Title
Strong Selmer Companion Elliptic Curves

Author
Chiu, Ching-Heng

Publication Date
2019

Peer reviewed|Thesis/dissertation

UNIVERSITY OF CALIFORNIA,
IRVINE

Strong Selmer Companion Elliptic Curves

DISSERTATION

submitted in partial satisfaction of the requirements
for the degree of

DOCTOR OF PHILOSOPHY

in Mathematics

by

Ching-Heng Chiu

Dissertation Committee:
Professor Karl Rubin, Chair
Professor Daqing Wan
Professor Nathan Kaplan

2019

TABLE OF CONTENTS

ACKNOWLEDGMENTS

First, I would like to express my sincere gratitude to my advisor Professor Rubin for the continuous support of my Ph.D. study and related research, for his patience, motivation, and immense knowledge. His guidance helped me during all the time of research and writing of this thesis. I could not have imagined having a better advisor and mentor for my Ph.D. study.

Besides my advisor, I would like to thank the rest of my thesis committee: Professor Wan and Professor Kaplan, for their insightful comments and encouragement, but also for the hard question which incited me to widen my research from various perspectives.

Last but not the least, I would like to thank my family: my parents for supporting me spiritually throughout writing this thesis and my life in general.

CURRICULUM VITAE

Ching-Heng Chiu

EDUCATION

Doctor of Philosophy in Mathematics **2019**
University of California, Irvine *Irvine, California*

Master of Science in Mathematics **2012**
National Taiwan University *Taipei, Taiwan*

Bachelor of Science in Mathematics **2010**
National Taiwan University *Taipei, Taiwan*

TEACHING EXPERIENCE

Teaching Assistant **2015–2019**
University of California, Irvine *Irvine, California*

ABSTRACT OF THE DISSERTATION

Strong Selmer Companion Elliptic Curves

By

Ching-Heng Chiu

Doctor of Philosophy in Mathematics

University of California, Irvine, 2019

Professor Karl Rubin, Chair

Let E_1, and E_2 be elliptic curves defined over a number field K. Suppose that for all but finitely many primes ℓ, and for all finite extension fields L/K,

$$\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(L, E_1) = \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(L, E_2).$$

We prove that E_1 and E_2 are isogenous over K.

Chapter 1

Introduction, preliminaries and results

1.1 INTRODUCTION

Yuri Zarhin posed the following question (see (**PZ**)):

Suppose that X_1 and X_2 are abelian varieties defined and isogenous over a number field K. Then for any finite extension field L/K,

$$\mathrm{rank}_{\mathbb{Z}}(X_1(L)) = \mathrm{rank}_{\mathbb{Z}}(X_2(L)).$$

Zarhin's question is whether the converse holds: Let X_1 and X_2 be abelian varieties defined over K. If $\mathrm{rank}_{\mathbb{Z}}(X_1(L)) = \mathrm{rank}_{\mathbb{Z}}(X_2(L))$ for every finite extension L/K, then are X_1 and X_2 isogenous over K?

Hershy Kisilevsky proved the following two analogous statements in (**Ki**):

Theorem 1.1.1. *Suppose that E_1 and E_2 are elliptic curves defined over $\mathbb{Q}$ such that*

$$\mathrm{ord}_{s=1} L(E_1/K, s) \equiv \mathrm{ord}_{s=1} L(E_2/K, s) \pmod 2$$

for all extensions $K/\mathbb{Q}$ with $[K : \mathbb{Q}] \leq 2$, then $N(E_1)$ and $N(E_2)$ are equal up to square factors (where $N(E)$ is the conductor of E).

Proof. This is Corollary 1. in (**Ki**). □

Theorem 1.1.2. *Suppose that E_1 and E_2 are elliptic curves defined over $\mathbb{Q}$ such that*

$$\mathrm{rank}_{\mathbb{Z}} E_1(K) \equiv \mathrm{rank}_{\mathbb{Z}} E_2(K) \pmod 2$$

for all extensions $K/\mathbb{Q}$ with $[K : \mathbb{Q}] \leq 2$ and suppose that the 2-primary part of their Tate-Shafarevich groups are finite for all such K, then $N(E_1)$ and $N(E_2)$ are equal up to square factors.

Proof. This is Corollary 2. in (**Ki**). □

Definition 1.1.3. Let E_1, and E_2 be elliptic curves defined over a number field K. If for all but finitely many primes ℓ, and for all finite extension fields L/K,

$$\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(L, E_1) = \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(L, E_2),$$

we say that E_1 and E_2 are *Strong Selmer Companions (SSC) over K.*

Remark 1.1.4. For definition of $\mathrm{Sel}_\ell(K, E)$, see Definition 1.4.1.

Remark 1.1.5. Let L be a finite extension of K. If E_1 and E_2 are SSC over K, then they are SSC over L. In other words, if E_1 and E_2 are not SSC over L, then they are not SSC over K.

Proposition 1.1.6. *Let E_1 and E_2 be elliptic curves defined over a number field K. If E_1 and E_2 are isogenous over K, then E_1 and E_2 are Strong Selmer Companions over K.*

Proof. Assume that E_1 is isogenous to E_2 over K. Let $\varphi : E_1 \to E_2$ be an isogeny and $\hat{\varphi}$ be its dual isogeny. Let $d := \deg \varphi$. Let ℓ be a prime which is coprime to d and L be a finite extension over K. Let φ' and $\hat{\varphi}'$ be the induced map of φ and $\hat{\varphi}$ on the Selmer group. Since $\hat{\varphi}' \circ \varphi'$ is the multiplication-by-d map, it is an isomorphism

$$\hat{\varphi}' \circ \varphi' : \mathrm{Sel}_\ell(L, E_1) \xrightarrow{\varphi'} \mathrm{Sel}_\ell(L, E_2) \xrightarrow{\hat{\varphi}'} \mathrm{Sel}_\ell(L, E_1).$$

Therefore, φ' is injective and we have

$$\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(L, E_1) \leq \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(L, E_2).$$

Similarly, if we consider $\varphi' \circ \hat{\varphi}'$, then we have

$$\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(L, E_2) \leq \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(L, E_1).$$

Hence,

$$\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(L, E_2) = \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(L, E_1)$$

for all ℓ coprime to d and all finite extensions L/K. So, E_1 and E_2 are Strong Selmer Companions over K. $\square$

Definition 1.1.7. Let E be an elliptic curve defined over a number field K. We say that *E has complex multiplication (CM) over K* if $\mathrm{End}_K \neq \mathbb{Z}$. We say that *$E$ has CM* if E has CM over $\bar{K}$. Otherwise, we say that *E has no complex multiplication.* In the case that E has CM, we say that *E has CM by M* if $\mathrm{End}_{\bar{K}}(E) \otimes \mathbb{Q} = M$ where $M \neq \mathbb{Q}$ in which case M is an imaginary quadratic field, and we say that *E has CM by $\mathcal{O}_M$ (the full ring of integers of M)* if $\mathrm{End}_{\bar{K}}(E) = \mathcal{O}_M$.

The main result of this paper is the following theorem. It is an analogous statement of Zarhin's question.

Theorem 1.1.8. *Let E_1 and E_2 be elliptic curves defined over a number field K. Then E_1 and E_2 are isogenous over K if and only if E_1 and E_2 are Strong Selmer Companions over K.*

The 'only if' direction is Proposition 1.1.6. We will prove the 'if' direction by discussing the following cases:

(1) E_1 and E_2 are elliptic curves defined over K without complex multiplication.

(2) E_2 has complex multiplication.

We will prove Theorem 1.1.8 in §4.1.

1.2 TWISTS OF ELLIPTIC CURVES

Let E be an elliptic curve defined over an arbitrary field K of characteristic 0 (in practice K will be a number field or one of its completions). Fix a rational prime ℓ.

Fix a cyclic extension L/K of degree ℓ. Let $G := \mathrm{Gal}(L/K)$.

Definition 1.2.1. Define an ideal $\mathcal{I}_L \subset \mathbb{Z}[G]$ by $\mathcal{I}_L := \ker(\mathbb{Z}[G] \to \mathbb{Z})$ where the map $\mathbb{Z}[G] \to \mathbb{Z}$ sends elements in G to 1.

Then $\mathrm{rank}_{\mathbb{Z}}(\mathcal{I}_L) = \ell - 1$, and we define the *$L/K$-twist* E_L of E to be the abelian variety $\mathcal{I}_L \otimes E$ of dimension $(\ell - 1)$ as defined in (**MRS**). Concretely,

$$E_L := \ker(\mathrm{Res}_K^L E \to E).$$

Here $\mathrm{Res}_K^L E$ denotes the Weil restriction of scalars of E from L to K.

See (**MRS**) for a discussion of E_L and its properties.

Definition 1.2.2. With notation as above, let $\mathbf{N}_{L/K} := \sum_{\sigma \in \mathrm{Gal}(L/K)} \sigma \in \mathbb{Z}[G]$, and define

$$R_L := \mathbb{Z}[G]/\mathbf{N}_{L/K}\mathbb{Z}[G]$$

so $\mathrm{rank}_{\mathbb{Z}} R_L = \ell - 1$.

Fixing an identification $G \xrightarrow{\sim} \boldsymbol{\mu}_\ell$ of G with the group of ℓ-th roots of unity in $\bar{\mathbb{Q}}$ induces an isomorphism

$$R_L \cong \mathbb{Z}[\boldsymbol{\mu}_\ell]$$

that identifies R_L with a maximal order in $\mathbb{Q}(\boldsymbol{\mu}_\ell)$. We have that ℓ is totally ramified in $\mathbb{Q}(\boldsymbol{\mu}_\ell)/\mathbb{Q}$, and we let λ_L denote the (unique) prime of R_L above ℓ.

Proposition 1.2.3. *(i) The natural action of G on $\mathrm{Res}_K^L(E)$ induces an inclusion $R_L \subset \mathrm{End}_K(E_L)$.*

(ii) For every $m \in \mathbb{Z}$, there is a natural isomorphism of $R_L[G_K]$-modules

$$E_L[m] \cong \mathcal{I}_L \otimes_{\mathbb{Z}} E[m].$$

Proof. This is Proposition 6.3. in (**MRL**). □

Corollary 1.2.4. *The isomorphism of Proposition 1.2.3(ii) induces an isomorphism of $\mathrm{End}_K(E)[G_K]$- modules*

$$E_L[\lambda_L] \cong E[\ell].$$

Proof. This is Corollary 6.4. in (**MRL**). □

1.3 LOCAL FIELDS AND LOCAL CONDITIONS

In this section we use the twists E_L to define the local conditions that will be used to define our relative Selmer groups $\mathrm{Sel}_\ell(L/K, E)$.

For this section we restrict to the case where K is a local field of characteristic zero, i.e., a finite extension of some $\mathbb{Q}_p$ or of $\mathbb{R}$. Fix for this section a prime ℓ a cyclic extension L/K of degree 1 or ℓ, and let $G := \mathrm{Gal}(L/K)$.

Definition 1.3.1. Define $\mathcal{H}_\ell(L/K) \subset H^1(K, E[\ell])$ to be the image of the composition

$$E_L(K)/\lambda_L E_L(K) \hookrightarrow H^1(K, E_L[\lambda_L]) \cong H^1(K, E[\ell]),$$

where the first map is the Kummer map, and the second map is the isomorphism of Corollary 1.2.4. (This Kummer map depends on the choice of a generator of λ_L/λ_L^2, but its image is independent of this choice.) When $L = K$, $\mathcal{H}_\ell(K/K)$ is just the image of the Kummer map

$$E(K)/\ell E(K) \hookrightarrow H^1(K, E[\ell]),$$

and we will denote it simply by $\mathcal{H}_\ell(K)$. We suppress the dependence on E from the notaion when possible, since E is fixed throughout §1.3 and §1.4.

If K is nonarchimedean of characteristic different from ℓ, and E/K has good reduction, we define

$$H^1_{\mathrm{ur}}(K, E[\ell]) := H^1(K^{\mathrm{ur}}/K, E[\ell]),$$

the unramified subgroup of $H^1(K, E[\ell])$.

Remark 1.3.2. If E has good reduction, and L/K is a ramified cyclic extension of degree ℓ, then $\mathcal{H}_\ell(L/K)$ is the "$L-$transverse" subgroup of $H^1(K, E[\ell])$, as defined in Definition 1.1.6 of (**MR2**).

Lemma 1.3.3. *Suppose K is nonarchimedean of residue characteristic different from ℓ.*

(i) We have $\dim_{\mathbb{F}_\ell}(\mathcal{H}_\ell(L/K)) = \dim_{\mathbb{F}_\ell} E(K)[\ell]$.

(ii) If E has good reduction and $\phi \in G_K$ is an automorphism that restricts to Frobenius in $\mathrm{Gal}(K^{\mathrm{ur}}/K)$, *then*

$$\dim_{\mathbb{F}_\ell}(\mathcal{H}_\ell(L/K)) = \dim_{\mathbb{F}_\ell} E[\ell]/(\phi - 1)E[\ell].$$

Proof. This is Lemma 7.2. in (**MRL**). □

Lemma 1.3.4. *Suppose K is nonarchimedean of residue characteristic different from ℓ, E/K has good reduction, and L/K is unramified.*

(i) If $\phi \in G_K$ is an automorphism that restricts to Frobenius in $\mathrm{Gal}(K^{\mathrm{ur}}/K)$, *then evaluation of cocycles at ϕ induces an isomorphism*

$$H^1_{\mathrm{ur}}(K, E[\ell]) \xrightarrow{\sim} E[\ell]/(\phi - 1)E[\ell].$$

(ii) The twist E_L has good reduction, and $\mathcal{H}_\ell(L/K) = H^1_{\mathrm{ur}}(K, E[\ell])$. In particular under these assumptions $\mathcal{H}_\ell(L/K)$ is independent of L.

Proof. This is Lemma 7.3. in (**MRL**). □

Proposition 1.3.5. *Suppose E/K has good reduction, K is nonarchimedean of residue characteristic different from ℓ, and L/K is ramified. Then*

$$H^1_{\mathrm{ur}}(K, E[\ell]) \cap \mathcal{H}_\ell(L/K) = 0.$$

Proof. This is Proposition 7.8. in (**MRL**). □

1.4 SELMER GROUPS AND SELMER STRUCTURES

In this section, let ℓ be a fixed prime. We define the relative Selmer groups $\mathrm{Sel}_\ell(L/K, E)$.

Now we assume that K is a number field and L be as in §1.3. If v is a place of K, we will denote by K_v the completion of K at v and denote by L_v the completion of L at some fixed place above v.

Definition 1.4.1. If L/K is a cyclic extension of degree 1 or ℓ, we define the ℓ-Selmer group $\mathrm{Sel}_\ell(L/K, E) \subset H^1(K, E[\ell])$ by

$$\mathrm{Sel}_\ell(L/K, E) := \{c \in H^1(K, E[\ell]) : \mathrm{loc}_v(c) \in \mathcal{H}_\ell(L_v/K_v) \text{ for every } v\}.$$

Here $\mathrm{loc}_v : H^1(K, E[\ell]) \to H^1(K_v, E[\ell])$ is the localization map. When $L = K$ this is the standard ℓ-Selmer group of E/K, and we denote it by $\mathrm{Sel}_\ell(K, E)$.

Lemma 1.4.2. *The isomorphism of Proposition 1.2.3(iii) identifies* $\mathrm{Sel}_\ell(L/K, E)$ *with the classical* λ_L*-Selmer group of* E_L*.*

Proof. This is Lemma 8.4. in (**MRL**). □

Definition 1.4.3. From now on let $\Sigma_{\ell,E}$ be a finite set of places of K containing all places where E has bad reduction, all places dividing $\ell\infty$, and large enough so that the primes in Σ generate the ideal class group of K. If ℓ and E are fixed, we write Σ instead of $\Sigma_{\ell,E}$. (If we have two curves E_1 and E_2, we assume in addition that Σ contains all places where E_1 or E_2 has bad reduction.) Define

$$\mathcal{O}_{K,\Sigma} := \{x \in K : x \in \mathcal{O}_{K_v} \text{ for every } v \notin \Sigma\},$$

the ring of Σ-integers of K. Define sets of primes $\mathcal{P}(\Sigma) \subset \mathcal{Q}(\Sigma)$ by

$$\mathcal{Q}(\Sigma) := \{\mathfrak{p} \notin \Sigma : \mathbf{N}\mathfrak{p} \equiv 1 \pmod{\ell}\}$$

$$\mathcal{P}(\Sigma) := \{\mathfrak{p} \in \mathcal{Q}(\Sigma) : \text{the inclusion } K^\times \hookrightarrow K_\mathfrak{p}^\times \text{ sends } \mathcal{O}_{K,\Sigma}^\times \text{ into } (\mathcal{O}_{K_\mathfrak{p}}^\times)^\ell\}.$$

If Σ is fixed, we omit it and simply write $\mathcal{P}$ and $\mathcal{Q}$. Define partitions of $\mathcal{P}, \mathcal{Q}$ into disjoint subsets $\mathcal{P}_i(E), \mathcal{Q}_i(E)$ for $i \geq 0$ by

$$\mathcal{Q}_i(E) := \{\mathfrak{p} \in \mathcal{Q} : \dim_{\mathbb{F}_\ell} H^1_{\mathrm{ur}}(K_\mathfrak{p}, E[\ell]) = i\}, \quad \mathcal{P}_i(E) := \mathcal{Q}_i(E) \cap \mathcal{P}.$$

Theorem 1.4.4. *For every prime v of K, Tate's local duality gives a perfect symmetric pairing*

$$< \, , \, >_v \colon H^1(K_v, E[\ell]) \times H^1(K_v, E[\ell]) \to H^2(K_v, \boldsymbol{\mu}_\ell) = \mathbb{F}_\ell.$$

Proof. See (**T**). □

Theorem 1.4.5. *Let M_K be a complete set of primes of $\mathcal{O}_K$. Let $c, d \in H^1(K, E[\ell])$. Then*

$$\sum_{v \in M_K} < \mathrm{loc}_v(c), \mathrm{loc}_v(d) >_v = 0.$$

Proof. Apply Theorem B in section 10 of Chapter VII in (**CF**) to the cup product $c \cup d \in H^2(K, \boldsymbol{\mu}_\ell) = \mathrm{Br}(K)[\ell]$.

□

Definition 1.4.6. Let V be an inner product space over $\mathbb{F}_\ell$ and W be a subspace of V. If $W \subset W^\perp$, then we call W an *isotropic subspace of V*.

Proposition 1.4.7. *$\mathcal{H}_\ell(K_\mathfrak{p})$ is an isotropic subspace of $H^1(K_\mathfrak{p}, E[\ell])$.*

Proof. This is Proposition 2.1. in (**MR3**). □

Proposition 1.4.8. *Let L/K be a cyclic extension of degree ℓ. Then $\mathcal{H}_\ell(L_\mathfrak{p}/K_\mathfrak{p})$ is an isotropic subspace of $H^1(K_\mathfrak{p}, E[\ell])$.*

Proof. This is Proposition 4.4. in (**MR3**). □

Remark 1.4.9. By Theorem 3.1. in (**KMR**), it is worth noting that if $\mathfrak{p} \notin \Sigma$ then $\dim_{\mathbb{F}_\ell} H^1(K_\mathfrak{p}, E[\ell]) = 2 \cdot \dim_{\mathbb{F}_\ell} H^1_{\mathrm{ur}}(K_\mathfrak{p}, E[\ell]) = 2 \cdot \dim_{\mathbb{F}_\ell} \mathcal{H}_\ell(K_\mathfrak{p})$.

1.5 TWISTING TO FIX THE SELMER RANK

Let ℓ be a fixed prime ≥ 5 and Σ be defined as in §1.4.

Definition 1.5.1. Suppose T is a finite subset of $\mathcal{P}$. We will say that an extension L/K is *T-ramified and Σ-split* if every $v \in T$ is ramified in L/K, every $v \in \Sigma$ splits completely in L/K, and all other v are unramified in L/K.

Lemma 1.5.2. *Suppose T is a nonempty finite subset of $\mathcal{P}$. Let ℓ be a prime. Then there is a cyclic extension L/K of degree ℓ that is T-ramified and Σ-split.*

Proof. This is Lemma 9.15. in (**MRL**). □

Proposition 1.5.3. *Let T be a finite subset of $\mathcal{P}_0(E)$. Suppose that L/K is a cyclic extension of K of degree ℓ that is T-ramified and Σ-split. Then*

$$\mathrm{Sel}_\ell(L/K, E) = \mathrm{Sel}_\ell(K, E).$$

Proof. This is Proposition 9.17 in (**MRL**).

By definition,

$$\mathrm{Sel}_\ell(L/K, E) = \{c \in H^1(K, E[\ell]) : \mathrm{loc}_\mathfrak{p}(c) \in \mathcal{H}_\ell(L_\mathfrak{p}/K_\mathfrak{p}) \text{ for every } \mathfrak{p}\}.$$

On the other hand,

$$\mathrm{Sel}_\ell(K,E) = \{c \in H^1(K, E[\ell]) : \mathrm{loc}_{\mathfrak{p}}(c) \in \mathcal{H}_\ell(K_{\mathfrak{p}}) \text{ for every } \mathfrak{p}\}.$$

If $\mathfrak{p} \in T \subseteq \mathcal{P}_0(E)$, then $H^1(K_{\mathfrak{p}}, E[\ell]) = \mathcal{H}_\ell(K_{\mathfrak{p}}) = \mathcal{H}_\ell(L_{\mathfrak{p}}/K_{\mathfrak{p}})$=0 by Lemma 1.3.3 and Lemma 1.3.4. If $\mathfrak{p} \notin T$ and $\mathfrak{p} \notin \Sigma$, by Lemma 1.3.4 (ii), $\mathcal{H}_\ell(K_{\mathfrak{p}}) = H^1_{\mathrm{ur}}(K_{\mathfrak{p}}, E[\ell]) = \mathcal{H}_\ell(L_{\mathfrak{p}}/K_{\mathfrak{p}})$. If $\mathfrak{p} \in \Sigma$, then $\mathfrak{p}$ splits in L, $\mathcal{H}_\ell(K_{\mathfrak{p}}) = \mathcal{H}_\ell(L_{\mathfrak{p}}/K_{\mathfrak{p}})$. Therefore, $\mathrm{Sel}_\ell(L/K, E) = \mathrm{Sel}_\ell(K, E)$. $\square$

Chapter 2

Elliptic curves without complex multiplication

2.1 MORE SELMER STRUCTURES

Let E be an elliptic curve defined over a number field K. Assume that E has no complex multiplication. We assume that $\mathrm{Gal}(K(E[\ell])/K) \cong \mathrm{Aut}_{\mathbb{Z}}(E[\ell]) \cong \mathrm{GL}_2(\mathbb{F}_\ell)$ for all the elliptic curves we discuss in this section. The following theorem shows that this restriction is not too severe.

Theorem 2.1.1. *Let K be a number field and let E/K be an elliptic curve without complex multiplication. Then for all but finitely many primes ℓ,* $\mathrm{Gal}(K(E[\ell])/K) \cong \mathrm{Aut}_{\mathbb{Z}}(E[\ell]) \cong \mathrm{GL}_2(\mathbb{F}_\ell)$.

Proof. This is the first theorem in Chapter IV 2.2 in (**Ser1**). □

Lemma 2.1.2. *If* $\dim_{\mathbb{F}_\ell} H^1(K_\mathfrak{p}, E[\ell]) = 2$*, then there are exactly two different 1-dimensional isotropic $\mathbb{F}_\ell$ subspaces of $H^1(K_\mathfrak{p}, E[\ell])$.*

Proof. See Lemma 3.7. in (**KMR**). □

Definition 2.1.3. If $\mathfrak{p} \in \mathcal{P}_0(E)$, we define $H^1_{\mathrm{ram}}(K_\mathfrak{p}, E[\ell]) := 0$. If $\mathfrak{p} \in \mathcal{P}_1(E)$, in this case $\dim_{\mathbb{F}_\ell} H^1(K_\mathfrak{p}, E[\ell]) = 2$ (for this, see Proposition 2.4., Theorem 3.1., and Lemma 3.4. in (**KMR**)), by Lemma 2.1.2, we define $H^1_{\mathrm{ram}}(K_\mathfrak{p}, E[\ell])$ to be the 1-dimensional isotropic $\mathbb{F}_\ell$ subspace of $H^1(K_\mathfrak{p}, E[\ell])$ which is different from $\mathcal{H}_\ell(K_\mathfrak{p})$.

Definition 2.1.4. If $\mathfrak{a}, \mathfrak{b}$, and $\mathfrak{c}$ are ideals of $\mathcal{O}_K$ such that $\mathfrak{a}, \mathfrak{b}$, and $\mathfrak{c}$ are product of primes in $\mathcal{P}_0(E) \cup \mathcal{P}_1(E)$, define

$$\mathrm{Sel}_\ell(K,E)^{\mathfrak{b}}_{\mathfrak{a}}(\mathfrak{c}) := \left\{ c \in H^1(K, E[\ell]) : \begin{array}{lll} \mathrm{loc}_v(c) \in \mathcal{H}_\ell(K_v) & \text{if} & v \nmid \mathfrak{abc} \\ \mathrm{loc}_v(c) = 0 & \text{if} & v | \mathfrak{a} \\ \mathrm{loc}_v(c) \in H^1_{\mathrm{ram}}(K_v, E[\ell]) & \text{if} & v | \mathfrak{c} \end{array} \right\}.$$

If $\mathcal{O}_K$ shows up in the notation, we omit it. The following are some examples.

If $\mathfrak{a} = \mathfrak{c} = \mathcal{O}_K$, we denote $\mathrm{Sel}_\ell(K,E)^{\mathfrak{b}}_{\mathcal{O}_K}(\mathcal{O}_K)$ by $\mathrm{Sel}_\ell(K,E)^{\mathfrak{b}}$, the relaxed-at-$\mathfrak{b}$ Selmer group.

If $\mathfrak{b} = \mathfrak{c} = \mathcal{O}_K$, we denote $\mathrm{Sel}_\ell(K,E)^{\mathcal{O}_K}_{\mathfrak{a}}(\mathcal{O}_K)$ by $\mathrm{Sel}_\ell(K,E)_{\mathfrak{a}}$, the strict-at-$\mathfrak{a}$ Selmer group.

If $\mathfrak{a} = \mathfrak{b} = \mathcal{O}_K$, we denote $\mathrm{Sel}_\ell(K,E)^{\mathcal{O}_K}_{\mathcal{O}_K}(\mathfrak{c})$ by $\mathrm{Sel}_\ell(K,E)(\mathfrak{c})$.

Note that

$$\mathrm{Sel}_\ell(K,E)_{\mathfrak{a}} \subset \mathrm{Sel}_\ell(K,E) \subset \mathrm{Sel}_\ell(K,E)^{\mathfrak{a}}.$$

Remark 2.1.5. Let L/K be a cyclic extension of degree ℓ and $\mathfrak{p} \in \mathcal{P}_1(E)$ be an ideal which ramifies in L/K. (For any prime $\mathfrak{p} \in \mathcal{P}_1(E)$, we can always find such L by Lemma 1.5.2.) Then by Proposition 1.3.5, we know that $\mathcal{H}_\ell(L_\mathfrak{p}/K_\mathfrak{p}) \neq \mathcal{H}_\ell(K_\mathfrak{p})$. They are two different 1-dimensional isotropic $\mathbb{F}_\ell$ subspaces of $H^1(K_\mathfrak{p}, E[\ell])$.

Lemma 2.1.6. *Let T be a finite subset of $\mathcal{P}_1(E)$ and $\mathfrak{a} := \prod_{\mathfrak{p} \in T} \mathfrak{p}$. If L/K is a cyclic*

extension of K of degree ℓ that is T-ramified and Σ-split, then

$$\mathrm{Sel}_\ell(L/K, E) = \mathrm{Sel}_\ell(K, E)(\mathfrak{a}).$$

Proof. By definition,

$$\mathrm{Sel}_\ell(L/K, E) = \{c \in H^1(K, E[\ell]) : \mathrm{loc}_\mathfrak{p}(c) \in \mathcal{H}_\ell(L_\mathfrak{p}/K_\mathfrak{p}) \text{ for every } \mathfrak{p}\}.$$

On the other hand,

$$\mathrm{Sel}_\ell(K, E)(\mathfrak{a}) := \left\{ \begin{array}{lll} c \in H^1(K, E[\ell]) : & \mathrm{loc}_\mathfrak{p}(c) \in \mathcal{H}_\ell(K_\mathfrak{p}) & \text{if} \quad \mathfrak{p} \nmid \mathfrak{a} \\ & \mathrm{loc}_\mathfrak{p}(c) \in H^1_{\mathrm{ram}}(K_\mathfrak{p}, E[\ell]) & \text{if} \quad \mathfrak{p} | \mathfrak{a} \end{array} \right\}.$$

If $\mathfrak{p}|\mathfrak{a}$, by Remark 2.1.5, Lemma 2.1.2 and Definition 2.1.3, $H^1_{\mathrm{ram}}(K_\mathfrak{p}, E[\ell]) = \mathcal{H}_\ell(L_\mathfrak{p}/K_\mathfrak{p})$. If $\mathfrak{p} \nmid \mathfrak{a}$, by Lemma 1.3.4 (ii) and the fact that primes in Σ split in L, $\mathcal{H}_\ell(K_\mathfrak{p}) = \mathcal{H}_\ell(L_\mathfrak{p}/K_\mathfrak{p})$. $\square$

2.2 TWISTING TO INCREASE THE SELMER RANK

Let E be an elliptic curve defined over a number field K. Let ℓ be a fixed prime such that $\mathrm{Gal}(K(E[\ell])/K) \cong \mathrm{GL}_2(\mathbb{F}_\ell)$. Let Σ be defined as in §1.4.

If $c \in H^1(K, E[\ell])$ and $\sigma \in G_K$, let

$$c(\sigma) \in E[\ell]/(\sigma - 1)E[\ell]$$

denote the image of σ under any cocycle representing c. This is well-defined.

Lemma 2.2.1. *Suppose that $\sigma \in G_K$. Suppose that C is a finite subgroup of $H^1(K, E[\ell])$. Then there is a $\tau \in G_{K(E[\ell])}$ such that $c(\tau\sigma) = 0$ for all $c \in C$.*

Proof. This is Lemma 3.5 in (**MR1**). Just replace 2 by ℓ and take $\phi = 0$ in (**MR1**).

Let $\Gamma := \mathrm{Gal}(K(E[\ell])/K) \cong \mathrm{GL}_2(\mathbb{F}_\ell)$. Then $H^1(\Gamma, E[\ell]) = 0$, so the restriction map

$$H^1(K, E[\ell]) \hookrightarrow \mathrm{Hom}(G_{K(E[\ell])}, E[\ell])^\Gamma$$

is injective.

Fix cocycles $\{c_1, ..., c_k\}$ representing an $\mathbb{F}_\ell$-basis of C. Then $c_1, ...c_k$ restrict to linearly independent homomorphisms $\tilde{c}_1, ..., \tilde{c}_k \in \mathrm{Hom}(G_{K(E[\ell])}, E[\ell])^\Gamma$.

Let $N \subset \bar{K}$ be the abelian extension of $K(E[\ell])$ fixed by $\cap_i \ker(\tilde{c}_i) \subset G_{K(E[\ell])}$. Put $W := G_{K(E[\ell])}/\cap_i \ker(\tilde{c}_i) = \mathrm{Gal}(N/K(E[\ell]))$. Then W is an $\mathbb{F}_\ell$-vector space with an action of Γ, $\tilde{c}_1, ..., \tilde{c}_k$ are linearly independent in $\mathrm{Hom}(W, E[\ell])^\Gamma$, and

$$\tilde{c}_1 \times ... \times \tilde{c}_k : W \hookrightarrow E[\ell]^k \tag{2.2.2}$$

is a Γ-equivariant injection. Thus W is isomorphic to a Γ-submodule of the semisimple module $E[\ell]^k$, so W is also semisimple. But if U is an irreducible constituent of W, then U is also an irreducible constituent of $E[\ell]^k$, so $U \cong E[\ell]$. Therefore $W \cong E[\ell]^j$ for some $j \leq k$. But then $j = \dim_{\mathbb{F}_\ell} \mathrm{Hom}(W, E[\ell])^\Gamma \geq k$, so $j = k$ and (2.2.2) is an isomorphism.

Since (2.2.2) is surjective, we can choose $\tau \in G_{K(E[\ell])}$ such that $c_i(\tau) = -c_i(\sigma)$ for $1 \leq i \leq k$. Then $c_i(\tau\sigma) = 0$ for every i. Since the c_i represent a basis of C, $c(\tau\sigma) = 0$ for all $c \in C$. $\square$

Definition 2.2.3. Let $F_1 := K(\boldsymbol{\mu}_\ell, (\mathcal{O}_{K,\Sigma}^\times)^{1/\ell})$. Suppose $\sigma \in G_{K(\boldsymbol{\mu}_\ell)}$ is such that $\dim_{\mathbb{F}_\ell}(E[\ell]/(\sigma - 1)E[\ell]) = 1$ and $\sigma|_{F_1} = 1$.

Suppose $\mathfrak{a}$ is an ideal of $\mathcal{O}_K$. If $c \in \mathrm{Sel}_\ell(K, E)(\mathfrak{a})$, let

$$\tilde{c} : G_{K(E[\ell])} \to E[\ell]/(\sigma - 1)E[\ell]$$

be the restriction of c to $G_{K(E[\ell])}$. Let $N_{\mathfrak{a}}$ be the abelian extension of $K(E[\ell])$ fixed by $\cap_{c\in \mathrm{Sel}_\ell(K,E)(\mathfrak{a})} \ker(\tilde{c})$.

Take $C = \mathrm{Sel}_\ell(K,E)(\mathfrak{a})$ in Lemma 2.2.1 and $N = N_{\mathfrak{a}}$ as in Definition 2.2.3. By Lemma 2.2.1, we can choose $\tau_{\mathfrak{a}} \in G_{K(E[\ell])}$ such that $c(\tau_{\mathfrak{a}}\sigma) = 0$ for all $c \in \mathrm{Sel}_\ell(K,E)(\mathfrak{a})$.

Lemma 2.2.4. *Suppose $\mathfrak{a}$ is product of primes in $\mathcal{P}_0(E)\cup\mathcal{P}_1(E)$. Let σ, $\tau_{\mathfrak{a}}$, and $N_{\mathfrak{a}}$ be as in Definition* 2.2.3. *Assume that $\mathfrak{p}$ is a prime whose Frobenius conjugacy class in* $\mathrm{Gal}(N_{\mathfrak{a}}F_1/K)$ *is the class of $\tau_{\mathfrak{a}}\sigma$. Then $\mathfrak{p} \in \mathcal{P}_1(E)$ and* $\mathrm{loc}_{\mathfrak{p}}(\mathrm{Sel}_\ell(K,E)(\mathfrak{a})) = 0$.

Proof. Since Frobenius fixes $\boldsymbol{\mu}_\ell$ and $(\mathcal{O}_{K,\Sigma}^\times)^{1/\ell}$, we have that $\boldsymbol{\mu}_\ell$ and $(\mathcal{O}_{K,\Sigma}^\times)^{1/\ell}$ are contained in $K_{\mathfrak{p}}^\times$. Hence $\mathbf{N}\mathfrak{p} \equiv 1 \pmod{\ell}$ and the inclusion $K^\times \hookrightarrow K_{\mathfrak{p}}^\times$ sends $\mathcal{O}_{K,\Sigma}^\times$ into $(\mathcal{O}_{K,\mathfrak{p}}^\times)^\ell$, so $\mathfrak{p} \in \mathcal{P}$.

By Lemma 1.3.4, evaluation of cocycles at a Frobenius element for $\mathfrak{p}$ in G_K induces an isomorphism

$$\mathcal{H}_\ell(K_{\mathfrak{p}}) = H^1_{\mathrm{ur}}(K_{\mathfrak{p}}, E[\ell]) \cong E[\ell]/(\sigma-1)E[\ell].$$

Thus $\mathfrak{p} \in \mathcal{P}_1(E)$. Furthermore, if $c \in \mathrm{Sel}_\ell(K,E)(\mathfrak{a})$, $\mathrm{loc}_{\mathfrak{p}}(c) = c(\tau_{\mathfrak{a}}\sigma)$=0 via the following maps

$$\mathrm{loc}_{\mathfrak{p}} : \mathrm{Sel}_\ell(K,E)(\mathfrak{a}) \to \mathcal{H}_\ell(K_{\mathfrak{p}}) \cong H^1_{\mathrm{ur}}(K, E[\ell]) \cong E[\ell]/(\tau_{\mathfrak{a}}\sigma - 1)E[\ell]$$

and Lemma 2.2.1. Therefore, $\mathrm{loc}_{\mathfrak{p}}(\mathrm{Sel}_\ell(K,E)(\mathfrak{a})) = 0$. □

Proposition 2.2.5. *Let $\mathfrak{p} \in \mathcal{P}_1(E)$. Suppose $\mathfrak{a}$ is product of primes in $\mathcal{P}_0(E)\cup\mathcal{P}_1(E)$. Then* $\mathrm{loc}_{\mathfrak{p}}(\mathrm{Sel}_\ell(K,E)^{\mathfrak{p}}(\mathfrak{a}))$ *is an isotropic subspace of $H^1(K_{\mathfrak{p}}, E[\ell])$.*

Proof. Let M_K be a complete set of primes of $\mathcal{O}_K$. Let $c, d \in \mathrm{Sel}_\ell(K,E)^{\mathfrak{p}}(\mathfrak{a}) \subset H^1(K, E[\ell])$. By Theorem 1.4.5,

$$\sum_{v\in M_K} < \mathrm{loc}_v(c), \mathrm{loc}_v(d) >_v = 0.$$

By Defininion 2.1.4, $\mathrm{loc}_v(c)$ and $\mathrm{loc}_v(d) \in H^1_{\mathrm{ram}}(K_v, E[\ell])$ for $v|\mathfrak{a}$. Since $H^1_{\mathrm{ram}}(K_v, E[\ell])$ is an isotropic subspace, we have $< \mathrm{loc}_v(c), \mathrm{loc}_v(d) >_v = 0$ for $v|\mathfrak{a}$. For $v \nmid \mathfrak{a}\mathfrak{p}$, $\mathrm{loc}_v(c)$ and $\mathrm{loc}_v(d) \in \mathcal{H}_\ell(K_v)$. Therefore, by Proposition 1.4.7, we have $< \mathrm{loc}_v(c), \mathrm{loc}_v(d) >_v = 0$ for $v \nmid \mathfrak{a}\mathfrak{p}$.

Hence, focus on $\mathfrak{p}$ alone, we have $< \mathrm{loc}_\mathfrak{p}(c), \mathrm{loc}_\mathfrak{p}(d) >_\mathfrak{p} = 0$ and $\mathrm{loc}_\mathfrak{p}(\mathrm{Sel}_\ell(K,E)^\mathfrak{p}(\mathfrak{a}))$ is an isotropic subspace. □

Proposition 2.2.6. *Let $\mathfrak{a}$ be product of primes in $\mathcal{P}_0(E) \cup \mathcal{P}_1(E)$. Let σ, $\tau_\mathfrak{a}$, and $N_\mathfrak{a}$ be as in Definition 2.2.3. If $\mathfrak{p}$ is a prime whose Frobenius conjugacy class in $\mathrm{Gal}(N_\mathfrak{a}F_1/K)$ is the class of $\tau_\mathfrak{a}\sigma$, then*

$$\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K,E)(\mathfrak{a}\mathfrak{p}) = \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K,E)(\mathfrak{a}) + 1.$$

Proof. By Lemma 2.2.4, if $\mathfrak{p}$ is a prime whose Frobenius conjugacy class in $\mathrm{Gal}(N_\mathfrak{a}F_1/K)$ is the class of $\tau_\mathfrak{a}\sigma$, then $\mathfrak{p} \in \mathcal{P}_1(E)$ and $\mathrm{loc}_\mathfrak{p}(\mathrm{Sel}_\ell(K,E)(\mathfrak{a})) = 0$. Consider the exact sequences

$$\begin{aligned} &0 \to \mathrm{Sel}_\ell(K,E)(\mathfrak{a}) \to \mathrm{Sel}_\ell(K,E)^\mathfrak{p}(\mathfrak{a}) \to H^1(K_\mathfrak{p}, E[\ell])/\mathcal{H}_\ell(K_\mathfrak{p}) \\ &0 \to \mathrm{Sel}_\ell(K,E)_\mathfrak{p}(\mathfrak{a}) \to \mathrm{Sel}_\ell(K,E)(\mathfrak{a}) \longrightarrow \mathcal{H}_\ell(K_\mathfrak{p}). \end{aligned} \tag{2.2.7}$$

We can use global duality (see for example Theorem 2.3.4 in (**MR2**)) to conclude that the images of the two right-hand maps in (2.2.7) are orthogonal complements of each other under the local Tate pairing. By our choice of $\mathfrak{p}$ the lower right-hand map is zero, so the upper right-hand map is surjective. And we get

$$\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K,E)_\mathfrak{p}(\mathfrak{a}) = \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K,E)(\mathfrak{a}). \tag{2.2.8}$$

Then we consider the exact sequences

$$\begin{aligned} &0 \to \mathrm{Sel}_\ell(K,E)_\mathfrak{p}(\mathfrak{a}) \to \mathrm{Sel}_\ell(K,E)(\mathfrak{a}\mathfrak{p}) \longrightarrow H^1_{\mathrm{ram}}(K_\mathfrak{p}, E[\ell]) \\ &0 \to \mathrm{Sel}_\ell(K,E)(\mathfrak{a}\mathfrak{p}) \to \mathrm{Sel}_\ell(K,E)^\mathfrak{p}(\mathfrak{a}) \to H^1(K_\mathfrak{p}, E[\ell])/H^1_{\mathrm{ram}}(K_\mathfrak{p}, E[\ell]). \end{aligned} \tag{2.2.9}$$

Again, global duality tells us that the images of the two right-hand maps are orthogonal complements of each other under the local Tate pairing. By Lemma 2.1.2, Definition 2.1.3, and Proposition 2.2.5, $\mathrm{loc}_{\mathfrak{p}}(\mathrm{Sel}_\ell(K,E)^{\mathfrak{p}}(\mathfrak{a})) = H^1_{\mathrm{ram}}(K_{\mathfrak{p}}, E[\ell])$ since they are 1-dimensional isotropic $\mathbb{F}_\ell$ subspaces of $H^1(K_{\mathfrak{p}}, E[\ell])$ and $\mathrm{loc}_{\mathfrak{p}}(\mathrm{Sel}_\ell(K,E)^{\mathfrak{p}}(\mathfrak{a}))$
$\neq \mathcal{H}_\ell(K_{\mathfrak{p}})$ by the fact that the upper right-hand map in (2.2.7) is surjective. So, the lower right-hand map in (2.2.9) is zero and the upper right-hand map in (2.2.9) is surjective. And we get

$$\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K,E)(\mathfrak{a}\mathfrak{p}) = \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K,E)_{\mathfrak{p}}(\mathfrak{a}) + 1. \tag{2.2.10}$$

Combine (2.2.8) and (2.2.10), we get

$$\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K,E)(\mathfrak{a}\mathfrak{p}) = \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K,E)(\mathfrak{a}) + 1.$$

□

2.3 FIELDS GENERATED BY TORSION POINTS OF ELLIPTIC CURVES

Let E_1 and E_2 be elliptic curves defined over a number field K. In this section, we show that $K(E_1[\ell]) \neq K(E_2[\ell])$ in different cases.

Definition 2.3.1. Let $A \in \mathrm{GL}_2(\mathbb{F}_\ell)$. A *radial automorphism* is an automorphism of the form:

$$A \longmapsto A(\det A)^m$$

where m is considered modulo $\ell - 1$, and has the property that $2m+1$ is relatively prime to

$\ell - 1$. The latter condition is necessary for invertibility.

Note that all the radial automorphisms commute with all the inner automorphisms.

Lemma 2.3.2. *The group* $\mathrm{Aut}(\mathrm{GL}_2(\mathbb{F}_\ell))$ *is the direct product of the group of inner automorphisms and the group of radial automorphisms.*

Proof. Let $R = \mathbb{F}_\ell$ in the Theorem of page 465 in (**Re**). □

Definition 2.3.3. For $i = 1, 2$, let E_i be elliptic curves over a number field K. Let v be a place of $\mathcal{O}_K$ where E_i has good reduction. Let $\mathbf{N}v$ be the norm of v. We denote the reduction of E_i modulo v by $\tilde{E}_{i,v}$. We also denote the Frobenius endomorphism of $\tilde{E}_{i,v}$ by $\mathrm{Fr}_{i,v}$ and we identify it to the corresponding automorphism of $T_\ell(E_i)$ where $T_\ell(E_i)$ are the Tate modules of E_i. Via the isomorphism $T_\ell(E_i) \cong T_\ell(\tilde{E}_{i,v})$, we can let $\mathrm{Fr}_{i,v}$ act on $T_\ell(E_i)$. Then we can talk about the trace of $\mathrm{Fr}_{i,v}$ and denote it by $\mathrm{Tr}(\mathrm{Fr}_{i,v})$. We also know that $\mathrm{Tr}(\mathrm{Fr}_{i,v}) = 1 + \mathbf{N}_v - t_{i,v} \in \mathbb{Z}$ where $t_{i,v}$ is the number of points of $\tilde{E}_{i,v}$. Note this is independent of ℓ. Define the Galois modules $V_\ell(E_i) := T_\ell(E_i) \otimes \mathbb{Q}_\ell$. (See Chapter IV in (**Ser1**).)

Proposition 2.3.4. *Let* $a \in \mathbb{N}$. *There are infinitely many primes* ℓ *satisfying*

$$\left(\frac{a}{\ell}\right) = 1.$$

Proof. This is a consequence of Dirichlet's theorem on primes in arithmetic progressions. □

Proposition 2.3.5 (Serre)**.** *Let* E_1 *and* E_2 *be elliptic curves defined over* K. *The following conditions are equivalent:*

(i) The Galois modules $V_\ell(E_1)$ *and* $V_\ell(E_2)$ *are isomorphic for at least one* ℓ.

(ii) For a set of places of K *of density one we have* $\mathrm{Tr}(\mathrm{Fr}_{1,v}) = \mathrm{Tr}(\mathrm{Fr}_{2,v})$.

Proof. This is the proposition in Chapter IV 2.3 in (**Ser1**). □

Proposition 2.3.6 (Faltings)**.** *Let E_1 and E_2 be elliptic curves defined over K. If* $\mathrm{Tr}(\mathrm{Fr}_{1,v}) = \mathrm{Tr}(\mathrm{Fr}_{2,v})$ *for a set of places of K of density one, then E_1 and E_2 are isogenous over K.*

Proof. By Proposition 2.3.5, the Galois modules $V_\ell(E_1)$ and $V_\ell(E_2)$ are isomorphic for some ℓ. Let $F : T_\ell(E_1) \otimes \mathbb{Q}_\ell \to T_\ell(E_2) \otimes \mathbb{Q}_\ell$ be such an isomorphism. Multiplying F by ℓ^n for some large n, we have $\ell^n F(T_\ell(E_1)) \subseteq T_\ell(E_2)$. This tells us that $\mathrm{Hom}_K(T_\ell(E_1), T_\ell(E_2))$ is nonempty. By Isogeny Theorem 7.7. in Chapter III of (**Si**) (this was proved by Faltings, see (**F1**) and (**F2**)), $\mathrm{Hom}_K(E_1, E_2)$ is also nonempty. Therefore, E_1 and E_2 are isogenous over K. $\square$

Theorem 2.3.7. *Let E_1 and E_2 be elliptic curves defined over a number field K without complex multiplication. If $K(E_1[\ell]) = K(E_2[\ell])$ for all but finitely many primes ℓ, then E_1 and E_2 are isogenous over K. In other words, if E_1 is not isogenous to E_2 over K, then $K(E_1[\ell]) \neq K(E_2[\ell])$ for infinitely many primes ℓ.*

Proof. Assume that $K(E_1[\ell]) = K(E_2[\ell])$ for all but finitely many primes ℓ. Let S be the set of primes such that E_1 and E_2 have good reduction.

Fix a prime v in S. By Proposition 2.1.1, Proposition 2.3.4, and the fact that $K(E_1[\ell]) = K(E_2[\ell])$ for all but finitely many primes ℓ, there are infinitely many primes ℓ such that $\mathrm{Gal}(K(E_1[\ell])/K) \cong \mathrm{Gal}(K(E_2[\ell])/K) \cong \mathrm{GL}_2(\mathbb{F}_\ell)$, $K(E_1[\ell]) = K(E_2[\ell])$, and $\left(\frac{\mathbf{N}v}{\ell}\right) = 1$. For this v, we run the following argument for all these ℓ. Let $\phi_1 : \mathrm{Gal}(K(E_1[\ell])/K) \cong \mathrm{GL}_2(\mathbb{F}_\ell)$ and $\phi_2 : \mathrm{Gal}(K(E_2[\ell])/K) \cong \mathrm{GL}_2(\mathbb{F}_\ell)$. Consider the commutative diagram

$$\begin{tikzcd}
\mathrm{Gal}(K(E_1[\ell])/K) \arrow[r, "\phi_1"] \arrow[d, equal] & \mathrm{GL}_2(\mathbb{F}_\ell) \arrow[d, "\phi_2\phi_1^{-1}"'] \arrow[dr, "\det"] & \\
\mathrm{Gal}(K(E_2[\ell])/K) \arrow[r, "\phi_2"] & \mathrm{GL}_2(\mathbb{F}_\ell) \arrow[r, "\det"'] & \mathbb{F}_\ell^\times
\end{tikzcd}$$

(For $\sigma \in \mathrm{Gal}(K(E_i[\ell])/K)$, $\sigma(x) = (x)^{\det(\phi_i(\sigma))} \quad \forall x \in \boldsymbol{\mu_\ell}$. Therefore, the whole diagram

commutes.) Then ${\phi_2\phi_1}^{-1} : \mathrm{GL}_2(\mathbb{F}_\ell) \cong \mathrm{GL}_2(\mathbb{F}_\ell)$ is an isomorphism. By Lemma 2.3.2, $\mathrm{Aut}(\mathrm{GL}_2(\mathbb{F}_\ell))$ is the direct product of inner automorphisms and radial automorphisms. Pick a $\mathbb{Z}/\ell\mathbb{Z}$-basis of $E_2[\ell]$ such that ${\phi_2\phi_1}^{-1} : \mathrm{GL}_2(\mathbb{F}_\ell) \cong \mathrm{GL}_2(\mathbb{F}_\ell)$ is an automorphism in the radial automorphism subgroup. That is to say, ${\phi_2\phi_1}^{-1}(A) = A(\det A)^{m_\ell}$ for some m_ℓ. Look at the comutative triangle in the diagram. Let $A \in \mathrm{GL}_2(\mathbb{F}_\ell)$, we have $\det A = (\det A)^{2m_\ell+1}$. So $(\det A)^{2m_\ell} = 1$ for all $A \in \mathrm{GL}_2(\mathbb{F}_\ell)$. Then either $m_\ell = 0$ or $m_\ell = \frac{\ell-1}{2}$.

Let σ_v be the Frobenius element of v in $\mathrm{Gal}(K(E_1[\ell])/K) = \mathrm{Gal}(K(E_2[\ell])/K)$. We know that

$$\det(\mathrm{Fr}_{i,v}) = \mathbf{N}v \equiv \det(\phi_i(\sigma_v)) \pmod{\ell}.$$

So $(\det(\phi_1(\sigma_v)))^{m_\ell} = (\overline{\mathbf{N}v})^{m_\ell} = 1$ (no matter $m_\ell = 0$ or $m_\ell = \frac{\ell-1}{2}$) since $(\overline{\mathbf{N}v})^{\frac{\ell-1}{2}} = \left(\frac{\mathbf{N}v}{\ell}\right) = 1$. And $\phi_2(\sigma_v) = \phi_2{\phi_1}^{-1}\phi_1(\sigma_v) = \phi_1(\sigma_v)(\det(\phi_1(\sigma_v)))^{m_\ell} = \phi_1(\sigma_v)$. We also know that

$$\mathrm{Tr}(\mathrm{Fr}_{i,v}) \equiv \mathrm{Tr}(\phi_i(\sigma_v)) \pmod{\ell}.$$

Therefore we get $\mathrm{Tr}(\mathrm{Fr}_{1,v}) \equiv \mathrm{Tr}(\mathrm{Fr}_{2,v}) \pmod{\ell}$. Run this argument for these infinitely many primes ℓ, then $\mathrm{Tr}(\mathrm{Fr}_{1,v}) = \mathrm{Tr}(\mathrm{Fr}_{2,v}) \in \mathbb{Z}$. This is true for all v in the set S of places of K of density one. Therefore, by Proposition 2.3.6, E_1 and E_2 are isogenous over K. $\square$

2.4 LINEARLY DISJOINT FIELDS

In this section, we prove that some important fields are linearly disjoint. Assume that $\ell \geq 5$. Assume that $\mathrm{Gal}(K(E_1[\ell])/K) \cong \mathrm{Gal}(K(E_2[\ell])/K) \cong \mathrm{GL}_2(\mathbb{F}_\ell)$.

Definition 2.4.1. Let $F_2 := K(E_1[\ell]) \cap K(E_2[\ell])$.

Lemma 2.4.2. *Let $F_2 = K(E_1[\ell]) \cap K(E_2[\ell])$.*

$$\begin{tikzcd}
K(E_1[\ell]) \arrow[dr, dash] & & K(E_2[\ell]) \arrow[dl, dash] \\
& F_2 \arrow[d, dash] & \\
& K(\boldsymbol{\mu}_\ell) &
\end{tikzcd}$$

Then either $F_2 = K(E_1[\ell]) = K(E_2[\ell])$, $[K(E_1[\ell]) : F_2] = [K(E_2[\ell]) : F_2] = 2$ or $F_2 = K(\boldsymbol{\mu}_\ell)$.

Proof. Since F_2 is Galois over $K(\boldsymbol{\mu}_\ell)$, $\mathrm{Gal}(K(E_1[\ell])/F_2)$ is a normal subgroup of $\mathrm{Gal}(K(E_1[\ell])/K(\boldsymbol{\mu}_\ell))$. For $\ell \geq 5$, $\mathrm{Gal}(K(E_1[\ell])/K(\boldsymbol{\mu}_\ell)) \cong \mathrm{SL}_2(\mathbb{F}_\ell)$ has only 3 normal subgroups.

- If $\mathrm{Gal}(K(E_1[\ell])/F_2) = \{1\}$, then $F_2 = K(E_1[\ell]) = K(E_2[\ell])$.
- If $\mathrm{Gal}(K(E_1[\ell])/F_2) = \{\pm 1\}$, then $[K(E_1[\ell]) : F_2] = [K(E_2[\ell]) : F_2] = 2$.
- If $\mathrm{Gal}(K(E_1[\ell])/F_2) = \mathrm{SL}_2(\mathbb{F}_\ell)$, then $F_2 = K(\boldsymbol{\mu}_\ell)$.

□

Lemma 2.4.3. *There is no nontrivial Galois ℓ-extension of F_2 in $K(E_1[\ell])$.*

Proof. There is no nontrivial ℓ-extension of F_2 in $K(E_1[\ell])$ by Lemma 2.4.2 and the fact that $\mathrm{SL}_2(\mathbb{F}_\ell)$ has no abelian quotient of order ℓ. □

Lemma 2.4.4. *Suppose that N is an abelian ℓ-extension of $K(E_2[\ell])$. Assume that $K(E_1[\ell]) \neq K(E_2[\ell])$. Then $K(E_1[\ell]) \cap N = F_2$.*

Proof. Consider the following diagram:

$$\begin{tikzcd}
 & K(E_1[\ell], E_2[\ell]) \arrow[dl, dash] \arrow[dr, dash] & & N \arrow[dl, dash] \\
K(E_1[\ell]) \arrow[dr, dash] & & K(E_2[\ell]) \arrow[dl, dash] & \\
 & F_2 & &
\end{tikzcd}$$

By the definition of F_2, $\mathrm{Gal}(K(E_1[\ell], E_2[\ell])/K(E_2[\ell])) \cong \mathrm{Gal}(K(E_1[\ell])/F_2)$. By Lemma 2.4.3,

$$K(E_1[\ell], E_2[\ell]) \cap N = K(E_2[\ell]). \tag{2.4.5}$$

By (2.4.5),we have

$$\begin{aligned}
K(E_1[\ell]) \cap N &\subseteq K(E_1[\ell]) \cap K(E_1[\ell], E_2[\ell]) \cap N \\
&= K(E_1[\ell]) \cap K(E_2[\ell]) \\
&= F_2.
\end{aligned}$$

□

2.5 FIX THE SELMER RANK OF E_1 AND INCREASE THE SELMER RANK OF E_2 SIMULTANEOUSLY

In this section, let ℓ be a fixed prime such that $\ell \geq 5$. Assume that $\mathrm{Gal}(K(E_i[\ell])/K) \cong \mathrm{GL}_2(\mathbb{F}_\ell)$ for $i \in \{1, 2\}$ and $K(E_1[\ell]) \neq K(E_2[\ell])$. Recall that Σ (associated to this ℓ) is defined as in §1.4.

Lemma 2.5.1. *If* $\mathrm{Gal}(K(E[\ell])/K) \cong \mathrm{GL}_2(\mathbb{F}_\ell)$*, then*

$$K(\boldsymbol{\mu}_\ell, (\mathcal{O}_{K,\Sigma}^\times)^{1/\ell}) \cap K(E[\ell]) = K(\boldsymbol{\mu}_\ell).$$

Proof. This is Lemma 9.3. in (**MRL**). □

Recall that $F_1 := K(\boldsymbol{\mu}_\ell, (\mathcal{O}_{K,\Sigma}^\times)^{1/\ell})$ and $F_2 := K(E_1[\ell]) \cap K(E_2[\ell])$.

Lemma 2.5.2. *There is a* $\tau \in G_{K(\boldsymbol{\mu}_\ell)}$ *such that* $\dim_{\mathbb{F}_\ell}(E_1[\ell]/(\tau-1)E_1[\ell]) = 0$ *and* $\dim_{\mathbb{F}_\ell}(E_2[\ell]/(\tau-1)E_2[\ell]) = 1$.

Proof. By Lemma 2.4.2 and the assumption that $K(E_1[\ell]) \neq K(E_2[\ell])$ at the beginning of this section, either $F_2 = K(\boldsymbol{\mu}_\ell)$ or $[K(E_1[\ell]) : F_2] = [K(E_2[\ell]) : F_2] = 2$.

(i) Assume that $K(E_1[\ell]) \cap K(E_2[\ell]) = F_2 = K(\boldsymbol{\mu}_\ell)$. Let $\tau \in G_{K(\boldsymbol{\mu}_\ell)}$ be an element that acts like $\begin{bmatrix} -1 & -1 \\ 0 & -1 \end{bmatrix}$ on $E_1[\ell]$ and acts like $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ on $E_2[\ell]$. We can find such τ since the determinant of these two matrices are 1. Therefore, $\dim_{\mathbb{F}_\ell}(E_1[\ell]/(\tau-1)E_1[\ell]) = 0$ and $\dim_{\mathbb{F}_\ell}(E_2[\ell]/(\tau-1)E_2[\ell]) = 1$.

(ii) Assume that $[K(E_1[\ell]) : F_2] = [K(E_2[\ell]) : F_2] = 2$. Pick an $\mathbb{F}_\ell$-basis $\mathcal{B}_2$ of $E_2[\ell]$. Let $\tau_2 \in \mathrm{SL}_2(\mathbb{F}_\ell) \cong \mathrm{Gal}(K(E_2[\ell]/K(\boldsymbol{\mu}_\ell)))$ be an element that acts like $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. Therefore, $\dim_{\mathbb{F}_\ell}(E_2[\ell]/(\tau_2-1)E_2[\ell]) = 1$.

We know that τ_2 has order ℓ. Now choose $\tau_1 \in \mathrm{Gal}(K(E_1[\ell]/K(\boldsymbol{\mu}_\ell)))$ to be an element

such that $\tau_1|_{F_2} = \tau_2|_{F_2}$.

$$\begin{tikzcd}
K(E_1[\ell]) \arrow[dr, dash] \arrow[ddr, dash, "\tau_1"'] & & K(E_2[\ell]) \arrow[dl, dash] \arrow[ddl, dash, "\tau_2"] \\
& F_2 \arrow[d, dash] & \\
& K(\boldsymbol{\mu}_\ell) &
\end{tikzcd}$$

If we view τ_1 as an element of order ℓ in $\mathrm{Gal}(F_2/K(\boldsymbol{\mu}_\ell))) \cong \mathrm{SL}_2(\mathbb{F}_\ell)/\{\pm 1\}$, then $\tau_1^\ell \in \{\pm 1\}$ in $\mathrm{Gal}(K(E_1[\ell]/K(\boldsymbol{\mu}_\ell)))$. Therefore, $\tau_1^{2\ell} = 1$ in $\mathrm{Gal}(K(E_1[\ell]/K(\boldsymbol{\mu}_\ell)))$. Then we have two different choices of τ_1 in $\mathrm{Gal}(K(E_1[\ell]/K(\boldsymbol{\mu}_\ell)))$. One has order ℓ and another one has order 2ℓ.

We choose τ_1 to be the one with order 2ℓ in $\mathrm{Gal}(K(E_1[\ell]/K(\boldsymbol{\mu}_\ell))) \cong \mathrm{SL}_2(\mathbb{F}_\ell)$. Therefore, τ_1 satisfies $x^{2\ell}-1 = (x+1)^\ell(x-1)^\ell = 0$ in $\mathbb{F}_\ell[x]$. Let $f(x)$ be the minimal polynomial of τ_1. We know that the characteristic polynomial of τ_1 has degree 2. Then $\deg f(x) \leq 2$. It can not be 1 since τ_1 has order ℓ in $\mathrm{Gal}(F_2/K(\boldsymbol{\mu}_\ell))) \cong \mathrm{SL}_2(\mathbb{F}_\ell)/\{\pm 1\}$. Hence $\deg f(x) = 2$. Either $f(x) = x^2 - 1, f(x) = (x-1)^2$ or $f(x) = (x+1)^2$.

- If $f(x) = x^2 - 1$, then order of τ_1 in $\mathrm{Gal}(K(E_1[\ell]/K(\boldsymbol{\mu}_\ell)))$ is at most 2. This contradicts to the fact that τ_1 has order 2ℓ.
- If $f(x) = (x-1)^2$, then τ_1 satisfies $(x-1)^2$ and also $x^\ell - 1 = (x-1)^\ell$. Then order of τ_1 in $\mathrm{Gal}(K(E_1[\ell]/K(\boldsymbol{\mu}_\ell)))$ is at most ℓ. This also contradicts to the fact that τ_1 has order 2ℓ.

Therefore, $f(x) = (x+1)^2$ and τ_1 has no eigenvalue 1. Hence, $\tau_1 - 1$ is invertible and $\dim_{\mathbb{F}_\ell}(E_1[\ell]/(\tau_1 - 1)E_1[\ell]) = 0$.

Finally, let $\tau \in G_{K(\boldsymbol{\mu}_\ell)}$ be an element such that $\tau|_{K(E_1[\ell])} = \tau_1$ and $\tau|_{K(E_1[\ell])} = \tau_2$. Then

$$\dim_{\mathbb{F}_\ell}(E_1[\ell]/(\tau - 1)E_2[\ell]) = \dim_{\mathbb{F}_\ell}(E_1[\ell]/(\tau_1 - 1)E_2[\ell]) = 0,$$

$$\dim_{\mathbb{F}_\ell}(E_2[\ell]/(\tau-1)E_2[\ell]) = \dim_{\mathbb{F}_\ell}(E_2[\ell]/(\tau_2-1)E_2[\ell]) = 1.$$

□

Definition 2.5.3. Let $\tau \in G_{K(\boldsymbol{\mu}_\ell)}$ be as in Lemma 2.5.2. Therefore, $\dim_{\mathbb{F}_\ell}(E_1[\ell]/(\tau - 1)E_1[\ell]) = 0$ and $\dim_{\mathbb{F}_\ell}(E_2[\ell]/(\tau-1)E_2[\ell]) = 1$.

By Lemma 2.5.1, $K(E_2[\ell])$ and F_1 are linearly disjoint over $K(\boldsymbol{\mu}_\ell)$. Let $\sigma_1 \in G_K$ such that

$$\sigma_1 = \tau \text{ on } K(E_2[\ell]),$$

$$\sigma_1 = 1 \text{ on } F_1 = K(\boldsymbol{\mu}_\ell, (\mathcal{O}_{K,\Sigma}^\times)^{1/\ell}).$$

This is possible since $\tau = 1$ on $F_1 \cap K(E_2[\ell]) = K(\boldsymbol{\mu}_\ell)$.

Suppose $\mathfrak{a}$ is product of primes in $\mathcal{P}_0(E_1) \cap \mathcal{P}_1(E_2)$. If $c \in \mathrm{Sel}_\ell(K, E_2)(\mathfrak{a})$, let

$$\tilde{c} : G_{K(E_2[\ell])} \to E_2[\ell]/(\sigma_1 - 1)E_2[\ell]$$

be the restriction of c to $G_{K(E_2[\ell])}$. Let $N_\mathfrak{a}$ be the abelian extension of $K(E_2[\ell])$ fixed by $\cap_{c \in \mathrm{Sel}_\ell(K,E_2)(\mathfrak{a})} \ker(\tilde{c})$.

If we take $C = \mathrm{Sel}_\ell(K, E_2)(\mathfrak{a})$ and $\sigma = \sigma_1$ in Lemma 2.2.1, then $K(E[\ell]) = K(E_2[\ell])$, and $N = N_\mathfrak{a}$. As in the proof of Lemma 2.2.1, we can choose $\tau_\mathfrak{a} \in G_{K(E_2[\ell])}$ such that $c(\tau_\mathfrak{a}\sigma_1) = 0$ for all $c \in \mathrm{Sel}_\ell(K, E_2)(\mathfrak{a})$.

Proposition 2.5.4. *Let $\mathfrak{a}$ be product of primes in $\mathcal{P}_0(E_1) \cap \mathcal{P}_1(E_2)$. Then there is a prime $\mathfrak{p}$ in $\mathcal{P}_0(E_1) \cap \mathcal{P}_1(E_2)$ such that*

$$\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, E_2)(\mathfrak{a}\mathfrak{p}) = \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, E_2)(\mathfrak{a}) + 1.$$

Proof. Since $N_\mathfrak{a} F_1$ is an abelian ℓ-extension of $K(E_2[\ell])$, by Lemma 2.4.4, $K(E_1[\ell]) \cap N_\mathfrak{a} F_1 =$

F_2. Since $\tau|_{F_2} = \tau_{\mathfrak{a}}\sigma_1|_{F_2}$, there is some $\sigma \in G_K$ such that

$$\sigma = \tau \text{ on } K(E_1[\ell]),$$

$$\sigma = \tau_{\mathfrak{a}}\sigma_1 \text{ on } N_{\mathfrak{a}}F_1.$$

Let $\mathfrak{p}$ be a prime whose Frobenius conjugacy class in $\mathrm{Gal}(K(E_1[\ell])N_{\mathfrak{a}}F_1/K)$ is the class of σ. Since Frobenius fixes $\boldsymbol{\mu}_\ell$ and $(\mathcal{O}_{K,\Sigma}^\times)^{1/\ell}$, we have that $\boldsymbol{\mu}_\ell$ and $(\mathcal{O}_{K,\Sigma}^\times)^{1/\ell}$ are contained in $K_{\mathfrak{p}}^\times$. Hence $\mathbf{N}\mathfrak{p} \equiv 1 \pmod{\ell}$ and the inclusion $K^\times \hookrightarrow K_{\mathfrak{p}}^\times$ sends $\mathcal{O}_{K,\Sigma}^\times$ into $(\mathcal{O}_{K,\mathfrak{p}}^\times)^\ell$, so $\mathfrak{p} \in \mathcal{P}$. By Lemma 1.3.4, evaluation of cocycles at a Frobenius element for $\mathfrak{p}$ in G_K induces an isomorphism

$$\mathcal{H}_\ell(K_{\mathfrak{p}}) = H^1_{\mathrm{ur}}(K_{\mathfrak{p}}, E_1[\ell]) \cong E_1[\ell]/(\tau - 1)E_1[\ell].$$

Thus $\mathfrak{p} \in \mathcal{P}_0(E_1)$. Again, by Lemma 1.3.4, evaluation of cocycles at a Frobenius element for $\mathfrak{p}$ in G_K induces an isomorphism

$$\mathcal{H}_\ell(K_{\mathfrak{p}}) = H^1_{\mathrm{ur}}(K_{\mathfrak{p}}, E_2[\ell]) \cong E_2[\ell]/(\tau - 1)E_2[\ell].$$

Thus $\mathfrak{p} \in \mathcal{P}_1(E_2)$.

Then by Proposition 2.2.6,

$$\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, E_2)(\mathfrak{a}\mathfrak{p}) = \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, E_2)(\mathfrak{a}) + 1.$$

□

Proposition 2.5.5. *Let* $t \geq \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, E_2)$.

(i) There is a finite set of primes $T \subseteq \mathcal{P}_0(E_1) \cap \mathcal{P}_1(E_2)$ such that

$$\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, E_2)(\mathfrak{a}) = t,$$

where $\mathfrak{a} := \prod_{\mathfrak{p} \in T} \mathfrak{p}$.

(ii) If T is as in (i), and L/K is a cyclic extension of K of degree ℓ that is T-ramified and Σ-split., then

$$\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(L/K, E_1) = \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, E_1), \quad \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(L/K, E_2) = t.$$

Proof. We apply Proposition 2.5.4 and induction on the cardinality of primes as in the proof of Proposition 9.17 in (**MRL**). This gives us (i).

Now if L/K is a cyclic extension of K of degree ℓ that is T-ramified and Σ-split, then by Proposition 1.5.3 and Lemma 2.1.6,

$$\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(L/K, E_1) = \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, E_1),$$

$$\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(L/K, E_2) = \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, E_2)(\mathfrak{a}) = t.$$

□

Chapter 3

Elliptic curves with complex multiplication

3.1 MORE SELMER STRUCTURES

Let E be an elliptic curve defined over a number field K. Assume that E has CM by $\mathcal{O}_M$, the full ring of integers of M. We assume that $M \subseteq K$. We assume that ℓ does not divide the discriminant of $\mathcal{O}_M$. We also assume that ℓ is inert in M. Therefore, $\mathcal{O}_M/\ell$ is a field.

The following two lemmas show that these restrictions are not too severe.

Lemma 3.1.1. *Let E be an elliptic curve defined over K. Assume that E has CM by $M \subseteq K$. There is an elliptic curve E', defined over K and isogenous over K to E, such that* $\mathrm{End}_K(E') = \mathcal{O}_M$.

Proof. This is Proposition 5.3. in (**Ru**) □

Lemma 3.1.2. *Let $M_i = \mathbb{Q}(\sqrt{D_i})$ be two imaginary quadratic fields (not necessarily distinct). Then there are infinitely many primes ℓ such that ℓ is inert in both M_1 and M_2.*

Proof. Let σ be the nontrivial element of $\mathrm{Gal}(\mathbb{Q}(\sqrt{D_1}, \sqrt{D_2})/\mathbb{Q}\sqrt{D_1 D_2}) \cong \mathbb{Z}/2\mathbb{Z}$. If ℓ is a prime whose Frobenius in $\mathrm{Gal}(\mathbb{Q}(\sqrt{D_1}, \sqrt{D_2})/\mathbb{Q}\sqrt{D_1 D_2})$ is σ, then ℓ is inert in both M_1 and M_2. The Cebotarev Theorem shows that there are infinitely many such primes ℓ. □

Proposition 3.1.3. *Let E be an elliptic curve with CM by $\mathcal{O}_M$ where $M \subseteq K$. Then $E[\ell] \cong \mathcal{O}_M/\ell$ as $\mathcal{O}_M$-modules.*

Proof. This is Proposition 5.4. in (**Ru**). □

We assume that $\mathrm{Gal}(K(E[\ell])/K) \cong (\mathcal{O}_M/\ell)^\times$ for all the elliptic curves we discuss in this section. The following proposition shows that this restriction is not too severe.

Theorem 3.1.4. *Let K be a number field and let E/K be an elliptic curve and has CM by $\mathcal{O}_M$ where $M \subseteq K$. Then for all but finitely many primes ℓ,* $\mathrm{Gal}(K(E[\ell])/K)$
$\cong \mathrm{Aut}_{\mathcal{O}_M}(E[\ell]) \cong (\mathcal{O}_M/\ell)^\times$.

Proof. This is the Corollary to Theorem 5 in section 4.5 in (**Ser2**). □

Remark 3.1.5. If E has CM, then $\dim_{\mathbb{F}_\ell} H^1(K_\mathfrak{p}, E[\ell])$ and $\dim_{\mathbb{F}_\ell} H^1_{\mathrm{ur}}(K_\mathfrak{p}, E[\ell])$ are even.

Lemma 3.1.6. *If $\mathfrak{p}$ is a prime and $\dim_{\mathbb{F}_\ell} H^1(K_\mathfrak{p}, E[\ell]) = 4$, then there are exactly $\ell + 1$ different 1-dimensional isotropic $\mathcal{O}_M/\ell$ subspaces of $H^1(K_\mathfrak{p}, E[\ell])$.*

Proof. Let L be a cyclic extension of degree ℓ over K such that $\mathfrak{p}$ ramifies in L/K. Let $V := H^1(K_\mathfrak{p}, E[\ell]), W_1 := \mathcal{H}_\ell(K_\mathfrak{p})$ and $W_2 := \mathcal{H}_\ell(L_\mathfrak{p}/K_\mathfrak{p})$. By Proposition 1.4.7 and Proposition 1.4.8 and Remark 2.1.5, we know that W_1 and W_2 are two different 2-dimensional isotropic $\mathbb{F}_\ell$ subspaces of V. We will use these two to generate the other $\ell - 1$ isotropic subspaces.

Claim that there exist $v_1 \in W_1$ and $v_2 \in W_2$ such that $< v_1, v_2 >= 0$:
Assume that W_1 is spanned w_1 and w_1' over $\mathbb{F}_\ell$ and w_2 is a nonzero vector in W_2. If $<$

$w_1, w_2 >= 0$, then we just take $v_1 = w_1$ and $v_2 = w_2$. Else, let $\alpha := -\frac{<w_1', w_2>}{<w_1, w_2>}$. Then $< w_1' + \alpha w_1, w_2 >= 0$ and we can take $v_1 = w_1' + \alpha w_1$ and $v_2 = w_2$.

Note that we have W_1 is spanned by v_1 over $\mathcal{O}_M/\ell$, W_2 is spanned by v_2 over $\mathcal{O}_M/\ell$, and $< v_1, v_2 >= 0$. Now we can start to generate the other isotropic subspaces. Let $\{1, \alpha\}$ be a basis of $\mathcal{O}_M/\ell$ over $\mathbb{F}_\ell$. Define $w_{k+2} := v_1 + kv_2, 1 \leq k \leq \ell - 1$.

$$
\begin{aligned}
< w_{k+2}, w_{k+2} > &= 2k < v_1, v_2 >= 0, \\
< w_{k+2}, \alpha w_{k+2} > &=< v_1, \alpha v_1 > + k < v_1, \alpha v_2 > + k < v_2, \alpha v_1 > + k^2 < v_2, \alpha v_2 > \\
&= k < v_1, \alpha v_2 > + k < v_2, \alpha v_1 > \\
&= k < v_1, \alpha v_2 + \bar{\alpha} v_2 > \quad \text{(using Lemma 16.2(a) in [\textbf{Mi}])} \\
&= k < v_1, (\alpha + \bar{\alpha}) v_2 > \\
&= k(\alpha + \bar{\alpha}) < v_1, v_2 > \quad (\text{since } \ (\alpha + \bar{\alpha}) \in \mathbb{F}_\ell) \\
&= 0, \\
< \alpha w_{k+2}, \alpha w_{k+2} > &=< w_{k+2}, \bar{\alpha}\alpha w_{k+2} > \\
&= (\bar{\alpha}\alpha) < w_{k+2}, w_{k+2} > \quad (\text{since } \ \bar{\alpha}\alpha \in \mathbb{F}_\ell) \\
&= 0.
\end{aligned}
$$

Therefore, W_{k+2} spanned by w_{k+2} over $\mathcal{O}_M/\ell$ for $1 \leq k \leq \ell - 1$ are different 1-dimensional isotropic $\mathcal{O}_M/\ell$ subspaces of $V = H^1(K_\mathfrak{p}, E[\ell])$. Now we have $\ell + 1$ different 2-dimensional isotropic $\mathbb{F}_\ell$ subspaces of $H^1(K_\mathfrak{p}, E[\ell])$. By Lemma 3.7 in (**KMR**), there are at most $\ell + 1$ such subspaces. Therefore, we have exactly $\ell + 1$ such subspaces. □

Remark 3.1.7. If $\mathfrak{p} \in \mathcal{P}_2(E)$, by Neron-Ogg-Shafarevich and the fact that the Frobenius of $\mathfrak{p}$ fixes $E[\ell]$, we have $G_{K_\mathfrak{p}}$ acts trivially on $E[\ell]$ and $H^1(G_{K_\mathfrak{p}}, E[\ell]) = \mathrm{Hom}(G_{K_\mathfrak{p}}, E[\ell])$.

Lemma 3.1.8. *If $\mathfrak{p} \in \mathcal{P}$, then $\mathcal{O}_\mathfrak{p}^\times/(\mathcal{O}_\mathfrak{p}^\times)^\ell \cong \mathbb{Z}/\ell\mathbb{Z}$ and $K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^\ell \cong (\mathbb{Z}/\ell\mathbb{Z})^2$.*

Proof. First we prove that $\mathcal{O}_\mathfrak{p}^\times/(\mathcal{O}_\mathfrak{p}^\times)^\ell \cong \mathbb{Z}/\ell\mathbb{Z}$. Let $k_\mathfrak{p}$ be the residue field of $K_\mathfrak{p}$. Since

$\mathfrak{p} \in \mathcal{P} \subseteq \mathcal{Q}$, $k_{\mathfrak{p}}^{\times}/(k_{\mathfrak{p}}^{\times})^{\ell} \cong \mathbb{Z}/\ell\mathbb{Z}$. Consider the commutative diagram of exact sequences,

$$\begin{tikzcd}
1 \arrow[r] & 1+\mathfrak{p}\mathcal{O}_{\mathfrak{p}} \arrow[r] \arrow[d, "\ell"] & \mathcal{O}_{\mathfrak{p}}^{\times} \arrow[r] \arrow[d, "\ell"] & (\mathcal{O}/\mathfrak{p}\mathcal{O})^{\times} \arrow[r] \arrow[d, "\ell"] & 1 \\
1 \arrow[r] & 1+\mathfrak{p}\mathcal{O}_{\mathfrak{p}} \arrow[r] & \mathcal{O}_{\mathfrak{p}}^{\times} \arrow[r] & (\mathcal{O}/\mathfrak{p}\mathcal{O})^{\times} \arrow[r] & 1.
\end{tikzcd}$$

Since $1+\mathfrak{p}\mathcal{O}_{\mathfrak{p}}$ is a pro-p group where p is the residue characteristic of $\mathfrak{p}$, raising to the ℓ-th power is an isomorphism. Apply snake lemma, we have

$$0 \to \mathcal{O}_{\mathfrak{p}}^{\times}/(\mathcal{O}_{\mathfrak{p}}^{\times})^{\ell} \to k_{\mathfrak{p}}^{\times}/(k_{\mathfrak{p}}^{\times})^{\ell} \to 0.$$

Therefore, $\mathcal{O}_{\mathfrak{p}}^{\times}/(\mathcal{O}_{\mathfrak{p}}^{\times})^{\ell} \cong \mathbb{Z}/\ell\mathbb{Z}$.

Next we prove that $K_{\mathfrak{p}}^{\times}/(K_{\mathfrak{p}}^{\times})^{\ell} \cong (\mathbb{Z}/\ell\mathbb{Z})^2$. Consider the commutative diagram of exact sequences,

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{O}_{\mathfrak{p}}^{\times} \arrow[r] \arrow[d, "\ell"] & K_{\mathfrak{p}}^{\times} \arrow[r] \arrow[d, "\ell"] & \mathbb{Z} \arrow[r] \arrow[d, "\ell"] & 0 \\
0 \arrow[r] & \mathcal{O}_{\mathfrak{p}}^{\times} \arrow[r] & K_{\mathfrak{p}}^{\times} \arrow[r] & \mathbb{Z} \arrow[r] & 0.
\end{tikzcd}$$

Again we apply snake lemma, then we have

$$0 \to \mathcal{O}_{\mathfrak{p}}^{\times}/(\mathcal{O}_{\mathfrak{p}}^{\times})^{\ell} \to K_{\mathfrak{p}}^{\times}/(K_{\mathfrak{p}}^{\times})^{\ell} \to \mathbb{Z}/\ell\mathbb{Z} \to 0.$$

Therefore, $K_{\mathfrak{p}}^{\times}/(K_{\mathfrak{p}}^{\times})^{\ell} \cong (\mathbb{Z}/\ell\mathbb{Z})^2$. $\square$

Lemma 3.1.9. *Let $\mathfrak{p} \in \mathcal{P}_2(E)$. Let $\mathcal{L}$ be an extension of $K_{\mathfrak{p}}$ of degree ℓ. Then*

$$\mathcal{H}_{\ell}(\mathcal{L}/K_{\mathfrak{p}}) = H^1(\mathrm{Gal}(\mathcal{L}/K_{\mathfrak{p}}), E[\ell]) = \mathrm{Hom}(\mathrm{Gal}(\mathcal{L}/\mathcal{K}_{\mathfrak{p}}), E[\ell]).$$

Proof. Consider the following commutative diagram:

$$\begin{tikzcd} A_{\mathcal{L}}(K_{\mathfrak{p}})/\lambda_{\mathcal{L}}A_{\mathcal{L}}(K_{\mathfrak{p}}) \arrow[r, "f"] \arrow[d, "i"'] & A_{\mathcal{L}}(\mathcal{L})/\lambda_{\mathcal{L}}A_{\mathcal{L}}(\mathcal{L}) \arrow[d] \\ H^1(K_{\mathfrak{p}}, A_{\mathcal{L}}[\lambda_{\mathcal{L}}]) \arrow[r, "g"] & H^1(\mathcal{L}, A_{\mathcal{L}}[\lambda_{\mathcal{L}}]) \end{tikzcd}$$

where $A_{\mathcal{L}}$ and $\lambda_{\mathcal{L}}$ are defined as in §1.2. By Lemma 7.4. in (**MRL**), f is the zero map. Therefore, $\mathcal{H}_\ell(\mathcal{L}/K_{\mathfrak{p}}) = \mathrm{im}(i) \subseteq \ker(g) = H^1(\mathrm{Gal}(\mathcal{L}/K_{\mathfrak{p}}), E[\ell])$. Since they have the same cardinality, $\mathcal{H}_\ell(\mathcal{L}/K_{\mathfrak{p}}) = H^1(\mathrm{Gal}(\mathcal{L}/K_{\mathfrak{p}}), E[\ell])$. □

Lemma 3.1.10. *If* $\dim_{\mathbb{F}_\ell} H^1(K_{\mathfrak{p}}, E[\ell]) = 4$*, then there is a one to one correspondence between extensions* $\mathcal{L}$ *of* $K_{\mathfrak{p}}$ *of degree* ℓ *and 1-dimensional isotropic* $\mathcal{O}_M/\ell$ *subspaces* W *of* $H^1(K_{\mathfrak{p}}, E[\ell])$*. This correspondence satisfies that* $\mathcal{H}_\ell(\mathcal{L}/K_{\mathfrak{p}}) = W$*.*

Proof. Let $\mathfrak{p} \in \mathcal{P}_2(E)$. Then we know that $G_{K_{\mathfrak{p}}}$ acts trivially on $E[\ell]$. Define $K_{\mathfrak{p}}^{(\ell)}$ to be the maximal abelian extension of exponent ℓ of $K_{\mathfrak{p}}$ and $G_\ell := \mathrm{Gal}(K_{\mathfrak{p}}^{(\ell)}/K_{\mathfrak{p}})$. By local class field theory, $G_\ell \cong K_{\mathfrak{p}}^\times/(K_{\mathfrak{p}}^\times)^\ell \cong (\mathbb{Z}/\ell\mathbb{Z})^2$. Therefore, there are $\ell + 1$ field extensions of $K_{\mathfrak{p}}$ of degree ℓ. One of them is unramified, the others are ramified. By Proposition 1.4.8, we know that if $\mathcal{L}$ is an extension of $K_{\mathfrak{p}}$ of degree ℓ, then $\mathcal{H}_\ell(\mathcal{L}/K_{\mathfrak{p}})$ is an isotropic subspace of $H^1(K_{\mathfrak{p}}, E[\ell])$. We claim that if $\mathcal{L}_1$ and $\mathcal{L}_2$ are two different extensions of $K_{\mathfrak{p}}$ of degree ℓ, then $\mathcal{H}_\ell(\mathcal{L}_1/K_{\mathfrak{p}})$ and $\mathcal{H}_\ell(\mathcal{L}_2/K_{\mathfrak{p}})$ are two different 2-dimensional isotropic $\mathbb{F}_\ell$ subspaces. Let $H_1 := \mathrm{Gal}((K_{\mathfrak{p}}^{(\ell)}/\mathcal{L}_1)$ and $H_2 := \mathrm{Gal}((K_{\mathfrak{p}}^{(\ell)}/\mathcal{L}_2)$. Then by Lemma 3.1.9,

$$\begin{aligned} \mathcal{H}_\ell(\mathcal{L}_i/K_{\mathfrak{p}}) &= H^1(\mathrm{Gal}(\mathcal{L}_i/K_{\mathfrak{p}}), E[\ell]) \\ &= \mathrm{Hom}(\mathrm{Gal}(\mathcal{L}_i/K_{\mathfrak{p}}), E[\ell]) \\ &= \{f \in \mathrm{Hom}(G_\ell, E[\ell]) : H_i \subseteq \ker(f)\}. \end{aligned}$$

Therefore,

$$\begin{aligned}\mathcal{H}_\ell(\mathcal{L}_1/K_\mathfrak{p}) \cap \mathcal{H}_\ell(\mathcal{L}_2/K_\mathfrak{p}) &= \{f \in \mathrm{Hom}(G_\ell, E[\ell]) : H_1 \cup H_2 \subseteq \ker(f)\} \\ &= \{f \in \mathrm{Hom}(G_\ell, E[\ell]) : \ker(f) = G_\ell\} \\ &= \{0\}.\end{aligned}$$

By Lemma 3.1.6, comparing the numbers of field extensions and isotropic subspaces, we know that there is a one to one correspondence between the extensions of $K_\mathfrak{p}$ of degree ℓ and the 2-dimensional isotropic $\mathbb{F}_\ell$ subspaces of $H^1(K_\mathfrak{p}, E[\ell])$. □

Definition 3.1.11. Assume that $\dim_{\mathbb{F}_\ell} H^1(K_\mathfrak{p}, E[\ell]) = 4$. Let W be a 1-dimensional isotropic $\mathcal{O}_M/\ell$ subspace of $H^1(K_\mathfrak{p}, E[\ell])$. Then we define $\mathcal{L}_W$ to be the extension of $K_\mathfrak{p}$ of degree ℓ corresponding to W in Lemma 3.1.10.

Conversely, let $\mathcal{L}$ be an extension of $K_\mathfrak{p}$ of degree ℓ. Then we define $W_\mathcal{L}$ to be the isotropic subspace corresponding to $\mathcal{L}$.

Definition 3.1.12. Let $\mathfrak{a}$ and $\mathfrak{b}$ be products of primes in $\mathcal{P}$. Let $\{\mathfrak{p}_i\}_{i=1}^r \subseteq \mathcal{P}_2(E)$ and W_i be isotropic subspaces of $H^1(K_{\mathfrak{p}_i}, E[\ell])$. We also assume that $\mathfrak{a}, \mathfrak{b}$, and $\mathfrak{p}_i$ are coprime. Define

$$\mathrm{Sel}_\ell(K,E)^\mathfrak{b}_\mathfrak{a}(\prod_{i=1}^r W_i) := \left\{ c \in H^1(K, E[\ell]) : \begin{array}{lll} \mathrm{loc}_v(c) \in \mathcal{H}_\ell(K_v) & \text{if} & v \nmid \mathfrak{a}\mathfrak{b}\prod_{i=1}^r \mathfrak{p}_i \\ \mathrm{loc}_v(c) = 0 & \text{if} & v | \mathfrak{a} \\ \mathrm{loc}_v(c) \in W_i & \text{if} & v = \mathfrak{p}_i \end{array} \right\}.$$

If $\mathcal{O}_K$ shows up in the notation, we omit it. If there is no $\mathfrak{p}_i$'s, we also omit the W_i. The following are some examples.

If $\mathfrak{a} = \mathcal{O}_K$, we denote $\mathrm{Sel}_\ell(K,E)^\mathfrak{b}_{\mathcal{O}_K}(\prod_{i=1}^r W_i)$ by $\mathrm{Sel}_\ell(K,E)^\mathfrak{b}(\prod_{i=1}^r W_i)$, the relaxed-at-$\mathfrak{b}$ Selmer group.

If $\mathfrak{b} = \mathcal{O}_K$, we denote $\mathrm{Sel}_\ell(K,E)_{\mathfrak{a}}^{\mathcal{O}_K}(\prod_{i=1}^r W_i)$ by $\mathrm{Sel}_\ell(K,E)_{\mathfrak{a}}(\prod_{i=1}^r W_i)$, the strict-at-$\mathfrak{a}$ Selmer group.

If $\mathfrak{a} = \mathfrak{b} = \mathcal{O}_K$, we denote $\mathrm{Sel}_\ell(K,E)_{\mathcal{O}_K}^{\mathcal{O}_K}(\prod_{i=1}^r W_i)$ by $\mathrm{Sel}_\ell(K,E)(\prod_{i=1}^r W_i)$.

If there is no $\mathfrak{p}_i$'s, we have simply $\mathrm{Sel}_\ell(K,E)_{\mathfrak{a}}^{\mathfrak{b}}$.

Definition 3.1.13. Suppose T_0 and $T_1 = \{\mathfrak{p}_i\}_{i=1}^r$ are finite subsets of $\mathcal{P}$. For each i, let $\mathcal{L}_i$ be a cyclic extension of $K_{\mathfrak{p}_i}$ of degree ℓ. Let $\mathcal{L} := (\mathcal{L}_1, \mathcal{L}_2, \cdots, \mathcal{L}_r)$. We will say that an extension L/K has *splitting data* $(\Sigma, T_0, T_1, \mathcal{L})$ if every $v \in \Sigma$ splits completely in L/K, every $v \notin T_0 \cup T_1$ is unramified in L/K, and every $L_{\mathfrak{p}_i}$ (the completion of L above $\mathfrak{p}_i$) is $\mathcal{L}_i$.

Lemma 3.1.14. *Suppose T_0 and $T_1 = \{\mathfrak{p}_i\}_{i=1}^r$ are subsets of $\mathcal{P}_0(E)$. For all $\mathcal{L}$, if L/K is a cyclic extension of K of degree ℓ that has splitting data $(\Sigma, T_0, T_1, \mathcal{L})$, then*

$$\mathrm{Sel}_\ell(L/K,E) = \mathrm{Sel}_\ell(K,E).$$

Proof. This follows immediately from Proposition 1.5.3. □

Lemma 3.1.15. *Suppose $T_0 \subseteq \mathcal{P}_0(E)$ and $T_1 = \{\mathfrak{p}_i\}_{i=1}^r \subseteq \mathcal{P}_2(E)$. Let W_i be 1-dimensional isotropic $\mathcal{O}_M/\ell$ subspaces of $H^1(K_{\mathfrak{p}_i}, E[\ell])$. Let $\mathcal{L} := (\mathcal{L}_{W_1}, \mathcal{L}_{W_2}, \cdots, \mathcal{L}_{W_r})$. If L/K is a cyclic extension of K of degree ℓ that has splitting data $(\Sigma, T_0, T_1, \mathcal{L})$, then*

$$\mathrm{Sel}_\ell(L/K,E) = \mathrm{Sel}_\ell(K,E)(W).$$

Proof. By definition, $\mathrm{Sel}_\ell(L/K,E) = \{c \in H^1(K,E[\ell]) : \mathrm{loc}_{\mathfrak{p}}(c) \in \mathcal{H}_\ell(L_{\mathfrak{p}}/K_{\mathfrak{p}}) \text{ for every } \mathfrak{p}\}$. On the other hand,

$$\mathrm{Sel}_\ell(K,E)(W) := \left\{ \begin{array}{lll} c \in H^1(K,E[\ell]) : & \mathrm{loc}_{\mathfrak{p}}(c) \in \mathcal{H}_\ell(K_{\mathfrak{p}}) & \text{if} \quad \mathfrak{p} \nmid \prod_{i=1}^r \mathfrak{p}_i \\ & \mathrm{loc}_{\mathfrak{p}}(c) \in W_i & \text{if} \quad \mathfrak{p} = \mathfrak{p}_i \end{array} \right\}.$$

If $\mathfrak{p} \in T_0$, then $H^1(K, E[\ell]) = \mathcal{H}_\ell(K_\mathfrak{p}) = \mathcal{H}_\ell(L_\mathfrak{p}/K_\mathfrak{p}) = 0$. If $\mathfrak{p} \in T_1$, by Lemma 3.1.10, Definition 3.1.11 and Definition 3.1.13, $W_i = \mathcal{H}_\ell(\mathcal{L}_{W_i}/K_{\mathfrak{p}_i}) = \mathcal{H}_\ell(L_{\mathfrak{p}_i}/K_{\mathfrak{p}_i})$. If $\mathfrak{p} \notin T_0 \cup T_1$, by Lemma 1.3.4 (ii) and the fact that primes in Σ split in L, $\mathcal{H}_\ell(K_\mathfrak{p}) = \mathcal{H}_\ell(L_\mathfrak{p}/K_\mathfrak{p})$. Therefore, $\mathrm{Sel}_\ell(L/K, E) = \mathrm{Sel}_\ell(K, E)(W)$. $\square$

3.2 TWISTING TO INCREASE THE SELMER RANK

Let E be an elliptic curve defined over a number field K. If E has CM by M for some imaginary quadratic field M, then we assume that E has CM by $\mathcal{O}_M$ and $M \subseteq K$. Let ℓ be a fixed prime such that $\mathrm{Gal}(K(E[\ell])/K) \cong (\mathcal{O}_M/\ell)^\times$. We also assume that ℓ does not divide the discriminant of $\mathcal{O}_M$. Let Σ be defined as in §1.4.

If $c \in H^1(K, E[\ell])$ and $\sigma \in G_K$, let

$$c(\sigma) \in E[\ell]/(\sigma - 1)E[\ell]$$

denote the image of σ under any cocycle representing c. This is well-defined.

Definition 3.2.1. Recall that $F_1 := K(\boldsymbol{\mu}_\ell, (\mathcal{O}_{K,\Sigma}^\times)^{1/\ell})$. Suppose $\sigma \in G_{F_1(E[\ell])}$.

Let $\{\mathfrak{p}_i\}_{i=1}^r \subseteq \mathcal{P}_2(E)$ and W_i be isotropic subspaces of $H^1(K_{\mathfrak{p}_i}, E[\ell])$. Let $W := \prod_{i=1}^r W_i \subseteq \prod H^1(K_{\mathfrak{p}_i}, E[\ell])$. If $c \in \mathrm{Sel}_\ell(K, E)(W)$, let

$$\tilde{c} : G_{K(E[\ell])} \to E[\ell]/(\sigma - 1)E[\ell] = E[\ell]$$

be the restriction of c to $G_{K(E[\ell])}$. Let N_W be the abelian extension of $K(E[\ell])$ fixed by $\cap_{c \in \mathrm{Sel}_\ell(K,E)(W)} \ker(\tilde{c})$.

Lemma 3.2.2. *Suppose $\sigma \in G_{F_1(E[\ell])}$. Let $\{\mathfrak{p}_i\}_{i=1}^r \subseteq \mathcal{P}_2(E)$ and W_i be isotropic subspaces of $H^1(K_{\mathfrak{p}_i}, E[\ell])$. Let $W := \prod_{i=1}^r W_i$. Let N_W be as in Definition* 3.2.1. *Assume that $\mathfrak{p}$ is a*

prime that splits completely in $N_W F_1/K$. Then $\mathfrak{p} \in \mathcal{P}_2(E)$ and $\mathrm{loc}_{\mathfrak{p}}(\mathrm{Sel}_\ell(K,E)(W)) = 0$.

Proof. Since $\mathfrak{p}$ splits completely in $N_W F_1/K$, we have that $\boldsymbol{\mu}_\ell$ and $(\mathcal{O}_{K,\Sigma}^\times)^{1/\ell}$ are contained in $K_{\mathfrak{p}}^\times$. Hence $\mathbf{N}\mathfrak{p} \equiv 1 \pmod{\ell}$ and the inclusion $K^\times \hookrightarrow K_{\mathfrak{p}}^\times$ sends $\mathcal{O}_{K,\Sigma}^\times$ into $(\mathcal{O}_{K,\mathfrak{p}}^\times)^\ell$, so $\mathfrak{p} \in \mathcal{P}$.

By Lemma 1.3.4, evaluation of cocycles at a Frobenius element for $\mathfrak{p}$ in G_K induces an isomorphism

$$\mathcal{H}_\ell(K_{\mathfrak{p}}) = H^1_{\mathrm{ur}}(K_{\mathfrak{p}}, E[\ell]) \cong E[\ell].$$

Thus $\mathfrak{p} \in \mathcal{P}_2(E)$. Furthermore, if $c \in \mathrm{Sel}_\ell(K,E)(W)$, $\mathrm{loc}_{\mathfrak{p}}(c) = c(1) = 0$ via the following maps

$$\mathrm{loc}_{\mathfrak{p}} : \mathrm{Sel}_\ell(K,E)(W) \to \mathcal{H}_\ell(K_{\mathfrak{p}}) \cong H^1_{\mathrm{ur}}(K, E[\ell]) \cong E[\ell].$$

Therefore, $\mathrm{loc}_{\mathfrak{p}}(\mathrm{Sel}_\ell(K,E)(W)) = 0$. □

Proposition 3.2.3. *Let $\mathfrak{p} \in \mathcal{P}_2(E)$. Let $\{\mathfrak{p}_i\}_{i=1}^r \subseteq \mathcal{P}_2(E)$ and W_i be isotropic subspaces of $H^1(K_{\mathfrak{p}_i}, E[\ell])$. Let $W = \prod_{i=1}^r W_i$. Then $\mathrm{loc}_{\mathfrak{p}}(\mathrm{Sel}_\ell(K,E)^{\mathfrak{p}}(W))$ is an isotropic subspace of $H^1(K_{\mathfrak{p}}, E[\ell])$.*

Proof. Let M_K be a complete set of primes of $\mathcal{O}_K$. Let $c, d \in \mathrm{Sel}_\ell(K,E)^{\mathfrak{p}}(W) \subset H^1(K, E[\ell])$. By Theorem 1.4.5,

$$\sum_{v \in M_K} < \mathrm{loc}_v(c), \mathrm{loc}_v(d) >_v = 0.$$

By Defininion 3.1.12, $\mathrm{loc}_{\mathfrak{p}_i}(c)$ and $\mathrm{loc}_{\mathfrak{p}_i}(d) \in W_i$. Therefore, we have $< \mathrm{loc}_{\mathfrak{p}_i}(c), \mathrm{loc}_{\mathfrak{p}_i}(d) >_{\mathfrak{p}_i} = 0$. For $v \nmid \mathfrak{p} \prod_{i=1}^r \mathfrak{p}_i$, $\mathrm{loc}_v(c)$ and $\mathrm{loc}_v(d) \in \mathcal{H}_\ell(K_v)$. Therefore, by Proposition 1.4.7, we have $< \mathrm{loc}_v(c), \mathrm{loc}_v(d) >_v = 0$ for $v \nmid \mathfrak{p} \prod_{i=1}^r \mathfrak{p}_i$.

Hence, focus on $\mathfrak{p}$ alone, we have $< \mathrm{loc}_{\mathfrak{p}}(c), \mathrm{loc}_{\mathfrak{p}}(d) >_{\mathfrak{p}} = 0$ and $\mathrm{loc}_{\mathfrak{p}}(\mathrm{Sel}_\ell(K,E)^{\mathfrak{p}}(W))$ is an isotropic subspace. □

Proposition 3.2.4. *Suppose $\sigma \in G_{F_1(E[\ell])}$. Let $\{\mathfrak{p}_i\}_{i=1}^r \subseteq \mathcal{P}_2(E)$ and W_i be isotropic subspaces of $H^1(K_{\mathfrak{p}_i}, E[\ell])$. Let $W = \prod_{i=1}^r W_i$. Let N_W be as in Definition 3.2.1. If $\mathfrak{p}$ is a prime that splits completely in $N_W F_1/K$, define $W_{r+1} := \mathrm{loc}_{\mathfrak{p}}(\mathrm{Sel}_\ell(K,E)^{\mathfrak{p}}(W))$ an isotropic subspace of $H^1(K_{\mathfrak{p}}, E[\ell])$. Then*

$$\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K,E)(W \times W_{r+1}) = \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K,E)(W) + 2.$$

Proof. By Lemma 3.2.2, since $\mathfrak{p}$ splits completely in $N_W F_1/K$, $\mathfrak{p} \in \mathcal{P}_2(E)$ and $\mathrm{loc}_{\mathfrak{p}}(\mathrm{Sel}_\ell(K,E)(W)) = 0$. Consider the exact sequence

$$0 \to \mathrm{Sel}_\ell(K,E)_{\mathfrak{p}}(W) \to \mathrm{Sel}_\ell(K,E)(W) \to \mathcal{H}_\ell(K_{\mathfrak{p}}).$$

By our choice of $\mathfrak{p}$ the right-hand map is zero and we get

$$\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K,E)_{\mathfrak{p}}(W) = \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K,E)(W). \tag{3.2.5}$$

Then we consider the exact sequences

$$\begin{aligned} 0 &\longrightarrow \mathrm{Sel}_\ell(K,E)_{\mathfrak{p}}(W) \longrightarrow \mathrm{Sel}_\ell(K,E)(W \times W_{r+1}) \longrightarrow W_{r+1} \\ 0 &\to \mathrm{Sel}_\ell(K,E)(W \times W_{r+1}) \longrightarrow \mathrm{Sel}_\ell(K,E)^{\mathfrak{p}}(W) \longrightarrow H^1(K_{\mathfrak{p}}, E[\ell])/W_{r+1}. \end{aligned} \tag{3.2.6}$$

Global duality (see for example Theorem 2.3.4 in (**MR2**)) tells us that the images of the two right-hand maps are orthogonal complements of each other under the local Tate pairing. By the definition of W_{r+1}, the lower right-hand map in (3.2.6) is zero so the upper right-hand map in (3.2.6) is surjective. Thus we get

$$\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K,E)(W \times W_{r+1}) = \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K,E)_{\mathfrak{p}}(W) + 2. \tag{3.2.7}$$

Combine (3.2.5) and (3.2.7), we get

$$\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K,E)(W \times W_{r+1}) = \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K,E)(W) + 2.$$

□

3.3 FIELDS GENERATED BY TORSION POINTS OF ELLIPTIC CURVES

Now we consider elliptic curves with complex multiplication. If E has CM by M for some imaginary quadratic field M, then we assume that E has CM by $\mathcal{O}_M$ ($\mathrm{End}_{\bar{K}}(E) = \mathcal{O}_M$) and $M \subseteq K$. We also assume that ℓ does not divide the discriminant of $\mathcal{O}_M$.

Let K^{ab} denote the maximal abelian extension of K and $[\cdot, K^{\mathrm{ab}}/K]$ the Artin map of global class field theory.

Theorem 3.3.1. *There is a Hecke character*

$$\psi = \psi_E : \mathbb{A}_K^\times / K^\times \to \mathbb{C}^\times$$

with the following properties.

(i) If $x \in \mathbb{A}_K^\times$ and $y = \mathbf{N}_{K/M} x \in \mathbb{A}_M^\times$, then

$$\psi(x)\mathcal{O}_M = y_\infty^{-1}(y\mathcal{O}_M) \subset \mathbb{C}.$$

(ii) If $x \in \mathbb{A}_K^\times$ is a finite idele (i.e., the archimedean component is 1) and $\mathfrak{p}$ is a prime of

M, then $\psi(x)(\mathbf{N}_{K/M}x)_{\mathfrak{p}}^{-1} \in \mathcal{O}_{M,\mathfrak{p}}^{\times}$ and for every $P \in E[\mathfrak{p}^{\infty}]$

$$[x, K^{\mathrm{ab}}/K]P = \psi(x)(\mathbf{N}_{K/M}x)_{\mathfrak{p}}^{-1}P.$$

(iii) If $\mathfrak{q}$ is a prime of K and $\mathcal{U}_{\mathfrak{q}}$ denotes the local units in the completion of K at $\mathfrak{q}$, then

$$\psi(\mathcal{U}_{\mathfrak{q}}) = 1 \Leftrightarrow E \text{ has good reduction at } \mathfrak{q}.$$

Proof. This is Theorem 5.15 in (**Ru**). □

Let $\mathfrak{f} = \mathfrak{f}_E$ denote the conductor of the Hecke character ψ of Theorem 3.3.1. We can view ψ as a character of fractional ideals of K prime to $\mathfrak{f}$ in the usual way.

Corollary 3.3.2. *As a character on ideals, ψ satisfies*

(i) if $\mathfrak{b}$ is an ideal of K prime to $\mathfrak{f}$, then $\psi(\mathfrak{b})\mathcal{O}_M = \mathbf{N}_{K/M}\mathfrak{b}$.

(ii) if $\mathfrak{q}$ is a prime of K not dividing $\mathfrak{f}$ and $\mathfrak{b}$ is an ideal of $\mathcal{O}_M$ prime to $\mathfrak{q}$, then $[\mathfrak{q}, K(E[\mathfrak{b}])/K]$ acts on $E[\mathfrak{b}]$ by multiplication by $\psi(\mathfrak{q})$.

(iii) if $\mathfrak{q}$ is a prime of K where E has good reduction and $q = \mathbf{N}_{K/\mathbb{Q}}\mathfrak{q}$, then $\psi(\mathfrak{q}) \in \mathcal{O}_M$ reduces modulo $\mathfrak{q}$ to the Frobenius endomorphism φ_q of $\tilde{E}$.

Proof. This is Corollary 5.16. in (**Ru**). □

If $\mathfrak{m}$ is an ideal of $\mathcal{O}_M$, then define $K^{\mathfrak{m}}$ to be the ray class field modulo $\mathfrak{m}$.

Lemma 3.3.3. *Let E be an elliptic curve defined over a number field K. Assume that E has complex multiplication by $\mathcal{O}_M$. Let $\mathfrak{m}$ be an ideal of $\mathcal{O}_M$. Let ℓ be a prime such that $\mathrm{Gal}(K(E[\ell])/K) \cong (\mathcal{O}_M/\ell)^{\times}$, ℓ is coprime to $\mathfrak{m}$, ℓ is unramified in $K/\mathbb{Q}$, ℓ is inert in M, and E has good reduction at all $\lambda|\ell$. Then $K(E[\ell])/K$ and $K^{\mathfrak{m}}$ are linearly disjoint over K.*

Proof. We prove that $K(E[\ell])/K$ and $K^{\mathfrak{m}}$ are linearly disjoint over K by showing that for $\lambda|\ell$, λ is totally ramified in $K(E[\ell])/K$:

$$\begin{tikzcd} K(E[\ell]) \arrow[dr, dash] & & K^{\mathfrak{m}} \arrow[dl, dash] \\ & K & \end{tikzcd}$$

Consider f to be the composition of the following maps:

$$f : \mathbb{A}_K^\times \to \mathrm{Gal}(K^{ab}/K) \twoheadrightarrow \mathrm{Aut}_{\mathcal{O}_M}(E[\ell]) \cong (\mathcal{O}_M/\ell)^\times.$$

The first map is the norm residue. And we call the second map $g : \mathrm{Gal}(K^{ab}/K) \cong \mathrm{Aut}_{\mathcal{O}_M}(E[\ell])$ and the third map $h : \mathrm{Aut}_{\mathcal{O}_M}(E[\ell]) \cong (\mathcal{O}_M/\ell)^\times$. Let $\mathcal{U}_\lambda$ denote the local units of K_λ and $I_\lambda(K^{\mathrm{ab}}/K)$ denote the inertia subgroup. Let $x \in \mathcal{U}_\lambda$. By Theorem 3.3.1 (ii) and (iii),

$$[x, K^{\mathrm{ab}}/K]P = (\mathbf{N}_{K/M}x)_\ell^{-1}P, \quad (\mathbf{N}_{K/M}x)_\ell^{-1} \in \mathcal{O}_{M,\ell}^\times.$$

Therefore, we have:

$$\begin{aligned} f : \quad & \mathcal{U}_\lambda \longrightarrow \mathcal{O}_{M,\ell}^\times \longrightarrow (\mathcal{O}_M/\ell)^\times. \\ & x \longrightarrow (\mathbf{N}_{K/M}x)_\ell^{-1} \longrightarrow f(x) \end{aligned}$$

The first map is surjective since ℓ is unramified in K/M. The second map is surjective since it is the reduction. The composition $f|_{\mathcal{U}_\lambda}$ is hence surjective to $(\mathcal{O}_M/\ell)^\times$ and $g|_{I_\lambda(K^{\mathrm{ab}}/K)}$ is also surjective to $\mathrm{Aut}_{\mathcal{O}_M}(E[\ell])$.

The projection $\pi : \mathrm{Gal}(K^{\mathrm{ab}}/K) \to \mathrm{Gal}(K(E[\ell])/K)$ induces $\pi' : I_\lambda(K^{\mathrm{ab}}/K) \to \mathrm{Gal}(K(E[\ell])/K)$.

Now consider the diagram:

$$\begin{tikzcd} I_\lambda(K^{\mathrm{ab}}/K) \arrow[rr, "g"] \arrow[dr, "\pi'"'] & & \mathrm{Aut}_{\mathcal{O}_M}(E[\ell]) \\ & \mathrm{Gal}(K(E[\ell])/K) \arrow[ur, "\cong"'] & \end{tikzcd}$$

The facts that $\mathrm{Gal}(K(E[\ell])/K) \cong \mathrm{Aut}_{\mathcal{O}_M}(E[\ell])$ and the top map $g : I_\lambda(K^{\mathrm{ab}}/K) \to \mathrm{Aut}_{\mathcal{O}_M}(E[\ell])$ is surjective tell us that π' is surjective. Therefore, $\mathrm{Gal}(K(E[\ell])/K) = I_\lambda(K(E[\ell])/K)$ and λ is totally ramified in $K(E[\ell])/K$.

Now we know that λ is totally ramified in $K(E[\ell])/K$ but unramified in $K^{\mathfrak{m}}/K$. Therefore, $K(E[\ell])/K$ and $K^{\mathfrak{m}}$ are linearly disjoint over K. □

Definition 3.3.4. Let E_1 and E_2 be elliptic curves defined over a number field K. Assume that E_1 and E_2 both have complex multiplication by $\mathcal{O}_M$ where $M \subseteq K$. There exist Hecke characters ψ_1 and ψ_2 for E_1 and E_2 respectively. Assume that ψ_1 has conductor $\mathfrak{f}_1$, and ψ_2 has conductor $\mathfrak{f}_2$. We view ψ_1 and ψ_2 as characters of conductor $\mathfrak{f} := \mathfrak{f}_1 \cdot \mathfrak{f}_2$.

Let $J_K^{\mathfrak{f}} :=$ the group of all fractional ideals relatively prime to $\mathfrak{f}$ and $P_K^{\mathfrak{f}} :=$ the group of all pricipal ideals (a) such that $a \equiv 1 (\mathrm{mod}\ \mathfrak{f})$ and a totally positive. Let $Cl_K^{\mathfrak{f}} := J_K^{\mathfrak{f}}/P_K^{\mathfrak{f}}$ and $K^{\mathfrak{f}} :=$ the ray class field modulo $\mathfrak{f}$. By class field theory, there is an isomorphism between $J_K^{\mathfrak{f}}/P_K^{\mathfrak{f}}$ and $\mathrm{Gal}(K^{\mathfrak{f}}/K)$.

If $\mathfrak{a} \in P_K^{\mathfrak{f}}$, then $\mathfrak{a} = (\alpha)$ for some $\alpha \equiv 1 \pmod{\mathfrak{f}}$. We have $\psi_1(\mathfrak{a}) = \psi_2(\mathfrak{a}) = \mathbf{N}_{K/M}(\alpha)$ and $\psi_1(\mathfrak{a})\psi_2^{-1}(\mathfrak{a}) = 1$. Define $\epsilon := \psi_1\psi_2^{-1}$. We can view ϵ as a character on $Cl_K^{\mathfrak{f}}$.

Proposition 3.3.5. *If $\epsilon = 1$, then $\psi_1 = \psi_2$ and E_1 is isogenous to E_2 over K.*

Proof. This is Theorem 5 in (**Shi**). □

Theorem 3.3.6. *Let E_1 and E_2 be elliptic curves defined over a number field K. Assume*

that E_1 and E_2 both have complex multiplication by $\mathcal{O}_M$ where $M \subseteq K$. If E_1 is not isogenous to E_2 over K, then for infinitely many primes ℓ, $K(E_1[\ell]) \neq K(E_2[\ell])$ and ℓ is inert in M.

Proof. Assume that E_1 is not isogenous to E_2 over K.

By Proposition 3.1.4, for all but finitely many ℓ, $\mathrm{Gal}(K(E_i[\ell])/K) \cong (\mathcal{O}_M/\ell)^\times$ for $i \in \{1, 2\}$. For these ℓ and for any place v of K, let $(\sigma_i)_v$ be the Frobenius element of v in $\mathrm{Gal}(K(E_i[\ell])/K) \cong (\mathcal{O}_M/\ell)^\times$. Then $\psi_i(v) \in \mathcal{O}_M$ and its reduction modulo ℓ equals to $(\sigma_i)_v \in (\mathcal{O}_M/\ell)^\times$. by Corollary 3.3.2(iii). If $\epsilon = 1$, then E_1 is isogenous to E_2 over K by Proposition 3.3.5. This is a contradiction to our assumption. Therefore, there exists some class $\mathcal{C} \in Cl_K^{\mathfrak{f}} \cong \mathrm{Gal}(K^{\mathfrak{f}}/K)$ such that $\epsilon(\mathcal{C}) \neq 1$.

By Lemma 3.1.2 and Proposition 3.1.4, for infinitely many primes ℓ, $\mathrm{Gal}(K(E_i[\ell])/K)$ $\cong (\mathcal{O}_M/\ell)^\times$, ℓ is coprime to $\mathfrak{f}$, ℓ is unramified in $K/\mathbb{Q}$, ℓ is inert in M, E_1 and E_2 both have good reduction at all $\lambda|\ell$, and $\ell \nmid (\epsilon(\mathcal{C})^{-1} - 1)$. We will prove that for these ℓ, $K(E_1[\ell]) \neq K(E_2[\ell])$.

By Lemma 3.3.3, $K(E_1[\ell])/K$ and $K^{\mathfrak{f}}$ are linearly disjoint over K. We can find a place v such that the Frobenius element $\sigma_v = 1$ on $E_1[\ell]$ and $\sigma_v = \phi_{\mathfrak{f}}(\mathcal{C})$ on $K^{\mathfrak{f}}$ where $\phi_{\mathfrak{f}}$ is defined to be the isomorphism $J_K^{\mathfrak{f}}/P_K^{\mathfrak{f}} \cong \mathrm{Gal}(K^{\mathfrak{f}}/K)$. By Corollary 3.3.2(iii) and the fact that the Frobenius endomorphism of $\tilde{E}$ corresponds to the Frobenius element σ_v, that is to say, $\psi_1(v) \equiv 1 \pmod{\ell}$ and $\psi_2(v) \equiv \epsilon(v)^{-1} = \epsilon(\mathcal{C})^{-1} \not\equiv 1 \pmod{\ell}$. Therefore, by Corollary 3.3.2 (ii) and (iii), σ_v fixes $K(E_1[\ell])$ but not $K(E_2[\ell])$, so $K(E_1[\ell]) \neq K(E_2[\ell])$. □

Theorem 3.3.7. *Let E_1 and E_2 be elliptic curves defined over a number field K. Assume that E_1 has complex multiplication by $\mathcal{O}_{M_1}$ where $M_1 \subseteq K$. Assume that E_2 has complex multiplication by $\mathcal{O}_{M_2}$ where $M_2 \subseteq K$. Assume that $M_1 \neq M_2$. Then for infinitely many primes ℓ, $K(E_1[\ell]) \neq K(E_2[\ell])$ and ℓ is inert in both M_1 and M_2.*

Proof. Consider those primes ℓ which are inert in both M_1 and M_2, unramified in $K/\mathbb{Q}$,

and E_1 and E_2 both have good reduction. By Lemma 3.1.2, there are infinitely many such primes ℓ. Pick any prime ℓ from this set. We will prove that $K(E_1[\ell]) \neq K(E_2[\ell])$.

Consider the following diagram:

$$\begin{tikzcd}
K(E_1[\ell]) \arrow[dr, dash] & & K(E_2[\ell]) \arrow[dl, dash] \\
& K \arrow[d, dash] & \\
& M_1M_2 \arrow[dl, dash, "<\sigma_1>"'] \arrow[dr, dash, "<\sigma_2>"] & \\
M_1 \arrow[dr, dash] & & M_2 \arrow[dl, dash] \\
& \mathbb{Q} &
\end{tikzcd}$$

Define notation $\mathcal{U}_{F,\ell} := \Pi_{\lambda|\ell}\mathcal{O}_{F,\lambda}^{\times} \subseteq \mathbb{A}_F^{\times}$ for any field F. For $i = 1$ or 2, the map

$$\pi_i := \pi \circ \mathbf{N}_{M_1M_2/M_i} : \mathcal{U}_{M_1M_2,\ell} \to \mathcal{U}_{M_i,\ell} \xrightarrow{\pi} (\mathcal{O}_{M_i}/\ell)^{\times}$$

is surjective since ℓ is unramified in $K/\mathbb{Q}$.

First choose $z \in \mathcal{U}_{M_1M_2,\ell}$ such that

$$\pi_2(z) \in (\mathcal{O}_{M_2}/\ell)^{\times} \setminus (\mathbb{Z}/\ell\mathbb{Z})^{\times}. \tag{3.3.8}$$

Take $y = z/z^{\sigma_1} \in \mathcal{U}_{M_1M_2,\ell}$ where $\mathrm{Gal}(M_1M_2/M_1) = \langle\sigma_1\rangle$, then

$$\pi_1(y) = \pi_1(z/z^{\sigma_1}) = 1,$$

$$\pi_2(y) = \pi_2(z)/\pi_2(z)^{\sigma_1} \tag{3.3.9}$$

Consider the action of σ_1 on $(\mathcal{O}_{M_2}/\ell)$, σ_1 is the generator of the decomposition group of ℓ which is isomorphic to $\mathrm{Gal}((\mathcal{O}_{M_2}/\ell)/(\mathbb{Z}/\ell\mathbb{Z}))$. By (3.3.8) and (3.3.9), we know that $\pi_2(y) \not\equiv 1 \pmod{\ell}$.

There exists $x \in \mathcal{U}_{K,\ell}$ such that $\mathbf{N}_{K/M_1M_2} = y$ since ℓ is unramified in $K/\mathbb{Q}$. Let $\sigma := [x, K^{\mathrm{ab}}/K]$. By Theorem 3.3.1 (ii) and (iii), σ acts on $E_i[\ell]$ by $\pi_i(y)^{-1}$. Therefore, σ acts trivially on $K(E_1[\ell])$ but nontrivially on $K(E_2[\ell])$. So, $K(E_1[\ell]) \neq K(E_2[\ell])$. □

Theorem 3.3.10. *Let E_1 and E_2 be elliptic curves defined over a number field K. Assume that E_1 has no complex multiplication. Assume that E_2 has complex multiplication by $\mathcal{O}_M$ where $M \subseteq K$. Then for all but finitely many primes ℓ, $K(E_1[\ell]) \neq K(E_2[\ell])$.*

Proof. By Proposition 2.1.1 and Proposition 3.1.4, for all but finitely many primes ℓ, $\mathrm{Gal}(K(E_1[\ell])/K) \cong \mathrm{GL}_2(\mathbb{F}_\ell)$ and $\mathrm{Gal}(K(E_2[\ell])/K) \cong (\mathcal{O}_M/\ell)^\times$. Therefore, for such ℓ, $K(E_1[\ell]) \neq K(E_2[\ell])$. □

3.4 LINEARLY DISJOINT FIELDS

In this section, we prove that some important fields are linearly disjoint. Fix E_1 and E_2 two curves defined over a number field K. Assume that $\ell \geq 5$. Assume that $\mathrm{Gal}(K(E_i[\ell])/K) \cong \mathrm{Aut}_{\mathrm{End}_{\bar{K}}(E_i)}(E_i[\ell])$ for $i \in \{1, 2\}$. If E_i has CM by $\mathcal{O}_{M_i}$ we further assume that ℓ is inert in M_i, $M_i \subseteq K$ and ℓ does not divide the discriminant of $\mathcal{O}_{M_i}$.

As in §2.4, let $F_2 := K(E_1[\ell]) \cap K(E_2[\ell])$.

Lemma 3.4.1. *Assume that E_1 has no complex multiplication and E_2 has complex multiplication. Then $F_2 := K(E_1[\ell]) \cap K(E_2[\ell]) = K(\boldsymbol{\mu}_\ell)$.*

Proof. In this case,

$$\begin{tikzcd}
K(E_1[\ell]) \arrow[dr, dash, "\mathrm{SL}_2(\mathbb{F}_\ell)"'] & & K(E_2[\ell]) \arrow[dl, dash, "\mathcal{C}_{\ell+1}"] \\
& K(\boldsymbol{\mu}_\ell) &
\end{tikzcd}$$

$\mathrm{Gal}(K(E_2[\ell])/K(\boldsymbol{\mu}_\ell)) \cong \mathcal{C}_{\ell+1}$ is a cyclic group of order $\ell+1$. But $\mathrm{Gal}(K(E_1[\ell])/K(\boldsymbol{\mu}_\ell)) \cong \mathrm{SL}_2(\mathbb{F}_\ell)$ has no nontrivial abelian quotient. Therefore, $F_2 = K(E_1[\ell]) \cap K(E_2[\ell]) = K(\boldsymbol{\mu}_\ell)$.

□

Lemma 3.4.2. *Assume that E_2 has CM by $\mathcal{O}_{M_2}$. There is no nontrivial Galois ℓ-extension of F_2 in $K(E_1[\ell])$.*

Proof.

- If E_1 has no CM, then there is no nontrivial ℓ-extension of F_2 in $K(E_1[\ell])$ by Lemma 3.4.1 and the fact that $\mathrm{SL}_2(\mathbb{F}_\ell)$ has no quotient of order ℓ.
- If E_1 has CM, then $\mathrm{Gal}(K(E_1[\ell])/F_2)$ is a subgroup of $\mathcal{C}_{\ell+1}$ and there is no nontrivial ℓ-extension of F_2 in $K(E_1)[\ell]$.

□

Lemma 3.4.3. *Suppose that N is an abelian ℓ-extension of $K(E_2[\ell])$. Assume $K(E_1[\ell]) \neq K(E_2[\ell])$. Then $K(E_1[\ell]) \cap N = F_2$.*

Proof. Consider the following diagram:

$$\begin{tikzcd}
& K(E_1[\ell], E_2[\ell]) \arrow[dl, dash] \arrow[dr, dash] & & N \arrow[dl, dash] \\
K(E_1[\ell]) \arrow[dr, dash] & & K(E_2[\ell]) \arrow[dl, dash] & \\
& F_2 & &
\end{tikzcd}$$

By the definition of F_2, $\mathrm{Gal}(K(E_1[\ell], E_2[\ell])/K(E_2[\ell])) \cong \mathrm{Gal}(K(E_1[\ell])/F_2)$. Therefore, by

Lemma 3.4.2,

$$K(E_1[\ell], E_2[\ell]) \cap N = K(E_2[\ell]). \tag{3.4.4}$$

By (3.4.4),we have

$$\begin{aligned} K(E_1[\ell]) \cap N &\subseteq K(E_1[\ell]) \cap K(E_1[\ell], E_2[\ell]) \cap N \\ &= K(E_1[\ell]) \cap K(E_2[\ell]) \\ &= F_2. \end{aligned}$$

□

3.5 FIX THE SELMER RANK OF E_1 AND INCREASE THE SELMER RANK OF E_2 SIMULTANEOUSLY

Assume that E_2 has CM by $\mathcal{O}_{M_2}$. In this section, let ℓ be a fixed prime such that $\ell \geq 5$, $\mathrm{Gal}(K(E_1[\ell])/K) \cong \mathrm{Aut}_{\mathrm{End}_{\bar{K}}(E_1)}(E_1[\ell])$, $\mathrm{Gal}(K(E_2[\ell])/K) \cong (\mathcal{O}_{M_2}/\ell)^\times$, $K(E_1[\ell]) \neq K(E_2[\ell])$. If E_i has complex multiplication by $\mathcal{O}_{M_i}$, assume in addition that ℓ is inert in M_i, $M_i \subseteq K$ and ℓ does not divide the discriminant of $\mathcal{O}_{M_i}$. Recall that Σ (associated to this ℓ) is defined as in §1.4.

Definition 3.5.1. Recall that $F_1 := K(\boldsymbol{\mu}_\ell, (\mathcal{O}_{K,\Sigma}^\times)^{1/\ell})$ and $F_2 := K(E_1[\ell]) \cap K(E_2[\ell])$.

If E_1 has no CM, let $\tau_1 \in G_{K(\boldsymbol{\mu}_\ell)}$ be an element that acts like $\begin{bmatrix} -1 & -1 \\ 0 & -1 \end{bmatrix}$ on $E_1[\ell]$. If E_1 has CM, let $\tau_1 \in G_{K(\boldsymbol{\mu}_\ell)}$ be a non-identity element in $\mathrm{Gal}(K(E_1[\ell])/F_2)$. Therefore, $\dim_{\mathbb{F}_\ell}(E_1[\ell]/(\tau_1 - 1)E_1[\ell]) = 0$.

Let $\tau_2 \in G_{K(\boldsymbol{\mu}_\ell)}$ be the identity map on $E_2[\ell]$. Therefore, $\dim_{\mathbb{F}_\ell}(E_2[\ell]/(\tau_2 - 1)E_2[\ell]) = 2$.

As Lemma 9.3 of (**MRL**), $K(E_2[\ell])$ and F_1 are linearly disjoint over $K(\boldsymbol{\mu}_\ell)$. Let $\sigma_1 \in G_K$ such that

$$\sigma_1 = \tau_2 \text{ on } K(E_2[\ell]),$$

$$\sigma_1 = 1 \text{ on } F_1 = K(\boldsymbol{\mu}_\ell, (\mathcal{O}_{K,\Sigma}^\times)^{1/\ell}).$$

Let $\{\mathfrak{p}_i\}_{i=1}^r \subseteq \mathcal{P}_2(E_2)$ and W_i be isotropic subspaces of $H^1(K_{\mathfrak{p}_i}, E_2[\ell])$. Let $W := \prod_{i=1}^r W_i$. If $c \in \mathrm{Sel}_\ell(K, E_2)(W)$, let

$$\tilde{c} : G_{K(E_2[\ell])} \to E_2[\ell]$$

be the restriction of c to $G_{K(E_2[\ell])}$. Let N_W be the abelian extension of $K(E_2[\ell])$ fixed by $\cap_{c \in \mathrm{Sel}_\ell(K,E_2)(W)} \ker(\tilde{c})$.

Proposition 3.5.2. *Let $\{\mathfrak{p}_i\}_{i=1}^r \subseteq \mathcal{P}$ and W_i be isotropic subspaces of $H^1(K_{\mathfrak{p}_i}, E_2[\ell])$. Let $W := \prod_{i=1}^r W_i$. Then there is a prime $\mathfrak{p}_{r+1}$ in $\mathcal{P}_0(E_1) \cap \mathcal{P}_2(E_2)$ and W_{r+1} an isotropic subspace of $H^1(K_{\mathfrak{p}_{r+1}}, E_2[\ell])$ such that*

$$\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, E_2)(W \times W_{r+1}) = \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, E_2)(W) + 2.$$

Proof. Since $N_W F_1$ is an abelian ℓ-extension of $K(E_2[\ell])$, by Lemma 3.4.3, $K(E_1[\ell]) \cap N_W F_1 = F_2$. We can see that $\tau_1|_{F_2} = 1$ by Lemma 3.4.1. Therefore, there is some $\sigma \in G_K$ such that

$$\sigma = \tau_1 \text{ on } K(E_1[\ell]),$$

$$\sigma = 1 \text{ on } N_W F_1.$$

Let $\mathfrak{p}_{r+1}$ be a prime whose Frobenius conjugacy class in $\mathrm{Gal}(K(E_1[\ell])N_W F_1/K)$ is the class of σ. Since Frobenius fixes $\boldsymbol{\mu}_\ell$ and $(\mathcal{O}_{K,\Sigma}^\times)^{1/\ell}$, we have that $\boldsymbol{\mu}_\ell$ and $(\mathcal{O}_{K,\Sigma}^\times)^{1/\ell}$ are contained in $K_{\mathfrak{p}_{r+1}}^\times$. Hence $\mathbf{N}\mathfrak{p}_{r+1} \equiv 1 \pmod{\ell}$ and the inclusion $K^\times \hookrightarrow K_{\mathfrak{p}_{r+1}}^\times$ sends $\mathcal{O}_{K,\Sigma}^\times$ into $(\mathcal{O}_{\mathfrak{p}_{r+1}}^\times)^\ell$,

so $\mathfrak{p}_{r+1} \in \mathcal{P}$. By Lemma 1.3.4, evaluation of cocycles at a Frobenius element for $\mathfrak{p}_{r+1}$ in G_K induces an isomorphism

$$\mathcal{H}_\ell(K_{\mathfrak{p}_{r+1}}) = H^1_{\mathrm{ur}}(K_{\mathfrak{p}_{r+1}}, E_1[\ell]) \cong E_1[\ell]/(\tau_1 - 1)E_1[\ell] = 0.$$

Thus $\mathfrak{p}_{r+1} \in \mathcal{P}_0(E_1)$. Again, by Lemma 1.3.4, evaluation of cocycles at a Frobenius element for $\mathfrak{p}_{r+1}$ in G_K induces an isomorphism

$$\mathcal{H}_\ell(K_{\mathfrak{p}_{r+1}}) = H^1_{\mathrm{ur}}(K_{\mathfrak{p}_{r+1}}, E_2[\ell]) \cong E_2[\ell]/(\tau_2 - 1)E_2[\ell] = E_2[\ell].$$

Thus $\mathfrak{p}_{r+1} \in \mathcal{P}_2(E_2)$.

Let $W_{r+1} = \mathrm{loc}_{\mathfrak{p}_{r+1}}(\mathrm{Sel}_\ell(K, E_2)^{\mathfrak{p}_{r+1}}(W))$. Then by Proposition 3.2.4,

$$\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, E_2)(W \times W_{r+1}) = \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, E_2)(W) + 2.$$

□

Proposition 3.5.3. *Let $t \geq \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, E_2)$, $t \equiv \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, E_2) \pmod 2$ and $r := (t - \dim_{\mathcal{O}_{M_2}/\ell} \mathrm{Sel}_\ell(K, E_2))/2$.*

(i) There is a finite set of primes $T_1 = \{\mathfrak{p}_i\}_{i=1}^r \subseteq \mathcal{P}_0(E_1) \cap \mathcal{P}_2(E_2)$ and isotropic subspaces W_i of $H^1(K_{\mathfrak{p}_i}, E_2[\ell])$ such that

$$\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, E_2)(W) = t,$$

where $W := \prod_{i=1}^r W_i$.

(ii) If T_1 and W_i are as in (i), $\mathcal{L} := (\mathcal{L}_{W_1}, \mathcal{L}_{W_2}, \cdots, \mathcal{L}_{W_r})$, $T_0 = \{\mathfrak{w}_i\}_{i=1}^r$ is a finite subset of $\mathcal{P}_0(E_1) \cap \mathcal{P}_0(E_2)$, and L/K is a cyclic extension of K of degree ℓ that has splitting

data $(\Sigma, T_0, T_1, \mathcal{L})$*, then*

$$\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(L/K, E_1) = \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, E_1), \quad \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(L/K, E_2) = t.$$

Proof. We apply Proposition 3.5.2 and induction on the cardinality of primes as in the proof of Proposition 9.17 in (**MRL**). This gives us (i).

Now if L/K is a cyclic extension of K of degree ℓ that has splitting data $(\Sigma, T_0, T_1, \mathcal{L})$, then by Proposition 3.1.14 and Lemma 3.1.15,

$$\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(L/K, E_1) = \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, E_1),$$

$$\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(L/K, E_2) = \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, E_2)(W) = t.$$

□

Definition 3.5.4. Suppose $T_1 = \{\mathfrak{p}_i\}_{i=1}^r$ is a finite subset of $\mathcal{P}_0(E_1) \cap \mathcal{P}_2(E_2)$. Let $\Sigma_i := \Sigma \cup \{\mathfrak{p}_j | 1 \leq j \leq r, j \neq i\}$ and $\Sigma' := \Sigma \cup \{\mathfrak{p}_j | 1 \leq j \leq r\}$. Consider the following exact sequence

$$\begin{tikzcd} 1 \arrow[r] & \mathcal{O}_{K,\Sigma_i}^\times \arrow[r] & \mathcal{O}_{K,\Sigma'}^\times \arrow[r, "\mathrm{ord}_{\mathfrak{p}_i}()"] & \mathbb{Z} \arrow[r] & 1 \\ & & \beta_i \arrow[r] & 1 & \end{tikzcd}$$

Define β_i to be a preimage of 1 in this diagram.

Lemma 3.5.5. *Suppose* $T_1 = \{\mathfrak{p}_i\}_{i=1}^r$ *is a finite subset of* $\mathcal{P}_0(E_1) \cap \mathcal{P}_2(E_2)$*. Then there exist* $\{\mathfrak{w}_i\}_{i=1}^r \subseteq \mathcal{P}_0(E_1) \cap \mathcal{P}_0(E_2)$ *such that* $\mathcal{O}_{K,\Sigma_i}^\times \subseteq (\mathcal{O}_{\mathfrak{w}_i}^\times)^\ell$ *and* $\beta_i \notin (\mathcal{O}_{\mathfrak{w}_i}^\times)^\ell$ *for all* i*.*

Proof. Let $\mathcal{M}_i := K(\boldsymbol{\mu}_\ell, (\mathcal{O}_{K,\Sigma_i}^\times)^{1/\ell})$, $\mathcal{M}' := K(\boldsymbol{\mu}_\ell, (\mathcal{O}_{K,\Sigma'}^\times)^{1/\ell})$, and $F_2 := K(E_1[\ell]) \cap K(E_2[\ell])$.

If E_1 has no CM, let $\tau_1 \in G_{K(\boldsymbol{\mu}_\ell)}$ be an element that acts like $\begin{bmatrix} -1 & -1 \\ 0 & -1 \end{bmatrix}$ on $E_1[\ell]$. If

E_1 has CM, let $\tau_1 \in G_{K(\boldsymbol{\mu}_\ell)}$ be a non-identity element in $\mathrm{Gal}(K(E_1[\ell])/F_2)$. Therefore, $\dim_{\mathbb{F}_\ell}(E_1[\ell]/(\tau_1 - 1)E_1[\ell]) = 0$.

Let $\tau_2 \in G_{K(\boldsymbol{\mu}_\ell)}$ be a non-identity element in $\mathrm{Gal}(K(E_2[\ell])/F_2)$. Therefore, $\dim_{\mathbb{F}_\ell}(E_2[\ell]/(\tau_2 - 1)E_2[\ell]) = 0$.

Let Let $\tau_{3,i} \in G_{K(\boldsymbol{\mu}_\ell)}$ be a non-identity element in $\mathrm{Gal}(\mathcal{M}'/\mathcal{M}_i)$.

By the same reason as Lemma 2.5.1, $K(E_2[\ell])$ and $\mathcal{M}'$ are linearly disjoint over $K(\boldsymbol{\mu}_\ell)$. Let $\sigma_{2,i} \in G_K$ such that

$$\sigma_{2,i} = \tau_2 \text{ on } K(E_2[\ell]),$$

$$\sigma_{2,i} = \tau_{3,i} \text{ on } \mathcal{M}' = K(\boldsymbol{\mu}_\ell, (\mathcal{O}_{K,\Sigma'}^\times)^{1/\ell}).$$

Since $\mathcal{M}'(E_2[\ell])$ is an abelian ℓ-extension of $K(E_2[\ell])$, by Lemma 3.4.3, $K(E_1[\ell]) \cap \mathcal{M}'(E_2[\ell]) = F_2$. We can see that $\tau_1|_{F_2} = \sigma_{2,i}|_{F_2} = 1$. Therefore, there is some $\sigma_i \in G_K$ such that

$$\sigma_i = \tau_1 \text{ on } K(E_1[\ell]),$$

$$\sigma_i = \sigma_{2,i} \text{ on } \mathcal{M}'(E_2[\ell]).$$

Let $\mathfrak{w}_i$ be a prime whose Frobenius conjugacy class in $\mathrm{Gal}(\mathcal{M}'(E_1[\ell], E_2[\ell])/K)$ is the class of σ_i. Since Frobenius fixes $\boldsymbol{\mu}_\ell$ and $(\mathcal{O}_{K,\Sigma_i}^\times)^{1/\ell}$, we have that $\boldsymbol{\mu}_\ell$ and $(\mathcal{O}_{K,\Sigma_i}^\times)^{1/\ell}$ are contained in $K_{\mathfrak{w}_i}^\times$. Hence $\mathbf{N}\mathfrak{w}_i \equiv 1 \pmod{\ell}$ and the inclusion $K^\times \hookrightarrow K_{\mathfrak{w}_i}^\times$ sends $\mathcal{O}_{K,\Sigma_i}^\times$ into $(\mathcal{O}_{\mathfrak{w}_i}^\times)^\ell$, so $\mathfrak{w}_i \in \mathcal{P}$. On the other hand, Frobenius does not fix $(\mathcal{O}_{K,\Sigma'}^\times)^{1/\ell}$, we have that $\beta_i \notin (\mathcal{O}_{\mathfrak{w}_i}^\times)^\ell$. By Lemma 1.3.4, evaluation of cocycles at a Frobenius element for $\mathfrak{w}_i$ in G_K induces an isomorphism

$$\mathcal{H}_\ell(K_{\mathfrak{w}_i}) = H^1_{\mathrm{ur}}(K_{\mathfrak{w}_i}, E_1[\ell]) \cong E_1[\ell]/(\tau_1 - 1)E_1[\ell] = 0.$$

Thus $\mathfrak{w}_i \in \mathcal{P}_0(E_1)$=0. Again, by Lemma 1.3.4, evaluation of cocycles at a Frobenius element

for $\mathfrak{w}_i$ in G_K induces an isomorphism

$$\mathcal{H}_\ell(K_{\mathfrak{w}_i}) = H^1_{\mathrm{ur}}(K_{\mathfrak{w}_i}, E_2[\ell]) \cong E_2[\ell]/(\tau_2 - 1)E_2[\ell] = 0.$$

Thus $\mathfrak{w}_i \in \mathcal{P}_0(E_2)$=0. □

Lemma 3.5.6. *Suppose $T_0 = \{\mathfrak{w}_i\}_{i=1}^r$ and $T_1 = \{\mathfrak{p}_i\}_{i=1}^r$ are finite subsets of $\mathcal{P}$. Let*

$$H' := K^\times \prod_{v\in\Sigma} K_v^\times (\prod_{v\notin\Sigma\cup T_0\cup T_1} \mathcal{O}_v^\times)(\prod_{i=1}^r (K_{\mathfrak{p}_i}^\times)^\ell)(\prod_{i=1}^r (\mathcal{O}_{\mathfrak{w}_i}^\times)^\ell).$$

Then $[\mathbb{A}_K^\times : H'] \leq \ell^{2r}$.

Proof. Consider the sujective map:

$$\phi : \prod_{i=1}^r \mathcal{O}_{\mathfrak{p}_i}^\times \times \prod_{i=1}^r \mathcal{O}_{\mathfrak{w}_i}^\times \twoheadrightarrow \mathbb{A}_K^\times / H'.$$

Then $\prod_{i=1}^r (\mathcal{O}_{\mathfrak{p}_i}^\times)^\ell \times \prod_{i=1}^r (\mathcal{O}_{\mathfrak{w}_i}^\times)^\ell \subseteq \ker\phi$. Therefore, we have the induced map:

$$\bar{\phi} : \prod_{i=1}^r (\mathcal{O}_{\mathfrak{p}_i}^\times/(\mathcal{O}_{\mathfrak{p}_i}^\times)^\ell) \times \prod_{i=1}^r (\mathcal{O}_{\mathfrak{w}_i}^\times/(\mathcal{O}_{\mathfrak{w}_i}^\times)^\ell) \twoheadrightarrow \mathbb{A}_K^\times / H'.$$

Thus we have $[\mathbb{A}_K^\times : H'] \leq \ell^{2r}$. □

Lemma 3.5.7. *Suppose $T_1 = \{\mathfrak{p}_i\}_{i=1}^r$ is a finite subset of $\mathcal{P}_0(E_1) \cap \mathcal{P}_2(E_2)$. Let $\mathcal{L}_i$ be extensions of $K_{\mathfrak{p}_i}$ of degree ℓ. Let $\mathcal{L} := (\mathcal{L}_1, \mathcal{L}_2, \cdots, \mathcal{L}_r)$. Then there exist a finite subset $T_0 = \{\mathfrak{w}_i\}_{i=1}^r$ of $\mathcal{P}_0(E_1) \cap \mathcal{P}_0(E_2)$ and a cyclic extension L/K of degree ℓ that has splitting data $(\Sigma, T_0, T_1, \mathcal{L})$.*

Proof. By Lemma 3.5.5, there exist $T_0 = \{\mathfrak{w}_i\}_{i=1}^r \subseteq \mathcal{P}_0(E_1) \cap \mathcal{P}_0(E_2)$ such that $\mathcal{O}_{K,\Sigma_i}^\times \subseteq$

$(\mathcal{O}_{\mathfrak{w}_i}^\times)^\ell$ and $\beta_i \notin (\mathcal{O}_{\mathfrak{w}_i}^\times)^\ell$ for all i. Let

$$H' := K^\times \prod_{v\in\Sigma} K_v^\times (\prod_{v\notin\Sigma\cup T_0\cup T_1} \mathcal{O}_v^\times)(\prod_{i=1}^r (K_{\mathfrak{p}_i}^\times)^\ell)(\prod_{i=1}^r (\mathcal{O}_{\mathfrak{w}_i}^\times)^\ell)$$

be a subgroup of $\mathbb{A}_K^\times$.

First we claim that $\prod_{i=1}^r (K_{\mathfrak{p}_i}^\times/(K_{\mathfrak{p}_i}^\times)^\ell) \cong \mathbb{A}_K^\times/H'$. Let $\phi : \prod_{i=1}^r K_{\mathfrak{p}_i}^\times \to \mathbb{A}_K^\times/H'$. We first find the kernel of ϕ.

(i) Assume that $(u_1, \cdots, u_r) \in (\mathcal{O}_{\mathfrak{p}_1}^\times \times \cdots \times \mathcal{O}_{\mathfrak{p}_r}^\times) \cap H'$. Then $(u_1, \cdots, u_r) = \alpha \cdot (\prod_{v\in\Sigma} \alpha^{-1}) \cdot (\prod_{v\notin\Sigma\cup T_0\cup T_1} \alpha^{-1}) \cdot (\prod_{i=1}^r v_i) \cdot (\prod_{i=1}^r \alpha^{-1})$, where $\alpha \in K$ and $v_i \in (K_{\mathfrak{p}_i}^\times)^\ell$. We have $\alpha \in \mathcal{O}_{K,\Sigma'}^\times$ and $u_i = \alpha \cdot v_i$. Compute the order, $\mathrm{ord}_{\mathfrak{p}_i}(\alpha) = -\mathrm{ord}_{\mathfrak{p}_i}(v_i) = k_i \cdot \ell$ for $k_i \in \mathbb{Z}$. Therefore,

$$\begin{aligned}
(\frac{\alpha}{\beta_1^{k_1\ell} \cdots \beta_r^{k_r\ell}}) \in \mathcal{O}_{K,\Sigma}^\times &\Rightarrow (\frac{\alpha}{\beta_1^{k_1\ell} \cdots \beta_r^{k_r\ell}}) \in (\mathcal{O}_{K_{\mathfrak{p}_i}}^\times)^\ell \\
&\Rightarrow \alpha \in (K_{\mathfrak{p}_i}^\times)^\ell \\
&\Rightarrow u_i \in (K_{\mathfrak{p}_i}^\times)^\ell \cap \mathcal{O}_{\mathfrak{p}_i}^\times \\
&\Rightarrow u_i \in (\mathcal{O}_{\mathfrak{p}_i}^\times)^\ell.
\end{aligned}$$

(ii) Assume that $(\lambda_1, \cdots, \lambda_r) \in K_{\mathfrak{p}_1}^\times \times \cdots \times K_{\mathfrak{p}_r}^\times \cap H'$. Then $(\lambda_1, \cdots, \lambda_r) = \alpha \cdot (\prod_{v\in\Sigma} \alpha^{-1}) \cdot (\prod_{v\notin\Sigma\cup T_0\cup T_1} \alpha^{-1}) \cdot (\prod_{i=1}^r \gamma_i) \cdot (\prod_{i=1}^r \alpha^{-1})$, where $\alpha \in K$ and $\gamma_i \in (K_{\mathfrak{p}_i}^\times)^\ell$. We have $\alpha \in \mathcal{O}_{K,\Sigma'}^\times$, $\alpha \in (\mathcal{O}_{\mathfrak{w}_i}^\times)^\ell$ and $\lambda_i = \alpha \cdot \gamma_i$. Define $n_i := \mathrm{ord}_{\mathfrak{p}_i}(\alpha)$. Compute the order, $\mathrm{ord}_{\mathfrak{p}_i}(\lambda_i) = n_i + g_i \cdot \ell$ for $g_i \in \mathbb{Z}$. Therefore,

$$\begin{aligned}
\frac{\alpha}{\beta_i^{n_i}} \in \mathcal{O}_{K,\Sigma_i}^\times \subseteq (\mathcal{O}_{\mathfrak{w}_i}^\times)^\ell &\Rightarrow \beta_i^{n_i} \in (\mathcal{O}_{\mathfrak{w}_i}^\times)^\ell \\
&\Rightarrow \ell | n_i \\
&\Rightarrow \ell | \mathrm{ord}_{\mathfrak{p}_i}(\lambda_i).
\end{aligned}$$

Then $(\lambda_1, \cdots, \lambda_r) = (u_1 \cdot \beta_1^{m_1\ell}, \cdots, u_r \cdot \beta_r^{m_r\ell}) \in H'$ where $m_i \in \mathbb{Z}$ and $u_i \in \mathcal{O}_{\mathfrak{p}_i}^\times$. Therefore,

$$\begin{aligned}(\beta_1^{m_1\ell}, \cdots, \beta_r^{m_r\ell}) \in H' &\Rightarrow (u_1, \cdots, u_r) \in H' \\ &\Rightarrow u_i \in (\mathcal{O}_{\mathfrak{p}_i}^\times)^\ell \text{ by (i)} \\ &\Rightarrow \lambda_i = u_i \cdot \beta_i^{m_i\ell} \in (K_{\mathfrak{p}_i}^\times)^\ell.\end{aligned}$$

Now we found that $\ker \phi = \prod_{i=1}^r (K_{\mathfrak{p}_i}^\times)^\ell$ and ϕ induces

$$\tilde{\phi} : \prod_{i=1}^r (K_{\mathfrak{p}_i}^\times/(K_{\mathfrak{p}_i}^\times)^\ell) \hookrightarrow \mathbb{A}_K^\times/H'.$$

Compare the order of both sides, $|\prod_{i=1}^r (K_{\mathfrak{p}_i}^\times/(K_{\mathfrak{p}_i}^\times)^\ell)| = \ell^{2r}$ and $[\mathbb{A}_K^\times : H'] \leq \ell^{2r}$ by Lemma 3.5.6, we know that $\tilde{\phi}$ is an isomorphism.

Let $V := \prod_{i=1}^r (K_{\mathfrak{p}_i}^\times/(K_{\mathfrak{p}_i}^\times)^\ell)$. Let $H_{\mathcal{L}_i}$ be the subgroup of $K_{\mathfrak{p}_i}^\times$ corresponding by local class field theory to $\mathcal{L}_i$. Let $W := \prod_{i=1}^r (H_{\mathcal{L}_i}/(K_{\mathfrak{p}_i}^\times)^\ell) \leq V$ and H'' be the subgroup of $\mathbb{A}_K^\times$ corresponding to W under $\tilde{\phi}$. That is to say,

$$\prod_{i=1}^r (H_{\mathcal{L}_i}/(K_{\mathfrak{p}_i}^\times)^\ell) \cong H''/H'.$$

Now we want to find $W \leq U \leq V$ such that $[V : U] = \ell$ and $(K_{\mathfrak{p}_i}^\times/(K_{\mathfrak{p}_i}^\times)^\ell) \nsubseteq U$ for all i. Fix an isomorphism $\rho_i : K_{\mathfrak{p}_i}^\times/H_{\mathcal{L}_i} \to \mathbb{F}_\ell$ for each i. Define

$$\begin{aligned}\psi : \prod_{i=1}^r \mathbb{F}_\ell &\longrightarrow \mathbb{F}_\ell \\ (a_1, \cdots, a_r) &\mapsto a_1 + \cdots + a_r.\end{aligned}$$

Then we have the following sequence

$$V/W \cong \prod_{i=1}^{r}(K_{\mathfrak{p}_i}^{\times}/H_{\mathcal{L}_i}) \xrightarrow{\oplus\rho_i} \prod_{i=1}^{r}\mathbb{F}_\ell \xrightarrow{\psi} \mathbb{F}_\ell.$$

Then $\dim_{\mathbb{F}_\ell}\ker\psi = r-1$ and $\mathbb{F}_\ell \not\subseteq \ker\psi$ for any copy $\mathbb{F}_\ell$ in $\prod_{i=1}^{r}\mathbb{F}_\ell$. The preimage of $\ker\psi$ in V/W gives us the subspace U with the desired properties.

Let H be the subgroup of $\mathbb{A}_K^{\times}$ corresponding by $\tilde{\phi}$ to U. Now the overall picture looks like

$$\begin{array}{ccc}
V = \prod_{i=1}^{r}(K_{\mathfrak{p}_i}^{\times}/(K_{\mathfrak{p}_i}^{\times})^{\ell}) & \overset{\tilde{\phi}}{\text{———}} & \mathbb{A}_K^{\times}/H' \\
| & & | \text{degree } \ell \\
U & \text{———} & H/H' \\
| & & | \text{degree } \ell^{r-1} \\
W = \prod_{i=1}^{r}(H_{\mathcal{L}_i}/(K_{\mathfrak{p}_i}^{\times})^{\ell}) & \text{———} & H''/H'.
\end{array}$$

Let L be the cyclic extension of K of degree ℓ corresponding by global class field theory to the subgroup H. Class field theory tells us that the inertia (resp., decomposition) group of a place v in $\mathrm{Gal}(L/K)$ is the image of $\mathcal{O}_v^{\times}$ (resp., $K_v^{\times}$) in $\mathbb{A}_K^{\times}/H$. If $v \in \Sigma$ then $K_v^{\times} \subseteq H' \subseteq H$, so every $v \in \Sigma$ splits completely in L/K. If $v \notin T_0 \cup T_1$ then $\mathcal{O}_v^{\times} \subseteq H' \subseteq H$, so v is unramified in L/K. If $v = \mathfrak{p}_i$ then

$$\mathbf{N}_{L_{\mathfrak{p}_i}/K_{\mathfrak{p}_i}} L_{\mathfrak{p}_i}^{\times} = H_{\mathcal{L}_i} = \mathbf{N}_{\mathcal{L}_i/K_{\mathfrak{p}_i}} \mathcal{L}_i^{\times},$$

so $L_{\mathfrak{p}_i} = \mathcal{L}_i$.

Therefore, we proved that L has splitting data $(\Sigma, T_0, T_1, \mathcal{L})$. $\square$

Chapter 4

Proof of the main theorem

4.1 PROOF OF THE MAIN THEOREM

Recall that E_L and λ_L are defined as in §1.2.

Lemma 4.1.1. *Let E be an elliptic curve defined over a number field K. Let ℓ be a prime such that* $\mathrm{Gal}(K(E[\ell])/K) \cong \mathrm{Aut}_{\mathrm{End}_{\bar{K}}(E)}(E[\ell])$. *If E has CM by M, we further assume that ℓ is inert in M, $M \subseteq K$, E has CM by $\mathcal{O}_M$ and ℓ does not divide the discriminant of $\mathcal{O}_M$. Let L/K be a cyclic extension of degree ℓ. Then*

(i) $\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(L/K, E) \leq \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, E_L)$.

(ii) $\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, E_L) \leq (\ell - 1)\ \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(L/K, E)$.

Proof. (i) Let $T = E_L[\ell], R = R_L/(\ell)$, and $I = (\lambda_L)$ in Lemma 3.5.3 in (**MR2**) (see also erratum at the end of (**MR4**)), we get

$$\mathrm{Sel}_{\lambda_L}(K, E_L) = \mathrm{Sel}_\ell(K, E_L)[\lambda_L].$$

By Lemma 1.4.2,

$$\mathrm{Sel}_\ell(L/K, E) = \mathrm{Sel}_{\lambda_L}(K, E_L) = \mathrm{Sel}_\ell(K, E_L)[\lambda_L].$$

This gives us (i).

For (ii), notice that $(\ell) = (\lambda_L^{\ell-1})$ and $\mathrm{Sel}_\ell(K, E_L) = \mathrm{Sel}_\ell(K, E_L)[\ell]$. It follows by induction from the exact sequence

$$0 \to \mathrm{Sel}_\ell(K, E_L)[\lambda_L] \to \mathrm{Sel}_\ell(K, E_L)[\lambda_L^{k+1}] \xrightarrow{\lambda_L} \mathrm{Sel}_\ell(K, E_L)[\lambda_L^k],$$

that

$$\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, E_L)[\lambda_L^k] \leq k \cdot \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, E_L)[\lambda_L].$$

Finally, take $k = \ell - 1$, we get

$$\begin{aligned}
\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, E_L) &= \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, E_L)[\ell] \\
&= \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, E_L)[\lambda_L^{\ell-1}] \\
&\leq (\ell - 1)\ \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, E_L)[\lambda_L] \\
&= (\ell - 1)\ \dim_{\mathbb{F}_\ell} \mathrm{Sel}_{\lambda_L}(K, E_L) \\
&= (\ell - 1)\ \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(L/K, E).
\end{aligned}$$

□

Lemma 4.1.2. *Let E be an elliptic curve defined over a number field K. Let ℓ be a prime. Let L/K be a cyclic extension of degree ℓ. Then*

$$H^1(K, \mathrm{Res}_K^L E[\ell]) \cong H^1(L, E[\ell]).$$

Proof. This is Shapiro's Lemma. (See for example the proof of Proposition 3.1. in (**MR3**).)

□

Recall that Σ is defined as in §1.4. Let L/K be a cyclic extension of degree ℓ. Define

$$M_E := \dim_{\mathbb{F}_\ell}(\oplus_{\mathfrak{p}\in\Sigma} H^1(K_\mathfrak{p}, E[\ell])/\mathcal{H}_\ell(K_\mathfrak{p})),$$
$$S_L := \{\text{primes of } K \text{ ramify in } L/K\},$$

and

$$C_{E,L} := \dim_{\mathbb{F}_\ell}(\oplus_{\mathfrak{p}\in S_L} H^1(K_\mathfrak{p}, E[\ell])/\mathcal{H}_\ell(K_\mathfrak{p})).$$

Lemma 4.1.3. *Let E be an elliptic curve defined over a number field K. Let ℓ be a prime such that $\mathrm{Gal}(K(E[\ell])/K) \cong \mathrm{Aut}_{\mathrm{End}_{\bar{K}}(E)}(E[\ell])$. If E has CM by M we further assume that ℓ is inert in M, $M \subseteq K$, E has CM by $\mathcal{O}_M$ and ℓ does not divide the discriminant of $\mathcal{O}_M$. Let L/K be a cyclic extension of degree ℓ. Then*

(i) $\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, E_L) \leq \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(L, E)$.

(ii) $\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(L, E) \leq \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, E_L) + \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, E) + M_E + C_{E,L}$.

Proof. Consider the exact sequence

$$0 \to E_L \to \mathrm{Res}_K^L E \to E \to 0$$

and take the ℓ-torsion, we get the exact sequence

$$0 \to E_L[\ell] \to \mathrm{Res}_K^L E[\ell] \to E[\ell] \to 0.$$

This induces the long exact sequence

$$H^0(K, E[\ell]) \to H^1(K, E_L[\ell]) \to H^1(K, \mathrm{Res}_K^L E[\ell]) \to ...$$

Since $\mathrm{Gal}(K(E[\ell])/K) \cong \mathrm{Aut}_{\mathrm{End}_{\bar{K}}(E)}(E[\ell])$, $H^0(K, E[\ell]) = E[\ell]^{G_K} = 0$. With Lemma 4.1.2,

we get

$$0 \to H^1(K, E_L[\ell]) \to H^1(L, E[\ell]) \to ...$$

This restricts to

$$0 \to \mathrm{Sel}_\ell(K, E_L) \to \mathrm{Sel}_\ell(L, E) \to ...$$

which gives us (i).

For (ii), first we define

$$\Sigma_L := \Sigma \cup S_L$$

and K_{Σ_L} denotes the maximal extension of K which is unramified outside Σ_L. Then we consider the exact sequence

$$0 \to \mathbb{Z} \to \mathbb{Z}[G] \xrightarrow{(1-\sigma)} \mathcal{I}_L \to 0$$

where σ is a generator of $G := \mathrm{Gal}(L/K)$, and the second map sends 1 to $\sum_{\tau \in G} \tau$ in $\mathbb{Z}[G]$. Tensoring with E as in (**MRS**), we get the exact sequence

$$0 \to E \to \mathrm{Res}_K^L E \to E_L \to 0.$$

Taking the ℓ-torsion, we get the exact sequence

$$0 \to E[\ell] \to \mathrm{Res}_K^L E[\ell] \to E_L[\ell] \to 0.$$

This induces the long exact sequence (writing $G' := \mathrm{Gal}(K_{\Sigma_L}/K)$)

$$0 = E_L[\ell]^{G'} \to H^1(G', E[\ell]) \to H^1(G', \mathrm{Res}_K^L E[\ell]) \xrightarrow{f} H^1(G', E_L[\ell]) \to ...$$

and restricts to

$$\mathrm{Sel}_\ell(K,E) \to \mathrm{Sel}_\ell(K, \mathrm{Res}_K^L E) = \mathrm{Sel}_\ell(L,E) \xrightarrow{g} \mathrm{Sel}_\ell(K,E_L) \to ...$$

(not necessarily exact). Then we have

$$\dim_{\mathbb{F}_\ell} \ker(g) \leq \dim_{\mathbb{F}_\ell} \ker(f) = \dim_{\mathbb{F}_\ell} H^1(G', E[\ell]) \tag{4.1.4}$$

and

$$\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(L,E) - \dim_{\mathbb{F}_\ell} \ker(g) \leq \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K,E_L). \tag{4.1.5}$$

Also, by the definition of the Selmer group, we have

$$0 \to \mathrm{Sel}_\ell(K,E) \to H^1(G', E[\ell]) \to \oplus_{\mathfrak{p}\in\Sigma_L} H^1(K_\mathfrak{p}, E[\ell])/\mathcal{H}_\ell(K_\mathfrak{p})$$

and

$$\begin{aligned}
&\dim_{\mathbb{F}_\ell} H^1(G', E[\ell]) - \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K,E) \\
&\leq \dim_{\mathbb{F}_\ell}(\oplus_{\mathfrak{p}\in\Sigma_L} H^1(K_\mathfrak{p}, E[\ell])/\mathcal{H}_\ell(K_\mathfrak{p})) \\
&= \dim_{\mathbb{F}_\ell}(\oplus_{\mathfrak{p}\in\Sigma} H^1(K_\mathfrak{p}, E[\ell])/\mathcal{H}_\ell(K_\mathfrak{p})) + \dim_{\mathbb{F}_\ell}(\oplus_{\mathfrak{p}\in S_L} H^1(K_\mathfrak{p}, E[\ell])/\mathcal{H}_\ell(K_\mathfrak{p})) \\
&= M_E + C_{E,L}.
\end{aligned} \tag{4.1.6}$$

Combine (4.1.4), (4.1.5), and (4.1.6),

$$\begin{aligned}\dim_{\mathbb{F}_\ell} \operatorname{Sel}_\ell(L,E) &\leq \dim_{\mathbb{F}_\ell} \operatorname{Sel}_\ell(K,E_L) + \dim_{\mathbb{F}_\ell} \ker(g) \\ &\leq \dim_{\mathbb{F}_\ell} \operatorname{Sel}_\ell(K,E_L) + \dim_{\mathbb{F}_\ell} H^1(G',E[\ell]) \\ &\leq \dim_{\mathbb{F}_\ell} \operatorname{Sel}_\ell(K,E_L) + \dim_{\mathbb{F}_\ell} \operatorname{Sel}_\ell(K,E) + M_E + C_{E,L}.\end{aligned}$$

□

Theorem 4.1.7. *Let E_1 and E_2 be elliptic curves defined over a number field K. Assume that E_1 and E_2 are without complex multiplication. If E_1 and E_2 are Strong Selmer Companions over K, then E_1 and E_2 are isogenous over K.*

Proof. Assume that E_1 is not isogenous to E_2 over K.

By Proposition 2.1.1, Theorem 2.3.7 and the fact that E_1 and E_2 are SSC, we can find some $\ell \geq 5$ such that $\operatorname{Gal}(K(E_i[\ell])/K) \cong \mathrm{GL}_2(\mathbb{F}_\ell)$ simultaneously for $i = 1, 2$, $K(E_1[\ell]) \neq K(E_2[\ell])$, and $\dim_{\mathbb{F}_\ell} \operatorname{Sel}_\ell(L,E_2) = \dim_{\mathbb{F}_\ell} \operatorname{Sel}_\ell(L,E_1)$ $\forall L/K$ finite extensions.

Choose some constant $C \geq M_{E_1} = \dim_{\mathbb{F}_\ell}(\oplus_{\mathfrak{p}\in\Sigma} H^1(K_\mathfrak{p}, E_1[\ell])/\mathcal{H}_\ell(K_\mathfrak{p}))$ and $C \geq \dim_{\mathbb{F}_\ell} \operatorname{Sel}_\ell(K,E_2)$. Taking $t = \ell \cdot \dim_{\mathbb{F}_\ell} \operatorname{Sel}_\ell(K,E_1) + C + 1$ in Proposition 2.5.5, there is a set of primes $T \subseteq \mathcal{P}_0(E_1) \cap \mathcal{P}_1(E_2)$ satisfying Proposition 2.5.5(i). Applying Lemma 1.5.2, we can find some degree ℓ cyclic extension L/K that is T-ramified and Σ-split. Therefore, by Proposition 2.5.5(ii),

$$\dim_{\mathbb{F}_\ell} \operatorname{Sel}_\ell(L/K,E_1) = \dim_{\mathbb{F}_\ell} \operatorname{Sel}_\ell(K,E_1)$$

and

$$\dim_{\mathbb{F}_\ell} \operatorname{Sel}_\ell(L/K,E_2) = \ell \cdot \dim_{\mathbb{F}_\ell} \operatorname{Sel}_\ell(K,E_1) + C + 1. \tag{4.1.8}$$

By Lemma 4.1.1(ii),

$$\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, (E_1)_L) \leq (\ell - 1) \ \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(L/K, E_1) = (\ell - 1) \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, E_1).$$

Then we apply Lemma 4.1.3(ii) to E_1. Since $T \subseteq \mathcal{P}_0(E_1)$, we have

$$C_{E_1,L} = \dim_{\mathbb{F}_\ell}(\oplus_{\mathfrak{p} \in S_L} H^1(K_\mathfrak{p}, E_1[\ell])/\mathcal{H}_\ell(K_\mathfrak{p})) = 0.$$

Lemma 4.1.3(ii) then tells us

$$\begin{aligned}
\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(L, E_1) &\leq \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, (E_1)_L) + \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, E_1) + M_{E_1} + C_{E_1,L} \\
&\leq (\ell - 1) \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, E_1) + \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, E_1) + M_{E_1} \\
&\leq \ell \cdot \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, E_1) + C.
\end{aligned}$$

By Lemma 4.1.3(i), Lemma 4.1.1(i), and 4.1.8,

$$\begin{aligned}
\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(L, E_2) &\geq \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, (E_2)_L) \\
&\geq \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(L/K, E_2) \\
&= \ell \cdot \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, E_1) + C + 1
\end{aligned}$$

This contradicts the assumption that E_1 and E_2 are Strong Selmer Companions over K.

Therefore, E_1 is isogenous to E_2 over K. □

Theorem 4.1.9. *Let E_1 and E_2 be elliptic curves defined over a number field K. Assume E_2 has complex multiplication by M_2 and $M_2 \subseteq K$. If E_1 has complex multiplication by M_1, further assume that $M_1 \subseteq K$. If E_1 and E_2 are Strong Selmer Companions over K, then E_1 and E_2 are isogenous over K.*

Proof. Assume that E_1 is not isogenous to E_2 over K.

By Lemma 3.1.1, if E_i has CM by $M_i \subseteq K$, we can assume that E_i has CM by $\mathcal{O}_{M_i}$. (Because isogenous curves are SSC by Proposition 1.1.6.)

By Theorem 2.1.1, Proposition 3.1.4, Theorem 3.3.6, Theorem 3.3.7, Theorem 3.3.10, Lemma 3.1.2, and the fact that E_1 and E_2 are SSC, we can find some ℓ such that $\mathrm{Gal}(K(E_i[\ell])/K) \cong \mathrm{Aut}_{\mathrm{End}_{\bar{K}}(E_i)}(E_i[\ell])$ simultaneously for $i = 1, 2$, $K(E_1[\ell]) \neq K(E_2[\ell])$, ℓ is inert in M_i, ℓ does not divide the discriminant of $\mathcal{O}_{M_i}$, and $\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(L, E_2) = \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(L, E_1)$ $\forall L/K$ finite extensions.

Choose some constant $C \geq M_{E_1} = \dim_{\mathbb{F}_\ell}(\oplus_{\mathfrak{p}\in\Sigma} H^1(K_\mathfrak{p}, E_1[\ell])/\mathcal{H}_\ell(K_\mathfrak{p}))$ and $C \geq \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, E_2)$. Take $t = \ell \cdot \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, E_1) + C + 1$ in Proposition 3.5.3, then there is a finite set $T_1 \subseteq \mathcal{P}_0(E_1) \cap \mathcal{P}_2(E_2)$ satisfying Proposition 3.5.3(i). Apply Lemma 3.5.7, we can find a finite subset T_0 of $\mathcal{P}_0(E_1) \cap \mathcal{P}_0(E_2)$ and a degree ℓ cyclic extension L/K that has splitting data $(\Sigma, T_0, T_1, \mathcal{L})$. We can adjust C to make sure that $t \equiv \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, E_2) \pmod 2$. Therefore, by Proposition 3.5.3(ii),

$$\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(L/K, E_1) = \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, E_1)$$

and

$$\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(L/K, E_2) = \ell \cdot \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, E_1) + C + 1. \tag{4.1.10}$$

By Lemma 4.1.1(ii),

$$\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, (E_1)_L) \leq (\ell - 1)\ \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(L/K, E_1) = (\ell - 1) \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K, E_1).$$

Then we apply Lemma 4.1.3(ii) to E_1. Since $T_0 \cup T_1 \subseteq \mathcal{P}_0(E_1)$, we have

$$C_{E_1,L} = \dim_{\mathbb{F}_\ell}(\oplus_{\mathfrak{p}\in S_L} H^1(K_\mathfrak{p}, E_1[\ell])/\mathcal{H}_\ell(K_\mathfrak{p})) = 0.$$

Lemma 4.1.3(ii) then tells us

$$\begin{aligned}\dim_{\mathbb{F}_\ell} \operatorname{Sel}_\ell(L, E_1) &\leq \dim_{\mathbb{F}_\ell} \operatorname{Sel}_\ell(K, (E_1)_L) + \dim_{\mathbb{F}_\ell} \operatorname{Sel}_\ell(K, E_1) + M_{E_1} + C_{E_1,L} \\ &\leq (\ell - 1) \dim_{\mathbb{F}_\ell} \operatorname{Sel}_\ell(K, E_1) + \dim_{\mathbb{F}_\ell} \operatorname{Sel}_\ell(K, E_1) + M_{E_1} \\ &\leq \ell \cdot \dim_{\mathbb{F}_\ell} \operatorname{Sel}_\ell(K, E_1) + C.\end{aligned}$$

By Lemma 4.1.3(i), Lemma 4.1.1(i), and 4.1.10,

$$\begin{aligned}\dim_{\mathbb{F}_\ell} \operatorname{Sel}_\ell(L, E_2) &\geq \dim_{\mathbb{F}_\ell} \operatorname{Sel}_\ell(K, (E_2)_L) \\ &\geq \dim_{\mathbb{F}_\ell} \operatorname{Sel}_\ell(L/K, E_2) \\ &= \ell \cdot \dim_{\mathbb{F}_\ell} \operatorname{Sel}_\ell(K, E_1) + C + 1\end{aligned}$$

This contradicts the assumption that E_1 and E_2 are Strong Selmer Companions over K.

Therefore, E_1 is isogenous to E_2 over K. □

The following lemma is in page 30 of (**L**).

Lemma 4.1.11. *Let E_1 and E_2 be elliptic curves defined over a number field K. If there exists some number field F such that E_1 and E_2 are isogenous over F, then* $\operatorname{End}_{\bar{K}}(E_1) \otimes \mathbb{Q} \cong \operatorname{End}_{\bar{K}}(E_2) \otimes \mathbb{Q}$.

Proof. Let $\varphi : E_1 \sim_F E_2$ be an isogeny defined over F and $\hat{\varphi}$ be its dual. Let $n := \deg \varphi$. Consider the map

$$\operatorname{End}_{\bar{K}}(E_1) \to \operatorname{End}_{\bar{K}}(E_2) \otimes \mathbb{Q}$$

$$f \mapsto \frac{1}{n} \varphi \circ f \circ \hat{\varphi}.$$

This gives an injective ring homomorphism since the composition of nonzero isogenies is nonzero. Therefore, $\operatorname{End}_{\bar{K}}(E_1)$ is a subring of $\operatorname{End}_{\bar{K}}(E_2) \otimes \mathbb{Q}$ and $\operatorname{End}_{\bar{K}}(E_1) \otimes \mathbb{Q}$ is a subfield

of $\mathrm{End}_{\bar{K}}(E_2) \otimes \mathbb{Q}$. For the same reason, $\mathrm{End}_{\bar{K}}(E_2) \otimes \mathbb{Q}$ is also a subfield of $\mathrm{End}_{\bar{K}}(E_1) \otimes \mathbb{Q}$. Therefore, $\mathrm{End}_{\bar{K}}(E_1) \otimes \mathbb{Q} \cong \mathrm{End}_{\bar{K}}(E_2) \otimes \mathbb{Q}$. $\square$

Lemma 4.1.12. *Let E_1 and E_2 be elliptic curves defined over a number field K. Assume that E_1 and E_2 both have complex multiplication by $\mathcal{O}_M$ where $M \nsubseteq K$. If E_1 is isogenous to E_2 over MK, then E_1 and E_2 are isogenous over K.*

Proof. Let $\varphi : E_1 \sim_{MK} E_2$ be an isogeny defined over MK and $\hat{\varphi}$ be its dual, $\mathrm{Gal}(MK/K) = \langle \sigma \rangle$, and $d := \deg \varphi$. Consider $f := \hat{\varphi} \circ \varphi^\sigma \in \mathrm{End}_{\bar{K}}(E_1) = \mathcal{O}_M$ and its dual $\hat{f} = \hat{\varphi}^\sigma \circ \varphi = f^\sigma$,

$$f \circ f^\sigma = f \circ \hat{f} = [\deg f] = [\deg \varphi]^2 = d^2.$$

Let $\alpha := \frac{f}{d} \in \mathrm{End}_{\bar{K}}(E_1) \otimes \mathbb{Q}$,

$$\mathbf{N}\alpha = \alpha \cdot \alpha^\sigma = \frac{f}{d} \cdot \frac{f^\sigma}{d^\sigma} = \frac{d^2}{d^2} = 1.$$

By Hilbert's Theorem 90, there exists $\beta \in \mathcal{O}_M$ such that $\frac{\beta}{\beta^\sigma} = \alpha = \frac{f}{d}$.

Consider $\varphi \circ \beta : E_1 \to E_1 \to E_2$,

$$d \circ \beta = f \circ \beta^\sigma,$$

$$\hat{\varphi} \circ \varphi \circ \beta = \hat{\varphi} \circ \varphi^\sigma \circ \beta^\sigma,$$

$$\varphi \circ \beta = \varphi^\sigma \circ \beta^\sigma.$$

Therefore, $\varphi \circ \beta$ gives an isogeny defined over K. $\square$

Theorem 4.1.13. *Let E_1 and E_2 be elliptic curves defined over a number field K. Assume that E_2 has complex multiplication. If E_1 and E_2 are Strong Selmer Companions over K, then E_1 and E_2 are isogenous over K.*

Proof. If E_1 and E_2 are Strong Selmer Companions over K, then E_1 and E_2 are Strong

Selmer Companions over KM_1M_2 where $M_i := \mathrm{End}_{\bar{K}}(E_i) \otimes \mathbb{Q}$. By Theorem 4.1.9, E_1 and E_2 are isogenous over KM_1M_2. By Lemma 4.1.11, $M_1 = M_2$. If $M_2 \subseteq K$, then E_1 and E_2 are isogenous over K. If $M_2 \nsubseteq K$, by Lemma 4.1.12, then E_1 and E_2 are isogenous over K $\square$

Combine Theorem 4.1.7 and Theorem 4.1.13, we finally get Theorem 1.1.8:

Theorem 1.1.8. *Let E_1 and E_2 be elliptic curves defined over a number field K. Then E_1 and E_2 are isogenous over K if and only if E_1 and E_2 are Strong Selmer Companions over K.*

Proof. The 'only if' direction is Proposition 1.1.6. The 'if' direction is a consequence of Theorem 4.1.7 and Theorem 4.1.13. $\square$

Bibliography

[**CF**] J.W.S.Cassels, A. Frohlich: *Algebraic Number Theory* London: London Mathematical Society

[**F1**] G. Faltings: *Endlichkeitssatze fur abelsche Varietaten uber Zahlkorpern.* Invent. Math., 73(3):349-366, 1983.

[**F2**] G.Faltings: *Finiteness theorems for abelian varieties over number fields.* In Arithmetic geometry (Storrs, Conn., 1984), pages 9-27. Springer, New York, 1986. Translated from the German original [Invent. Math. 73 (1983), no. 3, 349-366; ibid. 75 (1984), no. 2, 381; MR 85g:11026ab] by Edward Shipz.

[**Ki**] H. Kisilevsky: *Rank determines semi-stable conductor* J. Number Theory, to appear (doi:10.1016/S0022-314X(03)00157-4)

[**KMR**] Z. Klagsbrun, B. Mazur, K. Rubin: *Disparity in Selmer Ranks of Quadratic Twists of Elliptic Curves* Annals of Mathematics, 178:287-320, 2013.

[**L**] S. Lang:*Abelian varieties* 2nd edn. Springer Verlag, New York, 1983.

[**Mi**] J.S. Milne:*Abelian Varieties* In Arithmetic Geometry (Springer Verlag, New York, 1986) Chapter V pages 103-150.

[**MR1**] B. Mazur, K. Rubin: *Ranks of twists of elliptic curves and Hilberts's*

tenth problem Invent. Math. 181 (2010), 541?575. MR 2660452. Zbl 1227.11075. http://dx.doi.org/10.1007/s00222-010-0252-0.

[**MR2**] B. Mazur, K. Rubin: *Kolyvagin systems* Memoirs of the Amer. Math. Soc. 799 (2004).

[**MR3**] B. Mazur, K. Rubin: *Finding large Selmer rank via an arithmetic theory of local constants* Annals of Math. 166 (2007) 579-612.

[**MR4**] B. Mazur, K. Rubin: *Controlling Selmer groups in the higher core rank case* Journal de Theorie des Nombres de Bordeaux 28 (2016) 145-183

[**MRL**] B. Mazur, K. Rubin, M. Larsen: *Diophantine Stability* American J. Math 140 (2018) 571-616

[**MRS**] B. Mazur, K. Rubin, A. Silverberg: *Twisting commutative algebraic groups* Journal of Algebra 314 (2007) 419-438

[**PZ**] A. Parshin, Y. Zarhin: *Finiteness Problems in Diophantine Geometry* Amer. Math. Soc. Transl. (2) **143**(1989), 35 - 102

[**Re**] I.Reiner: *A New Type of Automorphism of the General Linear Group Over a Ring* Annals of Mathematics, vol. 66, no. 3, 1957, pp. 461-466. JSTOR

[**Ru**] K. Rubin: *Elliptic Curves with Complex Multiplication and the Conjecture of Birch and swinnerton-Dyer* in Arithmetic Theory of Elliptic Curves, Lecture Notes in Mathematics 1716, Springer 1999

[**Ser1**] J. Serre: *Abelian l-adic representations and elliptic curves*

[**Ser2**] J. Serre: *Points d'ordre fini des courbes elliptiques*

[**Shi**] G. Shimura: *On the Zeta-Function of an Abelian Variety with Complex Multiplication* Annals of Mathematics Second Series, Vol. 94, No. 3 (Nov., 1971), pp. 504-533

[**Si**] J. Silverman: *The Arithmetic of Elliptic Curves* Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986. MR817210 (87g:11070)

[**T**] J. Tate: *WC-groups over* $\mathfrak{p}$*-adic fields* Seminare Bourbaki 4, Exp. 156, Spc. Math. France, Paris (1995), 265-277