lambda}) \) and the local restriction of the \( p \)-Selmer group of
Thus, we can write $s_\lambda$ as $\sigma \mapsto \sigma(\frac{1}{pP_\lambda}) - \frac{1}{p}P_\lambda$ for some $P_\lambda$ in $E(K_\lambda)$ and a fixed choice of $\frac{1}{p}P_\lambda$. In particular, $[s, \text{Fr}_{M/K}(\lambda_M)] = \text{Fr}_{M/K}(\lambda_M)(\frac{1}{p}P_\lambda) - \frac{1}{p}P_\lambda$, which is 0 if and only if $\frac{1}{p}P_\lambda$ is in $E(K_\lambda)$, by the injectivity on $p$-torsion of the reduction map. And this is true if and only if $P_\lambda \in pE(K_\lambda)$, if and only if $s_\lambda = 0$. 