Title
Strong Selmer Companion Elliptic Curves

Permalink
https://escholarship.org/uc/item/17d2s662

Author
Chiu, Ching-Heng

Publication Date
2019

Peer reviewed|Thesis/dissertation
UNIVERSITY OF CALIFORNIA,
IRVINE

Strong Selmer Companion Elliptic Curves
DISSENTATION

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 iii  
CURRICULUM VITAE iv  
ABSTRACT OF THE DISSERTATION v  

1 Introduction, preliminaries and results 1  
1.1 INTRODUCTION ........................................ 1  
1.2 TWISTS OF ELLIPTIC CURVES ........................... 4  
1.3 LOCAL FIELDS AND LOCAL CONDITIONS ................ 6  
1.4 SELMER GROUPS AND SELMER STRUCTURES ............... 8  
1.5 TWISTING TO FIX THE SELMER RANK .................... 10  

2 Elliptic curves without complex multiplication 12  
2.1 MORE SELMER STRUCTURES .............................. 12  
2.2 TWISTING TO INCREASE THE SELMER RANK ............... 14  
2.3 FIELDS GENERATED BY TORSION POINTS OF ELLIPTIC CURVES 18  
2.4 LINEARLY DISJOINT FIELDS ........................... 21  
2.5 FIX THE SELMER RANK OF $E_1$ AND INCREASE THE SELMER RANK OF $E_2$ SIMULTANEOUSLY ................ 23  

3 Elliptic curves with complex multiplication 29  
3.1 MORE SELMER STRUCTURES .............................. 29  
3.2 TWISTING TO INCREASE THE SELMER RANK ............... 36  
3.3 FIELDS GENERATED BY TORSION POINTS OF ELLIPTIC CURVES 39  
3.4 LINEARLY DISJOINT FIELDS ........................... 45  
3.5 FIX THE SELMER RANK OF $E_1$ AND INCREASE THE SELMER RANK OF $E_2$ SIMULTANEOUSLY ................ 47  

4 Proof of the main theorem 56  
4.1 PROOF OF THE MAIN THEOREM ........................... 56  

Bibliography 67
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 $\ell$, and for all finite extension fields $L/K$,

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

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 \( L/K \),

\[
\text{rank}_\mathbb{Z}(X_1(L)) = \text{rank}_\mathbb{Z}(X_2(L)).
\]

Zarhin’s question is whether the converse holds: Let \( X_1 \) and \( X_2 \) be abelian varieties defined over \( K \). If \( \text{rank}_\mathbb{Z}(X_1(L)) = \text{rank}_\mathbb{Z}(X_2(L)) \) 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

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

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

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

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 $\ell$, and for all finite extension fields $L/K$,

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

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

**Remark 1.1.4.** For definition of $\text{Sel}_\ell(K, E)$, 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 $K$. 

2
**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 $\varphi : E_1 \rightarrow E_2$ be an isogeny and $\hat{\varphi}$ be its dual isogeny. Let $d := \deg \varphi$. Let $\ell$ be a prime which is coprime to $d$ and $L$ be a finite extension over $K$. Let $\varphi'$ and $\hat{\varphi}'$ be the induced map of $\varphi$ and $\hat{\varphi}$ on the Selmer group. Since $\hat{\varphi}' \circ \varphi'$ is the multiplication-by-$d$ map, it is an isomorphism

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

Therefore, $\varphi'$ is injective and we have

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

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

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

Hence,

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

for all $\ell$ coprime to $d$ and all finite extensions $L/K$. So, $E_1$ and $E_2$ are Strong Selmer Companions over $K$. \hfill \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 $\text{End}_K \neq \mathbb{Z}$. 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 $\text{End}_{\bar{K}}(E) \otimes \mathbb{Q} = M$ 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 $\text{End}_{\bar{K}}(E) = \mathcal{O}_M$. 

3
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 $\ell$.

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

**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 $\text{rank}_\mathbb{Z}(\mathcal{I}_L) = \ell - 1$, 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,

$$E_L := \ker(\text{Res}^L_K E \to E).$$

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

4
See (MRS) for a discussion of $E_L$ and its properties.

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

$$R_L := \mathbb{Z}[G]/N_{L/K}\mathbb{Z}[G]$$

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

Fixing an identification $G \xrightarrow{\sim} \mu_\ell$ of $G$ with the group of $\ell$-th roots of unity in $\overline{Q}$ induces an isomorphism

$$R_L \cong \mathbb{Z}[\mu_\ell]$$

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

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

(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 $\text{End}_K(E)[G_K]$-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 $\text{Sel}_\ell(L/K, E)$.

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 $\ell$ a cyclic extension $L/K$ of degree 1 or $\ell$, and let $G := \text{Gal}(L/K)$.

**Definition 1.3.1.** Define $H_\ell(L/K) \subset H^1(K, E[\ell])$ 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 $\lambda_L/\lambda_L^2$, but its image is independent of this choice.) When $L = K$, $H_\ell(K/K)$ 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 $H_\ell(K)$. We suppress the dependence on $E$ from the notation when possible, since $E$ is fixed throughout §1.3 and §1.4.

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

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

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 $\ell$, then $H_\ell(L/K)$ 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 $\ell$.

(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 $\text{Gal}(K^{ur}/K)$, 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 $\ell$, $E/K$ has good reduction, and $L/K$ is unramified.

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

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

(ii) The twist $E_L$ has good reduction, and $\mathcal{H}_\ell(L/K) = H^1_{\text{ur}}(K, E[\ell])$. 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 $\ell$, and $L/K$ is ramified. Then

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

Proof. This is Proposition 7.8. in (MRL).
1.4 SELMER GROUPS AND SELMER STRUCTURES

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

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 \( \ell \), we define the \( \ell \)-Selmer group \( \text{Sel}_\ell(L/K, E) \subset H^1(K, E[\ell]) \) by

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

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

**Lemma 1.4.2.** The isomorphism of Proposition 1.2.3(iii) identifies \( \text{Sel}_\ell(L/K, E) \) with the classical \( \lambda_L \)-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 \( \Sigma \) generate the ideal class group of \( K \). If \( \ell \) and \( E \) are fixed, we write \( \Sigma \) instead of \( \Sigma_{\ell, E} \). (If we have two curves \( E_1 \) and \( E_2 \), we assume in addition that \( \Sigma \) contains all places where \( E_1 \) or \( E_2 \) has bad reduction.) Define

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

8
the ring of $\Sigma$-integers of $K$. Define sets of primes $\mathcal{P}(\Sigma) \subset \mathcal{Q}(\Sigma)$ by

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

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

If $\Sigma$ 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

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

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

$$< , >_v : H^1(K_v, E[\ell]) \times H^1(K_v, E[\ell]) \rightarrow H^2(K_v, \mu_\ell) = \mathbb{F}_\ell.$$ 

*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

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

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

**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.** $\mathcal{H}_\ell(K_p)$ is an isotropic subspace of $H^1(K_p, E[\ell])$. 

*Proof.* This is Proposition 2.1. in (MR3).
Proposition 1.4.8. Let $L/K$ be a cyclic extension of degree $\ell$. Then $\mathcal{H}_\ell(L_p/K_p)$ is an isotropic subspace of $H^1(K_p, E[\ell])$.

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

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

1.5 TWISTING TO FIX THE SELMER RANK

Let $\ell$ be a fixed prime $\geq 5$ and $\Sigma$ 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 $\Sigma$-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 $\ell$ be a prime. Then there is a cyclic extension $L/K$ of degree $\ell$ that is $T$-ramified and $\Sigma$-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 $\ell$ that is $T$-ramified and $\Sigma$-split. Then

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

Proof. This is Proposition 9.17 in (MRL).

By definition,

$$\text{Sel}_\ell(L/K, E) = \{ c \in H^1(K, E[\ell]) : \text{loc}_p(c) \in \mathcal{H}_\ell(L_p/K_p) \text{ for every } p \}.$$
On the other hand,

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

If $p \in T \subseteq \mathcal{P}_0(E)$, then $H^1(K_p, E[\ell]) = \mathcal{H}_\ell(K_p) = \mathcal{H}_\ell(L_p/K_p) = 0$ by Lemma 1.3.3 and Lemma 1.3.4. If $p \notin T$ and $p \notin \Sigma$, by Lemma 1.3.4 (ii), $\mathcal{H}_\ell(K_p) = H^1_{\text{ur}}(K_p, E[\ell]) = \mathcal{H}_\ell(L_p/K_p)$. If $p \in \Sigma$, then $p$ splits in $L$, $\mathcal{H}_\ell(K_p) = \mathcal{H}_\ell(L_p/K_p)$. Therefore, $\text{Sel}_\ell(L/K, E) = \text{Sel}_\ell(K, E).$
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 \( \text{Gal}(K(E[\ell])/K) \cong \text{Aut}_\mathbb{Z}(E[\ell]) \cong \text{GL}_2(\mathbb{F}_\ell) \) 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 \( \ell \), \( \text{Gal}(K(E[\ell])/K) \cong \text{Aut}_\mathbb{Z}(E[\ell]) \cong \text{GL}_2(\mathbb{F}_\ell) \).

**Proof.** This is the first theorem in Chapter IV 2.2 in \textbf{(Ser1)}. \qed

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

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

\[
\text{Sel}_\ell(K, E)^b_a(c) := \begin{cases} 
\text{loc}_v(c) \in \mathcal{H}_\ell(K_v) & \text{if } v \nmid abc \\
\text{loc}_v(c) = 0 & \text{if } v|a \\
\text{loc}_v(c) \in H^1_{\text{ram}}(K_v, E[\ell]) & \text{if } v|c
\end{cases}
\]

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

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

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

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

Note that

\[
\text{Sel}_\ell(K, E)_a \subset \text{Sel}_\ell(K, E) \subset \text{Sel}_\ell(K, E)^a.
\]

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

Lemma 2.1.6. Let \( T \) be a finite subset of \( \mathcal{P}_1(E) \) and \( a := \prod_{p \in T} p \). If \( L/K \) is a cyclic
extension of \( K \) of degree \( \ell \) that is \( T \)-ramified and \( \Sigma \)-split, then

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

Proof. By definition,

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

On the other hand,

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

If \( p \mid \mathfrak{a} \), by Remark 2.1.5, Lemma 2.1.2 and Definition 2.1.3, \( H^1_{\text{ram}}(K_p, E[\ell]) = \mathcal{H}_\ell(L_p/K_p) \). If \( p \nmid \mathfrak{a} \), by Lemma 1.3.4 (ii) and the fact that primes in \( \Sigma \) split in \( L \), \( \mathcal{H}_\ell(K_p) = \mathcal{H}_\ell(L_p/K_p) \).

\[ \square \]

\section{2.2 Twisting to Increase the Selmer Rank}

Let \( E \) be an elliptic curve defined over a number field \( K \). Let \( \ell \) be a fixed prime such that \( \mathrm{Gal}(K(E[\ell])/K) \cong \mathrm{GL}_2(\mathbb{F}_\ell) \). Let \( \Sigma \) 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 \( \sigma \) 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 $\ell$ and take $\phi = 0$ in (MR1).

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

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

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 $\tilde{c}_1, ..., \tilde{c}_k \in \text{Hom}(G_{K(E[\ell])}, E[\ell])^\Gamma$.

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

$$\tilde{c}_1 \times ... \times \tilde{c}_k : W \hookrightarrow E[\ell]^k$$  \hspace{1cm} (2.2.2)

is a $\Gamma$-equivariant injection. Thus $W$ is isomorphic to a $\Gamma$-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 $j = \dim_{\mathbb{F}_\ell} \text{Hom}(W, E[\ell])^\Gamma \geq k$, 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 $c \in C$. \hfill \Box

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

Suppose $a$ is an ideal of $O_K$. If $c \in \text{Sel}_\ell(K, E)(a)$, 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 $N_a$ be the abelian extension of $K(E[\ell])$ fixed by $\cap_{c \in \text{Sel}_\ell(K, E)(a)} \ker(\tilde{c})$.

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

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

**Proof.** Since Frobenius fixes $\mu_\ell$ and $(O_{K, \Sigma}^\times)^{1/\ell}$, we have that $\mu_\ell$ and $(O_{K, \Sigma}^\times)^{1/\ell}$ are contained in $K_p^\times$. Hence $N_p \equiv 1 \pmod{\ell}$ and the inclusion $K^\times \hookrightarrow K_p^\times$ sends $O_{K, \Sigma}^\times$ into $(O_{K, p}^\times)^{\ell}$, so $p \in \mathcal{P}$.

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

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

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

$$\text{loc}_p : \text{Sel}_\ell(K, E)(a) \to \mathcal{H}_{\ell}(K_p) \cong H^1_{ur}(K, E[\ell]) \cong E[\ell]/(\tau_a \sigma - 1)E[\ell]$$

and Lemma 2.2.1. Therefore, $\text{loc}_p(\text{Sel}_\ell(K, E)(a)) = 0$. \qed

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

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

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

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

**Proposition 2.2.6.** Let $a$ be product of primes in $P_0(E) \cup P_1(E)$. Let $\sigma$, $\tau_a$, and $N_a$ be as in Definition 2.2.3. If $p$ is a prime whose Frobenius conjugacy class in $\text{Gal}(N_aF_1/K)$ is the class of $\tau_a \sigma$, then

$$\dim_{F_\ell} \text{Sel}_\ell(K, E)(ap) = \dim_{F_\ell} \text{Sel}_\ell(K, E)(a) + 1.$$  

**Proof.** By Lemma 2.2.4, if $p$ is a prime whose Frobenius conjugacy class in $\text{Gal}(N_aF_1/K)$ is the class of $\tau_a \sigma$, then $p \in P_1(E)$ and $\text{loc}_p(\text{Sel}_\ell(K, E)(a)) = 0$. Consider the exact sequences

$$0 \to \text{Sel}_\ell(K, E)(a) \to \text{Sel}_\ell(K, E)^p(a) \to H^1(K_p, E[\ell]) / H^1_{\text{ram}}(K_p)$$

$$(2.2.7)$$

$$0 \to \text{Sel}_\ell(K, E)(p) \to \text{Sel}_\ell(K, E)(a) \to \mathcal{H}_\ell(K_p).$$

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 $p$ the lower right-hand map is zero, so the upper right-hand map is surjective. And we get

$$\dim_{F_\ell} \text{Sel}_\ell(K, E)(p) = \dim_{F_\ell} \text{Sel}_\ell(K, E)(a).$$  

(2.2.8)

Then we consider the exact sequences

$$0 \to \text{Sel}_\ell(K, E)(p) \to \text{Sel}_\ell(K, E)(ap) \to H^1_{\text{ram}}(K_p, E[\ell])$$

$$0 \to \text{Sel}_\ell(K, E)(ap) \to \text{Sel}_\ell(K, E)^p(a) \to H^1(K_p, E[\ell]) / H^1_{\text{ram}}(K_p, E[\ell]).$$  

(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, $\text{loc}_p(\text{Sel}_\ell(K, E)^p(a)) = H^1_{\text{ram}}(K, E[\ell])$ since they are 1-dimensional isotropic $\mathbb{F}_\ell$ subspaces of $H^1(K, E[\ell])$ and $\text{loc}_p(\text{Sel}_\ell(K, E)^p(a)) \neq \mathcal{H}_\ell(K)$ 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
\[ \dim_{\mathbb{F}_\ell} \text{Sel}_\ell(K, E)(ap) = \dim_{\mathbb{F}_\ell} \text{Sel}_\ell(K, E)_p(a) + 1. \] (2.2.10)

Combine (2.2.8) and (2.2.10), we get
\[ \dim_{\mathbb{F}_\ell} \text{Sel}_\ell(K, E)(ap) = \dim_{\mathbb{F}_\ell} \text{Sel}_\ell(K, E)(a) + 1. \]

\[ \square \]

### 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 $A \in \text{GL}_2(\mathbb{F}_\ell)$. A *radial automorphism* is an automorphism of the form:
\[ A \mapsto A(\det A)^m \]
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 $\text{Aut}(\text{GL}_2(\mathbb{F}_\ell))$ 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 $N_v$ be the norm of $v$. We denote the reduction of $E_i$ modulo $v$ by $\bar{E}_{i,v}$. We also denote the Frobenius endomorphism of $\bar{E}_{i,v}$ by $\text{Fr}_{i,v}$ 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 $T_{\ell}(E_i) \cong T_{\ell}(\bar{E}_{i,v})$, we can let $\text{Fr}_{i,v}$ act on $T_{\ell}(E_i)$. Then we can talk about the trace of $\text{Fr}_{i,v}$ and denote it by $\text{Tr}(\text{Fr}_{i,v})$. We also know that $\text{Tr}(\text{Fr}_{i,v}) = 1 + N_v - t_{i,v} \in \mathbb{Z}$ where $t_{i,v}$ is the number of points of $\bar{E}_{i,v}$. Note this is independent of $\ell$. 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 $\ell$ 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 $\ell$.

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

**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 $\text{Tr}(\text{Fr}_{1,v}) = \text{Tr}(\text{Fr}_{2,v})$ 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 $\ell$. 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 $\ell^n$ for some large $n$, we have $\ell^n F(T_\ell(E_1)) \subseteq T_\ell(E_2)$. This tells us that $\text{Hom}_K(T_\ell(E_1), T_\ell(E_2))$ is nonempty. By Isogeny Theorem 7.7. in Chapter III of (Si) (this was proved by Faltings, see (F1) and (F2)), $\text{Hom}_K(E_1, E_2)$ is also nonempty. Therefore, $E_1$ and $E_2$ are isogenous over $K$. \qed

**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 $\ell$, 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 $\ell$.

**Proof.** Assume that $K(E_1[\ell]) = K(E_2[\ell])$ for all but finitely many primes $\ell$. 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 $\ell$, there are infinitely many primes $\ell$ such that $\text{Gal}(K(E_1[\ell])/K) \cong \text{Gal}(K(E_2[\ell])/K) \cong \text{GL}_2(\mathbb{F}_\ell)$, $K(E_1[\ell]) = K(E_2[\ell])$, and $\left(\frac{N_v}{\ell}\right) = 1$. For this $v$, we run the following argument for all these $\ell$. Let $\phi_1 : \text{Gal}(K(E_1[\ell])/K) \cong \text{GL}_2(\mathbb{F}_\ell)$ and $\phi_2 : \text{Gal}(K(E_2[\ell])/K) \cong \text{GL}_2(\mathbb{F}_\ell)$. Consider the commutative diagram

$$
\begin{array}{ccc}
\text{Gal}(K(E_1[\ell])/K) & \xrightarrow{\phi_1} & \text{GL}_2(\mathbb{F}_\ell) \\
\downarrow \phi_2 \phi_1^{-1} & & \downarrow \text{det} \\
\text{Gal}(K(E_2[\ell])/K) & \xrightarrow{\phi_2} & \text{GL}_2(\mathbb{F}_\ell)
\end{array}
$$

(For $\sigma \in \text{Gal}(K(E_i[\ell])/K)$, $\sigma(x) = (x)^{\text{det}(\phi_i(\sigma))} \quad \forall x \in \mu_\ell$. Therefore, the whole diagram
commutes.) Then $\phi_2\phi_1^{-1} : \text{GL}_2(\mathbb{F}_\ell) \cong \text{GL}_2(\mathbb{F}_\ell)$ is an isomorphism. By Lemma 2.3.2, $\text{Aut}(\text{GL}_2(\mathbb{F}_\ell))$ is the direct product of inner automorphisms and radial automorphisms. Pick a $\mathbb{Z}/\ell\mathbb{Z}$-basis of $E_2[\ell]$ such that $\phi_2\phi_1^{-1} : \text{GL}_2(\mathbb{F}_\ell) \cong \text{GL}_2(\mathbb{F}_\ell)$ 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 $m_\ell$. Look at the commutative triangle in the diagram. Let $A \in \text{GL}_2(\mathbb{F}_\ell)$, we have $\det A = (\det A)^{2m_\ell+1}$. So $(\det A)^{2m_\ell} = 1$ for all $A \in \text{GL}_2(\mathbb{F}_\ell)$. Then either $m_\ell = 0$ or $m_\ell = \frac{\ell-1}{2}$.

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

$$\det(Fr_{i,v}) = N_v \equiv \det(\phi_i(\sigma_v)) \pmod{\ell}.$$

So $(\det(\phi_1(\sigma_v)))^{m_\ell} = (N_v)^{m_\ell} = 1$ (no matter $m_\ell = 0$ or $m_\ell = \frac{\ell-1}{2}$) since $(N_v)^{\frac{\ell-1}{2}} = (N_v^\frac{\ell}{2}) = 1$. 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

$$\text{Tr}(Fr_{i,v}) \equiv \text{Tr}(\phi_i(\sigma_v)) \pmod{\ell}.$$

Therefore we get $\text{Tr}(Fr_{1,v}) \equiv \text{Tr}(Fr_{2,v}) \pmod{\ell}$. Run this argument for these infinitely many primes $\ell$, then $\text{Tr}(Fr_{1,v}) = \text{Tr}(Fr_{2,v}) \in \mathbb{Z}$. 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 $\text{Gal}(K(E_1[\ell])/K) \cong \text{Gal}(K(E_2[\ell])/K) \cong \text{GL}_2(\mathbb{F}_\ell)$.

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

---

21
Lemma 2.4.2. Let $F_2 = K(E_1[\ell]) \cap K(E_2[\ell])$.

$$
\begin{array}{c}
\text{K}(E_1[\ell]) \\
\downarrow
\end{array} 
\begin{array}{c}
F_2 \\
\downarrow
\end{array} 
\begin{array}{c}
K(E_2[\ell]) \\
K(\mu_\ell)
\end{array}
$$

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 $F_2 = K(\mu_\ell)$.

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

- If $\text{Gal}(K(E_1[\ell])/F_2) = \{1\}$, then $F_2 = K(E_1[\ell]) = K(E_2[\ell])$.

- If $\text{Gal}(K(E_1[\ell])/F_2) = \{\pm 1\}$, then $[K(E_1[\ell]) : F_2] = [K(E_2[\ell]) : F_2] = 2$.

- If $\text{Gal}(K(E_1[\ell])/F_2) = \text{SL}_2(\mathbb{F}_\ell)$, then $F_2 = K(\mu_\ell)$.

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

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

Lemma 2.4.4. Suppose that $N$ is an abelian $\ell$-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:

\[
\begin{array}{ccc}
K(E_1[\ell], E_2[\ell]) & \rightarrow & N \\
| & | & | \\
K(E_1[\ell]) & \leftarrow & K(E_2[\ell]) \\
| & | & | \\
F_2 & \leftarrow & \leftarrow \\
\end{array}
\]

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

\[K(E_1[\ell], E_2[\ell]) \cap N = K(E_2[\ell]).\] (2.4.5)

By (2.4.5), we have

\[
K(E_1[\ell]) \cap N \subseteq K(E_1[\ell]) \cap K(E_1[\ell], E_2[\ell]) \cap N \\
= K(E_1[\ell]) \cap K(E_2[\ell]) \\
= F_2.
\]

\[\square\]

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

In this section, let $\ell$ be a fixed prime such that $\ell \geq 5$. Assume that $\text{Gal}(K(E_i[\ell])/K) \cong \text{GL}_2(\mathbb{F}_\ell)$ for $i \in \{1, 2\}$ and $K(E_1[\ell]) \neq K(E_2[\ell])$. Recall that $\Sigma$ (associated to this $\ell$) is defined as in §1.4.
Lemma 2.5.1. If $\text{Gal}(K(E[\ell])/K) \cong \text{GL}_2(\mathbb{F}_\ell)$, then

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

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

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

Lemma 2.5.2. There is a $\tau \in G_{K(\mu_\ell)}$ 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 $F_2 = K(\mu_\ell)$ or $[K(E_1[\ell]) : F_2] = [K(E_2[\ell]) : F_2] = 2.$

(i) Assume that $K(E_1[\ell]) \cap K(E_2[\ell]) = F_2 = K(\mu_\ell).$ Let $\tau \in G_{K(\mu_\ell)}$ 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 $\tau$ 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 $B_2$ of $E_2[\ell].$ Let $\tau_2 \in \text{SL}_2(\mathbb{F}_\ell) \cong \text{Gal}(K(E_2[\ell]/K(\mu_\ell)))$ 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 $\tau_2$ has order $\ell.$ Now choose $\tau_1 \in \text{Gal}(K(E_1[\ell]/K(\mu_\ell)))$ to be an element
such that $\tau_1|_{F_2} = \tau_2|_{F_2}$. 

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

We choose $\tau_1$ to be the one with order $2\ell$ in $\text{Gal}(K(E_1[\ell]/K(\mu_\ell))).$ Therefore, $\tau_1^{2\ell} = 1$ in $\text{Gal}(K(E_1[\ell]/K(\mu_\ell)))$. 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 $\tau_1$ in $\text{Gal}(K(E_1[\ell]/K(\mu_\ell)))$ is at most $2$. This contradicts to the fact that $\tau_1$ has order $2\ell$.

- If $f(x) = (x - 1)^2$, then $\tau_1$ satisfies $(x - 1)^2$ and also $x^\ell - 1 = (x - 1)^\ell$. Then order of $\tau_1$ in $\text{Gal}(K(E_1[\ell]/K(\mu_\ell)))$ is at most $\ell$. This also contradicts to the fact that $\tau_1$ has order $2\ell$.

Therefore, $f(x) = (x + 1)^2$ and $\tau_1$ 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 $\tau \in G_{K(\mu_\ell)}$ be an element such that $\tau|_{K(E_1[\ell])} = \tau_1$ and $\tau|_{K(E_1[\ell])} = \tau_2$. Then $\dim_{\mathbb{F}_\ell}(E_1[\ell]/(\tau - 1)E_2[\ell]) = \dim_{\mathbb{F}_\ell}(E_1[\ell]/(\tau_1 - 1)E_2[\ell]) = 0$, 25
\[ \dim_{\mathbb{F}}(E_2[\ell]/(\tau - 1)E_2[\ell]) = \dim_{\mathbb{F}}(E_2[\ell]/(\tau_2 - 1)E_2[\ell]) = 1. \]

\[ \square \]

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

By Lemma 2.5.1, \( K(E_2[\ell]) \) and \( F_1 \) are linearly disjoint over \( K(\mu_\ell). \) Let \( \sigma_1 \in G_K \) such that

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

\[ \sigma_1 = 1 \text{ on } F_1 = K(\mu_\ell, (\mathcal{O}_{K, \Sigma}^\times)^{1/\ell}). \]

This is possible since \( \tau = 1 \) on \( F_1 \cap K(E_2[\ell]) = K(\mu_\ell). \)

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

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

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

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

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

\[ \dim_{\mathbb{F}}(\text{Sel}_\ell(K, E_2)(ap)) = \dim_{\mathbb{F}}(\text{Sel}_\ell(K, E_2)(a)) + 1. \]

**Proof.** Since \( N_a F_1 \) is an abelian \( \ell \)-extension of \( K(E_2[\ell]), \) by Lemma 2.4.4, \( K(E_1[\ell]) \cap N_a F_1 = \)
\( F_2 \). Since \( \tau|_{F_2} = \tau_0 \sigma_1|_{F_2} \), there is some \( \sigma \in G_K \) such that
\[
\sigma = \tau \text{ on } K(E_1[\ell]),
\]
\[
\sigma = \tau_0 \sigma_1 \text{ on } N_a F_1.
\]

Let \( p \) be a prime whose Frobenius conjugacy class in \( \text{Gal}(K(E_1[\ell])/N_a F_1/K) \) is the class of \( \sigma \). Since Frobenius fixes \( \mu_\ell \) and \( (O_{K,\Sigma}^\times)^{1/\ell} \), we have that \( \mu_\ell \) and \( (O_{K,\Sigma}^\times)^{1/\ell} \) are contained in \( K^\times_\ell \). Hence \( Np \equiv 1 \pmod{\ell} \) and the inclusion \( K^\times \hookrightarrow K^\times_\ell \) sends \( O_{K,\Sigma}^\times \) into \( (O_{K,p}^\times)^\ell \), so \( p \in \mathcal{P} \). By Lemma 1.3.4, evaluation of cocycles at a Frobenius element for \( p \) in \( G_K \) induces an isomorphism
\[
\mathcal{H}_\ell(K_p) = H^1_{ur}(K_p, E_1[\ell]) \cong E_1[\ell]/(\tau - 1)E_1[\ell].
\]

Thus \( p \in \mathcal{P}_0(E_1) \). Again, by Lemma 1.3.4, evaluation of cocycles at a Frobenius element for \( p \) in \( G_K \) induces an isomorphism
\[
\mathcal{H}_\ell(K_p) = H^1_{ur}(K_p, E_2[\ell]) \cong E_2[\ell]/(\tau - 1)E_2[\ell].
\]

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

Then by Proposition 2.2.6,
\[
\dim_{F_\ell} \text{Sel}_{\ell}(K, E_2)(ap) = \dim_{F_\ell} \text{Sel}_{\ell}(K, E_2)(a) + 1.
\]

Proposition 2.5.5. Let \( t \geq \dim_{F_\ell} \text{Sel}_{\ell}(K, E_2) \).
(i) There is a finite set of primes $T \subseteq \mathcal{P}_0(E_1) \cap \mathcal{P}_1(E_2)$ such that

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

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

(ii) If $T$ is as in (i), and $L/K$ is a cyclic extension of $K$ of degree $\ell$ that is $T$-ramified and $\Sigma$-split, then

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

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 $\ell$ that is $T$-ramified and $\Sigma$-split, then by Proposition 1.5.3 and Lemma 2.1.6,

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

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

\qed
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 $\ell$ does not divide the discriminant of $\mathcal{O}_M$. We also assume that $\ell$ 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 $\text{End}_K(E') = \mathcal{O}_M$.

*Proof.* This is Proposition 5.3. in (Ru) \hfill \Box

**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 $\ell$ such that $\ell$ is inert in both $M_1$ and $M_2$. 

29
Proof. Let $\sigma$ be the nontrivial element of $\text{Gal}(\mathbb{Q}(\sqrt{D_1}, \sqrt{D_2})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$. If $\ell$ is a prime whose Frobenius in $\text{Gal}(\mathbb{Q}(\sqrt{D_1}, \sqrt{D_2})/\mathbb{Q})$ is $\sigma$, then $\ell$ is inert in both $M_1$ and $M_2$. The Cebotarev Theorem shows that there are infinitely many such primes $\ell$. \hfill $\Box$

**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]). \hfill $\Box$

We assume that $\text{Gal}(K(E[\ell])/K) \cong (\mathcal{O}_M/\ell)^\times$ 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 $\ell$, $\text{Gal}(K(E[\ell])/K) \cong \text{Aut}_{\mathcal{O}_M}(E[\ell]) \cong (\mathcal{O}_M/\ell)^\times$.

**Proof.** This is the Corollary to Theorem 5 in section 4.5 in ([Ser2]). \hfill $\Box$

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

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

**Proof.** Let $L$ be a cyclic extension of degree $\ell$ over $K$ such that $p$ ramifies in $L/K$. Let $V := H^1(K_p, E[\ell]), W_1 := \mathcal{H}_\ell(K_p)$ and $W_2 := \mathcal{H}_\ell(L_p/K_p)$. 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 $<
\(w_1, w_2 \geq 0\), then we just take \(v_1 = w_1\) and \(v_2 = w_2\). Else, let \(\alpha := -\frac{\langle w_1', w_2 \rangle}{\langle w_1, w_2 \rangle}\). Then \(\langle w_1' + \alpha w_1, w_2 \rangle \geq 0\) 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 \(O_M/\ell\), \(W_2\) is spanned by \(v_2\) over \(O_M/\ell\), and \(\langle v_1, v_2 \rangle = 0\). Now we can start to generate the other isotropic subspaces. Let \(\{1, \alpha\}\) be a basis of \(O_M/\ell\) over \(F\). Define \(w_{k+2} := v_1 + kv_2, 1 \leq k \leq \ell - 1\).

\[
\begin{align*}
\langle w_{k+2}, w_{k+2} \rangle &= 2k < v_1, v_2 > = 0, \\
\langle w_{k+2}, \alpha w_{k+2} \rangle &= < v_1, \alpha v_1 > + k < v_1, \alpha v_2 > + k < v_2, \alpha v_1 > + k^2 < v_2, \alpha v_2 > \\
&= k < v_1, \alpha v_2 > + k < v_2, \alpha v_1 > \\
&= k < v_1, \alpha v_2 + \bar{\alpha} v_2 > \quad \text{(using Lemma 16.2(a) in [Mi])} \\
&= k < v_1, (\alpha + \bar{\alpha}) v_2 > \\
&= k(\alpha + \bar{\alpha}) < v_1, v_2 > \quad \text{(since } (\alpha + \bar{\alpha}) \in F\text{)} \\
&= 0, \\
\langle \alpha w_{k+2}, \alpha w_{k+2} \rangle &= < w_{k+2}, \bar{\alpha} \alpha w_{k+2} > \\
&= (\bar{\alpha} \alpha) < w_{k+2}, w_{k+2} > \quad \text{(since } \bar{\alpha} \alpha \in F\text{)} \\
&= 0.
\end{align*}
\]

Therefore, \(W_{k+2}\) spanned by \(w_{k+2}\) over \(O_M/\ell\) for \(1 \leq k \leq \ell - 1\) are different 1-dimensional isotropic \(O_M/\ell\) subspaces of \(V = H^1(K_p, E[\ell])\). Now we have \(\ell + 1\) different 2-dimensional isotropic \(F\) subspaces of \(H^1(K_p, E[\ell])\). 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 \(p \in P_2(E)\), by Neron-Ogg-Shafarevich and the fact that the Frobenius of \(p\) fixes \(E[\ell]\), we have \(G_{K_p}\) acts trivially on \(E[\ell]\) and \(H^1(G_{K_p}, E[\ell]) = \text{Hom}(G_{K_p}, E[\ell])\).

**Lemma 3.1.8.** If \(p \in P\), then \(O_p^\times/(O_p^\times)^\ell \cong \mathbb{Z}/\ell \mathbb{Z}\) and \(K_p^\times/(K_p^\times)^\ell \cong (\mathbb{Z}/\ell \mathbb{Z})^2\).

**Proof.** First we prove that \(O_p^\times/(O_p^\times)^\ell \cong \mathbb{Z}/\ell \mathbb{Z}\). Let \(k_p\) be the residue field of \(K_p\). Since
\( p \in \mathcal{P} \subseteq \mathcal{Q}, \ k_p^\times/(k_p^\times)^\ell \cong \mathbb{Z}/\ell \mathbb{Z} \). Consider the commutative diagram of exact sequences,

\[
\begin{array}{c}
1 \rightarrow 1 + p\mathcal{O}_p \rightarrow \mathcal{O}_p^\times \rightarrow (\mathcal{O}/p\mathcal{O})^\times \rightarrow 1 \\
\uparrow \ell & \uparrow \ell & \uparrow \ell \\
1 \rightarrow 1 + p\mathcal{O}_p \rightarrow \mathcal{O}_p^\times \rightarrow (\mathcal{O}/p\mathcal{O})^\times \rightarrow 1.
\end{array}
\]

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

\[
0 \rightarrow \mathcal{O}_p^\times/(\mathcal{O}_p^\times)^\ell \rightarrow k_p^\times/(k_p^\times)^\ell \rightarrow 0.
\]

Therefore, \( \mathcal{O}_p^\times/(\mathcal{O}_p^\times)^\ell \cong \mathbb{Z}/\ell \mathbb{Z} \).

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

\[
\begin{array}{c}
0 \rightarrow \mathcal{O}_p^\times \rightarrow K_p^\times \rightarrow \mathbb{Z} \rightarrow 0 \\
\downarrow \ell & \downarrow \ell & \downarrow \ell \\
0 \rightarrow \mathcal{O}_p^\times \rightarrow K_p^\times \rightarrow \mathbb{Z} \rightarrow 0.
\end{array}
\]

Again we apply snake lemma, then we have

\[
0 \rightarrow \mathcal{O}_p^\times/(\mathcal{O}_p^\times)^\ell \rightarrow K_p^\times/(K_p^\times)^\ell \rightarrow \mathbb{Z}/\ell \mathbb{Z} \rightarrow 0.
\]

Therefore, \( K_p^\times/(K_p^\times)^\ell \cong (\mathbb{Z}/\ell \mathbb{Z})^2 \).

\[\square\]

**Lemma 3.1.9.** Let \( p \in \mathcal{P}_2(E) \). Let \( \mathcal{L} \) be an extension of \( K_p \) of degree \( \ell \). Then

\[
\mathcal{H}_\ell(\mathcal{L}/K_p) = H^1(\text{Gal}(\mathcal{L}/K_p), E[\ell]) = \text{Hom}(\text{Gal}(\mathcal{L}/K_p), E[\ell]).
\]
Proof. Consider the following commutative diagram:

\[
\begin{array}{ccc}
A_{\mathcal{L}}(K_p)/\lambda_{\mathcal{L}}A_{\mathcal{L}}(K_p) & \xrightarrow{f} & A_{\mathcal{L}}(\mathcal{L})/\lambda_{\mathcal{L}}A_{\mathcal{L}}(\mathcal{L}) \\
\downarrow i & & \downarrow \\
H^1(K_p, A_{\mathcal{L}}[\lambda_{\mathcal{L}}]) & \xrightarrow{g} & H^1(\mathcal{L}, A_{\mathcal{L}}[\lambda_{\mathcal{L}}])
\end{array}
\]

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, $H_\ell(\mathcal{L}/K_p) = \text{im}(i) \subseteq \ker(g) = H^1(\text{Gal}(\mathcal{L}/K_p), E[\ell])$. Since they have the same cardinality, $H_\ell(\mathcal{L}/K_p) = H^1(\text{Gal}(\mathcal{L}/K_p), E[\ell])$.

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

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

\[
H_\ell(\mathcal{L}_i/K_p) = H^1(\text{Gal}(\mathcal{L}_i/K_p), E[\ell]) \\
= \text{Hom(\text{Gal}(\mathcal{L}_i/K_p), E[\ell])} \\
= \{ f \in \text{Hom}(G_\ell, E[\ell]) : H_i \subseteq \ker(f) \}.
\]
Therefore,

\[ \mathcal{H}_\ell(L_1/K_p) \cap \mathcal{H}_\ell(L_2/K_p) = \{ f \in \text{Hom}(G_\ell, E[\ell]) : H_1 \cup H_2 \subseteq \ker(f) \} = \{ f \in \text{Hom}(G_\ell, E[\ell]) : \ker(f) = G_\ell \} = \{0\}. \]

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 \( K_p \) of degree \( \ell \) and the 2-dimensional isotropic \( \mathbb{F}_\ell \) subspaces of \( H^1(K_p, E[\ell]) \). \( \square \)

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

Conversely, let \( \mathcal{L} \) be an extension of \( K_p \) of degree \( \ell \). Then we define \( W_\mathcal{L} \) to be the isotropic subspace corresponding to \( \mathcal{L} \).

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

\[
\text{Sel}_\ell(K, E)^b_a(\prod_{i=1}^r W_i) := \begin{cases} 
\text{loc}_v(c) \in \mathcal{H}_\ell(K_v) & \text{if } v \nmid ab \prod_{i=1}^r p_i \\
\text{loc}_v(c) = 0 & \text{if } v | a \\
\text{loc}_v(c) \in W_i & \text{if } v = p_i 
\end{cases}
\]

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

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

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

If there is no \( p_i \)'s, we have simply \( \text{Sel}_\ell(K, E)_a^b \).

**Definition 3.1.13.** Suppose \( T_0 \) and \( T_1 = \{p_i\}_{i=1}^r \) are finite subsets of \( \mathcal{P} \). For each \( i \), let \( \mathcal{L}_i \) be a cyclic extension of \( K_{p_i} \) of degree \( \ell \). Let \( \mathcal{L} := (\mathcal{L}_1, \mathcal{L}_2, \ldots, \mathcal{L}_r) \). 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 \( L_{p_i} \) (the completion of \( L \) above \( p_i \)) is \( \mathcal{L}_i \).

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

\[
\text{Sel}_\ell(L/K, E) = \text{Sel}_\ell(K, E).
\]

**Proof.** This follows immediately from Proposition 1.5.3. \( \square \)

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

\[
\text{Sel}_\ell(L/K, E) = \text{Sel}_\ell(K, E)(W).
\]

**Proof.** By definition, \( \text{Sel}_\ell(L/K, E) = \{c \in H^1(K, E[\ell]) : \text{loc}_p(c) \in \mathcal{H}_\ell(L_p/K_p) \text{ for every } p \} \).

On the other hand,

\[
\text{Sel}_\ell(K, E)(W) := \left\{ \begin{array}{ll}
c \in H^1(K, E[\ell]) : & \text{loc}_p(c) \in \mathcal{H}_\ell(K_p) \quad \text{if } p \nmid \prod_{i=1}^r p_i \\
& \text{loc}_p(c) \in W_i \quad \text{if } p = p_i
\end{array} \right\}.
\]
If $p \in T_0$, then $H^1(K, E[\ell]) = H_\ell(K_p) = H_\ell(L_p/K_p) = 0$. If $p \notin T_0 \cup T_1$, by Lemma 3.2.1, Definition 3.1.10, and Definition 3.1.13, $W_i = H_\ell(L_{W_i}/K_p) = H_\ell(L_p/K_p)$. If $p \notin T_0 \cup T_1$, by Lemma 3.1.10, Definition 3.1.11, and Definition 3.1.13, $W_i = H_\ell(L_{W_i}/K_p) = H_\ell(L_p/K_p)$. Therefore, $\text{Sel}_\ell(L/K, E) = \text{Sel}_\ell(K, E)(W)$.

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 $O_M$ and $M \subseteq K$. Let $\ell$ be a fixed prime such that $\text{Gal}(K(E[\ell])/K) \cong (O_M/\ell)^\times$. We also assume that $\ell$ does not divide the discriminant of $O_M$. Let $\Sigma$ 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 $\sigma$ under any cocycle representing $c$. This is well-defined.

**Definition 3.2.1.** Recall that $F_1 := K(\mu_\ell, (O_{K, \Sigma}^\times)^{1/\ell})$. Suppose $\sigma \in G_{F_1(E[\ell])}$.

Let $\{p_i\}_{i=1}^r \subseteq P_2(E)$ and $W_i$ be isotropic subspaces of $H^1(K_{p_i}, E[\ell])$. Let $W := \prod_{i=1}^r W_i \subseteq \prod H^1(K_{p_i}, E[\ell])$. If $c \in \text{Sel}_\ell(K, E)(W)$, 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 $\cap_{c \in \text{Sel}_\ell(K, E)(W)} \ker(\tilde{c})$.

**Lemma 3.2.2.** Suppose $\sigma \in G_{F_1(E[\ell])}$. Let $\{p_i\}_{i=1}^r \subseteq P_2(E)$ and $W_i$ be isotropic subspaces of $H^1(K_{p_i}, E[\ell])$. Let $W := \prod_{i=1}^r W_i$. Let $N_W$ be as in Definition 3.2.1. Assume that $p$ is a
prime that splits completely in $N_{W}F_1/K$. Then $p \in \mathcal{P}_2(E)$ and $\text{loc}_p(\text{Sel}_\ell(K,E)(W)) = 0$.

**Proof.** Since $p$ splits completely in $N_{W}F_1/K$, we have that $\mu_\ell$ and $(\mathcal{O}_{K,\Sigma}^\times)^{1/\ell}$ are contained in $K_p^\times$. Hence $Np \equiv 1 \pmod{\ell}$ and the inclusion $K^\times \hookrightarrow K_p^\times$ sends $\mathcal{O}_{K,\Sigma}^\times$ into $(\mathcal{O}_{K,p}^\times)^{1/\ell}$, so $p \in \mathcal{P}$.

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

$$H_\ell(K_p) = H^1_{ur}(K_p, E[\ell]) \cong E[\ell].$$

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

$$\text{loc}_p : \text{Sel}_\ell(K,E)(W) \to H_\ell(K_p) \cong H^1_{ur}(K_p, E[\ell]) \cong E[\ell].$$

Therefore, $\text{loc}_p(\text{Sel}_\ell(K,E)(W)) = 0$. □

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

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

By Theorem 1.4.5,

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

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

Hence, focus on $p$ alone, we have $<\text{loc}_p(c), \text{loc}_p(d)>_p = 0$ and $\text{loc}_p(\text{Sel}_\ell(K,E)^p(W))$ is an isotropic subspace. □
Proposition 3.2.4. Suppose $\sigma \in G_{F_1(E[\ell])}$. Let $\{p_i\}_{i=1}^r \subseteq \mathcal{P}_2(E)$ and $W_i$ be isotropic subspaces of $H^1(K_{p_i}, E[\ell])$. Let $W = \prod_{i=1}^r W_i$. Let $N_W$ be as in Definition 3.2.1. If $p$ is a prime that splits completely in $N_W F_1/K$, define $W_{r+1} := \text{loc}_p(\text{Sel}_\ell(K, E)^p(W))$ an isotropic subspace of $H^1(K_p, E[\ell])$. Then

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

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

$$0 \longrightarrow \text{Sel}_\ell(K, E)_p(W) \longrightarrow \text{Sel}_\ell(K, E)(W) \longrightarrow H_\ell(K_p).$$

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

$$\dim_{F_\ell} \text{Sel}_\ell(K, E)_p(W) = \dim_{F_\ell} \text{Sel}_\ell(K, E)(W). \quad (3.2.5)$$

Then we consider the exact sequences

$$0 \longrightarrow \text{Sel}_\ell(K, E)_p(W) \longrightarrow \text{Sel}_\ell(K, E)(W \times W_{r+1}) \longrightarrow W_{r+1}$$

and

$$0 \longrightarrow \text{Sel}_\ell(K, E)(W \times W_{r+1}) \longrightarrow \text{Sel}_\ell(K, E)^p(W) \longrightarrow H^1(K_p, E[\ell])/W_{r+1}. \quad (3.2.6)$$

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

$$\dim_{F_\ell} \text{Sel}_\ell(K, E)(W \times W_{r+1}) = \dim_{F_\ell} \text{Sel}_\ell(K, E)_p(W) + 2. \quad (3.2.7)$$
Combine (3.2.5) and (3.2.7), we get

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

\[\square\]

### 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 $\mathcal{O}_M$ (End$_K(E) = \mathcal{O}_M$) and $M \subseteq K$. We also assume that $\ell$ does not divide the discriminant of $\mathcal{O}_M$.

Let $K^{ab}$ denote the maximal abelian extension of $K$ and $[\cdot, K^{ab}/K]$ 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 $y = N_{K/M}x \in \mathbb{A}_M^\times$, 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 $p$ is a prime of
Then \( \psi(x)(N_{K/M}x)^{-1} \in \mathcal{O}_{M,p}^\times \) and for every \( P \in E[p^\infty] \)

\[
[x, K^{ab}/K]P = \psi(x)(N_{K/M}x)^{-1}P.
\]

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

\[
\psi(\mathcal{U}_q) = 1 \iff E \text{ has good reduction at } q.
\]

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

Let \( f = f_E \) denote the conductor of the Hecke character \( \psi \) of Theorem 3.3.1. We can view \( \psi \) as a character of fractional ideals of \( K \) prime to \( f \) in the usual way.

**Corollary 3.3.2.** As a character on ideals, \( \psi \) satisfies

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

(ii) if \( q \) is a prime of \( K \) not dividing \( f \) and \( b \) is an ideal of \( \mathcal{O}_M \) prime to \( q \), then \([q, K(E[b])/K]\)

acts on \( E[b] \) by multiplication by \( \psi(q) \).

(iii) if \( q \) is a prime of \( K \) where \( E \) has good reduction and \( q = N_{K/Q}q \), then \( \psi(q) \in \mathcal{O}_M \)

reduces modulo \( q \) to the Frobenius endomorphism \( \varphi_q \) of \( \tilde{E} \).

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

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

**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 \( m \) be an ideal of \( \mathcal{O}_M \). Let \( \ell \) be a prime such that \( \text{Gal}(K(E[\ell])/K) \cong (\mathcal{O}_M/\ell)^\times \), \( \ell \) is coprime to \( m \), \( \ell \) is unramified in \( K/Q \), \( \ell \) is inert in \( M \), and \( E \) has good reduction at all \( \lambda|\ell \). Then \( K(E[\ell])/K \) and \( K^m \) are linearly disjoint over \( K \).
Proof. We prove that $K(E[\ell])/K$ and $K^m$ are linearly disjoint over $K$ by showing that for $\lambda|\ell$, $\lambda$ is totally ramified in $K(E[\ell])/K$:

\begin{align*}
K(E[\ell]) & \xrightarrow{g} K^m \\
& \xrightarrow{h} K
\end{align*}

Consider $f$ to be the composition of the following maps:

$$f : \mathbb{A}_K^\times \to \text{Gal}(K^{ab}/K) \to \text{Aut}_{O_M}(E[\ell]) \cong (O_M/\ell)^\times.$$  

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

$$[x, K^{ab}/K]P = (N_{K/M}x)^{-1}_\ell P, \quad (N_{K/M}x)^{-1}_\ell \in O_M^{\times}.$$  

Therefore, we have:

$$f : \mathcal{U}_\lambda \longrightarrow O_M^{\times} \longrightarrow (O_M/\ell)^\times.$$  

The first map is surjective since $\ell$ 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 $(O_M/\ell)^\times$ and $g|_{I_\lambda(K^{ab}/K)}$ is also surjective to $\text{Aut}_{O_M}(E[\ell])$.

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

\[
\begin{array}{ccc}
I_\lambda(K^{ab}/K) & \xrightarrow{g} & \text{Aut}_{\mathcal{O}_M}(E[\ell]) \\
\downarrow{\pi'} & \cong & \downarrow{\cong} \\
\text{Gal}(K(E[\ell])/K) & \end{array}
\]

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

Now we know that \(\lambda\) is totally ramified in \(K(E[\ell])/K\) but unramified in \(K^m/K\). Therefore, \(K(E[\ell])/K\) and \(K^m\) 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 \(\psi_1\) and \(\psi_2\) for \(E_1\) and \(E_2\) respectively. Assume that \(\psi_1\) has conductor \(f_1\), and \(\psi_2\) has conductor \(f_2\). We view \(\psi_1\) and \(\psi_2\) as characters of conductor \(f := f_1 \cdot f_2\).

Let \(J^f_K := \text{the group of all fractional ideals relatively prime to } f\) and \(P^f_K := \text{the group of all principal ideals } (a) \text{ such that } a \equiv 1 \text{ (mod } f)\) and \(a\) totally positive. Let \(C^f_K := J^f_K/P^f_K\) and \(K^f := \text{the ray class field modulo } f\). By class field theory, there is an isomorphism between \(J^f_K/P^f_K\) and \(\text{Gal}(K^f/K)\).

If \(a \in P^f_K\), then \(a = (\alpha)\) for some \(\alpha \equiv 1 \text{ (mod } f)\). We have \(\psi_1(a) = \psi_2(a) = N_{K/M}(\alpha)\) and \(\psi_1(a)\psi_2^{-1}(a) = 1\). Define \(\epsilon := \psi_1\psi_2^{-1}\). We can view \(\epsilon\) as a character on \(C^f_K\).

**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 $\ell$, $K(E_1[\ell]) \neq K(E_2[\ell])$ and $\ell$ 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 $\ell$, $\text{Gal}(K(E_i[\ell])/K) \cong (\mathcal{O}_M/\ell)^\times$ for $i \in \{1, 2\}$. For these $\ell$ and for any place $v$ of $K$, let $(\sigma_i)_v$ be the Frobenius element of $v$ in $\text{Gal}(K(E_i[\ell])/K) \cong (\mathcal{O}_M/\ell)^\times$. Then $\psi_i(v) \in \mathcal{O}_M$ and its reduction modulo $\ell$ 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 $\mathcal{C} \in C]\ell^\dagger_K \cong \text{Gal}(K^\dagger/K)$ such that $\epsilon(\mathcal{C}) \neq 1$.

By Lemma 3.1.2 and Proposition 3.1.4, for infinitely many primes $\ell$, $\text{Gal}(K(E_i[\ell])/K) \cong (\mathcal{O}_M/\ell)^\times$, $\ell$ is coprime to $f$, $\ell$ is unramified in $K/\mathbb{Q}$, $\ell$ 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 $\ell$, $K(E_1[\ell]) \neq K(E_2[\ell])$.

By Lemma 3.3.3, $K(E_1[\ell])/K$ and $K^\dagger$ are linearly disjoint over $K$. We can find a place $v$ such that the Frobenius element $\sigma_v = 1$ on $E_1[\ell]$ and $\sigma_v = \phi_v(\mathcal{C})$ on $K^\dagger$ where $\phi_v$ is defined to be the isomorphism $J^\dagger_{\mathbb{Q}}/P^\dagger_{\mathbb{Q}} \cong \text{Gal}(K^\dagger/K)$. By Corollary 3.3.2(iii) and the fact that the Frobenius endomorphism of $\tilde{E}$ corresponds to the Frobenius element $\sigma_v$, that is to say, $\psi_1(v) \equiv 1 \pmod{\ell}$ and $\psi_2(v) \equiv \epsilon(v)^{-1} = \epsilon(\mathcal{C})^{-1} \neq 1 \pmod{\ell}$. Therefore, by Corollary 3.3.2 (ii) and (iii), $\sigma_v$ 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 $\ell$, $K(E_1[\ell]) \neq K(E_2[\ell])$ and $\ell$ is inert in both $M_1$ and $M_2$.

**Proof.** Consider those primes $\ell$ 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 $\ell$. Pick any prime $\ell$ from this set. We will prove that $K(E_1[\ell]) \neq K(E_2[\ell])$.

Consider the following diagram:

\[ \begin{array}{ccc}
K(E_1[\ell]) & \to & K(E_2[\ell]) \\
\downarrow & & \downarrow \\
K & \to & K \\
\downarrow & & \downarrow \\
M_1 M_2 & \to & M_1 M_2 \\
\downarrow & & \downarrow & & \downarrow \\
<\sigma_1> & <\sigma_2> & <\sigma_1> & <\sigma_2> & <\sigma_1> \\
\downarrow & & \downarrow & & \downarrow \\
M_1 & \to & M_2 \\
\downarrow & & \downarrow & & \downarrow \\
Q & \to & Q
\end{array} \]

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

\[ \pi_i := \pi \circ N_{M_1 M_2/M_i} : U_{M_1 M_2,\ell} \to U_{M_i,\ell} \to \mathcal{O}_{M_i/\ell}^\times \]

is surjective since $\ell$ is unramified in $K/Q$.

First choose $z \in U_{M_1 M_2,\ell}$ such that

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

(3.3.8)

Take $y = z/z^{\sigma_1} \in U_{M_1 M_2,\ell}$ where $\text{Gal}(M_1 M_2/M_1) = \langle \sigma_1 \rangle$, then

\[ \pi_1(y) = \pi_1(z/z^{\sigma_1}) = 1, \]
\[ \pi_2(y) = \pi_2(z)/\pi_2(z)^{\sigma_1} \] (3.3.9)

Consider the action of \( \sigma_1 \) on \((\mathcal{O}_{M_2}/\ell)\), \( \sigma_1 \) is the generator of the decomposition group of \( \ell \) which is isomorphic to \( \text{Gal}((\mathcal{O}_{M_2}/\ell)/\mathbb{Z}/\ell\mathbb{Z}) \). By (3.3.8) and (3.3.9), we know that \( \pi_2(y) \neq 1 \pmod{\ell} \).

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

**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 \( \ell \), \( K(E_1[\ell]) \neq K(E_2[\ell]) \).

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

### 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 \( \text{Gal}(K(E_i[\ell])/K) \cong \text{Aut}_{\text{End}_{K}(E_i)}(E_i[\ell]) \) for \( i \in \{1, 2\} \). If \( E_i \) has CM by \( \mathcal{O}_{M_i} \) we further assume that \( \ell \) is inert in \( M_i, M_i \subseteq K \) and \( \ell \) 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 \( F_2 := K(E_1[\ell]) \cap K(E_2[\ell]) = K(\mu_\ell) \).
Proof. In this case, 

\[
\begin{array}{c}
\text{SL}_2(\mathbb{F}_\ell) \\
\uparrow \\
K(\mu_\ell) \\
\downarrow \\
K(E_1[\ell]) \\
\end{array}
\xrightarrow{c_{\ell+1}} 
\begin{array}{c}
K(E_2[\ell]) \\
\end{array}
\]

\[\text{Gal}(K(E_2[\ell])/K(\mu_\ell)) \cong C_{\ell+1}\]

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

\[\square\]

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

*Proof.*

- If $E_1$ has no CM, then there is no nontrivial $\ell$-extension of $F_2$ in $K(E_1[\ell])$ by Lemma 3.4.1 and the fact that $\text{SL}_2(\mathbb{F}_\ell)$ has no quotient of order $\ell$.

- If $E_1$ has CM, then $\text{Gal}(K(E_1[\ell])/F_2)$ is a subgroup of $C_{\ell+1}$ and there is no nontrivial $\ell$-extension of $F_2$ in $K(E_1)[\ell]$.

\[\square\]

**Lemma 3.4.3.** Suppose that $N$ is an abelian $\ell$-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:

\[
\begin{array}{c}
K(E_1[\ell], E_2[\ell]) \\
\downarrow \\
K(E_1[\ell]) \\
\downarrow \\
F_2 \\
\end{array}
\xrightarrow{N} 
\begin{array}{c}
K(E_2[\ell]) \\
\end{array}
\]

By the definition of $F_2$, $\text{Gal}(K(E_1[\ell], E_2[\ell])/K(E_2[\ell])) \cong \text{Gal}(K(E_1[\ell])/F_2)$. Therefore, by
Lemma 3.4.2,

\[ K(E_1[\ell], E_2[\ell]) \cap N = K(E_2[\ell]). \quad (3.4.4) \]

By (3.4.4), we have

\[ K(E_1[\ell]) \cap N \subseteq K(E_1[\ell]) \cap K(E_1[\ell], E_2[\ell]) \cap N \]
\[ = K(E_1[\ell]) \cap K(E_2[\ell]) \]
\[ = F_2. \]

\[ \square \]

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

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

If \( E_1 \) has no CM, let \( \tau_1 \in G_{K(\mu_\ell)} \) be an element that acts like \( \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix} \) on \( E_1[\ell] \). If \( E_1 \) has CM, let \( \tau_1 \in G_{K(\mu_\ell)} \) be a non-identity element in \( \text{Gal}(K(E_1[\ell])/F_2) \). Therefore, \( \dim_{F_2}(E_1[\ell]/(\tau_1 - 1)E_1[\ell]) = 0. \)
Let $\tau_2 \in G_{K(\mu_\ell)}$ be the identity map on $E_2[\ell]$. Therefore, $\dim_{F_\ell}(E_2[\ell]/(\tau_2 - 1)E_2[\ell]) = 2$.

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

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

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

Let $\{p_i\}_{i=1}^r \subseteq \mathcal{P}_2(E_2)$ and $W_i$ be isotropic subspaces of $H^1(K_{p_i}, E_2[\ell])$. Let $W := \prod_{i=1}^r W_i$.

If $c \in \text{Sel}_\ell(K, E_2)(W)$, 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 $\cap_{c \in \text{Sel}_\ell(K, E_2)(W)} \ker(\tilde{c})$.

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

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

**Proof.** Since $N_W F_1$ is an abelian $\ell$-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 $p_{r+1}$ be a prime whose Frobenius conjugacy class in $\text{Gal}(K(E_1[\ell])N_W F_1/K)$ is the class of $\sigma$. Since Frobenius fixes $\mu_\ell$ and $(\mathcal{O}_{K,\Sigma}^{\times})^{1/\ell}$, we have that $\mu_\ell$ and $(\mathcal{O}_{K,\Sigma}^{\times})^{1/\ell}$ are contained in $K_{p_{r+1}}^{\times}$. Hence $Np_{r+1} \equiv 1 \pmod{\ell}$ and the inclusion $K^{\times} \hookrightarrow K_{p_{r+1}}^{\times}$ sends $\mathcal{O}_{K,\Sigma}$ into $(\mathcal{O}_{p_{r+1}}^{\times})^{\ell}$,
so $p_{r+1} \in P$. By Lemma 1.3.4, evaluation of cocycles at a Frobenius element for $p_{r+1}$ in $G_K$ induces an isomorphism

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

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

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

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

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

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

\[ \square \]

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

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

$$\dim_{F_{\ell}} \text{Sel}_\ell(K, E_2)(W) = t,$$

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

(ii) If $T_1$ and $W_i$ are as in (i), $\mathcal{L} := (\mathcal{L}_{W_1}, \mathcal{L}_{W_2}, \ldots, \mathcal{L}_{W_r})$, $T_0 = \{w_i\}_{i=1}^r$ 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 $\ell$ that has splitting
data \((\Sigma, T_0, T_1, \mathcal{L})\), then

\[
\dim_{\mathcal{F}} \text{Sel}_\ell(L/K, E_1) = \dim_{\mathcal{F}} \text{Sel}_\ell(K, E_1), \quad \dim_{\mathcal{F}} \text{Sel}_\ell(L/K, E_2) = t.
\]

**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 \(\ell\) that has splitting data \((\Sigma, T_0, T_1, \mathcal{L})\), then by Proposition 3.1.14 and Lemma 3.1.15,

\[
\dim_{\mathcal{F}} \text{Sel}_\ell(L/K, E_1) = \dim_{\mathcal{F}} \text{Sel}_\ell(K, E_1),
\]

\[
\dim_{\mathcal{F}} \text{Sel}_\ell(L/K, E_2) = \dim_{\mathcal{F}} \text{Sel}_\ell(K, E_2)(W) = t.
\]

\[\square\]

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

\[
1 \rightarrow \mathcal{O}_{K, \Sigma_i}^\times \rightarrow \mathcal{O}_{K, \Sigma'}^\times \xrightarrow{\text{ord}_{p_i}(\cdot)} \mathbb{Z} \rightarrow 1 \rightarrow 1.
\]

Define \(\beta_i\) to be a preimage of 1 in this diagram.

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

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

If \(E_1\) has no CM, let \(\tau_1 \in G_{K(\mu_\ell)}\) be an element that acts like

\[
\begin{pmatrix}
-1 & -1 \\
0 & -1
\end{pmatrix}
\]
on \(E_1[\ell]\). If
$E_1$ has CM, let $\tau_1 \in G_{K(\mu_\ell)}$ be a non-identity element in $\text{Gal}(K(E_1[\ell])/F_2)$. Therefore, 
$\dim_{F_\ell}(E_1[\ell]/(\tau_1 - 1)E_1[\ell]) = 0$.

Let $\tau_2 \in G_{K(\mu_\ell)}$ be a non-identity element in $\text{Gal}(K(E_2[\ell])/F_2)$. Therefore, 
$\dim_{F_\ell}(E_2[\ell]/(\tau_2 - 1)E_2[\ell]) = 0$.

Let $\tau_3, i \in G_{K(\mu_\ell)}$ be a non-identity element in $\text{Gal}(M'/M_i)$.

By the same reason as Lemma 2.5.1, $K(E_2[\ell])$ and $M'$ are linearly disjoint over $K(\mu_\ell)$. Let 
$\sigma_2, i \in G_K$ such that 
$\sigma_2, i = \tau_2$ on $K(E_2[\ell])$, 
$\sigma_2, i = \tau_3, i$ on $M' = K(\mu_\ell, (\mathcal{O}_{K, \Sigma_i}^\times)^{1/\ell})$.

Since $M'(E_2[\ell])$ is an abelian $\ell$-extension of $K(E_2[\ell])$, by Lemma 3.4.3, $K(E_1[\ell]) \cap M'(E_2[\ell]) = F_2$. 
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 
$\sigma_i = \tau_1$ on $K(E_1[\ell])$, 
$\sigma_i = \sigma_2, i$ on $M'(E_2[\ell])$.

Let $w_i$ be a prime whose Frobenius conjugacy class in $\text{Gal}(M'(E_1[\ell], E_2[\ell])/K)$ is the class of $\sigma_i$. 
Since Frobenius fixes $\mu_\ell$ and $(\mathcal{O}_{K, \Sigma_i}^\times)^{1/\ell}$, we have that $\mu_\ell$ and $(\mathcal{O}_{K, \Sigma_i}^\times)^{1/\ell}$ are contained 
in $K_w$. Hence $N w_i \equiv 1 \pmod{\ell}$ and the inclusion $K^\times \hookrightarrow K_w^\times$ sends $\mathcal{O}_{K, \Sigma_i}^\times$ into $(\mathcal{O}_{w_i}^\times)^{\ell}$, so 
w_i $\in \mathcal{P}$. On the other hand, Frobenius does not fix $(\mathcal{O}_{K, \Sigma_i}^\times)^{1/\ell}$, we have that $\beta_i \notin (\mathcal{O}_{w_i}^\times)^{\ell}$.

By Lemma 1.3.4, evaluation of cocycles at a Frobenius element for $w_i$ in $G_K$ induces an isomorphism

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

Thus $w_i \in \mathcal{P}_0(E_1) = 0$. Again, by Lemma 1.3.4, evaluation of cocycles at a Frobenius element
for \( w_i \) in \( G_K \) induces an isomorphism

\[
H_{\ell}(K_{w_i}) = H_{ur}^{1}(K_{w_i}, E_2[\ell]) \cong E_2[\ell]/(\tau_2 - 1)E_2[\ell] = 0.
\]

Thus \( w_i \in P_0(E_2) = 0 \). \( \square \)

**Lemma 3.5.6.** Suppose \( T_0 = \{ w_i \}_{i=1}^r \) and \( T_1 = \{ p_i \}_{i=1}^r \) are finite subsets of \( P \). Let

\[
H' := \mathbb{A}_K^\times \prod_{v \in \Sigma} K_v^\times \prod_{v \notin \Sigma \cup T_0 \cup T_1} \mathcal{O}_v^\times (\prod_{i=1}^r (K_{p_i}^\times)'(\prod_{i=1}^r (\mathcal{O}_{w_i}^\times)').
\]

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

**Proof.** Consider the surjective map:

\[
\phi : \prod_{i=1}^r \mathcal{O}_{p_i}^\times \times \prod_{i=1}^r \mathcal{O}_{w_i}^\times \to \mathbb{A}_K^\times / H'.
\]

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

\[
\bar{\phi} : \prod_{i=1}^r (\mathcal{O}_{p_i}^\times/(\mathcal{O}_{p_i}^\times)^\ell) \times \prod_{i=1}^r (\mathcal{O}_{w_i}^\times/(\mathcal{O}_{w_i}^\times)^\ell) \to \mathbb{A}_K^\times / H'.
\]

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

**Lemma 3.5.7.** Suppose \( T_1 = \{ p_i \}_{i=1}^r \) is a finite subset of \( P_0(E_1) \cap P_2(E_2) \). Let \( \mathcal{L}_i \) be extensions of \( K_{p_i} \) of degree \( \ell \). Let \( \mathcal{L} := (\mathcal{L}_1, \mathcal{L}_2, \cdots, \mathcal{L}_r) \). Then there exist a finite subset \( T_0 = \{ w_i \}_{i=1}^r \) of \( P_0(E_1) \cap P_0(E_2) \) and a cyclic extension \( L/K \) of degree \( \ell \) that has splitting data \( (\Sigma, T_0, T_1, \mathcal{L}) \).

**Proof.** By Lemma 3.5.5, there exist \( T_0 = \{ w_i \}_{i=1}^r \subseteq P_0(E_1) \cap P_0(E_2) \) such that \( \mathcal{O}_{K_{w_i}}^\times \subseteq \)
\( (\mathcal{O}_{m_i}^\infty)\ell \) and \( \beta_i \notin (\mathcal{O}_{m_i}^\infty)\ell \) for all \( i \). Let

\[
H' := K^\times \prod_{v \in \Sigma} K_v^\times \left( \prod_{v \notin \Sigma \cup T_0 \cup T_1} \mathcal{O}_v^\times \right)^\ell \left( \prod_{i=1}^r (K_{p_i}^\times)^\ell \right) \left( \prod_{i=1}^r (\mathcal{O}_{m_i}^\times)^\ell \right)
\]

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

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

(i) Assume that \( (u_1, \ldots, u_r) \in (\mathcal{O}_{p_1}^\times \times \cdots \times \mathcal{O}_{p_r}^\times) \cap H' \). Then \( (u_1, \cdots, u_r) = \alpha \cdot (\prod_{v \in \Sigma} \alpha^{-1}) \cdot (\prod_{e \notin \Sigma \cup T_0 \cup T_1} v_i) \cdot (\prod_{i=1}^r \alpha^{-1}) \), where \( \alpha \in K \) and \( v_i \in (K_{p_i}^\times)^\ell \). We have \( \alpha \in \mathcal{O}_{K, \Sigma}^\times \) and \( u_i = \alpha \cdot v_i \). Compute the order, \( \text{ord}_{p_i}(\alpha) = -\text{ord}_{p_i}(v_i) = k_i \cdot \ell \) for \( k_i \in \mathbb{Z} \).

Therefore,

\[
\left( \frac{\alpha}{\beta_1^{\ell k_1} \cdots \beta_r^{\ell k_r}} \right) \in \mathcal{O}_{K, \Sigma}^\times \Rightarrow \left( \frac{\alpha}{\beta_1^{\ell k_1} \cdots \beta_r^{\ell k_r}} \right) \in (\mathcal{O}_{K_{p_i}}^\times)^\ell \\
\Rightarrow \alpha \in (K_{p_i}^\times)^\ell \\
\Rightarrow u_i \in (K_{p_i}^\times)^\ell \cap \mathcal{O}_{p_i}^\times \\
\Rightarrow u_i \in (\mathcal{O}_{p_i}^\times)^\ell.
\]

(ii) Assume that \( (\lambda_1, \cdots, \lambda_r) \in K_{p_1}^\times \times \cdots \times K_{p_r}^\times \cap H' \). Then \( (\lambda_1, \cdots, \lambda_r) = \alpha \cdot (\prod_{v \in \Sigma} \alpha^{-1}) \cdot (\prod_{e \notin \Sigma \cup T_0 \cup T_1} \gamma_i) \cdot (\prod_{i=1}^r \alpha^{-1}) \), where \( \alpha \in K \) and \( \gamma_i \in (K_{p_i}^\times)^\ell \). We have \( \alpha \in \mathcal{O}_{K, \Sigma}^\times, \alpha \in (\mathcal{O}_{m_i}^\times)^\ell \) and \( \lambda_i = \alpha \cdot \gamma_i \). Define \( n_i := \text{ord}_{p_i}(\alpha) \). Compute the order, \( \text{ord}_{p_i}(\lambda_i) = n_i + g_i \cdot \ell \) for \( g_i \in \mathbb{Z} \).

Therefore,

\[
\left( \frac{\alpha}{\beta_i^{\ell n_i}} \right) \in \mathcal{O}_{K, \Sigma_i}^\times \subseteq (\mathcal{O}_{m_i}^\times)^\ell \Rightarrow \beta_i^{n_i} \in (\mathcal{O}_{m_i}^\times)^\ell \\
\Rightarrow \ell | n_i \\
\Rightarrow \ell | \text{ord}_{p_i}(\lambda_i).
\]
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 \(u_i \in \mathcal{O}_{p_i}^\times\).

Therefore,

\[
(\beta_1^{m_1 \ell}, \cdots, \beta_r^{m_r \ell}) \in H' \Rightarrow (u_1, \cdots, u_r) \in H'
\]

\[
\Rightarrow u_i \in (\mathcal{O}_{p_i}^\times)^\ell \text{ by (i)}
\]

\[
\Rightarrow \lambda_i = u_i \cdot \beta_i^{m_i \ell} \in (K_{p_i}^\times)^\ell.
\]

Now we found that \(\ker \phi = \prod_{i=1}^r (K_{p_i}^\times)^\ell\) and \(\phi\) induces

\[
\tilde{\phi} : \prod_{i=1}^r (K_{p_i}^\times/(K_{p_i}^\times)^\ell) \hookrightarrow \mathbb{A}_K^\times/H'.
\]

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

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

\[
\prod_{i=1}^r (H_{\mathcal{L}_i}/(K_{p_i}^\times)^\ell) \cong H''/H'.
\]

Now we want to find \(W \leq U \leq V\) such that \([V : U] = \ell\) and \((K_{p_i}^\times/(K_{p_i}^\times)^\ell) \not\subseteq U\) for all \(i\). Fix an isomorphism \(\rho_i : K_{p_i}^\times/H_{\mathcal{L}_i} \to \mathbb{F}_\ell\) for each \(i\). Define

\[
\psi : \prod_{i=1}^r \mathbb{F}_\ell \longrightarrow \mathbb{F}_\ell
\]

\[
(a_1, \cdots, a_r) \mapsto a_1 + \cdots + a_r.
\]
Then we have the following sequence

\[ V/W \cong \prod_{i=1}^{r} (K_{p_i}^\times/H_{L_i}) \xrightarrow{\psi_{\phi}} \prod_{i=1}^{r} \mathbb{F}_\ell \rightarrow \mathbb{F}_\ell. \]

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

\[
\begin{array}{c}
V = \prod_{i=1}^{r} (K_{p_i}^\times/(K_{p_i}^\times)^\ell) \xrightarrow{\tilde{\phi}} \mathbb{A}_K^\times/H' \\
U \xrightarrow{\text{degree } \ell} H/H' \\
W = \prod_{i=1}^{r} (H_{L_i}/(K_{p_i}^\times)^\ell) \xrightarrow{\text{degree } \ell^{-1}} H''/H'.
\end{array}
\]

Let \( L \) be the cyclic extension of \( K \) of degree \( \ell \) 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 \( \text{Gal}(L/K) \) 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 \( v = p_i \) then

\[ N_{L_{p_i}/K_{p_i}} L_{p_i}^\times = H_{L_i} = N_{L_{i}/K_{p_i}} L_i^\times, \]

so \( L_{p_i} = L_i \).

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 $\lambda_L$ are defined as in §1.2.

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

Let $L/K$ be a cyclic extension of degree $\ell$. Then

(i) $\dim_{F_\ell} \text{Sel}_\ell(L/K, E) \leq \dim_{F_\ell} \text{Sel}_\ell(K, E_L)$.

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

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

$$\text{Sel}_{\lambda_L}(K, E_L) = \text{Sel}_\ell(K, E_L)[\lambda_L].$$
By Lemma 1.4.2,
\[ \text{Sel}_\ell(L/K, E) = \text{Sel}_{\lambda_L}(K, E_L) = \text{Sel}_\ell(K, E_L)[\lambda_L]. \]

This gives us (i).

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

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

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

Finally, take \(k = \ell - 1\), we get

\[
\dim_{\mathbb{F}_\ell} \text{Sel}_\ell(K, E_L) = \dim_{\mathbb{F}_\ell} \text{Sel}_\ell(K, E_L)[\ell] \\
= \dim_{\mathbb{F}_\ell} \text{Sel}_\ell(K, E_L)[\lambda_L^{\ell - 1}] \\
\leq (\ell - 1) \dim_{\mathbb{F}_\ell} \text{Sel}_\ell(K, E_L)[\lambda_L] \\
= (\ell - 1) \dim_{\mathbb{F}_\ell} \text{Sel}_{\lambda_L}(K, E_L) \\
= (\ell - 1) \dim_{\mathbb{F}_\ell} \text{Sel}_\ell(L/K, E).
\]

\[\square\]

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

\[ H^1(K, \text{Res}_L^K E[\ell]) \cong H^1(L, E[\ell]). \]

**Proof.** This is Shapiro’s Lemma. (See for example the proof of Proposition 3.1. in (MR3).) \[\square\]
Recall that $\Sigma$ is defined as in §1.4. Let $L/K$ be a cyclic extension of degree $\ell$. Define

$$M_E := \dim_{\mathbb{F}_\ell}(\bigoplus_{p \in \Sigma} H^1(K_p, E[\ell])/\mathcal{H}_\ell(K_p)),$$

$$S_L := \{\text{primes of } K \text{ ramify in } L/K\},$$

and

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

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

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

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

**Proof.** Consider the exact sequence

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

and take the $\ell$-torsion, we get the exact sequence

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

This induces the long exact sequence

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

Since $\text{Gal}(K(E[\ell])/K) \cong \text{Aut}_{\text{End}_K(E)}(E[\ell])$, $H^0(K, E[\ell]) = E[\ell]^{G_K} = 0$. With Lemma 4.1.2,
we get
\[ 0 \rightarrow H^1(K, E_L[\ell]) \rightarrow H^1(L, E[\ell]) \rightarrow \ldots \]

This restricts to
\[ 0 \rightarrow \text{Sel}_\ell(K, E_L) \rightarrow \text{Sel}_\ell(L, E) \rightarrow \ldots \]

which gives us (i).

For (ii), first we define
\[ \Sigma_L := \Sigma \cup S_L \]
and \( K_{\Sigma_L} \) denotes the maximal extension of \( K \) which is unramified outside \( \Sigma_L \). Then we consider the exact sequence
\[ 0 \rightarrow \mathbb{Z} \rightarrow \mathbb{Z}[G] \xrightarrow{(1-\sigma)} \mathcal{I}_L \rightarrow 0 \]

where \( \sigma \) is a generator of \( G := \text{Gal}(L/K) \), 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
\[ 0 \rightarrow E \rightarrow \text{Res}_K^L E \rightarrow E_L \rightarrow 0. \]

Taking the \( \ell \)-torsion, we get the exact sequence
\[ 0 \rightarrow E[\ell] \rightarrow \text{Res}_K^L E[\ell] \rightarrow E_L[\ell] \rightarrow 0. \]

This induces the long exact sequence (writing \( G' := \text{Gal}(K_{\Sigma_L}/K) \))
\[ 0 = E_L[\ell]^{G'} \rightarrow H^1(G', E[\ell]) \rightarrow H^1(G', \text{Res}_K^L E[\ell]) \xrightarrow{f} H^1(G', E_L[\ell]) \rightarrow \ldots \]
and restricts to

\[ \text{Sel}_\ell(K, E) \to \text{Sel}_\ell(K, \text{Res}_K^L E) = \text{Sel}_\ell(L, E) \xrightarrow{g} \text{Sel}_\ell(K, E_L) \to \ldots \]

(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

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

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

\[ 0 \to \text{Sel}_\ell(K, E) \to H^1(G', E[\ell]) \to \bigoplus_{p \in \Sigma_L} H^1(K, E[\ell])/\mathcal{H}_\ell(K_p) \]

and

\[ \dim_{\mathbb{F}_\ell} H^1(G', E[\ell]) - \dim_{\mathbb{F}_\ell} \text{Sel}_\ell(K, E) \leq \dim_{\mathbb{F}_\ell} \big( \bigoplus_{p \in \Sigma_L} H^1(K, E[\ell])/\mathcal{H}_\ell(K_p) \big) = \dim_{\mathbb{F}_\ell} \big( \bigoplus_{p \in \Sigma_L} H^1(K, E[\ell])/\mathcal{H}_\ell(K_p) \big) + \dim_{\mathbb{F}_\ell} \big( \bigoplus_{p \in \Sigma_L} H^1(K, E[\ell])/\mathcal{H}_\ell(K_p) \big) = M_E + C_{E,L}. \tag{4.1.6} \]
Combine (4.1.4), (4.1.5), and (4.1.6),

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

\[\square\]

**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 $\text{Gal}(K(E_i[\ell])/K) \cong \text{GL}_2(\mathbb{F}_\ell)$ simultaneously for $i = 1, 2$, $K(E_1[\ell]) \neq K(E_2[\ell])$, and $\dim_{\mathbb{F}_\ell} \text{Sel}_\ell(L, E_2) = \dim_{\mathbb{F}_\ell} \text{Sel}_\ell(L, E_1) \forall L/K$ finite extensions.

Choose some constant $C \geq M_{E_1} = \dim_{\mathbb{F}_\ell}(\bigoplus_{p \in \Sigma} H^1(K_p, E_1[\ell]/\mathcal{H}_\ell(K_p)))$ and $C \geq \dim_{\mathbb{F}_\ell} \text{Sel}_\ell(K, E_2)$.

Taking $t = \ell \cdot \dim_{\mathbb{F}_\ell} \text{Sel}_\ell(K, E_1) + C + 1$ 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 $\ell$ cyclic extension $L/K$ that is $T$-ramified and $\Sigma$-split. Therefore, by Proposition 2.5.5(ii),

\[
\dim_{\mathbb{F}_\ell} \text{Sel}_\ell(L/K, E_1) = \dim_{\mathbb{F}_\ell} \text{Sel}_\ell(K, E_1)
\]

and

\[
\dim_{\mathbb{F}_\ell} \text{Sel}_\ell(L/K, E_2) = \ell \cdot \dim_{\mathbb{F}_\ell} \text{Sel}_\ell(K, E_1) + C + 1. \tag{4.1.8}
\]
By Lemma 4.1.1(ii),
\[
\dim_{\mathbb{F}_\ell} \text{Sel}_{\ell}(K,(E_1)_L) \leq (\ell - 1) \dim_{\mathbb{F}_\ell} \text{Sel}_{\ell}(L/K,E_1) = (\ell - 1) \dim_{\mathbb{F}_\ell} \text{Sel}_{\ell}(K,E_1).
\]

Then we apply Lemma 4.1.3(ii) to $E_1$. Since $T \subseteq \mathcal{P}_0(E_1)$, we have
\[
C_{E_1,L} = \dim_{\mathbb{F}_\ell}(\bigoplus_{p \in S_L} H^1(K_p,E_1[\ell])/\mathcal{H}_\ell(K_p)) = 0.
\]

Lemma 4.1.3(ii) then tells us
\[
\dim_{\mathbb{F}_\ell} \text{Sel}_{\ell}(L,E_1) \leq \dim_{\mathbb{F}_\ell} \text{Sel}_{\ell}(K,(E_1)_L) + \dim_{\mathbb{F}_\ell} \text{Sel}_{\ell}(K,E_1) + M_{E_1} + C_{E_1,L}
\]
\[
\leq (\ell - 1) \dim_{\mathbb{F}_\ell} \text{Sel}_{\ell}(K,E_1) + \dim_{\mathbb{F}_\ell} \text{Sel}_{\ell}(K,E_1) + M_{E_1}
\]
\[
\leq \ell \cdot \dim_{\mathbb{F}_\ell} \text{Sel}_{\ell}(K,E_1) + C.
\]

By Lemma 4.1.3(i), Lemma 4.1.1(i), and 4.1.8,
\[
\dim_{\mathbb{F}_\ell} \text{Sel}_{\ell}(L,E_2) \geq \dim_{\mathbb{F}_\ell} \text{Sel}_{\ell}(K,(E_2)_L)
\]
\[
\geq \dim_{\mathbb{F}_\ell} \text{Sel}_{\ell}(L/K,E_2)
\]
\[
= \ell \cdot \dim_{\mathbb{F}_\ell} \text{Sel}_{\ell}(K,E_1) + C + 1
\]

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 $K$. \qed

**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 $K$. 

62
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 $\ell$ such that $\text{Gal}(K(E_i[\ell])/K) \cong \text{Aut}_{\text{End}_K}(E_i[\ell])$ simultaneously for $i = 1, 2$, $K(E_1[\ell]) \neq K(E_2[\ell])$, $\ell$ is inert in $M_i$, $\ell$ does not divide the discriminant of $\mathcal{O}_{M_i}$, and $\dim_{\mathbb{F}_\ell} \text{Sel}_\ell(L, E_2) = \dim_{\mathbb{F}_\ell} \text{Sel}_\ell(L, E_1)$ for all $L/K$ finite extensions.

Choose some constant $C \geq M_{E_1} = \dim_{\mathbb{F}_\ell}(\oplus_{p \in \Sigma} H^1(K_p, E_1[\ell])/\mathcal{H}_\ell(K_p))$ and $C \geq \dim_{\mathbb{F}_\ell} \text{Sel}_\ell(K, E_2)$. Take $t = \ell \cdot \dim_{\mathbb{F}_\ell} \text{Sel}_\ell(K, E_1) + C + 1$ 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 $\ell$ cyclic extension $L/K$ that has splitting data $(\Sigma, T_0, T_1, \mathcal{L})$. We can adjust $C$ to make sure that $t \equiv \dim_{\mathbb{F}_\ell} \text{Sel}_\ell(K, E_2) \pmod{2}$.

Therefore, by Proposition 3.5.3(ii),

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

and

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

By Lemma 4.1.1(ii),

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

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

$$C_{E_1, L} = \dim_{\mathbb{F}_\ell}(\oplus_{p \in S_L} H^1(K_p, E_1[\ell])/\mathcal{H}_\ell(K_p)) = 0.$$
Lemma 4.1.3(ii) then tells us

\[ \dim_{\mathbb{F}} \text{Sel}_\ell(L, E_1) \leq \dim_{\mathbb{F}} \text{Sel}_\ell(K, (E_1)_L) + \dim_{\mathbb{F}} \text{Sel}_\ell(K, E_1) + M_{E_1} + C_{E_1, L} \]
\[ \leq (\ell - 1) \dim_{\mathbb{F}} \text{Sel}_\ell(K, E_1) + \dim_{\mathbb{F}} \text{Sel}_\ell(K, E_1) + M_{E_1} \]
\[ \leq \ell \cdot \dim_{\mathbb{F}} \text{Sel}_\ell(K, E_1) + C. \]

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

\[ \dim_{\mathbb{F}} \text{Sel}_\ell(L, E_2) \geq \dim_{\mathbb{F}} \text{Sel}_\ell(K, (E_2)_L) \]
\[ \geq \dim_{\mathbb{F}} \text{Sel}_\ell(L/K, E_2) \]
\[ = \ell \cdot \dim_{\mathbb{F}} \text{Sel}_\ell(K, E_1) + C + 1 \]

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 $K$. \qed

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 $\text{End}_K(E_1) \otimes \mathbb{Q} \cong \text{End}_K(E_2) \otimes \mathbb{Q}$.

*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

\[ \text{End}_K(E_1) \to \text{End}_K(E_2) \otimes \mathbb{Q} \]
\[ f \mapsto \frac{1}{n} \varphi \circ f \circ \hat{\varphi}. \]

This gives an injective ring homomorphism since the composition of nonzero isogenies is nonzero. Therefore, $\text{End}_K(E_1)$ is a subring of $\text{End}_K(E_2) \otimes \mathbb{Q}$ and $\text{End}_K(E_1) \otimes \mathbb{Q}$ is a subfield
of \( \text{End}_K(E_2) \otimes \mathbb{Q} \). For the same reason, \( \text{End}_K(E_2) \otimes \mathbb{Q} \) is also a subfield of \( \text{End}_K(E_1) \otimes \mathbb{Q} \). Therefore, \( \text{End}_K(E_1) \otimes \mathbb{Q} \cong \text{End}_K(E_2) \otimes \mathbb{Q} \). \( \square \)

**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 \( M \not\subseteq K \). 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, \( \text{Gal}(MK/K) = \langle \sigma \rangle \), and \( d := \text{deg} \varphi \). Consider \( f := \hat{\varphi} \circ \varphi^\sigma \in \text{End}_K(E_1) = \mathcal{O}_M \) and its dual \( \hat{f} = \hat{\varphi}^\sigma \circ \varphi = f^\sigma \),

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

Let \( \alpha := \frac{f}{d} \in \text{End}_K(E_1) \otimes \mathbb{Q} \),

\[
N \alpha = \alpha \cdot \alpha^\sigma = \frac{f}{d} \cdot \frac{f^\sigma}{d^\sigma} = \frac{d^2}{d^2} = 1.
\]

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

Consider \( \varphi \circ \beta : E_1 \rightarrow E_1 \rightarrow E_2 \),

\[
d \circ \beta = f \circ \beta^\sigma,
\]

\[
\hat{\varphi} \circ \varphi \circ \beta = \hat{\varphi} \circ \varphi^\sigma \circ \beta^\sigma,
\]

\[
\varphi \circ \beta = \varphi^\sigma \circ \beta^\sigma.
\]

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 $M_i := \text{End}_K(E_i) \otimes \mathbb{Q}$. 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 $M_2 \not\subseteq K$, by Lemma 4.1.12, then $E_1$ and $E_2$ are isogenous over $K$.

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.
Bibliography


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


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

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