IDEMPOTENT RELATIONS AND THE CONJECTURE OF BIRCH AND SWINNERTON-DYER

DISSERTATION

Presented in Partial Fulfillment of the Requirements for
the Degree Doctor of Philosophy in the Graduate
School of the Ohio State University

By

Hoseog Yu, M.S.

* * * * *

The Ohio State University
1999

Dissertation Commitee:

Professor Karl Rubin, Adviser

Professor Warren Sinnott

Professor David Goss

Approved by

Karl C Rubin

Adviser
Department of Mathematics

UMI Number: 9931706

ABSTRACT

Let A be an abelian variety defined over a number field K and let L be a finite Galois extension of K with Galois group G. Let $\mathrm{End}_L(A)[G]$ be the twisted group ring with multiplication defined by

$$(\sum_\sigma p_\sigma \sigma)(\sum_\tau q_\tau \tau) = \sum_{\sigma,\tau} (p_\sigma q_\tau^\sigma)\sigma\tau$$

for $p_\sigma, q_\tau \in \mathrm{End}_L(A)$ and $\sigma, \tau \in G$.

Write $Z^1(H, \mathrm{Aut}_L(A))$ for the group of 1-cocycles from a subgroup H of G to $\mathrm{Aut}_L(A)$. If $\chi \in Z^1(H, \mathrm{Aut}_L(A))$, define an idempotent $\epsilon(\chi) \in \mathrm{End}_L(A)[G] \otimes \mathbf{Q}$ by $\epsilon(\chi) = |H|^{-1} \sum_{\sigma \in H} \chi(\sigma)\sigma$. We will write A^χ for the twist of A by the element in $\mathrm{H}^1(Gal(\overline{L}/L^H), \mathrm{Aut}(A))$ induced by χ.

There is an L-function $L(A/K, s)$ attached to A, defined by an Euler product for $Re(s)$ large, which is conjectured to have an analytic continuation to all of $\mathbf{C}$. Assuming this analytic continuation we can write $L(A/K, s) \sim c(s-1)^r$ as $s \to 1$. There is a well-known conjecture for the order of vanishing r and the coefficient c.

Conjecture (Birch and Swinnerton-Dyer).

(1) the order of vanishing r is equal to the rank of $A(K)$

(2) the coefficient c is equal to a constant $C(A/K)$ defined explicitly in terms of the Tate-Shafarevich group $Ш(A/K)$, the regulator, the periods and Tamagawa factors of A.

Proposition. *If* $\sum_i n_i \epsilon(\chi_i) = 0$ *is an idempotent relation with* $n_i \in \mathbf{Z}$, *then* $\sum_i n_i rank_{\mathbf{Z}}(A^{\chi_i}(L^{H_i})) = 0$ *and*

$$\prod_i L(A^{\chi_i}/L^{H_i}, s)^{n_i} = 1.$$

Main Theorem. *Assume that the Tate-Shafarevich groups are finite and there is an idempotent relation* $\sum_i n_i \epsilon(\chi_i) = 0$. *Then*

$$\prod_i C(A^{\chi_i}/L^{H_i})^{n_i} = 1.$$

To my mother

ACKNOWLEDGMENTS

My sincere gratitude goes to my advisor, Dr. Karl Rubin. I was fortunate to have him as my advisor. Having the opportunity to study under his supervision was a watershed experience in my life. Throughout my graduate work, his intelligence and knowledge always inspired me to further growth. His invaluable suggestions and comments enabled me to complete this work. There is no way for me to thank him enough.

My appreciation is also extended to Dr. Sinnott and Dr. Goss for their interest in my work and support. Their lectures helped me expand my perspectives in Number Theory. Their warm presence and kindness will be cherished forever.

I am also grateful to Dr. Myunghwan Kim at Seoul National University for introducing me to the area of number theory and encouraging me to study further abroad. I would like to thank all my friends for their encouragement and prayer throughout the years.

My gratitude is also extended to my family, especially to my mother, for her enduring love and encouragement. Her patience and faith in me provided me a deeply felt motivation to finish this work. I thank my brother and sister for their support, and understanding, and for taking responsibility for the family in my place.

VITA

October 9, 1966	Born in Yeoju, Korea
1989	B. Sc., Mathematics Seoul National University, Seoul, Korea
1991	M. Sc., Mathematics Seoul National University, Seoul, Korea
1992 – Present	Graduate Teaching Associate, Department of Mathematics, The Ohio State University, Columbus, Ohio.

FIELDS OF STUDY

Major field: Mathematics

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

Let A be an abelian variety defined over a number field K. Birch and Swinnerton–Dyer developed a conjecture which connects the order of vanishing and the leading coefficient of the Taylor expansion for the L–function $L(A/K, s)$ at $s = 1$ with several algebraic invariants of the abelian variety A: the rank of the Mordell–Weil group $A(K)$, the regulator $R(A/K)$, the order of the Shafarevich–Tate group $Ш(A/K)$, and the Tamagawa number $\tau(A/K)$ (see pp. 9–10 for the definitions of these invariants).

Conjecture (Birch and Swinnerton–Dyer). *Assume the L-function $L(A/K, s)$ has an analytic continuation around $s = 1$ and the Shafarevich–Tate group $Ш(A/K)$ is finite. Write the Taylor expansion of $L(A/K, s)$ at $s = 1$:*

$$L(A/K, s) = c(A/K)(s-1)^{r(A/K)} + O((s-1)^{r(A/K)+1}).$$

Then

(a) the order of vanishing $r(A/K) = \mathrm{rank}_{\mathbf{Z}}(A(K))$ and

(b) the leading coefficient $c(A/K) = C(A/K)$,

where $C(A/K) = R(A/K)\cdot \#\text{Ш}(A/K)\cdot \tau(A/K)$, *called the constant of Birch and Swinnerton–Dyer.*

Tate [45, p.198] has mentioned that "this remarkable conjecture relates the behavior of a function L at a point where it is not at present known to be defined to the order of a group Ш which is not known to be finite!"

Kolyvagin [16] proved that if an abelian $A/\mathbf{Q}$ is a modular elliptic curve, and $L(A/\mathbf{Q}, 1) \neq 0$, then $\text{Ш}(A/\mathbf{Q})$ is finite (see also [29]).

Let L be a finite Galois extension of K with Galois group $G = Gal(L/K)$. Kani and Rosen [14] developed a relation among L–functions.

Theorem (Kani–Rosen [14]). *Define* $\varepsilon_H = |H|^{-1}\sum_{h\in H} h$ *for a subgroup* H *of* G. *If* $\sum_H n_H\varepsilon_H = 0$ *in* $\mathbf{Q}[G]$, *then* $\sum_H n_H \operatorname{rank}_{\mathbf{Z}}(A(L^H)) = 0$ *and*

$$(*) \qquad \prod_H L(A/L^H, s)^{n_H} = 1.$$

Park [25] developed a new conjecture by combining the above theorem and the conjecture of Birch and Swinnerton–Dyer.

Conjecture (Park [25]). *Suppose that the Shafarevich–Tate groups are finite. If* $\sum_H n_H\varepsilon_H = 0$, *then*

$$\prod_H C(A/L^H)^{n_H} = 1.$$

Note that this would be a consequence of $(*)$ if we knew that the conjecture of Birch and Swinnerton–Dyer were true. Park [25] also proved weaker form of this conjecture.

In this dissertation we prove Park's Conjecture, and even a generalization of it. We state the general version, the Main Theorem, at the beginning of Chapter 6.

The following is a brief outline for the proof of Park's Conjecture.

First, we define a map $\Upsilon : \mathrm{End}_L(A)[G] \longrightarrow \mathrm{End}_K(Res_{L/K}(A))$ (see Definition 4.12 p. 26), where $Res_{L/K}(A)$ is the restriction of scalars of A from L down to K (see Section 4.2 for the definition).

We can rewrite the given relation $\sum_H n_H \varepsilon_H = 0$ as, with $n_H,\ m_H > 0$,

$$\sum_H n_H \varepsilon_H = \sum_H m_H \varepsilon_H.$$

By applying Υ to the above equation, we derive

$$\sum_H n_H \Upsilon(\varepsilon_H) = \sum_H m_H \Upsilon(\varepsilon_H) \quad \text{in} \quad \mathrm{End}_K(Res_{L/K}(A)) \otimes \mathbf{Q}.$$

Then, by using Theorem 5.1, which was proved by Kani and Rosen [13], there exists an isogeny:

$$\prod_H \left(\Upsilon(\varepsilon_H)(Res_{L/K}(A))\right)^{n_H} \sim \prod_H \left(\Upsilon(\varepsilon_H)(Res_{L/K}(A))\right)^{m_H}.$$

Theorem 4.19 shows that $\Upsilon(\varepsilon_H)(Res_{L/K}(A)) \sim Res_{L^H/K}(A)$, so we get

$$\prod_H \left(Res_{L^H/K}(A)\right)^{n_H} \sim \prod_H \left(Res_{L^H/K}(A)\right)^{m_H}.$$

Since the constant of Birch and Swinnerton–Dyer is an isogeny invariant (see Theorem 5.2),

$$\prod_H C(Res_{L^H/K}(A)/K)^{n_H} = \prod_H C(Res_{L^H/K}(A)/K)^{m_H}.$$

A theorem of Milne (Theorem 5.3) shows that $C(A/L^H) = C(Res_{L^H/K}(A)/K)$, and Park's Conjecture follows.

In Chapter 2 we introduce the conjecture of Birch and Swinnerton–Dyer. In order to state the conjecture, we set the notation, define the objects involved and some of their properties.

Chapter 3 presents the definition of idempotent relation the conjecture of Park.

In Chapter 4 we define twists and restriction of scalars. Then we show that the abelian varieties $\left(\sum_{\sigma\in H} \widetilde{\chi(\sigma)} \circ \phi_\sigma\right)(Res_{L/K}(A))$ and $Res_{L^H/K}(A^\chi)$ are isogeneous (see Theorem 4.22). This isogeny will play a major role in the proof of the Main Theorem.

Chapter 5 states theorems of Kani–Rosen, Milne, and Tate. These theorems will be used to prove the Main Theorem.

In Chapter 6 we state the Main Theorem and prove it. Then, some corollaries will be presented.

In Chapter 7 the individual factors of the Birch and Swinnerton–Dyer constant are investigated.

CHAPTER 2

BIRCH AND SWINNERTON–DYER CONJECTURE

Let A be an abelian variety of dimension g defined over a number field K. Let v be a finite place of K and Nv be the cardinality of the residue field k_v. Let G_v be a decomposition group for v in $G_K = \mathrm{Gal}(\overline{K}/K)$. Let I_v be the inertia subgroup of G_v and let σ_v denote an arithmetic Frobenius which generates the quotient G_v/I_v. Let ℓ be a rational prime distinct from $\mathrm{char}(k_v)$. The ℓ^n–torsion subgroup of A, denoted $A(\overline{K})_{\ell^n}$, is the set of points of order ℓ^n in $A(\overline{K})$,

$$A(\overline{K})_{\ell^n} = \{P \in A(\overline{K}) \mid \ell^n P = 0\}.$$

The ℓ–adic Tate module of A is the group

$$T_\ell(A) = \varprojlim_n A(\overline{K})_{\ell^n},$$

the inverse limit being taken with respect to the natural maps

$$A(\overline{K})_{\ell^{n+1}} \xrightarrow{[\ell]} A(\overline{K})_{\ell^n}.$$

Note that the action of G_K on each $A(\overline{K})_{\ell^n}$ commutes with the multiplication by $[\ell]$ maps, which are used to form the inverse limit, so G_K also acts on $T_\ell(A)$. Further, since the profinite group G_K acts continuously on each finite (discrete) group $A(\overline{K})_{\ell^n}$, the resulting action on $T_\ell(A)$ is also continuous. See [9], [24], or [32] for more detail.

Proposition 2.1. *This ℓ–adic Tate module $T_\ell(A)$ is a free $\mathbf{Z}_\ell$-module of rank $2g$ which admits a continuous $\mathbf{Z}_\ell$–linear action of G_K.*

Proof. See [24] or [32]. □

We define the local L–factor of A at v by the formula:

$$L_v(A,t) = \det(1 - \sigma_v^{-1} t | \operatorname{Hom}_{\mathbf{Z}_\ell}(T_\ell(A), \mathbf{Z}_\ell)^{I_v}).$$

The characteristic polynomial $L_v(A,t)$ has integral coefficients which are independent of ℓ (see [31] and [49]).

The global L–function of A/K is defined by the formal Euler product

$$L(A,s) = L(A/K,s) = \prod_{v \text{ finite}} L_v(A, Nv^{-s})^{-1}.$$

Note that the global L–function is an isogeny invariant, i.e., if two abelian varieties A and A' are isogeneous over K, then $L(A,s) = L(A',s)$, because $L_v(A,t) = L_v(A',t)$ for every finite place v.

Let S be a finite set of places of K containing the archimedean places and large enough so that A has good reduction outside S. For each place $v \notin S$, let A_v be the Néron minimal model. Define the abelian variety $\widetilde{A}_v$ over the residue field k_v by $\widetilde{A}_v = A_v \otimes_{\mathcal{O}_v} k_v$, where $\mathcal{O}_v$ is the valuation ring of v (see [32]).

According to well known results of Weil [49],

$$L_v(A,t) = \prod_{i=1}^{2g}(1-\alpha_{i,v}t) = (Nv)^g t^{2g} L_v(A, Nv/t),$$

and $L_v(A,t)$ is a polynomial of degree $2g$, with coefficients in $\mathbf{Z}$, and with complex "reciprocal roots" $\alpha_{i,v}$ of absolute value $\sqrt{Nv}$. These roots $\alpha_{i,v}$, and hence $L_v(A,t)$, are characterized by the fact that for all $m \geq 1$

$$\prod_{i=1}^{2g}(1-\alpha_{i,v}^m) = \begin{cases} \text{Number of points of } \widetilde{A}_v \text{ with coordinates in the} \\ \text{extension of degree } m \text{ of the finite field } k_v. \end{cases}$$

Now $L(A,s)$ converges for $Re(s) > 3/2$ because it is dominated by the product for $(\zeta_K(s-\frac{1}{2}))^{2g}$. It is generally conjectured that $L(A,s)$ has an analytic continuation to the entire complex plane.

Conjecture (Hasse–Weil). *The L-function $L(A,s)$ has an analytic continuation to the entire complex plain and satisfies a functional equation relating the values at s and $2-s$.*

We will assume this conjecture in all that follows.

Actually this general conjecture has been verified in some special cases. Let the endomorphism ring $\mathrm{End}(A)$ be the set of all isogenies from A to itself. It is known that $\mathrm{End}(A)$ is a free $\mathbf{Z}$–module of finite rank $\leq 4g$ (see [23, Theorem 12.5] or [24]) and that it contains a submodule, denoted $\mathbf{Z}$, composed of multiplications. If $\mathrm{End}(A)$ contains a field of degree $2g$ over $\mathbf{Q}$, then we say that A has complex multiplication. If A has complex multiplication, then $L(A,s)$ has an analytic continuation and functional equation according to the work of Shimura–Taniyama and Hecke (see [36, p.145] and [39]).

For any positive integer N, let $X_0(N)$ be the compactification on $\mathcal{H}/\Gamma_0(N)$, where $\mathcal{H}$ is the complex upper half-plane and

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z}) \;\middle|\; c \equiv 0 \pmod{N} \right\}.$$

Let E be an elliptic curve, an abelian variety of dimension 1, defined over $\mathbf{Q}$. If there is a non-constant morphism $X_0(N) \longrightarrow E$ of algebraic curves defined over $\mathbf{Q}$, then we call E modular. In 1958, Shimura proved the Hasse–Weil conjecture for modular elliptic curves (see [36, p.145], [34] and [35]).

Conjecture (Taniyama–Shimura). *Every elliptic curve over* $\mathbf{Q}$ *is modular.*

If the conjecture of Taniyama–Shimura is true, then the Hasse–Weil conjecture is also true. Although these two conjectures are still open, thanks to the work of Wiles [50] and Taylor–Wiles [46], we know at least that it is true for a large and important class of elliptic curves, namely, the semistable ones.

Theorem 2.2 (Wiles). *Every semistable elliptic curve over* $\mathbf{Q}$ *is modular.*

This is a key theorem to prove Fermat's last theorem. In fact, by improving Wiles methods, Fred Diamond [7] has proved the much stronger result that every elliptic curve $E/\mathbf{Q}$ that is semistable at 3 and 5 is modular.

Under the assumption of the Hasse–Weil conjecture, we have the Taylor expansion of $L(A, s)$ at $s = 1$:

$$L(A, s) \sim c(A/K)(s-1)^{r(A/K)} \quad \text{as} \quad s \to 1,$$

where $r(A/K)$ is the order of vanishing. Birch and Swinnerton–Dyer conjectured the order of vanishing $r(A/K)$ and the leading coefficient $c(A/K)$ when A is an elliptic curve. Tate formulated the conjecture for abelian varieties (see [44]).

By the Mordell–Weil theorem, $A(K)$, the group of K–rational points of A, is a finitely generated abelian group, i.e.,

$$A(K) = A(K)_{\text{tors}} \oplus \mathbf{Z}^r$$

for some integer $r \geq 0$. We call r the rank of A/K.

Let A' be the dual abelian variety $\operatorname{Pic}^0 A$ over K. Let $\langle\ ,\ \rangle : A(K) \times A'(K) \to \mathbf{R}$ denote the canonical height pairing corresponding to the Poincaré divisor on $A \times A'$. Fix bases $\{x_1, \ldots, x_r\}$ and $\{y_1, \ldots, y_r\}$ for free subgroups $X \subset A(K)$ and $Y \subset A'(K)$ of finite index in the respective grouos of points. Define the regulator:

$$R(A/K) = \frac{|\det((\langle x_i, y_j \rangle))|}{\#(A(K)/X)\#(A'(K)/Y)} \quad .$$

Note that this nonzero real number is independent of the choice of x_i and y_j.

For each place v, we fix an extension of v to $\overline{K}$, which serves to fix an embedding $\overline{K} \subset \overline{K_v}$ and a decomposition group $G_v \subset G_K$. Then G_v acts on $A(\overline{K}_v)$. The natural inclusions $G_v \hookrightarrow G_K$ and $A(\overline{K}) \hookrightarrow A(\overline{K_v})$ give restriction maps on cohomology groups. Therefore, we have a homomorphism $\mathrm{H}^1(G_K, A) \longrightarrow \prod_v \mathrm{H}^1(G_v, A)$.

Define

$$Ш(A/K) = \mathrm{Ker}\left\{ \mathrm{H}^1(G_K, A) \longrightarrow \prod_v \mathrm{H}^1(G_v, A) \right\}$$

which is called the Shafarevich–Tate group of A over K. Note that $Ш(A/K)$ does not depend on the extension of the v's to $\overline{K}$. It depends only on A and K. It is known that $Ш(A/K)$ is a torsion group whose p-primary component $Ш(A/K)(p)$ is of finite corank for each prime p. Another deep conjecture underlying the Birch and Swinnerton–Dyer conjecture is that $Ш(A/K)$ is finite.

Conjecture. *Let A/K be an abelian variety. Then $Ш(A/K)$ is finite.*

In general, (assuming finiteness) we have $\#Ш(A/K) = \#Ш(A'/K)$.

Let ω be a non-zero invariant exterior differential form of degree g on the abelian variety A/K. Define

$$\lambda_v = \begin{cases} 1, & \text{if } v \text{ is archimedian;} \\ \dfrac{(Nv)^g}{n_v}, & \text{if } v \text{ is non-archimedian,} \end{cases}$$

where n_v is the order of $\widetilde{A}_v^\circ(k_v)$, the group of points on the connected component of zero of the reduction of the Néron minimal model of A. By Theorem 2.2.5 [48] the λ_v form a set of convergence factors for A. Let $\mathbb{A}_K$ be the adèle ring of K. We define $\tau(A)$ to be the measure of the adèle group $A(\mathbb{A}_K)$ of A relative to the Tamagawa measure $(\omega, (1))$ [48, p.23]:

$$\tau(A/K) = \int_{A(\mathbb{A}_K)/A(K)} (\omega, (1)).$$

With all these defined terms, the regulator, Shafarevich–Tate group, and Tamagawa number, we are now ready to formulate the conjecture of Birch and Swinnerton–Dyer.

Conjecture (Birch and Swinnerton–Dyer). *Assume the L-function* $L(A/K, s)$ *has an analytic continuation around* $s = 1$ *and the Shafarevich–Tate group* $\text{Ш}(A/K)$ *is finite. Write the Taylor expansion of* $L(A/K, s)$ *at* $s = 1$*:*

$$L(A/K, s) = c(A/K)(s-1)^{r(A/K)} + O((s-1)^{r(A/K)+1}).$$

Then

(a) the order of vanishing $r(A/K) = \mathrm{rank}_{\mathbf{Z}}(A(K))$ *and*

(b) the leading coefficient $c(A/K) = R(A/K) \cdot \#\text{Ш}(A/K) \cdot \tau(A/K)$.

For more details, see [3] for elliptic curves and [44] for abelian varieties.

Notation. Let $C(A/K)$ be the product $R(A/K) \cdot \#\text{Ш}(A/K) \cdot \tau(A/K)$. We call $C(A/K)$ the constant of Birch and Swinnerton–Dyer associated with the abelian variety A/K.

Remark 2.3. The constant $C(A/K)$ is an isogeny invariant. Cassels proved this for elliptic curves provided that Ш is finite. Tate extended that result to abelian varieties. See [6] for elliptic curves and [44] for abelian varieties.

If A is an elliptic curve, we have the following progress toward the Birch and Swinnerton–Dyer conjecture.

Theorem 2.4. *Let E be a modular elliptic curve defined over $\mathbf{Q}$. Suppose that* $\mathrm{order}_{s=1} L(A/\mathbf{Q},1) \leq 1$. *Then* $\mathrm{rank}_{\mathbf{Z}}(E(\mathbf{Q})) = \mathrm{order}_{s=1} L(A/\mathbf{Q},1)$ *and* $\text{Ш}(E/\mathbf{Q})$ *is finite.*

Proof. See [16]. □

Theorem 2.5 (Rubin [29]). *Suppose E is an elliptic curve defined over an imaginary quadratic field K, with complex multiplication by the ring of integers $\mathcal{O}_K$ of K, and with minimal period lattice generated by $\Omega \in \mathbf{C}^\times$. Write $w = \#(\mathcal{O}_K{}^\times)$.*

(1) If $L(E/K,1) \neq 0$ then $E(K)$ is finite, the Shafarevich–Tate group $\text{Ш}(A/K)$ of E is finite and there is a $u \in \mathcal{O}_K[w^{-1}]^\times$ such that

$$\#(\text{Ш}(E/K)) = u\#(E(K))^2 \frac{L(E/K,1)}{\Omega\overline{\Omega}}.$$

In other words, the full Birch and Swinnerton–Dyer conjecture for E is true up to an element of K divisible only by primes dividing $\#(\mathcal{O}_K{}^\times)$.

(2) If $L(E/K,1) = 0$ then either $E(K)$ is infinite or the $\wp$-part of $\text{Ш}(E/K)$ is infinite for all primes $\wp$ of K not dividing $\#(\mathcal{O}_K{}^\times)$.

Theorem 2.6. *For any positive integer d let $E^{(d)}$ denote the elliptic curve $y^2 = x^3 - d^2x$, which has complex multiplication by $\mathbf{Z}[i]$. Suppose p is a prime, $p \equiv 3 \pmod 8$. Then the full Birch and Swinnerton–Dyer conjecture is true for $E^{(p)}/\mathbf{Q}$.*

Proof. See [29]. □

Theorem 2.7 (Gonzalez–Avilés [8]). *Let E be an elliptic curve defined over the field $K = \mathbf{Q}(\sqrt{-7})$, with complex multiplication by the ring of integers of K. Suppose*

$L(E/K, 1) \neq 0$. *Then the full Birch and Swinnerton–Dyer conjecture is true for* E/K.

Theorem 2.8 (Gonzalez–Avilés [8]). *Let* E *be an elliptic curve defined over* $\mathbf{Q}$ *with complex multiplication by the ring of integers of* $\mathbf{Q}(\sqrt{-7})$. *Suppose* $L(E/K, 1) \neq 0$. *Then the full Birch and Swinnerton–Dyer conjecture is true for* $E/\mathbf{Q}$.

Proof. This follows from Theorem 2.7 by Corollary 6.4. □

CHAPTER 3

IDEMPOTENT RELATIONS

3.1 Definition

Let L be a finite Galois extension of K with Galois group G. Let $\mathrm{End}_L(A)$ be the ring of endomorphisms of A defined over L, and let $\mathrm{End}_L(A)[G]$ be the twisted group ring with multiplication defined by

$$(\sum_{\sigma} p_\sigma \sigma)(\sum_{\tau} q_\tau \tau) = \sum_{\sigma,\tau} (p_\sigma q_\tau^\sigma)\sigma\tau$$

for $p_\sigma, q_\tau \in \mathrm{End}_L(A)$ and $\sigma, \tau \in G$.

Let $\mathrm{Aut}_L(A)$ denote the automorphism group of A defined over L, that is, the set of invertible elements in $\mathrm{End}_L(A)$. Write $Z^1(H, \mathrm{Aut}_L(A))$ for the set of 1-cocycles from a subgroup H of G to $\mathrm{Aut}_L(A)$, i.e.,

$$Z^1(H, \mathrm{Aut}_L(A)) = \{\chi : H \to \mathrm{Aut}_L(A) \mid \chi(\sigma\tau) = \chi(\sigma)\chi(\tau)^\sigma\}.$$

If $\chi \in Z^1(H, \mathrm{Aut}_L(A))$, define an element $\varepsilon(\chi) \in \mathrm{End}_L(A)[G] \otimes \mathbf{Q}$ by

$$\varepsilon(\chi) = \frac{1}{|H|} \sum_{\sigma \in H} \chi(\sigma)\sigma.$$

Lemma 3.1. *The element $\varepsilon(\chi)$ is an idempotent in* $\mathrm{End}_L(A)[G] \otimes \mathbf{Q}$.

Proof.

$$\begin{aligned}\varepsilon(\chi)^2 &= \left(\frac{1}{|H|}\sum_{\sigma\in H}\chi(\sigma)\sigma\right)\left(\frac{1}{|H|}\sum_{\tau\in H}\chi(\tau)\tau\right)\\ &= \frac{1}{|H|^2}\sum_{\sigma,\tau\in H}\chi(\sigma)\chi(\tau)^{\sigma}\sigma\tau\\ &= \frac{1}{|H|^2}\sum_{\sigma,\tau\in H}\chi(\sigma\tau)\sigma\tau\\ &= \frac{1}{|H|}\sum_{\sigma\in H}\chi(\sigma)\sigma = \varepsilon(\chi).\end{aligned}$$

□

In particular, for the trivial cocycle $id_H \in Z^1(H, \mathrm{Aut}_L(A))$, we have the idempotent

$$\varepsilon(id_H) = \frac{1}{|H|}\sum_{\sigma\in H}\sigma \in \mathbf{Z}[G]\otimes\mathbf{Q} \subset \mathrm{End}_L(A)[G]\otimes\mathbf{Q}.$$

Definition 3.2. Let $\chi_i \in \coprod_{H\subset G} Z^1(H, \mathrm{Aut}_L(A))$. A relation of the form

$$\sum_i n_i\varepsilon(\chi_i) = 0, \quad n_i \in \mathbf{Q},$$

is called an idempotent relation in $\mathrm{End}_L(A)[G]\otimes\mathbf{Q}$.

Example 3.3. Let $G = \mathbf{Z}/2\mathbf{Z} = \{e, \sigma\}$, where σ is the non–trivial element. There is a non–trivial cocycle $\chi \in Z^1(G, \mathrm{Aut}_L(A))$ defined by $\chi(\sigma) = -1$. Then

$$\varepsilon(\chi) + \varepsilon(id_G) = \varepsilon(id_{\{e\}}).$$

Example 3.4. Let $G = (\mathbf{Z}/p\mathbf{Z})^2$, where p is a prime. Then it has $p+1$ subgroups $H_1, \dots, H_{p+1}$ of order p, and we obtain

$$\sum_{i=1}^{p+1}\varepsilon(id_{H_i}) = p\varepsilon(id_G) + \varepsilon(id_{\{e\}}).$$

Example 3.5. Let $G = (\mathbf{Z}/2\mathbf{Z})^n$ with $n \geq 1$. The automorphism group $\mathrm{Aut}_L(A)$ always has a subgroup $\{\pm 1\}$. Then $\mathrm{Hom}(G, \{\pm 1\})$ is a subset of $Z^1(G, \mathrm{Aut}_L(A))$ and

$$\sum_{f \in \mathrm{Hom}(G,\{\pm 1\})} \varepsilon(f) = \varepsilon(id_{\{e\}}).$$

Example 1 is a special case of Example 3 (when $n = 1$).

3.2 Independent idempotent relations

We consider the number of independent idempotent relations. The results of this section are not needed for the proof of our main result, but help to show how widely applicable that result is.

Define

$$IR(G) = \left\{ \sum_i n_i \chi_i \;\middle|\; \chi_i \in \bigcup_{H \subset G} Z^1(H, \mathrm{Aut}_L(A)) \text{ and } \sum_i n_i \varepsilon(\chi_i) = 0 \right\}.$$

Note that the idempotent relation in Example 2 involves only the idempotents coming from trivial cocycles. We will discuss first the number of independent relations which contain only the idempotents coming from trivial cocycles. See [27] and [13, Section 3]. Define

$$TIR(G) = \left\{ \sum_{H \subset G} n_H id_H \;\middle|\; \sum_{H \subset G} n_H \varepsilon(id_H) = 0 \right\}.$$

Note that $TIR(G)$ is a subspace of $IR(G)$.

Theorem 3.6 (Rehm). *The dimension of $TIR(G)$ is the number of non-cyclic subgroups of G.*

Proof. Let H be a noncyclic subgroup of G. Denote by $\mathcal{L}(H)$ the set of cyclic subgroups of H. For $J \in \mathcal{L}(H)$, define

$$a_J = a_J^H = \sum_{\substack{Z \in \mathcal{L}(H) \\ Z \supset J}} \mu([Z : J]),$$

where μ denotes the Möbius function.

Then a basis of the space $TIR(G)$ is

$$\left\{ |H| id_H - \sum_{J \in \mathcal{L}(H)} a_J |J| id_J \;\middle|\; H \text{ is a noncyclic subgroup of } G. \right\}.$$

For details see [27] and [13]. □

Remark 3.7. Wolfgang Happle in his Ph.D. thesis [10] has shown that a group G has a non-trivial idempotent relation $\sum_H n_H \varepsilon(id_H) = 0$ with $n_{\{e\}} \neq 0$, if and only if there is a subgroup of order pq, $p \leq q$ primes, which is not cyclic.

We will study another subspace of $IR(G)$ which contains $TIR(G)$. Let B be a finite commutative subgroup of $\mathrm{Aut}_L(A)$ which is stable under G. Define

$$IR_B(G) = \left\{ \sum_i n_i \chi_i \in IR(G) \;\middle|\; \bigcup_i \chi_i(H_i) \subset B \right\}.$$

Note that $TIR(G) = IR_{\{1\}}(G)$, where 1 denotes the identity automorphism.

Lemma 3.8. *If A is simple, then B is cyclic.*

Proof. Since A is simple, $\mathrm{End}(A) \otimes \mathbf{Q}$ is a division ring (see [17] or [24]). Since B is a commutative subgroup of $\mathrm{Aut}_L(A)$, $\mathbf{Q}[B]$ is a subfield of $\mathrm{End}(A) \otimes \mathbf{Q}$. So B is a finite subgroup of the multiplicative group of the field $\mathbf{Q}[B]$. Thus B is cyclic. □

For a cyclic subgroup H of G, define

$$\mathcal{U}_B(H) = \{\chi(\sigma) \in B \mid \chi \in Z^1(H, B),\ \sigma \in H\}.$$

Note that $\mathcal{U}_B(H)$ is a subgroup of B.

Theorem 3.9. *Suppose that A is simple, and B is a finite commutative subgroup of $\mathrm{Aut}_L(A)$ which is stable under G. Then the dimension of $IR_B(G)$ is*

$$\sum_{H \subset G} \#Z^1(H, B) - \sum_{\substack{H \subset G \\ H \text{ cyclic}}} \varphi(\#\mathcal{U}_B(H)),$$

where φ is the Euler function.

Proof. Let $\varpi : \mathbf{Q}[\coprod_{H \subset G} Z^1(H, B)] \longrightarrow \mathrm{End}_L(A)[G] \otimes \mathbf{Q}$ be the map defined by

$$\varpi(\sum_i n_i \chi_i) = \sum_i n_i \varepsilon(\chi_i).$$

Then $IR_B(G) = \ker(\varpi)$. Now we will compute the dimension of image(ϖ).

Suppose H is not cyclic. By using the idea of Rehm in the proof of Theorem 3.6, for $\chi \in Z^1(H, B)$ we have the following equality:

$$|H|\varepsilon(\chi) = \sum_{J \in \mathcal{L}(H)} a_J |J| \varepsilon(\chi|_J).$$

Thus image(ϖ) is generated by the set $\mathcal{S} = \{\varepsilon(\chi) \mid \chi \in Z^1(H, B)$ and H is cyclic.$\}$.

Assume H is cyclic. Because B is cyclic, the subgroup $\mathcal{U}_B(H)$ is cyclic. Then $\mathbf{Q}[\mathcal{U}_B(H)]$ is an extension field over $\mathbf{Q}$ of dimension $\varphi(\#\mathcal{U}_B(H))$. Actually $\mathbf{Q}[\mathcal{U}(H)] \cong$

$\mathbf{Q}[\zeta]$, where ζ is a primitive $\#\mathcal{U}_B(H)$–th root of unity. Through this isomorphism, $\mathcal{U}_B(H)$ can be identified as $\{1, \zeta, \ldots, \zeta^{\#\mathcal{U}_B(H)-1}\}$. Then $\{1, \zeta, \ldots, \zeta^{\varphi(\#\mathcal{U}_B(H))-1}\}$ is a basis for $\mathbf{Q}[\mathcal{U}_B(H)]$. Define

$$\mathcal{S}_H = \{\chi \in Z^1(H, B) \mid \chi(\sigma) = \zeta^i \text{ for } 1 \leq i \leq \varphi(\#\mathcal{U}_B(H)) - 1\},$$

where σ is a fixed generator of H.

Suppose we have a 1–cocycle $\nu \in Z^1(H, B)$ such that $\nu \notin \mathcal{S}_H$. Then $\nu(\sigma) = \sum_{i=0}^{\varphi(\#\mathcal{U}_B(H))-1} n_i \zeta^i$, with $n_i \in \mathbf{Z}$, that is, $\nu(\sigma) = \sum_{\chi \in \mathcal{S}_H} n_\chi \chi(\sigma)$. Then for another generator $\sigma' \in H$, $\nu(\sigma') = \sum_{\chi \in \mathcal{S}_H}, n_\chi \chi(\sigma')$ because all primitive $\#\mathcal{U}_B(H)$–th roots of unity are Galois–conjugate. Therefore,

$$|H|\varepsilon(\nu) = \sum_{\chi \in \mathcal{S}_H} n_\chi |H| \varepsilon(\chi) + \sum_{\tau \notin Gen(H)} \left(\nu(\tau) - \sum_{\chi \in \mathcal{S}_H} n_\chi \chi(\tau) \right) \tau,$$

where $Gen(H) = \{\text{generators of } H\}$. Now, from simple computation, we have

$$\sum_{\tau \notin Gen(H)} \left(\nu(\tau) - \sum_{\chi \in \mathcal{S}_H} n_\chi \chi(\tau) \right) \tau = \sum_{J \subsetneq H} a_J |J| \left(\varepsilon(\nu|_J) - \sum_{\chi \in \mathcal{S}_H} n_\chi \varepsilon(\chi|_J) \right),$$

where $a_J = \displaystyle\sum_{J \subset Z \subsetneq H} \mu([Z : J])$ with the Möbius function μ. So

$$\varepsilon(\nu) \in \mathbf{Q} \left[\varepsilon(\mathcal{S}_H) \bigcup \left(\bigcup_{J \subsetneq H} \varepsilon(Z^1(J, B)) \right) \right].$$

By induction, image(ϖ) is generated by the set $\displaystyle\bigcup_{H \text{ cyclic}} \varepsilon(\mathcal{S}_H)$.

Now we only have to show that this set is linearly independent to finish the proof of this theorem. Suppose

$$\sum_{H \text{ cyclic}} \sum_{\chi \in \mathcal{S}_H} n_\chi \varepsilon(\chi) = 0.$$

Choose H_0 to be a maximal cyclic subgroup of G such that $n_\chi \neq 0$ for some $\chi \in \mathcal{S}_{H_0}$. Thus for a cyclic subgroup H of G which strictly contains H_0, $n_\chi = 0$ for $\chi \in \mathcal{S}_H$. Fix a generator $\sigma \in H_0$. Then $\sum_{\chi \in \mathcal{S}_{H_0}} n_\chi \chi(\sigma) = 0$. Therefore, $n_\chi = 0$ for $\chi \in \mathcal{S}_{H_0}$ because the set $\{\chi(\sigma) \mid \chi \in \mathcal{S}_{H_0}\}$ is linearly independent in $\mathbf{Q}[\mathcal{U}_B(H_0)]$ and thus in $\mathrm{End}(A) \otimes \mathbf{Q}$. This contradicts to the assumption on H_0. So $\bigcup\limits_{H \text{ cyclic}} \varepsilon(\mathcal{S}_H)$ is a basis of image(ϖ), and the proof of the theorem is complete. □

Corollary 3.10. *Suppose that A is simple, and B is a finite commutative subgroup of $\mathrm{Aut}_K(A)$. Then the dimension of $IR_B(G)$ is*

$$\sum_{H \subset G} \#\,\mathrm{Hom}(H, B) - \sum_{\substack{H \subset G \\ H \text{ cyclic}}} \varphi(gcd(\#H, \#B)),$$

where φ is the Euler function and gcd means the positive greatest common divisor.

Proof. Because G acts trivially on $\mathrm{Aut}_K(A)$, $Z^1(H, B) = \mathrm{Hom}(H, B)$. It is obvious that $\#\mathcal{U}_B(H) = gcd(\#H, \#B)$. □

3.3 Conjecture of Park

Theorem 3.11 (Kani-Rosen). *Suppose that $\sum_H n_H \varepsilon(id_H) = 0$ in $\mathrm{End}_L(A)[G] \otimes \mathbf{Q}$ with $n_H \in \mathbf{Z}$. Then $\sum_H n_H \operatorname{rank}_{\mathbf{Z}}(A(L^H)) = 0$ and*

$$\prod_H L(A/L^H, s)^{n_H} = 1.$$

Proof. See [14]. □

By combining this theorem and the conjecture of Birch and Swinnerton–Dyer, Park made the following conjecture.

Conjecture (Park [25]). *Let E be an elliptic curve defined over K. Assume that the Shafarevich–Tate groups are finite. Given $\sum_H n_H \varepsilon(id_H) = 0$, then*

$$\prod_H C(E/L^H)^{n_H} = 1.$$

We will prove more general form of this conjecture by using the restriction of scalars. For the elliptic curves, Park proved weaker form of this conjecture by looking at each factor of the Birch and Swinnerton–Dyer constant (see Theorems 5.10 and 6.11 [25]).

CHAPTER 4

RESTRICTION OF SCALARS

4.1 Twist

Definition 4.1. Let A be an abelian variety defined over a number field K. A twist of A is an abelian variety A' defined over K which is isomorphic to A over $\overline{K}$. We generally identify two twists if they are isomorphic over K. The set of twists of A/K, modulo K–isomorphism, is denoted $Twist(A/K)$.

Note that Silverman [33] used the notation $Twist((E, 0)/K)$ for the set of twists of an elliptic curve E defined over K.

Now let A' be a twist of A/K. There exists an isomorphism $\alpha : A' \longrightarrow A$ defined over $\overline{K}$ with $\alpha(0) = 0$. Consider the map

$$\xi : G_K \to \mathrm{Aut}(A) \text{ defined by } \xi(\sigma) = \alpha \circ \alpha^{-\sigma}.$$

It turns out that ξ is a 1–cocycle, that is, it satisfies the equality

$$\xi(\sigma\tau) = \xi(\sigma)\xi(\tau)^{\sigma}.$$

The cohomology class of ξ is uniquely determined by the K–isomorphism class of A'. Further, every cohomology class in $\mathrm{H}^1(G_K, \mathrm{Aut}(A))$ comes from some twist of A/K. In this way, $Twist(A/K)$ may be identified with $\mathrm{H}^1(G_K, \mathrm{Aut}(A))$.

Definition 4.2. Let L be a finite Galois extension of the number field K. Define $Twist_L(A/K)$ to be the set of twists of A which are isomorphic to A over L, modulo K–isomorphism, that is,

$$Twist_L(A/K) = \{ \text{ abelian variety } A'/K \mid A' \text{ is isomorpic to } A \text{ over } L\}/\sim,$$

where $\sim$ means the equivalence relation defined by K–isomorphism.

Lemma 4.3. *Through the identification between* $Twist(A/K)$ *and* $\mathrm{H}^1(G_K, \mathrm{Aut}(A))$, $Twist_L(A/K)$ *can be identified with* $\mathrm{H}^1(G_{L/K}, \mathrm{Aut}_L(A))$.

Proof. See [15]. □

Remark 4.4. From the above lemma, we have the following diagram.

$$\begin{array}{ccccc}
Twist_L(A/K) & \xrightarrow{\mathcal{I}_{\mathcal{NF}}} & Twist(A/K) & \xrightarrow{\mathcal{R}_{\mathcal{ES}}} & Twist(A/L) \\
\| & & \| & & \| \\
\mathrm{H}^1(G_{L/K}, \mathrm{Aut}_L(A)) & \xrightarrow{\mathcal{I}_{\mathcal{NF}}} & \mathrm{H}^1(G_K, \mathrm{Aut}(A)) & \xrightarrow{\mathcal{R}_{\mathcal{ES}}} & \mathrm{H}^1(G_L, \mathrm{Aut}(A))
\end{array}$$

The maps in the first row can be defined naturally. In general, $\mathrm{Aut}(A)$ is not an abelian group, so the objects in the bottom row are just pointed sets and the arrows in the bottom row are not homomorphisms. But we can still show that the map $\mathcal{I}_{\mathcal{NF}}$ is injective and that $\mathcal{I}_{\mathcal{NF}}(Twist_L(A/K)) = \mathcal{R}_{\mathcal{ES}}{}^{-1}([A/L])$, where $[A/L]$ is the distinguished element in the pointed set $Twist(A/L) = \mathrm{H}^1(G_L, \mathrm{Aut}(A))$.

4.2 Restriction of scalars

Let L/K be a separable algebraic extension of degree d. Let V, W be varieties defined over L, K respectively. Let $\phi : W \to V$ be a map defined over L. Let $\Sigma = \{\sigma_1, \ldots, \sigma_d\}$ be the set of all distinct isomorphisms of L into $\overline{K}$. We can then define $\phi^\sigma : W \to V^\sigma$, and also

$$(\phi^{\sigma_1}, \ldots, \phi^{\sigma_d}) : W \to V^{\sigma_1} \times \cdots \times V^{\sigma_d}$$

this being the mapping $w \to (\phi^\sigma(w))_{\sigma\in\Sigma}$. If the latter map gives an isomorphism, we call W (actually the pair $\{W, \phi\}$) the variety obtained from V by the restriction of scalars from L to K and write $\{W, \phi\} = Res_{L/K}(V)$, or, by abuse of language, $W = Res_{L/K}(V)$. For more detail, see [48, page 5].

Theorem 4.5 (Existence). *Let A be an abelian variety defined over L. If L/K is a separable field extension, there exists a restriction of scalars of A from L to K, which is also an abelian variety.*

Proof. See [48] and [21]. □

Theorem 4.6 (Universal Mapping Property). *Let A be an abelian variety defined over L. Suppose L/K is a separable field extension. Let X be an abelian variety defined over K, and let $f : X \to A$ be defined over L. Then there is a unique $\mathcal{F} : X \to \{Res_{L/K}(A), \phi\}$ defined over K such that $f = \phi \circ \mathcal{F}$.*

Proof. See [48]. □

Note that from the universal mapping property, a restriction of scalars $Res_{L/K}(A)$ of A from L to K is uniquely determined up to K-isomorphism.

Lemma 4.7. *Let $\{Res_{L/K}(A), \phi\}$ be the restriction of scalars. Define a map*

$$\mathcal{T} : \mathrm{End}_L(Res_{L/K}(A)) \longrightarrow \mathrm{Hom}(Res_{L/K}(A), A)$$

by $\mathcal{T}(\mathcal{F}) = \phi \circ \mathcal{F}$ for $\mathcal{F} \in \mathrm{End}_L(Res_{L/K}(A))$. Then $\mathcal{T}$ is injective.

Proof. Let $\mathcal{F}$ be a homomorphism in $\mathrm{End}_L(Res_{L/K}(A))$ such that $\phi \circ \mathcal{F} = 0$. But $\phi \circ 0 = 0$. So by the universal mapping property, $\mathcal{F} = 0$. □

Remark 4.8. If $f \circ \phi = 0$ for $f \in \mathrm{End}_L(A)$, then $f = 0$. This follows from the surjectivity of the map ϕ.

Definition 4.9. For any $f \in \mathrm{End}_L(A)$, $f \circ \phi \in \mathrm{Hom}_L(Res_{L/K}(A), A)$. From the universal mapping property, there is a unique $\mathcal{F} \in \mathrm{End}_K(Res_{L/K}(A))$ such that $\phi \circ \mathcal{F} = f \circ \phi$. Denote this map $\mathcal{F}$ by $\widetilde{f}$.

From now on, we will assume that A **is an abelian variety defined over** K.

Definition 4.10. For each $\sigma \in G$, $\phi^\sigma \in \mathrm{Hom}_L(Res_{L/K}(A), A)$ because the abelian variety A is defined over K. From the universal mapping property, there is a unique $\mathcal{F} \in \mathrm{End}_K(Res_{L/K}(A))$ such that $\phi \circ \mathcal{F} = \phi^\sigma$. Denote this map $\mathcal{F}$ by ϕ_σ.

Lemma 4.11. *The map from $\mathrm{End}_L(A)$ to $\mathrm{End}_K(Res_{L/K}(A))$ defined by $f \mapsto \widetilde{f}$ is a homomorphism, that is, $\widetilde{f \circ g} = \widetilde{f} \circ \widetilde{g}$, and the map from G to $\mathrm{End}_K(Res_{L/K}(A))$ defined by $\sigma \mapsto \phi_\sigma$ is a homomorphism, i.e., $\phi_{\sigma\tau} = \phi_\sigma \circ \phi_\tau$.*

Proof.

$$\phi \circ \widetilde{f \circ g} = f \circ g \circ \phi = f \circ \phi \circ \widetilde{g} = \phi \circ \widetilde{f} \circ \widetilde{g}.$$

Then, from Lemma 4.7, $\widetilde{f \circ g} = \widetilde{f} \circ \widetilde{g}$.

Because ϕ_σ is defined over K, by letting $\tau \in G$ act on the identity $\phi \circ \phi_\sigma = \sigma(\phi)$, we have $\tau(\phi) \circ \phi_\sigma = \tau(\sigma(\phi))$. Now we have the following equality:

$$\phi \circ \phi_\tau \circ \phi_\sigma = \tau(\phi) \circ \phi_\sigma = \tau(\sigma(\phi)) = (\tau\sigma)(\phi) = \phi \circ \phi_{\tau\sigma}.$$

Then, from Lemma 4.7, $\phi_{\sigma\tau} = \phi_\sigma \circ \phi_\tau$. □

Notation. For notational convenience, in $\mathrm{End}_K(Res_{L/K}(A))$ we will write pq instead of $p \circ q$ where $p, q \in \mathrm{End}_K(Res_{L/K}(A))$.

Definition 4.12. Define a map $\Upsilon : \mathrm{End}_L(A)[G] \longrightarrow \mathrm{End}_K(Res_{L/K}(A))$ by

$$\Upsilon\left(\sum_{\sigma\in G} p_\sigma \sigma\right) = \sum_{\sigma \in G} \widetilde{p_\sigma}\phi_\sigma,$$

where $p_\sigma \in \mathrm{End}_L(A)$.

Lemma 4.13. *The map Υ is an injective homomorphism.*

Proof. We can check that the map Υ is a ring homomorphism in the following computation:

$$\begin{aligned}
\Upsilon\left((\sum_\sigma p_\sigma\sigma)(\sum_\tau q_\tau\tau)\right) &= \Upsilon\left(\sum_{\sigma,\tau}(p_\sigma q_\tau^\sigma)\sigma\tau\right) = \sum_{\sigma,\tau}\widetilde{(p_\sigma q_\tau^\sigma)}\phi_{\sigma\tau} \\
&= \sum_{\sigma,\tau}\widetilde{p_\sigma}\widetilde{q_\tau^\sigma}\phi_\sigma\phi_\tau = \sum_{\sigma,\tau}\widetilde{p_\sigma}\phi_\sigma\widetilde{q_\tau}\phi_\tau \\
&= \left(\sum_\sigma \widetilde{p_\sigma}\phi_\sigma\right)\left(\sum_\tau \widetilde{q_\tau}\phi_\tau\right) \\
&= \Upsilon\left(\sum_\sigma p_\sigma\sigma\right)\Upsilon\left(\sum_\tau q_\tau\tau\right).
\end{aligned}$$

Suppose $\Upsilon(\sum_{\sigma\in G} p_\sigma \sigma) = 0$, that is, $\sum_{\sigma\in G} \widetilde{p_\sigma}\phi_\sigma = 0$. Then $\sum_{\sigma\in G} p_\sigma \phi^\sigma = 0$ because

$$\sum_{\sigma\in G} p_\sigma \phi^\sigma = \sum_{\sigma\in G} p_\sigma \phi\phi_\sigma = \sum_{\sigma\in G} \phi\widetilde{p_\sigma}\phi_\sigma = \phi\sum_{\sigma\in G} \widetilde{p_\sigma}\phi_\sigma = 0.$$

By looking at $\sum_{\sigma\in G} p_\sigma\phi^\sigma$ carefully we can break this into a composition of three homomorphisms:

$$\textstyle\sum_{\sigma\in G} p_\sigma\phi^\sigma : Res_{L/K}(A) \xrightarrow{\prod_\sigma \phi^\sigma} A\times\cdots\times A \xrightarrow{\prod_\sigma p_\sigma} A\times\cdots\times A \xrightarrow{\Sigma} A,$$

where Σ means summation of all components. Because $\prod_{\sigma\in G}\phi^\sigma$ is an isomorphism, $\Sigma\circ\prod_{\sigma\in G} p_\sigma = 0$. So it follows that $p_\sigma = 0$ for $\sigma\in G$. $\square$

We can extend Υ to a map from $\mathrm{End}_L(A)[G]\otimes\mathbf{Q}$ to $\mathrm{End}_K(Res_{L/K}(A))\otimes\mathbf{Q}$, which again will be denoted by Υ.

Lemma 4.14. *The map $\Upsilon : \mathrm{End}_L(A)[G]\otimes\mathbf{Q} \longrightarrow \mathrm{End}_K(Res_{L/K}(A))\otimes\mathbf{Q}$ is a ring homomorphism which is injective.*

Definition 4.15. For every subgroup H of G, define $Res_{L^H/K}(A)$ to be the restriction of scalars of A from L^H to K with a fixed map $\phi_H : Res_{L^H/K}(A) \to A$ defined over L^H.

Definition 4.16. Because ϕ_H is defined over L, according to the universal mapping property for $\{Res_{L/K}(A), \phi\}$, there exists a unique $\mathcal{F} : Res_{L^H/K}(A) \to Res_{L/K}(A)$ such that $\phi\circ\mathcal{F} = \phi_H$. Denote this map $\mathcal{F}$ by Ψ_H.

Definition 4.17. Note that $\sum_{\sigma\in H}\phi^\sigma : Res_{L/K}(A) \to A$ is defined over L^H. According to the universal mapping property for $\{Res_{L^H/K}(A), \phi_H\}$, there exists a unique

$\mathcal{F} : Res_{L/K}(A) \to Res_{L^H/K}(A)$ such that $\phi_H \circ \mathcal{F} = \sum_{\sigma \in H} \phi^{\sigma}$. Denote this map $\mathcal{F}$ by Φ_H.

Lemma 4.18.

$$\Phi_H \circ \Psi_H = |H| \quad \textit{and} \quad \Psi_H \circ \Phi_H = \sum_{\sigma \in H} \phi_\sigma.$$

Proof. For any $\sigma \in H$, $\phi^{\sigma} \circ \Psi_H = \phi_H$. Then

$$\phi_H \circ \Phi_H \circ \Psi_H = \sum_{\sigma \in H} \phi^{\sigma} \circ \Psi_H = \sum_{\sigma \in H} \phi_H = \phi_H \circ |H|.$$

Then from Lemma 4.7, we have $\Phi_H \circ \Psi_H = |H|$.

$$\phi \circ \Psi_H \circ \Phi_H = \phi_H \circ \Phi_H = \sum_{\sigma \in H} \phi^{\sigma} = \phi \circ \left(\sum_{\sigma \in H} \phi_\sigma \right).$$

Then from Lemma 4.7, we have $\Psi_H \circ \Phi_H = \sum_{\sigma \in H} \phi_\sigma$. □

Theorem 4.19.

$$\left(\sum_{\sigma \in H} \phi_\sigma \right) (Res_{L/K}(A)) \sim Res_{L^H/K}(A),$$

where $\sim$ means K-isogeneous.

Proof. From the equation $\Phi_H \circ \Psi_H = |H|$, Φ_H is surjective and Ψ_H has a finite kernel. Then

$$\begin{aligned}
\left(\sum_{\sigma \in H} \phi_\sigma \right) (Res_{L/K}(A)) &= (\Psi_H \circ \Phi_H)(Res_{L/K}(A)) \\
&= \Psi_H(\Phi_H(Res_{L/K}(A))) \\
&= \Psi_H(Res_{L^H/K}(A)) \\
&\sim Res_{L^H/K}(A).
\end{aligned}$$

□

Remark 4.20. Let $\chi \in Z^1(H, \mathrm{Aut}_L(A))$ be a 1-cocycle. As in Remark 4.4, through the identification between $Twist_L(A/L^H)$ and $\mathrm{H}^1(H, \mathrm{Aut}_L(A))$, there is a corresponding twist A^χ defined over L^H which is isomorphic to A over L. Actually, we even have an isomorphism $\alpha : A^\chi \longrightarrow A$ defined over L such that $\alpha \circ \alpha^{-\sigma} = \chi(\sigma)$.

With this isomorphism α we have the following lemma.

Lemma 4.21. *The restriction of scalars of A^χ from L to K is $\{Res_{L/K}(A), \alpha^{-1} \circ \phi\}$, that is, $Res_{L/K}(A^\chi) \cong Res_{L/K}(A)$ over K.*

Proof. Because $\{Res_{L/K}(A), \phi\}$ represents a restriction of scalars of A from L to K, there is an isomorphism

$$(\phi^{\sigma_1}, \dots, \phi^{\sigma_d}) : Res_{L/K}(A) \longrightarrow A^{\sigma_1} \times \cdots \times A^{\sigma_d},$$

where $\{\sigma_1, \dots, \sigma_d\}$ is the set of all distinct isomorphisms of L into $\overline{K}$. Then the composition map $((\alpha^{-1} \circ \phi)^{\sigma_1}, \dots, (\alpha^{-1} \circ \phi)^{\sigma_d}) = \prod_i \alpha^{-\sigma_i} \circ (\phi^{\sigma_1}, \dots, \phi^{\sigma_d})$:

$$Res_{L/K}(A) \xrightarrow{(\phi^{\sigma_1}, \dots, \phi^{\sigma_d})} A^{\sigma_1} \times \cdots \times A^{\sigma_d} \xrightarrow{\prod_i \alpha^{-\sigma_i}} (A^\chi)^{\sigma_1} \times \cdots \times (A^\chi)^{\sigma_d}$$

is an isomorphism because these two maps, $(\phi^{-\sigma_1}, \dots, \phi^{-\sigma_d})$ and $\prod_i \alpha^{-\sigma_i}$, are isomorphisms. So by the definition of the restriction of scalars, the lemma follows.
$\square$

By the same computation as in Theorem 4.19 for $\{Res_{L/K}(A), \alpha^{-1} \circ \phi\}$, we can generalize Theorem 4.19.

Theorem 4.22 (Generalization of Theorem 4.19).

$$\left(\sum_{\sigma \in H} \widetilde{\chi(\sigma)} \circ \phi_\sigma \right) (Res_{L/K}(A)) \sim Res_{L^H/K}(A^\chi),$$

where $\sim$ means K-isogeneous.

Proof. For $\sigma \in H$, $(\alpha^{-1} \circ \phi) \circ \widetilde{\chi(\sigma)} \circ \phi_\sigma = (\alpha^{-1} \circ \phi) \circ (\alpha^{-1} \circ \phi)_\sigma$, because

$$\begin{aligned}
(\alpha^{-1} \circ \phi) \circ \widetilde{\chi(\sigma)} \circ \phi_\sigma &= \alpha^{-1} \circ \chi(\sigma) \circ \phi \circ \phi_\sigma \\
&= \alpha^{-1} \circ \alpha \circ \alpha^{-\sigma} \circ \phi \circ \phi_\sigma \\
&= \alpha^{-\sigma} \circ \phi^\sigma = (\alpha^{-1} \circ \phi)^\sigma \\
&= (\alpha^{-1} \circ \phi) \circ (\alpha^{-1} \circ \phi)_\sigma .
\end{aligned}$$

Then by Lemma 4.7, $\widetilde{\chi(\sigma)} \circ \phi_\sigma = (\alpha^{-1} \circ \phi)_\sigma$.

Therefore, from Theorem 4.19,

$$\begin{aligned}
\left(\sum_{\sigma \in H} \widetilde{\chi(\sigma)} \circ \phi_\sigma \right) (Res_{L/K}(A)) &= \left(\sum_{\sigma \in H} (\alpha^{-1} \circ \phi)_\sigma \right) (Res_{L/K}(A)) \\
&\sim Res_{L^H/K}(A^\chi).
\end{aligned}$$

□

CHAPTER 5

BACKGROUND RESULTS

Kani-Rosen

Let A be an abelian variety defined over K and ε an idempotent in $\mathrm{End}_K(A) \otimes \mathbf{Q}$. Here $\varepsilon(A)$ denotes any representative of the K-isogeny class containing the abelian subvarieties $(n\varepsilon)(A) \subset A$, where $n \in \mathbf{N}$ is chosen such that $n\varepsilon \in \mathrm{End}_K(A)$.

We say two elements a and b of $\mathrm{End}_K(A) \otimes \mathbf{Q}$ are characteristic equivalent, $a \sim b$, if $\chi(a) = \chi(b)$ for all rational characters χ of $\mathrm{End}_K(A) \otimes \mathbf{Q}$.

Theorem 5.1 (Kani–Rosen [13]). *Let $\varepsilon_1, \ldots, \varepsilon_n, \varepsilon'_1, \ldots, \varepsilon'_m \in \mathrm{End}_K(A) \otimes \mathbf{Q}$ be (not necessarily distinct) idempotents. Then idempotent relation*

$$\varepsilon_1 + \varepsilon_2 + \cdots + \varepsilon_n \sim \varepsilon'_1 + \cdots + \varepsilon'_m$$

holds in $\mathrm{End}_K(A) \otimes \mathbf{Q}$ if and only if we have the isogeny relation

$$\varepsilon_1(A) \times \varepsilon_2(A) \times \cdots \times \varepsilon_n(A) \sim \varepsilon'_1(A) \times \cdots \times \varepsilon'_m(A).$$

Tate

Theorem 5.2 (Tate [44]). *The truth of the Birch and Swinnerton–Dyer conjecture depends only on the K–isogeny class of A. Furthermore, if the two abelian varieties A and B are isogeneous over K, then $C(A/K) = C(B/K)$.*

This has been verified by Cassels [6] for elliptic curves.

Milne

Let L/K be a finite separable field extension, A be an abelian variety over L, and $Res_{L/K}(A)$ be the restriction of scalars of A from L to K.

Theorem 5.3 (Milne [21]).

(1) $L(A/L, s) = L(Res_{L/K}(A)/K, s)$.

(2) $\tau(A/L) = \tau(Res_{L/K}(A)/K)$.

(3) $R(A/L) = R(Res_{L/K}(A)/K)$.

(4) $\text{Ш}(A/L) \cong \text{Ш}(Res_{L/K}(A)/K)$.

(5) $C(A/L) = C(Res_{L/K}(A)/K)$.

(6) $\text{rank}_{\mathbf{Z}}(A(L)) = \text{rank}_{\mathbf{Z}}(Res_{L/K}(A)(K))$.

Theorem 5.4 (Milne [21]). *The Birch and Swinnerton–Dyer conjecture is true for A over L if and only if it is true for $Res_{L/K}(A)$ over K.*

Proof. This is an immediate consequence of Theorem 5.3. □

CHAPTER 6

MAIN THEOREM AND APPLICATIONS

We are ready to state the Main Theorem and we will prove this theorem right after Theorem 6.2.

Main Theorem. *Assume that the Shafarevich–Tate groups are finite and there is an idempotent relation* $\sum_i n_i\varepsilon(\chi_i) = 0$ *with* $n_i \in \mathbf{Z}$. *Then*

$$\text{(M1)} \qquad \sum_i n_i \operatorname{rank}_{\mathbf{Z}}(A^{\chi_i}(L^{H_i})) = 0.$$

$$\text{(M2)} \qquad \prod_i L(A^{\chi_i}/L^{H_i}, s)^{n_i} = 1.$$

$$\text{(M3)} \qquad \prod_i C(A^{\chi_i}/L^{H_i})^{n_i} = 1.$$

Notation. For $\chi \in Z^1(H, \operatorname{Aut}_L(A))$ with a subgroup H of G, let L^χ be the fixed field of L by H, i.e. $L^\chi = L^H$.

Lemma 6.1.

$$\Upsilon(\varepsilon(\chi))(Res_{L/K}(A)) \sim Res_{L^\chi/K}(A^\chi).$$

Proof.

$$\Upsilon(\varepsilon(\chi))(Res_{L/K}(A)) = \Upsilon\left(\frac{1}{|H_\chi|}\sum_{\sigma\in H_\chi}\chi(\sigma)\sigma\right)(Res_{L/K}(A))$$

$$= \left(\frac{1}{|H_\chi|}\sum_{\sigma\in H_\chi}\widetilde{\chi(\sigma)}\phi_\sigma\right)(Res_{L/K}(A))$$

$$\sim \left(\sum_{\sigma\in H_\chi}\widetilde{\chi(\sigma)}\phi_\sigma\right)(Res_{L/K}(A)) \tag{6.1}$$

$$\sim Res_{L^\chi/K}(A^\chi). \tag{6.2}$$

The isogeny (6.1) is from the definition of the action of idempotents on abelian varieties. The isogeny (6.2) is from Theorem 4.22. □

Theorem 6.2. *Assume that the Shafarevich–Tate groups are finite and there is an idempotent relation $\sum_i n_i\varepsilon(\chi_i) = \sum_j m_j\varepsilon(\mu_j)$, where n_i and m_j are positive integers. Then*

$$\prod_i Res_{L^{\chi_i}/K}(A^{\chi_i})^{n_i} \sim \prod_j Res_{L^{\mu_j}/K}(A^{\mu_j})^{m_j}.$$

Proof. By applying the homomorphism Υ to $\sum_i n_i\varepsilon(\chi_i) = \sum_j m_j\varepsilon(\mu_j)$, we have an idempotent relation in $\mathrm{End}_K(Res_{L/K}(A))\otimes\mathbf{Q}$,

$$\sum_i n_i\Upsilon(\varepsilon(\chi_i)) = \sum_j m_j\Upsilon(\varepsilon(\mu_j)).$$

Then, from Theorem 5.1,

$$\prod_i \left(\Upsilon(\varepsilon(\chi_i))(Res_{L/K}(A))\right)^{n_i} \sim \prod_j \left(\Upsilon(\varepsilon(\mu_j))(Res_{L/K}(A))\right)^{m_j}.$$

Now, the theorem follows from Lemma 6.1 . □

Proof of the Main Theorem

First, rewrite the given relation $\sum_i n_i\varepsilon(\chi_i) = 0$ as

$$\sum_i n_i\varepsilon(\chi_i) = \sum_j m_j\varepsilon(\mu_j),$$

where n_i and m_j are positive integers.

From Theorem 6.2

$$(*) \qquad \prod_i Res_{L^{\chi_i}/K}(A^{\chi_i})^{n_i} \sim \prod_j Res_{L^{\mu_j}/K}(A^{\mu_j})^{m_j}.$$

From the isogeny $(*)$, we have

$$\sum_i n_i \operatorname{rank}_{\mathbf{Z}}(Res_{L^{\chi_i}/K}(A^{\chi_i})(K)) = \sum_j m_j \operatorname{rank}_{\mathbf{Z}}(Res_{L^{\mu_j}/K}(A^{\mu_j})(K)).$$

By Theorem 5.3 (6),

$$\sum_i n_i \operatorname{rank}_{\mathbf{Z}}(A^{\chi_i}(L)) = \sum_j m_j \operatorname{rank}_{\mathbf{Z}}(A^{\mu_j}(L)).$$

Therefore, (M1) holds.

Because isogenous abelian varieties have the same L–function,

$$\prod_i L(Res_{L^{\chi_i}/K}(A^{\chi_i})/K, s)^{n_i} = \prod_j L(Res_{L^{\mu_j}/K}(A^{\mu_j})/K, s)^{m_j}.$$

Then from Theorem 5.3 (1),

$$\prod_i L(A^{\chi_i}/K, s)^{n_i} = \prod_j L(A^{\mu_j}/K, s)^{m_j},$$

which gives the result (M2).

By using Theorem 5.2, from the isogeny $(*)$ we also have

$$\prod_i C(Res_{L^{\chi_i}/K}(A^{\chi_i})/K)^{n_i} = \prod_j C(Res_{L^{\mu_j}/K}(A^{\mu_j})/K)^{m_j}.$$

Now, from Theorem 5.3 (5),

$$\prod_i C(A^{\chi_i}/K)^{n_i} = \prod_j C(A^{\mu_j}/K)^{m_j}.$$

So (M3) follows. □

Corollary 6.3. *The conjecture of Park is true.*

Proof. By applying the Main Theorem with all $\chi_i = 1$, we prove the conjecture of Park. □

Corollary 6.4. *Suppose E is an elliptic curve over $\mathbf{Q}$, with complex multiplication by the ring of integers of an imaginary quadratic field K. Then the Birch and Swinnerton–Dyer conjecture for E/K is equivalent to the Birch and Swinnerton–Dyer conjecture for $E/\mathbf{Q}$.*

Proof. If E^{χ} is the twist of E by the quadratic character of $K/\mathbf{Q}$, then E^{χ} is isogenous to E (see [28, Lemma 3]). From Theorem 5.2, $E/\mathbf{Q}$ satisfies the Birch and Swinnerton–Dyer conjecture if and only if E^{χ} does. By applying the Main Theorem on the idempotent relation in Example 3.3, p.15, the corollary follows. □

Corollary 6.5. *Assume that the Shafarevich–Tate groups are finite and there is an idempotent relation $\sum_i n_i \varepsilon(\chi_i) = 0$ with $n_i \in \mathbf{Z}$. If every A^{χ_i} but one, say A^{χ_1}, satisfies the Birch and Swinnerton–Dyer conjecture, then A^{χ_1} does too.*

Proof. This is an immediate result of the Main Theorem. □

Corollary 6.6. *Suppose E is an elliptic curve defined over $\mathbf{Q}$ with complex multiplication by $\mathbf{Z}[(1+\sqrt{-7})/2]$, $Gal(L/\mathbf{Q}) = (\mathbf{Z}/2\mathbf{Z})^n$, and $L(E/L,1) \neq 0$. Then the conjecture of Birch and Swinnerton-Dyer holds for E/L.*

Proof. From Example 3.5, there is an idempotent relation

$$\sum_{\chi \in \mathrm{Hom}(G,\{\pm 1\})} \varepsilon(\chi) = \varepsilon(1_{\{e\}}).$$

If $\chi = 1_G \in \mathrm{Hom}(G, \{\pm 1\})$, then $E^\chi = E$.

Suppose $\chi \in \mathrm{Hom}(G, \{\pm 1\})$ and $\chi \neq 1_G$. Then $L^{\ker(\chi)}$ is a quadratic extension over $\mathbf{Q}$, and E^χ is the twist of E by the quadratic character of $L^{\ker(\chi)}/\mathbf{Q}$.

If $\chi = 1_{\{e\}}$, $E^{1_{\{e\}}} = E/L$.

Now $L(E^\chi/\mathbf{Q}, 1) \neq 0$ for $\chi \in \mathrm{Hom}(G, \{\pm 1\})$ because $L(E/L, 1) \neq 0$. Then by Theorem 2.8, $E^\chi/\mathbf{Q}$ satisfies the Birch and Swinnerton–Dyer conjecture. Thus the corollary follows from Corollary 6.5. □

CHAPTER 7

SEPARATING THE FACTORS

7.1 Shafarevich–Tate groups in arbitrary Galois extension

The constant $C(A^{\chi_i}/L^{H_i})$ is defined as a product of various factors: $R(A^{\chi_i}/L^{H_i})$, $\#\text{Ш}(A^{\chi_i}/L^{H_i})$, and $\tau(A^{\chi_i}/L^{H_i})$. Given $\sum_i n_i\varepsilon(\chi_i) = 0$, although $\prod_i C(A^{\chi_i}/L^{H_i}) = 1$, the individual factors do not. In general,

$$\prod_i (\#\text{Ш}(A^{\chi_i}/L^{H_i}))^{n_i} \neq 1 \quad \text{and} \quad \prod_i (R(A^{\chi_i}/L^{H_i}))^{n_i} \neq 1.$$

In this chapter, we copmpute these products. Especially for quadratic extensions, we have the explicit result, Theorem 7.7 and Theorem 7.38.

Theorem 7.1 (Walter [47]). *Let G be a finite group, k a number field. and $\mathcal{O}$ the ring of integers of k. Let $T = \{\varepsilon_i\}$ be a finite set of idempotents in $k[G]$ and $\mathcal{O}_T$ the subring of k generated over $\mathcal{O}$ by $|G|^{-1}$ and the coefficients of the $\varepsilon_i \in T$. Suppose that there is an idempotent realtion $\sum n_i\varepsilon_i = \sum m_i\varepsilon_i$, where n_i and m_i are non-negative integers. If M is a finite $\mathcal{O}_T[G]$-module, then there is a $\mathcal{O}_T$-module isomorphism*

$$\bigoplus_i (M^{\varepsilon_i})^{n_i} \longrightarrow \bigoplus_i (M^{\varepsilon_i})^{m_i}.$$

Here $M^{\varepsilon_i} = \{x^{\varepsilon_i} \mid x \in M\}$.

In particular, $\prod_i |M^{\varepsilon_i}|^{n_i} = \prod_i |M^{\varepsilon_i}|^{m_i}$.

Notation. For any real numbers a, b and any positive integer n, $a \equiv_n b$ means that a is equal to b up to the prime factors of n, i.e.,

$$\frac{a}{b} = \pm p_1^{n_1} \cdots p_l^{n_l}$$

where $p_i | n$ and $n_i \in \mathbf{Z}$ for all i.

Lemma 7.2. *If* M *is a finite* G*-module, and if* $\sum_H n_H \varepsilon(id_H) = 0$*, then*

$$\prod_H |M^{\varepsilon(id_H)}|^{n_H} \equiv_{|G|} 1.$$

Proof. See [25]. □

Definition 7.3. For any finite abelian group M, define

$$\widetilde{M} = \{x \in M \mid \text{the order of } x \text{ is prime to } |G|.\}.$$

Note that $\widetilde{M}$ is a subgroup of M.

Lemma 7.4. *Let* $id_H \in Z^1(H, \mathrm{Aut}_L(A))$ *be the trivial cocycle for a subgroup* H *of* G*. Then*

$$\#\widetilde{\text{Ш}}(Res_{L/K}(A))^{\Upsilon(\varepsilon(id_H))} = \#\widetilde{\text{Ш}}(A/L^H).$$

Proof. From Definition 4.16 we have an induced map from $\mathrm{H}^1(G_K, Res_{L^H/K}(A))$ to $\mathrm{H}^1(G_K, Res_{L/K}(A))$ and we denote the restriction of this map on $\widetilde{\text{Ш}}(Res_{L^H/K}(A))$ by $\widetilde{\Psi_H}$. From Definition 4.17, we have an induced map from $\mathrm{H}^1(G_K, Res_{L/K}(A))$ to

$\mathrm{H}^1(G_K, Res_{L^H/K}(A))$ and we denote the restriction of this map on $\widetilde{\text{Ш}}(Res_{L/K}(A))$ by $\widetilde{\Psi_H}$. Now it is easy to check that

$$\text{Image}(\widetilde{\Psi_H}) \subset \widetilde{\text{Ш}}(Res_{L/K}(A)) \quad \text{and} \quad \text{Image}(\widetilde{\Phi_H}) \subset \widetilde{\text{Ш}}(Res_{L^H/K}(A)).$$

Because $\Phi_H \circ \Psi_H = |H|$, $\widetilde{\Phi_H} \circ \widetilde{\Psi_H} = |H|$. Note that the map $|H|$ is bijective on $\widetilde{\text{Ш}}(Res_{L/K}(A))$. Then $\widetilde{\Phi_H}$ is surjective and $\widetilde{\Psi_H}$ is injective.

$$\begin{aligned}
\#\widetilde{\text{Ш}}(Res_{L/K}(A))^{\Upsilon(\varepsilon(id_H))} &= \#\sum_{\sigma \in H} \phi_\sigma \left(\widetilde{\text{Ш}}(Res_{L/K}(A))\right) \\
&= \#\widetilde{\Psi_H} \circ \widetilde{\Phi_H} \left(\widetilde{\text{Ш}}(Res_{L/K}(A))\right) \\
&= \#\widetilde{\Psi_H} \left(\widetilde{\text{Ш}}(Res_{L^H/K}(A))\right) \\
&= \#\widetilde{\text{Ш}}(Res_{L^H/K}(A)) \\
&= \#\widetilde{\text{Ш}}(A/L^H)
\end{aligned}$$

The last equality comes from Theorem 5.3 (4). □

Lemma 7.5. *Let $\chi \in Z^1(H, \mathrm{Aut}_L(A))$ be a 1-cocycle for a subgroup H of G. Then*

$$\#\widetilde{\text{Ш}}(Res_{L/K}(A))^{\Upsilon(\varepsilon(\chi))} = \#\widetilde{\text{Ш}}(A^\chi/L^H).$$

Proof. Using Lemma 4.21, the lemma follows by the same computation as in the proof of Lemma 7.4. □

Theorem 7.6. *Suppose that the Shafarevich–Tate groups are finite and there is an idempotent relation $\sum_i n_i \varepsilon(\chi_i) = 0$ with $n_i \in \mathbf{Z}$. Assume that there is a finite subgroup B in $\mathrm{Aut}_L(A)$ containing $\bigcup_i \chi_i(H_i)$ and stable under G. Let $n = \#B \cdot [L : K]$. Then*

$$\prod_i \#\text{Ш}(A^{\chi_i}/L^{H_i})^{n_i} \equiv_n 1.$$

Proof. We can check very easily that the semi-direct product $\Upsilon(B) \ltimes \Upsilon(G)$ is a finite subgroup of $\mathrm{Aut}_K(Res_{L/K}(A))$ of order $n = \#B \cdot [L : K]$. Now $Ш(Res_{L/K}(A))$ is a finite $\Upsilon(B) \ltimes \Upsilon(G)$–module. We have an idempotent relation $\sum_i n_i \Upsilon(\varepsilon(\chi_i)) = 0$. From Lemma 7.2

$$\prod_i \left(\#\widetilde{Ш}(Res_{L/K}(A))^{\Upsilon(\varepsilon(\chi_i))}\right)^{n_i} \equiv_n 1.$$

Then the theorem follows from Lemma 7.5. □

7.2 Shafarevich–Tate groups in quadratic extensions

From now on we assume L/K is a quadratic extension of Galois group $Gal(L/K)$ and we fix $\sigma \in G_K - G_L$. Let M_K be a complete set of places on K and let M_L be a complete set of places on L. Denote $Gal(L/K)$ by G and $Gal(L_w/K_w)$ by G_w for $w \in M_L$.

In this section, we will prove the following theorem. The proof is on page 59.

Theorem 7.7. *Let A^χ denote the quadratic twist by the non–trivial character χ of G and A' be the dual variety of A. Then*

$$\frac{\#Ш(A/K)\#Ш(A^\chi/K)}{\#Ш(A/L)} = \frac{\#\,\widehat{\mathrm{H}}^0(G, A'(L))\#\,\mathrm{H}^1(G, A(L))}{\#\prod_{w\in M_L} \mathrm{H}^1(G_w, A(L_w))}.$$

7.2.1 Computing $\#Ш(A/L)^G/\#Ш(A/K)$

Now we start with a natural commutative diagram (see [33]): for a place $v \in M_K$,

$$\begin{array}{ccc} \mathrm{H}^1(G_K, A) & \xrightarrow{\phi} & \mathrm{H}^1(G_L, A) \\ \downarrow & & \downarrow \\ \mathrm{H}^1(G_{K_v}, A) & \xrightarrow{\oplus_{w|v}\phi_w} & \bigoplus_{\substack{w\in M_L \\ w|v}} \mathrm{H}^1(G_{L_w}, A), \end{array}$$

where ϕ and ϕ_w are the restriction maps in the *Inflation–Restriction* sequence. Note that $\mathrm{Ker}(\phi) = \mathrm{H}^1(G, A(L))$, and $\mathrm{Ker}(\phi_v) = \bigoplus_{w|v} \mathrm{H}^1(G_w, A(L_w))$.

With these kernels, we can construct the following commutative diagram:

$$\begin{array}{ccccccc} 0 \to & \mathrm{H}^1(G, A(L)) & \longrightarrow & \mathrm{H}^1(G_K, A) & \xrightarrow{\phi} & \phi(\mathrm{H}^1(G_K, A)) \to 0 \\ & \downarrow & & \downarrow & & \downarrow \\ 0 \to & \bigoplus_w \mathrm{H}^1(G_w, A(L_w)) & \longrightarrow & \bigoplus_v \mathrm{H}^1(G_{K_v}, A) & \xrightarrow{\oplus_w \phi_w} & \bigoplus_w \mathrm{H}^1(G_{L_w}, A). \end{array} \tag{7.1}$$

Lemma 7.8.

$$\bigoplus_{w\in M_L} \mathrm{H}^1(G_w, A(L_w)) \textit{ is finite.}$$

In particular, $\bigoplus_{w\in M_L} \mathrm{H}^1(G_w, A(L_w)) = \prod_{w\in M_L} \mathrm{H}^1(G_w, A(L_w))$.

Proof. First, it is obvious that $\mathrm{H}^1(G_w, A(L_w))$ is finite for $w \in M_L$.

Define $S_L = \{w \in M_L \mid A$ has bad reduction at w, w is above 2, or w is an infinite place.$\}$. Note that S_L is a finite set. We will show that if $w \notin S_L$, then $\# \mathrm{H}^1(G_w, A(L_w)) = 0$.

If $w \notin S_L$ splits, this is obvious because $G_w = 0$.

Assume that $w \notin M_L$ is inert. Since A has good reduction at w, we have the following exact sequence:

$$0 \longrightarrow A_1(L_w) \longrightarrow A(L_w) \longrightarrow \widetilde{A}(\ell_w) \longrightarrow 0,$$

where ℓ_w is the residue field of L_w (see [32]).

Note that $2 \cdot \mathrm{H}^1(G_w, A_1(L_w)) = 0$ because $\#G_w = 2$ (see Corollary 1 [30, p.130]). The map $2 : \mathrm{H}^1(G_w, A_1(L_w)) \longrightarrow \mathrm{H}^1(G_w, A_1(L_w))$ is an isomorphism because the map $2 : A_1(L_w) \longrightarrow A_1(L_w)$ is an isomorphism. Therefore,

$$\mathrm{H}^1(G_w, A_1(L_w)) = 0.$$

With $\mathrm{H}^1(Gal(\ell_w/k_w), \widetilde{A}(\ell_w)) = 0$ for $w \notin S_L$ (see [17] and [28, p.496]),

$$\mathrm{H}^1(G_w, A(L_w)) = 0.$$

□

Notation. Let $M^{(2)}$ denote the 2–component of a torsion abelian group M.

By considering the 2–component of diagram (7.1), we have the following commutative diagram:

(7.2)

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{H}^1(G, A(L)) \arrow[r] \arrow[d, "g_1"] & \mathrm{H}^1(G_K, A)^{(2)} \arrow[r] \arrow[d, "g_2"] & \phi(\mathrm{H}^1(G_K, A))^{(2)} \arrow[r] \arrow[d, "g_3"] & 0 \\
0 \arrow[r] & \bigoplus_w \mathrm{H}^1(G_w, A(L_w)) \arrow[r] & \bigoplus_v \mathrm{H}^1(G_{K_v}, A)^{(2)} \arrow[r] & \bigoplus_w \mathrm{H}^1(G_{L_w}, A)^{(2)}. &
\end{tikzcd}$$

Notation. Let $\varphi : \mathrm{H}^1(G_L, A)^G \longrightarrow \mathrm{H}^2(G, A(L))$ be the Transgression map.

Notation. Denote by $\mathcal{I}_C$ the map $\mathrm{Coker}(g_1) \longrightarrow \mathrm{Coker}(g_2)$ in the above sequence. Write $\mathcal{I}_w$ for the inflation map $\mathrm{H}^1(G_w, A(L)) \longrightarrow \mathrm{H}^1(G_{K_w}, A)$. Denote by $\mathcal{R}_A$ the restriction on $\text{Ш}(A/K)$ of the restriction map $\mathrm{H}^1(G_K, A) \longrightarrow \mathrm{H}^1(G_L, A)^G$.

Lemma 7.9.

$$0 \longrightarrow \mathrm{Ker}(g_1) \longrightarrow Ш(A/K)^{(2)} \longrightarrow Ш(A/L)^G \cap \mathrm{Ker}(\varphi)^{(2)} \longrightarrow \mathrm{Coker}(g_1) \longrightarrow \mathcal{I}_C(\mathrm{Coker}(g_1)) \longrightarrow 0. \tag{7.3}$$

Proof. Note that $\mathrm{Ker}(g_3) = Ш(A/L)^G \cap \phi(\mathrm{H}^1(G_K, A))^{(2)} = Ш(A/L)^G \cap \mathrm{Ker}(\varphi)^{(2)}$ and $\mathrm{Ker}(g_2) = Ш(A/K)^{(2)}$. Then the *Kernel-Cokernel* sequence of diagram (7.2) becomes the sequence (7.3). □

Lemma 7.10.

$$\frac{\#Ш(A/L)^G \cap \mathrm{Ker}(\varphi)}{\#Ш(A/K)} = \frac{\# \bigoplus_w \mathrm{H}^1(G_w, A(L_w))}{\# \mathrm{H}^1(G, A(L)) \# \mathcal{I}_C(\mathrm{Coker}(g_1))}.$$

Proof. From the sequence (7.3),

$$\# \mathrm{Ker}(g_1) \cdot \#Ш(A/L)^G \cap \mathrm{Ker}(\varphi)^{(2)} \cdot \#\mathcal{I}_C(\mathrm{Coker}(g_1)) = \#Ш(A/K)^{(2)} \cdot \# \mathrm{Coker}(g_1).$$

By looking at g_1 in diagram (7.2), we have

$$\# \mathrm{Ker}(g_1) \cdot \# \bigoplus_w \mathrm{H}^1(G_w, A(L_w)) = \# \mathrm{H}^1(G, A(L)) \cdot \# \mathrm{Coker}(g_1).$$

Therefore,

$$\frac{\#Ш(A/L)^G \cap \mathrm{Ker}(\varphi)}{\#Ш(A/K)} = \frac{\#Ш(A/L)^G \cap \mathrm{Ker}(\varphi)^{(2)}}{\#Ш(A/K)^{(2)}} = \frac{\# \bigoplus_w \mathrm{H}^1(G_w, A(L_w))}{\# \mathrm{H}^1(G, A(L)) \# \mathcal{I}_C(\mathrm{Coker}(g_1))},$$

where the first equality holds because $\dfrac{\#Ш(A/L)^G \cap \mathrm{Ker}(\varphi)}{\#Ш(A/K)}$ is only a power of 2.

□

Notation. For an abelian group M, denote $\varprojlim M/2^n M$ by $\overline{M}$.

Theorem 7.11 (Global Duality Theorem).

$$0 \longrightarrow Ш(A/K)^{(2)} \longrightarrow \mathrm{H}^1(G_K, A)^{(2)} \xrightarrow{g_2} \bigoplus_v \mathrm{H}^1(G_{K_v}, A)^{(2)} \xrightarrow{h_2} \mathrm{Hom}(\overline{A'(K)}, \mathbf{Q}/\mathbf{Z}) \longrightarrow 0.$$

Proof. See [2]. □

Definition 7.12. Define $N : A(L) \longrightarrow A(K)$ by $N(P) = P + \sigma(P)$ for $P \in A(L)$, and let $\overline{N} : \overline{A(L)} \longrightarrow \overline{A(K)}$ denote the map induced by N, i.e., defined by

$$\overline{N}(\{P_n + 2^n A(L)\}) = \{N(P_n) + 2^n A(K)\},$$

for $\{P_n + 2^n A(L)\} \in \overline{A(L)}$.

Lemma 7.13.

$$0 \longrightarrow \mathrm{Hom}(\widehat{\mathrm{H}}^0(G, A(L)), \mathbf{Q}/\mathbf{Z}) \xrightarrow{\mathfrak{N}} \mathrm{Hom}(\overline{A(K)}, \mathbf{Q}/\mathbf{Z}) \longrightarrow \mathrm{Hom}(\overline{A(L)}, \mathbf{Q}/\mathbf{Z}).$$

In particular, the map $\mathfrak{N}$ is injective.

Proof. For any $n \geq 1$,

$$\begin{array}{ccccccc}
A(L) & \xrightarrow{N} & A(K) & \longrightarrow & \widehat{\mathrm{H}}^0(G, A(L)) & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \| & & \\
A(L)/2^n A(L) & \longrightarrow & A(K)/2^n A(K) & \longrightarrow & \widehat{\mathrm{H}}^0(G, A(L)) & \longrightarrow & 0
\end{array}$$

because $2^n A(K) \subset N(A(L))$. So we have the following exact sequence:

$$\overline{A(L)} \xrightarrow{\overline{N}} \overline{A(K)} \longrightarrow \widehat{\mathrm{H}}^0(G, A(L)) \longrightarrow 0.$$

Now, by applying $\mathrm{Hom}(\cdot, \mathbf{Q}/\mathbf{Z})$, we have proved the lemma. □

Theorem 7.14 (Local Duality Theorem). *Let $v \in M_K$ be a place. Then there exists a bilinear, non–degenerate pairing*

$$\langle\ ,\ \rangle : \mathrm{H}^0(G_{K_v}, A) \times \mathrm{H}^1(G_{K_v}, A') \longrightarrow \mathbf{Q}/\mathbf{Z}.$$

Proof. See [42] and [43]. □

Lemma 7.15.

$$\mathrm{H}^1(G_{K_v}, A)^{(2)} \cong \mathrm{Hom}(\overline{A'(K_v)}, \mathbf{Q}/\mathbf{Z}).$$

Proof. From Theorem 7.14, $\mathrm{H}^1(G_{K_v}, A)_{2^n-\mathrm{torsion}} \cong \mathrm{Hom}(A'(K_v)/2^n A'(K_v), \mathbf{Q}/\mathbf{Z})$. Thus

$$\begin{aligned}\mathrm{H}^1(G_{K_v}, A)^{(2)} &= \varinjlim \mathrm{H}^1(G_{K_v}, A)_{2^n-\mathrm{torsion}} \cong \varinjlim \mathrm{Hom}(A'(K_v)/2^n A'(K_v), \mathbf{Q}/\mathbf{Z}) \\ &= \mathrm{Hom}(\varprojlim A'(K_v)/2^n A'(K_v), \mathbf{Q}/\mathbf{Z}) = \mathrm{Hom}(\overline{A'(K_v)}, \mathbf{Q}/\mathbf{Z}).\end{aligned}$$

□

Lemma 7.16. *Through the isomorphism in Lemma 7.15,*

$$\bigoplus_w \mathrm{H}^1(G_w, A(L_w)) \cong \mathrm{Hom}(\prod_w \widehat{\mathrm{H}}^0(G_w, A'(L_w)), \mathbf{Q}/\mathbf{Z}).$$

Proof. From Lemmas 7.13 and 7.15, we derive the following diagram:

$$\begin{array}{ccccc} 0 \to \quad \mathrm{H}^1(G_w, A(L_w)) & \longrightarrow & \mathrm{H}^1(G_{K_v}, A)^{(2)} & \longrightarrow & \mathrm{H}^1(G_{L_w}, A)^{(2)} \\ & & \downarrow\cong & & \downarrow\cong \\ 0 \to \mathrm{Hom}(\widehat{\mathrm{H}}^0(G_w, A'(L_w)), \mathbf{Q}/\mathbf{Z}) & \longrightarrow & \mathrm{Hom}(\overline{A'(K_v)}, \mathbf{Q}/\mathbf{Z}) & \longrightarrow & \mathrm{Hom}(\overline{A'(L_w)}, \mathbf{Q}/\mathbf{Z}), \end{array}$$

which is commutative (see [42]). Then

$$\begin{aligned}\bigoplus_w \mathrm{H}^1(G_w, A(L_w)) &\cong \bigoplus_w \mathrm{Hom}(\widehat{\mathrm{H}}^0(G_w, A'(L_w)), \mathbf{Q}/\mathbf{Z}) \\ &\cong \mathrm{Hom}(\prod_w \widehat{\mathrm{H}}^0(G_w, A'(L_w)), \mathbf{Q}/\mathbf{Z}).\end{aligned}$$

□

Lemma 7.17. *Let* $g_0' : \widehat{\mathrm{H}}^0(G, A'(L)) \longrightarrow \prod_w \widehat{\mathrm{H}}^0(G_w, A'(L_w))$*. Then*

$$\#\mathcal{I}_C(\mathrm{Coker}(g_1)) = \frac{\#\,\widehat{\mathrm{H}}^0(G, A'(L))}{\#\,\mathrm{Ker}(g_0')}.$$

Proof. First, $\#\mathcal{I}_C(\mathrm{Coker}(g_1)) = \#(h_2 \circ \bigoplus_w \mathcal{I}_w)(\bigoplus_w \mathrm{H}^1(G_w, A(L_w)))$ from the diagram

$$\begin{array}{ccc}
\bigoplus_w \mathrm{H}^1(G_w, A(L_w)) & \xrightarrow{\oplus_w \mathcal{I}_w} & \bigoplus_v \mathrm{H}^1(G_{K_v}, A)^{(2)} \\
{\scriptstyle \text{surjective}}\big\downarrow & & \big\downarrow{\scriptstyle h_2} \\
\mathrm{Coker}(g_1) & \xrightarrow{\mathcal{I}_C} & \mathrm{Hom}(\overline{A'(K)}, \mathbf{Q}/\mathbf{Z}).
\end{array}$$

From Lemmas 7.15 and 7.16, we can naturally identify $\bigoplus_w \mathrm{H}^1(G_w, A(L_w))$ with $\mathrm{Hom}(\prod_w \widehat{\mathrm{H}}^0(G_w, A'(L_w))$ and $\bigoplus_v \mathrm{H}^1(G_{K_v}, A)^{(2)}$ with $\mathrm{Hom}(\prod_v \overline{A'(K_v)}, \mathbf{Q}/\mathbf{Z})$.

Now, from the diagram

$$\begin{array}{ccc}
\mathrm{Hom}(\prod_w \widehat{\mathrm{H}}^0(G_w, A'(L_w)), \mathbf{Q}/\mathbf{Z}) & \xrightarrow{\oplus_w \mathcal{I}_w} & \mathrm{Hom}(\prod_v \overline{A'(K_v)}, \mathbf{Q}/\mathbf{Z}) \\
{\scriptstyle \mathrm{Hom}(g_0', \cdot)}\big\downarrow & & \big\downarrow{\scriptstyle h_2} \\
\mathrm{Hom}(\widehat{\mathrm{H}}^0(G, A'(L)), \mathbf{Q}/\mathbf{Z}) & \xrightarrow{\mathfrak{N}'} & \mathrm{Hom}(\overline{A'(K)}, \mathbf{Q}/\mathbf{Z}),
\end{array}$$

we obtain $h_2 \circ \bigoplus_w \mathcal{I}_w = \mathfrak{N}' \circ \mathrm{Hom}(g_0', \cdot)$. Because $\mathfrak{N}'$ is injective (Lemma 7.13), $\#\mathrm{Image}(h_2 \circ \bigoplus_w \mathcal{I}_w) = \#\mathrm{Image}(\mathrm{Hom}(g_0', \cdot))$.

Since $\#\,\mathrm{Coker}(\mathrm{Hom}(g_0', \cdot)) = \#\,\mathrm{Ker}(g_0')$,

$$\begin{aligned}
\#\mathcal{I}_C(\mathrm{Coker}(g_1)) &= \#\,\mathrm{Hom}(g_0', \cdot)(\mathrm{Hom}(\prod_w \widehat{\mathrm{H}}^0(G_w, A'(L_w)), \mathbf{Q}/\mathbf{Z})) \\
&= \frac{\#\,\mathrm{Hom}(\widehat{\mathrm{H}}^0(G, A'(L)), \mathbf{Q}/\mathbf{Z})}{\#\,\mathrm{Coker}(\mathrm{Hom}(g_0', \cdot))} \\
&= \frac{\#\,\widehat{\mathrm{H}}^0(G, A'(L))}{\#\,\mathrm{Ker}(g_0')}.
\end{aligned}$$

□

Theorem 7.18.

$$\frac{\#Ш(A/L)^G}{\#Ш(A/K)} = \frac{\#\prod_w \mathrm{H}^1(G_w, A(L_w))}{\#\widehat{\mathrm{H}}^0(G, A'(L))\#\mathrm{H}^1(G, A(L))}\#\operatorname{Ker}(g_0')\#\varphi(Ш(A/L)^G)$$

Proof. From Lemmas 7.10 and 7.17,

$$\begin{aligned}\frac{\#Ш(A/L)^G}{\#Ш(A/K)} &= \frac{\#Ш(A/L)^G}{\#Ш(A/L)^G \cap \operatorname{Ker}(\varphi)}\frac{\#Ш(A/L)^G \cap \operatorname{Ker}(\varphi)}{\#Ш(A/K)} \\ &= \#\varphi(Ш(A/L)^G)\frac{\#Ш(A/L)^G \cap \operatorname{Ker}(\varphi)}{\#Ш(A/K)} \\ &= \#\varphi(Ш(A/L)^G)\frac{\#\prod_w \mathrm{H}^1(G_w, A(L_w))}{\#\mathrm{H}^1(G, A(L))\#\mathcal{I}_C(\operatorname{Coker}(g_1))} \\ &= \#\varphi(Ш(A/L)^G)\frac{\#\prod_w \mathrm{H}^1(G_w, A(L_w))}{\#\mathrm{H}^1(G, A(L))}\frac{\#\operatorname{Ker}(g_0')}{\#\widehat{\mathrm{H}}^0(G, A'(L))}.\end{aligned}$$

□

7.2.2 Computing $\#Ш(A/K)/\#(1+\sigma)Ш(A/L)$

Theorem 7.19 (Cassels, Tate). *There is a canonical pairing*

$$Ш(A/K) \times Ш(A'/K) \longrightarrow \mathbf{Q}/\mathbf{Z},$$

which is non-degenerate if $Ш(A/K)$ *is finite.*

Proof. See [6] and [43]. □

Call this pairing Cassels pairing. Let $\langle -,-\rangle_K : Ш(A/K) \times Ш(A'/K) \longrightarrow \mathbf{Q}/\mathbf{Z}$ be the Cassels pairing for A/K, and let $\langle -,-\rangle_L : Ш(A/L) \times Ш(A'/L) \longrightarrow \mathbf{Q}/\mathbf{Z}$ be the Cassels pairing for A/L.

Now we want to introduce one description of Cassels pairing.

An element $a \in Ш(A/K)$ has a locally trivial principal homogeneous space C over K. Let $\overline{K}$ be the algebraic closure of K, and let $\overline{K}(C)$ be the function field of $C \otimes_K \overline{K}$. Then we have an exact sequence such that

$$0 \longrightarrow \overline{K}^\times \longrightarrow \overline{K}(C)^\times \longrightarrow Q \longrightarrow 0.$$

From this exact sequence, there is a commutative diagram:

$$(7.4) \qquad \begin{array}{ccccccc} & \mathrm{Br}(K) & \longrightarrow & \mathrm{H}^2(G_K, \overline{K}(C)^\times) & \longrightarrow & \mathrm{H}^2(G_K, Q) & \to 0 \\ & \downarrow & & \downarrow & & \downarrow & \\ 0 \to & \bigoplus_{v \in M_K} \mathrm{Br}(K_v) & \longrightarrow & \bigoplus_{v \in M_K} \mathrm{H}^2(G_v, \overline{K_v}(C)^\times) & \longrightarrow & \bigoplus_{v \in M_K} \mathrm{H}^2(G_v, Q). & \end{array}$$

The exact sequence

$$0 \longrightarrow Q \longrightarrow \mathrm{Div}^0(C \otimes \overline{K}) \longrightarrow \mathrm{Pic}^0(C \otimes \overline{K}) \longrightarrow 0$$

gives us a cohomology sequence

$$\mathrm{H}^1(G_K, \mathrm{Div}^0(C \otimes \overline{K})) \longrightarrow \mathrm{H}^1(G_K, \mathrm{Pic}^0(C \otimes \overline{K})) \longrightarrow \mathrm{H}^2(G_K, Q) \longrightarrow \cdots .$$

Since $\mathrm{Pic}^0(C \otimes \overline{K}) \cong \mathrm{Pic}^0(A \otimes \overline{K}) \cong A'$, the sequence gives a map

$$(7.5) \qquad Trans_K : \mathrm{H}^1(G_K, A') \longrightarrow \mathrm{H}^2(G_K, Q).$$

Choose an element $b \in Ш(A'/K)$. Then $Trans_K(b) \in \mathrm{H}^2(G_K, Q)$ lifts to an element of $\mathrm{H}^2(G_K, \overline{K}(C)^\times)$ in the diagram (7.4), and the image of this element in $\bigoplus_v \mathrm{H}^2(K_v, \overline{K_v}(C)^\times)$ lifts to an element $(c_v) \in \bigoplus_v \mathrm{Br}(K_v)$. Then

$$\langle a, b \rangle_K = \sum \mathrm{inv}_v(c_v) \in \mathbf{Q}/\mathbf{Z}.$$

See [22, pp.98–99] for the details.

Theorem 7.20. *For $a \in Ш(A/K)$ and $b \in Ш(A'/L)$*

$$\langle a, \mathrm{Cores}(b) \rangle_K = \langle \mathcal{R}_A(a), b \rangle_L ,$$

where $\mathcal{R}_A$ denotes the restriction to $Ш(A/K)$ of the restriction map $\mathrm{H}^1(G_K, A) \longrightarrow \mathrm{H}^1(G_L, A)^G$ and Cores *denotes the corestriction map.*

Proof. Let $a \in Ш(A/K)$. Then there is a locally trivial principal homogeneous space C/K. For $\mathcal{R}_A(a) \in Ш(A/L)$, C/K is a corresponding locally trivial principal homogeneous space. And $\overline{K} = L_s$. From the following commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \overline{K}^{\times} & \longrightarrow & \overline{K}(C)^{\times} & \longrightarrow & Q & \longrightarrow & 0 \\
 & & \| & & \| & & \| & & \\
0 & \longrightarrow & L_s^{\times} & \longrightarrow & L_s(C)^{\times} & \longrightarrow & Q & \longrightarrow & 0,
\end{array}$$

we can derive a commutative diagram:

$$\begin{tikzcd}
Br(L) \arrow[rr] \arrow[dr, "\mathrm{Cores}"] \arrow[dd] & & H^2(G_L, L_s(C)^{\times}) \arrow[rr] \arrow[dr, "\mathrm{Cores}"] \arrow[dd] & & H^2(G_L, Q) \arrow[r] \arrow[dr, "\mathrm{Cores}"] \arrow[dd] & 0 & \\
 & Br(K) \arrow[rr] \arrow[dd] & & H^2(G_K, \overline{K}(C)^{\times}) \arrow[rr] \arrow[dd] & & H^2(G_K, Q) \arrow[r] \arrow[dd] & 0 \\
\bigoplus_{v \in M_L} Br(L_v) \arrow[rr] \arrow[dr, "\mathrm{Cores}"'] & & \bigoplus_{v \in M_L} H^2(G_{L_v}, L_{v,s}(C)^{\times}) \arrow[rr] \arrow[dr, "\mathrm{Cores}"] & & \bigoplus_{v \in M_L} H^2(G_{L_v}, Q) \arrow[dr, "\mathrm{Cores}"'] & & \\
 & \bigoplus_{v \in M_L} Br(K_v) \arrow[rr] & & \bigoplus_{v \in M_L} H^2(G_{K_v}, \overline{K_v}(C)^{\times}) \arrow[rr] & & \bigoplus_{v \in M_L} H^2(G_{K_v}, Q). &
\end{tikzcd}$$

From the map (7.5), we have the commutative diagram

$$\begin{tikzcd}
Trans_L : \mathrm{H}^1(G_L, A) \arrow[r] \arrow[d, "\mathrm{Cores}"'] & \mathrm{H}^2(G_L, Q) \arrow[d, "\mathrm{Cores}"] \\
Trans_K : \mathrm{H}^1(G_K, A) \arrow[r] & \mathrm{H}^2(G_K, Q).
\end{tikzcd}$$

Let $b \in Ш(A'/L)$. Then $Trans_L(b)$ lifts to an element u of $\mathrm{H}^2(G_L, L_s(C)^\times)$, and the image of this in $\bigoplus \mathrm{H}^2(G_v, L_{v,s}(C)^\times)$ lifts to an element $(c_v) \in \bigoplus \mathrm{Br}(L_v)$. Now, for each element we think of the image of Cores. Then we obtain the following diagram:

$$\begin{tikzcd}[column sep=small]
 & & u \arrow[rr] \arrow[dr] \arrow[dd] & & Trans_L(b) \arrow[dr] \arrow[dd] & \\
 & & & \mathrm{Cores}(u) \arrow[rr] \arrow[dd] & & \mathrm{Cores}(Trans_L(b)) \arrow[dd] \\
(c_v) \arrow[rr] \arrow[dr] & & \begin{array}{c}\text{image of } u \text{ in} \\ \bigoplus_{v \in M_L} H^2(G_{L_v}, L_{v,s}(C)^\times)\end{array} \arrow[rr] \arrow[dr] & & 0 \arrow[dr] & \\
 & (\mathrm{Cores}(c_v)) \arrow[rr] & & \begin{array}{c}\text{image of } \mathrm{Cores}(u) \text{ in} \\ \bigoplus_{v \in M_L} \mathrm{H}^2(G_v, \overline{K_v}(C)^\times)\end{array} \arrow[rr] & & 0.
\end{tikzcd}$$

Then $\langle \mathcal{R}_A(a), b \rangle_L = \sum \mathrm{inv}_v(c_v) \in \mathbf{Q}/\mathbf{Z}$. From the commutativity of the corestriction map at each step, we have

$$\langle a, \mathrm{Cores}(b) \rangle_K = \sum \mathrm{inv}_v(\mathrm{Cores}(c_v)) = \sum \mathrm{inv}_v(c_v).$$

The last equality comes from [41]. Thus $\langle a, \mathrm{Cores}(b) \rangle_K = \langle \mathcal{R}_A(a), b \rangle_L$. $\square$

Lemma 7.21. *Let M and M' be finite abelian groups of the same order, and suppose that there exists a bilinear, non–degenerate pairing*

$$\Gamma : M \times M' \longrightarrow \mathbf{Q}/\mathbf{Z}.$$

For any subgroup B, define $B^{\perp} = \{b \in M' : \Gamma(a, b) = 0$ for any $a \in B\}$. Then

$$\#B\#B^{\perp} = \#M.$$

Proof. We have an isomorphism $\Phi : B^{\perp} \longrightarrow \mathrm{Hom}(M/B, \mathbf{Q}/\mathbf{Z})$ such that for $b \in B^{\perp}$, $\Phi(b)(a + B) = \Gamma(a, b)$ for any $a \in M$. Then

$$\#B^{\perp} = \#\,\mathrm{Hom}(M/B, \mathbf{Q}/\mathbf{Z}) = \#M/B = \frac{\#M}{\#B}.$$

□

Lemma 7.22. *Let $\mathcal{R}_{A'}$ denote the restriction to $\text{Ш}(A'/K)$ of the restriction map: $\mathrm{H}^1(G_K, A') \longrightarrow \mathrm{H}^1(G_L, A')^G$ and let Cores_A be the corestriction map: $\mathrm{H}^1(G_L, A) \longrightarrow \mathrm{H}^1(G_K, A)$. Then*

$$\#\,\mathrm{Ker}(\mathcal{R}_{A'})\#\,\mathrm{Cores}_A(\text{Ш}(A/L)) = \#\text{Ш}(A/K).$$

Proof. Define $\mathrm{Cores}_A(\text{Ш}(A/L))^{\perp} = \{b \in \text{Ш}(A'/K) \mid \langle a, b\rangle_K = 0,\ \text{ for every } a \in \mathrm{Cores}_A(\text{Ш}(A/L))\ \}$. Suppose that $\langle \mathrm{Cores}_A(\text{Ш}(A/L)), b\rangle_K = 0$, for $b \in \text{Ш}(A'/K)$. Then $\langle \text{Ш}(A/L), \mathcal{R}_{A'}(a)\rangle_L = 0$, so $\mathcal{R}_{A'}(a) = 0$ because Cassels pairing is non–degenerate. Thus $\mathrm{Cores}_A(\text{Ш}(A/L))^{\perp} \subset \mathrm{Ker}(\mathcal{R}_{A'})$. $\mathrm{Ker}(\mathcal{R}_{A'}) \subset \mathrm{Cores}_A(\text{Ш}(A/L))^{\perp}$ is obvious. Therefore,

$$\mathrm{Ker}(\mathcal{R}_{A'}) = \mathrm{Cores}_A(\text{Ш}(A/L))^{\perp}.$$

From Lemma 7.21, this Lemma follows. □

Lemma 7.23.

$$\frac{\#\,\mathrm{Cores}_A(\text{Ш}(A/L))}{\#(1+\sigma)\text{Ш}(A/L)} = \#\,\mathrm{Cores}_A(\text{Ш}(A/L)^{\chi}),$$

where $\text{Ш}(A/L)^{\chi} = \{a \in \text{Ш}(A/L) \mid \sigma(a) = -a\}$.

Proof. Note that $(\mathcal{R}_A \circ \mathrm{Cores}_A)(a) = (1+\sigma)(a)$ for $a \in Ш(A/L)$. By considering a restriction of $\mathcal{R}_A$ to $\mathrm{Cores}(Ш(A/L))$ we have the following sequence:

$$0 \to \mathrm{Ker}(\mathcal{R}_A) \cap \mathrm{Cores}_A(Ш(A/L)) \longrightarrow \mathrm{Cores}_A(Ш(A/L)) \longrightarrow (1+\sigma)(Ш(A/L)) \to 0.$$

It is easy to show that $\mathrm{Cores}_A(Ш(A/L)^{\times}) = \mathrm{Ker}(\alpha) \cap \mathrm{Cores}_A(Ш(A/L))$. □

Lemma 7.24.

$$\frac{\#Ш(A/K)}{\#(1+\sigma)Ш(A/L)} = \#\,\mathrm{Cores}_A(Ш(A/L)^{\times})\#\,\mathrm{Ker}(\mathcal{R}_{A'}).$$

Proof. From Lemmas 7.23 and 7.22,

$$\begin{aligned}\frac{\#Ш(A/K)}{\#(1+\sigma)Ш(A/L)} &= \frac{\#\,\mathrm{Cores}_A(Ш(A/L))}{\#(1+\sigma)Ш(A/L)}\frac{\#Ш(A/K)}{\#\,\mathrm{Cores}_A(Ш(A/L))}\\ &= \#\,\mathrm{Cores}_A(Ш(A/L)^{\times})\frac{\#Ш(A/K)}{\#\,\mathrm{Cores}_A(Ш(A/L))}\\ &= \#\,\mathrm{Cores}_A(Ш(A/L)^{\times})\#\,\mathrm{Ker}(\mathcal{R}_{A'}).\end{aligned}$$

□

7.2.3 Connection between Transgression and Corestriction

Let $C^1(G_K, A)$ be the set of cochains.

7.1.3.1 Transgression

Remark 7.25. Recall that $\varphi : \mathrm{H}^1(G_L, A)^G \longrightarrow \mathrm{H}^2(G, A(L))$ is the *Transgression* map. Now, for any element $x \in \mathrm{H}^1(G_L, A)^G$, $\varphi(x)$ is defined by the following condition: there are a cochain $f \in C^1(G_K, A)$ and a 2-cocycle $Y \in Z^2(G, A(L))$ such that the restriction of f to G_L is a representing cocycle for x, df is the natural image in $Z^2(G_K, A)$ of Y by inflation, and $\varphi(x) \in \mathrm{H}^2(G, A(L))$ is the element which is determined by Y.

$$\begin{array}{ccc} x \in \mathrm{H}^1(G_L, A)^G & \xleftarrow{Res} & f \in C^1(G_K, A) \\ \downarrow & & \downarrow \\ Y \in Z^2(G, A(L)) & \xrightarrow{Inf} & df \in Z^2(G_K, A) \end{array}$$

For more detail, see [11, p.129].

Lemma 7.26. *Let $f \in Z^2(G_K/G_L, A(L))$ be a 2-cocycle such that $f(\widetilde{id}, \widetilde{id}) = 0$. Then*

$$f(\widetilde{\sigma}, \widetilde{id}) = f(\widetilde{id}, \widetilde{\sigma}) = 0 \text{ and } f(\widetilde{\sigma}, \widetilde{\sigma})^\sigma = f(\widetilde{\sigma}, \widetilde{\sigma}).$$

Proof. See [30, p.113]. □

Definition 7.27. Let $\mathfrak{C}^1(G_K, A)$ be a subset of $C^1(G_K, A)$ defined by the condition: $f \in \mathfrak{C}^1(G_K, A)$ if , for $f \in C^1(G_K, A)$, there is $P \in A(K)$ such that f satisfies the equation

$$f(\tau_1\tau_2) = \begin{cases} f(\tau_1) + \tau_1 f(\tau_2) & \text{if } \tau_1 \in G_L \text{ or } \tau_2 \in G_L \\ f(\tau_1) + \tau_1 f(\tau_2) - P & \text{if } \tau_1 \notin G_L \text{ and } \tau_2 \notin G_L. \end{cases}$$

Notation. For n–cocycle $f \in Z^n(H, B)$ we denote by $[f]$ the cohomology class containing f.

Lemma 7.28. *For $x \in \mathrm{H}^1(G_L, A)^G$, there are a cochain $f \in \mathfrak{C}^1(G_K, A)$ and a 2–cocycle $Y \in Z^2(G, A(L))$ such that*

$$df = Inf(Y), \ [Y] = \varphi(x) \ \text{ and } \ [f|_{G_L}] = x.$$

Proof. From Remark 7.25, there are $f \in C^1(G_K, A)$ and $Y \in Z^2(G, A(L))$ such that

$$df = Inf(Y), \ [Y] = \varphi(x) \ \text{ and } \ [f|_{G_L}] = x.$$

The only thing we have to show here is $f \in \mathfrak{C}^1(G_K, A)$. Because $f|_{G_L} \in Z^1(G_L, A)$, $df(\tau_1, \tau_2) = 0$ for $\tau_1, \tau_2 \in G_L$. Then $Y(\widetilde{id}, \widetilde{id}) = 0$. From Lemma 7.26,

$$Y(\widetilde{\sigma}, \widetilde{id}) = Y(\widetilde{id}, \widetilde{\sigma}) = 0 \text{ and } \sigma(Y(\widetilde{\sigma}, \widetilde{\sigma})) = Y(\widetilde{\sigma}, \widetilde{\sigma}).$$

Write $P = Y(\widetilde{\sigma}, \widetilde{\sigma}) \in A(K)$. From the defintion of df [30, p.113], i.e., $df(\tau_1, \tau_2) = \tau_1 f(\tau_2) - f(\tau_1\tau_2) + f(\tau_1)$,

$$\tau_1 f(\tau_2) - f(\tau_1\tau_2) + f(\tau_1) = Inf(Y)(\tau_1, \tau_2) = \begin{cases} 0 & \text{if } \tau_1 \in G_L \text{ or } \tau_2 \in G_L \\ P & \text{if } \tau_1 \notin G_L \text{ and } \tau_2 \notin G_L. \end{cases}$$

Therefore, $f \in \mathfrak{C}^1(G_K, A)$. □

Definition 7.29. Define $\mathfrak{F} : \mathrm{H}^1(G_L, A)^G \longrightarrow \mathrm{H}^1(G_K, A^\chi)$ as the composition of the following series of maps:

$$\mathrm{H}^1(G_L, A)^G \xrightarrow{\varphi} \mathrm{H}^2(G, A(L)) \cong \widehat{\mathrm{H}}^0(G, A(L)) \cong \mathrm{H}^1(G, A^\chi(L)) \xrightarrow{Inf} \mathrm{H}^1(G_K, A^\chi).$$

Notation. Denote by $\mathfrak{J}$ the map:$A \longrightarrow A^\chi$ defined over L such that

$$\mathfrak{J}^{-1}\mathfrak{J}^\tau = \begin{cases} id & \text{if } \tau \in G_L \\ -id & \text{if } \tau \notin G_L. \end{cases}$$

Note that there exists $\mathfrak{J}$ because A^χ is the quadratic twist of A (see Defintion 4.1 or Remark 4.20).

Lemma 7.30. *Let $x \in \mathrm{H}^1(G_L, A)^G$ be a 1-cohomology. Then $\mathfrak{F}(x) \in \mathrm{H}^1(G_K, A^\times)$ is represented by a 1-cocycle $U \in Z^1(G_K, A)$ defined by*

$$U(\tau) = 0 \quad \text{if} \quad \tau \in G_L \quad \text{and} \quad U(\tau) = \mathfrak{J}(P) \quad \text{if} \quad \tau \notin G_L$$

where $P = Y(\widetilde{\sigma}, \widetilde{\sigma})$, which is defined in Lemma 7.28.

Proof. The image $\varphi(x)$ in $\widehat{\mathrm{H}}^0(G, A(L))$ is represented by $P = Y(\widetilde{\sigma}, \widetilde{\sigma})$ which is defined in Lemma 7.28. Then $\varphi(x) \in \mathrm{H}^1(G, A^\times(L))$ is represented by a 1-cocycle $u \in Z^1(G, A^\times(L))$ such that

$$u(\widetilde{\sigma}) = \mathfrak{J}(P) \quad \text{and} \quad u(\widetilde{id}) = 0.$$

The inflation map leads to the Lemma. □

7.1.3.2 Corestriction

Remark 7.31. Let X be a cocyle in $Z^1(G_L, A)$. Then with fixed $\sigma \in G_K - G_L$, we have $\mathrm{Cores}(X) \in Z^1(G_K, A)$ such that

$$\mathrm{Cores}(X)(\tau) = \begin{cases} X(\tau) + \sigma X(\sigma^{-1}\tau\sigma) & \tau \in G_L \\ X(\tau\sigma) + \sigma X(\sigma^{-1}\tau) & \tau \in G_K - G_L. \end{cases}$$

See [26, Theorem 3].

Notation. Write $\mathrm{Cores}_{A^\times}$ for the corestriction map from $\mathrm{H}^1(G_L, A^\times)$ to $\mathrm{H}^1(G_K, A^\times)$.

Definition 7.32. Define $\mathfrak{S} : \mathrm{H}^1(G_L, A)^G \longrightarrow \mathrm{H}^1(G_K, A^\times)$ by the composition of the following two maps:

$$\mathrm{H}^1(G_L, A)^G \xrightarrow[\cong]{\mathrm{H}^1(\cdot,\mathfrak{J})} \mathrm{H}^1(G_L, A^\times)^\chi \xrightarrow{\mathrm{Cores}_{A^\times}} \mathrm{H}^1(G_K, A^\times),$$

where $\mathrm{H}^1(G_L, A^\times)^\chi = \{x \in \mathrm{H}^1(G_L, A^\times) \mid \sigma(x) = -x\}$.

Lemma 7.33. *Let $x \in \mathrm{H}^1(G_L, A)^G$ be a 1-cohomology. Then $\mathfrak{S}(x) \in \mathrm{H}^1(G_K, A^\times)$ is represented by a 1-cocycle $U \in Z^1(G_K, A)$ defined by*

$$U(\tau) = 0 \;\; \textit{if} \;\; \tau \in G_L \;\; \textit{and} \;\; U(\tau) = \mathfrak{J}(P) \;\; \textit{if} \;\; \tau \notin G_L,$$

where $P = Y(\widetilde{\sigma}, \widetilde{\sigma})$, which is defined in Lemma 7.28.

Proof. By Lemma 7.28, there are a cochain $f \in \mathfrak{C}^1(G_K, A)$ and a 2-cocycle $Y \in Z^2(G, A(L))$ such that

$$df = Inf(Y), \;\; [Y] = \varphi(x) \;\; \text{and} \;\; [f|_{G_L}] = x.$$

Now, if $\tau \in G_L$,

$$\begin{aligned} \mathfrak{S}(f|_{G_L})(\tau) &= \mathfrak{J}(f(\tau)) + \sigma\mathfrak{J}(f(\sigma^{-1}\tau\sigma)) = \mathfrak{J}(f(\tau) - \sigma f(\sigma^{-1}\tau\sigma)) \\ &= \mathfrak{J}(f(\sigma) - \tau f(\sigma)) = \mathfrak{J}(f(\sigma)) - \tau\mathfrak{J}(f(\sigma)) \\ &= \mathfrak{J}(f(\sigma) - P) - \tau\mathfrak{J}(f(\sigma) - P). \end{aligned}$$

If $\tau \notin G_L$,

$$\begin{aligned} \mathfrak{S}(f|_{G_L})(\tau) &= \mathfrak{J}(f(\tau\sigma)) + \sigma\mathfrak{J}(f(\sigma^{-1}\tau)) = \mathfrak{J}(f(\tau\sigma) - \sigma f(\sigma^{-1}\tau)) \\ &= \mathfrak{J}(f(\sigma) + \tau f(\sigma) - P) = \mathfrak{J}(f(\sigma)) - \tau\mathfrak{J}(f(\sigma)) - \mathfrak{J}(P) \\ &= \mathfrak{J}(f(\sigma) - P) - \tau\mathfrak{J}(f(\sigma) - P) + \mathfrak{J}(P). \end{aligned}$$

□

Proposition 7.34.

$$\mathfrak{F} = \mathfrak{G}.$$

Proof. This is an immediate result of Lemmas 7.30 and 7.33. □

Theorem 7.35.

$$\#\varphi(\text{Ш}(A/L)^G) = \#\operatorname{Cores}_{A^\chi}(\text{Ш}(A^\chi/L)^\chi).$$

Proof. From the definition of $\mathfrak{F}$, $\#\varphi(\text{Ш}(A/L)^G) = \#\mathfrak{F}(\text{Ш}(A/L)^G)$. From the definition of $\mathfrak{F}$, $\#\operatorname{Cores}_{A^\chi}(\text{Ш}(A^\chi/L)^\chi) = \#\mathfrak{G}(\text{Ш}(A/L)^G)$. Thus the theorem follows from the previous proposition. □

7.2.4 Proof of Theorem 7.7

Lemma 7.36.

$$\frac{\#\text{Ш}(A^\chi/K)}{\#(1+\sigma)\text{Ш}(A^\chi/L)} = \#\operatorname{Cores}_{A^\chi}(\text{Ш}(A^\chi/L)^\chi)\#\operatorname{Ker}(\mathcal{R}_{A^{\chi'}}).$$

Proof. This is obvious from Lemma 7.24. □

Note that $(1+\sigma)\text{Ш}(A^\chi/L) \cong (1-\sigma)\text{Ш}(A/L)$.

Lemma 7.37.

$$\#\operatorname{Ker}(\mathcal{R}_{A^{\chi'}}) = \#\operatorname{Ker}(g_0').$$

Proof. First, $\operatorname{Ker}(\mathcal{R}_{A^{\chi'}}) = \operatorname{Ker}\{\mathrm{H}^1(G, A^{\chi\prime}(L)) \longrightarrow \bigoplus_w \mathrm{H}^1(G_w, A^{\chi\prime}(L_w))\}$. Now $\#\operatorname{Ker}(g_0') = \#\operatorname{Ker}\{\mathrm{H}^1(G, A^{\chi\prime}(L)) \longrightarrow \bigoplus_w \mathrm{H}^1(G_w, A^{\chi\prime}(L_w))\}$ by the isomorphisms $\mathrm{H}^1(G, A^{\chi\prime}(L)) \cong \widehat{\mathrm{H}}^0(G, A'(L))$ and $\mathrm{H}^1(G_w, A^{\chi\prime}(L_w) \cong \widehat{\mathrm{H}}^0(G_w, A'(L_w))$. □

Proof of Theorem 7.7

$$\frac{\#\text{Ш}(A/K)\#\text{Ш}(A^\chi/K)}{\#\text{Ш}(A/L)} = \frac{\#\text{Ш}(A/K)\#\text{Ш}(A^\chi/K)}{\#\text{Ш}(A/L)^G\#(1-\sigma)\text{Ш}(A/L)} = \frac{\dfrac{\#\text{Ш}(A^\chi/K)}{\#(1-\sigma)\text{Ш}(A/L)}}{\dfrac{\#\text{Ш}(A/L)^G}{\#\text{Ш}(A/K)}}$$

from Theorem 7.18 and Lemmas 7.36 and 7.37

$$= \frac{\#\operatorname{Cores}_{A^\chi}(\text{Ш}(A^\chi/L)^\chi)\#\operatorname{Ker}(\mathcal{R}_{A^{\chi\prime}})}{\dfrac{\#\prod_w \mathrm{H}^1(G_w, A(L_w))}{\#\widehat{\mathrm{H}}^0(G, A'(L))\#\mathrm{H}^1(G, A(L))}\#\operatorname{Ker}(g_0')\#\varphi(\text{Ш}(A/L)^G)}$$

$$= \frac{\#\operatorname{Cores}_{A^\chi}(\text{Ш}(A^\chi/L)^\chi)}{\#\varphi(\text{Ш}(A/L)^G)}\frac{\#\widehat{\mathrm{H}}^0(G, A'(L))\#\mathrm{H}^1(G, A(L))}{\#\prod_w \mathrm{H}^1(G_w, A(L_w))}$$

from Theorem 7.35

$$= \frac{\#\widehat{\mathrm{H}}^0(G, A'(L))\#\mathrm{H}^1(G, A(L))}{\#\prod_w \mathrm{H}^1(G_w, A(L_w))}.$$

□

7.3 Regulators in quadratic extension

In this section, we will prove the following theorem.

Theorem 7.38. *Suppose that L/K is a quadratic extension. Let A^χ denote the quadratic twist by the non-trivial character χ of $Gal(L/K)$ and A' be the dual variety of A. Then*

$$\frac{R(A/K)R(A^\chi/K)}{R(A/L)} = \frac{1}{\#\widehat{\mathrm{H}}^0(G, A'(L))\#\mathrm{H}^1(G, A(L))}.$$

Notation. Write M_t for the torsion subgroup of group M. Denote the quotient group M/M_t by M_f.

Lemma 7.39.

$$\frac{\#\mathrm{H}^1(G, A(L))}{\#\mathrm{H}^1(G, A(L)_t)} = \frac{\#A^\times(K)_f/(1+\sigma)A^\times(L)_f}{\#A(L)_f^G/A(K)_f}.$$

Proof. From the following short exact sequence

$$0 \longrightarrow A(L)_t \longrightarrow A(L) \longrightarrow A(L)_f \longrightarrow 0,$$

we have the long exact sequence

$$\begin{aligned} 0 \longrightarrow A(K)_t \longrightarrow A(K) \longrightarrow A(L)_f^G \longrightarrow \mathrm{H}^1(G, A(L)_t) \longrightarrow \\ \longrightarrow \mathrm{H}^1(G, A(L)) \longrightarrow \mathrm{H}^1(G, A(L)_f) \longrightarrow \mathrm{H}^2(G, A(L)_t) \longrightarrow \mathrm{H}^2(G, A(L)). \end{aligned}$$

In the above sequence, the first three terms can be shortened so that

$$0 \longrightarrow A(L)_f^G/A(K)_f \longrightarrow \mathrm{H}^1(G, A(L)_t) \longrightarrow \mathrm{H}^1(G, A(L)) \longrightarrow \cdots.$$

We can show that the kernel of the map $\mathrm{H}^2(G, A(L)_t) \longrightarrow \mathrm{H}^2(G, A(L))$ is isomorphic to $A^\times(L)_f^G/A^\times(K)_f$ by the following diagram:

$$\begin{tikzcd} & & \mathrm{H}^2(G, A(L)_t) \arrow[r] \arrow[d, "\cong"'] & \mathrm{H}^2(G, A(L)) \arrow[d, "\cong"'] \\ 0 \arrow[r] & A^\times(L)_f^G/A^\times(K)_f \arrow[r] & \mathrm{H}^1(G, A^\times(L)_t) \arrow[r] & \mathrm{H}^1(G, A^\times(L)). \end{tikzcd}$$

Thus we have the exact sequence

$$\begin{aligned} 0 \longrightarrow A(L)_f^G/A(K)_f \longrightarrow \mathrm{H}^1(G, A(L)_t) \longrightarrow \mathrm{H}^1(G, A(L)) \\ \longrightarrow \mathrm{H}^1(G, A(L)_f) \longrightarrow A^\times(L)_f^G/A^\times(K)_f \longrightarrow 0. \end{aligned}$$

Then

$$\begin{aligned}
\frac{\#\,\mathrm{H}^1(G,A(L))}{\#\,\mathrm{H}^1(G,A(L)_t)} &= \frac{\#\,\mathrm{H}^1(G,A(L)_f)}{\#A(L)_f^G/A(K)_f \cdot \#A^\chi(L)_f^G/A^\chi(K)_f} \\
&= \frac{\#A^\chi(L)_f^G/(1+\sigma)A^\chi(L)_f}{\#A(L)_f^G/A(K)_f \cdot \#A^\chi(L)_f^G/A^\chi(K)_f} \\
&= \frac{\#A^\chi(K)_f/(1+\sigma)A^\chi(L)_f}{\#A(L)_f^G/A(K)_f}.
\end{aligned}$$

□

Lemma 7.40.

$$\#\frac{A(L)_f}{A(L)_f^G \oplus A(L)_f^\chi} = \#\frac{(1-\sigma)A(L)_f}{2A(L)_f^\chi}.$$

Proof. From the commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & 0 & \longrightarrow & A(L)_f^\chi & \xrightarrow{1-\sigma} & 2A(L)_f^\chi & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A(L)_f^G & \longrightarrow & A(L)_f & \xrightarrow{1-\sigma} & (1-\sigma)A(L)_f & \longrightarrow & 0
\end{array}$$

by using the *Kernel-Cokernel* sequence, we have

$$0 \longrightarrow A(L)_f^G \longrightarrow A(L)_f/A(L)_f^\chi \longrightarrow \frac{(1-\sigma)A(L)_f}{2A(L)_f^\chi} \longrightarrow 0.$$

Therefore,

$$\frac{A(L)_f}{A(L)_f^G \oplus A(L)_f^\chi} \cong \frac{(1-\sigma)A(L)_f}{2A(L)_f^\chi}.$$

□

Remark 7.41. Through the map $\mathfrak{J}^{-1} : A^\chi \longrightarrow A$, we assume that $A^\chi(K)$ is a subgroup of $A(L)$.

Remark 7.42.

$$\#\frac{A(L)_f}{A(K)_f \oplus A^\times(K)_f} = \#\frac{A(L)_f}{A(L)_f^G \oplus A(L)_f^\times}\#\frac{A(L)_f^G}{A(K)_f}\#\frac{A(L)_f^\times}{A^\times(K)_f}.$$

Notation. Denote $\#\dfrac{A(L)_f}{A(K)_f \oplus A^\times(K)_f}$ by $\mathcal{Q}_f$.

Lemma 7.43.

$$\frac{\#\,\mathrm{H}^1(G, A(L))}{\#\,\mathrm{H}^1(G, A(L)_t)} \cdot \mathcal{Q}_f = 2^{\mathrm{rank}(A^\times(K))}.$$

Proof. From Lemmas 7.39 and 7.40 and Remark 7.42 we can prove this lemma as follows:

$$\begin{aligned}
&\frac{\#\,\mathrm{H}^1(G, A(L))}{\#\,\mathrm{H}^1(G, A(L)_t)}\#\frac{A(L)_f}{A(K)_f \oplus A^\times(K)_f} \\
&\qquad= \frac{\#A^\times(K)_f/(1+\sigma)A^\times(L)_f}{\#A(L)_f^G/A(K)_f}\#\frac{A(L)_f}{A(L)_f^G \oplus A(L)_f^\times}\#\frac{A(L)_f^G}{A(K)_f}\#\frac{A(L)_f^\times}{A^\times(K)_f} \\
&\qquad= \frac{\#A^\times(K)_f/(1+\sigma)A^\times(L)_f}{\#A(L)_f^G/A(K)_f}\#\frac{(1-\sigma)A(L)_f}{2A(L)_f^\times}\#\frac{A(L)_f^G}{A(K)_f}\#\frac{A(L)_f^\times}{A^\times(K)_f} \\
&\qquad= \#\frac{A(L)_f^\times}{A^\times(K)_f}\#\frac{A^\times(K)_f}{(1+\sigma)A^\times(L)_f}\#\frac{(1+\sigma)A^\times(L)_f}{2A(L)_f^\times} \\
&\qquad= \#\frac{A(L)_f^\times}{2A(L)_f^\times} = 2^{rank(A(L)^\times)} = 2^{rank(A^\times(K))}.
\end{aligned}$$

□

Definition 7.44. Let $\langle \cdot, \cdot \rangle_K : A(K) \times A'(K) \longrightarrow \mathbf{R}$ denote the canonical height pairing on $A(K) \times A'(K)$, and let $\langle \cdot, \cdot \rangle_L : A(L) \times A'(L) \longrightarrow \mathbf{R}$ denote the canonical height pairing on $A(L) \times A'(L)$.

Remark 7.45. Note that

$$\langle P, Q \rangle_L = [L : K] \cdot \langle P, Q \rangle_K,$$

for $P \in A(K)$ and $Q \in A'(K)$.

Lemma 7.46.

$$2^{rank(A(L))} \cdot \frac{R(A/K)R(A^{\chi}/K)}{R(A/L)} = \frac{Q_f Q'_f}{\#\mathrm{H}^1(G, A(L)_t)\#\mathrm{H}^1(G, A'(L)_t)}.$$

Proof. Let $P_1, P_2, \cdots, P_r \in A(K)$ be generators for the free part of $A(K)$, and let $P'_1, P'_2, \cdots, P'_r \in A'(K)$ be generators for the free part of $A'(K)$. Let $Q_1, Q_2, \cdots, Q_s \in A^{\chi}(K)$ be generators for the free part of $A^{\chi}(K)$, and let $Q'_1, Q'_2, \cdots, Q'_s \in A^{\chi}(K)$ be generators for the free part of $A'^{\chi}(K)$. Then

$$R(A/K) = \frac{\left|det(\langle P_i, P'_j\rangle_K)_{1\leq i,j\leq r}\right|}{\#A(K)_t \#A'(K)_t}.$$

$$R(A^{\chi}/K) = \frac{\left|det(\langle Q_i, Q'_j\rangle_K)_{1\leq i,j\leq s}\right|}{\#A^{\chi}(K)_t \#A'^{\chi}(K)_t}.$$

Let N be the subgroup of $A(L)$ which is generated by $\{P_1, \cdots, P_r, Q_1, \cdots, Q_s\}$. Let N' be the subgroup of $A'(L)$ which is generated by $\{P'_1, \cdots, P'_r, Q'_1, \cdots, Q'_s\}$. Then

$$R(A/L) = \frac{\left| det \begin{pmatrix} \langle P_i, P'_j\rangle_L & \langle P_i, Q'_k\rangle_L \\ \langle Q_l, P'_j\rangle_L & \langle Q_l, Q'_k\rangle_L \end{pmatrix}_{1\leq i,j\leq r,\ 1\leq l,k\leq s} \right|}{\#\frac{A(L)}{N}\#\frac{A'(L)}{N'}}.$$

Note that $\langle P_i, Q'_k\rangle_L = \langle Q_l, P'_j\rangle_L = 0$, and

$$\#\frac{A(L)}{N} = \#\frac{A(L)_f}{A(K)_f \oplus A^{\chi}(K)_f}\#A(L)_t = Q_f \cdot \#A(L)_t.$$

Thus

$$\begin{aligned}
R(A/L) &= \frac{\left|det(\langle P_i, P'_j\rangle_L)_{1\le i,j\le r}\right|}{Q_f \cdot \#A(L)_t} \cdot \frac{\left|det(\langle Q_i, Q'_j\rangle_L)_{1\le i,j\le s}\right|}{Q'_f \cdot \#A'(L)_t} \\
&= \frac{2^{rank(A(K))} \cdot \left|det(\langle P_i, P'_j\rangle_K)_{1\le i,j\le r}\right|}{Q_f \cdot \#A(L)_t} \cdot \frac{2^{rank(A^{\times}(K))} \cdot \left|det(\langle Q_i, Q'_j\rangle_K)_{1\le i,j\le s}\right|}{Q'_f \cdot \#A'(L)_t} \\
&= 2^{\mathrm{rank}(A(L))} \cdot \frac{R(A/K)\#A(K)_t\#A'(K)_t}{Q_f \cdot \#A(L)_t} \cdot \frac{R(A^{\times}/K)\#A^{\times}(K)_t\#A'^{\times}(K)_t}{Q'_f \cdot \#A'(L)_t}.
\end{aligned}$$

Therefore,

$$\begin{aligned}
2^{\mathrm{rank}(A(L))} \cdot \frac{R(A/K)R(A^{\times}/K)}{R(A/L)} &= \frac{\#A(L)_t}{\#A(K)_t\#A^{\times}(K)_t} \frac{\#A'(L)_t}{\#A'(K)_t\#A'^{\times}(K)_t} Q_f Q'_f \\
&= \frac{Q_f Q'_f}{\#\mathrm{H}^1(G, A(L)_t)\#\mathrm{H}^1(G, A'(L)_t)},
\end{aligned}$$

because $\dfrac{\#A(L)_t}{\#A(K)_t\#A^{\times}(K)_t} = \dfrac{1}{\#\mathrm{H}^1(G, A(L)_t)}$. □

Proof of Theorem 7.38

From Lemmas 7.43, and 7.46,

$$\begin{aligned}
&\#\mathrm{H}^1(G, A(L))\#\widehat{\mathrm{H}}^0(G, A'(L))\frac{R(A/K)R(A^{\times}/K)}{R(A/L)} \\
&\qquad = \#\mathrm{H}^1(G, A(L))\#\mathrm{H}^1(G, A'^{\times}(L))\frac{R(A/K)R(A^{\times}/K)}{R(A/L)} \\
&\qquad = \frac{2^{\mathrm{rank}(A^{\times}(K))}\#\mathrm{H}^1(G, A(L)_t)}{Q_f} \times \frac{2^{\mathrm{rank}(A'(K))}\#\mathrm{H}^1(G, A'^{\times}(L)_t)}{Q'_f} \\
&\qquad\quad \times \frac{1}{2^{\mathrm{rank}(A(L))}} \cdot \frac{Q_f Q'_f}{\#\mathrm{H}^1(G, A(L)_t)\#\mathrm{H}^1(G, A'(L)_t)} \\
&\qquad = 1,
\end{aligned}$$

because $\mathrm{rank}(A'(K)) = \mathrm{rank}(A(K))$ and $\#\mathrm{H}^1(G, A'^{\times}(L)_t) = \#\mathrm{H}^1(G, A'(L)_t)$. □

BIBLIOGRAPHY

[1] S. A. Amistur, *Finite subgroups of division rings*, Russian Math. Surveys **27**, no. 6 (1955), 361–386.

[2] M. I. Bashmakov, *The cohomology of abelian varieties over a number field*, Russian Math. Surveys **27**, no. 6 (1972), 25–70.

[3] B. Birch and H. P. F. Swinnerton-Dyer, *Notes on elliptic curves(I) and (II)*, J. Reine Angew. Math. **212**, **218** (1960,1965), 7–25, 79–108.

[4] A. Borel and J. P. Serre, *Théorèmes de finitude en cohomologie galoisienne*, Comment. Math. Helv. **39**, (1964), 111–164.

[5] S. Bloch, *A note on height pairings, Tamagawa numbers, and the Birch and Swinnerton–Dyer conjecture*, Inventiones Math. **58** (1980), 65–76.

[6] J. W. S. Cassels, *Arithmetic on curves of genus 1 (VIII). On the conjectures of Birch and Swinnerton-Dyer*, J. Reine Angrew. Math. **217** (1965), 180–189.

[7] F. Diamond, *On deformation rings and Hecke rings*, Ann. Math.(2) **144**, no. 1 (1996), 137–166.

[8] C. D. Gonzalez-Avilés, *On the conjecture of Birch and Swinnerton-Dyer*, Trans. Amer. Math. Soc. **349**, no. 10 (1997), 4181–4200.

[9] B. Gross, *On the conjecture of Birch and Swinnerton-Dyer for elliptic curves with complex multiplication*, In: Number Theory Related to Fermat's Last Theorem. Neal Koblitz (Eds.). Progress in Math. vol. **26**. Birkhäuser 1982.

[10] W. Happle, *Elimination in normrelatorenmoduln*, Ph.D. Thesis(1985), Karlsruhe.

[11] G. Hochschild and J-P. Serre, *Cohomology of Group Extension*, Trans. Amer. Math. Soc. **74** (1953), 110–134.

[12] E. Kani, *Relations between the genera and between the Hasse-Witt invariants of Galois coverings of curves*, Canad. Math. Bull. Vol. **28**(3)(1985), 321–327.

[13] E. Kani and M. Rosen, *Idempotent relations and factors of Jacobians* Math. Ann. **284**(1989), 307–327.

[14] E. Kani and M. Rosen, *Idempotent relations among arithmetic invariants attached to Number fields and algebraic varieties*, J. Number Theory **46** (1994), 230–254.

[15] M. Kida, *Galois descent and twists of an abelian variety*, Acta Arith. **73** (1995), 51–57.

[16] V. A. Kolyvagin, *On the structure of Selmer groups*, Math. Ann. **291**(1991), 253–259.

[17] S. Lang, *Abelian varieties*, Interscience, New York(1959).

[18] S. Lang, *Algebraic groups over finite fields*, Amer. J. Math. **78** (1956), 555–563.

[19] S. Lang and J. Tate, *Principal homogeneous spaces over abelian varieties*, Amer. J. Math., **80**(1958), 659–684.

[20] Liem Mai and M. Ram Murty, *A note on quadratic twists of an elliptic curve*, In: Elliptic curve and related topics. CRM Proc. Lecture Notes, vol. **4**, pp. 121–124.

[21] J. S. Milne, *On the arithmetic of abelian varieties*, Inventiones Math. **17** (1972), 177–190.

[22] J. S. Milne, *Arithmetic Duality Theorems*, Perspectives in Math. vol. **1**. Academic Press Inc. 1986.

[23] J. S. Milne, *Abelian varieties*, In: Arithmetic Geometry. G. Cornell and J. Silverman (Eds.). Springer–Verlag 1986.

[24] D. Mumford, *Abelian varieties*, Oxford U.P., London (1970).

[25] Hwasin Park, *Idempotent relations and the conjecture of Birch and Swinnerton-Dyer*, In: Algebra and Topology 1990 (Taejon, 1990), 97–125.

[26] Carl Riehm, *The Corestriction of Algebraic Structures*, Inven. Math. **11** (1970), 73–98.

[27] H. P. Riehm, *Über die gruppentheoretische structur der relationen zwischen relativnormabbildungen in endlichen Galoisschen Körpererweiterungen*, J. Number Theory **7** (1975), 49–70.

[28] M. I. Rosen, *Some confirming instances of the Birch-Swinnerton-Dyer conjecture over biquadratic fields*, In: Number Theory Proceedings of the First Conference of the Canadian Number Theory Association. R. A. Mollin (Eds.). Walter de Gruyter 1990.

[29] K. Rubin, *Tate–Shafarevich groups and L-functions of elliptic curves with complex multiplication*, Invent. Math. **89**(1987), 527–560.

[30] J. P. Serre, *Local Fields*, Grad. Texts in Math. **67**. Springer-Verlag 1979.

[31] J. P. Serre, *Facteurs locaux des fonctions zêta des variétés algébriques (définitions et conjectures)*, Séminaire Delange–Pisot–Poitou, 11^e année, n° 19 (1969/70).

[32] J. P. Serre and J. Tate, *Good reduction of abelian varieties*, Ann. of Math.(2) **88**(1968), 492–517

[33] J. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. **106**. Springer-Verlag 1986.

[34] G. Shimura, *Correspondances modulaires et les fontions ζ de courbes algébriques*, J. Math. Soc. Japan, **10**(1958), 1–28.

[35] G. Shimura, *Fontions automorphes et correspondances modulaires*, Proc. Intern. Congress Math., 1958, 330–338.

[36] G. Shimura and Y. Taniyama, *Complex multiplication of abelian varieties and its applications to number theory*, Publication of Math. Soc. Japan, **6**(1961).

[37] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Grad. Texts in Math. **151**. Springer-Verlag 1994.

[38] G. Steven, *An overview of the proof of fermat's last theorem*, In: Modular Forms and Fermat's Last Theorem. G. Cornell, J. Silverman and G. Steven (Eds.). Springer 1997.

[39] Y. Taniyama, *L-functions of number fields and zeta functions of abelian varieties*, J. Math. Soc. Japan, **9**(1957), 330–366.

[40] J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, In: Modular functions of one variable (IV). Lecture Notes in Math. vol. **476**, pp. 33-52. Springer-Verlag 1975.

[41] J. T. Tate, *Global class field theory*, In: Alg. Number Theory. J. W. S. Cassels and A. Fröhlich (Eds.). Academic Press 1967.

[42] J. Tate, *WC-group over p-adic fields*, In: Séminaire Bourbaki, 1957-58, exposé **156**.

[43] J. Tate, *Duality theorem in Galois cohomology over number fields*, Proc. Int. Cong. Math., Stockholm (1962), 288–295.

[44] J. Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, In: Séminaire Bourbaki, 1965-66, exposé **306**.

[45] J. Tate, *The arithmetic of elliptic curves*, Inven. math. **23**(1974), 170–206.

[46] R. L. Taylor and A. Wiles, *Ring theoretic properties of certain Hecke algebra*, Annals of Math **141**(1995), 553–572.

[47] C. Walter, *Brauer's class number relation*, Acta Arithmetic **XXXV**(1979), 33–40.

[48] A. Weil, *Adeles and algebraic groups*, Progress in math. vol. **23**, Birkhauser 1982.

[49] A. Weil, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. **55**(1949), 497–508.

[50] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Math **141**(1995), 443–551.