MTH699-MTH700

Heegner Points and Kolyvagin's Theorem

Professor: Dr. Somnath Jha

Notes By: Ajay Prajapati

Roll No: 17817063

Winter 2022

ANNEXURE-II

DECLARATION

I hereby declare that the work presented in the project report entitled "**Heegner Points and Kolyvagin's Theorem**" contains our own ideas in our own words. At places, where ideas and words are borrowed from other sources, proper references, as applicable have been cited. To the best of our knowledge this work does not emanate from or resemble other work created by person(s) other than mentioned herein.

Name: Ajay Prajapati

Date: 15-04-2022

This report is expository in nature and no new result is being claimed.

ABSTRACT

This report second part of a year long project on the topic "Heegner Points" under the guidance of Dr. Somnath Jha, IIT Kanpur. The first part can be found here. The Birch and Swinnerton-Dyer (BSD) conjecture is one of the central problems in the Theory of Elliptic Curves which predicts the rank of an elliptic curve defined over $\mathbb{Q}$. This was formulated in 1960's based on the numerical evidence found by Bryan Birch and Peter Swinnerton Dyer. Bryan Birch also found that elliptic curves over rationals are born with certain algebraic points(defined over imaginary quadratic fields) which he called Heegner points, named after the German mathematician Kurt Heegner. He believed that this Heegner point (well-defined upto torsion and sign) are key to the BSD conjecture for rank 1 case. Based on numerical evidence, he formulated a precise conjecture which was proved by the fruitful collaboration of Benedict Gross and Don Zagier in 1980's. They proved a spectacular formula (now known as Gross-Zagier formula) relating the first derivative of the L-function (something analytic) to the canonical height of the Heegner point (someting algebraic). This provided partial result in one direction of the BSD conjecture for rank 1. The rest of the work was done by Victor Kolyvagin in late 1980's thus completing that direction.

In this report, we will see the proof of Kolyvagin's theorem under some mild hypothesis to illustrate the main ideas. It is completely based on the wonderful paper of Gross, [Gro91], where he explain these ideas. The key to Kolyvagin's proof is that the Heegner point is not alone but lies at the bottom of a system of algebraic points defined over ring class fields. This system satisfies some nice properties which allows us to construct cohomology classes and apply techniques from Galois cohomology to give upper bound on the Selmer group.

Contents

§0. Pre-requisites and Notation

The reader is assumed to be fimiliar with:

- **Algebraic Number Theory:** Behaviour of primes (splitting, ramification, inert) in Galois extensions of number fields
- **Theory of Elliptic Curves:** Upto the level of [Sil86].
- **Theory of Complex Multiplication:** Upto the level of [Sil03], Chapter 2.
- **Modular Forms, Hecke operators, and Modular Curves:** Upto the level of [DS05], Chapters 1, 2, and 5.
- **Galois Cohomology:** only basic Galois cohomology (upto [Sil86], Appendix B)

Notation: All the notation in this note is standard and mostly follows [Sil86]'s notation.

$\mathrm{Gal}(L/K)$ denotes the Galois group of the Galois extension L/K.

$\mathrm{H}^n(K, M) := \mathrm{H}^n(\mathrm{Gal}(\overline{K}/K), M)$ where K is a field and M is a discrete $\mathrm{Gal}(\overline{K}/K)$-module. (All Galois modules we consider will be discrete)

$\mathrm{H}^n(L/K, M) := \mathrm{H}^n(\mathrm{Gal}(L/K), M)$ where M is a discrete $\mathrm{Gal}(L/K)$-module.

$A[n]$ denotes the n-torsion subgroup of an abelian group A.

$E(L)$ L-rational points of the elliptic curve E/K where $L \supset K$.

$\mathrm{Sel}^{(p)}(E/K)$ denotes the p-Selmer group of a elliptic curve E defined over a number field K.

$Ш(E/K)$ the Shafarevich-Tate group of the elliptic curve E/K.

$\mathbb{Q}(E[n])$ field extension obtained by adjoining the coordinates of all n-torsion points of E

$\mathcal{H}$ the Poincare upper-half plane $\{\tau \in \mathbb{C} : Im(\tau) > 0\}$

$\mathrm{Pic}^0(C)$ the Picard group of a non-singular algebraic curve C

K^{nr} the maximal unramified extension of a local field K

Few remarks:

1. **We will have frequent use for the following construction:** Let M/L and L/K be Galois extensions and assume that $\mathrm{Gal}(M/L)$ is abelian. There is a natural action of $\mathrm{Gal}(L/K)$ on $\mathrm{Gal}(M/L)$ defined as follows: given $\tau \in \mathrm{Gal}(L/K)$ and $\sigma \in \mathrm{Gal}(M/L)$, let $\tilde{\tau}$ be any lift of τ to $\mathrm{Gal}(M/K)$. Then the action of τ on σ is given by
$$\tau \cdot \sigma = \tilde{\tau}\sigma\tilde{\tau}^{-1}$$
(The fact that Gal(M/L) is abelian implies that this is independent of the choice of $\tilde{\tau}$.) The action of $\mathrm{Gal}(L/K)$ on $\mathrm{Gal}(M/L)$ is trivial precisely when M is an abelian extension of K.
2. We will often be working with eigenspaces for involutions, and we make the following sign convention: whenever $\pm$ appears in a formula, it is to be regarded as a fixed choice of sign, and every other $\pm$ in that formula should agree with this choice and a $\mp$ indicates the opposite of this initial choice.

§1. Introduction

Let L be an number field and E/L be an elliptic curve (EC) and $E(L) \subset E(\bar{L})$ is the group of L-rational points. A fundamental result in the study of ECs is the Mordell-Weil theorem.

Theorem 1.1. (Mordell-Weil theorem) The group $E(L)$ is finitely generated abelian group.

By the structure theorem of finitely generated abelian groups, we have the decomposition

$$E(L) \cong \mathbb{Z}^r \oplus E(L)_{tors}$$

Here r is called the (algebraic) *rank* of $E(L)$ and $E(L)_{tors}$ is the *torsion subgroup* of $E(L)$. The $E(L)_{tors}$ part is well understood by a theorem of Mazur. On the other hand, the rank is very mysterious and there are many unsolved conjectures about it even when $L = \mathbb{Q}$. Most prominent of those is the Birch and Swinnerton-Dyer (BSD) conjecture:

[Birch and Swinnerton-Dyer (BSD) Conjecture] Let $E/\mathbb{Q}$ be an elliptic curve and $L(E/\mathbb{Q}, s)$ be its L-function. Then (see (here) for precise formulation)

- $\text{rank}(E(\mathbb{Q})) = \text{ord}_{s=1} L(E, s)$. ($\text{ord}_{s=1} L(E, s)$ is called the *analytic rank of* E)
- **(BSD formula)** The leading term of the series expansion of $L(E/\mathbb{Q}, s)$ around $s = 1$ can be given in terms of certain arithmetic invariants of E.

This conjecture is one of the biggest unsolved mysteries in mathematics. This has been solved partially for rank 0 and rank 1 cases but nothing beyond. In this memoir, we see Kolyvagin's theorem, one of the great results towards proving one direction of BSD in rank 1 case by using so called Heegner points. Recall that in our previous semester work (here), we defined *Heegner points* on elliptic curves and saw some of their basic properties. In this memoir, we will study them more systematically and see how they can be used to understand the group structure of elliptic curves.

Let E be an elliptic curve over $\mathbb{Q}$ of conductor N and let K be an imaginary quadratic field in which all primes dividing N are split. The theory of complex multiplication and a modular parameterization $X_0(N) \longrightarrow E$ can be used to define a Heegner point $y_K \in E(K)$. The precise point y_K depends on some choices, but it is well-defined up to sign and torsion (so its canonical height $\hat{h}(y_K)$ is well-defined). If $L(E/K, s)$ is the L-function of E over K, one has $L(E/K, 1) = 0$ for trivial reasons, and Gross and Zagier proved the spectacular formula

$$L'(E/K, 1) = \left(\frac{1}{\sqrt{D}} \int_{E(\mathbb{C})} \omega \wedge i\omega \right) \cdot \hat{h}(y_K).$$

Here D is the discriminant of $K/\mathbb{Q}$ and ω is the differential on E coming from the fixed modular parameterization.

In particular, $L'(E/K, 1) \neq 0$ if and only if y_K has infinite order. i.e., analytic rank $= 1 \implies$ algebraic rank ≥ 1. We would like to know whether there is an equality. In the late 1980's, Victor Kolyvagin shows the equality and proves the following theorem ([KL89]).

Theorem 1.2. Let E be an EC over $\mathbb{Q}$. Assume the point y_K has infinite order in $E(K)$. Then:

1. the group $E(K)$ has rank 1.
2. the Shafarevich-Tate group, $Ш(E/K)$, is finite.

Morover, combining results of both Gross-Zagier and Kolyvagin, we can obtain: (For the proof, see [Dar04], theorem 3.22)

Theorem 1.3. (Gross-Zagier-Kolyvagin) Suppose $\mathrm{ord}_{s=1} L(E/\mathbb{Q}, s) = r$ with $r \in \{0, 1\}$. i.e., analytic rank is ≤ 1. Then

$$\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}) = r \quad \text{and} \quad Ш(E/\mathbb{Q}) \text{ is finite,}$$

with an upper bound consistent with the BSD formula.

Now we concentrate on theorem 1.2. In his paper [Gro91], Gross explains the main steps of Kolyvagin's method by proving the following slightly weaker version of theorem 1.2:

Theorem 1.4. Let p be an odd prime such that the extension $\mathbb{Q}(E[p])/\mathbb{Q}$ has Galois group $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ and assume that p does not divide y_K in $E(K)/E(K)_{tors}$. Then:

1. The group $E(K)$ has rank 1.
2. The p-torsion subgroup of the Shafarevich-Tate group, $Ш(E/K)[p^\infty]$, is trivial.

In view of the above theorem, we make the following definition:

Definition 1.5. We say that a prime p is *good prime* if p is odd, $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, and $y_K \notin pE(K)$.

Remark 1.6. (a) If E does not have CM then by Serre's open image theorem ([Sil86], Chapter III, Theorem 7.9), condition 2 holds for infinitely many primes.

(b) By Mordell-Weil theorem, condition 3 holds for infinitely many primes as well.

Recall that there exists an exact sequence of $\mathbb{F}_p$ vector spaces:

$$0 \longrightarrow E(K)/pE(K) \xrightarrow{\delta} \mathrm{Sel}^{(p)}(E/K) \longrightarrow Ш(E/K)[p] \longrightarrow 0 \tag{1.1}$$

Suppose p is a good prime. Then we can prove that there are no non-trivial p-torsion points over K. So we have

$$\mathrm{rank}(E(K)) = \dim_{\mathbb{F}_p} E(K)/pE(K). \tag{1.2}$$

and we are left to prove:

Proposition 1.7. Suppose p is a good prime. Then $\text{Sel}^{(p)}(E/K)$ is cyclic generated by $\delta(y_K)$.

Let us see how this proposition implies the result of theorem 1.4.

Proof. (1.7 implies 1.4) Since p is good prime, $0 \neq y_K \in E(K)/pE(K)$, so $\dim_{\mathbb{F}_p}(E(K)/pE(K)) \neq 0$. But $E(K)/pE(K)$ injects into $\text{Sel}^{(p)}(E/K)$, which has dimension 1 by proposition 1.7. Hence by equation 1.2, $\text{rank}(E(K)) = 1$.

Morover, $\delta : E(K)/pE(K) \xrightarrow{\sim} \text{Sel}^{(p)}(E/K)$ is an isomorphism of $\mathbb{F}_p$-vector spaces. Hence the cokernel, $Ш(E/K)[p]$, is trivial. □

The remaining part of this memoir is focused on proving proposition 1.7. In section 2, we define the system of Heegner points on the modular curve $X_0(N)$ (where N is the conductor of our elliptic curve E) and see some of their properties. In particular, how Galois group, Atkin-Lehner involution, and Hecke operators acts on these points. In section 3, we push this Heegner points on modular curves to E via a modular parametrization. In section 4, we show that these system of points satisfies the properties of an Euler system. In section 5, we construct a sequence of cohomology classes (defined over K) using these points and Kolyvagin's derivative operators. In section 6, we study the property of these cohomology classes which we continue in section 7, where we derive conditions for their local triviality. In section 8, we recall some results from local Tate duality. In particular, we use Weil pairing, cup product, and invariant map from local class field theory to construct a non-degenerate pairing. Using this pairing and Cartier duality, we construct another pairing whose properties we study in section 9. In particular, we derive when the elements of a Selmer group are locally trivial in terms of triviality of the cohomology classes constructed in section 5 (proposition 9.4). In section 10, we start with some Galois cohomology computations and prove an isomorphism which helps construct yet another pairing on Selmer group. Then we study the properties of this pairing and using it, see relation between different types of objects (proposition 10.8). Finally we finish the proof of proposition 1.7 in proposition 10.9.

§2. Heegner Points on modular curves

Recall that in our last semester work (here), we defined Heegner points as follows:

Let $\omega \in \mathcal{H}$ be a quadratic imaginary number satisfying $A\omega^2 + B\omega + C = 0$ where $(A, B, C) = 1$. Denote the discriminant of ω as $\Delta(\omega) := B^2 - 4AC$ and let K be the imaginary quadratic field $\mathbb{Q}(\omega)$. For a positive integer N, if

$$A \equiv 0 (\text{mod}\, N) \quad \text{and} \quad (\Delta(\omega), 4N) = 1$$

then $[\omega] \in X_0(N) = \Gamma_0(N)\backslash\mathcal{H}^*$ is called a *Heegner Point* (of *discriminant* $\Delta(\omega)$) on $X_0(N)$.

Then we saw that ω is a Heegner point of $X_0(N) \iff \Delta(\omega) = \Delta(N\omega)$. Hence if we let

$$E = \frac{\mathbb{C}}{\langle 1, \tau\rangle}, \quad E' = \frac{\mathbb{C}}{\langle 1, N\tau\rangle}, \quad \text{and the } N\text{-isogeny } E \longrightarrow E',$$

then a Heegner point $\omega \in X_0(N)$ corresponds to a pair of N-isogenous elliptic curves, each having CM by the same order of K because $\Delta(\omega) = \Delta(N\omega)$. Infact, this property characterizes Heegner points and we shall use this definition in the subsequent sections.

Let us first set the notation.

N A fixed positive integer

E An elliptic curve over $\mathbb{Q}$ of conductor N

K An imaginary quadratic field with discriminant $D \neq -3, -4$ (so $K = \mathbb{Q}(\sqrt{D})$)

$\mathcal{O}_K$ the ring of integers of K

n a squarefree integer relatively prime to N

$\mathcal{O}_n := \mathbb{Z} + n\mathcal{O}_K$, the order of conductor n in $\mathcal{O}_K$

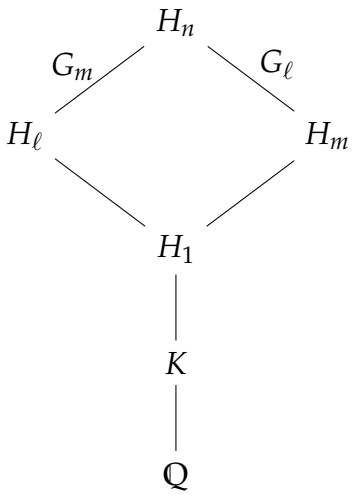
H_n the ring class field of K of conductor n

$\mathrm{Pic}(\mathcal{O}_n)$ the Picard group (or the Class group) of $\mathcal{O}_n$ (defined in [Cox03], section 7).

$H = H_1$, the Hilbert Class Field of K, the maximal unramified abelian extension

τ denotes the complex conjugation

Now we see some Galois group computations which will be useful later. Let n be a squarefree integer and $n = \ell \cdot m$, where $\ell \nmid m$. We have the following diagram:



(2.1)

Let us call $G_n := \mathrm{Gal}(H_n/H_1)$, the Galois group of the extension H_n/H_1. Since $\mathcal{O}_K^\times = \mathbb{Z}^\times = \{\pm 1\}$, by degree counting arguments (using the formula in Theorem 7.24, [Cox03]) we find that H_ℓ and H_m are linearly disjoint over H_1. Hence we have,

$$G_n \cong G_\ell \times G_m \cong \prod_{\ell | m} G_\ell.$$

Also by Galois theory, we find that $G_\ell = \mathrm{Gal}(H_\ell/H_1) \cong \mathrm{Gal}(H_n/H_m)$. We have following proposition which will be very useful later:

Lemma 2.1. If ℓ is inert in K then G_ℓ is a cyclic group of order $\ell + 1$.

Proof. First let us look at the diagram:

$$\begin{array}{c} H_n \\ \Big| \ (\mathcal{O}_K/n\mathcal{O}_K)^\times/(\mathbb{Z}/n\mathbb{Z})^\times \\ H_1 \\ \Big| \ \mathrm{Pic}(\mathcal{O}_K) \\ K \\ \Big| \ \langle 1, \tau \rangle \\ \mathbb{Q} \end{array}$$

We note that $\mathrm{Gal}(H_1/K) \cong \mathrm{Pic}(\mathcal{O}_K)$ by Artin reciprocity map from class field theory. Also,

$$\mathrm{Gal}(H_n/H_1) \cong \frac{\mathrm{Gal}(H_n/K)}{\mathrm{Gal}(H_1/K)} \cong \frac{\mathrm{Pic}(\mathcal{O}_n)}{\mathrm{Pic}(\mathcal{O}_K)} \xrightarrow{\sim} \frac{(\mathcal{O}_K/n\mathcal{O}_K)^\times}{(\mathbb{Z}/n\mathbb{Z})^\times}$$

where the last isomorphism is deduced by the fact that $\mathrm{Pic}(\mathcal{O}_n)/\mathrm{Pic}(\mathcal{O}_K)$ is isomorphic to $I_K(n) \cap P_K/P_{K,\mathbb{Z}}(n)$ and this group sits in the exact sequence:

$$0 \to (\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow (\mathcal{O}_K/n\mathcal{O}_K)^\times \longrightarrow \frac{I_K(n) \cap P_K}{P_{K,\mathbb{Z}}(n)} \to 0$$

Now we specialize ourselves to the case $n = \ell$ inert. Let $\lambda = \ell\mathcal{O}_K$ and $\mathbb{F}_\lambda = \mathcal{O}_K/\lambda$ then

$$G_\ell \cong \mathbb{F}_\lambda^\times/\mathbb{F}_\ell^\times$$

which is clearly of order $(\ell + 1)$ as λ is inert in K. □

Remark 2.2. The Galois group $\mathrm{Gal}(H_n/\mathbb{Q})$ is a generalised dihedral group:

$$\mathrm{Gal}(H_n/\mathbb{Q}) \simeq \mathrm{Gal}(H_n/K) \rtimes \mathrm{Gal}(K/\mathbb{Q})$$

where complex conjugation τ, which generates $\mathrm{Gal}(K/\mathbb{Q})$, acts on $\mathrm{Gal}(H_n/K)$ by sending an automorphism σ to its inverse, i.e. $\tau^{-1}\sigma\tau = \sigma^{-1}$.

Now we return to Heegner points. Since we have fixed a positive integer N and a quadratic imaginary field K, it is not clear whether there exists Heegner points $\omega \in X_0(N)$ with $E = \mathbb{C}/\langle 1, \omega \rangle$ having CM with an order of K. Infact, such Heegner point will always exist if

$$\text{every prime } p \text{ dividing } N \text{ splits in } K \tag{2.2}$$

This condition is called "*Heegner Hypothesis*" in literature and we will assume that our field K satisfies this. This gurantees the existence of an ideal $\mathcal{N} \subset \mathcal{O}_K$ such that $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$ ([Gro84], section 1). We also have $\mathcal{N}^{-1}/\mathcal{O}_K \cong \mathcal{N}\mathcal{N}^{-1}/\mathcal{N}\mathcal{O}_K = \mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$.

Let $\mathcal{N}_n = \mathcal{O}_n \cap \mathcal{N}$. Then $\mathcal{N}_n$ is an invertible ideal of $\mathcal{O}_n$ (since $(n, N) = 1$ so $\mathcal{O}_n \cap \mathcal{N}$ is a proper $\mathcal{O}_n$-ideal), with $\mathcal{N}_n^{-1}/\mathcal{O}_n \cong \mathbb{Z}/N\mathbb{Z}$. Hence

$$z_n := \left[\frac{\mathbb{C}}{\mathcal{O}_n} \longrightarrow \frac{\mathbb{C}}{\mathcal{N}_n^{-1}}\right] \tag{2.3}$$

is a point on the modular curve $X_0(N)$. The point z_n can also be denoted as

$$z_n = \left[\frac{\mathbb{C}}{\mathcal{O}_n}, \frac{\mathcal{N}_n^{-1}}{\mathcal{O}_n}\right],$$

isomorphism class of the pair, an elliptic curve together with a N-cyclic subgroup.

Definition 2.3. The point $z_n \in X_0(N)$ is called a *Heegner point of conductor n*.

Proposition 2.4. The point z_n as defined above (2.3) lies in $X_0(N)(H_n)$.

Proof. Recall that there is a canonical model for $X_0(N)$ over $\mathbb{Q}$ given by the *modular polynomial* defined as follows: F_N is the minimal polynomial of j_N over $\mathbb{C}(j)$ where $j(z)$ is the modular j-invariant and $j_N(z) := j(Nz)$. So $F_N(Y) \in \mathbb{C}(j)[Y]$. If we replace every occurence of j by X then we get $F_N(X, Y) \in \mathbb{C}[X, Y]$. We can prove that $F_N(X, Y) \in \mathbb{Z}[X, Y]$. By the way F_N is defined and using the correspondence between varieties and function fields from algebraic geometry, we obtain that

$$Z_0(N) : F_N(u, v) = 0 \tag{2.4}$$

is an irreducible plane model for $X_0(N)$.

Now the point $z_n \in \Gamma_0(N)\backslash\mathcal{H}^*$ can be taken in $z_n \in \mathcal{H}$. Because $\mathbb{C}/\mathcal{O}_n$ and $\mathbb{C}/\mathcal{N}_n^{-1}$ has CM by same order, $\mathcal{O}_n$, the discriminants of z_n and $N \cdot z_n$ are same and from theory of Complex Multiplication, $j(z_n)$ and $j(Nz_n)$ are both in H_n. □

So we have a set of Heegner points of conductor n

$$\mathcal{S}_n := \left\{\left[\frac{\mathbb{C}}{\mathcal{O}_n} \longrightarrow \frac{\mathbb{C}}{(\mathcal{N} \cap \mathcal{O}_n)^{-1}}\right] : \mathcal{N} \subset \mathcal{O}_K \text{ ideal such that } \frac{\mathcal{O}_K}{\mathcal{N}} \cong \frac{\mathbb{Z}}{N\mathbb{Z}}\right\}$$

$\mathcal{S}_n$ is stable under the action of $\mathrm{Gal}(H_n/\mathbb{Q})$:

Recall from 2.2 that $\mathrm{Gal}(H_n/\mathbb{Q}) \simeq \mathrm{Gal}(H_n/K) \rtimes \mathrm{Gal}(K/\mathbb{Q})$ where τ acts on $\sigma \in \mathrm{Gal}(H_n/K)$ by sending it to σ^{-1}. Hence we only need to know the action of τ and σ to know the action of whole group $\mathrm{Gal}(H_n/\mathbb{Q})$.

Proposition 2.5. The action of complex conjugation $\tau \in \mathrm{Gal}(H_n/\mathbb{Q})$ on $\mathcal{S}$ is the following:

$$\tau(z_n) = \tau\left(\frac{\mathbb{C}}{\mathcal{O}_n}, \frac{\mathcal{N}_n^{-1}}{\mathcal{O}_n}\right) = \left(\frac{\mathbb{C}}{\mathcal{O}_n}, \frac{\overline{\mathcal{N}_n^{-1}}}{\mathcal{O}_n}\right) = \left(\frac{\mathbb{C}}{\mathcal{O}_n}, \frac{N^{-1}\mathcal{N}_n}{\mathcal{O}_n}\right)$$

Morover, directly from the theory of complex multiplication, we have

Proposition 2.6. Let $\sigma \in \mathrm{Gal}(H_n/K)$. Then we have

$$\sigma(z_n) = \sigma\left(\frac{\mathbb{C}}{\mathcal{O}_n}, \frac{\mathcal{N}_n^{-1}}{\mathcal{O}_n}\right) = \left(\frac{\mathbb{C}}{\mathfrak{a}_\sigma^{-1}}, \frac{\mathcal{N}_n^{-1}\mathfrak{a}_\sigma^{-1}}{\mathfrak{a}_\sigma^{-1}}\right)$$

where $\mathfrak{a}_\sigma \in \mathrm{Pic}\,\mathcal{O}_n$ is the ideal that corresponds to σ under the isomorphism $\mathrm{Pic}\,\mathcal{O}_n \cong \mathrm{Gal}(H_n/K)$ induced by the Artin reciprocity map.

Proof. Recall that $\sigma \in \mathrm{Gal}(H_n/K)$ acts on $j(-)$ by $j(- \cdot \mathfrak{a}_\sigma^{-1})$. Hence we get that

$$\sigma(j(\mathcal{O}_n)) = j(\mathcal{O}_n \cdot \mathfrak{a}_\sigma^{-1}) \quad \text{and} \quad \sigma(j(\mathcal{N}_n^{-1})) = j(\mathcal{N}_n^{-1} \cdot \mathfrak{a}_\sigma^{-1})$$

Now the proposition is clear. □

Action of Atkin-Lehner involution:

Proposition 2.7. The Atkin-Lehner involution w_N acts on Heegner points as

$$w_N(z_n) = w_N\left(\frac{\mathbb{C}}{\mathcal{O}_n}, \frac{\mathcal{N}_n^{-1}}{\mathcal{O}_n}\right) = \left(\frac{\mathbb{C}}{\mathcal{N}_n^{-1}}, \frac{N^{-1}\mathcal{O}_n}{\mathcal{N}_n^{-1}}\right)$$

Action of Hecke operators:

We now define a norm map on the Jacobian of modular curve, $J(X_0(N))$, (by Abel-Jacobi theorem, we can identify the classical Jacobian variety $J(X_0(N))$ of $X_0(N)$ with $\mathrm{Pic}^0(X_0(N))$) and derive a very useful relation between it and the Hecke operators (2.8).

$$\mathrm{Norm}_{H_n/H_m} : J(X_0(N))(H_n) \longrightarrow J(X_0(N))(H_m), \quad x \longmapsto \sum_{\sigma \in G_\ell} \sigma(x).$$

Lemma 2.8. Let n be a squarefree integer and $n = \ell \cdot m$ where ℓ is a prime. Then

$$T_\ell(z_m) = \mathrm{Norm}_{H_n/H_m}(z_n)$$

where T_ℓ is the Hecke operator on $J(X_0(N))$.

Proof. Let $\mathcal{O}_n = \mathbb{Z} + n\mathcal{O}_K$ be the order of conductor n. Let $E = \mathbb{C}/\mathcal{O}_m$ and $C_N = \mathcal{N}_m^{-1}/\mathcal{O}_m$. By the definition of the Hecke operator, we have

$$T_\ell(z_m) = \sum_{C_\ell \subset E[\ell]} (E/C_\ell, (C_N + C_\ell)/C_\ell)$$

where the sum is over the $\ell + 1$ cyclic subgroups of $E[\ell]$ of order ℓ.

On the other hand, since ℓ and m are coprime, we have

$$z_n = \left(\frac{\mathbb{C}}{\mathcal{O}_n}, \frac{\mathcal{N}_n^{-1}}{\mathcal{O}_n}\right) = \left(\frac{\mathbb{C}/\mathcal{O}_m}{C_\ell}, \frac{\mathcal{N}_n^{-1}/\mathcal{O}_m}{C_\ell}\right)$$

for some cyclic subgroup C_ℓ of $\mathbb{C}/\mathcal{O}_m$ of order ℓ since $= \mathcal{O}_m/\mathcal{O}_n$ is of order ℓ. Now,

$$\begin{aligned}
\text{Norm}_{H_n/H_m}(z_n) &= \sum_{\sigma \in \text{Gal}(H_n/H_m)} \sigma\left(\frac{\mathbb{C}}{\mathcal{O}_n}, \frac{\mathcal{N}_n^{-1}}{\mathcal{O}_n}\right) \\
&= \sum_{\sigma \in \text{Gal}(H_n/H_m)} \sigma\left(\frac{\mathbb{C}/\mathcal{O}_m}{C_\ell}, \frac{\mathcal{N}_n^{-1}/\mathcal{O}_m}{C_\ell}\right) \\
&= \sum_{\sigma \in \text{Gal}(H_n/H_m)} \left(\frac{\mathbb{C}/\mathcal{O}_m}{\sigma(C_\ell)}, \frac{\mathcal{N}_n^{-1}/\mathcal{O}_m}{\sigma(C_\ell)}\right)
\end{aligned}$$

where $\sigma(C_\ell)$ is another cyclic subgroup of $\mathbb{C}/\mathcal{O}_m$ of order ℓ and as σ varies over all elements of $\text{Gal}(H_n/H_m) \cong G_\ell$, $\sigma(C_\ell)$ varies over all $(\ell+1)$ cyclic subgroups of order ℓ. □

§3. Heegner Points on Elliptic Curves

Since our elliptic curve E has conductor N, by modularity theorem we have a morphism (defined over $\mathbb{Q}$) of varieties

$$\Phi : X_0(N) \longrightarrow E \tag{3.1}$$

which is called a *modular parametrization of* E. We are going to use this map to transport the system of Heegner points on $X_0(N)$ constructed in previous section to define a system of Heegner points on E.

Definition 3.1. $y_n := \Phi(z_n) \in E$ is called a *Heegner point of conductor* n on E.

Since Φ is defined over $\mathbb{Q}$, by proposition 2.4 y_n actually belongs in $E(H_n)$.

Note that the modular parametrization Φ_E induces a map between the Picard groups of the modular curve and the elliptic curve ([Sil86], section 2.3). By [Sil86], proposition 3.4, $\text{Pic}^0(E) \cong E$ as groups and by Abel-Jacobi theorem ([DS05], theorem 6.1.2), $\text{Pic}^0(X_0(N)) \cong J(X_0(N))$. Hence we obtain a map (also denoted by Φ)

$$\Phi : J(X_0(N)) \longrightarrow E. \tag{3.2}$$

Moreover if $X_0(N)$ has genus greater than 0 then $X_0(N)$ embeds in $J(X_0(N))$ via the map $x \longmapsto [(x) - (\infty)]$ and Φ in equation 3.1 is just restriction of Φ in equation 3.2.

We also have a norm map on the elliptic curve E as follows:

$$\text{Norm}_{H_n/H_m} : E(H_n) \longrightarrow E(H_m), \quad P \longmapsto \sum_{\sigma \in G_\ell} \sigma(P).$$

Morover, this norm map is compatible with the norm map previously on $J(X_0(N))$ in the sense that the following diagram commutes:

$$\begin{array}{ccc} J(X_0(N))(H_n) & \xrightarrow{\Phi} & E(H_n) \\ \Big\downarrow{\scriptstyle \mathrm{Norm}_{Hn/Hm}} & & \Big\downarrow{\scriptstyle \mathrm{Norm}_{Hn/Hm}} \\ J(X_0(N))(H_m) & \xrightarrow{\Phi} & E(H_m) \end{array}$$

We now define the Heegner point (unique upto torsion and sign) which appears in the statement of Gross-Zagier formula and Kolyvagin's theorem:

$$y_K := \mathrm{Norm}_{H_1/K}(y_1) = \sum_{\sigma \in \mathrm{Gal}(H_1/K)} \sigma(y_1) \quad \in E(K) \tag{3.3}$$

§4. Euler System

In this section, we see that the set of Heegner points on elliptic curves defined above satisfies the properties of a so called Euler system.

Proposition 4.1. (Norm Relations) Suppose $n = \ell \cdot m$ with $\ell \nmid m$ inert in K. Then

$$\mathrm{Norm}_{H_n/H_m}(y_n) = a_\ell \cdot y_m$$

where $a_\ell = \ell + 1 - \#\tilde{E}(\mathbb{F}_\ell)$ is the trace of Frobenius.

Proof. This directly follows from lemma 2.8 by a simple computation:

$$\begin{aligned} \mathrm{Norm}_{H_n/H_m}(y_n) &= \mathrm{Norm}_{H_n/H_m}(\Phi(z_n)) \\ &= \Phi(\mathrm{Norm}_{H_n/H_m}(z_n)) \\ &= \Phi(T_\ell(z_m)) \\ &= T_\ell(\Phi(z_m)) \\ &= a_\ell \cdot y_m \end{aligned}$$

because by Eichler-Shimura, T_ℓ acts on an elliptic curve by multiplication-by-a_ℓ map. □

Proposition 4.2. (Congruence Relations) Suppose $n = \ell \cdot m$ with $\ell \nmid m$ inert in K and write $\ell\mathcal{O}_K = \lambda$. Then

(a) λ splits completely in H_m.

(b) Every prime λ_m lying over λ is totally ramified in H_n.

(c) If λ_n is the unique prime of H_n lying above λ_m, then

$$y_n \equiv \left(\frac{H_m/\mathbb{Q}}{\lambda_m}\right)(y_m) \pmod{\lambda_n}$$

Remark: $H_m/\mathbb{Q}$ is a non-abelian (generalized dihedral) extension so we get such an expression for every prime λ_m lying above λ.

Equivalently,

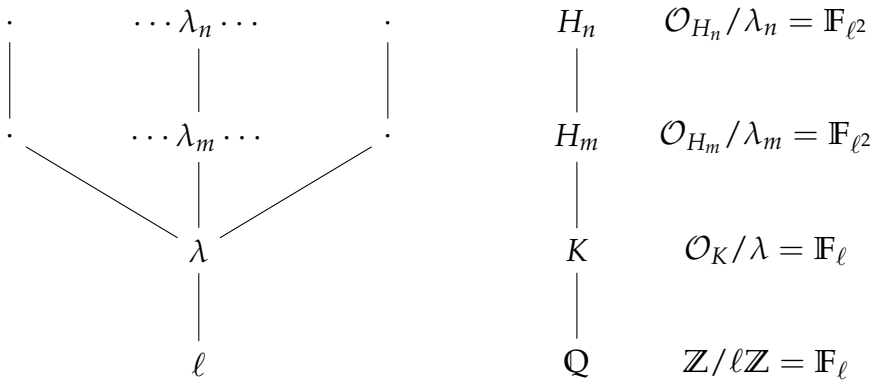
$$\mathrm{red}_{\lambda_n}(y_n) = \mathrm{Frob}_\ell(\mathrm{red}_{\lambda_m}(y_m)) \in \tilde{E}(\mathbb{F}_{\ell^2})$$

where

$$\mathrm{red}_{\lambda_n} : E(H_n) \longrightarrow \tilde{E}(\mathcal{O}_n/\lambda_n) = \tilde{E}(\mathbb{F}_{\ell^2})$$

is $\pmod{\lambda_n}$ reduction map, red_{λ_m} is $\pmod{\lambda_m}$ reduction map of E, and Frob_ℓ is the power ℓ Frobenius map on $\mathbb{F}_{\ell^2}$.

Proof. We have the following diagram:



(a) The prime $\lambda = \ell\mathcal{O}_K$ is principal in K and has norm ℓ^2 which is prime to m, the conductor of H_m. Hence λ is in kernel of the Artin map $I_K(m\mathcal{O}_K) \longrightarrow \mathrm{Gal}(H_m/K)$ i.e., $\left(\frac{H_m/K}{\lambda}\right) = 1$. Hence λ splits completely in H_m.

(b) Recall from diagram **??** that H_ℓ and H_m are linearly disjoint over H_1 and $H_n = H_\ell H_m$. In H_ℓ/H_1, all primes lying above λ are totally ramified Since $\mathcal{O}_K = \pm 1$ because they divide the conductor ℓ. Since ramification multiplies in tower this result follows.

(c) It is clear that the two statements are equivalent (by definition, the reduction of $\left(\frac{H_m/\mathbb{Q}}{\lambda_m}\right)$ is Frob_ℓ). Now we compute $a_\ell \cdot \mathrm{red}_{\lambda_m}(y_m)$ in two ways. Firstly, by Norm relations (4.1),

$$a_\ell \cdot y_m = \sum_{\sigma \in \mathrm{Gal}(H_n/H_m)} \sigma(y_n)$$

Reducing this $\pmod{\lambda_n}$, we get

$$\begin{aligned} a_\ell \,\mathrm{red}_{\lambda_m}(y_m) &= \sum_\sigma \tilde{\sigma}(\mathrm{red}_{\lambda_n}(y_n)) \\ &= \sum_\sigma \mathrm{red}_{\lambda_n}(y_n) \\ &= (\ell+1)\,\mathrm{red}_{\lambda_n}(y_n) \end{aligned}$$

Also, by the Eichler-Shimura congruence relation, we get

$$T_\ell(z_m) = \mathrm{Frob}_\ell(z_m) + \mathrm{Frob}_\ell^{tr}(z_m) \quad \text{as divisors on} X_0(N)_{/\mathbb{F}_{\ell^2}}$$

Now, apply $\pmod{\lambda_m}$ reduced modular parametrization $\tilde{\Phi}$ both sides,

$$\begin{aligned} a_\ell \cdot \mathrm{red}_{\lambda_m}(y_m) &= \mathrm{Frob}_\ell(\mathrm{red}_{\lambda_m}(y_m)) + \sum_{x \in \mathrm{Frob}^{-1}(y_m)} \mathrm{red}_{\lambda_m}(x) \\ &= (\ell+1)\,\mathrm{Frob}_\ell(\mathrm{red}_{\lambda_m}(y_m)) \end{aligned}$$

Thus we get the required result. (The last equality because $\alpha^\ell = \alpha^{1/\ell}$ for all $\alpha \in \mathbb{F}_{\ell^2}$) □

§5. Construction of Cohomology Classes

Definition 5.1. A prime $\ell \nmid N \cdot D \cdot p$ is called a *Kolyvagin prime* if it satisfies

(a) ℓ is inert in K

(b) $a_\ell \equiv (\ell+1) \equiv 0 \pmod{p}$ where $a_\ell == \ell + 1 - \#\tilde{E}(\mathbb{F}_\ell)$.

It is not obvious whether even a single Kolyvagin prime exists. But we will see that infact, there are infinitely many Kolyvagin primes. For this we study the extension $K(E[p])/K$.

Proposition 5.2. The extension $K(E[p])/K$ is unramified outside the primes which divide $p \cdot N$. (recall that N was the conductor of E)

Proof. Let λ be a prime of K which does not divide $p \cdot N$. Then E has good reduction over $\mathcal{O}_\lambda$. Let γ be a prime of $\mathcal{O}_{K(E[p])}$ lying above λ. Then we want to prove that the map

$$\mathrm{Gal}(K(E[p])_\gamma / K_\lambda) \longrightarrow \mathrm{Gal}(\mathbb{F}_\gamma / \mathbb{F}_\lambda), \quad \sigma \longmapsto \widetilde{\sigma} \tag{5.1}$$

is injective. Since E has good reduction $\pmod{\lambda}$, we have the injection

$$E(K(E[p])_\gamma)[p] = E[p] \hookrightarrow \widetilde{E}(\mathbb{F}_\gamma)$$

Let $\sigma \in \mathrm{Gal}(K(E[p])_\gamma / K_\lambda)$ be such that $\widetilde{\sigma}$ is trivial on $\mathbb{F}_\gamma$. Then because of above inclusion, σ fixes $E[p]$ hence it is trivial on $K(E[p])_\gamma$. So the map 5.1 is injective. □

Now we let τ be the complex conjugation and we define the set

$$\mathcal{L}_E = \left\{ \ell \text{ prime } : \ell \nmid N \cdot D \cdot p, \left(\frac{K(E[p])/\mathbb{Q}}{\ell}\right) \sim \tau \text{ in } \mathrm{Gal}(K(E[p])/\mathbb{Q}) \right\}$$

where $\sim$ means that τ lies in the Frobenius conjugacy class

$$\left(\frac{K(E[p])/\mathbb{Q}}{\ell}\right) := \left\{ \left(\frac{K(E[p])/\mathbb{Q}}{\gamma}\right) : \gamma \text{ is a prime lying over } \ell \right\}$$

First note that by 5.2, if $\ell \nmid N \cdot D \cdot p$ then ℓ is unramified in $K(E[p])/\mathbb{Q}$. Hence it makes sense to talk about Frobenius element of γ lying above ℓ. Also by Chebotarev Density theorem, the above set has positive density and hence it is infinite.

Proposition 5.3. Every $\ell \in \mathcal{L}_E$ is a Kolyvagin prime.

Proof. This follows directly from the computation of characteristic polynomial of the action of Frobenius and τ as linear transformations on $\mathbb{F}_p$ vector space $E[p]$. Characteristic polynomial of τ is $x^2 - 1 \pmod p$ and of $\left(\frac{K(E[p])/\mathbb{Q}}{\gamma}\right)$ is $x^2 - a_\ell x + \ell \pmod p$. Since they are conjugate, their characterstic polynomials must be the same. Hence

$$x^2 - a_\ell x + \ell \equiv x^2 - 1 \pmod p.$$

Finally, ℓ is inert in K since τ has order 2 in $\mathrm{Gal}(K/\mathbb{Q})$ so inertia of ℓ is non-trivial. □

Let $\ell \in \mathcal{L}_E$ be a Kolyvagin prime, $\lambda := \ell\mathcal{O}_K$, and $\mathbb{F}_\lambda$ be the residue field at λ. Since τ has order 2 and ℓ is inert in K, λ splits completely in $K(E[p])/K$ which means that $\mathbb{F}_{\lambda_i} \cong \mathbb{F}_\lambda$ for λ_i a prime in $K(E[p])$ lying above λ. Hence

$$\widetilde{E}(\mathbb{F}_\lambda)[p] = \widetilde{E}(\mathbb{F}_{\lambda_i})[p] \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$

We now consider the action of τ on this space to deduce:

Proposition 5.4. The $\mathbb{F}_p$-vector space $\widetilde{E}(\mathbb{F}_\lambda)[p]$ is decomposed as eigenspaces

$$\widetilde{E}(\mathbb{F}_\lambda)[p] = \widetilde{E}(\mathbb{F}_\lambda)[p]^+ \oplus \widetilde{E}(\mathbb{F}_\lambda)[p]^-$$

of the action of τ and both of these eigenspaces are isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

Proof. The decomposition exists because characteristic polynomial of τ can be factored into linear terms. To prove that they are isomorphic to $\mathbb{Z}/p\mathbb{Z}$, it is sufficient to prove that they both are non-trivial. If we call Frob_ℓ the Frobenius map $x \longmapsto x^\ell$ then $\mathrm{Frob}_\ell = \tau$ on $\mathbb{F}_\lambda$. Now we compute

$$\begin{aligned} |\widetilde{E}(\mathbb{F}_\lambda)[p]^+| &= |\{P \in \widetilde{E}(\mathbb{F}_\lambda)[p] : \mathrm{Frob}_\ell P = P\}| \\ &= |\widetilde{E}(\mathbb{F}_\ell)[p]| \equiv 0 \pmod p \end{aligned}$$

since $\widetilde{E}(\mathbb{F}_\ell)$ has order $\ell + 1 - a_\ell$ which is divisible by p. Similarly,

$$\begin{aligned} |\widetilde{E}(\mathbb{F}_\lambda)^-| &= |\{P \in \widetilde{E}(\mathbb{F}_\lambda) : \mathrm{Frob}_\ell P = -P\}| \\ &= |\ker(\mathrm{Frob}_\ell + 1)| \\ &= \deg(\mathrm{Frob}_\ell + 1) \quad \text{(since } (\mathrm{Frob}_\ell + 1) \text{ is a seperable map, [Sil86], Corollary III.5.5)} \\ &= \det(\mathrm{Frob}_\ell + 1) \quad \text{(using the properties of Weil pairing and dual isogeny)} \\ &= \mathrm{Tr}(\mathrm{Frob}_\ell) + \det(\mathrm{Frob}_\ell) + 1 \quad \text{(true for any } 2 \times 2 \text{ linear transformation)} \\ &= a_\ell + \ell + 1 \equiv 0 \pmod p \end{aligned}$$

so $\widetilde{E}(\mathbb{F}_\lambda)^-$ has order divisible by p hence $\widetilde{E}(\mathbb{F}_\lambda)[p]^-$ is non-trivial. □

We are going to use the system of Heegner points we have defined to construct cohomology classes in $\mathrm{H}^1(K, E[p])$. One way to do so would be to simply take the trace of the points y_n from H_n to K and then push it to $\mathrm{H}^1(K, E[p])$ through the map δ, but this does not yield interesting infomation. Instead we shall apply an operator to the y_n in order to obtain $\mathrm{Gal}(H_n/H_1)$-invariant elements, then computing the trace from H_1 to K will yield the desired $\mathrm{Gal}(H_n/K)$-invariant classes.

Let $\ell \in \mathcal{L}_E$ be a Kolyvagin prime, so ℓ is inert in K and by lemma 2.1, $G_\ell := \mathrm{Gal}(H_\ell/H_1)$ is cyclic. Fix a generator σ_ℓ of G_ℓ.

Definition 5.5. The group ring element

$$D_\ell := \sum_{i=1}^{\ell} i\sigma_\ell^i = \sum_{i=0}^{\ell+1} \frac{\sigma_\ell^i - 1}{\sigma_\ell - 1} \quad \in \mathbb{Z}[G_\ell]$$

is called the *Kolyvagin derivative operator*. Let

$$\mathcal{N}_E := \{\text{square-free product of primes } \ell \in \mathcal{L}_E\} \text{ (with convention that } 1 \in \mathcal{N}_E)$$

and for every $n \in \mathcal{N}_E$, let

$$G_n := \mathrm{Gal}(H_n/H_1) \cong \prod_{\ell|n} \mathrm{Gal}(H_\ell/H_1) = \prod_{\ell|n} G_\ell$$
$$D_n := \prod_{\ell|n} D_\ell \quad \in \mathbb{Z}[G_n]$$

with $G_1 := 1$ and $D_1 = 1$ by convention.

Remark 5.6. Gross ([Gro91]) defines these derivative operators in the following way: Let

$$\mathrm{Tr}_\ell := \sum_{\sigma \in G_\ell} \sigma \quad \in \mathbb{Z}[G_\ell].$$

Then D_ℓ is defined to be the solution of the following equation in $\mathbb{Z}[G_\ell]$:

$$(\sigma_\ell - 1) \cdot D_\ell = \ell + 1 - \mathrm{Norm}_{H_\ell/H_1}.$$

It is easy to see that D_ℓ defined above satisfies this.

Let $n \in \mathcal{N}_E$ and $y_n \in E(H_n)$ be a Heegner point of conductor n. Then we define

$$[D_n y_n] := D_n y_n \pmod{pE(H_n)} \quad \in E(H_n)/pE(H_n)$$

Proposition 5.7. $[D_n y_n] \in (E(H_n)/pE(H_n))^{G_n}$.

Proof. It suffices to show that for all $\ell|n$, $[D_n y_n]$ is fixed by σ_ℓ, the generator of G_ℓ. Hence we

must prove that: $(\sigma_\ell - 1)D_n y_n \in pE(H_n)$. We can immediately check that

$$(\sigma_\ell - 1)D_\ell = (\ell+1) - \sum_{i=1}^{\ell+1} \sigma_\ell^i = (\ell+1) - \mathrm{Norm}_{H_\ell/H_1}$$

This implies that

$$\begin{aligned}(\sigma_\ell - 1)D_n y_n &= (\sigma_\ell - 1)D_\ell D_m y_n \\ &= (\ell+1)D_m y_n - \mathrm{Norm}_{H_\ell/H_1}(D_m y_n) \\ &= (\ell+1)D_m y_n - D_m(\mathrm{Norm}_{H_\ell/H_1}\, y_n) \\ &= (\ell+1)D_m y_n - D_m(a_\ell y_m) \quad \in pE(H_n) \quad \text{(since } \ell \text{ is a Kolyvagin prime)}\end{aligned}$$

□

We would like to construct a point in $E(H_n)/pE(H_n)$ which is invariant not only for $G_n = \mathrm{Gal}(H_n/H_1)$ but also for $\mathcal{G}_n := \mathrm{Gal}(H_n/K)$ (an abelian group).

To do so, fix a set $\mathfrak{S}$ of coset representatives for the subgroup G_n in $\mathcal{G}_n$ and define:

$$P_n := \sum_{\sigma \in \mathfrak{S}} \sigma D_n y_n.$$

Then clearly the class $[P_n]$ is in $(E(H_n)/pE(H_n))^{\mathcal{G}_n}$.

In order to define a system of cohomology classes we first need a lemma:

Lemma 5.8. The curve E has no p-torsion rational over H_n.

Proof. If not, either $E(H_n)[p] = \mathbb{Z}/p\mathbb{Z}$ or $E(H_n)[p] = (\mathbb{Z}/p\mathbb{Z})^2$. The first implies that $E[p]$ has a cyclic subgroup scheme over $\mathbb{Q}$, as H_n is Galois over $\mathbb{Q}$. Hence the Galois group of $\mathbb{Q}(E[p])$ is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

If $E(H_n)[p] = (\mathbb{Z}/p\mathbb{Z})^2$, then $\mathbb{Q}(E[p])$ is a subfield of H_n and we have a surjective homomorphism $G_n \longrightarrow \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. This is impossible whenever $p > 2$ because $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ is not a quotient of a group of dihedral type. □

From this lemma it follows immediately:

Lemma 5.9. There exists an isomorphism induced by restriction:

$$\mathrm{H}^1(K, E[p]) \xrightarrow{\sim} \mathrm{H}^1(H_n, E[p])^{\mathcal{G}_n}.$$

Proof. Consider the inflation-restriction exact sequence for $\mathrm{Gal}(\overline{\mathbb{Q}}/H_n) \trianglelefteq \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$:

$$0 \longrightarrow \mathrm{H}^1(\mathcal{G}_n, E(H_n)[p]) \xrightarrow{\text{Inf}} \mathrm{H}^1(K, E[p]) \xrightarrow{\text{Res}} \mathrm{H}^1(H_n, E[p])^{\mathcal{G}_n} \longrightarrow \mathrm{H}^2(\mathcal{G}_n, E(H_n)[p])$$

From above lemma (5.8), we have $E(H_n)[p] = 0$, so the kernel of the map Res is 0, while the cokernel injects into a group which is 0. So it is an isomorphism. □

Now we define the cohomology classes. Consider the following diagram:

$$\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
 & & & & & & \mathrm{H}^1(H_n/K, E)[p] & & \\
 & & & & & & \downarrow{\scriptstyle \mathrm{Inf}} & & \\
0 & \longrightarrow & E(K)/pE(K) & \xrightarrow{\delta} & \mathrm{H}^1(K, E[p]) & \longrightarrow & \mathrm{H}^1(K, E)[p] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \mathrm{Res}} & & \\
0 & \longrightarrow & (E(H_n)/pE(H_n))^{\mathcal{G}_n} & \xrightarrow{\delta_n} & \mathrm{H}^1(H_n, E[p])^{\mathcal{G}_n} & \longrightarrow & \mathrm{H}^1(H_n, E)[p]^{\mathcal{G}_n} & &
\end{array} \tag{5.2}$$

The bottom row is exact because the Kummer map δ_n is Galois equivariant. The column on the right is the inflation-restriction sequence for $\mathrm{Gal}(\overline{K}/H_n) \trianglelefteq \mathrm{Gal}(\overline{K}/K)$ and the middle vertical map is an isomorphism from lemma 5.9.

Definition 5.10. Let $c(n)$ be the unique class in $\mathrm{H}^1(K, E[p])$ such that:

$$\mathrm{Res}\, c(n) = \delta_n[P_n] \quad \text{in } \mathrm{H}^1(H_n, E[p])^{\mathcal{G}_n}.$$

Let

$$d(n) = \mathrm{Image}\, c(n) \quad \text{in } \mathrm{H}^1(K, E)[p].$$

By commutativity of the diagram and exactness of the bottom row, $\mathrm{Res}\, c(n) = 0$. Hence there is a unique $\widetilde{d(n)} \in \mathrm{H}^1(H_n/K, E)[p]$ such that

$$\mathrm{Inf}\, \widetilde{d(n)} = d(n) \quad \text{in } \mathrm{H}^1(K, E)[p].$$

Remark 5.11. Observe that there is a natural action of complex conjugation τ on every group of above diagram (5.2). For example, τ acts on $\mathrm{H}^1(K, E[p])$ by acting pointwise on cocycles. Also note that this action of τ commutes with all the maps in the diagram. For example, let us verify that τ commutes with δ: Let $P \in E(K)$ then $\delta(P)$ is represented by the cocycle

$$\xi : \mathrm{Gal}(\overline{K}/K) \longrightarrow E[p], \quad \sigma \longmapsto \sigma(Q) - Q$$

where $[p]Q = P$. Then $\delta(\tau(P))$ is represented by the cocycle: $\sigma \longmapsto \sigma(\tau(Q)) - \tau(Q)$ as clearly $[p]\tau(Q) = \tau(P)$.

Now we derive conditions under which these cohomology classes are trivial.

Proposition 5.12. (a) $c(n)$ is trivial $\iff P_n \in pE(H_n)$.

(b) $d(n)$ and $\widetilde{d(n)}$ are trivial $\iff P_n \in pE(H_n) + E(K)$.

Proof. (a) $c(n) = 0 \iff \operatorname{Res} c(n) = 0 \iff \delta_n[P_n] = 0 \iff [P_n] = 0 \iff P_n \in pE(H_n)$.

(b) Since Inf is injective, $d(n) = 0 \iff \widetilde{d(n)} = 0$. And this happens if and only if either $c(n)$ is trivial, or $c(n)$ is in the image by δ of an element in $E(K)/pE(K)$. □

Remark 5.13. For $n = 1$, $\mathfrak{S}$ is the system of representatives of $\operatorname{Gal}(H_1/K)/\operatorname{Gal}(H_1/H_1)$. i.e., $\mathfrak{S} = \operatorname{Gal}(H_1/K)$

$$P_1 = \sum_{\sigma \in \operatorname{Gal}(H_1/K)} \sigma D_1 y_1 = \operatorname{Norm}_{H_1/K}(y_1) = y_K \quad \text{(by definition)}$$

so $y_K \notin pE(H_1) \iff c(1) \neq 0$. But $y_K \in E(K)$ hence $y_K \notin pE(K) \iff c(1) \neq 0$.

§6. Properties of Cohomology Classes

The cohomology classes we have just constructed are represented by explicit 1-cocycles:

$$\begin{aligned} c(n) : \operatorname{Gal}(\bar{K}/K) &\longrightarrow E[p] \\ \sigma &\longmapsto f(\sigma) := \sigma\left(\frac{1}{p}P_n\right) - \frac{1}{p}P_n - \frac{(\sigma-1)P_n}{p} \end{aligned}$$

and

$$\begin{aligned} \widetilde{d}(n) : \quad \mathcal{G}_n = \operatorname{Gal}(H_n/K) &\longrightarrow E[p] \\ \sigma &\longmapsto \widetilde{f}(\sigma) := -\frac{(\sigma-1)P_n}{p} \end{aligned}$$

Since p is odd, the action of $\tau \in \operatorname{Gal}(K/\mathbb{Q})$ gives direct sum decomposition:

$$\mathrm{H}^1(K, E[p]) \cong \mathrm{H}^1(K, E[p])^+ \oplus \mathrm{H}^1(K, E[p])^-$$

Now we would like to know in which eigenspace does the defined cohomology classes $c(n)$ lies. But before that we recall some standard facts and prove a lemma (6.1) which will be useful for this task (proposition 6.2).

Recall that there is some $-\epsilon \in \{\pm 1\}$, called the *sign of the functional equation*, such that

$$L(E/\mathbb{Q}, s) = -\epsilon L(E/\mathbb{Q}, 2-s)$$

where $L(E/\mathbb{Q}, s)$ is the L-function associated to E over $\mathbb{Q}$. Also recall that if $L(E/\mathbb{Q}, s) = \sum_{n=1}^{\infty} a_n q^n$ then $f_E(z) = \sum_{n=1}^{\infty} a_n q^n$, $q = e^{2\pi i}$ is a weight 2 cuspidal eigenform called the eigenform associated to E. Note that the Atkin-Lehner involution (or Fricke involution) w_N satisfies: $w_N(f_E)(z) = \epsilon f_E(z)$ where $-\epsilon$ is the sign of the functional equation.

Lemma 6.1. The Atkin-Lehner involution (or Fricke involution) w_N satisfies:

$$\tau(z_n) = w_N(\sigma(z_n)) \quad \text{on } X_0(N),$$

for some $\sigma \in \mathcal{G}_n = \operatorname{Gal}(H_n/K)$ which implies that

$$\tau(y_n) = \epsilon \cdot \sigma(y_n) + (\textit{torsion}) \quad \text{in } E(H_n).$$

Proof. Since w_N is an involution, it is sufficient to prove that $w_N(\tau(z_n)) = \sigma(z_n)$. Now $w_N(\tau(z_n)) = w_N\left(\frac{\mathbb{C}}{\mathcal{O}_n}, \frac{\overline{\mathcal{N}_n}^{-1}}{\mathcal{O}_n}\right) = \left(\frac{\mathbb{C}}{\overline{\mathcal{N}_n}^{-1}}, \frac{N^{-1}\mathcal{O}_n}{\overline{\mathcal{N}_n}^{-1}}\right)$. Now our required $\sigma \in \mathcal{G}_n$ is such that the ideal class $[\overline{\mathcal{N}_n}^{-1}] \in \operatorname{Pic}\mathcal{O}_n$ corresponds to σ under the Artin map isomorphism.

For the second relation, note that for each modular curve $X_0(N)$, the cusps 0 and ∞ are always defined over $\mathbb{Q}$ [Cus]. So we have:

$$\tau(x_n - \infty) = w_N(\sigma(x_n - \infty)) + (w_N(\infty) - \infty) \quad \text{on } J(X_0(N))$$

Now we apply Φ (from equation 3.2) to this and noting that w_N, σ, τ commutes with Φ, $w_N(\infty) = 0$ on $J(X_0(N))$, and that w_N acts on elliptic curve E via multiplication by ϵ, we get

$$\tau(y_n) = \epsilon(\sigma(y_n)) + \Phi(0 - \infty)$$

By Manin-Drinfeld theorem, the divisor class $(0 - \infty)$ is a torsion point in $J(X_0(N))$. □

Since $p > 2$, the action of $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ gives us the decomposition

$$\mathrm{H}^1(K, E[p]) = \mathrm{H}^1(K, E[p])^+ \oplus \mathrm{H}^1(K, E[p])^-$$
$$\mathrm{H}^1(K, E)[p] = \mathrm{H}^1(K, E)[p]^+ \oplus \mathrm{H}^1(K, E)[p]^-$$

Now we see where as n varies, where does the derivative classes we have defined lies:

Proposition 6.2. (a) The class $[P_n]$ lies in the $\epsilon_n = \epsilon \cdot (-1)^{f_n}$ eigenspace for τ in $(E(H_n)/pE(H_n))^{\mathcal{G}_n}$, where $f_n = |\{l \text{ prime } : l|n\}|$.

(b) The class $c(n)$ lies in the ϵ_n-eigenspace for τ in $\mathrm{H}^1(K, E[p])$ and the class $d(n)$ lies in the ϵ_n-eigenspace for τ in $\mathrm{H}^1(K, E)[p]$.

Proof. (a) The lift of complex conjugation $\tau \in \mathrm{Gal}(H_n/\mathbb{Q})$ acts on elements $\sigma \in \mathcal{G}_n$ by sending $\tau^{-1}\sigma\tau$ to σ^{-1}. Hence we have $\sigma\tau = \sigma^{-1}\tau$. Let us consider:

$$\tau(P_n) = \tau(\sum_{\sigma \in \mathfrak{S}} \sigma D_n y_n) = \sum_{\sigma \in \mathfrak{S}} \sigma^{-1}\tau(D_n y_n)$$

where $D_n = \prod_{\ell|n} D_\ell$ with D_ℓ such that $(\sigma_\ell - 1) \cdot D_\ell = \ell + 1 - \mathrm{Norm}_{H_\ell/H_1}$. Now compute

$$(\ell + 1 - \mathrm{Norm}_{H_\ell/H_1})\tau = \tau(\ell+1) - \sum_{\sigma \in G_\ell} \sigma\tau = \tau(\ell+1) - \tau \sum_{\sigma \in G_\ell} \sigma^{-1} = \tau(\ell + 1 - \mathrm{Norm}_{H_\ell/H_1})$$

This implies that

$$(\sigma_\ell - 1)D_\ell\tau = \tau(\sigma_\ell - 1)D_\ell = -\sigma_\ell^{-1}(\sigma_\ell - 1)\tau D_\ell$$

so that

$$(\sigma_\ell - 1)(\sigma_\ell D_\ell \tau + \tau D_\ell) = 0$$

which means that $(\sigma_\ell D_\ell \tau + \tau D_\ell) = k\,\mathrm{Norm}_{H_\ell/H_1}$ for some $\ell \in \mathbb{Z}$.

By norm relations, $\text{Norm}_{H_\ell/H_1}(y_n) = a_\ell \cdot y_m \equiv 0 \pmod{pE(H_n)}$, hence we have

$$\begin{aligned}\tau(P_n) &= \sum_{\sigma\in\mathfrak{S}} \sigma^{-1}\tau(\prod_{\ell|n} D_\ell)y_n \\ &\equiv \sum_{\sigma\in\mathfrak{S}} \sigma^{-1}(\prod_{\ell|n} -\sigma_\ell D_\ell)\tau y_n \pmod{pE(H_n)} \\ &\equiv (-1)^{f_n}(\prod_{\ell|n}\sigma_\ell)\sum_{\sigma\in\mathfrak{S}} \sigma^{-1}D_n(\tau(y_n)) \pmod{pE(H_n)}\end{aligned}$$

But $\tau(y_n) = \epsilon\cdot\sigma'(y_n) + (torsion)$ for some $\sigma' \in \mathcal{G}_n$ by lemma 6.1. And by lemma 5.8, $E(H_n)[p] = \{0\}$ hence every torsion point in $E(H_n)$ must be in $pE(H_n)$. Therefore

$$\tau P_n \equiv \epsilon_n(\prod_{\ell|n}\sigma_\ell)\sigma' \sum_{\sigma\in\mathfrak{S}} \sigma^{-1}D_n y_n \pmod{pE(H_n)}$$

But $(\prod_{\ell|n}\sigma_\ell)\sigma' \in \mathcal{G}_n$ and $\sum_{\sigma\in\mathfrak{S}}\sigma^{-1}D_n y_n$ is P_n (noting that if $s_1,\cdots s_n$ are coset representatives of quotient of an abelian group then so are $s_1^{-1},\cdots s_n^{-1}$) which is invariant under the action of $\mathcal{G}_n$ modulo $pE(H_n)$. So

$$\tau P_n \equiv \epsilon_n P_n \pmod{pE(H_n)}.$$

(b) This clearly follows from (a) and by remark 5.11 that the action of τ commutes with every map in diagram 5.2. □

§7. Local triviality of Cohomology Classes

In this section we shall derive conditions for when the cohomology classes $c(n)$ we have constructed lie in the p-Selmer group.

Recall the fundamental short exact sequence for E/K which gives us the diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \frac{E(K)}{pE(K)} & \xrightarrow{\delta_E} & \mathrm{H}^1(K,E[p]) & \xrightarrow{f} & \mathrm{H}^1(K,E)[p] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow g & & \\ 0 & \longrightarrow & \prod_{v\in M_K}\frac{E(K_v)}{pE(K_v)} & \xrightarrow{\delta} & \prod_{v\in M_K}\mathrm{H}^1(K_v,E[p]) & \longrightarrow & \prod_{v\in M_K}\mathrm{H}^1(K_v,E)[p] & \longrightarrow & 0 \end{array}$$

Now $c(n) \in \mathrm{H}^1(K,E[p])$ is in the p-Selmer group $(= \ker(g\circ f))$ if and only if the reduction $d(n)_v$ of $f(c(n)) = d(n) \in \mathrm{H}^1(K,E)[p]$ is trivial at every prime v.

Our first proposition is that if a place v does not divide n then $d(n)_v$ is trivial in $\mathrm{H}^1(K_v,E)[p]$. But first we recall a theorem of Lang about algebraic groups:

Theorem 7.1. (Lang) Let A be a smooth, connected, commutative algebraic group over a finite field $\mathbb{F}$. Then $\mathrm{H}^1(\mathbb{F},A(\mathbb{F})) = 0$.

Proposition 7.2. The class $d(n)_v$ is locally trivial in $\mathrm{H}^1(K_v, E)[p]$ at the archimedean prime $v = \infty$ and at all the finite primes v of K which do not divide n.

Proof. **Case 1:** When $v = \infty$ then $K_\infty = \mathbb{C}$, since K is imaginary quadratic, and hence Galois cohomology of E is trivial i.e., $\mathrm{H}^1(\mathbb{C}, E) = 0$.

Case 2: $(v, n \cdot N) = 1$: $d(n)$ is inflated from a class $\widetilde{d(n)} \in \mathrm{H}^1(H_n/K, E)[p]$ where H_n/K is unramified at v. Hence $d(n)_v$ lies in the image of the subgroup $\mathrm{H}^1(K_v^{nr}/K_v, E)[p]$, where K_v^{nr} is the maximal unramified extension. We are going to prove that this group is trivial when E has good reduction at v.

Let q be a prime lying under v. Recall that we have an exact sequence

$$0 \longrightarrow E_1 \longrightarrow E(\overline{K_v}) \xrightarrow{\text{red}} \widetilde{E}(\overline{\mathbb{F}_v}) \longrightarrow 0$$

where E_1 is a pro-q group. Taking $\mathrm{Gal}(K_v^{nr}/K_v)$-cohomology, we get an exact sequence

$$0 \longrightarrow E_1(K_v) \longrightarrow E(K_v) \longrightarrow \widetilde{E}(\mathbb{F}_v)$$
$$\mathrm{H}^1(K_v^{nr}/K_v, E_1) \longrightarrow \mathrm{H}^1(K_v^{nr}/K_v, E) \longrightarrow \mathrm{H}^1(\mathbb{F}_v, \widetilde{E})$$

Since E_1 is a pro-q group and $\mathrm{Gal}(K_v^{nr}/K_v) = \widehat{\mathbb{Z}}$, the profinite completion of $\mathbb{Z}$, we can deduce that $\mathrm{H}^1(K_v^{nr}/K_v, E)[p] = 0$. Hence we have an injection

$$\mathrm{H}^1(K_v^{nr}/K_v, E)[p] \hookrightarrow \mathrm{H}^1(\mathbb{F}_v, \widetilde{E}(\overline{\mathbb{F}_v}))[p]$$

By using Lang's theorem we conclude that $\mathrm{H}^1(\mathbb{F}_v, \widetilde{E}(\overline{\mathbb{F}_v}))$ is trivial and we are done.

Case 3: $v \nmid n$ but $v|N$:

Consider a Neron model $\mathcal{E}$ for E over $\mathcal{O}_v$ and let $\mathcal{E}^0$ be the connected component of the identity of $\mathcal{E}$ and $\mathcal{E}/\mathcal{E}^0$ the group of components. By Lang's theorem (7.1), $\mathrm{H}^1(\mathbb{F}_v, \mathcal{E}^0) = 0$. So we have the injection

$$\mathrm{H}^1(K_v^{nr}/K_v, \mathcal{E}^0) \hookrightarrow \mathrm{H}^1(\mathbb{F}_v, \mathcal{E}/\mathcal{E}^0)$$

So to check triviality of $d(n)_v$ in $\mathrm{H}^1(K_v^{nr}/K_v, \mathcal{E}^0)$, we need to check the triviality of its image in $\mathrm{H}^1(\mathbb{F}_v, \mathcal{E}/\mathcal{E}^0)$.

Let w be a place of H_n over v. Recall that $d(n)_v$ is represented by the cocyle

$$\mathrm{Gal}((H_n)_w/K_v) \longrightarrow E((H_n)_w), \quad \gamma \longmapsto -\frac{(\gamma - 1)P_n}{p}$$

where $-\frac{(\gamma-1)P_n}{p}$ is a combination of conjugates of $y_n \in E(H_n)$. Now $d(n)_v \in \mathrm{H}^1(K_v, E)[p]$ is killed by p hence in order to know that $d(n)_v$ is trivial, it is sufficient to show that the reduction of y_n in $\mathcal{E}/\mathcal{E}^0$ is killed by a number prime to p. We are going to show that reduction of y_n in $\mathcal{E}/\mathcal{E}^0$ lies in a subgroup of order prime to p.

First of all, we deduce from ([GZ86]; §III, 3.1) that the class of Heegner divisor $(x_n) - (\infty)$ lies, upto translation by the rational torsion point $(0) - (\infty)$, in $J(X_0(N))^0$, the identity component of the Néron model of the abelian variety $J(X_0(N))$ over $\mathcal{O}_v$. Hence y_n, upto translation by a rational torsion of $\mathcal{E}$, lies in $\mathcal{E}^0$. Since $E(\mathbb{Q})[p]$ is trivial by assumption, the rational torsion point must have order prime to p. Hence the y_n's lies in a subgroup whose image in $\mathcal{E}/\mathcal{E}^0$ has order prime to p. □

Now we look at places which does divide n.

Proposition 7.3. If $n = \ell m$ and $\lambda = \ell\mathcal{O}_K$, then

$d(n)_\lambda$ is trivial $\iff$ $P_m \in pE((H_m)_{\lambda_m}) = pE(K_\lambda)$ for one (and hence all) place(s) λ_m of H_m dividing λ

In particular taking $m = 1$, we get $d(\ell)_\lambda$ is non-trivial $\iff$ $P_1 = y_K \notin pE(K_\lambda)$. Note that the latter condition is independent of ℓ, hence we get that the system of cohomology classes $\{d(n)_\lambda\}_{n\in\mathcal{N}_E}$ are "Rigid" in the sense that $d(n)_\lambda \neq 0$ implies all other classes are non-trivial.

Proof. We recall from 4.2 that the prime λ splits completely in H_m, each factor λ_m is totally ramified in H_n, i.e. $\lambda_m\mathcal{O}_{H_n} = (\lambda_n)^{\ell+1}$, and $\mathbb{F}_{\lambda_n} = \mathbb{F}_{\lambda_m} = \mathbb{F}_\lambda$.

Recall that the cohomology class $d(n)_\lambda \in \mathrm{H}^1(K_\lambda, E)[p]$ is represented by the cocycle:

$$\mathrm{Gal}(\overline{K}_\lambda/K_\lambda) \longrightarrow E(K_\lambda), \quad \sigma \longmapsto -\frac{(\sigma-1)P_n}{p}.$$

Since $P_n \in E(H_n)$, we have that $d(n)_\lambda$ is trivial on $\mathrm{Gal}(\overline{K}_\lambda/K_{\lambda_n})$. Also $-\frac{(\sigma-1)P_n}{p}$ actually lives in $E(H_n) \subset E(K_{\lambda_n})$. Hence $d(n)_\lambda$ actually lives in $\mathrm{H}^1(G_\ell, E(K_{\lambda_n}))[p]$ (noting that $\mathrm{Gal}(K_{\lambda_n}/K_\lambda) = \mathrm{Gal}(K_{\lambda_n}/K_{\lambda_m}) \cong G_\ell$).

Since ℓ is a Kolyvagin prime, $\ell \nmid N$ and hence E has good reduction at ℓ. We know that there is an exact sequnce of G_ℓ-modules

$$0 \longrightarrow E_1(K_{\lambda_n}) \longrightarrow E_0(K_{\lambda_n}) \xrightarrow{\text{red}} \widetilde{E}(\mathbb{F}_{\lambda_n}) \longrightarrow 0$$

Since $E_1(K_{\lambda_n})$ is a pro-ℓ group and $p \neq \ell$, we have $\mathrm{H}^1(G_\ell, E_1(K_{\lambda_n}))[p] = 0$. So we have the injection:

$$\mathrm{H}^1(G_\ell, E(K_{\lambda_n}))[p] \hookrightarrow \mathrm{H}^1(G_\ell, \widetilde{E}(\mathbb{F}_\lambda))[p].$$

Since G_ℓ acts trivially on $\widetilde{E}(\mathbb{F}_\lambda)$, we have

$$\mathrm{H}^1(G_\ell, \widetilde{E}(\mathbb{F}_\lambda))[p] = \mathrm{Hom}(G_\ell, \widetilde{E}(\mathbb{F}_\lambda)[p])$$

Hence $d(n)_\lambda$ is trivial $\iff$ it has trivial image in $\mathrm{H}^1(G_\ell, \widetilde{E}(\mathbb{F}_\lambda))[p]$ $\iff$ $\frac{(\sigma-1)P_n}{p}$ has trivial reduction modulo λ_n for every $\sigma \in G_\ell$ $\iff$ the point $Q_n := \frac{(\sigma_\ell-1)P_n}{p}$ has trivial reduction modulo λ_n since G_ℓ is cyclic with generator σ_ℓ.

Recall that $P_n = \sum_{\sigma\in\mathfrak{S}} \sigma D_n y_n)$ and $(\sigma_\ell - 1)\cdot D_\ell = \ell + 1 - \mathrm{Norm}_{H_\ell/H_1}$, so we have

$$Q_n = \sum_{\sigma\in\mathfrak{S}} \sigma D_m \left(\frac{\ell+1}{p} y_n - \frac{a_\ell}{p} y_m\right) \quad \text{(also using norm relations 4.1)}$$

and by congruence relations (4.2), we have (denoting $\left(\frac{H_m/\mathbb{Q}}{\lambda_m}\right)$ by $\mathrm{Frob}(\lambda_m)$)

$$\frac{\ell+1}{p}y_n - \frac{a_\ell}{p}y_m \equiv \frac{(\ell+1)\,\mathrm{Frob}(\lambda_m) - a_\ell}{p}y_m \pmod{\lambda_n}$$

at all primes λ_n dividing λ in H_n. For $\sigma \in \mathrm{Gal}(H_n/K)$ we conjugate this congruence $(\mathrm{mod}\ \sigma^{-1}\lambda_n)$ by σ to obtain:

$$\sigma\left(\frac{\ell+1}{p}y_n - \frac{a_\ell}{p}y_m\right) \equiv \sigma\left(\frac{(\ell+1)\,\mathrm{Frob}(\sigma^{-1}\lambda_m) - a_\ell}{p}\right)y_m \pmod{\lambda_n}$$

but $\sigma\,\mathrm{Frob}(\sigma^{-1}\lambda_m) = \sigma\sigma^{-1}\,\mathrm{Frob}(\lambda_m)\sigma$ so we obtain:

$$\sigma\left(\frac{\ell+1}{p}y_n - \frac{a_\ell}{p}y_m\right) \equiv \left(\frac{(\ell+1)\,\mathrm{Frob}(\lambda_m) - a_\ell}{p}\right)\sigma y_m \pmod{\lambda_n}$$

Hence:

$$Q_n \equiv \frac{(\ell+1)\,\mathrm{Frob}(\lambda_m) - a_\ell}{p}P_m \pmod{\lambda_n}$$

We know by proposition 6.2 that the reduction of P_m modulo λ_m lies in the ϵ_m-eigenspace of $\widetilde{E}(\mathbb{F}_\lambda)/p\widetilde{E}(\mathbb{F}_\lambda)$ for the action of complex conjugation τ.

Consider the eigenspaces $E(\mathbb{F}_\lambda)^+, E(\mathbb{F}_\lambda)^- \subset E(\mathbb{F}_\lambda)$. On the eigenspace $\widetilde{E}(\mathbb{F}_\lambda)^+$ the automorphism $\mathrm{Frob}(\lambda_m)$ acts as the identity: since ℓ is a 'Kolyvagin's prime', τ is conjugate to $\mathrm{Frob}(\lambda_m)$ so it has order 2. Hence $(\ell+1)\,\mathrm{Frob}(\lambda_m) - a_\ell$ acts as multiplication by $\ell + 1 - a_\ell$, which is the order of $\widetilde{E}(\mathbb{F}_\lambda)^+$, by the proof of proposition (5.4). Similarly on $\widetilde{E}(\mathbb{F}_\lambda)^-$, $\mathrm{Frob}(\lambda_m)$ acts as minus the identity so that $(\ell+1)\,\mathrm{Frob}(\lambda_m) - a_\ell$ acts as the multiplication by minus the order of $\widetilde{E}(\mathbb{F}_\lambda)^-$. In any case we conclude that $(\ell+1)\,\mathrm{Frob}(\lambda_m) - a_\ell$ kills $\widetilde{E}(\mathbb{F}_\lambda)$.

The reduction of P_m modulo λ_n lies in $\widetilde{E}(\mathbb{F}_\lambda)_p^{\epsilon_m} \cong \mathbb{Z}/p\mathbb{Z}$, by proposition (5.4). So the reduction $\widetilde{Q}_n$ of Q_n is zero $\iff$ $\widetilde{P}_m/p \in \widetilde{E}(\mathbb{F}_\lambda)$, i.e. $\widetilde{P}_m \in p\widetilde{E}(\mathbb{F}_\lambda)$, which is if and only if $P_m \in p(K_\lambda)$ since $[p]$ is an isomorphism on E_1 (since it is a pro-ℓ group and $p \neq \ell$). □

§8. Local Tate duality

In this section we are going to review some basic results from Tate's local duality which we will use in order to prove proposition 1.7. We first fix notation:

$\mathcal{O}_\lambda$ a complete discrete valuation ring with maximal ideal $\mathfrak{m}$

$\mathbb{F}_\lambda := \mathcal{O}_\lambda/\mathfrak{m}$, the residue field which is a finite field of characteristic ℓ

K_λ field of fractions of $\mathcal{O}_\lambda$

K_λ^{nr} maximal unramified extension of K_λ

$\mathfrak{g} := \mathrm{Gal}(K_\lambda^{nr}/K_\lambda)$ is the Galois group of K_λ^{nr}/K_λ isomorphic to $\mathrm{Gal}(\overline{\mathbb{F}_\lambda}/\mathbb{F}_\lambda)$ which is isomorphic to profinite completion of $\hat{\mathbb{Z}}$ by sending the generator $1 \in \hat{\mathbb{Z}}$ to the Frobenius automorphism $\mathrm{Frob}(\lambda) \in \mathfrak{g}$.

Let E be an elliptic curve over K_λ with good reduction modulo $\mathfrak{m}$. Say $\widetilde{E}$ be the elliptic curve defined over $\mathbb{F}_\lambda$ obtained by reducing E. We have the exact sequence

$$0 \longrightarrow E_1 \longrightarrow E(\overline{K_\lambda}) \xrightarrow{\text{red}} \widetilde{E}(\overline{\mathbb{F}}_\lambda) \longrightarrow 0 \tag{8.1}$$

where E_1, the kernel of the reduction map is a pro-ℓ group.

Proposition 8.1. Let p be a prime different than ℓ. Then

$$E(K_\lambda)/pE(K_\lambda) \cong \mathrm{H}^1(\mathfrak{g}, E[p]).$$

Proof. Taking Galois cohomology of the exact sequence $0 \longrightarrow \widetilde{E}[p] \longrightarrow \widetilde{E} \xrightarrow{[p]} \widetilde{E} \longrightarrow 0$ of $\mathfrak{g}$-modules gives the following exact sequence:

$$0 \longrightarrow \widetilde{E}(\mathbb{F}_\lambda)/p\widetilde{E}(\mathbb{F}_\lambda) \longrightarrow \mathrm{H}^1(\mathfrak{g}, \widetilde{E}(\overline{\mathbb{F}}_\lambda)[p]) \longrightarrow \mathrm{H}^1(\mathfrak{g}, \widetilde{E}(\overline{\mathbb{F}}_\lambda)[p] \longrightarrow 0$$

By Lang's theorem (7.1), $\mathrm{H}^1(\mathfrak{g}, \widetilde{E}(\overline{\mathbb{F}}_\lambda) = 0$ so the middle two terms in above exact sequence are isomorphic. The proposition follows from the fact that

$$E(K_\lambda)/pE(K_\lambda) \cong \widetilde{E}(\mathbb{F}_\lambda)/p\widetilde{E}(\mathbb{F}_\lambda) \quad \text{and} \quad E[p] \cong \widetilde{E}(\overline{\mathbb{F}}_\lambda)[p].$$

(These both things follows from the following commutative diagram

$$\begin{array}{ccccccccc}
 & & 0 & \longrightarrow & E(K_\lambda)[p] & \longrightarrow & \widetilde{E}(\mathbb{F}_\lambda)[p] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & E_1(K_\lambda) & \longrightarrow & E(K_\lambda) & \xrightarrow{\text{red}} & \widetilde{E}(\mathbb{F}_\lambda) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \sim} & & \downarrow{\scriptstyle [p]} & & \downarrow{\scriptstyle [p]} & & \\
0 & \longrightarrow & E_1(K_\lambda) & \longrightarrow & E(K_\lambda) & \xrightarrow{\text{red}} & \widetilde{E}(\mathbb{F}_\lambda) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & \longrightarrow & E(K_\lambda)/pE(K_\lambda) & \longrightarrow & \widetilde{E}(\mathbb{F}_\lambda)/p\widetilde{E}(\mathbb{F}_\lambda) & \longrightarrow & 0
\end{array} \tag{8.2}$$

and the fact that E_1 in equation 8.1 is pro-ℓ group so $[p]$ is an isomorphism on E_1.) □

Theorem 8.2. (Tate-local duality). There exists a symmetric, non-degenerate pairing of $\mathbb{Z}/p\mathbb{Z}$-vector spaces:

$$\langle \cdot, \cdot \rangle : \mathrm{H}^1(K_\lambda, E[p]) \times \mathrm{H}^1(K_\lambda, E[p]) \longrightarrow \mathbb{Z}/p\mathbb{Z}$$

induced by Weil pairing, cup product, and the invariant map from local class field theory.

Proof. The (bilinear) Weil pairing $E[p] \times E[p] \longrightarrow \mu_p$ over K_λ induces a linear map

$$E[p] \otimes E[p] \longrightarrow \mu_p,$$

which induces a map on cohomology groups for every $j \geq 0$

$$\mathrm{H}^j(K_\lambda, E[p] \otimes E[p]) \longrightarrow \mathrm{H}^j(K_\lambda, \mu_p), \tag{8.3}$$

since Weil pairing is Galois equivariant (or invariant).

Now composing cup product with this map for $j = 2$ we obtain a pairing:

$$\mathrm{H}^1(K_\lambda, E[p]) \times \mathrm{H}^1(K_\lambda, E[p]) \longrightarrow \mathrm{H}^2(K_\lambda, \mu_p)$$

Moreover the invariant map from local class field theory gives a canonical isomorphism:

$$\mathrm{H}^2(K_\lambda, \mu_p) = \mathrm{Br}(K_\lambda)[p] \xrightarrow{\sim} \frac{1}{p}\mathbb{Z}/\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z}.$$

□

Now consider the following commutative diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E(K_\lambda)/pE(K_\lambda) & \longrightarrow & \mathrm{H}^1(K_\lambda, E[p]) & \longrightarrow & \mathrm{H}^1(K_\lambda, E)[p] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow\sim & & \downarrow & & \\
0 & \longrightarrow & \mathrm{H}^1(K_\lambda, E)[p]^* & \longrightarrow & \mathrm{H}^1(K_\lambda, E[p])^* & \longrightarrow & E(K_\lambda)/pE(K_\lambda)^* & \longrightarrow & 0
\end{array}$$

where $\cdot^* = \mathrm{Hom}_{\mathbb{Z}}(\cdot, \mu_p(\overline{K_\lambda}))$ is the Cartier dual. The rows are exact and the middle map is an isomorphism by Tate local duality. Because of the commutativity of the diagram the first vertical map is injective, but in fact it also an isomorphism since we have the following:

Lemma 8.3. $\dim_{\mathbb{Z}/p\mathbb{Z}} E(K_\lambda)/pE(K_\lambda) = \dim_{\mathbb{Z}/p\mathbb{Z}} \mathrm{H}^1(K_\lambda, E)[p]$.

Proof. First note that if M is any discrete $\mathfrak{g}$-module then $M^{\mathfrak{g}} = M^{\{\mathrm{Frob}(\lambda)\}}$, the elements fixed by $\mathrm{Frob}(\lambda)$ since $\mathfrak{g}$ is a pro-cyclic group generated by $\mathrm{Frob}(\lambda)$. Now consider the action of $\mathrm{Frob}(\lambda) - 1$ on $E[p]$. We have the following exact sequence of $\mathbb{F}_p$ vector spaces

$$0 \longrightarrow \ker(\mathrm{Frob}(\lambda) - 1) \longrightarrow E[p] \longrightarrow E[p] \longrightarrow \frac{E[p]}{(\mathrm{Frob}(\lambda) - 1)E[p]} \longrightarrow 0$$

so we have $\ker(\mathrm{Frob}(\lambda) - 1) = E[p]^{\{\mathrm{Frob}(\lambda)\}}$ and $E[p]/(\mathrm{Frob}(\lambda) - 1)E[p]$ have the same dimension. Since we have:

$$E(K_\lambda)/pE(K_\lambda) \cong \mathrm{H}^1(\mathfrak{g}, E[p]) = \frac{E[p]}{(\mathrm{Frob}(\lambda) - 1)E[p]} \quad \text{and} \quad E[p]^{\{\mathrm{Frob}(\lambda)\}} = \widetilde{E}(\mathbb{F}_\lambda)[p] \cong E(K_\lambda)[p],$$

we find that $E(K_\lambda)/pE(K_\lambda)$ and $E(K_\lambda)[p]$ have the same dimension over $\mathbb{F}_p$.

Now we check that $E(K_\lambda)[p]$ and $\mathrm{H}^1(K_\lambda, E)[p]$ have same dimension to complete the proof. Consider the inflation-restriction sequence for $\mathrm{Gal}(\overline{K}/K^{nr}) \trianglelefteq \mathrm{Gal}(\overline{K}/K)$:

$$0 \longrightarrow \mathrm{H}^1(\mathfrak{g}, E[p]) \longrightarrow \mathrm{H}^1(K, E[p]) \longrightarrow \mathrm{H}^1(K^{nr}, E[p])^{\{\mathrm{Frob}(\lambda)\}} \longrightarrow \mathrm{H}^2(\mathfrak{g}, E[p])$$

The last group is 0 by Galois cohomology. We also have

$$0 \longrightarrow E(K_\lambda)/pE(K_\lambda) \longrightarrow \mathrm{H}^1(K_\lambda, E[p]) \longrightarrow \mathrm{H}^1(K_\lambda, E)[p] \longrightarrow 0.$$

Since $\mathfrak{g} \cong E(K_\lambda)/pE(K_\lambda)$, we have

$$\begin{aligned}
\mathrm{H}^1(K_\lambda, E)[p] &\cong \mathrm{H}^1(K^{nr}, E[p])^{\{\mathrm{Frob}(\lambda)\}} \\
&= \mathrm{Hom}(K^{nr}, E[p])^{\{\mathrm{Frob}(\lambda)\}} \\
&= \mathrm{Hom}(\Delta, E[p])^{\{\mathrm{Frob}(\lambda)\}} \quad \text{(where } \Delta \text{ is tamely ramified inertia)} \\
&= \mathrm{Hom}(\mathbb{Z}_p(1), E[p])^{\{\mathrm{Frob}(\lambda)\}} \quad \text{(because } \Delta \cong \prod_{q \neq \ell} \mathbb{Z}_q(1)) \\
&= \mathrm{Hom}(\mu_p, E[p])^{\{\mathrm{Frob}(\lambda)\}}
\end{aligned}$$

This last group has the same dimension as $\widetilde{E}(F_\lambda)[p] \cong E(K_\lambda)[p]$ by Weil pairing. □

So we have an isomorphism $E(K_\lambda)/pE(K_\lambda) \xrightarrow{\sim} \mathrm{H}^1(K_\lambda, E)[p]^*$ and we get

Proposition 8.4. The pairing of (8.3) induces a non-degenerate pairing of $\mathbb{F}_p$-vector spaces

$$\langle \cdot, \cdot \rangle : E(K_\lambda)/pE(K_\lambda) \times \mathrm{H}^1(K_\lambda, E)[p] \longrightarrow \mathbb{Z}/p\mathbb{Z}. \tag{8.4}$$

Remark 8.5. When the p-torsion of E is rational over K_λ there exists an explicit formula for the pairing $\langle \cdot, \cdot \rangle$ of 8.4: Take $c_1 \in E(K_\lambda)/pE(K_\lambda)$ and construct the point

$$e_1 = \mathrm{Frob}(\lambda)\left(\frac{1}{p}c_1\right) - \frac{1}{p}c_1 \quad \text{in } E(K_\lambda)[p].$$

Take $c_2 \in \mathrm{H}^1(K_\lambda, E[p])$ and associate to it the homomorphism $\phi_2 : \mu_p \longrightarrow E(K_\lambda)[p]$ as in the proof of 8.3. Fix a primitive p^{th}-root ξ of unity in $K_\lambda^\times$ and let $\phi_2(\xi) = e_2$ in $E(K_\lambda)[p]$. Then:

$$\xi^{\langle c_1, c_2 \rangle} = \{e_1, e_2\},$$

where $\{,\}$ is the Weil pairing on $E[p] = E(K_\lambda)[p]$. A proof of this construction can be found in an appendix of [Was89].

§9. Criterion for locally vanishing of Selmer group

In this section we are going to apply proposition 8.4 in the specific local situation which arises in study of Heegner points: Let K is a quadratic imaginary extension of $\mathbb{Q}$ and K_λ is

the completion of K at the place $\lambda = \ell\mathcal{O}_K$ where $\ell \in \mathcal{L}_E$ is a Kolyvagin prime (so inert in K). First of all we claim that

Claim: The p-torsion of E is rational over K_λ. i.e., $E[p] = E(K_\lambda)[p]$.

Proof: Since ℓ is a Kolyvagin prime and τ has order 2, λ splits completely in $K(E[p])/K$. So if γ is a prime of $K(E[p])$ lying above λ, we have $\mathbb{F}_\lambda \cong \mathbb{F}_\gamma$, so that

$$E(K_\lambda)[p] \cong E(\mathbb{F}_\lambda)[p] \cong E(\mathbb{F}_\gamma)[p] \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$

In this situation the spaces involved in the pairing (8.4) have each dimension 2 over $\mathbb{Z}/p\mathbb{Z}$: $E(K_\lambda)/pE(K_\lambda)$ is isomorphic to $\widetilde{E}(\mathbb{F}_\lambda)/p\widetilde{E}(\mathbb{F}_\lambda)$ by diagram 8.2. The latter has dimension 2 because of the above claim. And $\mathrm{H}^1(K_\lambda, E)[p]$ is of dimension 2 from non-degeneracy of the pairing. However we wish to work with spaces of dimension 1, so we shall consider the action of τ on these spaces.

Lemma 9.1. The eigenspaces $(E(K_\lambda)/pE(K_\lambda))^\pm$ and $(\mathrm{H}^1(K_\lambda, E)[p])^\pm$ for $\mathrm{Gal}(K_\lambda/\mathbb{Q}_\ell) = \mathrm{Gal}(K/\mathbb{Q}) = \{1, \tau\}$ each have dimension 1 over $\mathbb{Z}/p\mathbb{Z}$.

Proof. For the first one, note that as remarked above, $E(K_\lambda)/pE(K_\lambda)$ has dimension 2 and $E(K_\lambda)[p]$ also has dimension 2. We have natural injection $E(K_\lambda)[p] \hookrightarrow E(K_\lambda)/pE(K_\lambda)$ which turns into isomorphism of vector spaces. Morover we can check that it is an isomorphism as $\mathrm{Gal}(K_\lambda/\mathbb{Q}_\ell)$-modules.

For the second, consider the following Inflation-Restriction sequence for the inertia $I_\lambda := \mathrm{Gal}(\overline{K_\lambda}/K_\lambda^{sep}) \trianglelefteq \mathrm{Gal}(\overline{K_\lambda}/K_\lambda) = G_{K_\lambda}$

$$0 \longrightarrow \mathrm{H}^1(K_\lambda^{sep}/K_\lambda, E(K_\lambda^{sep})[p]) \xrightarrow{\mathrm{Inf}} \mathrm{H}^1(K_\lambda, E[p]) \xrightarrow{\mathrm{Res}} \mathrm{H}^1(I_\lambda, E[p])^{G_{K_\lambda}/I_\lambda} \longrightarrow \mathrm{H}^2(K_\lambda^{sep}/K_\lambda, E[p])$$

Since $\mathrm{Gal}(K_\lambda^{sep}/K_\lambda) \cong \mathrm{Gal}(\overline{\mathbb{F}}_\lambda/\mathbb{F}_\lambda)$ is a pro-ℓ group, $\mathrm{H}^i(K_\lambda^{sep}/K_\lambda, E[p]) = 0$ for all $i \geq 1$. Hence we have isomorphisms (as $\mathrm{Gal}(K_\lambda/\mathbb{Q}_\ell)$-modules)

$$\begin{aligned}
\mathrm{H}^1(K_\lambda, E[p]) &\cong \mathrm{H}^1(I_\lambda, E[p])^{G_{K_\lambda}/I_\lambda} \\
&\cong \mathrm{Hom}(I_\lambda, E[p]) \quad \text{(since } G_{K_\lambda} \text{ and } I_\lambda \text{ acts trivially on } E[p]) \\
&\cong \mathrm{Hom}(\mu_p(\overline{K_\lambda}), E[p]) \quad \text{(any homomorphism will factor through tame inertia)}
\end{aligned}$$

From the congruence $\ell + 1 \equiv 0 \pmod{p}$, we get that $\mathbb{F}_\lambda$ contains all the p^{th}-roots of unity. Since p is odd, by Hensel's lemma we can lift these roots to K_λ. Morover, since p does not divide $\ell - 1$ and p is odd we have $\mu_p(\mathbb{Q}_\ell) = \{1\}$, which implies

$$\mu_p(K_\lambda) = \mu_p(K_\lambda)^-. \quad \text{i.e., } \tau \text{ acts non-trivially}$$

So we have $\mathrm{Hom}(\mu_p, E[p]) \cong E(K_\lambda)[p]$ as groups, but with reversed action of τ, i.e.,

$$\mathrm{H}^1(K_\lambda, E)[p]^\pm \cong \mathrm{Hom}(\mu_p, E[p])^\pm \cong E(K_\lambda)[p]^\mp.$$

□

Proposition 9.2. The pairing $\langle \cdot, \cdot \rangle$ of (8.4) induces non-degenerate pairings of one dimensional $\mathbb{Z}/p\mathbb{Z}$-vector spaces

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

In particular if $d_\lambda \neq 0$ lies in $(\mathrm{H}^1(K_\lambda, E)[p])^{\pm}$ and $s_\lambda \in (E(K_\lambda)/pE(K_\lambda))^{\pm}$ satisfies $\langle s_\lambda, d_\lambda \rangle$, then $s_\lambda \equiv 0 \pmod{pE(K_\lambda)}$.

Proof. Let's choose $+$ eigenspace. The proof for $-$ eigenspace is similar. Suppose $\langle s_\lambda, d_\lambda \rangle = 0$ for all $d_\lambda \in \mathrm{H}^1(K_\lambda, E)[p]^{+}$. It suffices to show that $+$ and $-$ eigenspaces are orthogonal to each other (because then we would get that $\langle s_\lambda, d_\lambda \rangle = 0$ for all d_λ in $\mathrm{H}^1(K_\lambda, E)[p]$ and conclude $s_\lambda = 0$ from the non-degeneracy of the pairing of (8.4).

Tate's pairing is Galois equivariant so it satisfies $\langle \tau(c_1), \tau(c_2) \rangle = \langle c_1, c_2 \rangle = \tau \langle c_1, c_2 \rangle$ since τ acts trivially on $\mathrm{H}^2(K_\lambda, \mu_p) \cong \mathbb{Z}/p\mathbb{Z}$ and the result follows. □

Now we shall apply the preceding considerations to classes which belong to the p-Selmer group of E, but for the proof we need to recall a result from global class field theory. Recall that for a field L the Brauer group is defined as

$$\mathrm{Br}(L) := \mathrm{H}^2(L, \bar{L}^{\times}).$$

Theorem 9.3. There exists the following short exact sequence:

$$0 \longrightarrow \mathrm{Br}(K) \longrightarrow \bigoplus_v \mathrm{Br}(K_v) \longrightarrow \frac{\mathbb{Q}}{\mathbb{Z}} \longrightarrow 0$$

where the first map is a product of restriction maps and the second one is the summation over the local invariants $\mathrm{inv}_v : \mathrm{Br}(K_v) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$ and possibly $\mathrm{inv}_\infty : \mathrm{Br}(\mathbb{R}) \xrightarrow{\sim} \frac{1}{2}\mathbb{Z}/\mathbb{Z}$.

Proposition 9.4. Assume that a class $d \in \mathrm{H}^1(K_\lambda, E)[p]^{\pm}$ is locally trivial at all places $v \neq \lambda$, but that $d_\lambda \neq 0$ in $\mathrm{H}^1(K_\lambda, E)[p]^{\pm}$. Then for any class $s \in \mathrm{Sel}^{(p)}(E/K)^{\pm} \subset \mathrm{H}^1(K_\lambda, E[p]))^{\pm}$ we have $s_\lambda = 0$ in $\mathrm{H}^1(K_\lambda, E[p]))^{\pm}$.

Proof. By the definition of p-Selmer group, the restriction $s_\lambda \in \mathrm{H}^1(K_\lambda, E[p])^{\pm}$ of s lies in $(E(K_\lambda)/pE(K_\lambda))^{\pm}$. So by lemma (9.1) we only need to check that $\langle s_\lambda, d_\lambda \rangle = 0$ to conclude the proof (since the spaces $\mathrm{H}^1(K_\lambda, E)[p]^{\pm}$ are one dimensional and $d_\lambda \not\equiv 0$, it spans the whole space and by non-degeneracy of pairing, we will be done).

To do this, lift $d \in \mathrm{H}^1(K, E)[p]$ to an element $c \in \mathrm{H}^1(K, E[p])$, which is well defined modulo $E(K)/pE(K)$. Consider the global pairing

$$\langle \cdot, \cdot \rangle_K : \mathrm{H}^1(K, E[p]) \times \mathrm{H}^1(K, E[p]) \longrightarrow \mathrm{H}^2(K, \mu_p) = \mathrm{Br}(K)[p]$$

induced by cup product and Weil pairing, which is constructed in the same way as local pairing was constructed in (8.2) (but in this case K is a number field). The image $\langle s, c\rangle_K$ lies in $\mathrm{Br}(K)[p]$. By theorem (9.3) we deduce that if we push $\langle s, c\rangle_K$ to $\mathbb{Q}/\mathbb{Z}$ we obtain zero, i.e.

$$\sum_v \mathrm{inv}_v(\langle s_v, c_v\rangle) = 0,$$

But we already know from the hypothesis that $\langle s_v, c_v\rangle = 0$ for every $v \neq \lambda$ since $d_v = 0$ in $\mathrm{H}^1(K_v, E[p])$. So this implies that $\sum_v \mathrm{inv}_v(\langle s_v, c_v\rangle) = \langle s_\lambda, c_\lambda\rangle = \langle s_\lambda, d_\lambda\rangle = 0$. □

§10. Finishing up: Computation of the Selmer Group

In this section, we shall use the cohomology classes $d = d(n) \in \mathrm{H}^1(K, E)[p]$, constructed in section (5), to bound the order of $Sel^{(p)}(E/K)$, but before we need a few more Galois cohomology computations. Call $L := K(E[p])$ and recall that we have assumed:

$$\mathcal{G} := \mathrm{Gal}(L/K) = \mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}).$$

where the equality comes from fact that K and $\mathbb{Q}(E[p])$ are linearly disjoint over $\mathbb{Q}$.

Proposition 10.1. $\mathrm{H}^n(\mathcal{G}, E[p]) = 0$ for all $n \geq 0$ and restriction induces an isomorphism:

$$\mathrm{Res} : \mathrm{H}^1(K, E[p]) \xrightarrow{\sim} \mathrm{H}^1(L, E[p])^{\mathcal{G}} = \mathrm{Hom}_{\mathcal{G}}(\mathrm{Gal}(\overline{\mathbb{Q}}/L), E[p]).$$

where the equality comes from the fact that $\mathrm{Gal}(\mathbb{Q}/L)$ acts trivially on $E[p]$.

Proof. $G \cong \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ has a central subgroup Z isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times$ which acts as homotheties on the torsion points $E[p]$. Since p is odd $Z \neq \{1\}$, so that $E_p^Z = \mathrm{H}^0(Z, E[p]) = 0$, moreover since Z has order $p-1$ which is prime to p we also have $H^i(Z, E[p]) = 0$ for all $i > 0$. We can now consider the Hochshild-Serre spectral sequence

$$\mathrm{H}^m(\mathcal{G}/Z, \mathrm{H}^n(Z, E[p])) \implies \mathrm{H}^{m+n}(\mathcal{G}, E[p])$$

to conclude that $\mathrm{H}^n(\mathcal{G}, E[p]) = 0$ for all $n \geq 0$.

On the other hand, by Inflation-Restriction exact sequence for $\mathcal{G} \trianglelefteq \mathrm{Gal}(\overline{K}/K)$, we have

$$0 \longrightarrow \mathrm{H}^1(\mathcal{G}, E[p]) \xrightarrow{\mathrm{Inf}} \mathrm{H}^1(K, E)[p] \xrightarrow{\mathrm{Res}} \mathrm{H}^1(L, E[p])^{\mathcal{G}} \longrightarrow \mathrm{H}^2(\mathcal{G}, E[p])$$

The vanishing of $\mathrm{H}^n(\mathcal{G}, E[p])$ for $n = 1, 2$ gives us the isomorphism in the proposition. □

From the last proposition we deduce that there exists a pairing: $[\cdot, \cdot] : \mathrm{H}^1(K, E[p]) \times \mathrm{Gal}(\overline{\mathbb{Q}}/L) \longrightarrow E[p]$ which satisfies for all $\sigma \in \mathcal{G}$:

$$[s, \sigma(\rho)] = \sigma([s, \rho]) \quad \text{for all } s \in \mathrm{H}^1(K, E[p]),\ \rho \in \mathrm{Gal}(\overline{\mathbb{Q}}/L)$$

Now let $S \subset \mathrm{H}^1(K, E[p])$ be a finite subgroup (=finite dimensional vector space over $\mathbb{Z}/p\mathbb{Z}$). We shall eventually apply this reasoning to $S = \mathrm{Sel}^{(p)}(E/K)$. Let

$$\mathrm{Gal}_S(\overline{\mathbb{Q}}/L) := \{\rho \in \mathrm{Gal}(\overline{\mathbb{Q}}/L) : [s, \rho] = 0 \text{ for all } s \in S\}$$

and let L^S be the fixed field of $\mathrm{Gal}_S(\overline{\mathbb{Q}}/L)$. We claim that L^S is a finite normal extension of L.

Let $s \in S$. Then by proposition 10.1 s defines a $\mathcal{G}$-module homomorphism $\mathrm{Gal}(\overline{\mathbb{Q}}/L) \longrightarrow E[p]$. Since $E[p]$ is finite, its kernel is some $\mathrm{Gal}(\overline{\mathbb{Q}}/L_s)$ where L_s/L is finite normal extension. Now take L^S to be the compositum of all fields L_s where $s \in S$. Then L^S/L is finite since S is finite and normality is clear.

Lemma 10.2. There is an induced pairing

$$[\cdot,\cdot] : S \times \mathrm{Gal}\left(L^S/L\right) \longrightarrow E_p$$

which is non-degenerate and which induces an isomorphism of $\mathcal{G} = \mathrm{Gal}(L/K)$ modules:

$$\mathrm{Gal}(L^S/L) \xrightarrow{\sim} \mathrm{Hom}_{\mathbf{Grp}}(S, E_p) = \mathrm{Hom}_{\mathbb{F}_p}(S, E_p),$$

as well as an ismorphism of $\mathrm{Gal}(K/\mathbb{Q})$-modules:

$$S \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{G}}(\mathrm{Gal}(L^S/L), E[p]).$$

Proof. We have the following injections, which follow from the definition of L^S and (10.1):

$$\mathrm{Gal}(L^S/L) \hookrightarrow \mathrm{Hom}(S, E_p) \quad \text{and} \quad S \hookrightarrow \mathrm{Hom}_{\mathcal{G}}(\mathrm{Gal}(L^S/L), E[p]). \tag{10.1}$$

In order to show that they are actually isomorphisms, let us compute their dimensions as $\mathbb{F}_p$ vector spaces. Let $r = \dim_{\mathbb{F}_p}(S)$. Then by equation (10.1), $\mathrm{Gal}(L^S/L)$ is a $\mathcal{G}$-submodule of $\mathrm{Hom}(S, E[p]) \cong E[p]^r$. Note that $E[p]$ is a simple $\mathcal{G}$-module as any proper subspace of $E[p]$ is not stable under action of $\mathcal{G} \cong \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, hence $E[p]^r$ is semi-simple. As any submodule of a semi-simple module is again semi-simple, we have an isomorphism

$$\mathrm{Gal}(L^S/L) \xrightarrow{\sim} E[p]^s \quad \text{for some } s \leq r. \tag{10.2}$$

Also it implies that

$$\mathrm{Hom}_{\mathcal{G}}(\mathrm{Gal}(L^S/L), E[p]) \cong (\mathbb{Z}/p\mathbb{Z})^s \quad \text{as } \mathrm{Hom}_{\mathcal{G}}(E[p], E[p]) \cong (\mathbb{Z}/p\mathbb{Z}))$$

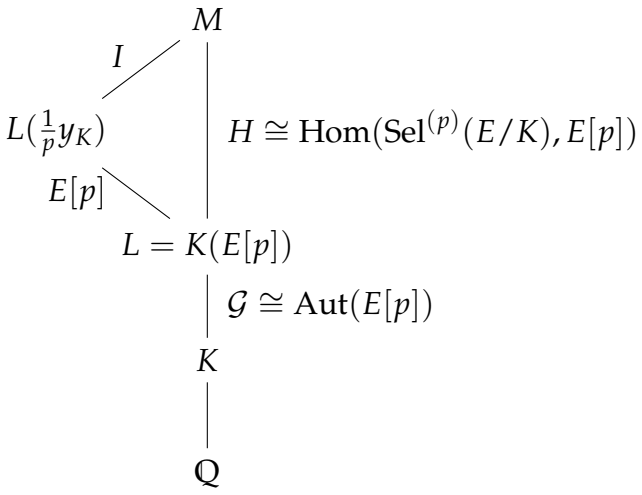
(Since $\mathcal{G} \cong \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) = \mathrm{Aut}(E[p])$, the only automorphisms of $\mathcal{G}$ which commutes with all the other elements of $\mathcal{G}$ are those which corresponds to scalar matrices).

This group contains $S \cong (\mathbb{Z}/p\mathbb{Z})^r$ by (10.2), so we must have $s \geq r$ which implies $s = r$. □

Recall from ([Sil86], Theorem X.4.2) that for any elliptic curve E/K, $\mathrm{Sel}^{(p)}(E/K)$ is finite. Now we would like to apply lemma (10.2) to $S = \mathrm{Sel}^{(p)}(E/K) \subset \mathrm{H}^1(K, E[p])$.

For simplicity of notation let $M = L^S$ and $H = \mathrm{Gal}(M/L) = \mathrm{Gal}(L^S/L)$. Since we eventually want to get to the proof of proposition (2.3), let $yK \in E(K)$ (defined in equation 3.3), have infinite order and let it not be divisible by p in $E(K)/E(K)_{tors}$, $\delta y_K \in \mathrm{Sel}^{(p)}(E/K)$ is its non-zero image inside the p-Selmer group.

Let I be the subgroup of H which fixes the subfield $L(\frac{1}{p}y_K)$. We have the following:



In this diagram, first of all note that $L(\frac{1}{p}y_K)$ is independent of choice of $\frac{1}{p}y_K$ and $\mathrm{Gal}(L(\frac{1}{p}y_K)/L) \cong E[p]$ because all the Galois conjugates of $\frac{1}{p}y_K$ are $\frac{1}{p}y_K + P$ for $P \in E[p]$. Also since we have taken $M = L^S$ where $S = \mathrm{Sel}^{(p)}(E/K)$ which contains image of $E(K)/pE(K)$ under Kummer map, it follows that M contains $\frac{1}{p}P$ for every $P \in E(K)$. In particular $L(\frac{1}{p}y_K) \subset M$.

Let τ be a fixed lifting of complex conjugation in $\mathrm{Gal}(M/\mathbb{Q})$ and let H^+ and I^+ denote the $+1$ eigenspaces for τ (acting by conjugation) in H and I.

Lemma 10.3. $H^+ = \{(\tau h)^2 : h \in H\}$, $I^+ = \{(\tau i)^2 : i \in I\}$, and $H^+/I^+ \cong \mathbb{Z}/p\mathbb{Z}$.

Proof. Let us define $H^{\tau+1} := \{(\tau \cdot h)h : h \in H\}$. Then clearly $H^{\tau+1} \subset H^+$ because

$$\tau \cdot ((\tau \cdot h)h) = \tau\tau h\tau^{-1}h\tau^{-1} = h(\tau h\tau^{-1}) = (\tau h\tau^{-1})h = (\tau \cdot h)h$$

Since action of τ is a linear map on $\mathbb{Z}/p\mathbb{Z}$ vector space H, H^+ is a subspace. Also since p is odd, 2 is an automorphism of H (and of H^+). Hence for any $h \in H^+$, $h^{1/2} \in H^+$. Now, $(\tau \cdot h^{1/2})h^{1/2} = h^{1/2}h^{1/2} = h$ so that $h \in H^{\tau+1}$. Then we have

$$H^+ = H^{\tau+1} = \{(\tau h)^2 : h \in H\}, \quad \text{since } \tau^{-1} = \tau$$

The same reasoning works for I^+. Finally $H^+/I^+ = (H/I)^+ = E[p]^+ \cong \mathbb{Z}/p\mathbb{Z}$. □

Proposition 10.4. Let $s \in \mathrm{Sel}^{(p)}(E/K)^{\pm}$. Then the following are equivalent:

(a) $[s, \rho] = 0$ for all $\rho \in H$,

(b) $[s, \rho] = 0$ for all $\rho \in H^+$,

(c) $[s, \rho] = 0$ for all $\rho \in H^+ - I^+$,

(d) $s = 0$.

Proof. Clearly $(d) \iff (a)$ by lemma 10.2 and clearly $(a) \implies (b) \implies (c)$. So it sufficies to prove that $(c) \implies (a)$.

$(c) \implies (a)$ First suppose that $s \in \mathrm{Sel}_{(p)}(E/K)^+$. By 10.2, s defines a $\mathcal{G}$-homomorphism $\varphi_s : H^+ \longrightarrow E[p]^+$. Let us assume that s vanishes on $H^+ - I^+$. This implies that it vanishes on the entire group H^+ (using the fact that $H^+/I^+ \cong \mathbb{Z}/p\mathbb{Z}$ from lemma 10.3). Also $s \in \mathrm{Sel}^{(p)}(E/K)$ so it induces a $\mathcal{G}$-homomorphism $\tilde{\varphi}_s : H \longrightarrow E[p]$ by (10.2), which maps $H^+ \longrightarrow E[p]^+$ and $H^- \longrightarrow E[p]^-$. If s vanishes on H^+, then $\tilde{\varphi}_s(H) \subset E[p]^-$, but $\tilde{\varphi}_s(H)$ is a $\mathcal{G}$-submodule of the simple $\mathcal{G}$-module $E[p]$, so if $\tilde{\varphi}_s(H) \neq E[p]$ we must have $\tilde{\varphi}_s(H) = 0$, which implies (a). The same reasoning is valid for $s \in \mathrm{Sel}_p(E/K)^-$ with $+$ and $-$ reversed. □

Remark 10.5. The same proof will show that the following statements are equivalent:

(a) $[s, \rho] = 0$ for all $\rho \in I$,

(b) $[s, \rho] = 0$ for all $\rho \in I^+$.

Now let λ be a prime of K which does not divide $N \cdot p$. Then λ is unramified in M/K; we assume further that λ splits completely in L/K and let λ_M be a prime of M above λ. Let Fr_{λ_M} (or $\mathrm{Fr}_{\lambda_M/\lambda}$) be the Frobenius element of λ_M in $\mathrm{Gal}(M/K)$. Because λ splits completely in L Fr_{λ_M} fixes L. i.e.,$\mathrm{Fr}_{\lambda_M} \in H = \mathrm{Gal}(M/L) \cong \mathrm{Hom}(\mathrm{Sel}^{(p)}(E/K), E[p])$. Let

$$\mathrm{Frob}(\lambda) := \{\sigma \cdot \mathrm{Fr}_{\lambda_M} : \sigma \in \mathcal{G}\}$$

$\mathcal{G}$-orbit of λ_M where $\mathcal{G}$ acts on H by conjugation (see notation on page 1). Because $\mathcal{G}$ is abelian $\mathrm{Frob}(\lambda)$ depends only on λ. By definition we will write $[s, \mathrm{Frob}(\lambda)] = 0$ if and only if $[s, \rho] = 0$ for every $\rho \in \mathrm{Frob}(\lambda)$.

Proposition 10.6. For $s \in \mathrm{Sel}^{(p)}(E/K) \subset \mathrm{H}^1(K, E[p])$ the following are equivalent:

(a) $[s, \mathrm{Fr}_{\lambda_M/\lambda}] = 0$.

(b) $[s, \mathrm{Frob}(\lambda)] = 0$.

(c) $s_\lambda = 0$ in $\mathrm{H}^1(K_\lambda, E[p])$.

Proof. $((a) \iff (b))$ This is because pairing in lemma 10.2 satisfies: for all $\sigma \in \mathcal{G}$

$$[s, \sigma(\rho)] = \sigma([s, \rho]) \quad \text{for all } s \in \mathrm{H}^1(K, E[p]),\ \rho \in \mathrm{Gal}(\overline{\mathbb{Q}}/L)$$

$((a) \iff (c))$ Let $P_\lambda \in E(K_\lambda)/pE(K_\lambda)$ be the element whose image is $s_\lambda \in \mathrm{Sel}^{(p)}(E/K)$ through the Kummer map. By definition of M, $\frac{1}{p}P_\lambda \in E(M_{\lambda_M})$ and

$$[s, \mathrm{Fr}_{\lambda_M/\lambda}] = \mathrm{Fr}_{\lambda_M/\lambda}\left(\frac{1}{p}P_\lambda\right) - \left(\frac{1}{p}P_\lambda\right) \quad \text{in } E(M_{\lambda_M})$$

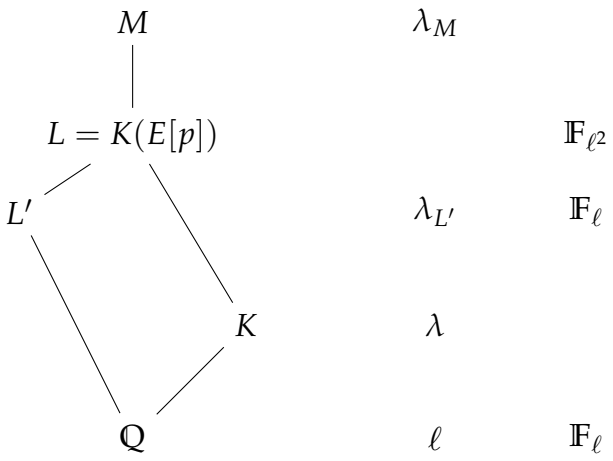
Hence $[s, \mathrm{Fr}_{\lambda_M/\lambda}] = 0 \iff \frac{1}{p}P_\lambda \in E(K_\lambda) \iff P_\lambda \in pE(K_\lambda) \iff$ condition (c) holds. □

We now finally turn to the proof of proposition (1.7). Recall that the Heegner point $y_K = P_1$ lies in the ϵ-eigenspace for complex conjugation on $E(K)/pE(K)$, where $-\epsilon$ is the sign of $L(E/K, s)$. Hence $\delta(y_K) \in \mathrm{Sel}^{(p)}(E/K)^{\epsilon}$.

Lemma 10.7. $\mathrm{Sel}^{(p)}(E/K)^{-\epsilon} = 0$.

Proof. Let $s \in \mathrm{Sel}^{(p)}(E/K)^{-\epsilon}$. To show that $s = 0$, by remark 10.5 it suffices to show that $[s, \rho] = 0$ for every $\rho \in H^+ - I^+$. By lemma (10.3) an element of H^+ is of the form $(\tau h)^2$ for some $h \in H$.

Let ℓ be a prime which is unramified in the extension $M/\mathbb{Q}$ and such that there is a factor λ_M above it in M, whose Frobenius element $\mathrm{Fr}_{\lambda_M/\lambda}$ equals τh in $\mathrm{Gal}(M/\mathbb{Q})$. The density of such primes is positive by Chebotarev density theorem and so we can always find a prime satisfying that condition. **Claim:** $\lambda = \ell\mathcal{O}_K$ is inert in K and λ splits completely in L.



In above figure L' is the field fixed by τh. It is the maximal totally real field contained in L. Since L' and K are linearly disjoint over $\mathbb{Q}$ and $\lambda_{L'}$ is inert in L, we have that $\mathbb{F}_\lambda = \mathbb{F}_{\ell^2}$ i.e., λ is inert in K. Also because ℓ splits completely in $L'/\mathbb{Q}$, λ splits completely in L.

The Frobenius substitution $\mathrm{Fr}_{\lambda_M/\lambda} = \mathrm{Fr}^2_{\lambda_M/\ell} = (\tau h)^2$, so to prove that $[s, \rho] = [s, \mathrm{Fr}_{\lambda_M/\lambda}] = 0$ if suffices to show that $s_\lambda \equiv 0$ in $\mathrm{H}^1(K_\lambda, E[p])$ by proposition (10.6). Let $c(\ell) \in \mathrm{H}^1(K, E[p])$ and $d(\ell) \in \mathrm{H}^1(K, E)[p]$ be the cohomology classes constructed in section 5. By proposition (6.2) both classes lie in the $-\epsilon$ eigenspace of τ and by proposition 7.2 $d(\ell)$ is locally trivial except possibly at λ. **Claim:** $d(\ell)_\lambda \neq 0$ in $\mathrm{H}^1(K, E)[p]$.

By proposition (7.3) $d(\ell)_\lambda = 0 \iff y_K = P_1 \in pE(K_\lambda) \iff$ the prime λ splits completely in the extension $L(\frac{1}{p}y_K)$. Since $\mathrm{Fr}_{\lambda_M/\lambda} = \rho$ is not in $I^+ = I \cap H^+$ by hypothesis, this splitting does not occur.

So we can apply proposition (9.4) to deduce that $s \in \mathrm{Sel}^{(p)}(E/K)^{-\epsilon}$ is such that $s = 0$. □

Now we put together some results (most of which we have already proved) for our convenience to use it in proposition (10.9).

Proposition 10.8. Assume that y_K (defined in (3.3)) is not divisible by p in $E(K)/E(K)_{tors}$. Let ℓ be a prime which is unramified in the extension $M/\mathbb{Q}$ and such that there is a factor λ_M above it in M, whose Frobenius element equals τh in $\mathrm{Gal}(M/\mathbb{Q})$, for some $h \in H$. Then $\lambda = \ell\mathcal{O}_K$ is inert in K and λ splits completely in $L = K(E[p])$. The following are equivalent:

(a) $c(\ell) \equiv 0$ in $\mathrm{H}^1(K, E[p])$,

(b) $c(\ell) \in \mathrm{Sel}^{(p)}(E/K) \subset \mathrm{H}^1(K, E[p])$,

(c) P_ℓ is divisible by p in $E(H_\ell)$,

(d) $d(\ell) \equiv 0$ in $\mathrm{H}^1(K, E)[p]$,

(e) $d(\ell)_\lambda \equiv 0$ in $\mathrm{H}^1(K_\lambda, E)[p]$,

(f) $P_1 = y_K$ is locally divisible by p in $E(K_\lambda)$,

(g) $(\tau h)^2$ lies in the subgroup $I^+ = H^+ \cap I$ of H^+.

Proof. $((a) \iff (b))$ By proposition 6.2 $c(\ell) \in \mathrm{H}^1(K, E[p])^{-\epsilon}$ and $\mathrm{Sel}^{(p)}(E/K)^{-\epsilon} = 0$ by lemma 10.7.

$((a) \iff (c))$ This is just a special case of proposition (5.12(a)).

$((a) \iff (d))$ Follows from proposition (5.12(b)) and the fact that $(E(K)/pE(K))^{-\epsilon} = 0$ because it injects in $\mathrm{Sel}^{(p)}(E/K)^{-\epsilon}$.

$((d) \iff (e))$ Since $d(\ell)$ is locally trivial except perhaps at λ (by proposition 7.2). So if $d(\ell)_\lambda$ is trivial then $d(\ell) \in \mathrm{Sel}^{(p)}(E/K)^{-\epsilon}$ which is 0 by lemma (10.7).

$((e) \iff (f))$ This follows immediately from proposition 7.3.

$((f) \iff (g))$ $\frac{1}{p}y_K \in E(K_\lambda) \iff \lambda$ splits completely in $L(\frac{1}{p}y_K)/K \iff$ Frobenius element $\mathrm{Fr}_{\lambda_M/\lambda}$ fixes $L(\frac{1}{p}y_K) \iff \mathrm{Fr}_{\lambda_M/\lambda} = \mathrm{Fr}^2_{\lambda_M/\ell} = (\tau h)^2$ is actually in I. □

Now we are ready to prove proposition 1.7. In view of lemma 10.7 we only need to prove:

Proposition 10.9. $\mathrm{Sel}^{(p)}(E/K)^\epsilon \cong \mathbb{Z}/p\mathbb{Z} \cdot \delta y_K$.

Proof. Let $s \in \mathrm{Sel}^{(p)}(E/K)^\epsilon$. To show that s is a multiple of δy_K it suffices to show that $[s, \rho] = 0$ for all $\rho \in I$, for then

$$s \in \mathrm{Hom}_{\mathcal{G}}(H/I, E[p]) = \mathrm{Hom}_{\mathcal{G}}(E[p], E[p]) \cong \mathbb{Z}/p\mathbb{Z} \cdot \delta y_K$$

since $E[p]$ is a simple $\mathcal{G}$-module. By remark 10.5 it is enough to show that $[s, \rho] = 0$ for all $\rho \in I^+$. By lemma 10.3 these elements have the form $\rho = (\tau i)^2$ for some $i \in I$.

Let ℓ' be a prime such that $c(\ell')$ is non-trivial in $\mathrm{H}^1(K, E[p])$. By proposition (10.8 (g)) we may obtain such an ℓ' by imposing the condition that its Frobenius substitution is conjugate to $\tau h \in \mathrm{Gal}(M/\mathbb{Q})$, where $h \in H$ and $(\tau h)^2 \notin I^+$. Then $c(\ell')$ is not in $\mathrm{Sel}^{(p)}(E/K)$ by (10.8

(b)). Let $L' = L^S$ be the extension constructed for $S = \langle c(\ell') \rangle$ as in lemma (10.2). It is easy to see that if $P' \in E(\overline{K})$ is the element such that $\delta(P') = c(\ell')$, then $L' = L(\frac{1}{p}P')$. Also $\mathrm{Gal}(L'/L) \cong E[p]$ and L'/L is disjoint from the extension M/L. A prime ideal $\ell\mathcal{O}_K = \lambda$ in K, which splits completely in L, is split completely in L' if and only if $L'_{\lambda_{\ell'}} = K_\lambda$ for every prime $\lambda_{\ell'}$ lying above λ in L'.

Now let ℓ be a prime whose Frobenius substitution is conjugate to τi in $\mathrm{Gal}(M/Q)$ for some $i \in I$, and to τj in $\mathrm{Gal}(L'/\mathbb{Q})$ for some $j \in \mathrm{Gal}(L'/L)$ satisfying $(\tau j)^2 \neq 1$. These conditions can be satisfied simultaneously because M and L' are linearly disjoint over L.

Claim: The class $d(\ell\ell') \in \mathrm{H}^1(K, E)$ is locally trivial for all places $v \neq \lambda$, but that $d(\ell\ell')_\lambda \neq 0$.

Let $\lambda' = \ell'\mathcal{O}_K$ then local triviality at primes $v \neq \lambda, \lambda'$ comes from proposition (7.2). Since $i \in I$, the global class $c(\ell)$ is zero by proposition (10.8(a)), and so by condition 10.8(c), P_ℓ is divisible by p in $E(H_\ell)$. Hence it follows directly from proposition (7.3) that $d(\ell\ell')_{\lambda'} = 0$. Again by proposition 7.3 $d(\ell\ell')_\lambda$ is trivial if and only if $P_{\ell'}$ is locally divisible by p in $E(K_\lambda)$. But this implies that λ splits completely in L', or equivalently that $(\tau j)^2 = 1$ which contradicts the hypothesis on j.

So $d(\ell\ell')$ satisfies the hypothesis of proposition (9.4) and using it we conclude that $s_\lambda = 0$. By proposition 10.6, we get that

$$[s, \rho] = [s, (\tau i)^2] = 0.$$

Since this process can be done for any $\rho \in I^+$ we have shown that $s(I^+) = s(I) = 0$. □

References

[Cox03] David Cox. *primes of the form $x^2 + ny^2$*. Wiley, 2003.

[Cus] *Cusps and Rational Points*. URL: https://www.math.uzh.ch/sepp/magma-2.25.2-ds/html/text1580.htm.

[Dar04] Henri Darmon. *Rational points on modular elliptic curves*. 101. American Mathematical Soc., 2004.

[DS05] Fred Diamond and Jerry Shurman. *A First Course in Modular Forms*. Springer, GTM 228, 2005.

[Gro84] B Gross. *Heegner points on $X_0(N)$*. 1984.

[GZ86] Benedict Gross and Don Zagier. *Heegner Points and Derivatives of L-Series*. Springer, 1986.

[Gro91] Benedict H Gross. "Kolyvagin's work on modular elliptic curves". In: *L-functions and arithmetic (Durham, 1989)* 153 (1991), pp. 235–256.

[KL89] Victor A Kolyvagin and Dmitry Yu Logachëv. "Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties". In: *Algebra i Analiz* 1.5 (1989), pp. 171–196.

[Sil86] Joseph Silverman. *Arithmetic of Elliptic Curves*. Springer, GTM, 1986.

[Sil03] Joseph Silverman. *Advanced Topics in Arithmetic of Elliptic Curves*. Springer, GTM, 2003.

[Was89] L Washington. "Number fields and elliptic curves". In: *Number theory and applications*. 1989, pp. 245–278.