APPLYING THE LOCAL PAIRING TO SELMER GROUPS

BRIAN OSSERMAN

1. The Eigenspace Decomposition

Let E be an elliptic curve defined over $\mathbb{Q}$, but we will primarily think of it as being over K, an imaginary quadratic extension of $\mathbb{Q}$. Let K_λ be the local completion of K at a place λ which is inert over an integer prime l. We have p an odd prime, and l satisfies the relations $l+1 = a_l = 0 \pmod{p}$.

In Mihran's lectures, we had done Proposition 7.5 of Gross' paper, namely:

Proposition 1. *(Gross 7.5) Cup product induces a non-degerate pairing of $\mathbb{Z}/p\mathbb{Z}$-vector spaces (of dimension ≤ 2)*

$$\langle , \rangle : E(K_\lambda)/pE(K_\lambda) \times H^1(G_{K_\lambda}, E)[p] \to \mathbb{Z}/p\mathbb{Z}$$

We showed in Alex's lecture that $E[p]$ splits into one-dimensional eigenspaces for τ, the complex conjugation map in $\mathrm{Gal}(K/\mathbb{Q}) = \mathrm{Gal}(K_\lambda/\mathbb{Q}_l)$, so using $\pm$ to denote eigenspaces for τ, $E(K_\lambda)[p]^\pm$ are each one dimensional over $\mathbb{Z}/p\mathbb{Z}$ (since we have also assumed that $E(K_\lambda)$ contains the full p-torsion subgroup of E). Then the first order of business is to show that the pairing of Gross' Proposition 7.5 decomposes over τ-eigenspaces:

Proposition 2. *(Gross 8.1) The τ-eigenspaces $(E(K_\lambda)/pE(K_\lambda))^\pm$ and $H^1(G_{K_\lambda}, E)[p]^\pm$ are each 1-dimensional, and the pairing $\langle , \rangle$ of Proposition 7.5 induces non-degenerate pairings*

$$\langle , \rangle^\pm : (E(K_\lambda)/pE(K_\lambda))^\pm \times H^1(G_{K_\lambda}, E)[p]^\pm \to \mathbb{Z}/p\mathbb{Z}$$

Proof: In his lecture, Mihran exhibited isomorphisms $E(K_\lambda)/pE(K_\lambda) \cong E(K_\lambda)[p]$ and $H^1(G_{K_\lambda}, E(\overline{K_\lambda}))[p] \cong \mathrm{Hom}(\mu_p(\overline{K_\lambda}), E(\overline{K_\lambda})[p])^g$, where g was $\mathrm{Gal}({K_\lambda}^{un}/K_\lambda)$. Now, $E(K_\lambda)[p]^\pm \cong (E(K_\lambda)/pE(K_\lambda))[p]^\pm$, as our isomorphism was one of $G_{\mathbb{Q}_l}$-modules, and we conclude that the eigenspaces $(E(K_\lambda)/pE(K_\lambda))[p]^\pm$ each have dimension 1. But for the second isomorphism, we have since assumed that $E(\overline{K_\lambda})[p] = E(K_\lambda)[p]$, and further, the hypothesis that $l+1 = 0 \pmod{p}$ implies that $\mu_p(\overline{K_\lambda}) = \mu_p(K_\lambda)$, so the action of g is trivial, and we just get $H^1(G_{K_\lambda}, E(\overline{K_\lambda}))[p] \cong \mathrm{Hom}(\mu_p(K_\lambda), E(K_\lambda)[p])$. On the other hand, since p is odd, $l+1 = 0 \pmod{p}$ implies that $l-1 \neq 0 \pmod{p}$, so $\mu_p(\mathbb{Q}_\lambda) = \{1\}$, and $\mu_p(K_\lambda) = \mu_p(K_\lambda)^-$. Since $\mu_p(K_\lambda)$ is cyclic, $\mathrm{Hom}(\mu_p(K_\lambda), E(K_\lambda)[p]) \cong E(K_\lambda)[p]$ as groups; however, the action of τ is reversed by our observation that τ acts as the involution on $\mu_p(K_\lambda)$, so $E(K_\lambda)[p]^\pm \cong H^1(G_{K_\lambda}, E(\overline{K_\lambda}))[p]^\mp$, and we conclude that the eigenspaces $H^1(G_{K_\lambda}, E(\overline{K_\lambda}))[p]^\pm$ also both have dimension 1.

To show that our local pairing induces a pairing of eigenspaces, it suffices to check that the eigenspaces of opposite sign are orthogonal under $\langle , \rangle$. But the Tate pairing is compatible with the action of τ, so $\langle \tau(c_1), \tau(c_2) \rangle = \tau \langle c_1, c_2 \rangle = \langle c_1, c_2 \rangle$, as the pairing takes values in $\mathbb{Z}/p\mathbb{Z}$, which is Galois invariant. This implies that

$\langle c_1, c_2 \rangle = \langle \tau(c_1), \tau(c_2) \rangle = -\langle c_1, c_2 \rangle$ whenever c_1, c_2 are in opposite eigenspaces, and since p is not 2, the desired orthogonality follows.

We remark that the reason for the continual focus on τ-eigenspace decompositions is now clear, as we have worked ourselves down to one dimensional spaces, which means that to show that an element of $E(K_\lambda)/pE(K_\lambda)$ is trivial, if it lies in a τ-eigenspace, it suffices to produce a non-trivial element of the corresponding eigenspace of $H^1(G_{K_\lambda}, E(\overline{K_\lambda}))[p]$ which pairs to 0 with it. If our spaces weren't one dimensional, we would need an entire basis of such elements.

2. Application of Sum of Local Invariants

'Recall' from global class field theory that if K is a number field, there is an exact sequence $0 \to \mathrm{Br}(K) \to \bigoplus_\nu Br(K_\nu) \to \mathbb{Q}/\mathbb{Z} \to 0$ where the first map is a product of restriction maps, and the second map is summation, making use of the equality $\mathrm{Br}(K_\nu) = \mathbb{Q}/\mathbb{Z}$. (For the proof of this, see [C-F, section 10 of Tate's article])

In actuality, all we will need is the fact that this sequence forms a complex; that is, that if we take an element of $\mathrm{Br}(K)$, map it into $\mathrm{Br}(K_\nu)$ for each each ν, and take the sum, we always get 0.

Now suppose that $\langle , \rangle_K$ is a global pairing induced by cup product, and mapping into $\mathrm{Br}(K)$. Since cup product is compatible with restriction of cycles, for any s, c the sum over all places ν of $\langle s, c \rangle_\nu$, where $\langle , \rangle_\nu$ denotes restricting the cocycles to K_ν and then taking the local cup product, must be 0.

For our case, $\langle , \rangle_K$ will be the pairing of $H^1(G_K, E[p])$ with itself, which we will be able to consider as an element of $\mathrm{Br}(K)$ thanks to the Weil pairing.

We apply this to deduce:

Proposition 3. *(Gross 8.2) Assume that $d \in H^1(G_K, E(\overline{K}))[p]^\pm$ is locally trivial at all places $\nu \neq \lambda$ of K, but $d_\lambda \neq 0$ in $H^1(G_{K_\lambda}, E(\overline{K_\lambda}))[p]^\pm$. Then if a class $s \in H^1(G_K, E[p])^\pm$ lies in $\mathrm{Sel}_p(E/K)$, we have $s_\lambda = 0$ in $H^1(G_{K_\lambda}, E[p])^\pm$.*

Proof: The Kummer sequence gives us

$$E(K_\lambda)/pE(K_\lambda) \to H^1(G_{K_\lambda}, E[p]) \to H^1(G_{K_\lambda}, E(\overline{K_\lambda}))$$

but for s to be in Sel_p means the second map is 0, so $s_\lambda \in (E(K_\lambda)/pE(K_\lambda))^\pm$. Therefore, it will be enough to show that $\langle s_\lambda, d_\lambda \rangle = 0$. Now, choose a lift of d to some $c \in H^1(G_K, E[p])$ (which will be well-defined modulo $E(K)/pE(K)$), and observe that at every place ν, $\langle s_\nu, c_\nu \rangle = \langle s_\nu, d_\nu \rangle$, as we can choose a ($\mathbb{Z}/p\mathbb{Z}$ vector space) splitting of the local exact sequence

$$0 \to E(K_\lambda)/pE(K_\lambda) \to H^1(G_{K_\lambda}, E[p]) \to H^1(G_{K_\lambda}, E)[p] \to 0$$

to write $c_\nu = d_\nu + s'$ for some $s' \in E(K_\lambda)/pE(K_\lambda)$, and then the observation from Mihran's lectures that $E(K_\lambda)/pE(K_\lambda)$ is isotropic for the pairing $\langle , \rangle$ leads to the desired conclusion. Furthermore (and this a subtlety which may or may not have any actual content), $\langle s_\nu, c_\nu \rangle$ is in fact the Galois module theoretic local restriction map at ν of $\langle s, c \rangle_K$, because $H^1(G_{K_\lambda}, E(\overline{K_\lambda})[p]) = H^1(G_{K_\lambda}, E(\overline{K})[p])$ (the latter being the group in which the Galois module theoretic restriction actual lies). Putting these together, our result on the sum of local invariants implies $\sum_\nu \langle s_\nu, d_\nu \rangle = 0$, but $d_\nu = 0$ for all $\nu \neq \lambda$, so this gives $\langle s_\lambda, d_\lambda \rangle = 0$ as well. Since d_λ is non-trivial by hypothesis, applying Gross' Proposition 8.1 implies that s_λ is trivial, as desired.

Lastly, we remark that this is why it was so crucial to be able to calculate at every place whether or not the $d(n)$ were locally trivial; throwing out, say, the places of bad reduction, would have made it impossible to apply the sum of local invariants theorem, and would ultimately have yielded no information at all.

3. References

[C-F] J. Cassels, A. Frohlich, *Algebraic Number Theory.* Academic Press, 1967.

[Gr] B. Gross, Kolyvagin's Work on Modular Elliptic Curves. In *L-Functions and Arithmetic*, LMS Lecture Notes 153, London Mathematical Society, Cambridge, 1991, pp. 235-256.

[Pa] Mihran Papikian, *On Tate Local Duality.* Seminar lecture notes.