Università degli Studi di Padova

Dipartimento di Matematica "Tullio Levi-Civita"
Corso di Dottorato di Ricerca in Scienze Matematiche
Curricolo Matematica
Ciclo XXXV

On the p-part of the Birch and Swinnerton-Dyer conjecture for elliptic curves over totally real number fields

Coordinatore
Ch.mo Prof. Giovanni Colombo

Supervisore
Ch.mo Prof. Matteo Longo

Dottorando
Daniele Troletti

Abstract

Let A be a modular abelian variety of GL_2-type over a totally real number filed F, let p be an odd rational prime and let $\mathfrak{P}$ be an unramified prime above p in its ring of endomorphisms. In this thesis we start by proving a structure theorem for the Shafarevich-Tate of A. We then proceed to prove that the Kolyvagin's conjecture holds for A and we provide some results on the structure of the Selmer group and the parity of its rank. Last we restrict ourselves to the case where A is a modular elliptic curve and prove the $\mathfrak{P}$-part of the Birch and Swinnerton-Dyer conjecture for A.

Sommario

Sia A una varietà abeliana modulare di tipo GL_2 definita sopra un campo di numeri totalmente reale, p un primo reale dispari e sia $\mathfrak{P}$ un primo non ramificato sopra p nell'anello degli endomorfismi di A. In questa tesi iniziamo mostrando un teorema di struttura per il gruppo di Shafarevich-Tate di A. Successivamente dimostriamo la congettura di Kolyvagin per A e alcuni risultati sulla struttura del gruppo di Selmer e la parità del suo rango. Infine ci restringiamo al caso in cui A è una curva ellittica modulare e dimostriamo la $\mathfrak{P}$-parte della congettura di Birch e Swinnerton-Dyer per A.

Contents

Introduction

The Birch and Swinnerton-Dyer conjecture, a Millennium Problem of the Clay Institute, is one of the most fascinating subjects in modern number theory. Arising as an analogue of the Class Number Formula, it has become one of the most interesting open problems, in which algebraic geometry, complex analysis and p-adic methods converge to obtain evidences and partial results. This conjecture has its roots long away, in fact mathematicians have always been interested in finding all rational solutions to a polynomial equation with rational coefficients; this type of problems dates back to the time of Diophantus and the Birch and Swinnerton-Dyer conjecture is strictly related to this problem: the rational points of an elliptic curve defined over $\mathbb{Q}$ are indeed the rational solutions of a polynomial equation of degree 3 with nonzero discriminant.

To explain the conjecture, let $E/\mathbb{Q}$ be an elliptic curve. By the Mordell-Weil Theorem

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

where $E(\mathbb{Q})_{tors}$ is a finite (torsion) group and r is a positive integer that we call the arithmetic rank of E. We can attach to E an L-function $L(E,s)$ where s is a complex variable and this function converges if $\Re(x) > 3/2$. The modularity theorem of Wiles states that this complex L-function can be holomorphically extended to all $\mathbb{C}$. One may then look at the value of this function at $s = 1$. The first part of the Birch and Swinnerton-Dyer conjecture states that

$$\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}) = \mathrm{ord}_{s=1} L(E,s)$$

namely, that the order of vanishing of the L-function $L(E,s)$ at $s = 1$ is equal to the algebraic rank r of E. The more precise version (the second part) of the Birch and Swinnerton-Dyer conjecture offers a precise formula for the leading term of the Taylor expansion of $L(E,s)$ in terms of important algebraic invariants of E, and can therefore be seen as a complete analogue of the Class Number Formula mentioned above. More precisely, the quantitative part of the Birch and Swinnerton-Dyer conjecture states that

$$\frac{L^{(r)}(E,1)}{\Omega_E \mathrm{Reg}_E r!} = \frac{\prod_p c_p \cdot \#Ш(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{tors})^2}$$

where

- $\Omega_E = \int_{E(\mathbb{R})} \omega_E$ is the period of the holomorphic differential ω_E of the Riemann surface $E(\mathbb{R})$;
- Reg_E is the regulator of E, defined as the determinant of a matrix whose entries are the values of the Néron-Tate height pairing on a $\mathbb{Z}$-basis of $E(\mathbb{Q})/E(\mathbb{Q})_{tors}$;
- $Ш(E/\mathbb{Q})$ is the Shafarevich-Tate group of E. A deep conjecture of Tate states that this group is finite, but the result in its generality is still unknown;

- c_p is the Tamagawa number of E at p.

This conjecture was proven in the cases when the rank is zero, i.e. when there is only a finite number of rational points, or one. The main result is the following, which is due to contributions of several mathematicians during the last fifty years ([BBV16], [KL89], [Gro91], [SU14], [Zha14] and others).

Theorem. *Suppose that $L(E, s)$ has a simple zero at $s = 1$. Then $r = 1$ and the Birch and Swinnerton-Dyer formula is true for all primes p except possibly a finite number.*

This result use heavily the fact proven by Wiles that all elliptic curves over $\mathbb{Q}$ are modular, which means that there exists a morphism

$$\iota \colon X_0(N) \to E$$

from the modular curve $X_0(N)$ of level $\Gamma_0(N)$ where the integer N is the conductor of E. In particular, we can produce a modular form such that the representation attached to the Tate module T_pE of E coincides with the one attached to the modular form.

We extend this result to the more general settings of elliptic curves (and when possible also of abelian varieties) over totally real fields.

Let F be a totally real number field of degree g and let $K/\mathbb{Q}$ be a CM extension of $\mathbb{Q}$. Denote the ring of integers of F with $\mathcal{O}_F$ and fix a prime $\mathfrak{p}$ of $\mathcal{O}_F$ over the rational prime p. Let N be an integral ideal of F which is prime to the relative discriminant of K/F. This ideal factorizes as $N = N^-N^+$ where all factors in N^- (resp. N^+) are inert (resp. split) in K. We assume that N^- is square-free and that the number of its prime factors $\nu(N^-)$ has opposite parity than g. This is usually called Heegner hypothesis.

We consider a principally polarized modular abelian variety of GL_2 type A, thus A is associated with a Hilbert modular form f whose L-function is the same as the one attached to A. The modularity assumption combined with the Jacquet-Langlands correspondence means that there exists a modular parametrization defined over F

$$\iota \colon X \to A$$

where X is the Shimura curve attached to an indefinite quaternion algebra B of discriminant N^- defined over F. To better describe it, recall that this map generalizes the modular parametrization $X_0(N) \to E$ when $F = \mathbb{Q}$ and E is an elliptic curve over $\mathbb{Q}$. The direct analogue of modular curves over totally real fields are the Hilbert modular varieties, which are quotients of a product of complex upper half-planes by some Hilbert modular group of $\mathrm{GL}_2(\mathcal{O}_F)$; however it is sometimes easier to use Shimura curves. In our setting, we can use the Jacquet-Langlands correspondence to realize an adelic Hilbert modular form as a function from a quaternion algebra. In this more general framework we assume modularity, since, to the best of our knowledge, a full result is not available, but see [TW95], [Buz12], [FLS15] and [Le 14] for recent results.

The case of totally real fields $F \neq \mathbb{Q}$ presents the following crucial difference: as a Riemann surface, the Shimura curve $X(\mathbb{C})$ can be described as

$$X(\mathbb{C}) = \coprod_{i=1}^{h_F} \Gamma_i \backslash \mathcal{H}$$

i.e. as a finite disjoint union of quotients $\Gamma_i \backslash \mathcal{H}$ of the upper complex half-plane

$$\mathcal{H} = \{z \in \mathbb{C} \mid \Re(z) > 0\}$$

by arithmetic subgroups Γ_i. Here h_F denotes the class number of F. In particular each of these quotients is compact, which is false when $F = \mathbb{Q}$. Thus we do not have cusps for a Shimura curve.

Another important tool used to study this type of problems is the theory of Galois representations. Let $\mathcal{O}_A$ denotes the ring of endomorphism of A, E the fraction field of $\mathcal{O}_A$ and $\mathfrak{P} \subset \mathcal{O}_A$ a prime over p and M a positive integer. We can define the $\mathfrak{P}$-adic Tate module $T_{\mathfrak{P}}A$ of A and the associated representation $\rho\colon \mathrm{Gal}(\overline{F}/F) \to \mathrm{Aut}(T_{\mathfrak{P}}A \otimes \mathbb{Q})$. Since A is modular this representation coincides with the $\mathfrak{P}$-adic representation attached to f. In particular the field generated by the Hecke eigenvalues of f is the same as the fraction field of $\mathcal{O}_A$. We denote with $\rho_{\mathfrak{P}}$ the residual representation at $\mathfrak{P}$. We assume that

Assumption 1.

1. p is coprime with $6DN$,
2. $p \nmid [\mathcal{O}_E\colon \mathcal{O}_A]$ where $\mathcal{O}_E$ is the ring of integers of E,
3. p is unramified in E,
4. For all $\mathfrak{P}$ extending p in $\mathcal{O}_A$, the map $\rho_{\mathfrak{P}}$ surjects onto the subgroup

$$\{g \in \mathrm{GL}_2(\mathcal{O}_{A,\mathfrak{P}}) \mid \det(g) \in \mathbb{Z}_p^*\}.$$

Using the theory of complex multiplication we define Heegner points $P_{\mathfrak{n}}$ on the abelian variety A for products of admissible prime ideals $\mathfrak{n} \subset \mathcal{O}_F$, which we call Kolyvagin's primes (see Definition 2.2.7). We follow the construction introduced by Nekovar in [Nek07]. These points arise from the complex multiplication points of the Shimura curve X. In the case $F = \mathbb{Q}$ the CM points on modular curves have a simple interpretation as point representing couples of elliptic curves with CM by an order in a quadratic field, but this simple idea does not carry over to Shimura curves. In this case it is still possible to introduce Heegner points via the moduli description of the Shimura curve, however we prefer an algebraic approach based on the structure of Eichler orders of level N^+ in the quaternion algebra B (see Definition 2.2.3): indeed the description of the objects that the Shimura curves parametrize is more involved than in the modular curves case. The Kolyvagin formalism applied to the image via the Kummer map of the Heegner points $P_{\mathfrak{n}}$ gives classes $c_{\mathfrak{n}} \in H^1(K, A[\mathfrak{P}^M])$ and $d_{\mathfrak{n}} \in H^1(K, A)[\mathfrak{P}^M]$. We can use an explicit description to compute some interesting properties.

We can define the order at $\mathfrak{P}$ of a Heegner point $P_{\mathfrak{n}}$ in the following way: write $\mathfrak{P}^M \mid P_{\mathfrak{n}}$ whenever $P_{\mathfrak{n}} \in \mathfrak{P}^M A(K[\mathfrak{n}])$ where $K[\mathfrak{n}]$ is the ring class field of conductor $\mathfrak{n}$ over K. Define

$$\mathrm{ord}_{\mathfrak{P}}(P_{\mathfrak{n}}) = \max\big\{M \in \mathbb{Z}_+ \;\big|\; \mathfrak{P}^M \mid P_{\mathfrak{n}}\big\}.$$

Finally let

$$M_r = \min\{\mathrm{ord}_{\mathfrak{P}}(P_{\mathfrak{n}}) \mid \mathfrak{n} \in \mathscr{S}_r(\mathrm{ord}_{\mathfrak{P}}(P_{\mathfrak{n}}) + 1)\}$$

where $\mathscr{S}_r(M)$ denotes the set of products of r Kolyvagin's primes for M.

If we assume that P_1 has infinite order we can find a structure theorem for the Shafarevich-Tate group of A. In the case of elliptic curves over $\mathbb{Q}$ this was done by Kolyvagin (see [McC91]), where under similar hypothesis he proved

Theorem (Kolyvagin)**.** *If A is an elliptic curve over $\mathbb{Q}$, then*

$$Ш(A/K) = \bigoplus_i \left(\mathbb{Z}/p^{N_i}\mathbb{Z}\right)$$

where $N_i = M_{i-1} - M_i$.

Our first result is a generalization of this theorem to our setting which is the following

Theorem (Th. 3.2.1)**.** *Under Assumptions 1,*

$$Ш(A/K) = \bigoplus_i (\mathcal{O}_A/\mathfrak{P}^{N_i})$$

where $N_i = M_{i-1} - M_i$.

This theorem is the first important step to prove the Birch and Swinnerton-Dyer conjecture in our framework.

At this point we need to make several technical assumptions on the prime $\mathfrak{p}$ we consider, hence, in addition to the previous ones, we assume that A has good ordinary reduction at $\mathfrak{p}$ and that $\mathrm{ord}_{\mathfrak{p}}(\prod_{\mathfrak{q}} c_{\mathfrak{q}}) = 0$, where $c_{\mathfrak{q}}$ is the Tamagawa number of A at the prime $\mathfrak{q} \subset \mathcal{O}_F$. Furthermore, we assume that $p \nmid \#A(F)_{tors}$ and p does not divide the conductor of $\mathcal{O}_A$ in E. These conditions exclude only a finite number of primes $\mathfrak{p}$. Finally, we make some assumption on the representation ρ:

Assumption 2.

1. $\rho_{\mathfrak{P}}$ is irreducible; in this case we say that ρ is residually irreducible.
2. The residual representation $\rho_{\mathfrak{P}}$ ramifies at all prime in N^+ and all $\mathfrak{q} \mid N^-$ such that $N(\mathfrak{q}) \equiv 1 \mod p$. Furthermore, there are no prime $\mathfrak{q} \mid N^-$ such that $N(\mathfrak{q}) \equiv -1 \mod p$.
3. If N is not square-free, then the residual representation ramifies at least at one place dividing exactly N^- or at least at two places dividing exactly N^+.
4. For all prime ℓ such that $\ell^2 \mid N^+$ we have $H^1(F_\ell, \rho_{\mathfrak{P}}) = \rho_{\mathfrak{P}}^{D_\ell} = 0$ where D_ℓ is the decomposition group at ℓ in $\mathrm{Gal}(\overline{F}/F)$.

In this setting, we may define Ω_f to be the period of the Hilbert modular form f attached to A, which is up to a constant the Petersson inner product $\langle f, f\rangle_{Pet}$ (see Definition 1.2.10). We can also attach a period Ω_A to an abelian variety, which is computed integrating a Neron differential, which is only guaranteed to exist when $F = \mathbb{Q}$, or a generator of $H^0(A, \Omega_{A/F})$ if the Neron differential does not exist.

Here lies the main obstruction to an unconditional result: we need to compare these two periods. The problem is that the period Ω_f arise from the generalization of the Gross-Zagier formula (see [YZZ13]) and is related to the Hilbert modular form f and not to a quaternionic form. This result is known for elliptic curves over $\mathbb{Q}$ thanks to [PW11], [GP12] and [Pra09] or when A has complex multiplication by [Bla86], but the general case is still a conjecture due to Shimura in [Shi83] and Yoshida in [Yos94] (up to algebraicity). It is also strictly related to the Shimura's conjecture on the P-invariants, which is partially proven by Yoshida in *loc. cit.* For a deeper discussion on this topic see [Dis15, Chaper 9].

Finally, consider the Néron-Tate height $\hat{h}(P_1)$ of the Heegner point P_1; note that the point P_1 under our assumptions is non-torsion and so if it actually belongs to $A(F)$ and $A(F) \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}$, then $\hat{h}(P_1)$ is by definition the regulator $\mathrm{Reg}_{A/F}$. The main result of the thesis is the following

Theorem (Th. 6.2.3)**.** *Assume Assumptions 1 and 2 and that the periods* Ω_A *and* Ω_f*, where* f *is the Hilbert modular form associated to* A*, are equal in* $\mathbb{C}^\times$ *up to a p-adic unit in* $\mathbb{Q}^\times$*, then if* $L(A, s)$ *has a simple zero at* $s = 1$*, then*

$$\mathrm{ord}_{\mathfrak{P}}\left(\frac{L'(A,s)}{\Omega_A \mathrm{Reg}_{A/F}}\right) = \mathrm{lenght}_{\mathcal{O}_{A,\mathfrak{P}}} Ш(A/K).$$

In other words, this result proves the $\mathfrak{P}$-part of the Birch and Swinnerton-Dyer conjecture for abelian varieties over totally real fields for infinitely many primes p. Furthermore, if this theorem holds for every $\mathfrak{P} \subset \mathcal{O}_A$ above p, then we can descend it to obtain the p-part of the Birch and Swinnerton-Dyer conjecture in the rank one case for infinitely many p.

We now give an idea of the structure of the proof. The most important tool used is the level raising/rank lowering method. One application is due to Zhang in [Zha14] for elliptic curves over $\mathbb{Q}$. We say that a prime ideal ℓ of $\mathcal{O}_F$ is *admissible* if

- $\ell \nmid N D_{K/F} p$;
- ℓ is inert in K;
- $p \nmid N(\ell)^2 - 1$;
- the $\mathfrak{P}$-adic valuation is $v_{\mathfrak{P}}((N(\ell)+1)^2 - a_\ell^2) \geq 1$.

Here $D_{K/F}$ is the discriminant of K/F. Given our Hilbert modular form f of level $\mathfrak{N}$ we can choose a product $\mathfrak{m}$ of some admissible primes and using the first two item in Assumptions 2 in Theorem 4.1.4 we construct another Hilbert modular form $f_{\mathfrak{m}}$ with level $\mathfrak{N}\mathfrak{m}$ such that the residual representations are isomorphic. Associated to $f_{\mathfrak{m}}$ there is another abelian variety $A_{\mathfrak{m}}$ and in particular we get that the rank of the Selmer group of $A_{\mathfrak{m}}$ is lower than the one of $\mathrm{Sel}_{\mathfrak{P}}(A/K)$: this is proved in Theorem 5.2.1 which requires the last item of Assumptions 2. We use this idea to prove a parity result about the rank of the Selmer groups: if $L(A,s)$ has a simple zero at $s=1$ then the rank of the Selmer group must be odd.

Next we produce a suitable Kolyvagin system and in particular we prove that it is non-trivial. This is the main problem to resolve in order to use Heegner points and it is usually called the Kolyvagin conjecture. In order to achieve this goal we construct another structure theorem in the same spirit of first one concerning the Selmer group: in Theorem 5.4.6 we provide a triangular basis for an eigenspace of the Selmer group composed only by Kolyvagin classes; this last element is the key result to prove the non-vanishing of the Kolyvagin system. For this we study the relation between the localizations of the classes $c(\mathfrak{n})$ at various primes and prove some explicit reciprocity laws, among which the most important is stated in Theorem 4.2.5; here we need also the third item of Assumptions 2. This problem has been studied by many authors: see among others [BD05], [Lon06], [Tam21] and [Nek07]. We follow the way traced by Bertolini and Darmon in [BD05] and generalized to totally real field by Longo in [Lon12]. A technical tools used is the Ihara's lemma for Shimura curves, recently proved over totally real field by Manning and Shotton. These explicit reciprocity laws, the theorem on the structure of the Selmer group and the level raising/rank lowering method allow us to prove the Kolyvagin's conjecture, which finally leads us to the proof our main result.

Chapter 1

Modular Abelian Varieties

Let F be a totally real number field of degree g, and let K be a CM-extension of F.

In this chapter we introduce the notations and the basic constructions that we need in order to define the Heegner points and Kolyvagin's classes on modular abelian varieties over a totally real field.

1.1 Shimura curves

Let ϵ be the quadratic character associated to K/F. Let N be an integral ideal of F which is prime to the relative discriminant of K/F. This ideal factorizes as $N = N^- N^+$ where all factors in N^- (resp. N^+) are inert (resp. split) in K. We assume that N^- is square-free and that the number of its prime factors $\nu(N^-)$ has opposite parity rather than g. This is usually called Heegner hypothesis.

Let us fix $\xi\colon F \to \mathbb{R}$ a real embedding of F. We want to construct a Shimura curves associated to K and N which will be the principal ingredient in order to define the modular abelian varieties.

By our assumption on the parity of the number of factors of N^-, there exists a unique quaternion algebra B over F which is ramified only at the prime divisors of N^- and all the archimedean prime but ξ. Using this information about the ramification at the archimedean places we can fix an isomorphism

$$B \otimes_{\mathbb{Q}} \mathbb{R} \cong M_{2\times 2}(F_\xi) \oplus \mathbb{H}^{g-1}$$

where F_ξ is the completion of F at ξ and $\mathbb{H}$ denotes the real quaternions.

Let $\mathbb{A}_F$ denotes the adele ring of F, $\mathbb{A}_F^f$ the subring of finite adeles and $\mathbb{A}_F^\infty$ the infinite part.

We consider the group of units $B^\times$ which can be endowed with some more structure: there exists an algebraic group G such that $B^\times$ is the set of F-rational points of G, i.e. $G(F) = B^\times$. Hence, taking the projection over the first factor in the previous isomorphism, we get a map

$$G(\mathbb{A}_F^\infty) \cong (B \otimes_{\mathbb{Q}} \mathbb{R})^\times \to \mathrm{GL}_2(F_\xi)$$

which defines an action of $\mathbb{A}_F^\infty$, and so also of $B^\times$ on the union of the upper and lower half-plane $\mathcal{H}^\pm$. We denote by U_∞ the stabilizer of i for this action, and so we identify

$$\mathcal{H}^\pm \cong G(\mathbb{A}_F^\infty)/U_\infty.$$

If we consider the quotient map $G(\mathbb{A}_F^\infty) \to \mathcal{H}^\pm$ we can easily see that it admits a section s defined as

$$s(x+iy) \mapsto \left(\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}, 1, \dots, 1 \right).$$

Following [How04, Section 1.2], at every place $v \in N^-$ where B ramifies, $K \otimes_F F_v$ is a field, and so we can find an embedding $q\colon K \to B$. Considering the action of $B^\times$ onto $\mathcal{H}^\pm$ we find that there is only one point $w(q) \in \mathcal{H}^\pm$ which is fixed by all $q(\alpha)$ varying $\alpha \in K^\times$.

Let $\mathcal{O}_B$ be a maximal (Eichler) order of B containing $q(\mathcal{O}_K)$ and define an order

$$R = q(\mathcal{O}_K) + q(N^+)\mathcal{O}_B$$

of reduced discriminant N. Let $H \subset G(\mathbb{A}_F^f)$ be the image of order $\hat{R}^\times$ under the isomorphism $\hat{B}^\times \cong G(\mathbb{A}_F^f)$ and let Z denote the center of G, so $Z(\mathbb{A}_F^f) = \hat{F}^\times$. To this datum we can associate a Shimura curves X which has the associated Riemann surface (which we will also denote by X) given by

$$\begin{aligned} X(\mathbb{C}) &= G(F)\backslash \mathcal{H}^\pm \times G(\mathbb{A}_F^f)/Z(\mathbb{A}_F^f)H \\ &= B^\times \backslash \mathcal{H}^\pm \times \hat{B}^\times / \hat{F}^\times R. \end{aligned}$$

In the case that $F = \mathbb{Q}$ to have a Shimura curve we need to add some extra points, the so-called cusps; in this case we recover the classical modular curves $X_0(N)$. If $F \neq \mathbb{Q}$ then X is proper over $\mathrm{Spec}(F)$.

We denote by $[z, b]$ the point of $X(\mathbb{C})$, which are represented by a pair $(z, b) \in \mathcal{H}^\pm \times \hat{B}^\times$.

This curve is irreducible but not necessarily geometrically irreducible. We have an action of the normalizer of U on the curve $X(\mathbb{C})$ given by $\alpha[z, b] = [z, b\alpha^{-1}]$; we denote this automorphism by $J(\alpha)$. Let ν denote the reduced norm $\nu\colon G(\mathbb{A}_F) \to \mathbb{A}_F^\times$, then the reciprocity map

$$rec_F\colon \hat{F}^\times \to \mathrm{Gal}(F^{ab}/F)$$

induces an isomorphism $\mathrm{Gal}(F_X/F) \cong F^\times \backslash \mathbb{A}_F^\times / \nu(Z(\mathbb{A}_F)UU_\infty)$ where F_X is an abelian extension of F by class field theory.

In many applications we are interested in integral model of these Shimura curves and they were studied by many authors. When $F = \mathbb{Q}$ and $B = M_2(\mathbb{Q})$ the curve X is the classical modular curve $X_0(N)$ which is a coarse moduli space of elliptic curves with $\Gamma_0(N)$-structure. Katz and Mazur in [KM85] studied this specific case in full detail and were able to construct an integral model and later to compactify into a regular integral model proper over $\mathrm{Spec}(\mathbb{Z}_p)$ for some prime p where B does not ramify. If $B \neq M_2(\mathbb{Q})$ we can still use some similar techniques and we can view X as a coarse moduli space of abelian surfaces with quaternionic multiplication and some suitable level structure. Thanks to the works of Buzzard we can obtain a proper regular integral model. Things are more difficult when $F \neq \mathbb{Q}$ because they are no more moduli space of abelian varieties with some structure, in fact we loose altogether the moduli interpretation. However, we can again find integral models but it is not straightforward. The Shimura curve X can be related to another unitary Shimura curve that parametrizes some class of abelian varieties of dimension $4\,[F\colon \mathbb{Q}]$. This was first studied by Carayol in [Car86] and using his results following the methods of [CV05] we can find an integral model.

So we can find canonical models, whose existence was proved by Shimura.

Theorem 1.1.1. *There is a smooth projective variety X defined and connected over F whose complex point are isomorphic to $X(\mathbb{C})$ as a Riemann surface. The action of $\mathrm{Gal}(\overline{F}/F)$ on the*

geometric components of factor through $\mathrm{Gal}(F_X/F)$ *and agrees with the action determined by* $J(\alpha)$. *If* $x \in X(\mathbb{C})$ *is a CM-point then* x *is defined over* K^{ab} *and the action of* $\mathrm{Gal}(K^{ab}/K)$ *agrees with the one defined above by the reciprocity map.*

Proof. See [How04, Proposition 1.2.2]. □

We now define some correspondences on the Shimura curve. Let $\mathfrak{m}$ be an integral ideal of F coprime to N. For every prime $\ell \mid \mathfrak{m}$ the quaternion algebra B is split. Define $\Delta(\mathfrak{m})$ (resp. $\Delta(1)$) to be the set of elements of $\hat{\mathcal{O}}_B$ with component 1 away from $\mathfrak{m}$ and such that their determinant generates $\mathfrak{m}$ (resp. is a unit) at every prime divisor of $\mathfrak{m}$. We define the Hecke correspondence or operator $T_{\mathfrak{m}}$ on $X(\mathbb{C})$ as

$$T_{\mathfrak{m}}\,[z,b] = \sum_{\gamma \in \Delta(\mathfrak{m})/\Delta(1)} [z, b\gamma]\,.$$

The collection of these operators forms and algebra which is called the Hecke algebra of the Shimura curve. For more details on this we refer to [Nek07, section 1.12].

There is an interesting class of points on a Shimura curve which will be important in order to construct the Heegner points later. Our ramification assumptions on the algebra B imply that there is an F-embedding $\tau\colon K \hookrightarrow B$. We fix such embedding and extend it to the completion at a prime v as $\tau_v\colon K \otimes_F F_v \hookrightarrow B_v$ and to the ring of finite adeles $\hat{\tau}\colon \hat{K} \hookrightarrow \hat{B}$. We recall that we fixed an embedding $\xi\colon F \hookrightarrow \mathbb{R}$, we extend it to $\xi_1\colon \overline{K} \hookrightarrow \mathbb{C}$.

Lemma 1.1.2. *There is a unique point* $\mathbf{z} \in \mathbb{C}$ *with* $\mathrm{Im}(z) > 0$ *which is fixed by the action of* $\tau(K^\times) \subset B^\times \subset B^\times_{\xi_1} \xrightarrow{\sim} \mathrm{GL}_2(\mathbb{R})$ *and furthermore we have that* $\{\lambda \in B^\times \mid \lambda(\mathbf{z}) = \mathbf{z}\} = \tau(K^\times)$.

Proof. See [Nek07, Lemma 2.2]. □

Definition 1.1.3. The *Complex Multiplication points*, or CM-points, by the CM field K on the Shimura curve X are the point in the following set

$$\mathrm{CM}(X,K) = \left\{ x = [\mathbf{z}, b] \in X(\mathbb{C}) \mid b \in \hat{B}^\times \right\}$$

where $\mathbf{z}$ is the same as in Lemma 1.1.2.

Remark 1.1.4. The point $\mathbf{z}$ depends on the choice of the embedding τ, but since two different F-embedding of K into B are conjugated by an element of $B^\times$ by the Skolem-Noether theorem the set of CM-points does not depend on this choice.

Using the reciprocity law of class field theory we can find the field of definition of the CM-points: we have $\mathrm{CM}(X,K) \subset X(K^{ab})$, so we can define an action of the Galois group of the abelian closure of K on these points in the following way:

$$\mathrm{rec}_K(s)[z,b] = [z, \hat{\tau}(s)b] \qquad \forall\, s \in \hat{K}^\times$$

where $\mathrm{rec}_K\colon \hat{K}^\times \to \mathrm{Gal}(K^{ab}/K)$ is the reciprocity map. In particular, we have the following result

Proposition 1.1.5. *Let* $x = [z,b] \in CM(X,K)$ *and* $K(x)$ *the field of definition of* x *over* K. *Then there is an isomorphism* $\mathrm{rec}_K\colon K^\times \backslash \hat{K}^\times / \hat{\tau}^{-1}(bH\hat{F}^\times b^{-1}) \xrightarrow{\sim} \mathrm{Gal}(K(x)/K)$.

Proof. See [Nek07, Proposition 2.5]. □

This isomorphism can be written in a simpler way:

$$\mathrm{rec}_K \colon \hat{K}^\times / K^\times \hat{F}^\times Z \xrightarrow{\sim} \mathrm{Gal}(K(x)/K)$$

where $Z = \hat{\tau}^{-1}(bH\hat{\mathcal{O}}_F^\times b^{-1}) \subset \mathcal{O}_K^\times$ is an open compact subgroup of $\hat{\mathcal{O}}_K^\times$ containing $\hat{\mathcal{O}}_F^\times$. This Z is the preimage of $\hat{R}$ under the map $b^{-1}\tau b$ and is called the *endomorphism ring* of the CM-point x. Furthermore, this ring arises from an O_F-order in K of the form $\mathcal{O}_c = \mathcal{O}_F + c\mathcal{O}_K$ for a non-zero ideal $c \subset \mathcal{O}_F$ as $Z = \hat{\mathcal{O}}_c^\times$. The ideal c is called the *conductor* of x. The corresponding abelian extension $K[c]/K$ is the ring class field of K of conductor c. The reciprocity map rec_K is also compatible with the action of $\mathrm{Gal}(K/F)$.

It is important to analyze the behavior of primes of K in the ring class field. Each prime not dividing $\mathcal{O}_K$ is unramified in $K[c]/K$. If a prime of F which does not divides c and which is inert in K/F then it splits completely in $K[c]/K$.

In this setting it is more difficult to construct explicitly CM-points of a given conductor rather than in the classical case of modular curves, so we give an example. We will follow [How04]. Fix a prime ℓ which does not divide the discriminant $D_{K/F}$ nor N and an isomorphism of the localization of the quaternion algebra $B_\ell \cong M_2(F_\ell)$ in such a way that we can identify R_ℓ with $M_2(\mathcal{O}_{F,\ell})$. So we get the following explicit embedding if ℓ is split in K

$$\tau(\mathcal{O}_{K,\ell}) = \left\{ \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} \mid x, y \in \mathcal{O}_{F,\ell} \right\}$$

and the following one if ℓ is inert in K

$$\tau(\mathcal{O}_{K,\ell}) = \left\{ \begin{pmatrix} x & yu \\ y & x \end{pmatrix} \mid x, y \in \mathcal{O}_{F,\ell} \right\}$$

for some $u \in \mathcal{O}_{F,\ell}^\times$ not a square. Let π be an uniformizer of F_ℓ and let $h[\ell^k]$ be the element of B_ℓ such that under the previous isomorphism behaves as following:

$$h[\ell^k] \mapsto \begin{cases} \begin{pmatrix} \pi^k & 1 \\ & 1 \end{pmatrix} & \text{if } \ell \text{ splits in } K \\ \begin{pmatrix} \pi^k & \\ & 1 \end{pmatrix} & \text{if } \ell \text{ is inert in } K \end{cases}$$

We can view $h[\ell^k]$ as an element of $G(\mathbb{A}_F)$ with trivial component away from ℓ and extend h multiplicatively to a map on all integral ideals prime to $D_{K/F}N$. These points have nice properties and in particular we have that

Proposition 1.1.6. *There is a collection of CM-points $h[\mathfrak{m}] \in X(\mathbb{C})$ where $\mathfrak{m}$ runs over all prime ideal coprime with $D_{K/F}N$ such that $h[\mathfrak{m}]$ has conductor $\mathfrak{m}$ and as divisors on $X(\mathbb{C})$*

$$\left[\mathcal{O}_\mathfrak{m}^\times : \mathcal{O}_{\mathfrak{m}\ell}^\times\right] \mathrm{norm}_{K[\mathfrak{m}\ell]/K[\mathfrak{m}]}(h[\mathfrak{m}\ell]) = \begin{cases} T_\ell(h[\mathfrak{m}]) & \text{if } \ell \nmid \mathfrak{m} \text{ and is inert in } K \\ T_\ell(h[\mathfrak{m}]) - h[\mathfrak{m}]^{\sigma_\ell} - h[\mathfrak{m}]^{\sigma_\ell^*} & \text{if } \ell \nmid \mathfrak{m} \text{ and is split in } K \\ T_\ell(h[\mathfrak{m}]) - h[\mathfrak{m}/\ell] & \text{if } \ell \mid \mathfrak{m} \end{cases}$$

where σ_ℓ and σ_ℓ^* are the Frobenius automorphisms of the primes of K above ℓ and $\mathcal{O}_\mathfrak{m}$ is the order defined above.

Proof. See [How04, Proposition 1.2.1]. □

1.2 Hilbert modular forms

We fix a totally real number field F, an integral ideal $N \subset \mathcal{O}_F$ and a positive number n. Let $\mathcal{H}$ denote the complex upper half-plane. An element $M = (M_1, \ldots, M_n)$ in the group $\mathrm{SL}_2(\mathbb{R})^n$ acts on the product of n complex upper half-planes as

$$M(z_1, \ldots, z_n) = (M_1 z_1, \ldots, M_n z_n)$$

where the action of $\mathrm{SL}_2(\mathbb{R})$ on $\mathcal{H}$ is the classical one.

Proposition 1.2.1. *A subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{R})^n$ is discrete if and only if it acts discontinuously on $\mathcal{H}^n$.*

Proof. See [Fre90, Chapter I, Proposition 2.1]. □

Since the field F is totally real of dimension g we can consider the set of real embeddings $J_F = \{\xi_1, \ldots, \xi_g\}$ and construct an injective map

$$\begin{aligned} F &\to \mathbb{R}^g \\ a &\mapsto (\xi_1(a), \ldots, \xi_g(a)) \,. \end{aligned}$$

We call an element $a \in F$ totally positive if for all $\xi \in \mathbb{J}_F$ the number $\xi(a)$ is positive. For ease of notation we are going to identify a and the vector $(a_1, \ldots, a_g) = (\xi_1(a), \ldots, \xi_g(a))$. Thus, we obtain an embedding of the groups $\mathrm{GL}_2(F) \hookrightarrow \mathrm{GL}_2(\mathbb{R})^g$ and $SL_2(F) \hookrightarrow \mathrm{SL}_2(\mathbb{R})^g$.

Definition 1.2.2. The *Hilbert modular group* of F is

$$\Gamma_F = \mathrm{SL}_2(\mathcal{O}_F).$$

The group $\mathcal{O}_F$ under the embedding $F \to \mathbb{R}^g$ is a lattice in $\mathbb{R}^g$, hence it is discrete; this implies that also $\mathrm{SL}_2(\mathcal{O}_F)$ is discrete in $\mathrm{SL}_2(\mathbb{R})^g$, in particular by the above theorem it acts discontinuously on $\mathcal{H}^g$. Let $\Gamma \subset \mathrm{SL}_2(\mathbb{R})^g$ a subgroup, we say that it is *commensurable* with the Hilbert modular subgroup if the intersection $\Gamma \cap \Gamma_F$ has finite index in both Γ and Γ_F.

Definition 1.2.3. The Hilbert modular variety is

$$X_{\Gamma_F} = \Gamma_F \backslash \mathcal{H}^g \cup F \cup \{\infty\} \,.$$

Let Γ be a subgroup commensurable with Γ_F, then the Hilbert modular variety of level Γ is

$$X_\Gamma = \Gamma \backslash \mathcal{H}^g \cup F \cup \{\infty\} \,.$$

Proposition 1.2.4. *X_Γ is compact for all Γ commensurable with the Hilbert modular group.*

Proof. This follows from [Fre90, Chapter I, Theorem 3.6]. □

Following [Fre90] we can give the definition of cusps for a discrete subgroup Γ, which is similar to the classical one. In particular, the cusps of the Hilbert modular variety are the elements of $F \cup \{\infty\}$.

Proposition 1.2.5. *The Hilbert modular variety has only finitely many cusps classes and their number is the class number of F.*

Proof. This follows from [Fre90, Chapter I, Proposition 3.4] and [Fre90, Chapter I, Corollary 3.5.1]. □

Let $r = (r_1, \dots, r_g)$ be a vector of positive integers, for $M \in \mathrm{SL}_2(\mathbb{R})^g$ and $z \in \mathcal{H}^g$ we define

$$j_r(M, z) = \prod_{i=1}^{g} (c_i z_i + d_i)^{r_i}$$

where $M = (M_1, \dots, M_g)$ and each $M_i = \left(\begin{smallmatrix} a_i & b_i \\ c_i & d_i \end{smallmatrix}\right)$.

Definition 1.2.6. Let $\Gamma \subset \mathrm{SL}_2(\mathbb{R})^g$ be a discrete subgroup that is commensurable with the Hilbert modular group. A *Hilbert modular form* of weight r of level Γ is a holomorphic function

$$f \colon \mathcal{H}^g \to \mathbb{C}$$

such that

- $f(Mz) = j_r(M, z) f(z)$ for all $M \in \Gamma$;
- f is regular at the cusps, i.e. all the negative index coefficients of the Fourier expansion at the cusps are zero.

If f vanishes at all the cusps, we call f a cusp form.

We now define a norm on the space of Hilbert modular forms. We start by recalling some basic properties of complex measures.

Proposition 1.2.7. *Let $z \in \mathcal{H}^g$, $z = (x_1 + iy_1, \dots, x_g + iy_g)$. The measure*

$$d\omega_z = \frac{dv_z}{(y_1 \dots y_g)^2}$$

where dv_z denotes the usual Euclidean measure, is invariant under the transformation $z \mapsto Mz$ for all $M \in \mathrm{SL}_2(\mathbb{R})^g$. Furthermore, the space $\Gamma \backslash \mathcal{H}^g$ has finite volume with respect to this measure.

Proof. This is [Fre90, Chapter II, Remark 1.1 and 1.4]. □

Using this proposition we can prove that if f, g are two Hilbert modular forms, where at least one of them is cuspidal, the integral

$$\int_{\Gamma \backslash \mathcal{H}^g} f(z) \overline{g(z)} \left(\prod_{i=1}^{g} (y_i^{r_i}) \right) d\omega_z$$

exists.

Theorem 1.2.8. *The* Petersson pairing

$$\langle f, g \rangle = \int_{\Gamma \backslash \mathcal{H}^g} f(z) \overline{g(z)} \left(\prod_{i=1}^{g} (y_i^{r_i}) \right) d\omega_z$$

is a Hermitian inner product on the space of Hilbert modular cusp forms of weight r.

Proof. The proof is the same as in [Fre90, Chapter II, Remark 1.5]. □

We can generalize this construction and switch to an adelic setting in order to define the adelic Hilbert modular forms. We follow [Ros16] for this construction. A weight $r = (r_1, \dots, r_g)$ is called *parallel* if $r_1 = \dots = r_g$. Let GL_2 be the algebraic group defined over F of 2 by 2 invertible matrices and $\mathrm{GL}_2(\mathbb{A}_F^\infty)^+$ be the connected component of $\mathrm{GL}_2(\mathbb{A}_F^\infty)$ containing the identity; the group $\mathrm{GL}_2(\mathbb{A}_F^\infty)^+$ can be embedded as before in $\mathrm{SL}_2(\mathbb{R})^g$, therefore it acts on $\mathcal{H}^g$ by fractional linear transformations. Let K_∞ be the stabilizer of $z_0 = (i, \dots, i) \in \mathcal{H}^g$ under this action.

For $\mathfrak{n}$ an ideal of F we define the group

$$K_0(\mathfrak{n}) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\hat{\mathcal{O}}_F) \mid c \in \hat{\mathfrak{n}} \right\}.$$

Definition 1.2.9. Let r, w be two g-tuple of positive integers, we define the space of *adelic Hilbert modular forms* of level $K_0(\mathfrak{n})$ and weight r as the space of complex-valued functions f on $\mathrm{GL}_2(\mathbb{A}_F)$, holomorphic on $\mathrm{GL}_2(\mathbb{A}_F^\infty)$, such that

$$f(axu) = f(x) j_{r,w}(u_\infty, z_0) \text{ for all } a \in \mathrm{GL}_2(F), u \in K_0(\mathfrak{n}) K_\infty$$

where u_∞ denote the infinite part of u and

$$j_{r,w}(M, z) = \prod_{i=1}^{g} (\det M_i)^{-w_i} \cdot j_r(M, z).$$

We say that f is cuspidal if

$$\int_{F \backslash \mathbb{A}_F} f(ga) da = 0 \text{ for all } g \in \mathrm{GL}_2(\mathbb{A}_F)$$

with respect to the Haar measure.

Let $G = \mathrm{Red}_{F/\mathbb{Q}} GL_2(F)$, then the adelic Hilbert modular functions can be seen as function on the Shimura variety

$$X_{K_0(\mathfrak{n})} = G(\mathbb{Q}) \backslash G(\mathbb{A}_F) / K_\infty K_(\mathfrak{n}).$$

In order to have non-zero adelic Hilbert modular forms the elements r and w must be in a precise relation, in fact $r - 2w$ must be parallel; let us call $m \in \mathbb{Z}$ the value of the entry of this vector.

Definition 1.2.10. Let f, g be adelic Hilbert modular forms, the *Petersson inner product* is defined as

$$\langle f, g \rangle = \int_{X_{K_0(\mathfrak{n})}} f(x) \overline{g(x)} |\det(x)|^m \, d\mu_{K_0(\mathfrak{n})}(x)$$

where $\mu_{K_0(\mathfrak{n})}$ is a measure on $X_{K_0(\mathfrak{n})}$ which is induced from the standard measure on the Borel of $\mathrm{GL}_2(\mathbb{A}_F)$. For a precise construction of this measure see [GG12, Section 5.7].

By the strong approximation theorem, the Shimura variety $X_{K_0(\mathfrak{n})}$ can be decomposed as

$$X_{K_0(\mathfrak{n})} = \bigcup_{i=1}^{h^+} \Gamma_{\mathfrak{a}_i} \backslash \mathcal{H}^g$$

where h^+ is the narrow class number of F and $\Gamma_{\mathfrak{a}_i}$ are suitable subgroup indexed by a set of representatives of the narrow ideal class group. As a consequence, the function f decomposes

as $(f_1, \dots, f_{h^+})$, where each f_i is a Hilbert modular forms. Then the two definition of Petersson product are linked by

$$\langle f, g\rangle = \sum_{i=1}^{h^+} N(\mathfrak{a}_i)^m \langle f_i, g_i\rangle.$$

From now on we work with adelic Hilbert modular forms, so to avoid verbosity we drop the adjective adelic.

Using the Whittaker operator defined in [Zha01b, Section 3] we can find a Fourier expansion for f and we call $a_{\mathfrak{m}}(f)$ the $\mathfrak{m}$-th coefficient of f for $\mathfrak{m}$ an ideal of $\mathcal{O}_F$.

Let $\mathfrak{m}$ be a non-zero ideal of $\mathcal{O}_F$. Let $H(\mathfrak{m})$ denote the following subset of $\mathrm{GL}_2(\hat{F})$:

$$H(\mathfrak{m}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\hat{\mathcal{O}}_F) \mid (d, N) = 1, c \in N\hat{\mathcal{O}}_F, (ad - bc)\hat{\mathcal{O}}_F = \mathfrak{m}\hat{\mathcal{O}}_F \right\}.$$

Definition 1.2.11. The $\mathfrak{m}$-th *Hecke operator* $T(\mathfrak{m})$ on the space of cusp form of parallel weight k is defined by the formula

$$(T(\mathfrak{m})f)(z) = N(\mathfrak{m})^{k/2-1} \int_{H(\mathfrak{m})} f(hz)\, dh$$

where dh is the Haar measure on $\mathrm{GL}_2(\hat{F})$ such that $K_0(N)$ has volume 1.

Proposition 1.2.12. *The Fourier coefficients of $T(\mathfrak{m})f$ are given by the formula*

$$a_{\mathfrak{n}}(T(\mathfrak{m})f) = \sum_{a|(\mathfrak{m},\mathfrak{n})} N(a)^{k-1} a_{mn/a^2}(f).$$

Proof. This is [Zha01b, Proposition 3.1.4]. □

Let N' be a factor of N, let $d \in \mathrm{GL}_2(\hat{F})$ such that

$$d^{-1}K_0(N)d \subset K_0(N')$$

and let f' be a Hilbert modular form for $K_0(N')$ of the same weight of f. Then by [Zha01b, Section 3.1.6] the function $f'_d(z) = f'(dz)$ is a Hilbert modular form for $K_0(N)$.

Definition 1.2.13. The subspace of the space of cuspidal Hilbert modular forms of level $K_0(N)$ generated by these f'_d varying $N' \neq N$ is called the *space of old forms*. The space perpendicular to the space of old forms is called the space of *new forms*.

The space of new forms is generated by the *newforms*, i.e. Hilbert modular forms which are new, they are eigenforms for all Hecke operators and their first coefficient is 1. Then we have a strong multiplicity one theorem.

Theorem 1.2.14. *Let f_1, f_2 be two newforms of parallel weight k of levels $K_0(N_1)$ and $K_0(N_2)$ respectively, such that $a_{\mathfrak{p}}(f_1) = a_{\mathfrak{p}}(f_2)$ for all but finitely many primes $\mathfrak{p}$ of $\mathcal{O}_F$. Then $N_1 = N_2$ and $f_1 = f_2$.*

Proof. See [Zha01b, Theorem 3.1.7]. □

Let $\mathbb{T}$ denote the subalgebra of the $\mathbb{C}$-endomorphisms of the space of cuspidal Hilbert modular forms generated by the $T(\mathfrak{m})$ with $(\mathfrak{m}, N) = 1$.

Corollary 1.2.15. *For any linear map $\alpha\colon \mathbb{T} \to \mathbb{C}$, there is a unique Hilbert modular form f such that*

$$a_{\mathfrak{m}}(f) = \alpha(T(\mathfrak{m}))$$

whenever $(\mathfrak{m}, N) = 1$.

Proof. See [Zha01b, Corollary 3.1.8]. □

1.3 Automorphic forms on definite quaternion algebras

Let N an ideal of $\mathcal{O}_F$ like before but here we want the number of factors of N^- to have the same parity as the degree of F. Let B' a quaternion algebra over F which ramifies at all archimedean places and at the places dividing N^- and R be an Eichler order of level N^+.

Definition 1.3.1. The *Gross curve* of level R is the curve defined as a double coset

$$\mathfrak{X} = B'^{\times} \backslash \hat{B'}^{\times} / \hat{F}^{\times} R.$$

Remark 1.3.2. The set $\mathfrak{X}$ is a finite set, so why is called a curve? Since all primes dividing the discriminant of B' are inert in K there is an embedding $\tau \colon K \hookrightarrow B'$. By [BD96, Section 1.2], we have that the set of homomorphisms $\mathrm{Hom}(K, B')$ con be identified with $\mathcal{H}^{\pm}$, so we can consider the curve

$$\widetilde{\mathfrak{X}} = B'^{\times} \backslash \hat{B'}^{\times} \times \mathrm{Hom}(K, B) / \hat{F}^{\times} R.$$

For $g \in \mathfrak{X}$ let $\Gamma_g = g^{-1}(\hat{F}^{\times} R) g \cap B^{\times}$, then $\mathcal{H}^{\pm}/\Gamma_g$ are curves of genus zero over F and

$$\widetilde{\mathfrak{X}} = \bigcup_{g \in \mathfrak{X}} \mathcal{H}^{\pm}/\Gamma_g.$$

For more details on this construction see [BD96, Section 1.3].

We can now define some special function from the Gross curve to $\mathbb{C}$:

Definition 1.3.3. The space of weight two $\mathbb{C}$-valued *automorphic forms* for $B'^{\times}$ of level R and trivial central character is

$$S^{B'^{\times}}(R) = \{ f \colon \mathfrak{X} \to \mathbb{C} \}.$$

Let f adelic Hilbert cuspidal modular forms of parallel weight 2, trivial central character and level $K_0(N)$. We can transfer it via the Jacquet-Langlands correspondence to a unique (up to scaling) automorphic form

$$\phi \colon \mathfrak{X} \to \mathbb{C}$$

having the same eigenvalues as f under the action of the Hecke algebra. If the Hecke eigenvalues of f are contained in a ring $\mathcal{O}$, then ϕ can be normalized to take values in $\mathcal{O}$. See [JL70] for the general theory and [Lon12, Section 4] for an application to our case of definite quaternion algebras.

1.4 Modular abelian varieties

As in the previous section we fix a real number field F, an integral ideal $N \subset \mathcal{O}_F$ such that either $[F \colon \mathbb{Q}]$ is odd or $\mathrm{ord}_v(N)$ is odd for some finite place v of F, a CM-filed K/F of relative discriminant $D_{K/F}$ which we assume satisfies the weak Heegner hypothesis, ϵ the quadratic character associated to the extension K/F. Let $\mathbb{T}$ denote the Hecke algebra for the Hilbert modular forms of level N. Let f be a Hilbert modular newform of level N and parallel weight 2 on $\mathbb{A}_F$ we can consider the map

$$\begin{aligned} \lambda_f \colon \mathbb{T}_N &\to \overline{\mathbb{Q}} \\ T &\mapsto a_1(Tf) \end{aligned}$$

We denote its kernel by $\mathcal{I}_f$. This homomorphism surjects onto the coefficient ring of f which is a finitely generated $\mathbb{Z}$-module and its field of fractions is hence a real number field. In particular

since the action of the absolute Galois group of F commutes with the Hecke operators action f^σ is again a Hilbert newform for all $\sigma \in \mathrm{Gal}(\overline{F}/F)$, in particular all its coefficients are real. So the field of coefficients E of f is a totally real number field.

Let X be the canonical model over F of the complex Shimura curve $X(\mathbb{C})$ defined beforehand. This curve splits into its irreducible geometric components over a field F_X, so $X \times_F F_X = \coprod X_i$. By [How04, Section 1.3] we have that every field L/F with $X(L) \neq \emptyset$ must contain F_X. Let us fix one of the irreducible components and we call it X_0. We define J_X to be the abelian variety over F obtained by the restriction of scalars of $\mathrm{Jac}(X_0)$ from F_X to F. J_X has good reduction away from N and for every algebraic extension L/F with $X(L) \neq \emptyset$

$$J_X(L) = \prod_i \mathrm{Jac}(X_i)(L) = \prod_i \mathrm{Pic}^0(X_i \times_{F_X} L).$$

We denote by $\mathbb{T}_X$ the $\mathbb{Q}$-algebra generated by the Hecke operators acting on J_X.

Using the Jacquet-Langlands correspondence for every algebra homomorphism $\alpha\colon \mathbb{T}_X \to \mathbb{C}$ we can find a level N parallel weight 2 Hilbert newform f such that $\alpha(T) = \lambda_f(T)$, so we can associate to every maximal ideal of $\mathbb{T}_X$ a Galois conjugacy class of Hilbert newforms and also we can provide a surjective map $\mathbb{T} \to \mathbb{T}_X$ which endows the Lie algebra of J_X with an action of $\mathbb{T}$. This follows from [Zha01b, Theorem 3.2.1] and the construction in [How04, Section 1.3].

Theorem 1.4.1. *There is an isogeny $J_X \to \bigoplus_\phi A_\phi$ where the sum is over all conjugacy classes of Hilbert newform of parallel weight 2 and level dividing N and the A_ϕ are abelian varieties, such that the induced map on Lie algebras is $\mathbb{T}$-equivariant. If ϕ is of level exactly N then Lie(A_ϕ) is free of rank 1 over $F_\phi \otimes_{\mathbb{Q}} \mathbb{C}$. Furthermore, for each ϕ there is an equality of L-functions*

$$L_N(s, A_\phi) = \prod_{\sigma\colon F_\phi \hookrightarrow \mathbb{C}} L_N(s, \phi^\sigma)$$

where the subscript N means that the Euler factor at primes dividing N is removed.

Proof. See [How04, Theorem 1.3.1]. □

The A_ϕ of this theorem are the abelian varieties associated to the Hilbert newform ϕ.

Definition 1.4.2. An abelian variety A is called a *modular abelian variety* if it admits a surjective morphism from J_X.

We now define and embedding of X into J_X which will be very useful in the next sections. In the classical case we would use the cusps, but there are none in our setting, so we need something more subtle. We use the Hodge class $\xi \in \mathrm{Pic}(X)$: the unique up to a constant multiple class whose degree is constant on each geometric component and which satisfies $T_{\mathfrak{m}}\xi = \deg(T_{\mathfrak{m}})\xi$ for every Hecke operator with $\mathfrak{m}$ prime to $D_{K/F}N$. In our case the Hodge class is simply the canonical divisor on each geometric component. Let $X(\mathbb{C}) = \bigcup_i X_i(\mathbb{C})$ the decomposition of X into connected components and let ξ_i the restriction of ξ to X_i. Let d_i the degree of ξ_i. There is a unique morphism $X \to J_X$ defined over F such that on complex point it takes $p_i \in X_i(\mathbb{C})$ to the divisor $d_i p_i - \xi_i \in J_X(\mathbb{C})$. Hence we have a map also from X to the abelian variety: $X \to J_X \to A_\phi$.

1.5 Pairings

Let A be a modular abelian variety over any number field F. For a place v of F we call F_v the completion of F at v. Let p be a rational prime, $\mathfrak{p}$ an unramified prime of F above p and $\mathfrak{P}$ a prime of $\mathcal{O}_A$ above p.

For any abelian variety and for every m not dividing the characteristic of F we have the Weil pairing

$$e_m \colon A[m](\overline{F}) \times A^\vee[m](\overline{F}) \to \mu_m(\overline{F})$$

where $\mu_m(\overline{F})$ is the set of m-th root of the unity in $\overline{F}$ and $A^\vee$ is the dual abelian variety. This pairing is non-degenerate and commutes with the action of the absolute Galois group of F. In order to define this pairing we use the dual variety which is no more isomorphic in general to A, so given a polarization λ we can define a pairing on A

$$e_m^\lambda \colon A[m](\overline{F}) \times A[m](\overline{F}) \to \mu_m(\overline{F})$$

where $e_m^\lambda(a,b) = e_m(a, \lambda(b))$. This depends on the choice of the polarization. It becomes more simple if A is principally polarized.

For an explicit definition of the Weil pairing and more properties we refer to [Mil08, p. I.13].

For abelian varieties whose endomorphism ring is an order in a number field the e_m-pairing naturally generalizes to an $e_{\mathfrak{P}^M}$-pairing as follows:

Lemma 1.5.1. *For any abelian variety A/F whose endomorphism ring is an order $\mathcal{O}_A$ in an finite extension $E/\mathbb{Q}$, and for any unramified, invertible prime $\mathfrak{P}$ of $\mathcal{O}_A$ with residue characteristic p, the restriction of the e_{p^M}-pairing to the $\mathfrak{P}^M$-torsion of A defines a non-degenerate pairing*

$$e_{\mathfrak{P}^M} : A[\mathfrak{P}^M] \times A^\vee[\mathfrak{P}^M] \to \mu_{p^M}.$$

Moreover, if A admits a principal polarization, this pairing is alternating.

Proof. Let A be an abelian variety as above, let $\mathfrak{P}$ be an invertible prime of $\mathcal{O}_A$, and let $M > 0$ be an integer. Denote by p the characteristic of its residue field and let $\mathfrak{Q}$ be any another prime extending p. The $\mathfrak{Q}^M$-torsion points of $A^\vee$ carry the structure of an $\mathcal{O}_A$-module and of an $\mathcal{O}_A/\mathfrak{Q}^M$-module. By the Chinese remainder theorem, there exists an $x \in \mathfrak{P}^M$ such that x reduces to 1 modulo $\mathfrak{Q}^M$. In particular, x acts as trivially on $A^\vee_{\mathfrak{Q}^M}$. Let $a \in A_{\mathfrak{P}^M}$ and $b \in A^\vee[\mathfrak{Q}^M]$. Since the e_{p^M}-pairing is $\mathcal{O}_A$-bilinear, it follows that

$$e_{p^M}(a,b) = e_{p^M}(a,xb) = e_{p^M}(xa,b) = 1.$$

This shows that the $\mathfrak{P}^M$-torsion points of A are orthogonal to the $\mathfrak{P}^M$-torsion points of $A^\vee$ for all primes $\mathfrak{Q} \neq \mathfrak{P}$. Hence, the e_{p^M} pairing restricts to a pairing as described in the Lemma. As the e_{p^M} pairing is non-degenerate and alternating when A admits a principal polarization, this shows that its restriction to $A[\mathfrak{P}^M]$ is non-degenerate as well. □

Let v be a place of F, then the Weil pairing induces also a cup product in cohomology

$$H^1(F_v, A[m]) \smile H^1(F_v, A^\vee[m]) \to H^2(F_v, \mathbb{G}_m) \xrightarrow{inv_v} \mathbb{Q}/\mathbb{Z}$$

which is again non-degenerate and if F is Galois then it is $\mathrm{Gal}(F/\mathbb{Q})$-equivariant. If we assume A to be principally polarized we can forget the dual symbol on the second factor.

The group $H^2(F_v, \mathbb{G}_m)$ is the Brauer group of the multiplicative group $\mathbb{G}_m$ and it fits in a short exact sequence

$$0 \to \mathrm{Br}(F) \to \bigoplus_v \mathrm{Br}(F_v) \to \mathbb{Q}/\mathbb{Z} \to 0.$$

In this direct sum, v ranges over all places of F and the second map is given by taking the sum of the Hasse invariants as before. From the exact sequence we deduce that for $c \in H^1(F, A[m])$ and $c' \in H^1(F, A^\vee[m])$ we have

Lemma 1.5.2.

$$\sum_v \mathrm{inv}_v(c_v \smile c_v') = 0.$$

Proof. The sum of invariants of a global class is zero. See [McC91, Proposition 2.2]. □

Assume that A has multiplication by an order $\mathcal{O}_A$ in a finite extension $E/\mathbb{Q}$. Assume moreover that A admits a principal polarization. The cup product then becomes a pairing on $H^1(F, A[\mathfrak{P}^M])$ which acts on $A(F)/\mathfrak{P}^M A(F)$.

Proposition 1.5.3. *Assume that the abelian variety A admits a principal polarization, and let v be a non-archimdean place of F, coprime to $p\mathcal{O}_F$, such that A has good reduction at v. Then the image of $A(F_v)/\mathfrak{P}^M A(F_v)$ under δ is a maximal isotropic subgroup of $H^1(F_v, A[\mathfrak{P}^M])$. In particular, it gives rise to a non-degenerate pairing*

$$\langle \cdot, \cdot \rangle_v : H^1(F_v, A)[\mathfrak{P}^M] \times A(F_v)/\mathfrak{P}^M A(F_v) \to \mathbb{Q}/\mathbb{Z}.$$

Proof. Let v be such a place of F. By [Sil09, Lemma VIII.2.1], the image of δ is unramified. In particular, the Kummer sequence reduces to

$$0 \to A(F_v)/\mathfrak{P}^M A(F_v) \xrightarrow{\delta} H^1(F_v^{\mathrm{ur}}/F_v, A[\mathfrak{P}^M]) \to H^1(F_v^{\mathrm{ur}}/F_v, A)[\mathfrak{P}^M] \to 0,$$

where $H^1(F_v^{\mathrm{ur}}/F_v, A[\mathfrak{P}^M])$ is embedded into $H^1(F_v, A[\mathfrak{P}^M])$ via the inflation map. As A has good reduction at v, the group $H^1(F_v^{\mathrm{ur}}/F_v, A)$ vanishes [see Mil06, Chapter 1, Lemma 3.8], and hence δ is an isomorphism. We claim that this inflated group is isotropic. As the cup product commutes with inflation, the restriction of the cup pairing to $H^1(F_v^{\mathrm{ur}}/F_v, A[\mathfrak{P}^M])$ is given by a pairing

$$H^1(F_v^{\mathrm{ur}}/F_v, A[\mathfrak{P}^M]) \times H^1(F_v^{\mathrm{ur}}/F_v, A[\mathfrak{P}^M]) \to H^2(F_v^{\mathrm{ur}}/F_v, \mu_{p^M}).$$

But as v is coprime to p, it can be deduced from the Hochschild-Serre spectral sequence that latter group vanishes (see [Mil06, Lemma 2.9]). It follows that the inflated group us isotropic and hence so $\delta(A(F_v)/\mathfrak{P}^M A(F_v))$.

In order to prove maximality, it suffices to show that the group $H^1(F_v, A)[\mathfrak{P}^M]$ is isomorphic to $A(F_v)/\mathfrak{P}^M A(F_v)$. As $H^1(F_v^{\mathrm{ur}}/F_v, A)$ vanishes, it follows from inflation-restriction that restriction induces an isomorphism $H^1(F_v, A)[\mathfrak{P}^M] \xrightarrow{\sim} H^1(F_v^{\mathrm{ur}}, A)[\mathfrak{P}^M]^{\mathcal{G}}$, where $\mathcal{G}$ denotes the Galois group of F_v^{ur}/F_v. Moreover, as $A(F_v^{\mathrm{ur}})$ is p-divisible, the Kummer sequence induces an isomorphism $H^1(F_v^{\mathrm{ur}}, A[\mathfrak{P}^M]) \cong H^1(F_v^{\mathrm{ur}}, A)[\mathfrak{P}^M]$, and so an isomorphism of their $\mathcal{G}$-invariant subgroups. Since the $\mathfrak{P}^M$-torsion points of A are unramified over F_v, the action of the inertia group I of F_v on $A[\mathfrak{P}^M]$ is trivial. This gives rise to the natural identification $H^1(F_v^{\mathrm{ur}}, A[\mathfrak{P}^M]) = \mathrm{Hom}(I, A[\mathfrak{P}^M])$. Let l denote the characteristic of the residue field of F_v. It follows from ramification theory that the wild ramification group I^{wild} of F_v is a maximal pro-l subgroup of I, and since $l \neq p$ any homomorphism $f : I \to A[\mathfrak{P}^M]$ must therefore vanish on I^{wild}. Serre showed that the quotient I/I^{wild} is canonically isomorphic to the product $\prod_{q \neq l} \mathbb{Z}_q(1)$, where $\mathbb{Z}_q(1) := \varprojlim \mu_{q^n}$. For a proof of this see [Wei, Section 3.3] and [RS01, Section 2.1.2]. As any homomorphism f as above factors through this group, we conclude that $H^1(F_v, A)[\mathfrak{P}^M]$ is isomorphic to the group $\mathrm{Hom}(\mu_{p^M}, A[\mathfrak{P}^M])^{\mathcal{G}}$. The group of p^M-roots of unity is cyclic, hence this group of homomorphisms is naturally isomorphic to $A[\mathfrak{P}^M](F_v)$, and since multiplication by p is an isomorphism on $\mathcal{O}_v$, it follows from [Mil06, Lemma 3.3] that $A(F_v)/\mathfrak{P}^M A(F_v)$ is isomorphic to $A[\mathfrak{P}^M](F_v)$ as well. It follows that $\delta(A(F_v)/\mathfrak{P}^M A(F_v))$ is maximal isotropic.

Since it is maximal isotropic, it fits in a short exact sequence

$$0 \to \delta(A(F_v)/\mathfrak{P}^M A(F_v)) \to H^1(F_v, A[\mathfrak{P}^M]) \xrightarrow{\mathrm{ev}} \delta\left(A(F_v)/\mathfrak{P}^M A(F_v)\right)^* \to 0.$$

Hence consider the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A(F_v)/\mathfrak{P}^M A(F_v) & \xrightarrow{\delta} & H^1(F_v, A[\mathfrak{P}^M]) & \xrightarrow{\iota_*} & H^1(F_v, A)[\mathfrak{P}^M] & \longrightarrow & 0 \\ & & \| & & \| & & \uparrow \varphi & & \\ 0 & \longrightarrow & A(F_v)/\mathfrak{P}^M A(F_v) & \xrightarrow{\delta} & H^1(F_v, A[\mathfrak{P}^M]) & \xrightarrow{\mathrm{ev}} & \delta\left(A(F_v)/\mathfrak{P}^M A(F_v)\right)^* & \longrightarrow & 0. \end{array}$$

Here φ is the map making this diagram commutative. It is given by the composition $\iota_* \circ \mathrm{ev}^{-1}$, which is well-defined by exactness. Because all groups are finite, φ is an isomorphism. For any $y \in A(F_v)/\mathfrak{P}^M A(F_v)$ and $d \in H^1(F_v, A)[\mathfrak{P}^M]$, the pairing is now defined as

$$\langle d, y \rangle_v = \varphi^{-1}(d)(\delta(y)).$$

The non-degeneracy of the pairing follows immediately from the fact that φ is an isomorphism. The pairing is alternating as it is induced by the cup product. □

This pairing is also known as the Tate-pairing. In proving the previous proposition, we have also shown the following useful relation between the cup-product and the Tate pairing:

$$\langle \iota_{v*}(c), x \rangle_v = c \smile \delta(x) \tag{1.1}$$

1.6 Selmer and Shafarevich-Tate groups

Let α be an endomorphism of A, then

$$0 \to A[\alpha] \xrightarrow{\iota} A \xrightarrow{\alpha} A \to 0$$

Passing to cohomology we get a short exact sequence

$$0 \to A(F)/\alpha A(F) \xrightarrow{\delta} H^1(F, A[\alpha]) \to H^1(F, A)[\alpha] \to 0$$

where δ is the Kummer map. If we consider the localization at the places of F we get the following commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A(F)/\alpha A(F) & \xrightarrow{\delta} & H^1(F, A[\alpha]) & \xrightarrow{\iota_*} & H^1(F, A)[\alpha] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \prod_v A(F_v)/\alpha A(F_v) & \xrightarrow{\delta_v} & \prod_v H^1(F_v, A[\alpha]) & \xrightarrow{\iota_{v*}} & \prod_v H^1(F_v, A)[\alpha] & \longrightarrow & 0 \end{array}$$

Using this diagram we can define two fundamental groups associated to A:

Definition 1.6.1. Let A be an abelian variety over F and let α be an endomorphism of A. The *α-Selmer group* of A over F is given by

$$S_\alpha(A/F) = \ker\left(H^1(F, A[\alpha]) \to \prod_v H^1(F_v, A)[\alpha]\right).$$

The *Shafarevich-Tate group* of A over F is given by

$$Ш(A/F) = \ker\left(H^1(F, A) \to \prod_v H^1(F_v, A).\right)$$

Let $m \in \mathbb{Z}$, then we can consider the multiplication-by-m map α_m and we write $S_m(A/F)$ for $S_{\alpha_m}(A/F)$. By the snake lemma, the Selmer group and the Shafarevich-Tate group fit in the α-descent sequence

$$0 \to A(F)/\alpha A(F) \to S_\alpha(A/F) \to Ш(A/F)[\alpha] \to 0$$

Let p be a prime number that is unramified in E and invertible in $\mathcal{O}_A$, and let $\mathfrak{P}$ be any prime extending p. Define for any $M > 0$, the group of $\mathfrak{P}^M$-torsion points of A as

$$A[\mathfrak{P}^M] = \{P \in A \mid \alpha \cdot P = 0, \text{ for all } \alpha \in \mathfrak{P}^M\}$$

This group carries a natural structure of a torsion-free $\mathcal{O}_A/\mathfrak{P}^M$-module. Let $f_\mathfrak{P}$ denote the inertia degree of $\mathfrak{P}$ over p. As $\mathcal{O}_A/\mathfrak{P}^M$ is a finite $\mathbb{Z}/p^M\mathbb{Z}$-algebra with additive group isomorphic to $(\mathbb{Z}/p^M\mathbb{Z})^{f_\mathfrak{P}}$, these modules carry a natural structure of $\mathbb{Z}/p^M\mathbb{Z}$-module as well. This gives rise to a decomposition of $\mathbb{Z}/p^M\mathbb{Z}$-modules

$$A[p^M] = \prod_{\mathfrak{P}|\mathfrak{p}} A[\mathfrak{P}^M].$$

Multiplication by p^M is an isogeny of degree p^{2gM} on A, where g is the genus of A, hence the p^M-torsion group of A is free of rank $2g$ over $\mathbb{Z}/p^M\mathbb{Z}$. Notice that $A[p^M]$ moreover carries the structure of an $\mathcal{O}_A/p^M\mathcal{O}_A$-module. As $\mathcal{O}_A/p^M\mathcal{O}_A$ has rank g as a $\mathbb{Z}/p^M\mathbb{Z}$-module, that $A[p^M]$ is free of degree 2 as an $\mathcal{O}_A/p^M\mathcal{O}_A$-module. In particular, by the structure of the decomposition of this module, it follows that $A[\mathfrak{P}^M]$ is free of rank 2 over $\mathcal{O}_A/\mathfrak{P}^M$.

For any $m < M$, restriction of scalars equips $A[\mathfrak{P}^m]$ with an $\mathcal{O}_A/\mathfrak{P}^M$-module structure. Under this structure, multiplication by p gives rise to a short exact sequence of $\mathcal{O}_A/\mathfrak{P}^M$-modules

$$0 \to A[\mathfrak{P}] \to A[\mathfrak{P}^M] \xrightarrow{p} A[\mathfrak{P}^{M-1}] \to 0.$$

Remark 1.6.2. If $\mathfrak{P}$ is a principal ideal with generator π, there exists another natural short exact sequence

$$0 \to A[\mathfrak{P}] \to A[\mathfrak{P}^M] \xrightarrow{\pi} A[\mathfrak{P}^{M-1}] \to 0.$$

While the maps π and p are not the same in general, they induce the same map up to composition with an automorphism of $A[\mathfrak{P}^M]$.

Analogously to the rational case, the $\mathfrak{P}$-adic Tate module is defined as $T_\mathfrak{P} A = \varprojlim_M A[\mathfrak{P}^M]$, and by the same argument, this is a free $\mathcal{O}_\mathfrak{P}$-module of rank 2. Here $\mathcal{O}_\mathfrak{P}$ denotes the completion of $\mathcal{O}_A$ at $\mathfrak{P}$. Since p is invertible and unramified in $\mathcal{O}_A$, this is the ring of integers of a finite, unramified extension of $\mathbb{Q}_p$. As the Tate module is free of degree 2, its automorphism group is naturally isomorphic to $\mathrm{GL}_2(\mathcal{O}_\mathfrak{P})$. The absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $T_\mathfrak{P}$, and hence the $\mathfrak{P}$-adic Tate module gives rise to a representation

$$\rho_\mathfrak{P} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathcal{O}_\mathfrak{P}).$$

It follows from [Rib92, Lemma 3.1] that the determinant of this representation is in fact the p-th cyclotomic character

$$\chi_p : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{Z}_p^\times.$$

The Shaferevich-Tate group of A carries a natural structure of an $\mathcal{O}_A$-module. When it is finite, it is a torsion module and hence the structure of this group can be analyzed by looking at its $\mathfrak{P}$-primary parts, where $\mathfrak{P}$ ranges over the primes of $\mathcal{O}_A$. When $\mathcal{O}_A$ is a principal ideal domain,

this is immediate, but this is not the case in general. Similar to the previous decomposition, there is a natural decomposition of $\mathbb{Z}/p^M\mathbb{Z}$-modules

$$A(F)/p^M A(F) \cong \prod_{\mathfrak{P}|p} A(F)/\mathfrak{P}^M A(F).$$

As taking cohomology commutes with direct sums, we can define the Kummer map for a prime $\mathfrak{P}$ by taking the composition

$$A(F)/\mathfrak{P}^M A(F) \hookrightarrow A(F)/p^M A(F) \xrightarrow{\delta} H^1(F, A[p^M]) \xrightarrow{\text{proj}} H^1(F, A[\mathfrak{P}^M])$$

Explicitly, let $P \in A(F)$ and consider its reduction modulo $\mathfrak{P}^M A(F)$. By the decomposition above, there exists a $Q \in A(F)$ such that $Q \equiv P$ modulo $\mathfrak{P}^M A(F)$ and $Q \in \mathfrak{Q}^M A(F)$ for all other primes $\mathfrak{Q}$ dividing p. The image of P under the Kummer map is then the class generated by $\sigma \to \sigma(Q/p^M) - Q/p^M$. For any $\sigma \in \mathrm{Gal}(\overline{F}/F)$ this is indeed a $\mathfrak{P}^M$-torsion point, and the class is independent of a choice of Q. This map therefore gives rise to the short exact sequence

$$0 \to A(F)/\mathfrak{P}^M A(F) \xrightarrow{\delta} H^1(F, A[\mathfrak{P}^M]) \to H^1(F, A)[\mathfrak{P}^M] \to 0. \tag{1.2}$$

We define the $\mathfrak{P}^M$-Selmer group as

$$S_{\mathfrak{P}^M}(A/F) = \ker\left(H^1(F, A[\mathfrak{P}^M]) \to \bigoplus_v H^1(F, A)\right)$$

and retain the short exact sequence

$$0 \to A(F)/\mathfrak{P}^M A(F) \to S_{\mathfrak{P}^M}(A/F) \to Ш(A/F)[\mathfrak{P}^M] \to 0.$$

Let

$$H^1(F, A[\mathfrak{P}^\infty]) = \varinjlim H^1(F, A[\mathfrak{P}^M]), \qquad \text{and} \qquad S_{\mathfrak{P}^\infty}(A/F) = \varinjlim S_{\mathfrak{P}^M}(A/F),$$

where the direct limit is taken over all M. They carry a natural structure of $\mathcal{O}_\mathfrak{P}$-modules and we obtain a $\mathfrak{P}^\infty$-descent sequence of $\mathcal{O}_\mathfrak{P}$-modules

$$0 \to A(F) \otimes_{\mathcal{O}_A} F_\mathfrak{P}/\mathcal{O}_\mathfrak{P} \to S_{\mathfrak{P}^\infty}(A/F) \to Ш(A/F)_{\mathfrak{P}^\infty} \to 0, \tag{1.3}$$

where $F_\mathfrak{P}$ is the field of fractions of $\mathcal{O}_\mathfrak{P}$.

1.7 A pairing on the Tate-Shafarevich group

One of the main tool to study the Tate-Shafarevich group is the Cassels-Tate pairing, which is derived from the Tate pairing.

$$\langle \cdot, \cdot \rangle : Ш(A/F) \times Ш(A^\vee/F) \to \mathbb{Q}/\mathbb{Z}$$

We will define the pairing only on the $\mathfrak{P}$-primary part of the Shafarevich-Tate group. The construction for arbitrary integers m and n is identical.

Let M and $M' \in \mathbb{Z}$, and let $d \in Ш(A/F)[\mathfrak{P}^M]$ and $d' \in Ш(A^\vee/F)[\mathfrak{P}^{M'}]$ be two cohomology classes. Let $c' \in S_{\mathfrak{P}^{M'}}(A^\vee/F)$ be a lift of d' to the Selmer group of $A^\vee$. By definition of the

Shafarevich-Tate group, the reduction of d' modulo v vanishes at every place of F. Hence, via the Kummer sequence, we can choose a set $\{y'_v \in A(F_v)\}$ such that

$$\delta(y'_v) = c'_v.$$

Next assume that there exists a $d_1 \in H^1(F, A)[\mathfrak{P}^{M+M'}]$ such that $p^{M'} d_1 = d$. Multiplication by $p^{M'}$ sends $\mathfrak{P}^{M+M'}$-torsion elements to $\mathfrak{P}^{M}$-torsion elements. Since the reduction of d vanishes at every place of F, the reduction $d_{1,v}$ must necessarily be a $\mathfrak{P}^{M'}$-torsion point of $H^1(F_v, A)$. The Cassels-Tate pairing is now defined as

$$\langle d, d' \rangle = \sum_v \langle d_{1,v}, y'_v \rangle_v.$$

To see that this pairing is well-defined, let v be a valuation of F and assume that $y_v \in A(F_v)$ is another point such that $\delta(y_v) = c'_v$. Then $y'_v - y_v$ vanishes under δ and is therefore contained in $\mathfrak{P}^{M'} A(F_v)$. Write $y'_v - y_v = \alpha P$, as the pairing commutes with the action of $\mathcal{O}_A$, it follows that

$$\langle d_{1,v}, y'_v - y_v \rangle_v = \langle d_{1,v}, \alpha P \rangle_v = \langle \alpha \cdot d_{1,v}, P \rangle_v = 0,$$

since $d_{1,v}$ is $\mathfrak{P}^{M'}$-torsion. Hence this definition is independent of the choice of y'_v. To see that it is independent of the choice of d_1 consider another point $d_2 \in H^1(F, A)[\mathfrak{P}^{M+M'}]$ in the pre-image of d. The difference $d_1 - d_2$ is contained in $H^1(F, A)[\mathfrak{P}^{M'}]$, and hence originates from a global cocycle $c \in H^1(F, A[\mathfrak{P}^{M'}])$. Using the relation with the cup product, this implies that

$$\langle d_{1,v} - d_{2,v},\ y'_v \rangle_v = c_v \cup c'_v.$$

But this implies that the Cassels-Tate pairing vanishes here as the sum of Hasse invariants of a global class is zero.

Remark 1.7.1. It is not generally known if such a d_1 exists. By the clever use of cochains, the use of such a d_1 can be avoided, without altering the pairing. This as well as other interpretations are illustrated in [Mil06, Proposition 6.9] and the corresponding remarks. Other constructions can also be found in [PS99]. For the classes d considered in this thesis, such a d_1 always exists.

Note that any polarization ϕ on A gives rise to a pairing

$$\langle \cdot, \cdot \rangle_\phi : Ш(A/F) \times Ш(A/F) \to \mathbb{Q}/\mathbb{Z},$$
$$\langle d, d' \rangle_\phi = \langle d, \phi d' \rangle$$

Tate showed that this pairing is alternating if ϕ was a polarization arising from F-rational divisor. Such a polarization need not exist in general, and one can find examples where the order of the Shafarevich-Tate group is not a perfect square (see [PS99] or [Kei14]). Flach later showed that such a pairing is antisymmetric if ϕ is a principal polarization.

Chapter 2

Heegner points and classes

In this section we introduce the Heegner point and construct the associated derivative classes in a way that enables us to prove a structure theorem for the Tate-Shafarevich group. We follow the construction made by Nekovar in [Nek07]. We use the same notation of the previous section.

2.1 Čebotarev density theorem

From now on assume that K/F is a CM extension of F of discriminant $D = d_{K/F} \neq 3, 4$ and that N splits completely in K. Let A be a modular abelian variety such that its ring of $\mathbb{Q}$-rational endomorphism $\mathcal{O}_A$ is an order in a field E. Let N as in the first section and let p be a prime number such that

Assumption 2.1.1.

1. p is coprime with $6DN$,
2. $p \nmid [\mathcal{O}_E \colon \mathcal{O}_A]$ where $\mathcal{O}_E$ is the ring of integers of E,
3. p is unramified in E,
4. For all $\mathfrak{P}$ extending p in $\mathcal{O}_A$, the map $\rho_{\mathfrak{P}} : \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_2(\mathcal{O}_{A,\mathfrak{P}})$ surjects onto the subgroup
$$\{g \in \mathrm{GL}_2(\mathcal{O}_{A,\mathfrak{P}}) \mid \det(g) \in \mathbb{Z}_p^*\}.$$

Note that these conditions hold for all but finitely many primes p, [see LV17, Lemma 3.7]. Let $\mathfrak{P}$ be any prime of $\mathcal{O}_A$ extending p, and let $M > 0$ be an integer. Denote $L = K(A[\mathfrak{P}^M])$, and $\mathcal{O}_M = \mathcal{O}_A/\mathfrak{P}^M$.

Lemma 2.1.2. *There is a natural injection of* $\mathrm{Gal}(L/F)$*-modules*

$$H^1(K, A[\mathfrak{P}^M]) \hookrightarrow H^1(L, A[\mathfrak{P}^M]) = \mathrm{Hom}(\mathrm{Gal}(\overline{F}/L), A[\mathfrak{P}^M]).$$

Proof. As N splits completely in K, it is necessarily coprime to D. As by assumption p is coprime to D as well, the fields K and $F(A[p])$ are disjoint over F, hence so are the fields K and $F(A[\mathfrak{P}])$. Hence $\mathrm{Gal}(K(A[\mathfrak{P}])/K) \cong \mathrm{Gal}(F(A[\mathfrak{P}])/F)$. This group naturally injects in $\mathcal{G} = \mathrm{Gal}(L/K)$, and contains the cyclic subgroup $\mathcal{F}_p^*$ of order $p-1$. As $p-1$ is coprime to p it follows that $H^n(\mathcal{F}_p^*, A[\mathfrak{P}^M]) = 0$ for all $n \geq 1$. For $n = 0$, we have that $H^0(\mathcal{F}_p^*, A[\mathfrak{P}^M]) = (A[\mathfrak{P}^M])^{\mathcal{F}_p^*} = 0$ by [Gro91, Section 9]. Inflation-restriction now gives an exact sequence

$$0 \to H^n(\mathcal{G}/\mathcal{F}_p^*, (A[\mathfrak{P}^M])^{\mathbb{F}_p^*}) \to H^n(\mathcal{G}, A[\mathfrak{P}^M]) \to H^n(\mathcal{F}_p^*, A[\mathfrak{P}^M]).$$

By the above, the last term vanishes and as $(A[\mathfrak{P}^M])^{\mathcal{F}_p^*} = 0$ the first term vanishes as well, hence $H^n(\mathcal{G}, A[\mathfrak{P}^M]) = 0$ for all $n \geq 1$. Using inflation-restriction again, we obtain an exact sequence

$$0 \to H^1(\mathcal{G}, A[\mathfrak{P}^M]) \to H^1(K, A[\mathfrak{P}^M]) \to H^1(L, A[\mathfrak{P}^M])^{\mathcal{G}} \to H^2(\mathcal{G}, A[\mathfrak{P}^M]).$$

The vanishing of the outer terms now induces an isomorphism

$$H^1(K, A[\mathfrak{P}^M]) \cong H^1(L, A[\mathfrak{P}^M])^{\mathcal{G}},$$

which concludes the proof. □

Proposition 2.1.3. *Let $C \subset \mathrm{Hom}(\mathrm{Gal}(\overline{F}/L), A[\mathfrak{P}^M])$ be a finite $\mathcal{G}$-submodule, free of rank r over $\mathcal{O}_M$. Then there exists a finite Galois extension L_C/L such that there is a natural isomorphism*

$$\begin{aligned} \mathrm{Gal}(L_C/L) &\xrightarrow{\sim} \mathrm{Hom}_{\mathcal{G}}(C, A[\mathfrak{P}^M]), \\ \sigma &\mapsto \phi_\sigma \colon \alpha \mapsto \alpha(\sigma). \end{aligned}$$

Proof. Let C be given as in the proposition, let $\alpha_1, ..., \alpha_r$ generate C as an $\mathcal{O}_M$-module, and let $H = \bigcap \ker(\alpha_i)$. As each of the kernels in the intersection is an open normal subgroup of $\mathrm{Gal}(\overline{F}/L)$ of finite index, so is its intersection. Hence L^H is Galois over L, and we have a natural injection $\mathrm{Gal}(L^H/L) \hookrightarrow \mathrm{Hom}_{\mathcal{G}}(C, A[\mathfrak{P}^M])$. Thus it remains to show that the map

$$\mathrm{Gal}(\overline{F}/L) \to \mathrm{Hom}_{\mathcal{G}}(C, A[\mathfrak{P}^M])$$

is surjective. We proceed by induction on r. Observe that there is a natural isomorphism of free $\mathcal{O}_M$-modules of rank $2r$

$$\begin{aligned} \mathrm{Hom}_{\mathcal{G}}(C, A[\mathfrak{P}^M]) &\xrightarrow{\sim} \mathrm{Hom}_{\mathcal{G}}(C/\langle\alpha_1\rangle, A[\mathfrak{P}^M]) \times \mathrm{Hom}_{\mathcal{G}}(\langle\alpha_1\rangle, A[\mathfrak{P}^M]) \\ \phi &\mapsto (\phi_1, \phi_2) \end{aligned}$$

Where ϕ_1 and ϕ_2 are the natural projection and restriction. Consider the fields $L_{C/\langle\alpha_1\rangle}$ and $L_{\langle\alpha_1\rangle}$. By the induction hypothesis, their Galois groups over L can be viewed as subgroups of $\mathrm{Gal}(L_C/L)$ and they carry the structure of free $\mathcal{O}_M$-modules. Hence so does the Galois group G of the intersection $L_{C/\langle\alpha_1\rangle} \cap L_{\langle\alpha_1\rangle}$. We claim that G is trivial. The fact that the intersection is a subfield of $L_{\langle\alpha_1\rangle}$, shows that the group G is a submodule of $\mathrm{Gal}(L_{\langle\alpha_1\rangle}/L)$. Consequently the image of G under the evaluation map is contained in the $\langle\alpha_1\rangle$ component of $\mathrm{Hom}_{\mathcal{G}}(C, A[\mathfrak{P}^M])$. Since G is also a submodule of $\mathrm{Gal}(L_{C/\langle\alpha_1\rangle}/L)$, it follows from the same argument that the image of G is contained in the $C/\langle\alpha_1\rangle$ component of this group. The intersection of these components is trivial, hence by injectivity of the evaluation map, so is G. In particular, the fields have trivial intersection and are therefore linearly disjoint over L.

Let $\phi \in \mathrm{Hom}_{\mathcal{G}}(C, A[\mathfrak{P}^M])$. By the induction hypothesis, there exist $\sigma,\ \tau \in \mathrm{Gal}(\overline{F}/L)$ such that $\phi_1 = \phi_\sigma$ and $\phi_2 = \phi_\tau$. Since the fields are linearly disjoint, we can impose that $\sigma \in \ker(\alpha)$ and $\tau \in \bigcap_{i>1} \ker(\alpha_i)$. It follows that $\phi = \phi_{\sigma\tau}$, and thus the map is surjective.

To prove the statement for $r = 1$, we observe that evaluation at α induces an isomorphism

$$\mathrm{Hom}_{\mathcal{G}}(\langle\alpha\rangle, A[\mathfrak{P}^M]) \cong A[\mathfrak{P}^M].$$

Hence, let $R \in A[\mathfrak{P}^M]$, and consider the exact sequence

$$0 \to A[\mathfrak{P}^{M-1}] \to A[\mathfrak{P}^M] \xrightarrow{p^{M-1}} A[\mathfrak{P}] \to 0.$$

As α has order p^M, there must exist a $\sigma \in \mathrm{Gal}(\overline{F}/L)$ whose image has order p^M. Let Q denote the image of this σ. Without loss of generality we may assume that R has order p^M. As $A[\mathfrak{P}]$ is a simple $\mathcal{G}$-module, there exists an $\eta \in \mathcal{G}$ such that

$$\eta * p^{M-1}Q = p^{M-1}R.$$

As the action of $\mathcal{G}$ commutes with addition, it follows that $R - \alpha(\eta * \sigma) \in A[\mathfrak{P}^{M-1}]$. Surjectivity now follows inductively by repeating this procedure for $A[\mathfrak{P}^{M-1}]$. □

Let C be a free $\mathcal{O}_M$-submodule of $H^1(K, A[\mathfrak{P}^M])$ of rank r. We can identify C as a subgroup of $\mathrm{Hom}(\mathrm{Gal}(\overline{F}/L), A[\mathfrak{P}^M])$ by Lemma 2.1.2, and hence find a Galois extension L_C/L with Galois group isomorphic to $\mathrm{Hom}_{\mathcal{G}}(C, A[\mathfrak{P}^M])$. It is important to remark that these homomorphisms are in fact $\mathcal{O}_M$-linear homomorphisms. Write $\phi = \phi_\sigma$ for $\phi \in \mathrm{Hom}_{\mathcal{G}}(C, A[\mathfrak{P}^M])$ and let λ be any prime of K. Fix an extension λ_L of λ to L and denote its decomposition group in $\mathrm{Gal}(L_C/L)$ by $G(\lambda_L, L_C)$. Then for any $c \in C$,

$$c_\lambda = 0 \Leftrightarrow \phi_\sigma(c) = 0 \text{ for all } \sigma \in G(\lambda_L, L_C). \tag{2.1}$$

Fix $\tau \in \mathrm{Frob}(\infty)$, as its action on $A[\mathfrak{P}^M]$ satisfies the equation $\tau^2 = 1$, its eigenvalues are ± 1, and as the order of $A[\mathfrak{P}^M]$ is odd, $A[\mathfrak{P}^M]$ decomposes as a sum of its τ-eigenspaces,

$$A[\mathfrak{P}^M] \cong (A[\mathfrak{P}^M])^+ \oplus (A[\mathfrak{P}^M])^-.$$

As p is odd, the e_{p^M} pairing is non-degenerate, alternating, and preserved by τ. It is easy to verify that $(A[\mathfrak{P}^M])^+$ and $(A[\mathfrak{P}^M])^-$ are isotropic subgroups with respect to e_{p^M}. Observe that $A[\mathfrak{P}^M] \cong (\mathcal{O}_M)^2$ as a module. Since the order of an isotropic subgroup is bounded by the square root of the order of the group, it follows from the above decomposition that the eigenspaces must both be isomorphic to $\mathcal{O}_M$. Consider the group of τ-invariant $\mathcal{O}_M$-linear maps $h : H^1(K, A[\mathfrak{P}^M]) \to A[\mathfrak{P}^M]$. As the image of any such function must be τ-invariant, it is valued in the $+1$ eigenspace of τ. Hence we obtain

$$\mathrm{Hom}_{\mathcal{O}_M}(H^1(K, A[\mathfrak{P}^M]), A[\mathfrak{P}^M])^{\langle\tau\rangle} \cong \mathrm{Hom}_{\mathcal{O}_M}(H^1(K, A[\mathfrak{P}^M]), \mathcal{O}_M).$$

On the other hand, we can identify

$$H^1(K, A[\mathfrak{P}^M])^* = \mathrm{Hom}_{\mathbb{Z}}(H^1(K, A[\mathfrak{P}^M]), \mathbb{Q}/\mathbb{Z})$$

as a $\mathcal{O}_M$-module. A simple counting argument shows that both modules are isomorphic to $H^1(K, A[\mathfrak{P}^M])$ as modules. As both are modules of τ-invariant functions, this allows for a natural identification

$$\mathrm{Hom}_{\mathcal{O}_M}(H^1(K, A[\mathfrak{P}^M]), A[\mathfrak{P}^M])^{\langle\tau\rangle} \cong H^1(K, A[\mathfrak{P}^M])^*.$$

This identification allows us to associate a $\sigma \in \mathrm{Gal}(L_C/L)$ to any $\phi \in C^*$, and hence a collection of primes of F. This is illustrated in the following proposition.

Proposition 2.1.4. *Let $M > 1$ be an integer. Let C be a finite submodule of $H^1(K, A[\mathfrak{P}^M])$, identify C^* with $\mathrm{Hom}(C, A[\mathfrak{P}^M])^{\langle\tau\rangle}$, and let $\phi \in C^*$. There exist infinitely many prime l, unramified in L such that*

1. $\mathrm{Frob}(l) = \mathrm{Frob}(\infty)$ *in* $\mathrm{Gal}(L/F)$,
2. $\phi = \phi_{\mathrm{Frob}(\lambda')}$ *for some prime λ' of L extending l.*

Proof. Let $\sigma \in \mathrm{Gal}(L_C/L)$ be the automorphism such that $\phi = \phi_\sigma$. Since the order of $\mathrm{Gal}(L_C/L)$ is odd, and since σ is contained in the $+1$ eigenspace of τ, there exists a unique $\rho \in \mathrm{Gal}(L_C/L)$ such that $\sigma = \rho^\tau \rho$. Notice that τ acts by conjugation and is its own inverse, hence the expression simplifies to $\sigma = (\tau\rho)^2$. By the Čebotarev Density Theorem there exist infinitely many unramified primes l such that $\tau\rho \in \mathrm{Frob}(l)$. As $\tau\rho|_L = \tau$, condition 1 is satisfied. In particular, l has degree two in L/F. Thus, for any prime λ' of L above l, there exists a $\eta \in \mathrm{Frob}(l)$ such that $\eta^2 = \mathrm{Frob}(\check{\lambda})$. Thus, for appropriate choice of λ', we conclude that $\mathrm{Frob}(\lambda') = \sigma$. □

Let $c_1, ..., c_n \in H^1(K, A[\mathfrak{P}^M])$, we say that they are *independent* elements if any relation $\sum_i a_i c_i = 0$ with the $a_i \in \mathbb{Z}$ implies that $\mathrm{ord} c_i$ divides a_i for all $1 \leq i \leq r$.

Corollary 2.1.5. *Let $c_1, ..., c_n \in H^1(K, A[\mathfrak{P}^M])$ be independent elements of order p^{M_i} respectively. Then for all $0 \leq N_i \leq M_i$ there exist infinitely many primes l such that*

1. $\mathrm{Frob}(l) = \mathrm{Frob}(\infty)$ *in* $\mathrm{Gal}(L/F)$,
2. *For λ the unique prime of K extending l we have*

$$\mathrm{ord}\ c_{i,\lambda} = p^{N_i} \text{ for all } 1 \leq i \leq n.$$

Proof. Let $C = \langle c_1, ..., c_r \rangle$, as the c_i are independent, there exists a $\phi = \phi_\sigma \in C^*$ such that $\mathrm{ord}\phi(c_i) = p^{N_i}$. Thus using Proposition 2.1.4 we have that there exist infinitely many l such that $\mathrm{Frob}(l) = \mathrm{Frob}(\infty)$ in $\mathrm{Gal}(L/F)$ and $\sigma = \mathrm{Frob}(\lambda')$ for some λ' extending l. By condition 1, the prime l is inert in K, hence λ' extends λ as well. Choose l outside the finitely many prime numbers that ramify in L_C. The decomposition group $G(\lambda', L_C)$ is then cyclic and generated by σ. Thus we conclude from (2.1) that $\mathrm{ord}\ c_{i,\lambda} = \mathrm{ord}\ \phi_\sigma(c_i) = p^{N_i}$ which concludes the proof. □

2.2 Heegner points on modular abelian varieties

We consider a modular abelian variety A and let X be the associated Shimura curve and let $\iota\colon X \to A$ be the modular map. Let $x = [z, b]$ be a CM-point of X of conductor $c(x)$. We recall that $K[c(x)]$ is the smallest ring class field of K containing $K(x)$, the field of definition of the point x. We also fix a rational prime p, a prime $\mathfrak{p}$ of F and a prime $\mathfrak{P}$ of $\mathcal{O}_A$ over p. There is a finite set S of non-archimedean primes of F containing all the ones dividing N^- and such that we can decompose H (the image of R under the isomorphism $\hat{B}^\times \cong G(\mathbb{A}_F^f)$) as $H = H_S H^S$ where

$$H_S \subset \prod_{v \in S} B_v^\times$$

$$H^S = \prod_{v \notin S} H_v = \text{ a maximal compact subgroup of } G(\mathbb{A}_F^f)^S.$$

Let $I_0 \subset \mathcal{O}_K$ be the non-zero ideal given by

$$I_0 = \mathrm{lcm}\{(u-1) \mid u \in (\mathcal{O}_K^\times)_{tors}, u \neq 1\}.$$

Proposition 2.2.1. *If I is an ideal of $\mathcal{O}_F$ such that $I\mathcal{O}_K \nmid I_0$ and Z is a subgroup of $\hat{\mathcal{O}}_I^\times$, the completion of the order associated to I, then $K^\times \cap \hat{F}^\times Z = F^\times$ and $\mathcal{O}_K^\times \cap Z = \mathcal{O}_F^\times$.*

Proof. This follows from [Nek07, Proposition 2.10]. □

In order to work with Heegner points and classes we need to restrict the prime of F which are admissible.

Definition 2.2.2. Let $\mathscr{S} = \bigcup_{r\geq 0} \mathscr{S}_r$ be the following set of square-free ideals of $\mathcal{O}_F$:

$$\mathscr{S}_0 = \{(1)\}$$

$$\mathscr{S}_1 = \{\ell \text{ maximal ideal of } \mathcal{O}_F \mid \ell \text{ is inert in } K/F, \ell \notin S, \ell \nmid (p)c(x), \ell\mathcal{O}_K \nmid I_0\}$$

$$\mathscr{S}_r = \{\ell_1 \dots \ell_r \mid \ell_i \in \mathscr{S}_1 \text{ distinct } \forall\, i = 1, \dots, r\} \qquad r > 1$$

We now define a special class of CM points on X which are the main ingredient in the later definition of the Heegner point on A.

Definition 2.2.3. For each $\mathfrak{n} \in \mathscr{S}$ we define an element $h(\mathfrak{n})$ of $\hat{B}^\times$ as follows: $h((1)) = 1$, if $\mathfrak{n} = \ell \in \mathscr{S}_1$ then the ℓ part of H is $H_\ell = R(\ell)^\times$ for some maximal $\mathcal{O}_{F_\ell}$-order $R(\ell) \subset B_\ell$ and we take $h(\ell) \in R(l) \cap B_\ell^\times \subset B_\ell^\times \subset \hat{B}^\times$ such that it satisfies $\mathrm{ord}_\ell(\mathrm{nr}(h(\ell))) = 1$, finally if $\mathfrak{n} = \ell_1 \dots \ell_r \in \mathscr{S}_r$ with $r > 1$ and the $\ell_i \in \mathscr{S}_1$ distinct for all i then $h(\mathfrak{n}) = h(\ell_1) \dots h(\ell_r) \in \hat{B}^\times$.

Using the $h(\mathfrak{n})$ we define the CM-point

$$x(\mathfrak{n}) = [z, bh(\mathfrak{n})] \in \mathrm{CM}(X, K) \qquad \mathfrak{n} \in \mathscr{S}.$$

From the definition of conductor easily follows that the field of definition of $x(\mathfrak{n})$ is contained in the ring class field $K[c(x)\mathfrak{n}]$. We define the subfield $K(x(\mathfrak{n}))' \subseteq K(x(\mathfrak{n}))$ as

$$K(x(\mathfrak{n}))' = \begin{cases} K(x) & \text{if } \mathfrak{n} = (1) \\ K(x(\ell_1)) \dots K(x(\ell_r)) & \text{if } \mathfrak{n} = \ell_1 \dots \ell_r \text{ with } r > 1 \text{ and } \ell_i \in \mathscr{S}_1\ \forall\, i \end{cases}$$

Let $u(r) = 1$ for $r > 0$ and $u(0) = (K^\times \cap \hat{F}^\times Z \colon F^\times)$, where Z is the endomorphism ring of the point x. If we chose the CM-point x such that $c(x)\mathcal{O}_K \nmid I_0$ then by Proposition 2.2.1 we have that $u(0) = 1$. We assume this simplification from now on in view of Remark 2.2.8.

Definition 2.2.4 (Heegner points)**.** For each $\mathfrak{n} \in \mathscr{S}$ we define the Heegner point

$$y(\mathfrak{n}) = u(0)u(r)^{-1} \operatorname{Tr}_{K(x(\mathfrak{n}))/K(x(\mathfrak{n}))'} \iota(x(\mathfrak{n})) \in A(K(x(\mathfrak{n}))').$$

We can now analyze the behavior of the Galois group of the extension $K(x(\mathfrak{n}))'/K(x)$ and prove some interesting relations.

Proposition 2.2.5. *Let $G(\mathfrak{n}) = \mathrm{Gal}(K(x(\mathfrak{n}))'/K(x))$, then*

1. *For each $\ell \in \mathscr{S}_1$ the group $G(\ell)$ is cyclic of order $(N(\ell) + 1)/u(0)$;*
2. *For each $\mathfrak{n} = \ell_1 \dots \ell_r \in \mathscr{S}_r$ with $r > 1$ the map $G(\mathfrak{n}) \to G(\ell_1) \times \cdots \times G(\ell_r)$ is an isomorphism;*
3. *For each $\mathfrak{n} \in \mathscr{S}_r$ with $r \geq 0$ the degree becomes $[K(x(\mathfrak{n})) \colon K(x(\mathfrak{n}))'] = u(r)u(0)^{r-1}$.*

Proof. See [Nek07, Proposition 4.10]. □

This proposition and the relation between the CM-points imply that the Heegner points $x(\mathfrak{n})$ form an Euler system.

Theorem 2.2.6 (Euler system relations)**.** *Let $r \geq 0$ and $\mathfrak{n}\ell \in \mathscr{S}_{r+1}$ such that $\mathfrak{n} \in \mathscr{S}_r$ and $\ell \in \mathscr{S}_1$. We have that*

1. $\mathrm{Tr}_{K(x(\mathfrak{n}\ell))'/K(x(\mathfrak{n}))'}\, y(\mathfrak{n}\ell) = a_\ell y(\mathfrak{n})$ *where* a_ℓ *is the eigenvalue of the Hecke operator* $T(\ell)$ *acting on* f*;*

2. *For each prime* $\lambda \mid \ell$ *of* $(x(\mathfrak{n}\ell))'$ *we have*

$$y(\mathfrak{n}\ell) \equiv u(0)\,\mathrm{Frob}(\ell)_{\mathrm{arith}}\, y(\mathfrak{n}) \equiv u(0)\,\mathrm{Frob}(\ell)_{\mathrm{geom}}\, y(\mathfrak{n}) \pmod{\lambda}.$$

Let $\mathcal{O}_A$ be the ring of $\mathbb{Q}$-rational endomorphism of A. We define the set of Kolyvagin primes in a similar way of the set of admissible primes we used before.

Definition 2.2.7 (Kolyvagin primes)**.** Let $M \geq 1$ be an integer, let $\mathscr{S}_1(M)$ be the set of the maximal ideals of $\mathcal{O}_F$ such that

$$\ell \notin S, \qquad \ell \nmid (p)c(x)D_{K/F}, \qquad \ell\mathcal{O}_K \nmid I_0$$

and the conjugacy class of $\mathrm{Frob}(\ell)_{arith}$ in the Galois group $\mathrm{Gal}(K(x)(A[\mathfrak{P}^M])/F)$ coincides with the conjugacy class of the complex conjugation. Let us defines also

$$\mathscr{S}_0(M) = \{(1)\},$$
$$\mathscr{S}_r(M) = \{\ell_1 \dots \ell_r \mid \ell_i \in \mathscr{S}_1(M) \text{ distinct } \forall\, i = 1, \dots, r\} \qquad r > 1.$$

Finally define $\mathscr{S}(M) = \bigcup_{r\geq 1} \mathscr{S}_r(M)$.

The set $\mathscr{S}_1(M)$ is not empty and furthermore has positive density by the Čebotarev theorem. Let $\ell \in \mathscr{S}_1(M)$, then since $\ell \nmid (p)c(x)d_{K/F}$ and $\ell \notin S$ we have that the extension $K(x)(A[\mathfrak{P}^M])/F$ is unramified at ℓ by [Nek07, 5.2.2], so it makes sense to consider the conjugacy class of the Frobenius morphism. Furthermore ℓ is inert in K/F and so we have an inclusion $\mathscr{S}_1(M) \subset \mathscr{S}_1$. Finally by [Nek07, 5.2.5] we have the following important congruences in $\mathcal{O}_A$:

$$a_\ell \equiv 0 \pmod{\mathfrak{P}^M}, \qquad N(\ell) + 1 \equiv 0 \pmod{\mathfrak{P}^M}. \tag{2.2}$$

Remark 2.2.8. Here we use our hypothesis that $c(x)\mathcal{O}_K \nmid I_0$ because otherwise the first congruence would be modulo $\mathfrak{P}^{M+M_0}$ where $M_0 = \mathrm{ord}_{\mathfrak{P}}(u(0))$ and the second one modulo $u(0)\mathfrak{P}^M$. In the proof of our result this would give us trouble so we chose the CM-point x in such a way to avoid this problem.

We recall that for each $\ell \in \mathscr{S}_1(M)$ the group $G(\ell) = \mathrm{Gal}(K(x(\ell))/K(x)$ is cyclic so we can fix a generator σ_ℓ.

Definition 2.2.9 (Kolyvagin derivatives)**.** Let $\ell \in \mathscr{S}_1(M)$, then we define

$$\mathrm{Tr}_\ell = \sum_{i=0}^{|G(\ell)|-1} \sigma_\ell^i$$

$$\mathrm{D}_\ell = \sum_{i=0}^{|G(\ell)|-1} i\sigma_\ell^i \in \mathbb{Z}[G(\ell)]$$

If $\mathfrak{n} = \ell_1 \dots \ell_r \in \mathscr{S}_r(M)$ with the $\ell_i \in \mathscr{S}_1(M)$, we define

$$\mathrm{D}_\mathfrak{n} = \mathrm{D}_{\ell_1} \dots \mathrm{D}_{\ell_r} \in \mathbb{Z}[G(\ell_1)] \otimes \dots \otimes \mathbb{Z}[G(\ell_r)] = \mathbb{Z}[G(\mathfrak{n})]$$

and these elements satisfies the relation

$$(\sigma_\ell - 1)\,\mathrm{D}_\ell = |G(\ell)| - \mathrm{Tr}_\ell = N(l) + 1 - \mathrm{Tr}_\ell\,. \tag{2.3}$$

Definition 2.2.10. Let S be a set of representatives of $G(\mathfrak{n})$ in $\mathrm{Gal}(K(x(\mathfrak{n}))'/K)$ then

$$P_{\mathfrak{n}} = \sum_{\sigma \in S} \sigma(\mathrm{D}_{\mathfrak{n}}\, y_{\mathfrak{n}}).$$

In particular $P_1 = P_{(1)} = \mathrm{Tr}_{K(x)/K}\, y_{(1)}$.

Proposition 2.2.11. *Let $\mathfrak{n} \in \mathscr{S}_r(M)$ for some $r \geq 1$, then the image of the point $\mathrm{D}_{\mathfrak{n}}\, y(\mathfrak{n})$ in $A(K(x(\mathfrak{n}))') \otimes \mathcal{O}_{A,\mathfrak{P}}/\mathfrak{P}^M$ is contained in $(A(K(x(\mathfrak{n}))') \otimes \mathcal{O}_{A,\mathfrak{P}}/\mathfrak{P}^M)^{G(\mathfrak{n})}$, so by abuse of notation we can write*

$$\mathrm{D}_{\mathfrak{n}}\, y(\mathfrak{n}) \in \left(A(K(x(\mathfrak{n}))')/\mathfrak{P}^M A(K(x(\mathfrak{n}))')\right)^{G(\mathfrak{n})}.$$

Proof. If $\mathfrak{n} = \ell_1 \dots \ell_r$ with all $\ell_i \in \mathscr{S}_1(M)$, let $\mathfrak{m} = \ell_2 \dots \ell_r$. Decomposing $\mathrm{D}_{\mathfrak{n}} = \mathrm{D}_{\ell_1}\, \mathrm{D}_{\mathfrak{m}}$ we have that

$$(\sigma_{\ell_1} - 1)\, \mathrm{D}_{\mathfrak{n}} = (\sigma_{\ell_1} - 1)\, \mathrm{D}_{\ell_1}\, \mathrm{D}_{\mathfrak{m}} = (N(\ell_1) + 1 - \mathrm{Tr}_{\ell_1})\, \mathrm{D}_{\mathfrak{m}}$$

where the last equality follows from the relation 2.3. Using the Euler system relations and the congruences (2.2) we get that

$$(\sigma_{\ell_1} - 1)\, \mathrm{D}_{\mathfrak{n}}\, y(\mathfrak{n}) \equiv 0 \pmod{\mathfrak{P}^M}$$

so $\sigma_{\ell_1}\, \mathrm{D}_{\mathfrak{n}}\, y(\mathfrak{n}) \equiv \mathrm{D}_{\mathfrak{n}}\, y(\mathfrak{n}) \pmod{\mathfrak{P}^M}$. Since this can be done for all ℓ_i dividing $\mathfrak{n}$ we get that $\mathrm{D}_{\mathfrak{n}}\, y(\mathfrak{n})$ is fixed by all the σ_{ℓ_i} which are the generators of $G(\mathfrak{n})$. □

In particular also $P_{\mathfrak{n}} \in \left(A(K(x(\mathfrak{n}))')/\mathfrak{P}^M A(K(x(\mathfrak{n}))')\right)^{G(\mathfrak{n})}$.

2.3 Kolyvagin classes

We impose another condition on the CM-point x in order to simplify the exposition. We assume that the conductor of x is 1. Under this assumption the previous hypothesis that $c(x) \nmid I_0$ is satisfied.

When defining the Heegner points we worked over the smaller field possible $K(x(\mathfrak{n}))'$ and we can define the Kolyvagin classes over it as well, but it is not convenient for our goal. The usual definition of Heegner point and classes is over the ring class field and in order to get our results and interface with other work it is better to pursue this way. So we consider that for $\mathfrak{n} \in \mathscr{S}(M)$ by the definition of conductor of a CM-point we have $K(x(\mathfrak{n}))' \subseteq K(x(\mathfrak{n})) \subseteq K[\mathfrak{n}]$ and $K(x) \subseteq K[1]$, which is the Hilbert class field. By our assumption that the conductor of x is 1 we get that $y(\mathfrak{n}) \in A(K[\mathfrak{n}])$ and the same is true for $P_{\mathfrak{n}}$. We recall that there is an exception which is $P_1 \in A(K)$ due to the definition.

Remark 2.3.1. For $n \in \mathscr{S}(M)$ we have that $A[\mathfrak{P}^M](K[n]) = 0$ by [LV17, Proposition 3.9] as the Galois group $\mathrm{Gal}(K[n]/F)$ is solvable and under our Assumption 2.1.1 the same argument holds.

The exact sequence $\mathrm{Gal}(\overline{F}/F)$-modules

$$0 \to A[\mathfrak{P}^M] \to A(\overline{\mathbb{Q}}) \xrightarrow{\mathfrak{P}^M} A(\overline{\mathbb{Q}}) \to 0$$

yields an exact sequence in cohomology for all the extensions E/F

$$0 \to A(E) \otimes \mathcal{O}_{A,\mathfrak{P}}/\mathfrak{P}^M \xrightarrow{\delta} \mathrm{H}^1(E, A[\mathfrak{P}^M] \to \mathrm{H}^1(E, A)[\mathfrak{P}^M]) \to 0$$

and we can apply this construction for $\mathfrak{n}$ a product of admissible primes with $E = K$ and $E = K(x(\mathfrak{n}))$ taking the invariants under the action of $G(\mathfrak{n})$. So we get the following diagram:

$$\begin{array}{ccccc} A(K)\otimes \mathcal{O}_{A,\mathfrak{P}}/\mathfrak{P}^M & \longrightarrow & \mathrm{H}^1(K, A[\mathfrak{P}^M]) & \longrightarrow & \mathrm{H}^1(K,A)[\mathfrak{P}^M] \\ \downarrow & & \downarrow{\scriptstyle \mathrm{res}} & & \\ (A(K(x(\mathfrak{n}))')\otimes \mathcal{O}_{A,\mathfrak{P}}/\mathfrak{P}^M)^{G(\mathfrak{n})} & \xrightarrow{\delta_n} & \mathrm{H}^1(K(x(\mathfrak{n}))', A[\mathfrak{P}^M])^{G(\mathfrak{n})} & & \end{array}$$

where the vertical res map is the restriction map in cohomology. We want to find a natural lift of $\delta_{\mathfrak{n}}(P_{\mathfrak{n}} \pmod{\mathfrak{P}^M})$ under the restriction map res.

Let $\mathfrak{n} \in \mathscr{S}(M)$ be a fixed Kolyvagin prime.

Definition 2.3.2. Let $c_M(\mathfrak{n}) \in \mathrm{H}^1(K, A[\mathfrak{P}^M])$ be the unique natural lift of $\delta_{\mathfrak{n}}(P_{\mathfrak{n}} \pmod{\mathfrak{P}^M})$ and let $d_M(\mathfrak{n})$ the image of $c_M(\mathfrak{n})$ in $\mathrm{H}^1(K, A)$.

Lemma 2.3.3. *Let $Q_{\mathfrak{n}} \in A(K[\mathfrak{n}])$ be any point congruent to $P_{\mathfrak{n}}$ modulo $\mathfrak{P}^M$ and congruent to 0 modulo $\mathfrak{Q}^M$ for all other primes $\mathfrak{Q}$ lying above p. Then the cocycle*

$$\sigma \mapsto -\frac{(\sigma-1)Q_n}{p^M} + \sigma\frac{Q_n}{p^M} - \frac{Q_n}{p^M}$$

is a representative for $c_M(\mathfrak{n})$, where $\frac{(\sigma-1)Q_n}{p^M}$ is the unique p^M-division point of $(\sigma-1)Q_n$ in $A(K[\mathfrak{n}])$.

Proof. This proof is based on [Nek07, Propositions 5.9 and 5.10]. Let $Q_{\mathfrak{n}}$ be any such point, and observe that $\delta_{\mathfrak{n}}(P_{\mathfrak{n}}) \in H^1(K[n], A[\mathfrak{P}^M])$ is represented by the cocycle

$$\sigma \mapsto \sigma\frac{Q_{\mathfrak{n}}}{p^M} - \frac{Q_{\mathfrak{n}}}{p^M}.$$

The existence of the p^M-division point of $(\sigma-1)Q_{\mathfrak{n}}$ follows from the statement of Proposition 2.2.11 and the fact that $Q_{\mathfrak{n}} \in \mathfrak{Q}^M A(K[\mathfrak{n}])$ for all other primes $\mathfrak{Q} \mid p$. Since two distinct p^M-division points differ by a p^M-torsion point we have the uniqueness of the point. The term $\sigma \mapsto -\frac{(\sigma-1)Q_{\mathfrak{n}}}{p^M}$ is a cocycle. The expression given in the lemma is therefore a cocycle as well and it is easy to see that this cocycle takes values in $A[\mathfrak{P}^M]$. As the first term vanishes for all $\sigma \in \mathrm{Gal}(K(x(\mathfrak{n}))'/K)$, its restriction to $K[\mathfrak{n}]$ is precisely the representative of $\delta_{\mathfrak{n}}(P_{\mathfrak{n}})$ describe above. □

Corollary 2.3.4. *The class $d_M(n)$ is represented by the cocycle*

$$\sigma \mapsto -\frac{(\sigma-1)Q_{\mathfrak{n}}}{p^M}.$$

Corollary 2.3.5. *For all integer $M > 2$ and $\mathfrak{n} \in \mathscr{S}(M)$ we have*

$$pc_M(\mathfrak{n}) = c_{M-1}(\mathfrak{n}).$$

Proof. Let $Q_{\mathfrak{n}}$ be a point as described in Lemma 2.3.3, and write $c_M(\mathfrak{n})$ for the associated cocycle. As $(\sigma-1)Q_{\mathfrak{n}}$ has a unique p^M-division point in $A(K(x(\mathfrak{n})))$, it also has a unique p^{M-1}-division point. As multiplication commutes with the action of $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$, we obtain

$$\begin{aligned}(pc_M(\mathfrak{n}))(\sigma) &= -\frac{(\sigma-1)Q_{\mathfrak{n}}}{p^{M-1}} + p\sigma\frac{Q_{\mathfrak{n}}}{p^M} - p\frac{Q_{\mathfrak{n}}}{p^M} \\ &= -\frac{(\sigma-1)Q_{\mathfrak{n}}}{p^{M-1}} + \sigma\frac{Q_{\mathfrak{n}}}{p^{M-1}} - \frac{Q_{\mathfrak{n}}}{p^{M-1}} = c_{M-1}(\mathfrak{n})(\sigma).\end{aligned}$$

□

Write $\mathfrak{P}^M \mid P_{\mathfrak{n}}$ if $P_{\mathfrak{n}} \in \mathfrak{P}^M A(K[n])$, and define

$$\mathrm{ord}_{\mathfrak{P}}(P_{\mathfrak{n}}) = \max\{M \in \mathbb{Z}_+ \mid \mathfrak{P}^M \mid P_{\mathfrak{n}}\}.$$

Observe that $c_M(\mathfrak{n}) = 0$ if $\mathfrak{P}^M \mid P_n$. In fact for $M > \mathrm{ord}_{\mathfrak{P}}(P_{\mathfrak{n}})$ we have

$$\mathrm{ord} c_M(\mathfrak{n}) = p^{M - \mathrm{ord}_{\mathfrak{P}}(P_{\mathfrak{n}})} \tag{2.4}$$

whenever $c_M(\mathfrak{n})$ exists. Let

$$M_r = \min\{\mathrm{ord}_{\mathfrak{P}}(P_{\mathfrak{n}}) \mid \mathfrak{n} \in \mathscr{S}_r(\mathrm{ord}_{\mathfrak{P}}(P_{\mathfrak{n}}) + 1)\}.$$

Equivalently M_r is the smallest integer M such that there exists an $n \in S_r(M+1)$ for which the associated class $c_{M+1}(n)$ is non-trivial. These numbers will later shown to be bounded and decreasing, allowing us to give an explicit description of the Shafarevich-Tate group.

Let $\mathfrak{n} \in \mathscr{S}(M)$ and let $\ell \in \mathscr{S}_1(M)$ and $\mathfrak{m} \in \mathscr{S}(M)$ such that $n = \ell\mathfrak{m}$. Let λ be the unique prime of K above ℓ. By class field theory we have that λ splits completely in $K[\mathfrak{m}]$ and furthermore each prime above ℓ of $K(x(\mathfrak{m}))$ is totally (tamely) ramified in $K(x(\mathfrak{n}))$ (see [Nek07, Proposition 4.6]). Hence we have an embedding $K[\mathfrak{m}] \hookrightarrow K_\lambda$ and so we can embed $P_{\mathfrak{m}}$ in $A(K_\lambda)/\mathfrak{P}^M A(K_\lambda)$ and the image is independent on the choice of the embedding by Proposition 2.2.11.

Let v be a prime of K dividing N (hence a prime where A has bad reduction), and denote by A_0 the component of the identity of the special fiber of A at v. This subgroup is of finite index in $A(K_v^{\mathrm{ur}})$, and by abuse of notation, we denote A/A_0 for the quotient of these groups. We impose that A and $\mathfrak{P}$ satisfy the following conditions If v is a finite place of K where A has bad reduction then v satisfies one of the following conditions:

1. v is a principal of K,
2. $p \nmid [A : A_0]$.

Notice that the second condition fails to hold for only finitely many primes p since there are only finitely many places of K where A has bad reduction and the component group is finite for any such place.

Lemma 2.3.6. *Let $\mathfrak{n} \in \mathscr{S}(M)$, and let v be a valuation of K prime to $\mathfrak{n}$, then we have that $c_M(\mathfrak{n})_v \in \delta_v(A(K_v))$ where δ_v is the Kummer map. Moreover, if $v = v_\lambda$ for some prime ℓ below λ inert in K, we have $c_M(\mathfrak{n})_\lambda = \delta_\lambda(P_{\mathfrak{n}})$.*

Proof. Notice that the first statement is equivalent to the vanishing of $d_M(\mathfrak{n})_v$ and this follows from [Nek07, Proposition 5.12].

Let λ be an inert prime of K. By class field theory λ is totally split in $K[\mathfrak{n}]$. Hence $K[\mathfrak{n}]$ injects into K_λ, and therefore $P_{\mathfrak{n}} \in A(K_\lambda)/\mathfrak{P}^M A(K_\lambda)$. Its image $\delta_\lambda(P_{\mathfrak{n}})$ is represented by the cocycle $\sigma \mapsto \sigma\frac{Q_{\mathfrak{n}}}{p^M} - \frac{Q_{\mathfrak{n}}}{p^M}$, and $c_M(\mathfrak{n})$ is represented by

$$\sigma \mapsto -\frac{(\sigma-1)Q_{\mathfrak{n}}}{p^M} + \sigma\frac{Q_{\mathfrak{n}}}{p^M} - \frac{Q_{\mathfrak{n}}}{p^M}.$$

As $Q_{\mathfrak{n}}$ is defined over $K[n]$, the first term of this expression is determined solely by its restriction to $\mathrm{Gal}(K[\mathfrak{n}]/K)$. As a cocycle over K_λ it is therefore determined uniquely by its action on the decomposition group of λ in $K[\mathfrak{n}]$. But as λ splits completely, its decomposition group is trivial and hence the term vanishes. The statement is therefore proved. □

This lemma allows us to prove the following strong relation between the constructed cohomology classes

Theorem 2.3.7. *Let $\ell \in \mathscr{S}_1(M)$, with extension λ in K. There exists a homomorphism*

$$\chi_\ell : A(K_\lambda) \to H^1(K_\lambda, A[\mathfrak{P}^M])$$

such that

1. *for all $\mathfrak{m} \in \mathscr{S}(M)$ coprime to ℓ we have*

$$c_M(\mathfrak{m}\ell)_\lambda = \chi_\ell(P_\mathfrak{m}),$$

2. $\ker \chi_\ell = \mathfrak{P}^M A(K_\lambda)$ *and*

$$\chi_\ell(A(K_\lambda)/\mathfrak{P}^M A(K_\lambda)^{\pm}) \subset H^1(K_\lambda, A[\mathfrak{P}^M])^{\mp},$$

3. *χ_ℓ induces an isomorphism*

$$A(K_\lambda)/\mathfrak{P}^M A(K_\lambda) \xrightarrow{\sim} H^1(K_\lambda, A)[\mathfrak{P}^M].$$

Moreover, we have

$$\text{ord } d_M(\mathfrak{m}\ell)_\lambda = \text{ord } c_M(\mathfrak{m}\ell)_\lambda = \text{ord } c_M(\mathfrak{m})_\lambda.$$

Proof. Let $\ell \in \mathscr{S}_1(M)$, with extension λ in K and fix an extension $\overline{\lambda} \in \overline{K}$. We denote by k_v the residue field at v. Recall that k_λ has degree 2 over k_ℓ. In particular, $\text{Frob}(\ell)^2 = 1$ in $\text{End}(A(k_\lambda))$. Consequently it follows that

$$a_\ell - (\ell+1)\text{Frob}(\ell) = -\text{Frob}(\ell)(\text{Frob}(\ell)^2 - a_\ell \text{Frob}(\ell) + \ell). \tag{2.5}$$

As this is divisible by the characteristic polynomial of $\text{Frob}(\ell)$, this endomorphism must vanish on $A(k_\lambda)$. Notice that λ splits completely in $K(A[\mathfrak{P}^M])$. In particular the extension $K_\lambda(A[\mathfrak{P}^M])/K_\lambda$ has degree 1 and therefore $A[\mathfrak{P}^M]$ can be injected into $A(K_\lambda)$. As A has good reduction modulo λ and ℓ is coprime to p, reduction modulo λ acts injectively on $A[p^M]$. Let $P \in A(K_\lambda)$ be any point, since $A[p^M]$ injects into $A(k_{\overline{\lambda}})$ and since the expression in (2.5) vanishes, there exists a unique $\tilde{T}_P \in A_{p^M}$ such that

$$\frac{a_\ell - (\ell+1)\text{Frob}(\ell)}{p^M} P \equiv \tilde{T}_P \mod \overline{\lambda}.$$

Denote its $\mathfrak{P}^M$-torsion component by T_P and observe that it is K_λ-rational. Let λ_ℓ denote the restriction of $\overline{\lambda}$ to $K[\ell]$. As λ is principal in K by class field theory it splits completely in $K(x)$, and hence $K_{\lambda_1} = K_\lambda$. In particular, the extension $K_{\lambda_\ell}/K_\lambda$ is totally ramified with cyclic Galois group generated by σ_ℓ. Given P as above, define $\chi_\ell(P)$ to be the inflation of the unique cocycle on $\text{Gal}(K_{\lambda_\ell}/K_\lambda)$ defined by sending σ_ℓ to T_P. It is clear from its construction that χ_ℓ is a homomorphism.

To verify the first property, let $\mathfrak{n} = \mathfrak{m}\ell \in \mathscr{S}(M)$, let $\lambda_\mathfrak{n}$ be the restriction of $\overline{\lambda}$ to $K[\mathfrak{n}]$, and let $\lambda_\mathfrak{m}$ be its restriction to $K[\mathfrak{m}]$. As λ splits completely in $K[\mathfrak{m}]$, it follows that $K_{\lambda_\mathfrak{m}} = K_\lambda$ and that

$K_{\lambda_\mathfrak{n}} = K_{\lambda_\ell}$. We claim that $P_\mathfrak{n} \in p^M A(K_{\lambda_\mathfrak{n}})$. As the extension $K_{\lambda_\mathfrak{n}}/K_\lambda$ is totally ramified and generated by σ_ℓ, this automorphism acts trivially on $k_{\lambda_\mathfrak{n}}$, hence D_ℓ acts on $A(k_{\lambda_\mathfrak{n}})$ as $\ell(\ell+1)/2$. As $\mathfrak{P}^M$ divides $N(\ell)+1$, so does p^M and it follows that $P_\mathfrak{n} \in p^M A(k_{\lambda_\mathfrak{n}})$. In particular there exists a $Q \in A(K_{\lambda_\mathfrak{n}})$ such that $p^M Q \equiv P_\mathfrak{n} \mod \lambda_\mathfrak{n}$, and therefore $p^M Q - P_\mathfrak{n} \in A_1(K_{\lambda_\mathfrak{n}})$, where A_1 denotes the kernel of the reduction map to the residue field. This group is naturally isomorphic to $\hat{A}(\lambda_\mathfrak{n})$, the formal group associated to A over the maximal ideal of $K_{\lambda_\mathfrak{n}}$. As p is coprime to l, multiplication by p is an isomorphism on this group, and hence on $A_1(K_{\lambda_\mathfrak{n}})$ as well. It follows that $p^M Q - P_\mathfrak{n} \in p^M A(K_{\lambda_\mathfrak{n}})$, and thus that $P_\mathfrak{n} \in p^M A(K_{\lambda_\mathfrak{n}})$ proving the claim.

Consider the p^M-torsion point

$$-\frac{(\sigma_\ell - 1)P_\mathfrak{n}}{p^M} + \sigma_\ell \frac{P_\mathfrak{n}}{p^M} - \frac{P_\mathfrak{n}}{p^M} \in A(K_{\lambda_\mathfrak{n}}). \tag{2.6}$$

The extension $K_{\lambda_\mathfrak{n}}/K_\lambda$ is totally ramified, hence σ_ℓ acts trivially on $A(k_{\lambda_\mathfrak{n}})$. The reduction of this point modulo $\overline{\lambda}$ is therefore congruent to $-\frac{(\sigma_\ell - 1)P_\mathfrak{n}}{p^M}$. Recall from (2.3) and the Euler relation 2.2.6 that

$$a_\ell D_\mathfrak{m} y_\mathfrak{m} - (\ell+1) D_\mathfrak{m} y_\mathfrak{n} = -(\sigma_\ell - 1) D_\mathfrak{n} y_\mathfrak{n}.$$

Applying the second part of the same relations shows that

$$\frac{a_\ell - (\ell+1)\mathrm{Frob}(\ell)}{p^M} P_\mathfrak{m} \equiv -\frac{(\sigma_\ell - 1)P_\mathfrak{n}}{p^M} \mod \overline{\lambda},$$

This shows that $\chi_\ell(P_\mathfrak{m})$ is defined to be the inflation of the cocycle determined by

$$\sigma_\ell \mapsto \left(-\frac{(\sigma_\ell - 1)P_\mathfrak{n}}{p^M} + \sigma \frac{P_\mathfrak{n}}{p^M} - \frac{P_\mathfrak{n}}{p^M} \right) [\mathfrak{P}^M].$$

Recall that $c_M(\mathfrak{n})$ is represented by

$$\sigma \mapsto -\frac{(\sigma - 1)Q_\mathfrak{n}}{p^M} + \sigma \frac{Q_\mathfrak{n}}{p^M} - \frac{Q_\mathfrak{n}}{p^M},$$

hence this cocycle vanishes when restricted to $H^1(K_{\lambda_\mathfrak{n}}, A[\mathfrak{P}^M])$. The class $c_M(\mathfrak{n})$ is therefore inflated from a class in $H^1(K_{\lambda_\mathfrak{n}}/K_\lambda, A[\mathfrak{P}^M])$. In particular, using the same cocycle as representative, we see that the class $c_M(\mathfrak{n})_\lambda$ is defined uniquely by

$$\sigma_\ell \mapsto -\frac{(\sigma_\ell - 1)Q_\mathfrak{n}}{\mathfrak{P}^M} + \sigma_\ell \frac{Q_\mathfrak{n}}{\mathfrak{P}^M} - \frac{Q_\mathfrak{n}}{\mathfrak{P}^M}.$$

But as this $\mathfrak{P}^M$-torsion point is precisely the $\mathfrak{P}^M$-component (2.6), we are able to conclude that $\chi_\ell(P_\mathfrak{m}) = c_M(\mathfrak{m}\ell)_\lambda$.

The first part of property (2) follows directly from the uniqueness of the point T_P. In order to prove the second part of property (2) it suffices to show that

$$\chi_\ell(\tau P)^\tau_{\sigma_\ell} = -\chi_\ell(P)_{\sigma_\ell}.$$

As σ_ℓ is in the -1 eigenspace of τ and σ_ℓ acts trivially on $A[\mathfrak{P}^M]$, the former is equal to $-\tau\chi_\ell(\tau P)_{\sigma_\ell}$. Since the natural action of τ coincides with the action of $\mathrm{Frob}(\ell)$, on k_λ, it follows that $\tau T_P = T_{\tau P}$. But as $\chi_\ell(P)_{\sigma_\ell} = T_P$, this proves the property. Recall that $A(K_\lambda)/\mathfrak{P}^M A(K_\lambda)$ and $H^1(K_\lambda, A)[\mathfrak{P}^M]$ are isomorphic as $\mathcal{O}_M$-modules. To see that χ_ℓ induces such an isomorphism,

it suffices to show that im $\chi_\ell \cap$ im $\delta_\lambda = 0$. But this follows directly as δ_λ maps onto unramified cocycles and χ_ℓ maps onto ramified cocycles.

Finally, using (1) and (3), we see that $P_\mathfrak{m}$ maps to $d_M(\mathfrak{m}\ell)_\lambda$ via $c_M(\mathfrak{m}\ell)_\lambda$ hence they must all have the same order (here $P_\mathfrak{m}$ is viewed as an element of $A(K_\lambda)/\mathfrak{P}^M A(K_\lambda)$). By Lemma 2.3.6 this order is equal to ord $c_M(\mathfrak{m})_\lambda$. □

This theorem allow us to relate the classes $c_M(\mathfrak{n})$ with the classes of the divisors of $\mathfrak{n}$. In particular, for any $\mathfrak{m}, \ell \in \mathscr{S}(M)$ such that $(\mathfrak{m}, \ell) = 1$ define

$$\mathrm{ord}_\mathfrak{P}(P_\mathfrak{m})_\lambda = \max\{M \mid P_\mathfrak{m} \in \mathfrak{P}^M A(K_\lambda)\}.$$

Notice that this is well-defined since it is indeed possible to inject $K[\mathfrak{m}]$ into K_λ whenever $\ell \nmid \mathfrak{m}$. This enables us to formulate several useful consequences of the theorem.

Corollary 2.3.8. *Let $\mathfrak{n} \in \mathscr{S}(M)$. The following statements hold.*

1. *For all primes $\ell \mid \mathfrak{n}$ we have*

$$\mathrm{ord}_\mathfrak{P}(P_\mathfrak{n}) \leq \mathrm{ord}_\mathfrak{P}(P_{\mathfrak{n}/\ell})_\lambda,$$

with equality if and only if ord $c_M(\mathfrak{n}) =$ ord $c_M(\mathfrak{n})_\lambda$. *Consequently*

$$\text{if } P_{\mathfrak{n}/\ell} \notin \mathfrak{P}^M A(K_\lambda), \text{ then } P_\mathfrak{n} \notin \mathfrak{P}^M A(K[\mathfrak{n}]).$$

2. *For any $M > 0$*

$$d_M(\mathfrak{n}) \in Ш(A/K), \text{ if and only if, } M \leq \min_{\ell|\mathfrak{n}} \mathrm{ord}_\mathfrak{P}(P_{\mathfrak{n}/\ell})_\lambda.$$

3. *If $\mathfrak{n} \in \mathscr{S}_r(M_{r-1})$, then*

$$d_{M_{r-1}}(\mathfrak{n}) \in Ш(A/K).$$

Proof. The second part of the first statement is a direct consequence of the first. Whenever $M \geq \mathrm{ord}_\mathfrak{P}(P_{\mathfrak{n}/\ell})_\lambda$, the order of $P_{\mathfrak{n}/\ell}$ in $A(K_\lambda)/\mathfrak{P}^M A(K_\lambda)$ is naturally given by $p^{M-\mathrm{ord}_\mathfrak{P}(P_{\mathfrak{n}/\ell})_\lambda}$. By Theorem 2.3.7 this order is equal to ord $c_M(\mathfrak{n})_\lambda$. Hence

$$p^{M-\mathrm{ord}_\mathfrak{P}(P_{\mathfrak{n}/\ell})_\lambda} = \text{ord } c_M(\mathfrak{n})_\lambda \leq \text{ord } c_M(\mathfrak{n}) = p^{M-\mathrm{ord}_\mathfrak{P}(P_\mathfrak{n})},$$

which proves the first statement. By Lemma 2.3.6, $d_M(\mathfrak{n})$ vanishes at all valuations prime to $\mathfrak{n}$. For the valuations dividing $\mathfrak{n}$, we have

$$\text{ord } d_M(\mathfrak{n})_\lambda = \max\{1, p^{M-\mathrm{ord}_\mathfrak{P}(P_{\mathfrak{n}/\ell})_\lambda}\},$$

which vanishes if and only if $M \leq \mathrm{ord}_\mathfrak{P}(P_\mathfrak{m})_\lambda$. Applying this condition to all primes dividing $\mathfrak{n}$ gives the desired conclusion. Finally, let $\mathfrak{n} \in S_r(M_{r-1})$ be given. It follows from the definition of M_{r-1} that $M_{r-1} \leq \mathrm{ord}_\mathfrak{P}(P_{\mathfrak{n}/\ell}) \leq \mathrm{ord}_\mathfrak{P}(P_{\mathfrak{n}/\ell})_\lambda$ for all $\ell \mid \mathfrak{n}$. The conclusion now follows from the second statement. □

In light of this corollary we can prove a notable property of the M_r defined earlier.

Corollary 2.3.9. *Assume that $y_K = \mathrm{Tr}_{K(x)/K}\, y((1))$ has infinite order in $A(K)$.*
Then $M_0 = \mathrm{lenght}_{\mathcal{O}_{A,\mathfrak{P}}}(A(K)/\mathcal{O}_A y_K)$ and $M_r \geq M_{r+1}$ for all $r \geq 0$. In particular M_r is finite for all r

Proof. Assume that y_K has infinite order, then by [How04, Theorem A], $\mathcal{O}_A y_K$ is of finite index in $A(K)$. Since $\mathscr{S}_0 = \{1\}$ and $P_1 = y_K$, we have

$$M_0 = \mathrm{ord}_{\mathfrak{P}}(y_K) = \max\{M \mid y_K \in \mathfrak{P}^M A(K[1])\}.$$

Simultaneously

$$\mathrm{lenght}_{\mathcal{O}_{A,\mathfrak{P}}}(A(K)/\mathcal{O}_A y_K) = \max\{M \mid y_K \in \mathfrak{P}^M A(K)\}.$$

As $A(K[1])$ has no $\mathfrak{P}^M$-torsion, $A(K)/\mathfrak{P}^M A(K)$ injects into $A(K[1])/\mathfrak{P}^M A(K[1])$, hence these numbers are equal.

To prove the second statement, let $\mathfrak{m} \in \mathscr{S}_r(M)$. By Corollary 2.1.5, there exists a prime $\ell \nmid \mathfrak{m}$ such that $\ell \in \mathscr{S}_1(M)$ and ord $c_M(\mathfrak{m})_\lambda =$ ord $c_M(\mathfrak{m})$. In particular, this implies that

$$\mathrm{ord}_{\mathfrak{P}}(P_{\mathfrak{m}}) = \mathrm{ord}_{\mathfrak{P}}(P_{\mathfrak{m}})_\lambda \geq \mathrm{ord}_{\mathfrak{P}}(P_{\mathfrak{m}\ell})$$

by Corollary 2.3.8. Hence for any $\mathfrak{m} \in \mathscr{S}_r(M)$, there exists an $\mathfrak{n} \in \mathscr{S}_{r+1}(M)$ such that $\mathrm{ord}_{\mathfrak{P}}(P_{\mathfrak{m}}) \geq \mathrm{ord}_{\mathfrak{P}}(P_{\mathfrak{n}})$. □

This corollary allows the formulation of the following simple but important consequence of Theorem 2.3.7.

Proposition 2.3.10. *Let M and M' be two positive integers and let $\mathfrak{n} \in \mathscr{S}(M + M')$ and $\mathfrak{n}' \in \mathscr{S}(M')$ be two integers such that $d_M(\mathfrak{n}), d_{M'}(\mathfrak{n}') \in Ш(A/K)$. Then the Cassels pairing is given by*

$$\langle d_M(\mathfrak{n}), d_{M'}(\mathfrak{n}')\rangle = \sum_{\substack{\ell \mid \mathfrak{n} \\ (\ell, \mathfrak{n}')=1}} \langle d_{M+M'}(\mathfrak{n}), P_{\mathfrak{n}'}\rangle_\lambda.$$

Proof. Recall the construction of the Cassels pairing described in the previous section. Indeed $d_{M+M'}(\mathfrak{n})$ is a suitable choice for d_1 as $p^{M'} d_{M+M'}(\mathfrak{n}) = d_M(\mathfrak{n})$. By Lemma 2.3.6, it vanishes for all valuations v prime to $\mathfrak{n}$. Hence this sum can be restricted to the primes dividing $\mathfrak{n}$. By the same lemma, $P_{\mathfrak{n}'}$ is a suitable choice for those y_λ, for each of those $\ell \nmid \mathfrak{n}'$. If $\ell \mid \mathfrak{n}'$, then $d_{M'}(\mathfrak{n}')_\lambda = 0$ as it is contained in $Ш(A/K)$. Hence by Theorem 2.3.7, $c_{M'}(\mathfrak{n}')_\lambda = 0$, and hence there is no contribution to the pairing for this prime. Summing up the remaining terms gives the desired conclusion. □

2.4 Gross points

We define an analogue of Heegner points on the Gross curve. Assume that the number of factors of N^- has the same parity as the degree of F. Let B' denote a definite quaternion algebra over F ramified at all archimedean primes and at each prime dividing N^-. Let R be an Eichler order of level N^+. We denoted by $\mathfrak{X}$ the Gross curve associated to B' of level R. Let τ denote the embedding of K into B as constructed in the first chapter.

Definition 2.4.1. The set of *CM-points* by R is

$$\mathrm{CM}(\mathfrak{X}, R) = \tau(K)^\times \backslash \hat{B'}^\times / \hat{F}^\times R.$$

We say that $x \in \mathrm{CM}(\mathfrak{X}, R)$ has conductor c if $\tau(K) \cap x\hat{F}Rx^{-1}$ is an order of conductor c.

Inside that set of CM-points we can define some analogue of the Heegner points which we call Gross points.

Definition 2.4.2. For each $\mathfrak{n} \in \mathscr{S}$ we define an element $h(\mathfrak{n})$ of $\hat{B'}^{\times}$ as follows: $h((1)) = 1$, if $\mathfrak{n} = \ell \in \mathscr{S}_1$ then the ℓ part of R is $R(\ell)^{\times}$ for some maximal $\mathcal{O}_{F_\ell}$-order $R(\ell) \subset B_\ell$ and we take $h(\ell) \in R(l) \cap B_\ell^{\times} \subset B_\ell^{\times} \subset \hat{B}^{\times}$ such that it satisfies $\mathrm{ord}_\ell(\mathrm{nr}(h(\ell))) = 1$, finally if $\mathfrak{n} = \ell_1 \dots \ell_r \in \mathscr{S}_r$ with $r > 1$ and the $\ell_i \in \mathscr{S}_1$ distinct for all i then $h(\mathfrak{n}) = h(\ell_1) \dots h(\ell_r) \in \hat{B}^{\times}$. The *Gross points* on $\mathfrak{X}$ are the points

$$\mathfrak{x}_\mathfrak{n} \in \mathfrak{X}$$

defined by $h(\mathfrak{n})$.

Chapter 3

Structure Theorem for Shafarevich-Tate groups

In this section we provide a generalization of Kolyvagin's results ([McC91]) in the setting of modular abelian varieties over totally real fields. We continue to follow the notation of the previous section. We start by reviewing an application of the Fricke involution to the Selmer and Shafarevich-Tate group of an abelian variety. In the last part we use all the previous results to prove a structure theorem for the Tate-Shafarevich group.

3.1 Eigenspaces for the Fricke involution

Let f be the Hilbert newform associated to the modular abelian variety A. Let W_N be the matrix

$$\begin{pmatrix} 0 & 1 \\ t & 0 \end{pmatrix}$$

where $t \in \mathbb{A}_F$ such that the projection on the finite adeles generates $N\hat{\mathcal{O}}_F$.

Definition 3.1.1. The Fricke involution is defined as

$$(w_N(f))(g) = f(gW_N).$$

Proposition 3.1.2. *w_N is an involution and if f is a new-eigenform for all Hecke operator then f is an eigenvector for w_N with eigenvalue $\epsilon \in \{\pm 1\}$. Furthermore ϵ is the sign of the functional equation associated to the L-function of f:*

$$L(f, s) = \epsilon L(f, 2 - s).$$

Proof. See [How04, chapter 1]. □

From now on let ϵ be the eigenvalue of the Fricke involution for f and let $\epsilon_r = (-1)^r \epsilon$.

Lemma 3.1.3. *Let $\mathfrak{n} \in \mathscr{S}_r(M)$. The point $P_{\mathfrak{n}}$ is in the ϵ_r-eigenspace of $(A(K)/\mathfrak{P}^M A(K))$.*

Proof. This follows from the results in [KL91, Pag. 851 - 852], [Zha01b] and [Zha01a].

□

The Fricke involution plays an important role in analyzing the structure of the Shafarevich-Tate group; it also imposes conditions on the groups $A(K)/\mathfrak{P}^M A(K)$. This is illustrated in the following Lemma.

Lemma 3.1.4. *For all integers M, the group $A(K)/\mathfrak{P}^M A(K)^{-\epsilon}$ vanishes. In particular the map*

$$S_{\mathfrak{P}^\infty}(A/K)^{-\epsilon} \to Ш(A/K)^{-\epsilon}_{\mathfrak{P}^\infty}$$

is an isomorphism.

Proof. Notice that the submodule $\mathcal{O}_A y_K \subset A(K)$ is of finite index. For any integer M, $y_K = P_1$ is contained in the ϵ-eigenspace of $A(K)/\mathfrak{P}^M A(K)$ by Lemma 3.1.3. The decomposition into eigenspaces

$$A(K)/\mathfrak{P}^M A(K) \cong \left(A(K)/\mathfrak{P}^M A(K)\right)^{\epsilon} \oplus \left(A(K)/\mathfrak{P}^M A(K)\right)^{-\epsilon},$$

shows that the order of the $-\epsilon$-eigenspace equals the index of the ϵ-eigenspace in this group. As this index is bounded by the index of $\mathcal{O}_A y_K$ in $A(K)$, the order of the $-\epsilon$-eigenspace is bounded independently of M. Hence $A(K)^{-\epsilon}$ is a finite group and therefore a torsion group. Since $A[\mathfrak{P}](K) = 0$ by Proposition 2.2.11, it follows that $A(K)/\mathfrak{P}^M A(K)^{-\epsilon} = 0$. Consequently $A(K)^{-\epsilon} \otimes F_{\mathfrak{P}}/\mathcal{O}_{A,\mathfrak{P}}$ vanishes and thus we obtain the desired isomorphism by the $\mathfrak{P}^\infty$-descent sequence (1.3). □

3.2 Structure Theorem

Since we assumed that y_K has infinite order, the Shafarevich-Tate group is finite and so the Cassels-Tate pairing is non-degenerate and alternating on $Ш(A/K)_{\mathfrak{P}^\infty}$ for all primes of odd characteristic. Hence the order of $Ш(A/K)$ is either a perfect square or twice a perfect square. Recall that the Tate pairing is τ-equivariant, hence so is the Cassels-Tate pairing. In particular, the ϵ and $-\epsilon$ eigenspaces of $Ш(A/K)_{\mathfrak{P}^\infty}$ are orthogonal and must therefore both be perfect squares as well. Let

$$N_1 \geq N_3 \geq N_5 \geq \cdots$$

be the integers such that

$$Ш(A/K)^{-\epsilon}_{\mathfrak{P}^\infty} \cong (\mathcal{O}_A/\mathfrak{P}^{N_1})^2 \times (\mathcal{O}_A/\mathfrak{P}^{N_3})^2 \times \cdots$$

and let

$$N_2 \geq N_4 \geq N_6 \geq \cdots$$

be the integers such that

$$Ш(A/K)^{\epsilon}_{\mathfrak{P}^\infty} \cong (\mathcal{O}_A/\mathfrak{P}^{N_2})^2 \times (\mathcal{O}_A/\mathfrak{P}^{N_4})^2 \times \cdots$$

By Lemma 1.5.1 the groups $Ш(A/K)^{\pm}_{\mathfrak{P}^\infty}$ admit maximal isotropic subgroups $D^{\pm}$ inducing split exact sequences

$$0 \to D^{\pm} \to Ш(A/K)^{\pm}_{\mathfrak{P}^\infty} \to D^{*\pm} \to 0.$$

Notice that $D^{-\epsilon}$ can be decomposed as $D_1 \times D_3 \times \cdots$ where D_i is a cyclic $\mathcal{O}_A/\mathfrak{P}^{N_i}$-module. Analogously, D^{ϵ} admits a decomposition $D_2 \times D_4 \times \cdots$. Since the $\mathfrak{P}$-primary part of the Shafarevich-Tate group decomposes as a sum of its τ-eigenspaces we conclude that $Ш(A/K)_{\mathfrak{P}^\infty}$ admits a maximal isotropic subgroup $D = D_1 \times D_2 \times D_3 \times \cdots$ such that the exact sequence

$$0 \to D \to Ш(A/K)_{\mathfrak{P}^\infty} \to D^* \to 0 \tag{3.1}$$

is split. We can now state the fundamental result of this paper which is the relation between the N_r and the earlier defined M_r.

Theorem 3.2.1. *Assume that y_K has infinite order. Then*

$$N_r = M_{r-1} - M_r \tag{3.2}$$

for all $r \geq 1$.

Before proving Theorem 3.2.1 we mention a few direct corollaries.

Corollary 3.2.2. *We have that*

$$M_r - M_{r+1} \geq M_{r+2} - M_{r+3}, \ \forall\ r \geq 0,$$

Moreover if $M_r = M_{r+2}$, then $M_r = M_j$ for all $j \geq r$.

Notice that while the difference $M_r - M_{r+1}$ decreases if we increase r by 2, this is not necessarily true if we increase r only by 1.

Additionally, Theorem 3.2.1 allows us to give an explicit description of the p-torsion order of the Shafarevich-Tate group.

Corollary 3.2.3. *Let $m = \min\{M_r, r \geq 0\}$. Then*

$$\text{lenght}_{\mathcal{O}_{A,\mathfrak{P}}} Ш(A/K) = 2(M_0 - m).$$

In order to prove Theorem 3.2.1 we need some more preparation in the form of several lemmas.

Lemma 3.2.4. *Let $\ell \in \mathscr{S}_1(M)$ be a prime, then $\text{im}\chi_\ell$ is a maximal isotropic subgroup of $H^1(K_\lambda, A[\mathfrak{P}^M])$.*

Proof. Let $x, y \in \text{im}\chi_\ell$. Recall from the proof of Theorem 2.3.7 that x and y are inflated from cocycles in $H^1(\langle\sigma_\ell\rangle, A[\mathfrak{P}^M])$. As the Tate-pairing is a cup-product, it satisfies

$$x \smile y = \text{Inf}(x') \smile \text{Inf}(y') = \text{Inf}(x' \smile y').$$

As σ_ℓ is totally ramified, its second cohomology group injects in the group $H^2(I, \mu_{p^M})$, where I is the inertia group of K_λ. But this group is trivial as $\ell \neq p$ (see [Mil06, Lemma 1.2.9]). Hence $x \smile y = 0$. Maximality follows from the second statement of Theorem 2.3.7. □

Lemma 3.2.5. *Let $\ell \in \mathscr{S}_1(M)$ and let $S \subset \mathscr{S}_1(M)$ be a finite set not containing ℓ. Then there exists a $c \in H^1(K, A[\mathfrak{P}^M])^{\pm}$ such that*

1. *$c \neq 0$,*
2. *$c_v \in \delta(A(K_v))$ for all valuations v prime to $S \cup \{\ell\}$,*
3. *$c_{v_\lambda} \in \text{im}\ \chi_q$ for all $q \in S$.*

Proof. Let T be the union of S, ℓ, the primes of K extending p, the infinite primes and the primes where A has bad reduction. Let K_T be the maximal extension of K that is ramified only at the primes in T. Tate global duality [Mil06, Theorem I.4.10] gives a self dual exact sequence

$$H^1(K_T/K, A[\mathfrak{P}^M]) \to \bigoplus_{v \in T} H^1(K_v, A[\mathfrak{P}^M]) \to H^1(K_T/K, A[\mathfrak{P}^M])^*.$$

Let G denote the intermediate group. Due to exactness, the image of $H^1(K_T/K, A[\mathfrak{P}^M])$ is an isotropic subgroup of G, and by self duality it must be maximal isotropic. As the exponent of

every group divides p^M, all groups can be decomposed as a sum of their τ-eigenspaces. Since the pairing giving rise to this duality arises from the Tate-pairing, the pairing is τ-equivariant and hence the eigenspaces are orthogonal. Consequently, the image of $H^1(K_T/K, A[\mathfrak{P}^M])^{\pm}$ is a maximal isotropic subgroup of $G^{\pm}$. For all $q \in S$, let $H_{v_q} = \mathrm{Im}\chi_q$. For all other places $v \in T\backslash\{\ell\}$, let $H_v = \delta(A(K_v))$. Notice that for all the places $v \neq \ell$ there is an inequality $|H_v| \geq |H^1(K_v, A[\mathfrak{P}^M])|^{1/2}$. Hence the group $H^1(K_T/K, A[\mathfrak{P}^M])^{\pm}$ is a strictly larger subgroup of G than the group

$$\bigoplus_{v\in T\backslash\{\ell\}} \frac{H^1(K_v, A[\mathfrak{P}^M])^{\pm}}{H_v^{\pm}}.$$

In particular $H^1(K_T/K, A[\mathfrak{P}^M])$ cannot map injectively into this group. Hence we can choose a $c \in H^1(K_T/K, A[\mathfrak{P}^M])$ satisfying properties 1 and 3. It also satisfies 2; By construction of K_T, c is unramified outside T. It follows from [Mil06, Proposition 3.8] that $H^1(K_v^{\mathrm{ur}}/K_v, A) = 0$. Consequently, the map $\delta_v : A(K_v) \to H^1(K_v^{\mathrm{ur}}/K_v, A[\mathfrak{P}^M])$ is surjective. □

The strategy for proving Theorem 3.2.1 is the following: let r be an integer and assume $M_{r-1} > M_r$. Let $\mathfrak{n} \in \mathscr{S}_r(M_{r-1})$, Corollary 2.3.8 imposes that $d_{M_{r-1}}(\mathfrak{n}) \in Ш(A/K)$. As $\mathrm{ord}_{\mathfrak{P}}(P_{\mathfrak{n}}) \geq M_r$, it follows from (2.4) that the order of $d_{M_{r-1}}(\mathfrak{n})$ is at most $p^{M_{r-1}-M_r}$. For properly chosen $\mathfrak{n}_r$, it will be shown that $d_{M_{r-1}}(\mathfrak{n}_r)$ attains this order. Proceeding inductively, and choosing the $\mathfrak{n}_r$ independent of $\mathfrak{n}_s, s \leq r$, we will show that $N_r = M_{r-1} - M_r$ which will complete the proof. In order to guarantee the independence of the $\mathfrak{n}_r$, we need the following proposition.

Proposition 3.2.6. *Let r be a positive integer and let $C \subset S_{\mathfrak{P}^\infty}(A/K)^{\epsilon_r}$ be a sub $\mathcal{O}_{A,\mathfrak{P}}$-module generated by r independent elements. Let $M > M_r$ be a square-free integer. Then there exists an $\mathfrak{n} \in \mathscr{S}_r(M)$ such that* ord $c_M(\mathfrak{n}) = p^{M-M_r}$ *and $\langle c_M(\mathfrak{n})\rangle \cap C = \{0\}$.*

Proof. As $p^{M'}c_M(\mathfrak{n}) = c_{M-M'}(\mathfrak{n})$ for all $M' \leq M$. It suffices to show that the statement holds for all M large enough. Hence let $M \geq M_{r-1}$ be such that

$$p^M \geq \text{exponent of } C.$$

Let $\mathfrak{n} \in \mathscr{S}_r(M_r + 1)$ be such that $\mathrm{ord}_{\mathfrak{P}}(P_{\mathfrak{n}}) = M_r$, and let $L = K(A[\mathfrak{P}^M])$. Recall that there exists a Galois extension L_C/L such that $\mathrm{Gal}(L_C/L) \cong C^*$. Let S be the set of primes dividing $\mathfrak{n}$. For every $\ell \in S$, fix an extension λ_L in L. Let $X \subset C^*$ denote the submodule generated by the characters of all $\ell \in S \cap \mathscr{S}(M)$, and let k denote the rank of the image of X in C^*/pC^*. Assume that $k < r$, then there exists an ℓ_0 in S such that the primes in $S \cap \mathscr{S}(M)\backslash\{\ell_0\}$ generate the image of X, and we can choose a $\psi \in C^*$ such that

$$\psi \notin X + pC^*.$$

If $c_{M_r+1}(\mathfrak{n}) \in C$, we can impose the additional condition that $\psi(c_{M_r+1}(\mathfrak{n})) \neq 0$, as a finite group cannot be the union of two proper subgroups. By replacing ℓ_0 with a carefully chosen prime ℓ', ψ can be added to X. Using Lemma 3.2.5, we choose a $c \in H^1(K, A[\mathfrak{P}])^{-\epsilon_r}$ such that

$$\begin{aligned} &c \neq 0, \\ &c_v \in \delta_v(A(K_v)), && \text{for all } v \notin S, \\ &c_\lambda \in \mathrm{im}\chi_\ell, && \text{for all } \ell \in S\backslash\{\ell_0\}. \end{aligned} \tag{3.3}$$

Let $\langle C, c_{M_r+1}(\mathfrak{n})\rangle$ denote the subgroup of $H^1(K, A[\mathfrak{P}^M])$ generated by C and $c_{M_r+1}(\mathfrak{n})$. As both are contained in the ϵ_r-eigenspace and c is not, the intersection of this group and $\langle c\rangle$ is trivial.

Thus, we can define $\phi \in \langle C, c_{M_r+1}(\mathfrak{n}), c\rangle^*$ such that

$$\begin{aligned}\phi|_C &= \psi,\\ \phi(c_{M_r+1}(\mathfrak{n})) &\neq 0,\\ \phi(c) &\neq 0.\end{aligned}$$

By Proposition 2.1.4, there exists an $\ell' \in \mathscr{S}_1(M)$ such that $\phi = \phi_{\mathrm{Frob}(\lambda'_L)}$, and hence that $\psi = \psi_{\mathrm{Frob}(\lambda'_L)}$. Moreover, observe that the sum

$$\sum_v c_{M_r+1}(\mathfrak{n}\ell')_v \smile c_v = 0$$

vanishes as the sum of invariants of a global class is 0. Let us consider the cup products for the valuations v not contained in $S \cup \{\lambda'\}$. In this case it follows from Lemma 2.3.6 that $c_{M_r+1}(\mathfrak{n}\ell')_v \in \delta_v(A(K_v))$. Equation (3.3) guarantees that $c_v \in \delta_v(A(K_v))$ as well. Since this is an isotropic subgroup, the cup product vanishes. For the primes $\ell \in S\backslash\{\ell_0\}$, it follows from Theorem 2.3.7 that $c_{M_r+1}(\mathfrak{n}\ell')_\lambda = \chi_\ell(P_{\mathfrak{n}\ell'/\ell})$. By construction c_λ is contained in $\mathrm{im}\chi_\ell$ as well. Since this group is again isotropic, the cup product vanishes here as well. Hence the only remaining terms are the cup products at the primes λ' and λ_0, and we conclude that

$$c_{M_r+1}(\mathfrak{n}\ell')_{\lambda'} \smile c_{\lambda'} = -c_{M_r+1}(\mathfrak{n}\ell')_{\lambda_0} \smile c_{\lambda_0}.$$

For λ', it follows from (1.1) and (3.3) that

$$c_{M_r+1}(\mathfrak{n}\ell')_{\lambda'} \smile c_{\lambda'} = \langle d_{M_r+1}(\mathfrak{n}\ell')_{\lambda'}, x\rangle_{\lambda'},$$

for some $x \in A(K_{\lambda'})$. Theorem 2.3.7 gives the equality

$$\mathrm{ord} d_{M_r+1}(\mathfrak{n}\ell')_{\lambda'} = \mathrm{ord}\ c_{M_r+1}(\mathfrak{n}\ell')_{\lambda'} = \mathrm{ord}\ c_{M_r+1}(\mathfrak{n})_{\lambda'}.$$

The choice of ϕ, now guarantees that this cocycle is non-zero by (2.1) and since we have that $\mathrm{ord}_{\mathfrak{P}}(P_{\mathfrak{n}}) = M_r$, equation (2.4) shows that $\mathrm{ord} c_{M_r+1}(\mathfrak{n}) = p$, which implies that the class $d_{M_r+1}(\mathfrak{n}\ell') \in H^1(K, A)[\mathfrak{P}]^{-\epsilon_r}$. By the choice of c we made, $c_{\lambda'}$ has order at most p, and as $\phi(c) = \phi_{\mathrm{Frob}(\lambda'_L)}(c) \neq 0$, we conclude that $c_{\lambda'}$ is non-zero as well. As $c_{\lambda'}$ is in the $-\epsilon_r$-eigenspace of $H^1(K_{\lambda'}, A[\mathfrak{P}])$, x is determined uniquely in $(A(K_{\lambda'})/\mathfrak{P}A(K_{\lambda'}))^{-\epsilon_r}$. As both eigenspaces are cyclic $\mathcal{O}_A/\mathfrak{P}^M$-modules, it follows from the non-degeneracy of the Tate pairing that

$$c_{M_r+1}(\mathfrak{n}\ell')_{\lambda'} \smile c_{\lambda'} \neq 0.$$

It follows that $c_{M_r+1}(\mathfrak{n}\ell')_{\lambda_0} \neq 0$, and by Theorem 2.3.7 that $P_{\mathfrak{n}\ell'/\ell_0} \notin \mathfrak{P}^{M_r+1}A(K_{\lambda_0})$. By the definition of M_r we must therefore have that $\mathrm{ord}_{\mathfrak{P}}(P_{\mathfrak{n}\ell'/\ell_0}) = M_r$. Thus by replacing $\mathfrak{n}$ with $\mathfrak{n}' = \mathfrak{n}\ell'/\ell_0$, we can add ψ to X and increase the rank of its image by 1.

If $k = r$, we have that $X = C^*$. In particular we have that $S \subset \mathscr{S}_1(M)$, hence $c_M(\mathfrak{n})$ exists and has order p^{M-M_r}. Observe that

$$\begin{aligned}\{c \in C \mid\ & c_\lambda = 0 \text{ for all } \ell \in S\} =\\ \{c \in C \mid\ & \phi_{\mathrm{Frob}(\lambda_L)}(c) = 0 \text{ for all } \ell \in S\} =\\ & \{c \in C \mid\ \phi(c) = 0 \text{ for all } \phi \in C^*\} = \{0\}.\end{aligned}$$

On the other hand since $\mathrm{ord}_{\mathfrak{P}}(P_{\mathfrak{n}/\ell}) \geq M_{r-1}$, it follows that

$$\mathrm{ord}\ c_{M_{r-1}}(\mathfrak{n})_\lambda = \mathrm{ord}\ c_{M_{r-1}}(\mathfrak{n}/\ell)_\lambda = 1$$

for all $\ell \in S$. Hence

$$C \cap \langle c_{M_{r-1}}(\mathfrak{n}) \rangle = 0.$$

Since $c_{M_{r-1}}(\mathfrak{n})$ is a multiple of $c_M(\mathfrak{n})$ of order $p^{M_{r-1}-M_r}$, the statement is therefore proved when $M_{r-1} > M_r$. Hence assume $M_{r-1} = M_r$. By relaxing the condition that C has rank r, it is easily shown that the lemma holds for $C = \{0\}$. In particular, there exists an $\mathfrak{m} \in \mathscr{S}_{r-1}(M)$ such that ord $c_M(\mathfrak{m}) = p^{M-M_{r-1}}$. By Proposition 2.1.4, there exists an $\ell \in \mathscr{S}_1(M)$ such that $c_{M_r+1}(\mathfrak{m})_\lambda \neq 0$. By Theorem 2.3.7, we hence have that $d_{M_r+1}(\mathfrak{m}\ell)_\lambda \neq 0$. In particular this means that $d_{M_r+1}(\mathfrak{m}\ell) \notin Ш(A/K)$ and hence $c_{M_r+1}(\mathfrak{m}\ell) \notin S_{\mathfrak{P}^\infty}(A/K)$. As C is contained in this group, we conclude

$$C \cap \langle c_{M_r+1}(\mathfrak{n}) \rangle = 0,$$

and thus the proposition is proved. □

In the process of proving Proposition 3.2.6, the following weaker statement has been proven as well.

Corollary 3.2.7. *Let r be a square-free integer and let $M' \geq M \geq M_r$ be two integers. Then for all primes $\mathfrak{n} \in \mathscr{S}_r(M)$, there exists an $\mathfrak{n}' \in \mathscr{S}_r(M')$ such that* ord $c_{M'}(\mathfrak{n}') \geq$ ord $c_M(\mathfrak{n})$.

Using this, let r be an odd number and let $\mathfrak{n} \in \mathscr{S}_r(M_{r-1})$ be such that $c_{M_{r-1}}(\mathfrak{n})$ has order $p^{M_{r-1}-M_r}$. By Corollary 2.3.8 we have that $d_{M_{r-1}}(\mathfrak{n}) \in Ш(A/K)^{-\epsilon}_{\mathfrak{P}^\infty}$, and therefore that $c_{M_{r-1}}(\mathfrak{n}) \in S_{\mathfrak{P}^\infty}(A/K)$. By Lemma 3.1.4 $d_{M_{r-1}}(\mathfrak{n})$ has order $p^{M_{r-1}-M_r}$ in this group. As the Cassels-Tate pairing is alternating on the $\mathfrak{P}$-primary part, we conclude that $Ш(A/K)^{-\epsilon}_{\mathfrak{P}^\infty}$ has a submodule isomorphic to $(\mathcal{O}_A/\mathfrak{P}^{M_{r-1}-M_r})^2$. We let $c_{M_{r-1}}$ and $\tilde{c}_{M_{r-1}}$ denote the natural generators of this module.

By proceeding inductively on $r = 2m+1$, and imposing by Proposition 3.2.6 that $c_{M_{r-1}}$ is chosen independent of $\{c_{M_{2k}}, \tilde{c}_{M_{2k}} \mid k < m\}$, it follows that $Ш(A/K)^{-\epsilon}_{\mathfrak{P}^\infty}$ contains a submodule isomorphic to

$$(\mathcal{O}_A/\mathfrak{P}^{M_0-M_1})^2 \times (\mathcal{O}_A/\mathfrak{P}^{M_2-M_3})^2 \times \cdots .$$

Let us prove the main theorem.

Proof of Theorem 3.2.1. We proceed by induction on r. By applying Proposition 3.2.6 to $C = \{0\}$ and $r = 1$, it is shown above that there exists an $\ell \in \mathscr{S}_1(M_0 - M_1)$ such that the class $d_{M_0-M_1}(\ell) \in Ш(A/K)^{-\epsilon}_{\mathfrak{P}^\infty}$ has order $p^{M_0-M_1}$. By the definition of N_1 we conclude that

$$M_0 - M_1 \leq N_1.$$

Conversely recall that $Ш(A/K)_{\mathfrak{P}^\infty}$ admits a maximal isotropic subgroup

$$D = D_1 \times D_2 \times D_3 \times \cdots ,$$

where D_i is a cyclic $\mathcal{O}_A/\mathfrak{P}^{N_i}$-module contained in the ϵ_i-eigenspace of $Ш(A/K)_{\mathfrak{P}^\infty}$. Let d_i be a generator for D_i. As y_K has infinite order, the sequence in (1.3) is split. For every i, let c_i denote the lift of d_i to $S_{\mathfrak{P}^\infty}(A/K)$ under this splitting. For any valuation v, let $y_{i,v} \in A(K_v)$ be an element such that $\delta_v(y_{i,v}) = c_i$. It follows from the definition of $M_0 = \mathrm{ord}_{\mathfrak{P}}(y_K)$ that ord $c_{M_0+N_1}(1) = p^{N_1}$. Hence by Corollary 2.1.5, there exists a prime number ℓ_1 such that

$$\begin{aligned} \mathrm{ord} c_{M_0+N_1}(1)_{\lambda_1} &= p^{N_1}, \\ \mathrm{ord} c_{1,\lambda_1} &= p^{N_1}, \\ c_{i,\lambda_1} &= 0, \text{ for all } i \geq 2. \end{aligned} \tag{3.4}$$

The first condition of Corollary 2.1.5 is equivalent to the property that $\ell_1 \in \mathscr{S}_1(M_0 + N_1)$. Therefore by Corollary 2.3.8, it follows that $d_{M_0}(\ell_1) \in Ш(A/K)$. Thus for all i and for any $0 \leq M \leq N_i - 1$ we have that

$$\langle d_{M_0}(\ell_1), p^M d_i \rangle = \langle d_{M_0-M}(\ell_1), d_i \rangle = \langle d_{M_0-M+N_i}(\ell_1)_{\lambda_1}, y_{i,\lambda_1} \rangle_{\lambda_1}, \tag{3.5}$$

To see that the last equality holds, observe that $d_{M_0-M+N_i}(\ell_1)$ satisfies the properties of d_1 in the definition of the Cassels-Tate pairing. Moreover, all other terms in this sum vanish by Lemma 2.3.6. By (1.1) and the choice of ℓ_1, this term vanishes for $i \geq 2$. For $i = 1$, recall that this pairing on

$$A(K_{\lambda_1})/\mathfrak{P}^{N_1} A(K_{\lambda_1}) \times H^1(K, A)[\mathfrak{P}^{N_1}]$$

is non-degenerate and τ-invariant. In particular the τ-eigenspaces are cyclic submodules. As y_{i,λ_1} has order p^{N_1}, it is a generator for $A(K_\lambda)/\mathfrak{P}^{N_1} A(K_\lambda)^{-\epsilon}$. By Theorem 2.3.7 we have that ord $d_{M_0+N_1-M}(\ell_1)_{\lambda_1} =$ ord $c_{M_0+N_1-M}(1)_{\lambda_1} = p^{N_1-M} > 1$. It therefore follows from the non-degeneracy of this pairing that (3.5) is non-trivial for all $0 \leq M \leq N_1 - 1$. We conclude that the character

$$\mathcal{X}_1 : \ d \mapsto \langle d_{M_0}(\ell_1), d \rangle \in D^*$$

vanishes on $D_2 \times D_3 \times \cdots$. Observe that this character is the image of $d_{M_0}(\ell_1)$ in D^* under the map in (3.1). As D_1 is a cyclic $\mathcal{O}_A/\mathfrak{P}^{N_1}$-module, so is D_1^*, and since $\mathcal{X}_1$ does not vanish anywhere on D_1, we conclude that it must be a generator for D_1^*. In particular $d_{M_0}(\ell_1)$ has order at least p^{N_1}. But as its order is bounded by $p^{M_0-M_1}$, we conclude that

$$N_1 \leq M_0 - M_1,$$

and hence that

$$N_1 = M_0 - M_1.$$

Proceeding inductively, let $r > 1$ be an integer and assume that for all $1 \leq j < r$ we have $N_j = M_{j-1} - M_j$. Moreover assume that there exist $\ell_1, ..., \ell_{r-1} \in \mathscr{S}_1(M')$ such that

$$c_{i,\lambda_j} = 0 \text{ for all } i > j,$$

and that the characters

$$\mathcal{X}_j : d \mapsto \langle d_{M_{j-1}}(\mathfrak{n}_j), d \rangle, \ 1 \leq j < r$$

vanish on $D_r \times D_{r+1} \times \cdots$ and form a diagonal basis for $(D_1 \times \cdots \times D_{r-1})^*$, where $\mathfrak{n}_j = \prod_{i \leq j} \ell_i$, and M' is chosen sufficiently large. Let h_1 and $h_2 \in A(K)^\epsilon$ be two elements forming a $\mathcal{O}_A/\mathfrak{P}^{M'}$ for $A(K)/\mathfrak{P}^{M'} A(K)$ and let

$$C = \langle \delta(h_1), \delta(h_2), c_1, ..., c_{r-1}, c_{M_0}(\mathfrak{n}_1), ..., c_{M_{r-2}}(\mathfrak{n}_{r-1}) \rangle^{\epsilon_k}.$$

This module is generated by at most r independent elements. Using Proposition 3.2.6, choose any $\mathfrak{n} \in \mathscr{S}_r(M')$ such that ord $c_{M_{r-1}}(\mathfrak{n}) = p^{M_{r-1}-M_r}$ and $C \cap \langle c_{M_{r-1}}(\mathfrak{n}) \rangle = 0$. Assume that ord$d_{M_{r-1}}(\mathfrak{n}) > N_r$. As the sequence in (3.1) splits, we observe that $d_{M_{r-1}}(\mathfrak{n})$ is contained in the submodule generated by $d_1, ..., d_{r-1}, d_{M_0}(\mathfrak{n}_1), ..., d_{M_{r-2}}(\mathfrak{n}_{r-1})$. Let c denote the lift of $d_{M_{r-1}}(\mathfrak{n})$ to $S_{\mathfrak{P}^\infty}(A/K)$. If r is odd, the lift is unique and must therefore equal $c_{M_{r-1}}(\mathfrak{n})$, which gives a contradiction as the lift is contained in C. Otherwise, $c_{M_{r-1}}(\mathfrak{n}) - c$ is contained in the image of $A(K)^\epsilon \otimes F_\mathfrak{P}/\mathcal{O}_{A,\mathfrak{P}}$. After multiplying by a power of p if necessary, one can assume that $c_{M_{r-1}}(\mathfrak{n}) - c \in \delta(A(K)/\mathfrak{P}^{M'} A(K))$. As this module is generated by $\delta(h_1)$ and $\delta(h_2)$, we conclude that $c_{M_{r-1}}(\mathfrak{n}) \in C$. This gives a contradiction, hence ord$d_{M_{r-1}}(\mathfrak{n}) \leq N_r$. Notice that multiplying

$c_{M_{r-1}}(\mathfrak{n})$ with the order of $d_{M_{r-1}}(\mathfrak{n})$ gives an element in $\langle \delta(h_1), \delta(h_2) \rangle$. By construction this must be 0, hence $c_{M_{r-1}}(\mathfrak{n})$ has the same order as $d_{M_{r-1}}(\mathfrak{n})$ and therefore

$$M_{r-1} - M_r \leq N_r.$$

Conversely, by Corollary 2.1.5 there exists a prime number $\ell_r \in \mathscr{S}_1(M')$ such that

$$\begin{aligned} \mathrm{ord} c_{M_{r-1}+N_r}(\mathfrak{n}_{r-1})_{\lambda_r} &= p^{N_r}, \\ \mathrm{ord} c_{r,\lambda_r} &= p^{N_r}, \\ c_{i,\lambda_r} &= 0 \text{ for all } i > r. \end{aligned}$$

Letting $\mathfrak{n}_r = \ell_r \mathfrak{n}_{r-1}$ and $0 \leq M \leq N_i - 1$, we observe

$$\langle d_{M_{r-1}}(\mathfrak{n}_r), p^M d_i \rangle = \langle d_{M_{r-1}-M}(\mathfrak{n}_r), d_i \rangle = \sum_{j=1}^{r} \langle d_{M_{r-1}-M+N_i}(\mathfrak{n}_r)_{\lambda_j}, y_{i,\lambda_j} \rangle_{\lambda_j}.$$

Notice that this sum vanishes for $i > r$ by the choice of ℓ_j. By the same argument, for $i = r$, the ℓ_j term vanishes for all $j < r$. Notice that y_{r,λ_r} has order p^{N_r} in $A(K_\lambda)/\mathfrak{P}^{N_r} A(K_\lambda)^{\epsilon_r}$. Likewise

$$\begin{aligned} \mathrm{ord} d_{M_{r-1}+N_r-M}(\mathfrak{n}_r)_{\lambda_r} &= \mathrm{ord} c_{M_{r-1}+N_r-M}(\mathfrak{n}_r)_{\lambda_r} \\ &= \mathrm{ord} c_{M_{r-1}+N_r-M}(\mathfrak{n}_{r-1})_{\lambda_r} \\ &= p^{N_r-M} > 1. \end{aligned}$$

Hence by the non-degeneracy of the Tate pairing described in Proposition 1.5.3, we conclude that this pairing is non-trivial for $i = r$ and all $0 \leq M \leq N_r - 1$. Therefore the character

$$\mathcal{X}_r : d \mapsto \langle d_{M_{r-1}}(\mathfrak{n}_r), d \rangle$$

generates D_r^* when restricted to D_r and vanishes when restricted to D_i for $i > r$. Hence the set $\{\mathcal{X}_j \mid j \leq r\}$ vanishes on $D_{r+1} \times D_{r+2} \times \cdots$ and forms a diagonal basis for $(D_1 \times \cdots \times D_r)^*$. The character $\mathcal{X}_r$ has order at least p^{N_r}, and as it is induced by $d_{M_{r-1}}(\mathfrak{n}_r)$ we conclude that $d_{M_{r-1}}(\mathfrak{n}_r)$ has order at least p^{N_r}. As its order is bounded by $p^{M_{r-1}-M_r}$, we conclude that

$$N_r \leq M_{r-1} - M_r$$

and hence that

$$N_r = M_{r-1} - M_r.$$

□

Chapter 4

Level raising

In this chapter we slightly modify our description of Shimura curve to use a formalism which will allow us to be more clear in the next chapter. Using this new formalism we can introduce two important construction which will play an important role later.

4.1 Level raising

Let p be a rational prime, $\mathfrak{p} \subset \mathcal{O}_F$ and $\mathfrak{P} \subset \mathcal{O}_A$ be prime above p as in the previous chapter. We recall that f is the Hilbert newform associated to our abelian variety A, ρ the $\mathfrak{P}$-adic representation of A and $\rho_{\mathfrak{P}}$ is the residual representation at the prime $\mathfrak{P}$. By our surjectivity assumption it follows that the representation is irreducible, so ρ is residually irreducible. We recall that $N = N^+N^-$ where the primes in N^+ split in K and those of N^- are inert. We had assumed that N^- is square-free and that N^- as different parity than the degree of F.

From now on we assume that

Assumption 4.1.1.

1. The residual representation $\rho_{\mathfrak{P}}$ ramifies at all prime in N^+ and all $\mathfrak{q} \mid N^-$ such that $N(\mathfrak{q}) \equiv 1 \mod p$. Furthermore there are no prime $\mathfrak{q} \mid N^-$ such that $N(\mathfrak{q}) \equiv -1 \mod p$.
2. If N is not square-free, then the residual representation ramifies at least at one place dividing exactly N^- or at least at two places dividing exactly N^+.
3. For all prime ℓ such that $\ell^2 \mid N^+$ we have $H^1(F_\ell, \rho_{\mathfrak{P}}) = \rho_{\mathfrak{P}}^{D_\ell} = 0$ where D_ℓ is the decomposition group at ℓ in $\mathrm{Gal}(\overline{F}/F)$.

We are going to vary the ramification locus of the quaternion algebra B, and so we use a notation which is more explicit about it, hence we denote by X_{N^+,N^-} the Shimura curve attached to this datum.

Definition 4.1.2. A prime ideal ℓ of $\mathcal{O}_F$ is called *admissible* if

- $\ell \nmid N D_{K/F} p$;
- ℓ is inert in K;
- $p \nmid N(\ell)^2 - 1$;
- the $\mathfrak{P}$-adic valuation is $v_{\mathfrak{P}}((N(\ell)+1)^2 - a_\ell^2) \geq 1$.

Let Λ be the set of square-free product of admissible primes and Λ^+ (Λ^-) be the subset of Λ where the element are product of an even (odd) number of primes.

Since we assumed that A is a modular abelian variety of GL_2 type, the field $E = \mathcal{O}_A \otimes \mathbb{Q}$ is the field over $\mathbb{Q}$ generated by all the eigenvalues of the Hecke operators acting on f.

Let $\mathfrak{m}_f$ denote the kernel of the morphism from the Hecke algebra $\mathbb{T}$ acting on the space of Hilbert modular forms

$$\mathbb{T} \to \mathcal{O}_{A,\mathfrak{P}}/\mathfrak{P}.$$

Definition 4.1.3. We say that f is $\mathfrak{P}$-*isolated* if the completion of $\mathbb{T}$ at $\mathfrak{m}_f$ is isomorphic to $\mathcal{O}_{A,\mathfrak{P}}$.

From now on we chose p such that f is $\mathfrak{P}$-isolated and p is unramified in $\mathcal{O}_A$. By [Car94] and [Lon07, Chapter 2.5] we know that the $\mathfrak{P}$-adic representation associated to f is equivalent to the representation ρ associated to the Tate module $T_{\mathfrak{P}}A$. Hence when we consider the residual representation the underlying vector space to $\rho_{\mathfrak{P}}$ is $V = A[\mathfrak{P}]$.

Theorem 4.1.4. *For each admissible prime ℓ there exists a Hilbert newform f' of level $N\ell$ and a prime $\mathfrak{P}'$ in the field of fraction of $\mathcal{O}_{A'}$, which is generated by the Hecke eigenvalues of f', $\mathcal{O}_{A'}/\mathfrak{P}' \cong \mathcal{O}_A/\mathfrak{P}$ and for all primes $\mathfrak{q} \neq \ell$ we have*

$$a_{\mathfrak{q}}(f) \pmod{\mathfrak{P}} \equiv a_{\mathfrak{q}}(f') \pmod{\mathfrak{P}'}$$

where both sides lie in $\mathcal{O}_A/\mathfrak{P}$. Equivalently

$$\rho_{\mathfrak{P}} \cong \rho_{f',\mathfrak{P}'}$$

where $\rho_{f'}$ is the representation associated to f'.

Proof. By our assumption ρ is residually irreducible and $\mathfrak{P}$-isolated, so we can apply [Lon07, Theorem 3.3] and [DS74] to get our claim. Another approach can be found in [Jar99]. This allows us to raise the level at one admissible prime, but using our assumption on the ramification of the residual representation we can apply the same argument as in [Zha14, Theorem 2.1] to raise the level at a product of admissible primes. □

Let $\mathfrak{m} \in \Lambda$ then using this theorem we can get a Hilbert newform $f_{\mathfrak{m}}$ of level $N\mathfrak{m}$. We adopt the same notation we used for f adding an index $\mathfrak{m}$, so we have a prime $\mathfrak{P}_{\mathfrak{m}}$ such that the field generated by the Hecke eigenvalues $\mathcal{O}_{A_{\mathfrak{m}}}/\mathfrak{P}_{\mathfrak{m}} \cong \mathcal{O}_A/\mathfrak{P}$. We fix this isomorphism. By the equivalence of the residual representation the underlying two-dimensional $\mathcal{O}_A/\mathfrak{P}$-vector space does not change, so we denote it by V.

4.2 Kolyvagin system revisited

Let $\mathfrak{m} \in \Lambda^+$ be admissible with an even number of prime factors, we denote by $X_{\mathfrak{m}} = X_{N^+,N^-\mathfrak{m}}$ the Shimura curves arising from the quaternion algebra $B(\mathfrak{m})$ which ramifies also at the places dividing $\mathfrak{m}$. If $\mathfrak{m} \in \Lambda^-$ we need some extra step because we are changing the parity of the number of factor of $N^-\mathfrak{m}$, so in this case we consider the Gross curve $\mathfrak{X}_{\mathfrak{m}}$ associated to the quaternion algebra $B(\mathfrak{m}\xi)$ ramifying also at the infinite place ξ and at the places dividing $\mathfrak{m}$.

The first case is called the *indefinite* case and the second one is the *definite* case. If we consider the sign of the functional equation of the L-function associated to f in the indefinite case it is -1 and in the definite one is 1. Due to this we usually want to change the ramification only by elements of Λ^+ because otherwise we would change the sign.

For ease of notation we write in both case $B_{\mathfrak{m}}$ for the quaternion algebra we are considering and $R_{\mathfrak{m}}$ for the subgroup generated by the Eichelr order.

Tracing back our construction we have the abelian variety A associated to the Hilbert newform f and the Shimura curve X. Given $\mathfrak{m} \in \Lambda^+$ we get a new Shimura curve $X_{\mathfrak{m}}$ which generates an abelian variety $A_{\mathfrak{m}}$ associated to the Hilbert newform $f_{\mathfrak{m}}$ that we got by raising the level of f at $\mathfrak{m}$. We denote by $\mathcal{O}_{A_{\mathfrak{m}}}$ the endomorphism ring of $A_{\mathfrak{m}}$.

In this same spirit we can define Heegner points and classes on the object related to the raised Hilbert modular form. We consider from now on $M = 1$, and so we drop it from the notation. Let $\mathfrak{n} \in \mathscr{S}(1)$, we define the Heegner points

$$x_{\mathfrak{n}}(\mathfrak{m}) \in X_{\mathfrak{m}}(K[\mathfrak{n}]) \qquad \text{and} \qquad y_{\mathfrak{n}}(\mathfrak{m}) \in A_{\mathfrak{m}}(K[\mathfrak{n}])$$

in the same way as before; similarly, we define the Gross points

$$\mathfrak{x}_{\mathfrak{n}}(\mathfrak{m}) \in \mathfrak{X}_{\mathfrak{m}}.$$

Following the construction of [Zha14] we con provide a reduction and a specialization map acting on Heegner points. Since this construction is a simple generalization of the work of Zhang we just sketch the main steps and provide the required results in our setting. Let $\mathscr{H}_{\mathfrak{m}}$ denotes the set of CM-point on the Shimura curve $X_{\mathfrak{m}}$ of conductor 1 with positive orientation (for the precise definition see [Zha01b]).

Lemma 4.2.1. *Let $\mathfrak{m} \in \Lambda^+$, $q \in \Lambda$ a prime not dividing $\mathfrak{m}$ and $q' \in \Lambda$ a prime dividing $\mathfrak{m}$, let $\mathfrak{n} \in \mathscr{S}(1)$, then there are two maps*

$$\mathrm{Red}_q \colon \mathscr{H}_{\mathfrak{m}} \to \mathfrak{X}_{\mathfrak{m}q},$$

$$\mathrm{Sp}_{q'} \colon \mathscr{H}_{\mathfrak{m}} \to \mathfrak{X}_{\mathfrak{m}/q'}$$

such that

$$\mathrm{Red}_q(x_{\mathfrak{n}}(\mathfrak{m})) = \mathfrak{x}_{\mathfrak{n}}(\mathfrak{m}q) \in \mathfrak{X}_{\mathfrak{m}q},$$

$$\mathrm{Sp}_{q'}(x_{\mathfrak{n}}(\mathfrak{m})) = \mathfrak{x}_{\mathfrak{n}}(\mathfrak{m}/q) \in \mathfrak{X}_{\mathfrak{m}/q'}.$$

Proof. We use the reduction of the canonical integral models as constructed by Zhang in [Zha01b] and [Zha01a]: $X_{\mathfrak{m}}$ has an integral model over $\mathbb{Z}_q$ parametrizing abelian varieties with auxiliary structure. Then the integral model has good reduction at q and the set of supersingular points is $X_{\mathfrak{m}}^{ss} \cong \mathfrak{X}_{\mathfrak{m}q}$, thus giving us an embedding $K \hookrightarrow B_{\mathfrak{m}q}$. The Heegner points $x_{\mathfrak{n}}(\mathfrak{m})$ reduce to supersingular points in $X_{\mathfrak{m}}^{ss}$ when reducing modulo a prime above q (see [Zha14, Section 3.5]), so composing with the isomorphism to $\mathfrak{X}_{\mathfrak{m}q}$ we get the map Red_q.

Using the theory of Drinfeld and Cerednik we can study the irreducible components of $X_{\mathfrak{m}}$ and the graph associated to them. Using [Zha01b, Proposition 1.3.4] and [Zha01a, Lemma 5.4.4] we have an adelic description of the group of irreducible components of $X_{\mathfrak{m}}$. Then following [Zha14, Section 3.4] we construct another embedding $K \hookrightarrow B_{\mathfrak{m}/q'}$ and by [Lon12, Section 7.5] we find a relation between the set of vertices of the graph associated to the geometrically irreducible components of $X_{\mathfrak{m}}$ and $\mathfrak{X}_{\mathfrak{m}/q'}$. The Heegner points $x_{\mathfrak{n}}(\mathfrak{m})$ reduce to non-singular points in the special fiber of $X_{\mathfrak{m}}$ when reducing modulo a prime above q' (see [Zha14, Section 3.5]), hence we have a map from $\mathscr{H}_{\mathfrak{m}}$ to the set of irreducible components, and so composing with the map to $\mathfrak{X}_{\mathfrak{m}/q'}$ we get the map $\mathrm{Sp}_{q'}$.

Using the adelic description the required relations follow immediately. □

We now want to define the Kolyvagin classes using the idea of level raising. Let $\mathbb{T}_{\mathfrak{m}}$ denote the algebra of Hecke operators on the space Hilbert modular form of parallel weight 2 which are new at all places dividing $N^-\mathfrak{m}$, we have a morphism

$$\lambda_{f_{\mathfrak{m}}} : \mathbb{T}_{\mathfrak{m}} \to \mathcal{O}_{A_{\mathfrak{m}}}$$

that gives the eigenvalue of the Hecke operator. We can consider the reduction modulo $\mathfrak{P}_{\mathfrak{m}}$, and we get a map

$$\overline{\lambda}_{f_{\mathfrak{m}}} : \mathbb{T}_{\mathfrak{m}} \to \mathcal{O}_{A_{\mathfrak{m}}}/\mathfrak{P}_{\mathfrak{m}}.$$

Let $\mathfrak{M}$ denote the kernel of $\overline{\lambda}_{f_{\mathfrak{m}}}$. We have that $\mathrm{Jac}(X_{\mathfrak{m}})[\mathfrak{M}] \cong V \cong A_{\mathfrak{m}}[\mathfrak{P}_{\mathfrak{m}}]$ since the residual representation are isomorphic.

Now for every $\mathfrak{n} \in \mathscr{S}(1)$ and $\mathfrak{m} \in \Lambda^+$ we can define a Kolyvagin class

$$c(\mathfrak{n}, \mathfrak{m}) \in H^1(K, A_{\mathfrak{m}}[\mathfrak{P}_{\mathfrak{m}}]) \cong H^1(K, V)$$

derived as before from the Heegner points $x_{\mathfrak{n}}(\mathfrak{m})$ and $y_{\mathfrak{n}}(\mathfrak{m})$. When $\mathfrak{m} = 1$ we have the classical case, so we drop the index: $c(\mathfrak{n}, 1) = c(\mathfrak{n})$.

Definition 4.2.2. Let $\mathfrak{m} \in \Lambda^+$, then we denote by $\kappa_{\mathfrak{m}}$ the *Kolyvagin system*

$$\kappa_{\mathfrak{m}} = \left\{ c(\mathfrak{n}, \mathfrak{m}) \in H^1(K, V) \mid \mathfrak{n} \in \mathscr{S}(1) \right\}.$$

We now introduce some local cohomology group which are used to impose local condition on cohomology classes.

Definition 4.2.3. Let v be a prime non dividing N,then we define the *finite* or *unramified* part of $H^1(K_v, V)$

$$H^1_{fin}(K_v, V) = H^1_{ur}(K_v, V)$$

as the inflation of $H^1(K_v^{ur}/K_v, V)$ where K_v^{ur} is the maximal unramified extension of K_v.

The *singular* part is

$$H^1_{sing}(K_v, V) = H^1(I_v, V)^{\mathrm{Gal}(K_v^{ur}/K_v)}$$

where I_v is the ramification group at v.

By the inflation-restriction exact sequence we get that

$$0 \to H^1_{fin}(K_v, V) \to H^1(K_v, V) \to H^1_{sing}(K_v, V).$$

We now assume that q is an admissible prime, then the Galois module V is unramified at q, so as $\mathrm{Gal}(\overline{K}_q/K_q)$-module the space V splits as

$$V \cong \mathcal{O}_A/\mathfrak{P} \oplus \mathcal{O}_A/\mathfrak{P}(1)$$

where $\mathcal{O}_A/\mathfrak{P}(1)$ is the usual twist. Following [Tam21, Lemma 6.6] this decomposition indices a direct sum in cohomology

$$H^1(K_q, V) = H^1(K_q, \mathcal{O}_A/\mathfrak{P}) \oplus H^1(K_q, \mathcal{O}_A/\mathfrak{P}(1)).$$

Lemma 4.2.4. *Let q be an admissible prime, then*

1. $\dim H^1(K_q, \mathcal{O}_A/\mathfrak{P}) = \dim H^1(K_q, \mathcal{O}_A/\mathfrak{P}(1)) = 1$;

2. In $H^1(K_q, V)$ we have that

$$H^1_{fin}(K_q, V) = H^1(K_q, \mathcal{O}_A/\mathfrak{P}),$$
$$H^1_{sing}(K_q, V) \cong H^1(K_q, \mathcal{O}_A/\mathfrak{P}(1)).$$

Proof. The first part and the equality for the unramified part follows from [Tam21, Lemma 6.19]. For the last part the required isomorphism is induced by the restriction map. □

For an admissible prime q we have the following decomposition

$$H^1(K_q, V) = H^1_{fin}(K_q, V) \oplus H^1_{sing}(K_q, V).$$

Let v be a place of K, then we define $\mathrm{loc}_v \colon H^1(K, V) \to H^1(K_v, V)$ the localization map. We have the following important congruence between Heegner points which in the classical case over $\mathbb{Q}$ is due to Bertolini and Damon and in the case over totally real filed to Longo ([Lon12]).

Theorem 4.2.5. *Let $\mathfrak{m} \in \Lambda^+$ and q_1, q_2 be two admissible primes not dividing $\mathfrak{m}$, then we have*

$$\mathrm{loc}_{q_1}(c(\mathfrak{n}, \mathfrak{m})) \in H^1(K_q, \mathcal{O}_A/\mathfrak{P}) \qquad \text{and} \qquad \mathrm{loc}_{q_2}(c(\mathfrak{n}, \mathfrak{m}q_1q_2)) \in H^1(K_q, \mathcal{O}_A/\mathfrak{P}(1)).$$

Fixing isomorphisms $H^1(K_{q_1}, \mathcal{O}_A/\mathfrak{P}) \cong \mathcal{O}_A/\mathfrak{P} \cong H^1(K_{q_2}, \mathcal{O}_A/\mathfrak{P}(1))$ we have an equality for all $\mathfrak{n} \in \mathscr{S}(1)$ up to a unit in $\mathcal{O}_A/\mathfrak{P}$:

$$\mathrm{loc}_{q_1}(x(\mathfrak{n}, \mathfrak{m})) = \mathrm{loc}_{q_2}(c(\mathfrak{n}, \mathfrak{m}q_1q_2)).$$

Proof. Let A^0, A^0_1, A^0_2 the abelian varieties associated to the Hilbert newforms $f_{\mathfrak{m}}$, $f_{\mathfrak{m}q_1}, f_{\mathfrak{m}q_1q_2}$, they all have the same vector space V associated to their representation by level raising.

We start from calculating $\mathrm{loc}_{q_1}(x(\mathfrak{n}, \mathfrak{m}))$. We have the Kummer map which goes into the finite part of the cohomology, so we have

$$\delta_{q_1} \colon J(X_{\mathfrak{m}})(K_{q_1}) \to A^0(K_{q_1}) \to H^1_{fin}(K_{q_1}, A^0[\mathfrak{P}_{\mathfrak{m}}]) \cong H^1_{fin}(K_{q_1}, V) = H^1(K_{q_1}, \mathcal{O}_A/\mathfrak{P}).$$

It follows from [Lon12, Section 7.4] that there exists an eigenform

$$\phi \colon \mathfrak{X}_{\mathfrak{m}q_1} \to \mathcal{O}_A/\mathfrak{P}$$

such that

- ϕ is the reduction of the Jacquet-Langlands correspondence of $f_{\mathfrak{m}q_1}$, this determines ϕ uniquely up to a scalar;
- It calculates the image of the local Kummer map of Heegner points on $X_{\mathfrak{m}}$: for a suitable choice of isomorphism $H^1(K_{q_1}, \mathcal{O}_A/\mathfrak{P}) \cong \mathcal{O}_A/\mathfrak{P}$ we have

  $$\phi(\mathrm{Red}_{q_1}(x)) = \delta_{q_1}(x) \in \mathcal{O}_A/\mathfrak{P}$$

  for all Heegner points.
  This follows from [Lon12, Lemma 7.20] as a consequence of Ihara's lemma for Shimura curves over totally real fields ([MS21]).

We now calculate $\mathrm{loc}_{q_2}(c(\mathfrak{n}, \mathfrak{m}q_1q_2))$. Again we want to compute the local Kummer map

$$\delta_{q_2} \colon J(X_{\mathfrak{m}q_1q_2})(K_{q_2}) \to A^0_2(K_{q_2}) \to H^1_{sing} = H^1(K_{q_2}, \mathcal{O}_A/\mathfrak{P}(1)).$$

The image of $A^0_2(K_{q_2})$ is in the singular part since $J(X_{\mathfrak{m}q_1q_2})(K_{q_2})$ has purely multiplicative reduction at q_2 by [Tam21, Theorem 6.13] and [Lon12]. This completes the proof of the first claim.

Let $J = J(X_{\mathfrak{m}q_1q_2})$, by [Lon12, Section 7.5] it follows that

- The Kummer map $J(K_{q_2}) \to H^1(K_{q_2}, J[\mathfrak{M}]) = H^1(K_{q_2}, V)$ factors through the group $\Phi(J/K_{q_2})$ of connected components of the Neron model of J over K_{q_2};
- The specialization map always lies in $\mathfrak{X}_{\mathfrak{m}q_1}$. By [Lon12, Pag. 344] there is a homomorphism which calculates the specialization to the group $\Phi(J/K_{q_2})$;
- The Hecke eigenform ϕ also calculate the local Kummer map on $X_{\mathfrak{m}q_1q_2}$: for a suitable choice of the isomorphism $H^1(K_{q_2}, \mathcal{O}_A/\mathfrak{P}(1)) \cong \mathcal{O}_A/\mathfrak{P}$ we have

$$\phi(\mathrm{Sp}_{q_2}(x)) = \delta_{q_2}(x) \in \mathcal{O}_A/\mathfrak{P}$$

  for all Heegner points in $\mathscr{H}_{\mathfrak{m}}$.

From the previous analysis of the geometric behavior of these two maps in 4.2.1 and the above description of the Kummer maps in terms of ϕ we get for all $\mathfrak{n} \in \mathscr{S}(1)$

$$\mathrm{loc}_{q_1} \circ \delta_{q_1}(y_n(\mathfrak{m})) = \mathrm{loc}_{q_2} \circ \delta_{q_2}(y_n(\mathfrak{m}q_1q_2))$$

up to a unit in $\mathcal{O}_A/\mathfrak{P}$. Now the classes $c(\mathfrak{n}, \mathfrak{m})$ are derived from the Heegner points, so from the Kummer images of the $y_{\mathfrak{n}}(\mathfrak{m})$ applying the Kolyvagin derivative operator, which by the construction are compatible when varying $\mathfrak{m}$. Then clearly this equality implies the last claim of the theorem. □

Remark 4.2.6. There is an analogue of this theorem in the other index of the class $c(\mathfrak{n}, \mathfrak{m})$ arising from a finite/singular morphism ψ_ℓ at $\ell \in \mathscr{S}(1)$ (cf. 2.3.7):

$$\psi_\ell(\mathrm{loc}_\ell c(\mathfrak{n}, \mathfrak{m})) = \mathrm{loc}_\ell(c(\mathfrak{n}\ell, \mathfrak{m})).$$

Chapter 5

Selmer groups

In this chapter we want to study some properties of the Selmer groups attached to A and the effect of the level raising on them. This will be important as it is one of the main technique used in the proof of the final results. The main reference for this chapter is [Tam21].

5.1 Local conditions

Let ℓ be a prime, then we denote by δ_ℓ the Kummer map. We recall the classical definition of Selmer groups can be written as

$$\mathrm{Sel}_{\mathfrak{p}}(A/K) = \left\{ c \in H^1(K, A[\mathfrak{p}]) \mid \mathrm{loc}_\ell(c) \in \mathrm{Im}(\delta_\ell) \text{ for all } \ell \right\}.$$

Since we have identified $A[\mathfrak{P}]$ with V we can see the image of the Kummer map as a subspace of $H^1(K_\ell, V)$.

Definition 5.1.1. A *system of local conditions* is a choice of a subspace

$$H^1_f(K_\ell, A[\mathfrak{P}]) \subseteq H^1_f(K_\ell, A[\mathfrak{P}])$$

for all places ℓ.

We take $H^1_f(K_\ell, A[\mathfrak{P}]) = \mathrm{Im}(\delta_\ell)$ for all ℓ. Under suitable hypothesis we can describe a system of local conditions only in terms of Galois structure on V together with the information of the reduction type at every prime.

Lemma 5.1.2. *1. Let ℓ be a prime and let Gal_ℓ denote the decomposition group at ℓ, then*

$$H^1(F_\ell, V) = 0 \iff V^{\mathrm{Gal}_\ell} = 0.$$

2. If A is an elliptic curve with additive reduction at a prime $\ell \nmid p$, then

$$H^1(F_\ell, V) = 0.$$

Proof. Since $\ell \nmid p$ by Tate Theorem [Mil06, Theorem 2.8] the Euler-Poincaré characteristic is $\chi(\mathrm{Gal}_\ell, V) = 1$. We recall that V is self dual ($\det(\rho)$ is the p-adic cyclotomic character), so the local duality tells us that $H^0(\mathrm{Gal}_\ell, V)$ is dual to $H^2(\mathrm{Gal}_\ell, V^*) = H^2(\mathrm{Gal}_\ell, V)$, hence they

have the same dimension. Since $H^0(\mathrm{Gal}_\ell, V) = V^{\mathrm{Gal}_\ell}$, by the definition of the Euler-Poincaré characteristic

$$\chi(\mathrm{Gal}_\ell, V) = \frac{\#H^0(\mathrm{Gal}_\ell, V)\#H^2(\mathrm{Gal}_\ell, V)}{\#H^1(\mathrm{Gal}_\ell, V)},$$

so the first part of the lemma is proved.

To show the second part we can just prove that $V^{\mathrm{Gal}_\ell} = 0$ and since $\ell \nmid p$ it is equivalent to $A(F_\ell)/pA(F_\ell) = 0$. A has additive reduction, so there is a filtration $A_1(F_\ell) \subset A_0(F_\ell) \subset A(F_\ell)$ such that $A_1(F_\ell)$ is a pro-ℓ-group, $A_0(F_\ell)/A_1(F_\ell)$ is isomorphic to the residue field of F_ℓ and $A(F_\ell)/A_0(F_\ell)$ is isomorphic to the component group of the Neron model of A/F_ℓ. The component group of an elliptic curve has order at most 4, hence $A(f_\ell)/pA(F_\ell) = 0$. □

We now want to study how the local conditions change with level raising, so let q be an admissible prime.

Theorem 5.1.3. *For all prime $\ell \neq q$ the local conditions does not change*

$$H^1_f(K_\ell, A[\mathfrak{P}]) = H^1_f(K_\ell, A_q[\mathfrak{P}_q]).$$

If $\ell = q$ then

$$H^1_f(K_q, A[\mathfrak{P}]) = H^1(K_q, \mathcal{O}_A/\mathfrak{P}) \qquad \text{and} \qquad H^1_f(K_q, A_q[\mathfrak{P}_q]) = H^1(K_q, \mathcal{O}_A/\mathfrak{P}(1)).$$

Proof. The proof is a direct generalization of [Zha14, Theorem 5.2] and [GP12, Lemma 8] using the analogues result of [Lon12, Section 5.2], [Tam21, Proof of Theorem 6.17] and [Nek12]. This is the only place where we need the last item of Assumptions 4.1.1. At primes not dividing Nq both varieties have good reduction and at primes dividing N both have purely toric reduction, so the condition are the same. The only prime where things go differently is q since one has good reduction and the other one purely toric. At primes dividing p we can describe the local condition using flat cohomology, and they coincide. □

We can define four important local condition: we keep the local condition at all primes different from q and then one of the following at q

- The unramified condition: $H^1_u(K_q, A[\mathfrak{P}]) = H^1(K_q, \mathcal{O}_A/\mathfrak{P})$;
- The transverse condition: $H^1_t(K_q, A[\mathfrak{P}]) = H^1(K_q, \mathcal{O}_A/\mathfrak{P}(1))$;
- The relaxed condition: $H^1_r(K_q, A[\mathfrak{P}]) = H^1(K_q, A[\mathfrak{P}])$;
- The strict condition: $H^1_s(K_q, A[\mathfrak{P}]) = 0$.

We define the Selmer groups

$$\mathrm{Sel}_*(A/K) = \left\{c \in H^1(K, A[\mathfrak{P}]) \mid \mathrm{loc}_\ell(c) \in H^1_*(K_\ell, A[\mathfrak{P}]) \text{ for all } \ell\right\}$$

where $*$ can be one of the previous four possible condition at q, and we have the following lemma about the parity of the dimensions of these groups

Lemma 5.1.4. *If* $\mathrm{loc}_q\colon \mathrm{Sel}_u(A/K) \to H^1_u(K_q, A[\mathfrak{P}])$ *is non-zero, then*

1. $\dim_{\mathcal{O}_A/\mathfrak{P}} \mathrm{Sel}_r(A/K) = \dim_{\mathcal{O}_A/\mathfrak{P}} \mathrm{Sel}_s(A/K) + 1$,
2. $\mathrm{Sel}_u(A/K) = \mathrm{Sel}_r(A/K)$ *and* $\mathrm{Sel}_t(A/K) = \mathrm{Sel}_s(A/K)$.

If $\mathrm{loc}_q\colon \mathrm{Sel}_t(A/K) \to H^1_t(K_q, A[\mathfrak{P}])$ *is non-zero, then*

1. $\dim_{\mathcal{O}_A/\mathfrak{P}} \mathrm{Sel}_r(A/K) = \dim_{\mathcal{O}_A/\mathfrak{P}} \mathrm{Sel}_s(A/K) + 1$,
2. $\mathrm{Sel}_t(A/K) = \mathrm{Sel}_r(A/K)$ *and* $\mathrm{Sel}_u(A/K) = \mathrm{Sel}_s(A/K)$.

Proof. This follows from the proof of [Tam21, Lemma 7.8]. □

5.2 Rank lowering

Using the parity lemma we can prove the main theorem about the relation between Selmer group and level raising.

Theorem 5.2.1. *If the localization* $\mathrm{loc}_q\colon \mathrm{Sel}_{\mathfrak{P}}(A/K) \to H^1_{fin}(K_q, V) = H^1(K_q, \mathcal{O}_A/\mathfrak{P})$ *is surjective, then we have*

$$\dim_{\mathcal{O}_{A_q}/\mathfrak{P}_q} \mathrm{Sel}_{\mathfrak{P}_q}(A_q/K) = \dim_{\mathcal{O}_A/\mathfrak{P}} \mathrm{Sel}_{\mathfrak{P}}(A/K) - 1.$$

Moreover we have

$$\mathrm{Sel}_{\mathfrak{P}_q}(A_q/K) = \mathrm{K}er(\mathrm{loc}_q\colon \mathrm{Sel}_{\mathfrak{P}}(A/K) \to H^1_{fin}(K_q, V)).$$

Proof. The first part follows immediately from the parity lemma. The second part follows since $\mathrm{Sel}_{\mathfrak{P}_q}(A_q/K) = \mathrm{Sel}_s(A/K)$ is the strict Selmer group and $\mathrm{Sel}_{\mathfrak{P}}(A_q/K) = \mathrm{Sel}_r(A/K)$ is the relaxed Selmer group. □

This principle of level raising and rank lowering is at the base of the proof of our main result. Using this we can prove the non-vanishing of the Kolyvagin system, so our Kolyvagin classes are non-trivial and can be used to deduce the $\mathfrak{P}$-part of the Birch and Swinnerton-Dyer conjecture.

5.3 L-functions

In order to obtain information about the non-vanishing of Heegner points we use the central values of some L-function and in particular a formula of Zhang [Zha01a] which generalize the usual Gross formula for modular curves. Let $\mathfrak{X}$ denote the Gross curve.

Using the Jacquet-Langlands correspondence we can find a normalized eigenform $\phi\colon \mathfrak{X} \to \mathcal{O}_A$. We normalize ϕ in such a way that its Petersson norm is 1 and its image in $\mathcal{O}_{A,\mathfrak{P}}$ contains a $\mathfrak{P}$-adic unit. This determines ϕ up to a $\mathfrak{P}$-adic unit. In this case the Petersson product is defined using the counting measure since the set $\mathfrak{X}$ is finite. Let $\mathfrak{x}_K = \mathrm{Tr}_{K[1]/K}\, \mathfrak{x}(1)$. We recall that the degree of the field F is g.

Theorem 5.3.1 (Gross-Zhang formula)**.** *The following equality holds*

$$|\phi(\mathfrak{x}_K)|^2 = \frac{N(D_{K/F})^{1/2}}{2^g} \frac{L(f/K, 1)}{\langle f, f\rangle_{Pet}}$$

where $D_{K/F}$ *is the relative discriminant of* K/F, $\langle\cdot,\cdot\rangle_{Pet}$ *is the Petersson inner product and* $L(f/K, s)$ *is the L-function over* K*.*

Let $\mathbb{T}_{N^+,N^-}$ be the N^--new quotient of the Hecke algebra generated by the Hecke operators acting on the parallel weight 2 forms of level N^+. Let λ_f be the morphism associated to f

$$\lambda_f\colon \mathbb{T}_{N^+,N^-} \to \mathcal{O}_A \hookrightarrow \mathcal{O}_{A,\mathfrak{P}}.$$

Definition 5.3.2.

- The *congruence number* η_B is a generator of the congruence ideal, so

$$(\eta_B) = \lambda_f(\mathrm{Ann}_{\mathbb{T}_{N^+,N^-}} \ker(\lambda_f))\mathcal{O}_{A,\mathfrak{P}}.$$

It is well-defined up to a $\mathfrak{P}$-adic unit.

- The *canonical* or *Gross period* is

$$\Omega_f^{can} = \frac{\langle f, f\rangle_{Pet}}{\eta_B}.$$

- The *algebraic part* of the special value of $L(f/K, 1)$ is

$$L^{alg}(f/K, 1) = \frac{L(f/K, 1)}{\Omega_f^{can}\eta_B}.$$

Remark 5.3.3. We use the congruence number just to define the Gross period, but it has some really deep application. For example, it is strictly related to the idea of complete intersection algebras (see [Dia97] and [Len95]) and to the theory of the congruence of modular forms thanks to the works of Hida.

In particular since f has trivial central character the field E, i.e. the fraction field of $\mathcal{O}_A$, is totally real, hence $|\phi(\mathfrak{x}_K)|^2 = \phi(\mathfrak{x}_K)^2$. Recall that $v_{\mathfrak{P}}$ is the $\mathfrak{P}$-adic valuation, then

Corollary 5.3.4.

$$2v_{\mathfrak{P}}(\phi(\mathfrak{x}_K)) = v_{\mathfrak{P}}(L^{alg}(f/K, 1)).$$

Assume to be in the indefinite case, i.e. the number of prime factor in N^- has different parity than $[F\colon \mathbb{Q}]$. In particular in this case the sign of the functional equation for the L-function is -1 and so $L(f/K, 1) = 0$, so we cannot use the Gross-Zhang formula. However, we can find a criterion to test the vanishing of the Heegner points y_K using the level raising.

Theorem 5.3.5. *Let q be an admissible prime. Assume to be in the indefinite case, then the class $c(1) \in H^1(K, A[\mathfrak{P}])$ is locally non-trivial at q if and only if the algebraic part $L^{alg}(f_q/K, 1)$ is a $\mathfrak{P}_q$-adic unit.*

Proof. Since we are in the indefinite case, the number of factor of N^-q has the same parity as $[F\colon \mathbb{Q}]$, so the central value is not zero.

Let $\mathfrak{n} \in \mathscr{S}(1)$, by the Lemma 4.2.1, the reduction at q of the Heegner point $x_{\mathfrak{n}}(1)$ is $\mathrm{Red}_q(x_{\mathfrak{n}}(1)) = \mathfrak{x}_{\mathfrak{n}}(q)$. Hence, we can compare the Heegner divisor $x_K = x_{1,K}$ and $\mathfrak{x}_{q,K}$ which is the one associated to the reduction:

$$x_{1,K} = \mathrm{Tr}_{K[1]/K}\, x_1(1),$$

$$\mathfrak{x}_{q,K} = \mathrm{Tr}_{K[1]/K}\, \mathfrak{x}_1(q).$$

Let ϕ_q be the normalized eigenform obtained from the Jacquet-Langlands correspondence on f_q, then the reduction

$$\phi_q \mod \mathfrak{P}_q\colon \mathfrak{X}_q \to \mathcal{O}_{A_q}/\mathfrak{P}_q$$

is a Hecke eigenform and hence equal to a multiple of the function ϕ of Theorem 4.2.5 considering $\mathfrak{m} = 1$ by [Man21]. Possibly replacing ϕ_q by a multiple we may assume that $\phi_q \mod \mathfrak{P}_q = \phi$, in particular we have

$$\phi_q(\mathfrak{x}_{q,K}) \mod \mathfrak{P}_q = \phi(\mathfrak{x}_{q,K}).$$

Fixing an isomorphism $H^1_{fin}(K_q, V) \cong \mathcal{O}_A/\mathfrak{P}$, by 4.2.5 we have that

$$\mathrm{loc}_q(c(1)) = \phi(\mathfrak{x}_{q,K}) \in \mathcal{O}_A/\mathfrak{P}.$$

So by the Gross-Zhang formula, up to a $\mathfrak{P}$-adic unit, we have

$$\mathrm{loc}_q(c(1))^2 = \phi(\mathfrak{x}_{q,K})^2 = \phi_q(\mathfrak{x}_{q,K})^2 = L^{alg}(f_q/K, 1) \mod \mathfrak{P}_q$$

where all values are in $\mathcal{O}_A/\mathfrak{P}$. The theorem then follows. □

Remark 5.3.6. There is also an analogue version when we are in the definite case, see [Tam21, Thorem 6.19]. In this case we take q as the product of two different admissible primes.

This theorem and its analogue rely heavily on the Ihara's lemma which has been proven for Shimura curve over totally real field in [MS21].

The Birch and Swinnerton-Dyer formula over $\mathbb{Q}$ was proved in rank zero by Kato, Skinner and Urban. We need a similar version over totally real fields.

Theorem 5.3.7. *Assume that p is a good ordinary prime, the image of the residual Galois representation contains $\mathrm{SL}_2(\mathbb{F}_\mathfrak{p})$ and if $[F\colon \mathbb{Q}]$ is even and the global sign of f is -1 then the automorphic representation of f is special in at least one finite place, then $L(f/K,1)\neq 0$ if and only if $\mathrm{Sel}_{\mathfrak{P}^\infty}(A/K)$ is finite, furthermore in this case we have*

$$\mathrm{lenght}_{\mathcal{O}_{A,\mathfrak{P}}}\mathrm{Sel}_{\mathfrak{P}^\infty}(A/K)=v_\mathfrak{P}(L^{alg}(f/K,1)).$$

Proof. This follows from [Tam21, Theorem 5.2]. Since our representation is residually irreducible then we can use [Wan15] to apply [Tam21, Remark 6.11] and prove the theorem. □

We can now state an important non-vanishing result in the rank one case, but before we need the following

Lemma 5.3.8. *Let $c\in H^1(K,A[\mathfrak{P}])$ be a non-zero class. There exists a positive density of admissible primes q such that the localization $\mathrm{loc}_q(c)$ is non-zero.*

Proof. This is [Tam21, Lemma 7.4]. It is a simple application of the Čebotarev density theorem. □

Theorem 5.3.9. *If $\dim_{\mathcal{O}_A/\mathfrak{P}}\mathrm{Sel}_\mathfrak{P}(A/K)=1$ then the class $c(1)$ is non-zero.*

Proof. Let c be a generator of $\mathrm{Sel}_\mathfrak{P}(A/K)\subset H^1(K,A[\mathfrak{P}])$. We can choose an admissible prime q such that $\mathrm{loc}_q(c)\neq 0$. Using level raising we can find a Hilbert newform f_q of level Nq. Note that our Assumptions 4.1.1 are stable under level raising. Then clearly the localization

$$\mathrm{loc}_q\colon \mathrm{Sel}_\mathfrak{P}(A/K)\to H^1_{fin}(K_q,A[\mathfrak{P}])$$

is surjective. By Proposition 5.2.1, we have that $\dim_{\mathcal{O}_{A_q,\mathfrak{P}_q}}\mathrm{Sel}_{\mathfrak{P}_q}(A_q/K)=0$. In particular $\mathrm{Sel}_{\mathfrak{P}^\infty}(A_q/K)=0$. Therefore, by 5.3.7, we have

$$v_\mathfrak{P}(L^{alg}(f_q/K,1))=0,$$

so $L^{alg}(f_q/K,1)$ is a $\mathfrak{P}_q$-adic unit, hence by 5.3.5 the class $c(1)$ is non-zero. □

5.4 Triangulization of Selmer groups

We recall some properties of the Kolyvagin system and some consequence for the Selmer groups which will lead us to construct a triangular basis for it. Let $\mathfrak{m}\in\Lambda^+$ be a fixed element throughout this section. Since it is fixed we drop it from the notation to simplify it.

Definition 5.4.1. Let $\ell\in\mathscr{S}_1(1)$, the *transverse* part $H^1_{tr}(K_\ell,V)$ is the subspace of $H^1(K_\ell,V)$ arising from the inflation of $H^1(K[\ell]_\lambda,V)$ where λ is a prime of $K[\ell]$ over ℓ.

Following [How04] we have a finite/singular split exact sequence giving the decomposition

$$H^1(K_\ell,V)=H^1_{fin}(K_\ell)\oplus H^1_{tr}(K_\ell,V)$$

where each component is totally maximal isotropic under the action of the local Tate pairing. In general the finite part is, by definition, the local condition of Theorem 5.1.3.

Proposition 5.4.2. *The Kolyvagin system κ has the following properties*

1. *For every prime ℓ and $\mathfrak{n} \in \mathscr{S}(1)$ we have*

$$\mathrm{loc}_\ell(c(\mathfrak{n})) \in \begin{cases} H^1_{fin}(K_\ell, V) & (\ell, \mathfrak{n}) = 1 \\ H^1_{tr}(K_\ell, V) & \ell \mid \mathfrak{n} \end{cases}$$

2. *For each prime $\ell \in \mathscr{S}_1(1)$ there is a finite/singular morphism*

$$\psi_\ell \colon H^1_{fin}(K_\ell, V) \to H^1_{tr}(K_\ell, V)$$

such that for all $\mathfrak{n} \in \mathscr{S}(1)$ with $(\ell, \mathfrak{n}) = 1$ we have

$$\mathrm{loc}_\ell(c(\mathfrak{n}\ell)) = \psi_\ell(\mathrm{loc}_\ell(c(\mathfrak{n}))).$$

Proof. The first statement follows by [Tam21], the second one from Theorem 2.3.7. □

Recall our surjectivity assumptions on the residue Galois representation, then

Lemma 5.4.3. *Let c_1, c_2 be two $\mathcal{O}_A/\mathfrak{P}$-linear independent elements in $H^1(K, V)$, then there exists a positive density of primes $\ell \in \mathscr{S}_1(1)$ such that*

$$\mathrm{loc}_\ell(c_1) \neq 0 \qquad i = 1, 2.$$

Proof. This follows from Proposition 2.1.4. □

Lemma 5.4.4. *Let $\ell \in \mathscr{S}_1(1)$ and S a finite subset of $\mathscr{S}(1)$ not containing ℓ. Then there exists $c \in H^1(K, V)^{\pm}$ such that*

- *$c \neq 0$;*
- *$\mathrm{loc}_v c \in H^1_{fin}(K_v, V)$ for all v outside $S \cup \{\ell\}$;*
- *$\mathrm{loc}_v c \in H^1_{tr}(K_v, V)$ for all $v \in S$.*

Proof. The same proof of Lemma 3.2.5 works. □

This last lemma tells us that we can pick up an element with a prescribed set of places where it lays in the transverse part of the cohomology.

Definition 5.4.5.

- Let κ be a Kolyvagin system. The *vanishing order* ν of κ is

$$\nu = \min\{r \in \mathbb{Z}_+ \mid \exists\ \mathfrak{n} \in \mathscr{S}_r(1) \text{ such that } c(\mathfrak{n}) \neq 0\}.$$

  If $\kappa = \{0\}$ we say that $\nu = \infty$.

- A prime ℓ is called a *base point* of κ if $\ell \nmid D_{K/F} Np$ and $\mathrm{loc}_\ell(c(\mathfrak{n})) = 0$ for all $\mathfrak{n} \in \mathscr{S}(1)$. The set of all base point is called the *base locus* of κ and is denoted by $\mathscr{B}(\kappa)$.

The following theorem gives us the structure of the Selmer group, providing it with a triangular basis for some eigenspaces. The important aspect is that this basis is composed only of Kolyvagin classes. This will be important in the argument to prove the main result. The proof of this theorem is very similar to the one of the structure theorem for Shafarevich-Tate groups, in fact it relies more or less on the same technique.

Theorem 5.4.6. *Assume that κ is not trivial (i.e. ν is finite), then we have*

1. *The ϵ_ν-eigenspace $\mathrm{Sel}^{\epsilon_\nu}_{\mathfrak{P}}(A/K)$ is of dimension $\nu+1$ and $\mathrm{Sel}^{-\epsilon_\nu}_{\mathfrak{P}}(A/K)$ has dimension at most ν;*

2. *There exist $2\nu+1$ distinct prime $l_1,\cdots,l_{2\nu+1}\in\mathscr{S}_1(1)$ such that the classes*

$$c(\mathfrak{n}_i)\in H^1(K,V)\qquad \mathfrak{n}_i=l_il_{i+1}\dots l_{i+\nu-1}$$

for $1\le i\le\nu+1$ form a basis of $\mathrm{Sel}^{\epsilon_\nu}_{\mathfrak{P}}(A/K)$ with the property that for all $1\le i,j\le\nu+1$

$$\mathrm{loc}_{l_{\nu+j}}(c(\mathfrak{n}_i))\begin{cases}=0 & \text{if } i>j,\\ \neq 0 & \text{if } i=j.\end{cases}$$

3. *Let $\mathrm{Sel}^{\pm}_{\mathfrak{P},\mathscr{B}(\kappa)}(A/K)$ be the relaxed Selmer group at the base locus $\mathscr{B}(\kappa)$, i.e. the Selmer group where we take the relaxed condition at the primes dividing $\mathscr{B}(\kappa)$, then*

$$\mathrm{Sel}^{\epsilon_\nu}_{\mathfrak{P},\mathscr{B}(\kappa)}(A/K)=\mathrm{Sel}^{\epsilon_\nu}_{\mathfrak{P}}(A/K)\ \text{and}\ \dim\mathrm{Sel}^{-\epsilon_\nu}_{\mathfrak{P},\mathscr{B}(\kappa)}(A/K)\le\nu.$$

Proof. We start with proving by induction the following claim: if $0\le j\le\nu$, then there exists a sequence of primes $l_1,\cdots,l_{\nu+j}$ such that

- $c(\mathfrak{n}_i)\neq 0$ for all $1\le i\le j+1$ where $\mathfrak{n}_i=l_i\dots l_{\nu+i-1}$;
- $\mathrm{loc}_{l_{\nu+i}}c(\mathfrak{n}_i)\neq 0$ for all $1\le i\le j$.

When $j=0$ it follows from the definition of ν that there exists $\mathfrak{n}_1=l_1\dots l_\nu\in\mathscr{S}_\nu(1)$ such that $c(\mathfrak{n}_1)\neq 0$. This proves the claim in the case $j=0$. Note that the second statement is void in this case. Now suppose by induction that we have found primes $l_1,\dots,l_{\nu+j}$ satisfying the claim with $0\le j\le\nu-1$. We apply Lemma 5.4.4 to $S=\{l_{j+2},\dots,l_{\nu+j}\}$ and $\ell=l_{j+1}$ to obtain $c\in H^1(K,V)^{-\epsilon_\nu}$ such that

- $c\neq 0$;
- $\mathrm{loc}_v(c)\in H^1_{fin}(K_v,V)$ for all v outside $\{l_{j+1},\dots,l_{\nu+j}\}$;
- $\mathrm{loc}_v(c)\in H^1_{tr}(K_v,V)$ for all $v\in\{l_{j+2},\dots,l_{\nu+j}\}$.

In particular, we have that the class c lies in the opposite eigenspace to $c(\mathfrak{n}_{j+1})$. Using the Lemma 5.4.3 we get a prime $l_{\nu+j+1}$ distinct from $l_1,\dots,l_{\nu_m+j}$ such that $\mathrm{loc}_{l_{\nu+j+1}}(c)\neq 0$ and $\mathrm{loc}_{l_{\nu+j+1}}c(\mathfrak{n}_{j+1})\neq 0$. We now use the Tate pairing and calculate it as a sum of the local pairings over all places

$$0=\langle c,c(\mathfrak{n}_{j+1}l_{\nu+j+1})\rangle=\sum_v\langle c,c(\mathfrak{n}_{j+1}l_{\nu+j+1})\rangle_v.$$

Now c and $c(\mathfrak{n}_{j+1}l_{\nu+j+1})$ lies in the same eigenspace, so the possibly non-zero contribution only comes from $v\in\{l_{j+1},\dots,l_{\nu+j+1}\}$. When $v\in\{l_{j+2},\dots,l_{\nu+j}\}$ both loc_vc and $\mathrm{loc}_vc(\mathfrak{n}_{j+1}l_{\nu+j+1})$ lies in the transverse part $H^1_{tr}(K_v,V)$, thus the local pairing is zero. When $v=l_{\nu+j+1}$ we have $\mathrm{loc}_{l_{\nu+j+1}}(c)\neq 0$ in $H^1_{fin}(K_v,V)^{\epsilon_{\nu+1}}$ and

$$\mathrm{loc}_{l_{\nu+j+1}}c(\mathfrak{n}_{j+1}l_{\nu+j+1})=\psi_{l_{\nu+j+1}}(\mathrm{loc}_{l_{\nu+j+1}}c(\mathfrak{n}_{j+1}))\neq 0$$

in $H^1_{tr}(K_v,V)^{\epsilon_{\nu+1}}$. Thus the local pairing at $l_{\nu+j+1}$ is non-zero. Hence also the other local contribution cannot be zero, so we have $\mathrm{loc}_{l_{j+1}}c \neq 0$ and $\mathrm{loc}_{l_{j+1}}c(\mathfrak{n}_{j+1}l_{\nu+j+1}) \neq 0$. Hence

$$\mathrm{loc}_{l_{j+1}}c(\mathfrak{n}_j l_{\nu+j+1}/l_{j+1}) \neq 0$$

or equivalently

$$\mathrm{loc}_{l_{j+1}}c(\mathfrak{n}_{j+2}) \neq 0 \qquad \mathfrak{n}_{j+2} = l_{j+2}\dots l_{\nu+j+1}.$$

In particular, we get that $c(\mathfrak{n}_{j+2}) \neq 0$, which completes the proof of the claim.

We add a prime $l_{2\nu+1} \in \mathscr{S}_1(1)$ such that $\mathrm{loc}_{l_{2\nu+1}}c(\mathfrak{n}_{\nu+1}) \neq 0$. Such a prime exists since $c(\mathfrak{n}_{\nu+1}) \neq 0$. Thus we have constructed $\{l_1,\dots,l_{2\nu+1}\}$ satisfying the statement (2) of the theorem.

By this construction it follows easily that the $c(\mathfrak{n}_i)$ for $1 \leq i \leq \nu+1$ are linearly independent and belong to the Selmer group $\mathrm{Sel}^{\epsilon_\nu}_{\mathfrak{P}}(A/K)$. To complete the proof of the theorem we need to show that they generate the whole eigenspace of the Selmer group. In order to achieve this we can prove the stronger statement that they generate the relaxed Selmer group $\mathrm{Sel}^{\epsilon_\nu}_{\mathfrak{P},\mathscr{B}(\kappa)}(A/K)$.

Let $c \in \mathrm{Sel}^{\epsilon_\nu}_{\mathfrak{P},\mathscr{B}(\kappa)}(A/K)$, without loss of generality we may assume, up to changing c by subtracting a suitable linear combination of $c(\mathfrak{n}_i)$'s, that $\mathrm{loc}_{l_{\nu+j}}(c) = 0$ for all $1 \leq j \leq \nu+1$. Let $\mathfrak{n}' = l_{\nu+1}\dots l_{2\nu}l_{2\nu+1} \in \mathscr{S}_{\nu+1}(1)$, then $c(\mathfrak{n}')$ is non-zero since by our claim $\mathrm{loc}_{2\nu+1}c(\mathfrak{n}') \neq 0$. In particular, we find that the classes c and $c(\mathfrak{n}')$ are in different eigenspaces. Assume, by contradiction, that $c \neq 0$. By Lemma 5.4.3 there exists a prime $l_{2\nu+2} \notin \{l_i \mid 1 \leq i \leq 2\nu+1\}$ such that $\mathrm{loc}_{l_{2\nu+2}}(c) \neq 0$ and $\mathrm{loc}_{l_{2\nu+2}}(c(\mathfrak{n}')) \neq 0$. Let $\mathfrak{n}'' = \mathfrak{n}'l_{2\nu+2} \in \mathscr{S}_{\nu+2}(1)$. Then also $c(\mathfrak{n}'')$ is non-zero since our requests on the prime $l_{2\nu+2}$ imply that $\mathrm{loc}_{l_{2\nu+2}}(c) \neq 0$ and $\mathrm{loc}_{l_{2\nu+2}}(c(\mathfrak{n}'')) \neq 0$. Moreover the class $c(\mathfrak{n}'')$ lies in the same eigenspace of c.

We use again the Tate pairing

$$0 = \langle c, c(\mathfrak{n}'')\rangle = \sum_{v\in\mathscr{B}(\kappa)} \langle c, c(\mathfrak{n}'')\rangle_v + \sum_{\ell|\mathfrak{n}''} \langle c, c(\mathfrak{n}'')\rangle_\ell$$

and by the definition of base locus we have $\mathrm{loc}_v(c(\mathfrak{n}'')) = 0$ for all $v \in \mathscr{B}(\kappa)$, so the first sum on the right-hand side is zero. Furthermore, $\mathrm{loc}_{l_i}(c) = 0$ for all $\nu+1 \leq i \leq 2\nu+1$ but not for $i = 2\nu+2$ and so finally we get

$$0 = \langle c, c(\mathfrak{n}'')\rangle = \sum_{\ell|n''} \langle c, c(\mathfrak{n}'')\rangle_\ell = \langle c, c(\mathfrak{n}'')\rangle_{l_{2\nu+2}} \neq 0$$

which is a contradiction, hence $c = 0$. This implies that $\mathrm{Sel}^{\epsilon_\nu}_{\mathfrak{P},\mathscr{B}(\kappa)}(A/K) = \mathrm{Sel}^{\epsilon_\nu}_{\mathfrak{P}}(A/K)$ and that it is generated by the $c(\mathfrak{n}_i)$ for all $1 \leq i \leq \nu+1$.

The last step in our proof is to show that $\dim \mathrm{Sel}^{-\epsilon_\nu}_{\mathfrak{P},\mathscr{B}(\kappa)}(A/K) \leq \nu$. Suppose, by contradiction, that $\dim \mathrm{Sel}^{-\epsilon_\nu}_{\mathfrak{P},\mathscr{B}(\kappa)}(A/K) > \nu$. By a dimensional argument, there exists a class $\tilde{c} \in \mathrm{Sel}^{-\epsilon_\nu}_{\mathfrak{P}}(A/K)$ such that $\tilde{c} \neq 0$ and $\mathrm{loc}_{l_{\nu+i}}(\tilde{c}) = 0$ for all $1 \leq i \leq \nu$. Since $\tilde{c}$ and $c(\mathfrak{n}_{\nu+1})$ belongs to different eigenspaces we can apply Lemma 5.4.3 to choose a different a prime $l_{2\nu+1}$ such that $\mathrm{loc}_{l_{2\nu+1}}(\tilde{c}) \neq 0$ and $\mathrm{loc}_{l_{2\nu+1}}(c(\mathfrak{n}_{\nu+1})) \neq 0$. Then we conclude as before calculating the Tate pairing

$$0 = \langle \tilde{c}, c(\mathfrak{n}_{\nu+1}l_{2\nu+1})\rangle = \sum_{\ell|\mathfrak{n}_{\nu+1}l_{2\nu+1}} \langle \tilde{c}, c(\mathfrak{n}_{\nu+1}l_{2\nu+1})\rangle_\ell = \langle \tilde{c}, c(\mathfrak{n}_{\nu+1}l_{2\nu+1})\rangle_{l_{2\nu+1}} \neq 0$$

which gives us a contradiction, thus finishing the proof. □

Chapter 6

Birch and Swinnerton-Dyer formula in the rank one case

We are now ready for the proof of our main result. We will first prove the non-vanishing of our Kolyvagin system and a parity theorem and then proceed to the main proof.

6.1 Kolyvagin's conjecture

In order to use our Kolyvagin system we need to know that it is not trivial.

Theorem 6.1.1. *Assume that the parity of the number of factor of N^- is different from the one of $[F\colon \mathbb{Q}]$ and our Assumptions 4.1.1 hold. Then*

$$\kappa = \left\{c(\mathfrak{n}) \in H^1(K,V) \mid \mathfrak{n} \in \mathscr{S}(1)\right\} \neq 0.$$

Proof. We work by induction on the rank

$$r = \dim \mathrm{Sel}_{\mathfrak{P}}(A/K).$$

We assume that the parity conjecture for Selmer group holds for A/K (see [Nek09] and [Nek06]), so r is always odd since we are in the rank 1 case.

The case $r = 1$ is Theorem 5.3.9. Suppose now that $r \geq 3$ and that $\mu \in \{\pm\}$ is chosen such that $\mathrm{Sel}^{\mu}_{\mathfrak{P}}(A/K)$ has higher rank than $\mathrm{Sel}^{-\mu}_{\mathfrak{P}}(A/K)$. In particular, we have that $\dim \mathrm{Sel}^{\mu}_{\mathfrak{P}}(A/K) \geq 2$. We proceed in the following way: first chose a non-zero $c_1 \in \mathrm{Sel}^{\mu}_{\mathfrak{P}}(A/K)$. In particular, we want that $c_1 \in H^1(K,V)$. Chose an admissible prime q_1 such that the image of c_1 under the homomorphism

$$\mathrm{loc}_{q_1}\colon \mathrm{Sel}_{\mathfrak{P}}(A/K) \to H^1_{fin}(K_{q_1},V)$$

is non-zero, thus this homomorphism is surjective. Using level raising we get a Hilbert newform f_{q_1} of level Nq_1 together with a prime $\mathfrak{P}_{q_1}$. By Proposition 5.2.1, we have

$$\dim_{\mathcal{O}_A/\mathfrak{P}} \mathrm{Sel}_{\mathfrak{P}_{q_1}}(A_{q_1}/K) = \dim_{\mathcal{O}_A/\mathfrak{P}} \mathrm{Sel}_{\mathfrak{P}}(A/K) - 1$$

and

$$\mathrm{Sel}_{\mathfrak{P}_{q_1}}(A_{q_1}/K) = \ker \mathrm{loc}_{q_1}.$$

Then we chose a non-zero $c_2 \in \mathrm{Sel}^{\mu}_{\mathfrak{P}_{q_1}}(A_{q_1}/K)$ and an admissible prime q_2 as before. Since $\dim \mathrm{Sel}^{\mu}_{\mathfrak{P}_{q_1}}(A_{q_1}/K) \geq 2$, such c_2 exists. Again we want $c_2 \in H^1(K,V)$. Then again by level raising we obtain a Hilbert newform $f_{q_1q_2}$ of level Nq_1q_2 and a prime $\mathfrak{P}_{q_1q_2}$. Again by rank lowering we have

$$\dim_{\mathcal{O}_A/\mathfrak{P}} \mathrm{Sel}_{\mathfrak{P}_{q_1q_2}}(A_{q_1q_2},K) = \dim_{\mathcal{O}_A/\mathfrak{P}} \mathrm{Sel}_{\mathfrak{P}_{q_1}}(A_{q_1}/K) - 1 = \dim_{\mathcal{O}_A/\mathfrak{P}} \mathrm{Sel}_{\mathfrak{P}}(A/K) - 2$$

and

$$\mathrm{Sel}_{\mathfrak{P}_{q_1q_2}}(A_{q_1q_2},K) = \ker \mathrm{loc}_{q_1q_2}.$$

Moreover this process is compatible this the action of complex conjugation, hence the dimension of the μ eigenspace decreases whereas the dimension of the $-\mu$ one remain constant.

By induction hypothesis and noting that $f_{q_1q_2}$ still satisfies all the hypothesis of this theorem, we may assume that the family

$$\kappa_{q_1q_2} = \left\{c(\mathfrak{n}, q_1q_2) \in H^1(K,V) \mid \mathfrak{n} \in \mathscr{S}(1)\right\} \neq \{0\}.$$

By the reciprocity law 4.2.5 we have for all $\mathfrak{n} \in \mathscr{S}(1)$ that $\mathrm{loc}_{q_1}(c(\mathfrak{n},1)) = \mathrm{loc}_{q_2}(c(\mathfrak{n}, q_1q_2))$. To complete the proof it is enough to show that q_2 is not a base point for the Kolyvagin system $\kappa_{q_1q_2}$. We do this by contradiction, so assume that $q_2 \in \mathscr{B}(\kappa_{q_1q_2})$.

The local condition defining the Selmer groups of $A_{q_1q_2}$ and A_{q_1} differs only at q_2, thus we have a trivial inclusion into thee relaxed Selmer group

$$\mathrm{Sel}^{\pm}_{\mathfrak{P}_{q_1}}(A_{q_1}/K) \subset \mathrm{Sel}_{\mathfrak{P}_{q_1q_2},\mathscr{B}(\kappa_{q_1q_2})}(A_{q_1q_2}/K).$$

We have two cases:

1. $\dim \mathrm{Sel}^{\mu}_{\mathfrak{P}_{q_1q_2}}(A_{q_1q_2}/K)$ remains bigger that $\dim \mathrm{Sel}^{-\mu}_{\mathfrak{P}_{q_1q_2}}(A_{q_1q_2}/K)$;
2. $\dim \mathrm{Sel}^{\mu}_{\mathfrak{P}_{q_1q_2}}(A_{q_1q_2}/K)$ is smaller than $\dim \mathrm{Sel}^{-\mu}_{\mathfrak{P}_{q_1q_2}}(A_{q_1q_2}/K)$. This happens exactly when $\dim \mathrm{Sel}^{-\mu}_{\mathfrak{P}}(A/K) = \dim \mathrm{Sel}^{-\mu}_{\mathfrak{P}}(A/K) + 1$.

In the first case by the Theorem 5.4.6 we have an equality

$$\mathrm{Sel}^{\mu}_{\mathfrak{P}_{q_1q_2}}(A_{q_1q_2}/K) = \mathrm{Sel}^{\mu}_{\mathfrak{P}_{q_1q_2},\mathscr{B}(\kappa_{q_1q_2})}(A_{q_1q_2}/K).$$

Hence $\mathrm{Sel}^{\mu}_{\mathfrak{P}_{q_1}}(A_{q_1}/K) \subset \mathrm{Sel}^{\mu}_{\mathfrak{P}_{q_1q_2}}(A_{q_1q_2}/K)$ by the previous inclusion. By our previous choice the class c_2 lies in the first space but not in the second and so we have a contradiction.

In the second case, let $\nu_{q_1q_1}$ denote the vanishing order of $\kappa_{q_1q_2}$ as usual. Then by the Theorem 5.4.6 we have

$$\dim \mathrm{Sel}^{-\mu}_{\mathfrak{P}_{q_1q_2}}(A_{q_1q_2}/K) = \nu_{q_1q_2} + 1,$$
$$\dim \mathrm{Sel}^{\mu}_{\mathfrak{P}_{q_1q_2},\mathscr{B}(\kappa_{q_1q_2})}(A_{q_1q_2}/K) \leq \nu_{q_1q_2}.$$

However, by the previous inclusions the dimension of the relaxed Selmer is at least that of $\mathrm{Sel}^{\mu}_{\mathfrak{P}_{q_1}}(A_{q_1}/K)$ which is $\nu_{q_1q_2}+1$ by the previous considerations and thus we have a contradiction also in this case. □

In our particular case we can avoid using the parity conjecture and instead prove it for our specific case.

Proposition 6.1.2. *Assume that we are in the indefinite case, then* $\dim \mathrm{Sel}_{\mathfrak{P}}(A/K)$ *is odd and hence* $\mathrm{Sel}_{\mathfrak{P}^\infty}(A/K)$ *has odd* $\mathcal{O}_{A,\mathfrak{P}}$*-corank.*

Proof. Under our hypothesis we are in the indefinite case, so the root number is -1 and thus $L(f/K,1)=0$. The case $r=\dim \mathrm{Sel}_{\mathfrak{P}}(A/K)=0$ cannot happen by Theorem 5.3.7.

Suppose by contradiction that $r\geq 2$ is even. We have two cases: if one eigenspace has dimension strictly larger than the other we can apply the same argument as in Theorem 6.1.1 and produce $A_{q_1q_2}$ with $\dim \mathrm{Sel}_{\mathfrak{P}_{q_1q_2}}(A_{q_1q_2}/K)=r-2$. Otherwise, the two eigenspaces have the same dimension and we can modify the choice of c_2 in the proof of the above theorem and force $c_2\in \mathrm{Sel}_{\mathfrak{P}_{q_1}}^{-\nu_{q_1q_2}}(A_{q_1}/K)$. Then we get again an $A_{q_1q_2}$ with $\dim \mathrm{Sel}_{\mathfrak{P}_{q_1q_2}}(A_{q_1q_2}/K)=r-2$. Therefore, by induction we get a contradiction. So we have proved the parity in the indefinite case.

Under our hypothesis the $\mathcal{O}_A/\mathfrak{P}$-vector space $\mathrm{Sel}_{\mathfrak{P}}(A/K)$ can be identified with the $\mathfrak{P}$-torsion of $\mathrm{Sel}_{\mathfrak{P}^\infty}(A/K)$. By the non-degeneracy of the Cassels-Tate pairing on the indivisible quotient of $Ш(A/K)$ the $\mathcal{O}_{A,\mathfrak{P}}$-corank of $\mathrm{Sel}_{\mathfrak{P}^\infty}(A/K)$ has the same parity as the dimension of $\mathrm{Sel}_{\mathfrak{P}}(A/K)$, so it has odd corank. □

We can now state a more general result which is the Kolyvagin's conjecture. Let $\nu(\mathfrak{n})$ denote the number of factor of $\mathfrak{n}\in\mathscr{S}(M)$, so $\mathfrak{n}\in\mathscr{S}_{\nu(\mathfrak{n})}(M)$.

Theorem 6.1.3. *Let f be a Hilbert newform over F of parallel weight 2 and level N with trivial nebentypus, A the associated abelian variety, $\mathfrak{P}$ a prime ideal of $\mathcal{O}_A$ above the prime number p and D_K/F the relative discriminant of a CM extension K of F with $(D_{K/F},N)=1$. Assume that*

- *N^- is square-free and the number of prime factor has opposite parity of $[F\colon \mathbb{Q}]$;*
- *The residue representation is surjective;*
- *Assumptions 4.1.1 holds;*
- *The prime p is ordinary and p is coprime with $D_{K/F}N$.*

Then we have

$$\kappa^\infty=\left\{c_M(\mathfrak{n})\in H^1(K,A[\mathfrak{P}^M])\mid \mathfrak{n}\in\mathscr{S}(1),M\in\mathbb{Z}_+\right\}\neq 0.$$

Indeed we have

$$M_\infty=\lim_{r\to\infty}M_r=0.$$

Proof. This follows easily from Theorem 6.1.1. □

From this theorem we can also deduce a construction of the Selmer groups using the Kolyvagin's classes.

Corollary 6.1.4. *Let ν be the vanishing order of the Kolyvagin system κ. Then*

1. *The vector space $\mathrm{Sel}_{\mathfrak{P}}^{\epsilon_\nu}(A/K)$ is contained in the subspace of $H^1(K,V)$ spanned by all $c(\mathfrak{n},1)$ for $\mathfrak{n}\in\mathscr{S}(1)$;*
2. *The vector space $\mathrm{Sel}_{\mathfrak{P}}(A/K)$ is contained in the subspace of $H^1(K,V)$ spanned by all $c(\mathfrak{n},\mathfrak{m})$ for $\mathfrak{n}\in\mathscr{S}(1)$ and $\mathfrak{m}\in\Lambda^+$.*

Proof. The first statement is a consequence of Theorem 5.4.6 and Theorem 6.1.1 above. To prove the second statement is enough to show that the other eigenspace is generated by the classes $c(\mathfrak{n},\mathfrak{m})$. We use induction on the dimension of $\mathrm{Sel}_{\mathfrak{P}}(A/K)$ in the same way as in the proof of Theorem 6.1.1. In fact $\dim \mathrm{Sel}_{\mathfrak{P}_{q_1q_2}}(A_{q_1q_2}/K)=\dim \mathrm{Sel}_{\mathfrak{P}}(A/K)-2$ and by induction hypothesis we may assume that $\mathrm{Sel}_{\mathfrak{P}_{q_1q_2}}(A_{q_1q_2}/K)$ is generated by the classes $c(\mathfrak{n},q_1q_2\mathfrak{m})$. In particular, the subspace $\mathrm{Sel}_{\mathfrak{P}_{q_1q_2}}^{-\epsilon_\nu}(A_{q_1q_2}/K)$ is generated by them. But this two subspace share the same underlying $\mathcal{O}_A/\mathfrak{P}$-vector subspace by level raising so the corollary follows. □

6.2 The main formula

In this last section we prove the $\mathfrak{P}$-part of the Birch and Swinnerton-Dyer conjecture in the rank one case. We assume to be in the indefinite case. We restrict ourselves to the case where A is an elliptic curve.

We assume also that $v_{\mathfrak{p}}(\prod_v c_v) = 0$ where c_v denotes the Tamagawa number at v. This assumption excludes only a finite set of primes $\mathfrak{p}$. We also assume that $p \nmid \#A(F)_{tors}$ and $p \nmid D_F$ where D_F is the discriminant of F. Let $\langle \cdot, \cdot \rangle_{NT}$ denote the Neron-Tate height pairing.

Lemma 6.2.1. *Under our assumptions, if $L(A/K, s)$ has a simple zero at $s = 1$ then the $\mathfrak{P}$-part of the Birch and Swinnerton-Dyer conjecture for A/K is equivalent to*

$$2 \cdot \text{lenght}_{\mathcal{O}_{A,\mathfrak{P}}}(A(K)/\mathcal{O}_A y_K) = \text{lenght}_{\mathcal{O}_{A,\mathfrak{P}}} Ш(A/K).$$

Proof. We have assumed that N^- is square-free, so by [Zha01b], [Zha04] and [YZZ13] the Gross-Zagier formula con be written as

$$\frac{L'(A/K, 1)}{\Omega_f} = \frac{\langle y_K, y_K \rangle_{NT}}{D_F^2 D_{K/F}^{1/2}}.$$

We can also rewrite the Birch and Swinnerton-Dyer formula following [Dis15] and [GP12] as

$$\frac{L'(A/K, 1)}{\Omega_A} = \frac{D_{K/F}^{-1/2} \# Ш(A/K) \langle y_K, y_K \rangle_{NT} \prod_v c_v}{[A(K) \colon \mathcal{O}_A y_K]^2}$$

where Ω_A is the period associated to A. This period can be computed by integrating a Neron differential ω_A, if it exists, along the quotients composing the Shimura curve X; the Neron differential is guaranteed to exist only when $F = \mathbb{Q}$, otherwise we should take as ω_A any generator of $H^0(A, \Omega_{A/F})$ and divide by the product over all places v of the indices

$$\prod_v \left[H^0(\mathscr{A}_v, \Omega_{\mathscr{A}_v/\mathcal{O}_{F,v}}) \colon \mathcal{O}_{F,v} \widetilde{\omega}_A \right]$$

of the extension of ω_A in the space of top differential on the local Neron models $\mathscr{A}_v/\mathcal{O}_{F,v}$ of A.

Here we have our main problem that arise in the totally real case: we need to compare these two periods. The problem is that f is a Hilbert modular form and not a quaternionic one, otherwise we would have the comparison. In particular, this can be rewritten as a comparison between the periods of f and that of its Jacquet-Langlands transfers to quaternionic forms. For elliptic curve over $\mathbb{Q}$ it was done in [PW11], [GP12] and [Pra09], and the quotient of the periods is the product of some Tamagawa numbers; hence, in our case, it has valuation zero. In the totally real case the relation is only conjectured. For a more in depth review of this fact see [Dis15, Chpater 9]. The conjecture is known to hold in some specific case, for example when A has complex multiplication (over $\overline{\mathbb{Q}}$) by [Bla86]. Moreover the comparison of these two periods is also related to the Bloch-Kato conjecture (see [Tam21, Remark 5.5]). We assume this conjecture to holds, so comparing the two identities and taking the $\mathfrak{P}$-adic valuation we get

$$2 \cdot \text{lenght}_{\mathcal{O}_{A,\mathfrak{P}}}(A(K)/\mathcal{O}_A y_K) = \text{lenght}_{\mathcal{O}_{A,\mathfrak{P}}} Ш(A/K)$$

which completes the proof. □

Theorem 6.2.2. *Under our assumptions, if $L(A/K, s)$ has a simple zero at $s = 1$ then the $\mathfrak{P}$-part of the Birch and Swinnerton-Dyer conjecture for A/K holds, so we have*

$$v_{\mathfrak{P}}\left(\frac{L'(A/K,1)}{\Omega_A \mathrm{Reg}_{A/K}}\right) = \mathrm{lenght}_{\mathcal{O}_{A,\mathfrak{P}}} Ш(A/K)$$

where $\mathrm{Reg}_{A/K}$ is by definition the Neron-Tate height of y_K divided by the square of the cardinality of the torsion part.

Proof. By Lemma 6.2.1 it is enough to show that

$$2 \cdot \mathrm{lenght}_{\mathcal{O}_{A,\mathfrak{P}}}(A(K)/\mathcal{O}_A y_K) = \mathrm{lenght}_{\mathcal{O}_{A,\mathfrak{P}}} Ш(A/K)$$

but by Corollary 3.2.3 we have

$$\mathrm{lenght}_{\mathcal{O}_{A,\mathfrak{P}}} Ш(A/K) = 2(M_0 - M_\infty)$$

hence, by Theorem 6.1.3 we have that $M_\infty = 0$ and so the theorem follows from Corollary 2.3.9. □

We can now use the standard argument to descend the result to F.

Theorem 6.2.3. *Under our assumptions, if $L(A/F, s)$ has a simple zero at $s = 1$ then the $\mathfrak{P}$-part of the Birch and Swinnerton-Dyer conjecture for A/F holds, so we have*

$$v_{\mathfrak{P}}\left(\frac{L'(A/K,1)}{\Omega_A \mathrm{Reg}_{A/F}}\right) = \mathrm{lenght}_{\mathcal{O}_{A,\mathfrak{P}}} Ш(A/K).$$

Proof. Following the proof of [Zha14, Theorem 1.4] we can pick a field K satisfying all our assumptions, so the $\mathfrak{P}$-part of the Birch and Swinnerton-Dyer conjecture holds for A/K by Theorem 6.2.2. Let A^K denote the quadratic twist of A by K, since $L(A^K, 1) \neq 0$ the $\mathfrak{P}$-part of the conjecture for A^K/F holds true thanks to the work of Xin Wan in [Wan15]. Then the $\mathfrak{P}$-part of the Birch and Swinnerton-Dyer conjecture for A/F follows. □

If this theorem holds for every $\mathfrak{P} \subset \mathcal{O}_A$ above p, then we can descend it to obtain the p-part of the Birch and Swinnerton-Dyer conjecture in the rank one case for infinitely many p.

Bibliography

[BBV16] Andrea Berti, Massimo Bertolini and Rodolfo Venerucci, "Congruences between modular forms and the Birch and Swinnerton-Dyer conjecture", in: *Elliptic curves, modular forms and Iwasawa theory*, vol. 188, Springer Proc. Math. Stat. Springer, Cham, 2016, pp. 1–31, DOI: 10.1007/978-3-319-45032-2_1, URL: https://doi.org/10.1007/978-3-319-45032-2_1.

[BD05] M. Bertolini and H. Darmon, "Iwasawa's main conjecture for elliptic curves over anticyclotomic $\mathbb{Z}_p$-extensions", in: *Ann. of Math. (2)* 162.1 (2005), pp. 1–64, ISSN: 0003-486X, DOI: 10.4007/annals.2005.162.1, URL: https://doi.org/10.4007/annals.2005.162.1.

[BD96] M. Bertolini and H. Darmon, "Heegner points on Mumford-Tate curves", in: *Invent. Math.* 126.3 (1996), pp. 413–456, ISSN: 0020-9910, DOI: 10.1007/s002220050105, URL: https://doi.org/10.1007/s002220050105.

[Bla86] Don Blasius, "On the critical values of Hecke L-series", in: *Ann. of Math. (2)* 124.1 (1986), pp. 23–63, ISSN: 0003-486X, DOI: 10.2307/1971386, URL: https://doi.org/10.2307/1971386.

[Buz12] Kevin Buzzard, "Potential modularity - a survey", in: *Non-abelian fundamental groups and Iwasawa theory*, vol. 393, London Math. Soc. Lecture Note Ser. Cambridge Univ. Press, Cambridge, 2012, pp. 188–211.

[Car86] Henri Carayol, "Sur la mauvaise réduction des courbes de Shimura", in: *Compositio Math.* 59.2 (1986), pp. 151–230, URL: http://www.numdam.org/item?id=CM_1986__59_2_151_0.

[Car94] Henri Carayol, "Formes modulaires et représentations galoisiennes à valeurs dans un anneau local complet", in: *p-adic monodromy and the Birch and Swinnerton-Dyer conjecture (Boston, MA, 1991)*, vol. 165, Contemp. Math. Amer. Math. Soc., Providence, RI, 1994, pp. 213–237, DOI: 10.1090/conm/165/01601, URL: https://doi.org/10.1090/conm/165/01601.

[CV05] C. Cornut and V. Vatsal, "CM points and quaternion algebras", in: *Doc. Math.* 10 (2005), pp. 263–309.

[Dar06] Henri Darmon, "Heegner points, Stark-Heegner points, and values of L-series", in: *International Congress of Mathematicians. Vol. II*, Eur. Math. Soc., Zürich, 2006, pp. 313–345.

[Dav10] A. Davydov, "Twisted automorphisms of group algebras", in: *Noncommutative structures in mathematics and physics*, K. Vlaam. Acad. Belgie Wet. Kunsten (KVAB), Brussels, 2010, pp. 131–150.

[Dia97] Fred Diamond, "Congruences between modular forms: raising the level and dropping Euler factors", in: vol. 94, 21, Elliptic curves and modular forms (Washington, DC, 1996), 1997, pp. 11143–11146, DOI: 10.1073/pnas.94.21.11143, URL: https://doi.org/10.1073/pnas.94.21.11143.

[Dis15] Daniel Disegni, "p-adic heights of Heegner points on Shimura curves", in: *Algebra Number Theory* 9.7 (2015), pp. 1571–1646, ISSN: 1937-0652, DOI: 10.2140/ant.2015.9.1571, URL: https://doi.org/10.2140/ant.2015.9.1571.

[DS05] Fred Diamond and Jerry Shurman, *A first course in modular forms*, vol. 228, Graduate Texts in Mathematics, Springer-Verlag, New York, 2005, pp. xvi+436, ISBN: 0-387-23229-X.

[DS74] Pierre Deligne and Jean-Pierre Serre, "Formes modulaires de poids 1", in: *Ann. Sci. École Norm. Sup. (4)* 7 (1974), 507–530 (1975), ISSN: 0012-9593, URL: http://www.numdam.org/item?id=ASENS_1974_4_7_4_507_0.

[FLS15] Nuno Freitas, Bao V. Le Hung and Samir Siksek, "Elliptic curves over real quadratic fields are modular", in: *Invent. Math.* 201.1 (2015), pp. 159–206, ISSN: 0020-9910, DOI: 10.1007/s00222-014-0550-z, URL: https://doi.org/10.1007/s00222-014-0550-z.

[Fre90] Eberhard Freitag, *Hilbert modular forms*, Springer-Verlag, Berlin, 1990, pp. viii+250, ISBN: 3-540-50586-5, DOI: 10.1007/978-3-662-02638-0, URL: https://doi.org/10.1007/978-3-662-02638-0.

[GG12] Jayce Getz and Mark Goresky, *Hilbert modular forms with coefficients in intersection homology and quadratic base change*, vol. 298, Progress in Mathematics, Birkhäuser/Springer Basel AG, Basel, 2012, pp. xiv+256, ISBN: 978-3-0348-0350-2, DOI: 10.1007/978-3-0348-0351-9, URL: https://doi.org/10.1007/978-3-0348-0351-9.

[GP12] Benedict H. Gross and James A. Parson, "On the local divisibility of Heegner points", in: *Number theory, analysis and geometry*, Springer, New York, 2012, pp. 215–241, DOI: 10.1007/978-1-4614-1260-1_11, URL: https://doi.org/10.1007/978-1-4614-1260-1_11.

[Gro84] Benedict H. Gross, "Heegner points on $X_0(N)$", in: *Modular forms (Durham, 1983)*, Ellis Horwood Ser. Math. Appl.: Statist. Oper. Res. Horwood, Chichester, 1984, pp. 87–105.

[Gro91] Benedict H. Gross, "Kolyvagin's work on modular elliptic curves", in: *L-functions and arithmetic (Durham, 1989)*, vol. 153, London Math. Soc. Lecture Note Ser. Cambridge Univ. Press, Cambridge, 1991, pp. 235–256, URL: https://doi.org/10.1017/CBO9780511526053.009.

[GS93] Ralph Greenberg and Glenn Stevens, "p-adic L-functions and p-adic periods of modular forms", in: *Invent. Math.* 111.2 (1993), pp. 407–447, ISSN: 0020-9910, DOI: 10.1007/BF01231294, URL: https://doi.org/10.1007/BF01231294.

[GZ86] Benedict H. Gross and Don B. Zagier, "Heegner points and derivatives of L-series", in: *Invent. Math.* 84.2 (1986), pp. 225–320, ISSN: 0020-9910, DOI: 10.1007/BF01388809, URL: https://doi.org/10.1007/BF01388809.

[Hel07] David Helm, "On maps between modular Jacobians and Jacobians of Shimura curves", in: *Israel J. Math.* 160 (2007), pp. 61–117, ISSN: 0021-2172, DOI: 10.1007/s11856-007-0056-0, URL: https://doi.org/10.1007/s11856-007-0056-0.

[How04] Benjamin Howard, "Iwasawa theory of Heegner points on abelian varieties of GL_2 type", in: *Duke Math. J.* 124.1 (2004), pp. 1–45, ISSN: 0012-7094, DOI: 10.1215/S0012-7094-04-12411-X, URL: https://doi.org/10.1215/S0012-7094-04-12411-X.

[Jar99] Frazer Jarvis, "Level lowering for modular mod l representations over totally real fields", in: *Math. Ann.* 313.1 (1999), pp. 141–160, ISSN: 0025-5831, DOI: 10.1007/s002080050255, URL: https://doi.org/10.1007/s002080050255.

[JL70] H. Jacquet and R. P. Langlands, *Automorphic forms on* GL(2), Lecture Notes in Mathematics, Vol. 114, Springer-Verlag, Berlin-New York, 1970, pp. vii+548.

[Kei14] Stefan Keil, "Examples of non-simple abelian surfaces over the rationals with non-square order Tate-Shafarevich group", in: *J. Number Theory* 144 (2014), pp. 25–69, DOI: 10.1016/j.jnt.2014.04.018, URL: https://doi.org/10.1016/j.jnt.2014.04.018.

[KL89] V. A. Kolyvagin and D. Yu. Logachëv, "Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties", in: *Algebra i Analiz* 1.5 (1989), pp. 171–196, ISSN: 0234-0852.

[KL91] V. A. Kolyvagin and D. Yu. Logachëv, "Finiteness of Ш over totally real fields", in: *Izv. Akad. Nauk SSSR Ser. Mat.* 55.4 (1991), pp. 851–876, ISSN: 0373-2436, URL: https://doi.org/10.1070/IM1992v039n01ABEH002228.

[KM85] Nicholas M. Katz and Barry Mazur, *Arithmetic moduli of elliptic curves*, vol. 108, Annals of Mathematics Studies, Princeton University Press, Princeton, NJ, 1985, ISBN: 0-691-08349-5; 0-691-08352-5, DOI: 10.1515/9781400881710, URL: https://doi.org/10.1515/9781400881710.

[Kol90] V. A. Kolyvagin, "Euler systems", in: *The Grothendieck Festschrift, Vol. II*, vol. 87, Progr. Math. Birkhäuser Boston, Boston, MA, 1990, pp. 435–483.

[Le 14] Bao Viet Le Hung, *Modularity of some elliptic curves over totally real fields*, Thesis (Ph.D.)–Harvard University, ProQuest LLC, Ann Arbor, MI, 2014, p. 67, ISBN: 978-1321-01858-5, URL: http://gateway.proquest.com/openurl?url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mtx:dissertation&res_dat=xri:pqm&rft_dat=xri:pqdiss:3626808.

[Len95] H. W. Lenstra Jr., "Complete intersections and Gorenstein rings", in: *Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993)*, Ser. Number Theory, I, Int. Press, Cambridge, MA, 1995, pp. 99–109.

[Lon06] Matteo Longo, "On the Birch and Swinnerton-Dyer conjecture for modular elliptic curves over totally real fields", in: *Ann. Inst. Fourier (Grenoble)* 56.3 (2006), pp. 689–733, ISSN: 0373-0956, URL: http://aif.cedram.org/item?id=AIF_2006__56_3_689_0.

[Lon07] Matteo Longo, "Euler systems obtained from congruences between Hilbert modular forms", in: *Rend. Semin. Mat. Univ. Padova* 118 (2007), pp. 1–34, ISSN: 0041-8994.

[Lon12] Matteo Longo, "Anticyclotomic Iwasawa's main conjecture for Hilbert modular forms", in: *Comment. Math. Helv.* 87.2 (2012), pp. 303–353, ISSN: 0010-2571, DOI: 10.4171/CMH/255, URL: https://doi.org/10.4171/CMH/255.

[LV17] Matteo Longo and Stefano Vigni, "A refined Beilinson-Bloch conjecture for motives of modular forms", in: *Trans. Amer. Math. Soc.* 369.10 (2017), pp. 7301–7342, ISSN: 0002-9947, DOI: 10.1090/tran/6947, URL: https://doi.org/10.1090/tran/6947.

[Man21] Jeffrey Manning, "Patching and multiplicity 2^k for Shimura curves", in: *Algebra Number Theory* 15.2 (2021), pp. 387–434, ISSN: 1937-0652, DOI: 10.2140/ant.2021.15.387, URL: https://doi.org/10.2140/ant.2021.15.387.

[Mas19] Daniele Masoero, "On the structure of Selmer and Shafarevich-Tate groups of even weight modular forms", in: *Trans. Amer. Math. Soc.* 371.12 (2019), pp. 8381–8404, ISSN: 0002-9947, DOI: 10.1090/tran/7407, URL: https://doi.org/10.1090/tran/7407.

[McC91] William G. McCallum, "Kolyvagin's work on Shafarevich-Tate groups", in: *L-functions and arithmetic (Durham, 1989)*, vol. 153, London Math. Soc. Lecture Note Ser. Cambridge Univ. Press, Cambridge, 1991, pp. 295–316, URL: https://doi.org/10.1017/CBO9780511526053.012.

[MGH12] B. Heinrich Matzat, Gert-Martin Greuel and Gerhard Hiss, *Algorithmic algebra and number theory: selected papers from a conference held at the University of Heidelberg in October 1997*, Springer Science & Business Media, 2012.

[Mil06] James S. Milne, *Arithmetic Duality Theorems*, BookSurge, LLC, 2006, pp. viii+339, ISBN: 1-4196-4274-X.

[Mil08] James S. Milne, *Abelian Varieties (v2.00)*, Available at www.jmilne.org/math/, 2008.

[Mil90] J. S. Milne, "Canonical models of (mixed) Shimura varieties and automorphic vector bundles", in: *Automorphic forms, Shimura varieties, and L-functions, Vol. I (Ann Arbor, MI, 1988)*, vol. 10, Perspect. Math. Academic Press, Boston, MA, 1990, pp. 283–414.

[Mok09] Chung Pang Mok, "The exceptional zero conjecture for Hilbert modular forms", in: *Compos. Math.* 145.1 (2009), pp. 1–55, ISSN: 0010-437X, URL: https://doi.org/10.1112/S0010437X08003813.

[MS21] Jeffrey Manning and Jack Shotton, "Ihara's lemma for Shimura curves over totally real fields via patching", in: *Math. Ann.* 379.1-2 (2021), pp. 187–234, ISSN: 0025-5831, DOI: 10.1007/s00208-020-02048-8, URL: https://doi.org/10.1007/s00208-020-02048-8.

[Nek06] Jan Nekovář, "Selmer complexes", in: *Astérisque* 310 (2006), pp. viii+559, ISSN: 0303-1179.

[Nek07] Jan Nekovář, "The Euler system method for CM points on Shimura curves", in: *L-functions and Galois representations*, vol. 320, London Math. Soc. Lecture Note Ser. Cambridge Univ. Press, Cambridge, 2007, pp. 471–547.

[Nek09] Jan Nekovář, "On the parity of ranks of Selmer groups. IV", in: *Compos. Math.* 145.6 (2009), With an appendix by Jean-Pierre Wintenberger, pp. 1351–1359, ISSN: 0010-437X, DOI: 10.1112/S0010437X09003959, URL: https://doi.org/10.1112/S0010437X09003959.

[Nek12] Jan Nekovář, "Level raising and anticyclotomic Selmer groups for Hilbert modular forms of weight two", in: *Canad. J. Math.* 64.3 (2012), pp. 588–668, ISSN: 0008-414X, DOI: 10.4153/CJM-2011-077-6, URL: https://doi.org/10.4153/CJM-2011-077-6.

[Per14] Corentin Perret-Gentil, "Associating abelian varieties to weight-2 modular forms: the Eichler-Shimura construction", MA thesis, Ecole Polytechnique Fédérale de Lausanne, 2014.

[Pol03] Alexander Polishchuk, *Abelian varieties, theta functions and the Fourier transform*, vol. 153, Cambridge Tracts in Mathematics, Cambridge University Press, Cambridge, 2003, pp. xvi+292, ISBN: 0-521-80804-9, DOI: 10.1017/CBO9780511546532, URL: https://doi.org/10.1017/CBO9780511546532.

[Pra09] Kartik Prasanna, "Arithmetic properties of the Shimura-Shintani-Waldspurger correspondence", in: *Invent. Math.* 176.3 (2009), With an appendix by Brian Conrad, pp. 521–600, ISSN: 0020-9910, DOI: 10.1007/s00222-008-0169-z, URL: https://doi.org/10.1007/s00222-008-0169-z.

[PS99] Bjorn Poonen and Michael Stoll, "The Cassels-Tate pairing on polarized abelian varieties", in: *Ann. of Math. (2)* 150.3 (1999), pp. 1109–1149, ISSN: 0003-486X, DOI: 10.2307/121064, URL: https://doi.org/10.2307/121064.

[PW11] Robert Pollack and Tom Weston, "On anticyclotomic μ-invariants of modular forms", in: *Compos. Math.* 147.5 (2011), pp. 1353–1381, ISSN: 0010-437X, DOI: 10.1112/S0010437X11005318, URL: https://doi.org/10.1112/S0010437X11005318.

[Rib92] Kenneth A. Ribet, "Abelian varieties over $\mathbf{Q}$ and modular forms", in: *Algebra and topology 1992 (Taejŏn)*, Korea Adv. Inst. Sci. Tech., Taejŏn, 1992, pp. 53–79.

[Ros16] Giovanni Rosso, "Derivative at $s = 1$ of the p-adic L-function of the symmetric square of a Hilbert modular form", in: *Israel J. Math.* 215.1 (2016), pp. 255–315, ISSN: 0021-2172, DOI: 10.1007/s11856-016-1379-5, URL: https://doi.org/10.1007/s11856-016-1379-5.

[RS01] Kenneth A. Ribet and William A. Stein, "Lectures on Serre's conjectures", in: *Arithmetic algebraic geometry (Park City, UT, 1999)*, vol. 9, IAS/Park City Math. Ser. Amer. Math. Soc., Providence, RI, 2001, pp. 143–232, DOI: 10.1090/pcms/009/04, URL: https://doi.org/10.1090/pcms/009/04.

[RS11] Kenneth A. Ribet and William A. Stein, "Lectures on modular forms and Hecke operators", 2011, URL: http://wstein.%20org/books/ribet-stein/main.%20pdf.

[Shi83] Goro Shimura, "Algebraic relations between critical values of zeta functions and inner products", in: *Amer. J. Math.* 105.1 (1983), pp. 253–285, ISSN: 0002-9327, DOI: 10.2307/2374388, URL: https://doi.org/10.2307/2374388.

[Sil09] Joseph H. Silverman, *The arithmetic of elliptic curves*, Second, vol. 106, Graduate Texts in Mathematics, Springer, Dordrecht, 2009, pp. xx+513, ISBN: 978-0-387-09493-9, DOI: 10.1007/978-0-387-09494-6, URL: https://doi.org/10.1007/978-0-387-09494-6.

[Sil94] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, vol. 151, Graduate Texts in Mathematics, Springer-Verlag, New York, 1994, pp. xiv+525, ISBN: 0-387-94328-5, DOI: 10.1007/978-1-4612-0851-8, URL: https://doi.org/10.1007/978-1-4612-0851-8.

[Spi14] Michael Spieß, "On special zeros of p-adic L-functions of Hilbert modular forms", in: *Invent. Math.* 196.1 (2014), pp. 69–138, ISSN: 0020-9910, DOI: 10.1007/s00222-013-0465-0, URL: https://doi.org/10.1007/s00222-013-0465-0.

[SU14] Christopher Skinner and Eric Urban, "The Iwasawa main conjectures for GL_2", in: *Invent. Math.* 195.1 (2014), pp. 1–277, ISSN: 0020-9910, DOI: 10.1007/s00222-013-0448-1, URL: https://doi.org/10.1007/s00222-013-0448-1.

[Tam21] Matteo Tamiozzo, "On the Bloch-Kato conjecture for Hilbert modular forms", in: *Math. Z.* 299.1-2 (2021), pp. 427–458, ISSN: 0025-5874, DOI: 10.1007/s00209-020-02689-0, URL: https://doi.org/10.1007/s00209-020-02689-0.

[TW95] Richard Taylor and Andrew Wiles, "Ring-theoretic properties of certain Hecke algebras", in: *Ann. of Math. (2)* 141.3 (1995), pp. 553–572, ISSN: 0003-486X, DOI: 10.2307/2118560, URL: https://doi.org/10.2307/2118560.

[Wan15] Xin Wan, "The Iwasawa main conjecture for Hilbert modular forms", in: *Forum Math. Sigma* 3 (2015), Paper No. e18, 95, DOI: 10.1017/fms.2015.16, URL: https://doi.org/10.1017/fms.2015.16.

[Wei] Ariel Weiss, *Serre's Conjecture*, Accessed: 27/12/2022.

[Yos94] Hiroyuki Yoshida, "On the zeta functions of Shimura varieties and periods of Hilbert modular forms", in: *Duke Math. J.* 75.1 (1994), pp. 121–191, ISSN: 0012-7094, DOI: 10.1215/S0012-7094-94-07505-4, URL: https://doi.org/10.1215/S0012-7094-94-07505-4.

[YZZ13] Xinyi Yuan, Shou-Wu Zhang and Wei Zhang, *The Gross-Zagier formula on Shimura curves*, vol. 184, Annals of Mathematics Studies, Princeton University Press, Princeton, NJ, 2013, pp. x+256, ISBN: 978-0-691-15592-0.

[Zha01a] Shou-Wu Zhang, "Gross-Zagier formula for GL_2", in: *Asian J. Math.* 5.2 (2001), pp. 183–290, ISSN: 1093-6106, DOI: 10.4310/AJM.2001.v5.n2.a1, URL: https://doi.org/10.4310/AJM.2001.v5.n2.a1.

[Zha01b] Shouwu Zhang, "Heights of Heegner points on Shimura curves", in: *Ann. of Math. (2)* 153.1 (2001), pp. 27–147, DOI: 10.2307/2661372, URL: https://doi.org/10.2307/2661372.

[Zha04] Shou-Wu Zhang, "Gross-Zagier formula for GL(2). II", in: *Heegner points and Rankin L-series*, vol. 49, Math. Sci. Res. Inst. Publ. Cambridge Univ. Press, Cambridge, 2004, pp. 191–214, DOI: 10.1017/CBO9780511756375.008, URL: https://doi.org/10.1017/CBO9780511756375.008.

[Zha14] Wei Zhang, "Selmer groups and the indivisibility of Heegner points", in: *Camb. J. Math.* 2.2 (2014), pp. 191–253, ISSN: 2168-0930, DOI: 10.4310/CJM.2014.v2.n2.a2, URL: https://doi.org/10.4310/CJM.2014.v2.n2.a2.