國立台灣大學理學院數學系

碩士論文

Department of Mathematics
National Taiwan University
Master Thesis

探討橢圓曲線經扭變後之秩
On Rank of Twists of Elliptic Curves

王家成
Chia-Chen Wang

指導教授：陳其誠博士
Advisor: Ki-Seng Tan, Ph.D

中華民國 104 年 6 月
June, 2015

口試委員會審定書

誌謝

感謝陳其誠教授這兩年來的辛勞。許多問題即便我無法一聽就懂，教授仍能不厭其煩地再三解釋。此外，教授給予很大的空間讓我決定要做的事情，這磨練了我自己設定目標以及尋找解決方式的能力。而教授對於學習數學的態度也讓我耳目一新，讓我深深地體會到學習應該要由學生主動開始才能有效果。

感謝一同跟隨陳其誠教授努力的研究生們。從膺任學長身上我多次體悟到自己大學課程的基礎有多麼薄弱。與健樺不斷討論的過程中我逐漸了解 Global Field 和 Local Field 以及 Class Field Theory 的內容。與宗堂相處的過程中我看到了數學學習的多種面向。在建鑫的報告中我學習到如何有條理地闡述一篇論文。

最後，我要感謝我的父母。對於我念數學研究所採取完全支持的態度，即使不知道我到底在做什麼，也沒有任何質疑的聲音，讓我能夠好好地把這篇論文完成。

摘要

對一條橢圓曲線，我們通常關心它的加法結構，尤其關心其加法群之秩的大小。另外，我們知道橢圓曲線之賽爾曼群為一兩個元素的有限體之向量空間，且其維度為加法群之秩的有限上界。

這篇論文主要的內容是研讀 Mazur 和 Rubin 的成果，他們將扭變前後的賽爾曼群放在同一個集合下考慮，並分析了局部賽爾曼群的特性，了解在何種情況下扭變前後的局部賽爾曼群會相同或者交集為零，進而藉由局部的資訊得到賽爾曼群在扭變前後維度的變化，並藉此得知對於某些橢圓曲線，我們可以找到它的扭變，其對應的賽爾曼群有特定的維度。

Abstract

For an elliptic curve, we care about the Mordell-Weil group on it. Espically we care about the rank of this group. On the other hand, it is known that the $\mathbb{F}_2$-dimension of Selmer group of an elliptic curve is an finite upper bound of the rank of the Mordell-Weil group.

In this thesis, we study the result of Mazur and Rubin. They view the Selmer group and the twisted Selmer group as contained in the same set. Analyzing the local Selmer group, which tells us when will them be the same or intersect to zero. By this we can see the relation between the dimension of Selmer group and that of twisted Selmer group. Then we know that under some conditions, elliptic curve have abitrary twisted Selmer rank.

Contents

1. Introduction

Let K be a number field and let E be an elliptic curve (as a curve in the projective plane) defined by the equation

$$y^2 = f(x) := x^3 + Ax + B, \quad A, B \in K. \tag{1}$$

Recall that the m-Selmer group of E over K is defined to be (see Definition 2.2.2)

$$\mathrm{Sel}_m(E/K) := \ker\{\mathrm{H}^1(K, E[m]) \longrightarrow \prod_{\text{all } v} \mathrm{H}^1(K_v, E)\},$$

where $E[m]$ denotes the m-torsion group of E and for each place v of K, K_v denote the completion of K at v, while the map above is by putting together all the compositions

$$\mathrm{H}^1(K, E[m]) \longrightarrow \mathrm{H}^1(K, E) \longrightarrow \mathrm{H}^1(K_v, E).$$

It is known that $\mathrm{Sel}_m(E/K)$ is a finite group (see [2, Ch.X Thm 4.2]) and is closely related to the (finitely generated) Mordell-Weil group $E(K)$, as we have (see §2.2.1)

$$E(K)/mE(K) \hookrightarrow \mathrm{Sel}_m(E/K)\ . \tag{2}$$

In particular, $\mathrm{Sel}_2(E/K)$ is a finite dimensional vector space over $\mathbb{F}_2$, the finite field of order 2. Denote

$$d_2(E/K) := \dim_{F_2} \mathrm{Sel}_2(E/K).$$

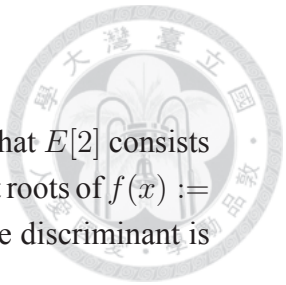
For each non-zero $D \in K$, the isomorphism class (over K) of the elliptic curve defined by

$$Dy^2 = x^3 + Ax + B \tag{3}$$

only depends on the residue class of D in K^*/K^{*2}, or equivalently the field extension $F = K(\sqrt{D})$. Let E^F denote this elliptic curve and call it the F-twist of E, or the quadratic twist of E by F (even when $F = K$ and hence $E^F = E$).

How $d_2(E^F)$ varies with F is an interesting question to which we are looking for an answer. A folklore conjecture says the rank of $E^F(K)$ can be arbitrary large, and hence by (2) it implies the following:

Conjecture 1. *For a given elliptic curve E defined over a number field K, the $\mathbb{F}_2$-rank $d_2(E^F)$ of the 2-Selmer group of E^F, for F running through all quadratic extension of K, can be arbitrary large.*



Rubin and Mazur [1] prove this conjecture partially as follows. Note that $E[2]$ consists of the identity element and $(a,0)$, $(b,0)$, $(c,0)$, where a, b, c are the distinct roots of $f(x) := x^3 + Ax + B = 0$. Let $K(E[2])$ denote the splitting field of $f(x)$ whose discriminant is defined to be $\Delta_f := -16(4A^3 + 27B^2)$.

Theorem 1. *Suppose K is a number field, E is an elliptic curve defined by* (1) *such that* $\mathrm{Gal}(K(E[2])/K) \cong S_3$. *Suppose further that K has a place v_0 satisfying :*

(a) *v_0 is real and $\Delta_f < 0$ in K_{v_0}, or*

(b) *v_0 is non-archimedean, not dividing 2, E has multiplicative reduction at v_0, and $\mathrm{ord}_{v_0}(\Delta_f)$ is odd.*

Then for every $r \geq 0$, E has quadratic twist E^F/K with $d_2(E^F/K) = r$.

Under the weaker condition $E(K)[2] = 0$, they also obtain the following.

Theorem 2. *Suppose K is a number field, and E is an elliptic curve over K such that $E(K)[2] = 0$. If $0 \leq r \leq d_2(E/K)$ and $r \equiv d_2(E/K) \pmod 2$, then E has quadratic twist E'/K such that $d_2(E'/K) = r$.*

This thesis is a report on the study of the paper [1], especially on the above main theorems. In the thesis, I try to fill in all the details not given in the paper, except maybe the proofs of one or two statements. Basically, there is no new thoughts originated from me, only some scattered simplifications of the deduction here and there. The thesis is organized as follow. In Section 2, we set the notation and review some background knowledge. In Section 3, we work on results on various cohomology groups over local fields. Section 4 deals with Galois groups over number fields as well as the comparison of 2-Selmer groups of E ad E^F. Finally, in Section 5, we complete the proof of the above main theorems, which will be restated as Theorem 5.1.4 and Theorem 5.2.2 for convenience, in §5.1 and §5.2.

2. Settings and basic facts

In this section, we set the notation and recall some basic facts. Let M_K denote the set of all places of K. For each $v \in M_K$, let K_v denote the completion of K. If $v \in M_K$ is a non-archimedean place of K, let $\mathcal{R}_v$ denote the ring of integer of K_v, π_v (or just π) be a prime element so that $\mathcal{M}_v := \pi\mathcal{R}_v$ is the maximal ideal of $\mathcal{R}_v$, $U_v = \mathcal{R}_v^*$ and $k_v = \mathcal{R}_v/\mathcal{M}_v$ be the residue field. When a finite extension of K_v is denoted by L_w, we mean that w is the place of L_w sitting over v. If L_w is defined by some characteristic property to which

the place w is irrelevant, we might write L_v for L_w. As an example, K_v^{ur} will denote the maximal unramifield extension of K_v. Let $\mathrm{Frob}_v \in \mathrm{Gal}(K_v^{ur}/K_v)$ be the Frobenius element whose image under the natural isomorphism

$$\mathrm{Gal}(K_v^{ur}/K_v) \xrightarrow{\sim} \mathrm{Gal}(\bar{k}_v/k_v)$$

is the Frobenius substitution F_v: $x \mapsto x^{|k_v|}$.

2.1. **Settings.**

2.1.1. *Field extensions and Galois groups.* Let $\bar{K}$ and $\bar{K}_v$ denote the algebraic closures of K and K_v. If L/K (resp. L_w/K_v) is a Galois extension, let $G_{L/K}$ or $\mathrm{Gal}(L/K)$ (resp. G_{L_w/K_v} or $\mathrm{Gal}(L_w/K_v)$) denote the Galois group of L/K (resp. K_w/K_v). Especially, we denote $G_K = G_{\bar{K}/K}$ (resp. $G_v = G_{\bar{K}_v/K_v}$).

The restriction of the action of G_v on $\bar{K}$ give rise the embedding

$$G_v \hookrightarrow G_K$$

that identifies G_v with the decomposition subgroup of G_K at v.

2.1.2. *Galois cohomology.* Every G_K-module (resp. G_v-module) A considered in this thesis is a continuous module in the sense that the stabilizer of every element of A is an open subgroup of G_K (resp. G_v). Let $\mathrm{H}^q(K, A)$ (resp. $\mathrm{H}^q(K_v, A)$ denote the Galois cohomology $\mathrm{H}^q(G_K, A)$ (resp. $\mathrm{H}^q(G_v, A)$). Also, $\mathrm{H}^q(K, E)$, $\mathrm{H}^q(K_v, E)$ denote $\mathrm{H}^q(K, E(\bar{K}))$, $\mathrm{H}^q(K_v, E(\bar{K}_v))$, and so on.

2.1.3. *Localization maps.* The localization map $\mathrm{H}^q(K, E) \longrightarrow \mathrm{H}^q(K_v, E)$ is the composition

$$\mathrm{H}^q(K, E(\bar{K})) \longrightarrow \mathrm{H}^q(K_v, E(\bar{K})) \longrightarrow \mathrm{H}^q(K_v, E(\bar{K}_v))$$

where the first map is the restriction map and the second is induced from the embedding

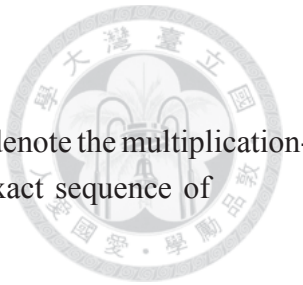
$$E(\bar{K}) \longrightarrow E(\bar{K}_v).$$

We also call the above embedding the localization map. We define similarly the localization map $\mathrm{H}^q(K, E[m]) \longrightarrow \mathrm{H}^q(K_v, E[m])$.

2.2. **Selmer groups.** If $\phi : A \longrightarrow B$ is a group homomorphism, denote

$$A[\phi] = \ker \phi \subset A.$$

If ϕ is a homomorphism of G-modules, for some group G, then $A[\phi]$ is a G-module.



2.2.1. *The Kummer exact sequence.* For each positive integer m, let $[m]$ denote the multiplication-by-m map on $E(\bar{K})$. it is surjective. Hence we have the Kummer exact sequence of G_K-modules:

$$0 \longrightarrow E[m] \xrightarrow{i} E(\bar{K}) \xrightarrow{[m]} E(\bar{K}) \longrightarrow 0$$

It induces the long exact sequence

$$\begin{array}{ccccccc} 0 \longrightarrow & E(K)[m] & \xrightarrow{i} & E(K) & \xrightarrow{[m]} & E(K) & \\ & & & & \overset{\delta}{\searrow} & & \\ & \mathrm{H}^1(K, E[m]) & \xrightarrow{i_*} & \mathrm{H}^1(K, E) & \xrightarrow{[m]_*} & \mathrm{H}^1(K, E) & \longrightarrow \cdots, \end{array}$$

and hence the short exact sequence

$$0 \longrightarrow E(K)/mE(K) \longrightarrow \mathrm{H}^1(K, E[m]) \longrightarrow \mathrm{H}^1(K, E)[m_*] \longrightarrow 0. \tag{4}$$

By replacing K by K_v, the above argument also leads to the exact sequence

$$0 \longrightarrow E(K_v)/mE(K_v) \longrightarrow \mathrm{H}^1(K_v, E[m]) \longrightarrow \mathrm{H}^1(K_v, E)[m_*] \longrightarrow 0. \tag{5}$$

Definition 2.2.1. *For each $v \in M_K$, let $\mathrm{H}^1_f(K_v, E[m])$ denote the image of the map*

$$E(K_v)/mE(K_v) \hookrightarrow \mathrm{H}^1(K_v, E[m]) \ .$$

2.2.2. *Selmer groups and Tate-Shafarevich groups.* Putting (4) and (5) (for all v) together, we obtain the commutative diagram of exact sequences:

(6)

$$\begin{array}{ccccc} E(K)/mE(K) & \hookrightarrow & \mathrm{H}^1(K, E[m]) & \twoheadrightarrow & \mathrm{H}^1(K, E)[m_*] \\ \downarrow & & \downarrow l & & \downarrow \\ \prod_{v\in M_K} E(K_v)/mE(K_v) & \hookrightarrow & \prod_{v\in M_K} \mathrm{H}^1(K_v, E[m]) & \xrightarrow{i_*} & \prod_{v\in M_K} \mathrm{H}^1(K_v, E)[m_*], \end{array}$$

where all vertical arrows are formed by localization maps.

Definition 2.2.2. *Define the m-Selmer group*

$$\begin{aligned} \mathrm{Sel}_m(E/K) &:= \ker\{\ \mathrm{H}^1(K, E[m]) \xrightarrow{i_*\circ l} \textstyle\prod_{v\in M_K} \mathrm{H}^1(K_v, E)\ \} \\ &= \textstyle\bigcap_{v\in M_K} \ker\{\ \mathrm{H}^1(K, E[m]) \longrightarrow \mathrm{H}^1(K_v, E)\ \} \end{aligned}$$

and the Tate-Shafarevich group

$$\begin{aligned} Ш(E/K) &:= \ker\{\ \mathrm{H}^1(K,E) \longrightarrow \textstyle\prod_{v\in M_K} \mathrm{H}^1(K_v,E)\ \} \\ &= \textstyle\bigcap_{v\in M_K} \ker\{\ \mathrm{H}^1(K,E) \longrightarrow \mathrm{H}^1(K_v,E)\ \}. \end{aligned}$$

In view of (5) and Definition 2.2.1, we can write

$$\mathrm{Sel}_m(E/K) = l^{-1}(\prod_{v\in M_K} \mathrm{H}^1_f(K_v, E[m])). \tag{7}$$

Lemma 2.2.3. *We have the exact sequence*

$$0 \longrightarrow E(K)/mE(K) \longrightarrow \mathrm{Sel}_m(E/K) \longrightarrow Ш(E/K)[m] \longrightarrow 0.$$

Proof. Apply snake lemma on the commutative diagram of exact sequences

$$\begin{array}{ccccccc} 0 & \longrightarrow & E(K)/mE(K) & \longrightarrow & \mathrm{H}^1(K,E[m]) & \longrightarrow & \mathrm{H}^1(K,E)[m] \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ & & 0 & \longrightarrow & \prod_{v\in M_K} \mathrm{H}^1(K_v,E) & \longrightarrow & \prod_{v\in M_K} \mathrm{H}^1(K_v,E) \longrightarrow 0. \end{array}$$

□

2.3. **The quadratic twists.** If E and E' are elliptic curve over K isomorphic over a quadratic extension F, then they are quadratic twist of each other by F (see [2, Ch.X §5]).

Suppose E^F is a quadratic twist of E by F/K and let $\psi : E \to E^F$ be an isomorphism defined over F.

Lemma 2.3.1. *If σ is an element of G_K not in G_F, then the diagram*

$$\begin{array}{ccc} E(\bar{K}) & \xrightarrow{\psi} & E^F(\bar{K}) \\ \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \sigma} \\ E(\bar{K}) & \xrightarrow{-\psi} & E^F(\bar{K}) \end{array}$$

is commutative.

Proof. In fact, if $F = K(\sqrt{D})$, and E and E^F are defined by (1) and (3), respectively, then $\psi : E \longrightarrow E^F$ can be taken to be $(x, y) \mapsto (x, \sqrt{D}y)$. It follows that

$$(\sigma \circ \psi)(x, y) = \sigma(x, \sqrt{D}y) = (x^\sigma, -\sqrt{D}y^\sigma)$$

while

$$(-\psi \circ \sigma)(x, y) = -\psi(x^\sigma, y^\sigma) = (x^\sigma, -\sqrt{D}y^\sigma).$$

□

Now we consider the case where $m = 2$.

Lemma 2.3.2. *If E is an elliptic curve defined over K and E^F is a quadratic twist of E, then there is a natural identification of Galois module $E[2] = E^F[2]$.*

Proof. The identification of $E[2]$ and $E^F[2]$ as Galois modules is due to the fact that $\psi = -\psi$ when restricted to $E[2]$. □

This lemma allows us to view both $\mathrm{Sel}_2(E/K)$ and $\mathrm{Sel}_2(E^F/K)$ as subgroup of $\mathrm{H}^1(K, E[2])$, but defined by different sets of local conditions. In this thesis, we aim to construct F so that the local condition defining $\mathrm{Sel}_2(E/K)$ and $\mathrm{Sel}_2(E^F/K)$ agree everywhere except at most one place, and use that place to vary the rank of 2-Selmer group.

2.4. **The structure of $E(K_v)$.** The proof of the facts mentioned below can be found in [2, Ch.§VII]. The defining equation (1) might not have $A, B \in \mathcal{R}_v$. However, such requirement can be easily fulfilled by making the change of coordinates

$$x \mapsto \alpha^2 x, \quad y \mapsto \alpha^3 y,$$

for some $\alpha \in K_v^*$. We call the resulting equation a model of (1) over $\mathcal{R}_v$, or a model of E. We can assume that (1) is already a model.

Lemma 2.4.1. *If K_v is a real place, then the sign of Δ_f remains the same for all models of E; if v is non-archimedean, then the parity of* $\mathrm{ord}_v(\Delta_f)$ *remains the same for all models.*

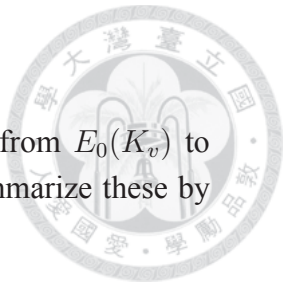
Proof. Under the above change of variables, Δ_f becomes $\alpha^{12}\Delta_f$. □

Suppose the model is minimal in the sense that $\mathrm{ord}_v(\Delta_f)$ is minimal among all models. Let $\tilde{E}$ denote the projective curve defined by (1) modulo π_v and call it the reduction of E at v, or the reduction in K_v. If $P \in E(K_v)$ is given by a projective coordinate $[\alpha : \beta : \gamma]$ with $\alpha, \beta, \gamma \in \mathcal{R}_v$ such that the residue classes $\bar{\alpha}, \bar{\beta}, \bar{\gamma} \in k_v$ not all zero, then the point $\bar{P} = [\bar{\alpha} : \bar{\beta} : \bar{\gamma}] \in \tilde{E}(k_v)$. We denote the reduction map by

$$\varphi_v : E(K_v) \longrightarrow \tilde{E}(k_v), \quad P \mapsto \bar{P}$$

Let $\tilde{E}_{ns}$ denote the subset of $\tilde{E}$ consisting of non-singular points. Then $\tilde{E}_{ns}$ has the natural structure of an abelian group so that

$$E_0(K_v) := \varphi_v^{-1}(\tilde{E}_{ns}(k_v))$$



is a subgroup of $E(K_v)$ and φ_v induces a surjective homomorphism from $E_0(K_v)$ to $\tilde{E}_{ns}(k_v)$. Hence $E_1(K_v) := \varphi_v^{-1}(0)$ is a subgroup of $E_0(K_v)$. We summarize these by the following exact sequence:

$$0 \longrightarrow E_1(K_v) \longrightarrow E_0(K_v) \xrightarrow{\varphi_v} \tilde{E}_{ns}(k_v) \longrightarrow 0. \tag{8}$$

It is known that $E_1(K_v)$ is a compact pro-p group, if $p = char.\ k_v$.

Proposition 2.4.2. *There is a formal group law $\hat{E}$ defined on $\mathcal{R}_v$ such that*

$$E_1(K_v) = \hat{E}(\mathcal{M}_v). \tag{9}$$

Furthermore, for each $i > 0$,

$$\hat{E}(\mathcal{M}_v^i)/\hat{E}(\mathcal{M}_v^{i+1}) \cong \mathcal{M}_v^i/\mathcal{M}_v^{i+1}.$$

If $p = char.\ k_v$ and $r > \mathrm{ord}_v(p)/(p-1)$, then

$$\hat{E}(\mathcal{M}_v^r) \cong \mathcal{M}_v^r.$$

Remark 2.4.3. *The formal group law $\hat{E}$ depends on the minimal model chosen. If $\tilde{E}$ is either an elliptic curve* (good reduction) *or its singularity consists of a unique double point with distinct tangent lines* (multiplicative reduction)*, then a minimal model of E over K_v remains minimal over every finite extension L_w/K_v, and hence $\hat{E}$ is also the formal group law in the L_w-version of* Proposition 2.4.2. *Moreover, if L_w/K_v is a Galois extension, then the identity and isomorphisms in the proposition respect the action of* $\mathrm{Gal}(L_w/K_v)$.

2.4.1. *Good reduction case.*

Lemma 2.4.4. *Suppose E has good reduction in K_v and m is relatively prime to $p := char.k_v$. Then the reduction map φ_v induces*

$$E(K_v)[m] \cong \tilde{E}(k_v)[m] \ \text{ and } \ E(K_v)/mE(K_v) \cong \tilde{E}(k_v)/m\tilde{E}(k_v).$$

Proof. Since $E_1(K_v)$ is a pro-p group, the multiplication by m on $E_1(K_v)$ is a bijection. Therefore, the snake lemma applied on the commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E_1(K_v) & \longrightarrow & E(K_v) & \xrightarrow{\varphi_v} & \tilde{E}(k_v) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle [m]} & & \downarrow{\scriptstyle [m]} & & \downarrow{\scriptstyle [m]} & & \\
0 & \longrightarrow & E_1(K_v) & \longrightarrow & E(K_v) & \xrightarrow{\varphi_v} & \tilde{E}(k_v) & \longrightarrow & 0
\end{array}$$

leads to the exact sequence

$$0 \longrightarrow E(K_v)[m] \longrightarrow \tilde{E}(k_v)[m] \longrightarrow 0 \longrightarrow E(K_v)/mE(K_v) \twoheadrightarrow \tilde{E}(k_v)/m\tilde{E}(k_v) \longrightarrow 0 \ .$$

□

Corollary 2.4.5. *Under the condition of the above lemma,*

$$E[m] \cong \tilde{E}[m].$$

Proof. Replace K_v, k_v by K_v^{ur}, $\bar{k}_v$. □

2.4.2. *The case of split-multiplicative reduction.* The proof of the following statements can be found in [3, Ch.V §5]. Recall that E has multiplicative reduction in K_v if and only if $\tilde{E}$ has a double point as the unique singularity with two distinct tangent lines, if the tangent lines at this node is defined (resp. not defined) over k_v then E is said to have split (resp, non-split) multiplicative reduction.

If E has split-multiplicative reduction in K_v, then E is a Tate curve, and vice versa, in the sense that there is a $q \in \mathcal{M}_v$, called local Tate period, such that for every extension L_w/K_v, $E(L_w) = L_w^*/q^{\mathbb{Z}}$. Here $q^{\mathbb{Z}}$ stands for the discrete subgroup generated by q. In particular, as a G_v-module

$$E(\bar{K}_v) = \bar{K}_v^*/q^{\mathbb{Z}}. \tag{10}$$

Recall that the j-invariant $j(E)$ of E is defined to be

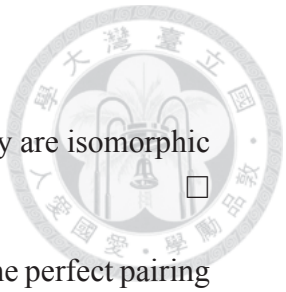
$$1728(4A)^3/\Delta_f = -1728(4A)^3/16(4A^3 + 27B^2).$$

It is an invariant of the elliptic curve independent of the defining equation (1).

Theorem 3 (Tate)**.** *If $j(E) \notin \mathcal{R}_v$, then E is a quadratic twist of a Tate curve with local Tate period q such that* $\operatorname{ord}_v q = -\operatorname{ord}_v j(E)$. *Two Tate curves are isomorphic if and only their local Tate periods are the same.*

Corollary 2.4.6. *If E has non-split reduction in K_v, then E is the twist of a Tate curve by the unique unramified quadratic extension.*

Proof. Let L_w and k_w denote this quadratic extension and its residue field. Since the two distinct tangent lines of the double point are defined over k_w, E is a Tate curve over L_w. In particular, the j invariant of E is an non-integral element of K_v, and hence by Theorem 3, E is a quadratic twist of a Tate curve E^t defined over K_v. Since over certain finite extension E and E^t are isomorphic Tate curves, they have the same local Tate period.



But, since over L_w they are both Tate curve of the same local period, they are isomorphic over L_w. Hence E is the L_w twist of E^t. □

2.5. **Local Tate duality.** The Weil pairing and cup product give rise to the perfect pairing ([10, Ch I Cor 3.4]):

$$< , >_v : \mathrm{H}^1(K_v, E[m]) \times \mathrm{H}^1(K_v, E[m]) \longrightarrow \mathbb{Q}/\mathbb{Z}, \tag{11}$$

such that the annihilator of $\mathrm{H}^1_f(K_v, E[m]) = E(K_v)/mE(K_v)$ is itself. Hence, via the exact sequence (5), we have the induced pairing

$$(,)_v : E(K_v)/mE(K_v) \times \mathrm{H}^1(K_v, E)[m] \longrightarrow \mathbb{Q}/\mathbb{Z}.$$

It is also a perfect pairing. These pairings respect the action of Galois group: if L_w/K_v is a Galois extension, then for every $\sigma \in G_{L_w/K_v}$

$$< a^\sigma, b^\sigma >_w = < a, b >_w . \tag{12}$$

For a finite extension L_w/K_v let

$$\mathrm{N}_{L_w/K_v} : E(L_w) \longrightarrow E(K_v)$$

denote the norm map $P \mapsto \sum_\sigma P^\sigma$, where σ runs through G_v/G_w. We have the commutative diagram:

$$\begin{array}{ccccc} (,)_w : E(L_w)/mE(L_w) & \times & \mathrm{H}^1(L_w, E)[m] & \longrightarrow & \mathbb{Q}/\mathbb{Z} \\ \downarrow \bar{\mathrm{N}}_{L_w/K_v} & & \uparrow \mathrm{res}_{L_w/K_v} & & \| \\ (,)_v : E(K_w)/mE(K_w) & \times & \mathrm{H}^1(K_w, E)[m] & \longrightarrow & \mathbb{Q}/\mathbb{Z} \end{array} \tag{13}$$

where $\bar{\mathrm{N}}_{L_w/K_v}$ is induced from the norm map and res_{L_w/K_v} is the restriction.

3. Local results

Recall that F_v is the Frobenius substitution and if k/k_v is a finite extension, then its Galois group is generated by the restriction of F_v to k. If E has good reduction at v, let

$$\mathrm{N}_{k/k_v} : \tilde{E}(k) \longrightarrow \tilde{E}(k_v)$$

denote the norm map sending P to $\sum_\sigma P^\sigma$ where σ runs through $\mathrm{Gal}(k/k_v)$.

3.1. **The size of $\mathrm{H}^1_f(K_v, E[2])$.**

Lemma 3.1.1. *The group $E(K_v)/2E(K_v)$ is finite.*

Proof. If v is complex, then $E(\mathbb{C})$ is connected and hence $2E(\mathbb{C}) = E(\mathbb{C})$; if v is real, then $E(\mathbb{R})$ has only finite components and $2E(\mathbb{R})$ contains the identity component.

If v is non-archimedean, write $Q = E(K_v)/E_1(K_v)$ and apply the snake lemma to the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E_1(K_v) & \longrightarrow & E(K_v) & \longrightarrow & Q & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle [2]} & & \downarrow{\scriptstyle [2]} & & \downarrow{\scriptstyle [2]} & & \\ 0 & \longrightarrow & E_1(K_v) & \longrightarrow & E(K_v) & \longrightarrow & Q & \longrightarrow & 0. \end{array} \tag{14}$$

Since Q is finite, the lemma follows from Proposition 2.4.2.

□

Lemma 3.1.2. *The following holds:*

(i) *If $v \nmid 2\infty$, then* $\dim_{\mathbb{F}_2}(\mathrm{H}^1_f(K_v, E[2])) = \dim_{\mathbb{F}_2}(E(K_v)[2])$.

(ii) *If $v \nmid 2\infty$ and E has good reduction at v, then*

$$\mathrm{H}^1_f(K_v, E[2]) \cong E[2]/(\mathrm{Frob}_v - 1)E[2]$$

with the isomorphism given by evaluating cocycles at the Frobenius automorphism Frob_v.

Proof. By Proposition 2.4.2, the multiplication by 2 on $E_1(K_v)$ is an isomorphism. Hence by (14) and the snake lemma

$$E(K_v)[2] \cong Q[2] \quad \text{and} \quad E(K_v)/2E(K_v) \cong Q/2Q.$$

But since Q is finite, the exact sequence

$$0 \longrightarrow Q[2] \longrightarrow Q \xrightarrow{[2]} Q \longrightarrow Q/2Q \longrightarrow 0$$

implies $|Q[2]| = |Q/2Q|$. These imply $\dim_{\mathbb{F}_2} \mathrm{H}^1_f(K_v, E[2]) = \dim_{\mathbb{F}_2} E(K_v)[2]$ and prove (i).

If E has good reduction at v, then by Lemma 2.4.4

$$E(K_v)[2] \cong \tilde{E}(k_v)[2] \quad \text{and} \quad E(K_v)/2E(K_v) \cong \tilde{E}(k_v)/2\tilde{E}(k_v). \tag{15}$$

Consider the commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \tilde{E}[2] & \longrightarrow & \tilde{E}(\bar{k}_v) & \xrightarrow{[2]} & \tilde{E}(\bar{k}_v) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{F}_v-1} & & \downarrow{\scriptstyle \mathrm{F}_v-1} & & \downarrow{\scriptstyle \mathrm{F}_v-1} & & \\ 0 & \longrightarrow & \tilde{E}[2] & \longrightarrow & \tilde{E}(\bar{k}_v) & \xrightarrow{[2]} & \tilde{E}(\bar{k}_v) & \longrightarrow & 0. \end{array}$$

We claim that the middle down-arrow is surjective. Then by snake lemma, we obtain the exact sequence

$$0 \longrightarrow \tilde{E}(k_v)[2] \longrightarrow \tilde{E}(k_v) \xrightarrow{[2]} \tilde{E}(k_v) \longrightarrow \tilde{E}[2]/(\mathrm{F}_v - 1)\tilde{E}[2] \longrightarrow 0. \tag{16}$$

Now (15) and (16) together imply

$$\begin{aligned} \mathrm{H}^1_f(K_v, E[2]) &\cong E(K_v)/2E(K_v) \\ &\cong \tilde{E}(k_v)/2\tilde{E}(k_v) \\ &\cong \tilde{E}[2]/(\mathrm{F}_v - 1)\tilde{E}[2] \\ &\cong E[2]/(\mathrm{Frob}_v - 1)E[2]. \end{aligned}$$

For a point $z \in E(K_v)$ let $\bar{z}$ denote its reduction at v and let $[z]$ (resp. $[\bar{z}]$) denote the class of z (resp. $\bar{z}$) in $E(K_v)/2E(K_v)$ (resp. $\tilde{E}(k_v)/2\tilde{E}(k_v)$). Let ρ be the cocycle given by $\rho(\sigma) = y^\sigma - y$ where $2y = x$ for some $x \in E(K_v)$ and let $[\rho]$ be its class in $\mathrm{H}^1_f(K_v, E[2])$. Then above isomorphisms can be described as

$$[\rho] \mapsto [x] \mapsto [\bar{x}] \mapsto (\mathrm{F}_v - 1)\bar{y} \mapsto (\mathrm{Frob}_v - 1)y = \rho(\mathrm{Frob}_v),$$

which means the resulting isomorphism is given by evaluating cocyles at the Frobenius automorphism Frob_v.

To prove our claim, for every $P \in \tilde{E}(\bar{k}_v)$, we shall show that $P \in (\mathrm{F}_v - 1)(\tilde{E}(\bar{k}_v))$. Assume that $P \in \tilde{E}(k_1)$ for some finite extension k_1/k_v of degree n and $[m]P = 0$ for some $m \in \mathbb{N}$ (since $\tilde{E}(k_1)$ is a finite group). Let k_2/k_1 be the field extension of degree m. Then k_2/k_v is a cyclic extension with Galois group generated by $\bar{\mathrm{F}}_v$, the restriction of F_v to k_2. Since

$$\mathrm{N}_{k_2/k_v}(P) = \mathrm{N}_{k_1/k_v}(\mathrm{N}_{k_2/k_1}(P)) = \mathrm{N}_{k_1/k_v}([m]P) = 0,$$

the point P determines a class in $\mathrm{H}^1(k_2/k_v, \tilde{E}(k_2))$, which by Lang's theorem ([4, Theorem 2]) is trivial. Therefore $P = Q^{\mathrm{F}_v} - Q$ for some $Q \in \tilde{E}(k_2)$.

□

3.2. **Relations involving E and E^F.** Let E^F be the twist of E by a quadratic extension F. Let w be a place of F sitting over v, and for simplicity write

$$E_N(K_v) := \mathrm{N}_{L_w/K_v}(E(L_w))$$

which contains $2E(K_v)$.

Recall that (5) identify $\mathrm{H}^1_f(K_v, E[2]) = E(K_v)/2E(K_v)$ as a subgroup of $\mathrm{H}^1(K_v, E[2])$ and by Lemma 2.3.2 we have

$$\mathrm{H}^1(K_v, E^F[2]) = \mathrm{H}^1(K_v, E[2]). \tag{17}$$

Lemma 3.2.1. *Under the identification* (17)*, we have*

$$\mathrm{H}^1_f(K_v, E[2]) \cap \mathrm{H}^1_f(K_v, E^F[2]) = E_N(K_v)/2E(K_v).$$

Proof. Under the local Tate pairing $< \ , \ >_v$, each of $\mathrm{H}^1_f(K_v, E[2])$ and $\mathrm{H}^1_f(K_v, E^F[2])$ is the annihilator of itself (see §2.5). Therefore, the left-hand side of the equality is the annihilator of $\mathrm{H}^1_f(K_v, E[2]) + \mathrm{H}^1_f(K_v, E^F[2])$, and we need to show that the same holds for the right-hand side.

Let Υ denote the image of $\mathrm{H}^1_f(K_v, E^F[2])$ under the map

$$\mathrm{H}^1(K_v, E[2]) \longrightarrow \mathrm{H}^1(K_v, E)[2].$$

Since the kernel of the map is $\mathrm{H}^1_f(K_v, E[2])$, we need to prove that under the induced pairing $(\ ,\ )_v$, Υ is precisely the annihilator of $E_N(K_v)/2E(K_v)$. Now the diagram (13) implies that the annihilator of $E_N(K_v)/2E(K_v)$ equals

$$\ker \{\ \mathrm{H}^1(K_v, E)[2] \xrightarrow{\mathrm{res}_{F_w/K_v}} \mathrm{H}^1(F_w, E)[2]\ \} = \mathrm{H}^1(F_w/K_v, E(F_w)).$$

Thus, it remains to show that

$$\Upsilon = \mathrm{H}^1(F_w/K_v, E(F_w)).$$

Let σ denote the generator of $\mathrm{Gal}(F_w/K_v)$. Then a class in $\mathrm{H}^1(F_w/K_v, E(F_w))$ is represented by a cocycle ρ such that $P := \rho(\sigma) \in E(F_w)$ satisfies $P + P^\sigma = 0$, and vice versa. P and P' give the same class if and only if $P - P' \in (\sigma - 1)(F_w)$. By Lemma 2.3.1, P can be viewed as a point of $E^F(K_v)$, while its image under

$$E^F(K_v) \longrightarrow E^F(K_v)/2E^F(K_v) \longrightarrow \mathrm{H}^1_f(K_v, E[2])$$

is represented by the cocycle η such that if Q is a chosen point satisfying $2Q = P$, then for every $\tau \in G_v$,

$$\eta(\tau) = \begin{cases} Q^\tau - Q \in E[2], & \text{if } \tau \in G_w; \\ -Q^\tau - Q \in E[2], & \text{if } \tau \notin G_w. \end{cases}$$

View eta as a $E(K_v)$-valued cocycle and write $\xi = \rho - \eta$. It follows that

$$\xi(\tau) = -Q^\tau + Q, \quad \text{for all } \tau \in G_v,$$

and hence ξ is a coboundary.

□

The proof of above lemma also prove the following. Let C^* denote the dual group (also the Pontryagin dual) of a finite abelian group C.

Lemma 3.2.2. *The local Tate duality pairing induces an isomorphism*

$$\mathrm{H}^1(F_w/K_v, E(F_w))^* \cong E(K_v)/E_N(K_v).$$

Definition 3.2.3. *Let notation be as above. Define*

$$\delta_v(E, F/K) := \dim_{\mathbb{F}_2}(E(K_v)/E_N(K_v)).$$

Lemma 3.2.4. $\delta_v(E, F/K)$ *is finite*

Proof. The lemma is a consequence of Lemma 3.1.1 as $E_N(K_v)$ contains $2E(K_v)$.

□

3.3. **The unramified case.** As before, F/K is a quadratic extension and w is a place of F sitting over v. The following proposition and lemma hold trivially true if v splits over F, in the proofs we can assume that F_w/K_v is a quadratic extension.

Proposition 3.3.1. *If F_w/K_v is unramified, then the natural map*

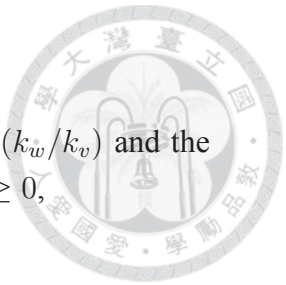
$$\mathrm{H}^1(F_w/K_v, E_0(F_w)) \longrightarrow \mathrm{H}^1(k_w/k_v, \tilde{E}_{ns}(k_w))$$

is an isomorphism.

Proof. The exact sequence (8) gives rise to the long exact sequence

$$M \longrightarrow \mathrm{H}^1(F_w/K_v, E_0(F_w)) \longrightarrow \mathrm{H}^1(F_w/K_v, \tilde{E}_{ns}(k_v)) \longrightarrow N$$

where $M = \mathrm{H}^1(F_w/K_v, E_1(F_w))$ and $N = \mathrm{H}^2(F_w/K_v, E_1(F_w))$. Thus, it suffices to show that $\mathrm{H}^q(F_w/K_v, E_1(F_w)) = 0$ for all $q > 0$.



Since F_w/K_v is unramified, $\mathrm{Gal}(F_w/K_v)$ can be identified with $\mathrm{Gal}(k_w/k_v)$ and the prime element π_v is also a prime element of L_w. Hence, we have, for $r \geq 0$,

$$\mathcal{M}_w^r/\mathcal{M}_w^{r+1} \cong k_w$$

as $\mathrm{Gal}(k_w/k_v)$-modules. In particular, Lang's theorem ([4, Theorem 2]) implies that

$$\mathrm{H}^q(F_w/K_v, \mathcal{M}_w^r/\mathcal{M}_w^{r+1}) = 0, \quad \text{for all } \ q > 0.$$

By Proposition 2.4.2, we have the exact sequence

$$0 \longrightarrow \hat{E}(\mathcal{M}_w^{r+1}) \longrightarrow \hat{E}(\mathcal{M}_w^r) \longrightarrow \mathcal{M}_w^r/\mathcal{M}_w^{r+1} \longrightarrow 0$$

that implies

$$\mathrm{H}^q(F_w/K_v, \hat{E}(\mathcal{M}_w^r)) = \mathrm{H}^q(F_w/K_v, \hat{E}(\mathcal{M}_w^{r+1})).$$

Hence a given q-cocycle ρ_r representing a cohomology class in $\mathrm{H}^q(F_w/K_v, \hat{E}(\mathcal{M}_w^r))$ can be written as $\rho_{r+1} + \partial\xi_r$ where ρ_{r+1} represents the corresponding cohomology class in $\mathrm{H}^q(F_w/K_v, \hat{E}(\mathcal{M}_w^{r+1}))$ and ξ_r is a $\hat{E}(\mathcal{M}_w^{r+1})$-valued cochain. Denote $\xi = \sum_{r=0}^{\infty} \xi_r$. Since $\bigcap_{r=0}^{\infty} \hat{E}(\mathcal{M}_r) = 0$, we have $\rho_1 = \partial\xi$. This shows $\mathrm{H}^q((F_w/K_v, \hat{E}(\mathcal{M}_w)) = 0$ and proves the proposition as $E_1(F_w) = \hat{E}(\mathcal{M}_w)$ by Proposition 2.4.2 and Remark 2.4.3.

□

Corollary 3.3.2. *If F_w/K_v is unramified, E is an elliptic curve with good reduction at v. Then $N_{F_w/K_v}(E(F_w)) = E(K_v)$.*

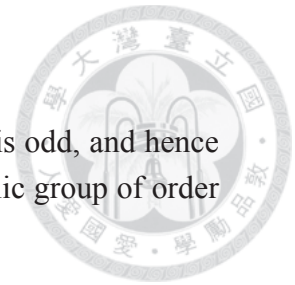
Proof. By Lemma 3.2.2, $(E(K_v)/N_{F_w/K_v}(E(F_w)))^* \cong \mathrm{H}^1(F_w/K_v, E(F_w))$. Applying Lemma 3.3.1, we have $\mathrm{H}^1(F_w/K_v, E(F_w)) \cong H^1(k_w/k_v, \tilde{E}(k_w))$. Then apply Lang's theorem ([4, Theorem 2]). □

3.3.1. *The multiplicative reduction case.*

Lemma 3.3.3. *Suppose F/K is unramified at v, E is a Tate curve over K_v and* $\mathrm{ord}_v(\Delta_f)$ *is odd, then $E_N(K_v) = E(K_v)$.*

Proof. By Lemma 2.4.1, we may assume that the defining equation (1) is minimal. Then

$$\Delta_f = q\prod_{n\geq 1}(1-q^n)^{24},$$



where q is the local Tate period [3, Ch V Theorem 3.1]. Then $\mathrm{ord}_v(q)$ is odd, and hence $q \notin \mathrm{N}_{F_w/K_v}(F_w^*)$. By local class field theory, $K_v^*/N_{F_w/K_v}(F_w^*)$ is a cyclic group of order 2. Since the residue class of q generates this group, we have

$$E(K_v)/E_N(K_v) \cong K_v^*/N_{F_w/K_v}(F_w^*)q^{\mathbb{Z}} = 1.$$

□

Corollary 3.3.4. *Under the condition in the above lemma,* $\mathrm{H}^1(F_w/K_v, E(F_w)) = 0$.

Proof. By Lemma 3.2.2. □

Lemma 3.3.5. *Suppose that F_w/K_v is an unramified quadratic extension. If E/K_v has multiplicative reduction and* $\mathrm{ord}_v(\Delta_f)$ *is odd, then $E_N(K_v) = E(K_v)$.*

Proof. If E has split multiplicative reduction, then E is a Tate curve and the lemma follows from Lemma 3.3.3.

If E has non-split multiplicative reduction, then E^F is a Tate curve over K_v. By Corollary 3.3.4, we have

$$\mathrm{H}^1(F_w/K_v, E^F(F_w)) = 0.$$

Let σ be the generator of $\mathrm{Gal}(F_w/K_v)$, Then by Lemma 2.3.1

$$E(K_v)/E_N(K_v) = \{P \in E^F(F_w) \mid P^\sigma + P = 0\}/(\sigma - 1)E^F(F_w),$$

which is isomorphic to $\mathrm{H}^1(F_w/K_v, E^F(F_w))$.

□

3.4. **Summary.** Now we summarize the results in this section. Let F/K be a given quadratic extension and w be a place of F sitting over v.

Lemma 3.4.1. *Suppose at least one of the following conditions holds:*

(a) *v split in F/K,*
(b) *$v \nmid 2\infty$ and $E(K_v)[2] = 0$,*
(c) *E has multiplicative reduction at v, F/K is unramified at v, and* $\mathrm{ord}_v(\Delta_f)$ *is odd,*
(d) *v is real and $\Delta_f < 0$,*
(e) *v is a prime where E has good reduction and v is unramified in F/K.*

Then $\mathrm{H}^1_f(K_v, E[2]) = \mathrm{H}^1_f(K_v, E^F[2])$ *and* $\delta_v(E, F/K) = 0$.

Proof. First we note that by Lemma 3.2.1 and Definition 3.2.3 the three assertions

$$\mathrm{H}^1_f(K_v, E[2]) = \mathrm{H}^1_f(K_v, E^F[2]),$$

$$E_N(K_v) = E(K_v),$$

$$\delta_v(E, F/K) = 0,$$

are equivalent. If (a) holds, then $F_w = K_v$. Hence $E_N(K_v) = E(K_v)$. If (b) holds, then the lemma follows from Lemma 3.1.2(i). Similarly, apply Lemma 3.3.5 (resp. Corollary 3.3.2), if (c) (resp. (e)) holds. If v is real and $\Delta_f < 0$ in K_v, then the defining polynomial f has a unique root in K_v. This implies as a topological group $E(K_v) \cong \mathrm{S}^1$ and is connected. If F_w/K_v is a quadratic extension, then $F_w = \mathbb{C}$ and $E(F_w)$ is compact and connected. Therefore, $E_N(K_v)$ is a closed subgroup of $E(K_v)$ of finite index. Then $E_N(K_v)$ is also an open subgroup. Hence $E_N(K_v) = E(K_v)$.

□

Lemma 3.4.2. *If $v \nmid 2\infty$, E has good reduction at v, and v is ramified in F/K, then*

$$\mathrm{H}^1_f(K_v, E[2]) \cap \mathrm{H}^1_f(K_v, E^F[2]) = 0,\ \delta_v(E, F/K) = \dim_{\mathbb{F}_2}(E(K_v)[2]).$$

Proof. Since v is ramified, $k_w = k_v$. Then Lemma 2.4.4 applied to K_v and F_w respectively gives rise to

$$E(K_v)/2E(K_v) \cong \tilde{E}(k_v)/2\tilde{E}(k_v) \cong E(F_w)/2E(F_w).$$

Since the isomorphism respects the $\mathrm{Gal}(F_w/K_v)$ actions, we have

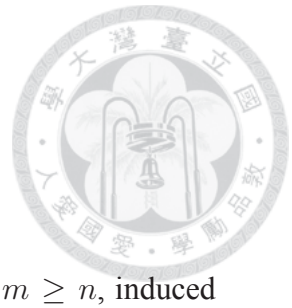
$$0 = 2E(K_v)/2E(K_v) = E_N/2E(K_v).$$

Therefore, by Lemma 3.2.1, $\mathrm{H}^1_f(K_v, E[2]) \cap \mathrm{H}^1_f(K_v, E^F[2]) = E_N(K_v)/2E(K_v) = 0$, and by Lemma 3.1.2(i), $\delta_v(E, F/K) = \dim_{\mathbb{F}_2}(E(K_v)[2])$. □

4. Global results

Let F be a quadratic extension and let σ denote the generator of $G_{F/K}$. For a $G_{F/K}$-module C, denote the ± 1-eigenspace

$$C^{(\pm 1)} = \{c \in C \mid c^\sigma = \pm c\}.$$



4.1. **The parity of $d_2(E/K)$.** Define

$$\text{Sel}_{2^\infty}(E/K) := \varinjlim_n \text{Sel}_{2^n}(E/K)$$

where the injective limit is taken over $\text{Sel}_{2^n}(E/K) \longrightarrow \text{Sel}_{2^m}(E/K)$, $m \geq n$, induced from the natural embedding $E[2^n] \longrightarrow E[2^m]$. Write $E[2^\infty]$ for $\bigcup_n E[2^n]$. Then we have the exact sequence

$$0 \longrightarrow \text{Sel}_{2^\infty}(E/K) \longrightarrow \text{H}^1(K, E[2^\infty]) \xrightarrow{loc} \prod_v \text{H}^1(K_v, E). \tag{18}$$

Also, from the long exact sequence derived from

$$0 \longrightarrow E[2] \longrightarrow E[2^\infty] \xrightarrow{[2]} E[2^\infty] \longrightarrow 0$$

we deduce the exact sequence

$$\text{Sel}_2(E/K) \longrightarrow \text{Sel}_{2^\infty}(E/K) \xrightarrow{[2]} \text{Sel}_{2^\infty}(E/K).$$

The 2-torsion group $\text{Sel}_{2^\infty}(E/K)[2]$ are obtained from $\text{Sel}_2(E/K)$, and hence finite. In particular, $\text{Sel}_{2^\infty}(E/K)$ is a cofinitely generated $\mathbb{Z}_2$-module. The restriction map

$$\text{H}^1(K, E[2^\infty]) \xrightarrow{\text{Res}} \text{H}^1(F, E[2^\infty])^{G_{F/K}} = \text{H}^1(F, E[2^\infty])^{(1)} , \tag{19}$$

induces

$$\text{Sel}_{2^\infty}(E/K) \xrightarrow{\text{res}} \text{Sel}_{2^\infty}(E/F)^{(1)}. \tag{20}$$

Lemma 4.1.1. *the homomorphism* (20) *has finite kernel and cokernel.*

Proof. The kernel of Res equals $\text{H}^1(F/K, E(K)[2^\infty])$ which is a finite group because $E(K)[2^\infty]$ is finite. hence the kernel of res is also finite. Write $B = \text{Res}^{-1}(\text{Sel}_{2^\infty}(E/F)^{(1)})$. Then we have the exact sequence

$$B \xrightarrow{\text{Res}} \text{Sel}_{2^\infty}(E/F)^{(1)} \longrightarrow \text{H}^2(F/K, E(K)[2^\infty])$$

and, by (18), the exact sequence

$$0 \longrightarrow \text{Sel}_{2^\infty}(E/K) \longrightarrow B \xrightarrow{loc} \prod_v \text{H}^1(F_v/K_v, E(F_v)).$$

Now $\text{H}^2(F/K, E(K)[2^\infty])$ is finite and by Lemma 3.2.2, Lemma 3.2.4 and Corollary 3.3.2, the group $\prod_v \text{H}^1(F_v/K_v, E(F_v))$ is also finite. Hence the cokernel of res is finite.

□

Note that since $E \cong E^F$ over F, we have $\mathrm{Sel}_{2^\infty}(E^F/F) = \mathrm{Sel}_{2^\infty}(E/F)$, while Lemma 2.3.1 implies

$$\mathrm{Sel}_{2^\infty}(E^F/F)^{(\mp 1)} = \mathrm{Sel}_{2^\infty}(E/F)^{(\pm 1)}.$$

Apply Lemma 4.1.1 to E^F, we have the restriction map

$$\mathrm{Sel}_{2^\infty}(E^F/K) \xrightarrow{\mathrm{res}^F} \mathrm{Sel}_{2^\infty}(E/F)^{(-1)} \tag{21}$$

of finite kernel and cokernel.

Lemma 4.1.2. *If E^F is the quadratic twist of E by F, then the natural map*

$$\mathrm{Sel}_{2^\infty}(E/K) \oplus \mathrm{Sel}_{2^\infty}(E^F/K) \longrightarrow \mathrm{Sel}_{2^\infty}(E/F)$$

has finite kernel and cokernel.

Proof. Before getting started, we note that if $f : A \to B$ and $g : B \to C$ both have finite kernel (cokernel), then $g \circ f : A \to C$ also have finite kernel (cokernel). This comes from the diagram chasing (the ``snake lemma'') on

$$\begin{array}{ccccccc} A & \xrightarrow{f} & B & \longrightarrow & \mathrm{coker}\, f & \longrightarrow & 0 \\ & \searrow^{g\circ f} & \downarrow g & & \downarrow & & \\ 0 & \longrightarrow & C & = & C & \longrightarrow & 0, \end{array}$$

which gives the exact sequence

$$\ker f \longrightarrow \ker(g \circ f) \longrightarrow \ker g \longrightarrow \mathrm{coker}\, f \longrightarrow \mathrm{coker}(g \circ f) \longrightarrow \mathrm{coker}\, g.$$

The conclusion follows easily.

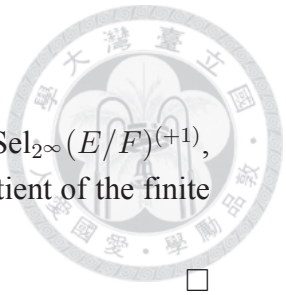
Since the desired map is the composition of

$$\mathrm{Sel}_{2^\infty}(E/K) \oplus \mathrm{Sel}_{2^\infty}(E^F/K) \xrightarrow{\mathrm{res} \oplus \mathrm{res}^F} \mathrm{Sel}_{2^\infty}(E/F)^{(+1)} \oplus \mathrm{Sel}_{2^\infty}(E/F)^{(-1)},$$

obtained by putting (21) and (21) together, and

$$\mathrm{Sel}_{2^\infty}(E/F)^{(+1)} \oplus \mathrm{Sel}_{2^\infty}(E/F)^{(-1)} \longrightarrow \mathrm{Sel}_{2^\infty}(E/F), \tag{22}$$

mapping (x, y) to $x+y$, we only need to show the latter map has finite kernel and cokernel. But this follows form the fact that $\mathrm{Sel}_{2^\infty}(E/F)$ is a cofinitely generated $\mathbb{Z}_2$-module, and hence so are the subgroups $\mathrm{Sel}_{2^\infty}(E/F)^{(+1)}$ and $\mathrm{Sel}_{2^\infty}(E/F)^{(-1)}$. If (x, y) is in the kernel of the map, then $x = x^\sigma = -y^\sigma = y = -x$, and hence $2x = 0$. Therefore, the kernel is finite since it is contained in the finite group $\mathrm{Sel}_{2^\infty}(E/F)^{(+1)}[2] \oplus \mathrm{Sel}_{2^\infty}(E/F)^{(-1)}[2]$. Also,



for every $z \in \text{Sel}_{2^\infty}(E/F)$, $2z$ satisfies $2z = x + y$, with $x = z + z^\sigma \in \text{Sel}_{2^\infty}(E/F)^{(+1)}$, $y = z - z^\sigma \in \text{Sel}_{2^\infty}(E/F)^{(-1)}$. Hence the cokernel of the map is a quotient of the finite group $\text{Sel}_{2^\infty}(E/F)/2\,\text{Sel}_{2^\infty}(E/F)$.

□

We have the exact sequence

$$0 \longrightarrow \mathbb{Q}_2/\mathbb{Z}_2 \otimes_{\mathbb{Z}} E(K) \longrightarrow \text{Sel}_{2^\infty}(E/K) \longrightarrow Ш(E/K)_2 \longrightarrow 0 \tag{23}$$

where $Ш(E/K)_2$ denote the 2-primary part of $Ш(E/K)$.

It is obtained by taking the injective limits of the vertical arrows in the diagram:

$$\begin{array}{ccccccc}
0 & \longrightarrow & E(K)/2E(K) & \longrightarrow & \text{Sel}_2(E/K) & \longrightarrow & Ш(E/K)[2] \longrightarrow 0 \\
 & & \downarrow{\scriptstyle [2]} & & \downarrow{\scriptstyle i_*} & & \downarrow{\scriptstyle i} \\
0 & \longrightarrow & E(K)/2^2E(K) & \longrightarrow & \text{Sel}_{2^2}(E/K) & \longrightarrow & Ш(E/K)[2^2] \longrightarrow 0 \\
 & & \downarrow{\scriptstyle [2]} & & \downarrow{\scriptstyle i_*} & & \downarrow{\scriptstyle i} \\
 & & \vdots & & \vdots & & \vdots \\
 & & \downarrow{\scriptstyle [2]} & & \downarrow{\scriptstyle i_*} & & \downarrow{\scriptstyle i} \\
0 & \longrightarrow & E(K)/2^nE(K) & \longrightarrow & \text{Sel}_{2^n}(E/K) & \longrightarrow & Ш(E/K)[2^n] \longrightarrow 0 \\
 & & \downarrow{\scriptstyle [2]} & & \downarrow{\scriptstyle i_*} & & \downarrow{\scriptstyle i} \\
 & & \vdots & & \vdots & & \vdots
\end{array}$$

If r denote the rank of $E(K)$, by lemma 2.2.3, we have

$$d_2(E/K) = r + \dim_{\mathbb{F}_2} E(K)[2] + \dim_{\mathbb{F}_2} Ш(E/K)[2], \tag{24}$$

while (23) implies

$$\dim_{\mathbb{F}_2} \text{Sel}_{2^\infty}(E/K)[2] = r + \dim_{\mathbb{F}_2} Ш(E/K)[2]. \tag{25}$$

Therefore,

$$\dim_{\mathbb{F}_2} \text{Sel}_{2^\infty}(E/K)[2] = d_2(E/K) - \dim_{\mathbb{F}_2} E(K)[2]. \tag{26}$$

Lemma 4.1.3. *If F is a quadratic extension of K, then*

$$d_2(E/K) + d_2(E^F/K) \equiv d_2(E/F) + \dim_{\mathbb{F}_2}(E(F)[2]) \pmod 2.$$

Proof. It is a consequence of Lemma 4.1.2 together with the equalities (26) applied to E and E^F, because $E[2] = E^F[2]$ (Lemma 2.3.2). □

Lemma 4.1.4. *We have*

$$\text{rank}(E(F)) + \dim_{\mathbb{F}_2}(Ш(E/F)[2]) \equiv \sum_v \delta_v(E, F/K) \pmod 2.$$

Proof. This is [5, Theorem 1,2] □

Theorem 4.1.5. *We have*

$$d_2(E^F/K) \equiv d_2(E/K) + \sum_v \delta_v(E, F/K) \pmod 2.$$

Proof. The theorem is a consequence of Lemma 4.1.4, (25) (applied to E/F), (26) (applied to E/F), and Lemma 4.1.3 as follow:

$$\begin{aligned}
\textstyle\sum_v \delta_v(E, F/K) &\equiv \text{rank}(E(F)) + \dim_{\mathbb{F}_2}(Ш(E/F)[2]) \pmod 2 \\
&\equiv \dim_{\mathbb{F}_2} \text{Sel}_{2^\infty}(E/F) \pmod 2 \\
&\equiv d_2(E/F) - \dim_{\mathbb{F}_2}(E(F)[2]) \pmod 2 \\
&\equiv d_2(E/K) + d_2(E^F/K) \pmod 2.
\end{aligned}$$

□

4.2. **Comparing Selmer groups.** Similar to the localization map in the diagram (6), for every set T of places of K, consider the localization map

$$\text{H}^1(K, E[2]) \longrightarrow \prod_{v \notin T} \text{H}^1(K_v, E).$$

Also, denote the localization map

$$loc_T : \text{H}^1(K, E[2]) \longrightarrow \prod_{v \in T} \text{H}^1(K_v, E[2]).$$

Definition 4.2.1. *If T is a finite set of places of K, we define the strict and relaxed 2-Selmer groups $S_T \subset S^T \subset \text{H}^1(K, E[2])$ as follows:*

$$\begin{aligned}
S^T &= \ker\{\text{H}^1(K, E[2]) \longrightarrow \textstyle\prod_{v \notin T} \text{H}^1(K_v, E[2])/\,\text{H}^1_f(K_v, E[2])\} \\
S_T &= \ker\{S^T \longrightarrow \textstyle\prod_{v \in T} \text{H}^1(K_v, E[2])\}.
\end{aligned}$$

Let $(S^F)^T$ and S^F_T denote the strict and relaxed 2-Selmer groups for E^F. By definition, $S_T \subset \text{Sel}_2(E/K) \subset S^T$. Put

$$V_T := loc_T(\text{Sel}_2(E/K)) \subset \prod_{v \in T} \text{H}^1_f(K_v, E[2])$$

and

$$V^F_T := loc_T(\text{Sel}_2(E^F/K)) \subset \prod_{v \in T} \text{H}^1_f(K_v, E^F[2]).$$

Lemma 4.2.2. $\dim_{\mathbb{F}_2} S^T - \dim_{\mathbb{F}_2} S_T = \sum_{v\in T} \dim_{\mathbb{F}_2} \mathrm{H}^1_f(K_v, E[2])$

Proof. This is [8, Theorem 1.7.3] □

Proposition 4.2.3. *Suppose that all places v of multiplicative reduction such that* $\mathrm{ord}_v(\Delta_f)$ *is odd are unramified in F/K and all of the following places split in F/K:*

(a) *all places where E has additive reduction,*
(b) *all places v of multiplicative reduction such that* $\mathrm{ord}_v(\Delta_f)$ *is even,*
(c) *all places above 2,*
(d) *all real places v with $\Delta_f > 0$ in K_v.*

Let T be the set consisting of all (finite) places $\mathfrak{p}$ of K such that F/K is ramified at $\mathfrak{p}$ and $E(K_\mathfrak{p})[2] \neq 0$. Then

$$d_2(E^F/K) = d_2(E/K) - \dim_{\mathbb{F}_2} V_T + d$$

for some d satisfying

$$0 \leq d \leq \dim_{\mathbb{F}_2}(\bigoplus_{\mathfrak{p}\in T} \mathrm{H}^1_f(K_\mathfrak{p}, E[2])/V_T)$$

and

$$d \equiv \dim_{\mathbb{F}_2}(\bigoplus_{\mathfrak{p}\in T} \mathrm{H}^1_f(K_\mathfrak{p}, E[2])/V_T) \pmod 2.$$

Proof. First we deduce the equality

$$d_2(E^F/K) - \dim_{\mathbb{F}2} V_T^F = d_2(E/K) - \dim_{\mathbb{F}2} V_T. \tag{27}$$

By the assumption on T, every $v \notin T$ satisfies the condition in Lemma 3.4.1, and hence $\mathrm{H}^1_f(K_v, E[2]) = \mathrm{H}^1_f(K_v, E^F[2])$. Then

$$S^T = \ker\{\mathrm{H}^1(K, E[2]) \longrightarrow \prod_{v\notin T} \mathrm{H}^1(K_v, E[2])/\mathrm{H}^1_f(K_v, E[2])\} = (S^F)^T$$

$$S_T = \ker\{S^T \longrightarrow \prod_{v\in T} \mathrm{H}^1(K_v, E)[2])\} = S_T^F$$

Therefore we have $S_T \subset \mathrm{Sel}_2(E^F/K) \subset S^T$. Then (27) follows from the exact sequences

$$0 \longrightarrow S_T \longrightarrow \mathrm{Sel}_2(E/K) \xrightarrow{loc_T} V_T \longrightarrow 0$$

and

$$0 \longrightarrow S_T \longrightarrow \mathrm{Sel}_2(E^F/K) \xrightarrow{loc_T} V_T^F \longrightarrow 0.$$

Next we prove that $d := \dim_{\mathbb{F}_2} V_T^F$ satisfies the required condition. For simplicity, denote $t := \Sigma_{\mathfrak{p}\in T} \dim_{\mathbb{F}_2} \mathrm{H}^1_f(K_\mathfrak{p}, E[2])$. Note that every $\mathfrak{p} \in T$, satisfies the condition of lemma 3.4.2 and that of Lemma 3.1.2 as well. By Lemma 3.4.2,

$$\mathrm{H}^1_f(K_\mathfrak{p}, E[2]) \cap \mathrm{H}^1_f(K_\mathfrak{p}, E^F[2]) = 0, \quad \text{for all } \mathfrak{p} \in T.$$

Thus, if $c \in \mathrm{Sel}_2(E/K) \cap \mathrm{Sel}_2(E^F/K)$, then

$$loc_T(c) \in \prod_{\mathfrak{p}\in T} \mathrm{H}^1_f(K_\mathfrak{p}, E[2]) \cap \mathrm{H}^1_f(K_\mathfrak{p}, E^F[2]) = 0,$$

and hence $c \in S_T$. Therefore we must have

$$\mathrm{Sel}_2(E/K) \cap \mathrm{Sel}_2(E^F/K) = S_T.$$

Since $\mathrm{Sel}_2(E/K) + \mathrm{Sel}_2(E^F/K) \subset S^T$, by Lemma 4.2.2, we have

$$\begin{aligned} \dim_{\mathbb{F}_2} V_T + d &= \dim_{\mathbb{F}_2}(\mathrm{Sel}_2(E/K)/S_T) + \dim_{\mathbb{F}_2}(\mathrm{Sel}_2(E^F/K)/S_T) \\ &\leq \dim_{\mathbb{F}_2}(S^T/S_T) \\ &= \Sigma_{\mathfrak{p}\in T} \dim_{\mathbb{F}_2} \mathrm{H}^1_f(K_\mathfrak{p}, E[2]). \\ &= t \end{aligned}$$

Hence

$$0 \leq d \leq t - \dim_{\mathbb{F}_2} V_T = \dim_{\mathbb{F}_2}(\bigoplus_{\mathfrak{p}\in T} \mathrm{H}^1_f(K_\mathfrak{p}, E[2])/V_T),$$

as required. Lemma 3.4.1 says $\delta_v(E, F/K) = 0$ if $v \notin T$, this together with Lemma 3.1.2 and Lemma 3.4.2 imply

$$\sum_v \delta_v(E, F/K) = \sum_{\mathfrak{p}\in T} \delta_\mathfrak{p}(E, F/K) = \sum_{\mathfrak{p}\in T} \dim_{\mathbb{F}_2}(E(K_\mathfrak{p})[2]) = t$$

Then Theorem 4.1.5 says $d_2(E^F/K) \equiv d_2(E/K) + t \pmod 2$. This and (27) imply

$$d \equiv t - \dim_{\mathbb{F}_2} V_T \equiv \dim_{\mathbb{F}_2}(\bigoplus_{\mathfrak{p}\in T} \mathrm{H}^1_f(K_v, E[2])/V_T) \pmod 2.$$

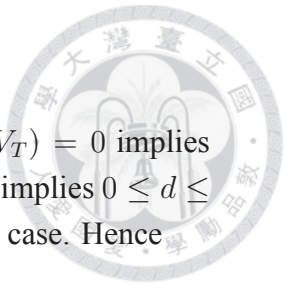
□

Corollary 4.2.4. *Suppose E, F/K, and T are as in* Proposition 4.2.3. *Then the following holds:*

(a) *If* $\dim_{\mathbb{F}_2}(\bigoplus_{\mathfrak{p}\in T} \mathrm{H}^1_f(K_\mathfrak{p}, E[2])/V_T) \leq 1$, *then*

$$d_2(E^F/K)) = d_2(E/K) - 2\dim_{\mathbb{F}_2} V_T + \sum_{\mathfrak{p}\in T} \dim_{\mathbb{F}_2} \mathrm{H}^1_f(K_\mathfrak{p}, E[2])$$

(b) *If* $E(K_\mathfrak{p})[2] = 0$ *for every* $\mathfrak{p} \in T$, *then* $d_2(E^F/K) = d_2(E/K)$



Proof. By Proposition 4.2.3, the condition $\dim_{\mathbb{F}_2}(\bigoplus_{\mathfrak{p}\in T} \mathrm{H}^1_f(K_\mathfrak{p}, E[2])/V_T) = 0$ implies $0 \le d \le 0$, and hence $d = 0$; while $\dim_{\mathbb{F}_2}(\bigoplus_{\mathfrak{p}\in T} \mathrm{H}^1_f(K_\mathfrak{p}, E[2])/V_T) = 1$ implies $0 \le d \le 1$ and $d \equiv 1 \pmod 2$. Thus, $d = \dim_{\mathbb{F}_2}(\oplus_{\mathfrak{p}\in T} \mathrm{H}^1_f(K_\mathfrak{p}, E[2])/V_T)$ in both case. Hence

$$\begin{aligned} d_2(E^F/K) &= d_2(E/K) - \dim_{\mathbb{F}_2} V_T + d \\ &= d_2(E/K) - 2\dim_{\mathbb{F}_2} V_T + \textstyle\sum_{\mathfrak{p}\in T} \mathrm{H}^1_f(K_\mathfrak{p}, E[2]) \end{aligned}$$

the assertion (b) follows from (a) since in this case, T is empty. □

4.3. **Special results on Galois groups.** Let $M := K(E[2])$. If $c \in \mathrm{H}^1(K, E[2])$ is a cohomology class represented by a 1-cocycle ρ and $\sigma \in G_K$, let

$$c(\sigma) \in E[2]/(\sigma - 1)E[2]$$

denote the residue class of $\rho(\sigma)$ which is independent of the choice of ρ. Let $\tilde{c} \in \mathrm{H}^1(M, E[2])$ denote the image of c under the restriction map

$$\mathrm{H}^1(K, E[2]) \longrightarrow \mathrm{H}^1(M, E[2]).$$

Then $\tilde{c}$ gives rise to a group homomorphism (also denoted by $\tilde{c}$, by abuse of notation)

$$\tilde{c} : G_M \longrightarrow E[2].$$

Lemma 4.3.1. *Suppose* $\mathrm{Gal}(M/K) \cong S_3$ *and* $\sigma \in G_K$. *Let* C *be a finite subgroup of* $\mathrm{H}^1(K, E[2])$ *and let* $\phi : C \longrightarrow E[2]/(\sigma - 1)E[2]$ *be a group homomorphism. Then there is a* $\gamma \in G_K$ *such that* $\gamma|_{MK^{ab}} = \sigma|_{MK^{ab}}$ *and* $c(\gamma) = \phi(c)$ *for all* $c \in C$.

Proof. Fix an $\mathbb{F}_2$-basis $\{c_1, \ldots, c_k\}$ of C. We will show that there exists a finite extension N/M such that $MK^{ab} \cap N = M$ and

$$\tilde{c}_1 \times \cdots \times \tilde{c}_k : G_M \longrightarrow E[2]^k$$

gives rise to an isomorphism $\mathrm{Gal}(N/M) \cong E[2]^k$. Then the first property of N gives

$$\mathrm{Gal}(NK^{ab}/M) \cong \mathrm{Gal}(N/M) \times \mathrm{Gal}(MK^{ab}/M),$$

which combining with the second property implies

$$G_M \twoheadrightarrow \mathrm{Gal}(NK^{ab}/M) \cong E[2]^k \times \mathrm{Gal}(MK^{ab}/M).$$

Now we may take $\tau \in G_M$ such that $\tau|_{MK^{ab}} = 1$ and

$$c_i(\tau) \equiv \phi(c_i) - c_i(\sigma) \pmod{(\sigma - 1)E[2]}, \quad \text{for} 1 \le i \le k.$$

Then

$$c_i(\tau\sigma) = c_i(\tau) + c_i(\sigma)^\tau \equiv \phi(c_i) \pmod{(\sigma-1)E[2]}, \quad \text{for} 1 \le i \le k.$$

Since $\{c_i\}_{i=1}^k$ is a basis of C, we can take $\gamma := \tau\sigma$.

To prove the existence of N, let $\Gamma := \mathrm{Gal}(M/K) \cong \mathrm{Aut}(E[2])$. Then we have exact sequence

$$0 \longrightarrow \mathrm{H}^1(\Gamma, E[2]) \xrightarrow{\text{Inf}} \mathrm{H}^1(K, E[2]) \xrightarrow{\text{Res}} \mathrm{H}^1(M, E[2])^\Gamma.$$

We first show that $\mathrm{H}^1(\Gamma, E[2]) = 0$. Let Γ' be the subgroup of Γ of order 2 generated by the permutation $\beta := (12)$. The composition of restriction and corestriction map

$$\mathrm{H}^1(\Gamma, E[2]) \xrightarrow{\text{Res}} \mathrm{H}^1(\Gamma', E[2]) \xrightarrow{\text{Cor}} \mathrm{H}^1(\Gamma, E[2])$$

is multiplication by $[\Gamma : \Gamma'] = 3$. Since $\mathrm{H}^1(\Gamma, E[2])$ is a 2-group, $\mathrm{Cor} \circ \mathrm{Res}$ is an isomorphism, and hence Res is injective. Now we compute the group $\mathrm{H}^1(\Gamma', E[2])$. Since $\Gamma' = \{e, \beta\}$ and $E[2] = \{0, (x_1, 0), (x_2, 0), (x_3, 0)\}$, if a class $[\varphi] \in \mathrm{H}^1(\Gamma', E[2])$ is represented by the cocycle φ, then $\varphi(\beta)^\beta + \varphi(\beta) = 0$. Hence $\varphi(\beta) = 0$ or $(x_3, 0)$. But for the latter case, we have $\varphi(\beta) = (x_1, 0)^\beta - (x_1, 0)$, and hence φ is a coboundary. This shows $\mathrm{H}^1(\Gamma', E[2]) = 0$ and so is $\mathrm{H}^1(\Gamma, E[2])$. Therefore,

$$\mathrm{H}^1(K, E[2]) \hookrightarrow \mathrm{H}^1(M, E[2])^\Gamma = \mathrm{Hom}(G_M, E[2])^\Gamma.$$

In particular, $\tilde{c}_1, \ldots, \tilde{c}_k \in \mathrm{Hom}(G_M, E[2])^\Gamma$ are linearly independent over $\mathbb{F}_2$. Set

$$W := G_M / \ker(\tilde{c}_1 \times \cdots \times \tilde{c}_k)$$

and let N be the fixed field of W so that $W = \mathrm{Gal}(N/M)$. Then $\tilde{c}_1 \times \cdots \times \tilde{c}_k$ induces an injection

$$\psi : \ W \hookrightarrow E[2]^k.$$

Furthermore, since each $\tilde{c}_i$ is fixed by the action of Γ, ψ is a homomorphism of Γ-modules. Here Γ acts on W by conjugation as usual: if $w \in W$ and $\tilde{\alpha} \in \mathrm{Gal}(N/K)$ is a lift of $\alpha \in \Gamma$, then $w^\alpha := \tilde{\alpha} \cdot w \cdot \tilde{\alpha}^{-1}$; this action is independent of the lifting, indeed if $\tilde{\alpha}'$ is another lifting, then $\tilde{\alpha}' = \tilde{\alpha} \cdot w'$, for some w' in W, and hence $\tilde{\alpha}' \cdot w \cdot \tilde{\alpha}'^{-1} = \tilde{\alpha} \cdot w \cdot \tilde{\alpha}^{-1}$, because W is commutative. Since $E[2]$ is a simple Γ-module, $W \cong E[2]^j$ for some $j \le k$. Actually $j = k$ holds since we also have

$$j = \dim_{\mathbb{F}_2} \mathrm{Hom}(W, E[2])^\Gamma \ge k,$$

where the equality is due to

$$\mathrm{Hom}(E[2], E[2])^{\Gamma} = \mathrm{Hom}_{\Gamma}(E[2], E[2]) = \{0, id\},$$

while the inequality holds because $\{\tilde{c}_1, \ldots, \tilde{c}_k\}$ are linearly independent.

It remains to show that $MK^{ab} \cap N = M$. Since $\mathrm{Gal}(MK^{ab}/M)$ is commutative, we can also apply the conjugation action of Γ on it. The intersection $Q := M \cap K^{ab}$ is a quadratic extension of K. Write $G := \mathrm{Gal}(K^{ab}/K)$, $H := \mathrm{Gal}(K^{ab}/Q)$, and also $\tilde{G} := \mathrm{Gal}(MK^{ab}/K)$, $\tilde{H} := \mathrm{Gal}(MK^{ab}/Q)$. Since both M/Q and K^{ab}/Q are abelian extension, $\tilde{H}$ is commutative and can be written as $\mathrm{Gal}(M/Q) \times \mathrm{Gal}(K^{ab}/Q)$. This implies that the conjugation action of $\mathrm{Gal}(M/Q)$ on $\mathrm{Gal}(MK^{ab}/M)$ is the trivial action. Thus, action of Γ on $\mathrm{Gal}(MK^{ab}/M)$ can be obtained from the conjugation action of $\mathrm{Gal}(Q/K)$ on $\mathrm{Gal}(K^{ab}/Q) = H$. But since G is commutative, this action is also trivial. Therefore, the action of Γ on $\mathrm{Gal}(MK^{ab}/M)$ is trivial. This implies that the action of Γ on $\mathrm{Gal}(MK^{ab} \cap N/M)$ is also trivial. But $\mathrm{Gal}(MK^{ab} \cap N/M)$ is a quotient of $\mathrm{Gal}(N/M) = W$ and $W \cong E[2]^k$ has no nontrivial quotients on which Γ acts trivially, so $MK^{ab} \cap N = M$. □

Lemma 4.3.2. *Suppose $E(K)[2] = 0$, and c_1, c_2 are distinct non-zero elements of $\mathrm{H}^1(K, E[2])$. Then there is a $\gamma \in G_K$ such that $\gamma|_{MK^{ab}} = 1$ and $c_1(\gamma)$, $c_2(\gamma)$ form an $\mathbb{F}_2$-basis of $E[2]$.*

Proof. As lemma 4.3.1, let $\Gamma := \mathrm{Gal}(M/K)$. Then either $\Gamma \cong S_3$ or $\Gamma \cong \mathbb{Z}/3\mathbb{Z}$. In both case, $E[2]$ are irreducible Γ-module, and $\mathrm{H}^1(\Gamma, E[2]) = 0$.(the case $\Gamma \cong \mathbb{Z}/3\mathbb{Z}$ is easy to check.) Thus, we again have

$$\mathrm{Res}: \ \mathrm{H}^1(K, E[2]) \hookrightarrow \mathrm{Hom}(G_M, E[2])^{\Gamma}.$$

Let $\tilde{c}_1$, $\tilde{c}_2$ be the images of c_1, c_2 and consider $\tilde{c}_i : G_M \longrightarrow E[2]$. let N_i be the fixed field of $\ker(\tilde{c}_i)$. Then $\tilde{c}_i : \mathrm{Gal}(N_i/M) \longrightarrow E[2]$ is nonzero and respects the Γ-action as in the proof of lemma 4.3.1. But $E[2]$ have no nontrivial Γ-submodule, hence $\tilde{c}_i$ is an isomorphism. In particular each $\mathrm{Gal}(N_i/M)$ is a simple Γ-module containing no nontrivial submodule.

Denote $N = N_1 \cap N_2$. Then $\mathrm{Gal}(N_i/N)$ is a submodule of $\mathrm{Gal}(N_i/M)$. Hence, we either have $N_1 = N_2$ or $N_1 \cap N_2 = M$.

If $N_1 = N_2$, then $\tilde{c}_1$, $\tilde{c}_2 : \mathrm{Gal}(N/M) \to E[2]$ are different isomorphisms, so there exists $\tau \in \mathrm{Gal}(N/M)$ such that $\tilde{c}_1(\tau)$ and $\tilde{c}_2(\tau)$ are distinct and nonzero.

If $N_1 \cap N_2 = M$, then $\mathrm{Gal}(N_1N_2/M) \cong \mathrm{Gal}(N_1/M) \times \mathrm{Gal}(N_2/M) \cong E[2] \times E[2]$, hence we may choose two distinct, nonzero elements $P_1, P_2 \in E[2]$ and pull back (P_1, P_2) to $\tau \in \mathrm{Gal}(N_1N_2/M)$. The $\tilde{c}_1(\tau) = P_1$, $\tilde{c}_2(\tau) = P_2$ are distinct and nonzero.

As lemma 4.3.1, Γ act trivially on $\mathrm{Gal}(MK^{ab} \cap N_1N_2/M)$, and $\mathrm{Gal}(N_1N_2/M)$, being isomorphic to $E[2]$ or $E[2]^2$, has no nonzero quotient on which Γ act trivially, hence

$$MK^{ab} \cap N_1N_2 = M.$$

Therefore, we have

$$G_M \twoheadrightarrow \mathrm{Gal}(N_1N_2K^{ab}/M) \cong \mathrm{Gal}(MK^{ab}/M) \times \mathrm{Gal}(N_1N_2/M).$$

We complete the proof by taking $\gamma \in G_M$ such that $\gamma|_{MK^{ab}} = 1$ and $\gamma|_{N_1N_2} = \tau$. □

5. Twisting to lower and raise the Selmer rank

Recall (see [9, Ch V]) that a modulus $\mathfrak{m}$ for a number field K is a function from places of K to $\mathbb{Z}$ such that

(a) $\mathfrak{m}(\mathfrak{p}) \leq 0$ for all primes $\mathfrak{p}$, and $\mathfrak{m}(\mathfrak{p}) = 0$ for all but finitely many $\mathfrak{p}$;
(b) if $\mathfrak{p}$ is real, then $\mathfrak{m}(\mathfrak{p}) = 0$ or 1;
(c) if $\mathfrak{p}$ is complex, then $\mathfrak{m}(\mathfrak{p}) = 0$.

For simplicity denote $\mathfrak{m} := \prod_{\mathfrak{p}} \mathfrak{p}^{\mathfrak{m}(\mathfrak{p})}$. Let I denote the group of fractional ideals of K and for a modulus $\mathfrak{m}$, let $I^{S(\mathfrak{m})}$ denote the subgroup of I generated by

$$\{\mathfrak{p} \in I |\ \mathfrak{p} \text{ not dividing } \mathfrak{m}\},$$

let $K_{\mathfrak{m},1}$ denote the set of $a \in K^\times$ such that

$$\begin{cases} \mathrm{ord}_{\mathfrak{p}}(a-1) \geq m(\mathfrak{p}), & \text{for all finite } \mathfrak{p} \text{ dividing } \mathfrak{m} \\ a_{\mathfrak{p}} > 0, & \text{for all real } \mathfrak{p} \text{ dividing } \mathfrak{m}. \end{cases}$$

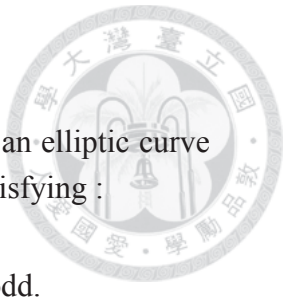
Denote $i : K_{\mathfrak{m},1} \longrightarrow I^{S(\mathfrak{m})}, a \mapsto (a)$. The quotient

$$C_{\mathfrak{m}} = I^{S(\mathfrak{m})}/i(K_{\mathfrak{m},1})$$

is called the (ray) class group modulo $\mathfrak{m}$, which is finite. For each modulus $\mathfrak{m}$, there corresponds an abelian extension $K(\mathfrak{m})/K$, the ray class field modulo $\mathfrak{m}$, which only ramified at primes (including infinite primes) dividing $\mathfrak{m}$. The Artin map is the isomorphism

$$C_{\mathfrak{m}} \longrightarrow \mathrm{Gal}(L(\mathfrak{m})/K),\ \mathfrak{p}_1^{n_1} \dots \mathfrak{p}_t^{n_t} \mapsto \prod (\mathfrak{p}_i, K(\mathfrak{m})/K)^{n_i},$$

where $(\mathfrak{p}_i, K(\mathfrak{m})/K)$ is the Frobenius automorphism of $K(\mathfrak{m})/K$ at $\mathfrak{p}_i$.



5.1. **The proof of Theorem 1.** In this section we assume that E/K is an elliptic curve such that $\mathrm{Gal}(K(E[2])/K) \cong S_3$. Also assume that K has a place v_0 satisfying :

- v_0 is real and $\Delta_f < 0$, in K_{v_0}, or
- $v_0 \nmid 2\infty$, E has multiplicative reduction at v_0, and $\mathrm{ord}_{v_0}(\Delta_f)$ is odd.

5.1.1. *Basic setting.* Denote $M := K(E[2])$ as before. Let Σ denote the set of places of K consists of all real places, all primes above 2, and all primes where E has bad reduction. Write $\mathfrak{d}$ for the formal product of all places in $\Sigma - \{v_0\}$ and consider it as a modulus. Let $K(8\mathfrak{d})$ be the ray class field of K modulo $8\mathfrak{d}$, let $K[8\mathfrak{d}]$ denote the maximal 2-power extension of K in $K(8\mathfrak{d})$.

Lemma 5.1.1. *We may find a $\sigma \in G_K$ satisfying the condition:*

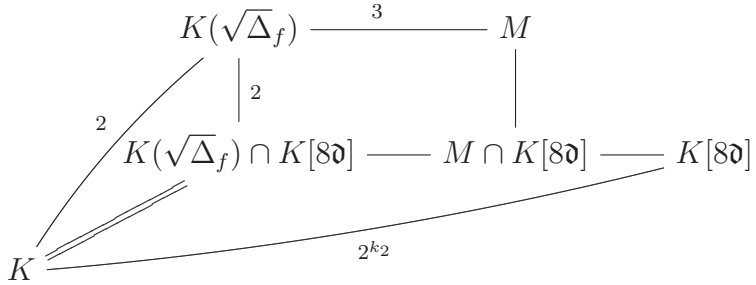
(a) $\sigma|_M \in \mathrm{Gal}(M/K) \cong S_3$ *has order* 2,
(b) $\sigma|_{K[8\mathfrak{d}]} = 1$.

It is clear that, by our choice of σ, $E[2]/(\sigma - 1)E[2] \cong \mathbb{Z}/2\mathbb{Z}$.

Proof. To prove the existence of σ, we show that

$$\mathrm{Gal}(MK[8\mathfrak{d}]/K) \cong \mathrm{Gal}(M/K) \times \mathrm{Gal}(K[8\mathfrak{d}]/K)$$

by showing $M \cap K[8\mathfrak{d}] = K$. The degree $[M : K(\sqrt{\Delta_f})] = 3$. We claim that $K(\sqrt{\Delta_f}) \cap K[8\mathfrak{d}] = K$. Then in view of the diagram



we see that $[M \cap K[8\mathfrak{d}] : K] = 1$ or 2 since it divides 2^{k_2} and 6. But S_3 has only one (normal) subgroup of order 3 implies $M \cap K[8\mathfrak{d}] \subset K(\sqrt{\Delta_f})$ which means $M \cap K[8\mathfrak{d}] = K$.

To prove our claim, note that $K[8\mathfrak{d}]/K$ is unramified at v_0. Hence it suffice to show that $K(\sqrt{\Delta_f})/K$ is ramified at v_0. If v_0 is real, then it is clear since $\Delta_f < 0$ in K_{v_0}. If $v_0 \nmid 2\infty$, let w_0 be a place of $K(\sqrt{\Delta_f})$ dividing v_0. Then

$$e\,\mathrm{ord}_{v_0}(\Delta_f) = \mathrm{ord}_{w_0}(\Delta_f) = 2\,\mathrm{ord}_{w_0}(\sqrt{\Delta_f})$$

and the fact that $\mathrm{ord}_{v_0}(\Delta_f)$ is odd implies $2 \mid e$. Hence $e = 2$. □

Let $\sigma \in G_K$ be an element satisfying the condition of Lemma 5.1.1. For simplicity, denote $C := \mathrm{Sel}_2(E/K) \subset \mathrm{H}^1(K, E[2])$ and let $\phi : C \longrightarrow E[2]/(\sigma - 1)E[2]$ be a group homomorphism.Since $K[8\mathfrak{d}]$ is an abelian extension of K, by Lemma 4.3.1, we can find $\gamma \in G_K$ such that $\gamma|_{MK[8\mathfrak{d}]} = \sigma|_{MK[8\mathfrak{d}]}$ and $c(\gamma) = \phi(c)$ for all $c \in C$.

Lemma 5.1.2. *Given ϕ, σ, γ as above, there is a quadratic extension F/K, depending on γ, such that*

(a) *all places $v \in \Sigma - \{v_0\}$ split in F.*
(b) *F/K is ramified at a place $\mathfrak{p} \notin \Sigma$ and nowhere else.*
(c) *$E(K_\mathfrak{p})[2] \neq 0$*

Proof. We know that (see the proof of Lemma 4.3.1) the restriction map $c \mapsto \tilde{c}$ induces

$$C \subset \mathrm{H}^1(K, E[2]) \longrightarrow \mathrm{Hom}(M, E[2])^\Gamma.$$

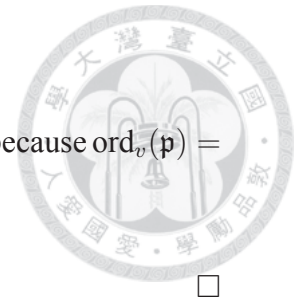
Let N_1/M be the fixed field of $\bigcap_{c \in C} \ker \tilde{c}$ and $N = N_1 K(8\mathfrak{d})$.Then, for every $c \in C$, we have the commutative diagram

$$\begin{array}{ccccc} G_N & \hookrightarrow & G_{N_1} & \hookrightarrow & G_M \\ & & & \searrow^{0} & \downarrow{\scriptstyle \tilde{c}} \\ & & & & E[2] \end{array}$$

By Chebotarev Density Theorem (see [9, Ch.V]), we can choose $\mathfrak{p}$ to be a place of K outside Σ, whose Frobenius in $\mathrm{Gal}(N/K)$ is the conjugacy class of γ. Since $\gamma|_{K[8\mathfrak{d}]} = \sigma|_{K[8\mathfrak{d}]} = 1$, and $[K(8\mathfrak{d}) : K[8\mathfrak{d}]]$ is odd, there is an odd positive integer h such that $\gamma^h\big|_{K(8\mathfrak{d})} = 1$. But $\mathrm{Gal}(K(8\mathfrak{d})/K) \cong I^{S(8\mathfrak{d})}/i(K_{8\mathfrak{d},1})$ via Artin map, and $\mathfrak{p}$ correspond to $\gamma|_{K(8\mathfrak{d})} \in \mathrm{Gal}(K(8\mathfrak{d})/K)$, we see that $\mathfrak{p}^h \in i(K_{8\mathfrak{d},1})$, which means $\mathfrak{p}^h = (\pi)$ with $\pi \equiv 1 \pmod{8\mathfrak{d}}$, positive at all real embeddings different from v_0.

Let $F = K(\sqrt{\pi})$, then we check the following holds.

- All places $v \in \Sigma - \{v_0\}$ split in F : if $v \nmid 2$ and is non-archimedean, $\pi \in 1 + \mathcal{M}_v^n \subset K_v$ and the map $1 + \mathcal{M}_v \longrightarrow 1 + \bar{\mathcal{M}}_v$, taking every element to its square, is an automorphism, which means π is a square in K_v; if v is real, then $\pi > 0$ in K_v; if $v \mid 2$, then π is also a square in K_v, by Hensel's lemma since $\pi \equiv 1 \pmod{8}$.



- F/K is ramified at $\mathfrak{p}$, because $\mathrm{ord}_{\mathfrak{p}}(\pi)$ is odd; and nowhere else, because $\mathrm{ord}_v(\mathfrak{p}) = 0$, if $v \neq \mathfrak{p}$ and $v \notin \Sigma$.
- $E(K_{\mathfrak{p}})[2] \neq 0$: $\mathrm{Frob}_{\mathfrak{p}}|_{E[2]} = \sigma|_{E[2]}$ has order 2.

□

Proposition 5.1.3. *Let notation be as above, Then the following holds*

(i) *There is a quadratic twist E^F of E, where F/K is ramified at exactly a place $\mathfrak{p} \notin \Sigma$, such that $d_2(E^F/K) = d_2(E/K) + 1$.*

(ii) *If $d_2(E/K) > 0$, then there is a quadratic twist E^F of E, where F/K is ramified at exactly a place $\mathfrak{p} \notin \Sigma$, such that*

$$d_2(E^F/K) = d_2(E/K) - 1.$$

Proof. Let $\mathfrak{p}$ be as in Lemma 5.1.2. We will apply Corollary 4.2.4, with $T = \{\mathfrak{p}\}$. Since $\mathfrak{p} \notin \Sigma$, $\mathfrak{p} \nmid 2\infty$ and E has good reduction at $\mathfrak{p}$, it follows from Lemma 3.1.2(ii) that

$$\mathrm{H}^1_f(K_{\mathfrak{p}}, E[2]) \cong E[2]/(\mathrm{Frob}_{\mathfrak{p}} - 1)E[2] = E[2]/(\sigma - 1)E[2].$$

Hence

$$\dim_{\mathbb{F}_2} \mathrm{H}^1_f(K_{\mathfrak{p}}, E[2]) = 1.$$

Further, the following composition of maps, also denoted by

$$loc_T : \mathrm{Sel}_2(E/K) \longrightarrow \mathrm{H}^1_f(K_{\mathfrak{p}}, E) \xrightarrow{\sim} E/(\sigma - 1)E$$

is given by evaluation of cocycle at $\mathrm{Frob}_{\mathfrak{p}} = \gamma$. Hence by our choice of γ, we have

$$loc_T(\mathrm{Sel}_2(E/K)) \;\; = \;\; \phi(\mathrm{Sel}_2(E/K))$$

By corollary 4.2.4(a) with $V_T = \phi(\mathrm{Sel}_2(E/K))$ we have

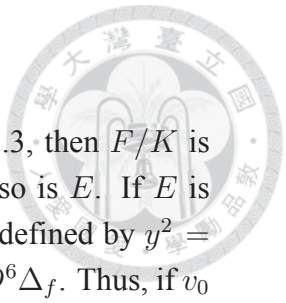
$$d_2(E^F/K) = d_2(E/K) - 2\dim_{\mathbb{F}_2} V_T + \dim_{\mathbb{F}_2} \mathrm{H}^1_f(K_{\mathfrak{p}}, E),$$

and hence

$$d_2(E^F/K) = \begin{cases} d_2(E/K) + 1, & \text{if } \phi(\mathrm{Sel}_2(E/K)) = 0; \\ d_2(E/K) - 1, & \text{if } \phi(\mathrm{Sel}_2(E/K)) \neq 0. \end{cases}$$

We have the freedom to choose ϕ. For the assertion (i), we choose $\phi = 0$. For (ii), since $d_2(E/K) > 0$ we choose a ϕ nonzero on $\mathrm{Sel}_2(E/K)$. □

Theorem 5.1.4. *Suppose E/K satisfies the hypotheses of this section. Then for every $r \geq 0$, E has quadratic twist E'/K with $d_2(E'/K) = r$.*



Proof. If E^F is a twist of E satisfying the condition of Proposition 5.1.3, then F/K is unramified at v_0. Hence E^F also has multiplicative reduction at v_0 if so is E. If E is defined by $y^2 = f(x) = x^3 + Ax + B$ and $F = K(\sqrt{D})$, then E^F is defined by $y^2 = f^D(x) := x^3 + D^2Ax + D^3B$. By direct computation, we have $\Delta_{f^D} = D^6\Delta_f$. Thus, if v_0 is real then $\Delta_{f^D} = D^6\Delta_f < 0$; if $v_0 \nmid 2\infty$ implies $\mathrm{ord}_{v_0}(\Delta_{f^D}) = 6\,\mathrm{ord}_{v_0} D + \mathrm{ord}_{v_0}(\Delta_f)$ is odd.

Lemma 2.3.2 says $E^F[2] = E[2]$ as Galois modules, hence $K(E^F[2]) = M$ and $\mathrm{Gal}(K(E^F[2])/K) \cong S_3$.

The above shows E^F/K also satisfies the hypotheses of this section. Thus, we can repeatedly apply Proposition 5.1.3 to achieve the required rank of Selmer group. If $r \geq d_2(E/K)$, then applying $r - d_2(E/K)$ times Proposition 5.1.3(i) shows that E has a twist E' with $d_2(E/K) = r$; if $0 \leq r \leq d_2(E/K)$, then applying $d_2(E/K) - r$ times Proposition 5.1.3(ii) shows that E has a twist E' with $d_2(E'/K) = r$. □

5.2. **The proof of Theorems 2.**

Proposition 5.2.1. *Suppose E/K is an elliptic curve such that $E(K)[2] = 0$. If $d_2(E/K) > 1$, then E has a quadratic twist E^F over K such that $d_2(E^F/K) = d_2(E/K) - 2$.*

Proof. Let $M := K(E[2])$ as before. Choose the defining $f(x) = x^3 + Ax + B$ such that A, B are algebraic integer. Then Δ_f is also an integer. View $8\Delta\infty$ as the modulus which is the product of 8Δ and all infinite places. Let $K(8\Delta\infty)$ denote the corresponding ray class field of K.

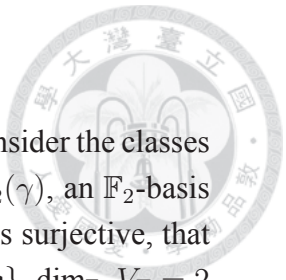
Since $d_2(E/K) > 1$, we can choose c_1, c_2 two $\mathbb{F}_2$-independent elements of $\mathrm{Sel}_2(E/K)$. By Lemma 4.3.2 we can find $\gamma \in G_K$ such that

- $\gamma|_{MK(8\Delta\infty)} = 1$,
- $c_1(\gamma), c_2(\gamma)$ are an $\mathbb{F}_2$-basis of $E[2]$.

As in the proof of Proposition 5.1.3, let N be a Galois extension of K containing $MK(8\Delta\infty)$, large enough so that the restriction of $\mathrm{Sel}_2(E/K)$ to N is zero. Let $\mathfrak{p}$ be a place of K where E has good reduction, not dividing 2, whose Frobenius in $\mathrm{Gal}(N/K)$ is the conjugacy class of γ. Then $\mathfrak{p}$ has a totally positive generator $\pi \equiv 1 \pmod{8\Delta}$. Let $F = K(\sqrt{\pi})$, then all place v dividing $2\Delta\infty$ split in F/K, and $\mathfrak{p}$ is the only prime that ramifies in F/K.

Take $T = \{\mathfrak{p}\}$. Since E has good reduction at $\mathfrak{p}$, it follows from Lemma 3.1.2(ii) that

$$\mathrm{H}^1_f(K_\mathfrak{p}, E[2]) \cong E[2]/(\mathrm{Frob}_\mathfrak{p} - 1)E[2] = E[2]/(\gamma - 1)E[2] = E[2]$$



where the isomorphism is given by evaluating cocycles at $\mathrm{Frob}_{\mathfrak{p}} = \gamma$. Consider the classes $loc_T(c_1)$ and $loc_T(c_2)$ in $\mathrm{H}^1_f(K_{\mathfrak{p}}, E[2])$, they are mapped to $c_1(\gamma)$ and $c_2(\gamma)$, an $\mathbb{F}_2$-basis of $E[2]$. This implies that the map $loc_T : \mathrm{Sel}_2(E/K) \to \mathrm{H}^1_f(K_{\mathfrak{p}}, E[2])$ is surjective, that is $\dim_{\mathbb{F}_2} \mathrm{H}^1_f(K_{\mathfrak{p}}, E[2])/V_T = 0$. Applying Corollary 4.2.4(i) with $T = \{\mathfrak{p}\}$, $\dim_{\mathbb{F}_2} V_T = 2$ and $\dim_{\mathbb{F}_2} \mathrm{H}^1_f(K_{\mathfrak{p}}, E[2]) = 2$, we have

$$\begin{aligned} d_2(E^F/K) &= d_2(E/K) - 2\dim_{\mathbb{F}_2} V_T + \dim_{\mathbb{F}_2} \mathrm{H}^1_f(K_{\mathfrak{p}}, E[2]) \\ &= d_2(E/K) - 2 \end{aligned}$$

as desired. □

Theorem 5.2.2. *Suppose K is a number field, and E is an elliptic curve over K such that $E(K)[2] = 0$. If $0 \le r \le d_2(E/K)$ and $r \equiv d_2(E/K) \pmod 2$, then E has quadratic twist E'/K such that $d_2(E'/K) = r$.*

Proof. Similar to the proof of Theorem 5.1.4, we we may inductively apply Proposition 5.2.1 if the $\mathbb{F}_2$-dimension of twisted Selmer group greater than 1. Now, since $0 \le r \le d_2(E/K)$, applying $(d_2(E/K) - r)/2$ times Proposition 5.2.1 shows that E has a twist E' with $d_2(E'/K) = r$. □

5.2.1. *Elliptic curve with constant 2-Selmer parity.* We say that E is an elliptic curve with constant 2-Selmer parity, if all $d_2(E^F/K)$ has the same parity.

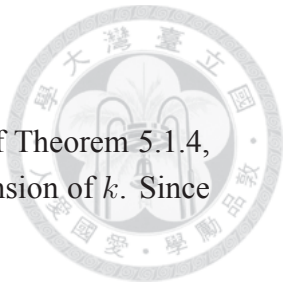
Corollary 5.2.3. *Suppose K is a number field, and E is an elliptic curve over K with constant 2-Selmer parity such that $\mathrm{Gal}(K(E[2])/K) \cong S_3$. Let $j(E)$ be the j-invariant of E, and suppose further that $j(E) \neq 0$ and K has an archimedean place v such that $(j(E))_v \in \mathbb{R}$ and $(j(E))_v < 1728$. Then for every $r \equiv d_2(E/K) \pmod 2$, E has quadratic twists E'/K such that $d_2(E'/K) = r$.*

Proof. Let $k = \mathbb{Q}(j(E)) \subset K$. Then there exists an elliptic E_0 defined over k with j-invariant $j(E_0) = j(E)$. But E_0 and E have the same j-invariant implies they are isomorphic over $\bar{K}$, or more precisely, some finite extension F of K. Since $\mathrm{Gal}(K(E[2])/K) \cong S_3$, $j(E) \neq 0, 1728$. Hence E_0 is a quadratic twist of E over K, and $K(E_0[2]) = K(E[2])$. From this, we see that

$$[k(E_0[2]) : k] \ge [K(E_0[2]) : K] = [K(E[2]) : K],$$

and hence $\mathrm{Gal}(k(E_0[2])/k) \cong S_3$. Also, if E_0 is defined by $y^2 = f_0(x)$, then

$$j(E) - 1728 = j(E_0) - 1728 = c_6(E_0)^2/\Delta_{f_0}.$$



Thus, $\Delta_{f_0} < 0$ in $k_v \subset K_v$. Therefore E_0/k satisfies the hypotheses of Theorem 5.1.4, and $d_2(E_0^F/k)$ can be arbitrary large as F varies through quadratic extension of k. Since $E^F(K)[2] = E(K)[2] = 0$, $\mathrm{H}^1(K/k, E^F(K)[2]) = 0$ and we have

$$\text{Res}: \ \mathrm{H}^1(k, E^F[2]) \hookrightarrow \mathrm{H}^1(K, E^F[2]) \ .$$

This means $\mathrm{Sel}_2(E_0^F/k) \xrightarrow{\text{Res}} \mathrm{Sel}_2(E_0^F/K)$ is injective, and so $d_2(E^F/K)$ can be arbitrarily large as F varies through quadratic extensions of K. This corollary follows from Theorem 5.2.2. □

References

[1] Mazur B.,Rubin K.:Ranks of twists of elliptic curves and Hilbert's tenth problem. Invent. Math. 181 (2010), 541-575.

[2] Silverman J.H.: The Arithmetic of Elliptic Curves, Springer GTM 106, 1986

[3] Silverman J.H.: Advanced Topics in the Arithmetic of Elliptic Curves, Springer GTM 151, 1994

[4] Lang S.: Algebraic groups over finite fields. Amer.J.Math.78(1956),555-563

[5] Kramer,K.:Arithmetic of elliptic curves upon quadratic extension, Trans.Am.Math.Soc,264, 121-135(1981)

[6] Tate, J.:Duality theorems in Galois cohomology over number fields. In: Proc. Intern. Congr. Math., Stockholm, pp.234-241(1962)

[7] Cassels, J.W.S.: Arithmetic on curves of genus 1. VII. On conjectures of Birch and Swinnerton-Dyer. J. Reine Angew. Math. 217, 180-199(1965)

[8] Rubin, K.: Euler Systems. Annals of Math. Studies, vol. 147. Princeton University Press, Princetion (2000)

[9] Milne, J.S.: Class Field Theory (v4.02). 2013, Available at www.jmilne.org/math/

[10] Milne, J.S.: Arithmetic Duality Theorems. Perspectives in Math., vol. 1. Academic Press, San Diego (1986)