Shafarevich-Tate groups for some Modular Abelian Varieties

Casper M. Barendrecht

A Thesis

in

The Department

of

Mathematics and Statistics

Presented in Partial Fulfillment of the Requirements

for the Degree of

Master of Science (Mathematics) at

Concordia University

Montréal, Québec, Canada

September 2020

CONCORDIA UNIVERSITY

School of Graduate Studies

This is to certify that the thesis prepared

By: **Casper M. Barendrecht**

Entitled: **Shafarevich-Tate groups for some Modular Abelian Varieties**

and submitted in partial fulfillment of the requirements for the degree of

Master of Science (Mathematics)

complies with the regulations of this University and meets the accepted standards with respect to originality and quality.

Signed by the Final Examining Committee:

_____ Chair
Dr. Giovanni Rosso

_____ Examiner
Dr. Matteo Longo

_____ Supervisor
Dr. Adrian Iovita

Approved by _____
Galia Dafni, Chair
Department of Mathematics and Statistics

_____ 2020

_____
Pascale Sicotte, Dean
Faculty of Arts and Science

Abstract

Shafarevich-Tate groups for some Modular Abelian Varieties

Casper M. Barendrecht

Let $f = \sum_{n=1}^{\infty} a_n q^n$ be a weight 2 newform of level N, and let A be the associated modular abelian variety. Let K be an imaginary quadratic field of discriminant $D \neq -3, -4$, and let $\mathfrak{p}$ be a prime of the endomorphism ring $\mathcal{O}_A$ of A outside a finite set S. If A admits a principal polarization, and the Heegner point y_K has infinite order in $A(K)$, then the Shafarevich-Tate group is finite and its $\mathfrak{p}$-primary part is a perfect square. Generalizing the work of Kolyvagin and McCallum, we give an explicit structure of the $\mathfrak{p}$-primary part of the Shafarevich-Tate group,

$$\text{ord}_{\mathfrak{p}}|Ш(A/K)| = 2(M_0 - m),$$

where $M_0 = [A(K) : \mathcal{O}_A y_K]$ and m is the minimum of a decreasing sequence of positive integers. This thesis aims to provide an accessible proof of this statement for those with restricted knowledge on the subject.

The first three chapters offer an introduction to the basic notion of arithmetic geometry. Chapters 4 and 5 expand on the theory spefic to the thesis. Finally chapter 6 combines the developed theory to proof this structure theorem for Shafarevich-Tate groups.

Contents

Introduction

Let A be an abelian variety defined over a number field K. A significant group that naturally arises in the study of the arithmetic of A is the Shafarevich-Tate group, given by

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

where v ranges over all places of K. It is widely conjectured that the Shafarevich-Tate group $Ш(A/K)$ is finite. While currently unproven, the finiteness of the Shafarevich-Tate group guarantees that generators for the group $A(K)$ can be computed effectively.

Let E be a modular elliptic curve, whose conductor N is split in a quadratic imaginary field K. In 1984, Benedict Gross and Don Zagier showed that the Heegner point y_K has infinite order if and only if the L-series of E over K has order at most 1 at 1, that is $L'(E/K, 1) \neq 0$ (Gross 1991). Victor Kolyvagin later showed that any such elliptic curve has analytic rank at most one, and moreover has a finite Shafarevich-Tate group over K.

In his 1991 paper, William McCallum, elaborates on some of the later work by Kolyvagin and gives an explicit description of the p-primary part of the Shafarevich-Tate group of E over K in terms of derived Heegner points P_n as defined in chapter 5. Let $p \geq 11$ be a prime number and let $M > 0$ be an integer. An *M-Kolyvagin prime* is a rational prime l whose Frobenius symbol $\mathrm{Frob}(l)$ in the extension $K(A_{p^M})/\mathbb{Q}$ coincides with the symbol of complex conjugation on K. For a non-negative integer r, define $S_r(M)$ to be the collection collection of products of r distinct M-Kolyvagin primes, and let

$$M_r = \min\{\mathrm{ord}_p(P_n) \mid n \in S_r(\mathrm{ord}_p(P_n) + 1)\}.$$

Using these integers, McCallum gave the following description of the Shafarvich-Tate group

Theorem (McCallum 1991)**.** *Let $p \geq 11$ be an integer and assume that y_K has infinite order in $E(K)$. Then the integers M_r are decreasing and $M_0 = [E(K) : \mathbb{Z}y_K]$. Moreover, the p-primary part of the Shafarevich-Tate group, decomposes as*

$$Ш(A/K)_{p^\infty} = \prod_{r=1}^{\infty} \mathbb{Z}/p^{M_{r-1}-M_r}\mathbb{Z}.$$

This thesis aims to generalize the results of McCallum to modular abelian varieties associated to weight 2 newforms whose conductor is split in the field K. We aim to provide accessible Lemmas and proofs for people with limited knowledge of the subject. The reader is expected to be familiar with the theory of elliptic curves, for example the book *The arithmetic of elliptic curves* by Joseph Silverman.

The first three chapters serve as an introduction to the general theory of arithemtic geometry and modular forms, most theory found in these chapters is widely available

from other sources. The first chapter serves as an introduction to the Shafarevich-Tate group and ideal torsion groups. The second chapter constructs several important pairings in the groups to abelian varieties and remarks several important properties. The third chapter is an introduction to the theory of Hecke operators and newforms, based on the book *A first course in modular forms* by Fred Diamond and Jerry Shurman. In Section 3.3, we moreover construct the abelian varieties that will be considered in this thesis. Chapter 4 provides some technical consequences of the Chebotärev Density Theorem. Chapter 5 introduces the notion of Heegner points and construct the classes associated to them. It lays the ground work for the proof of the structure theorem in Chapter 6 (Theorem 6.3). Moreover, Chapter 5 offers a proof of an important theorem by Kolyvagin (Theorem 5.5), and illustrates several important consequences.

Chapter 1

The Shafarevich-Tate group

This first chapter serves as an introduction to the basic principles in the study of the arithemtic of abelian varieties. The first section defines the Shafarevich-Tate group associated to an abelian variety A, as well as justifies its significance in the study of the variety. The second section generalizes the results of the first section for non-principal prime ideals.

1.1 Selmer groups and the Hasse principle

Let A be any abelian variety over $\mathbb{Q}$ such that its ring of $\mathbb{Q}$-rational endomorphism is an order $\mathcal{O}_A$ in a number field F, and let K be another number field. For any place v of K, denote by K_v the completion of K with respect to this valuation. If $v = v_\lambda$ for a prime λ of K, we denote K_λ for K_{v_λ}.

We wish to determine the structure of the algebraic group $A(K)$. One of the most fundamental results in determining this structure is the Mordell-Weil theorem which states that $A(K)$ is finitely generated. In order to find those generators or give a bound on the rank of $A(K)$, more work needs to be done. Let $\alpha \in \mathcal{O}_A$ be an endomorphism of A, and consider the short exact sequence of group schemes

$$0 \to A_\alpha \xrightarrow{\iota} A \xrightarrow{\alpha} A \to 0,$$

where A_α denote the α-torsion points of A. A direct consequence of the Mordell-Weil theorem is that the corresponding sequence of K-rational points will never be exact when α is not a unit. The extent to which this sequence fails to be exact, is determined by the corresponding cohomology groups, which fit in a short exact sequence

$$0 \to A_\alpha(K) \xrightarrow{\iota} A(K) \xrightarrow{\alpha} A(K) \xrightarrow{\delta} H^1(K, A_\alpha) \xrightarrow{\iota_*} H^1(K, A) \xrightarrow{\alpha_*} H^1(K, A) \to H^2(K, A_\alpha)$$

where δ denotes the Kummer map. This sequence in turn gives rise to an exact sequence

$$0 \to A(K)/\alpha A(K) \xrightarrow{\delta} H^1(K, A_\alpha) \to H^1(K, A)_\alpha \to 0. \tag{1.1}$$

This sequence is of particular interest, as it can be shown that generators for $A(K)$ can be computed effectively if given a finite set of points in $A(K)$ generating $A(K)/nA(K)$ for some $n \in \mathbb{Z}$ (see Silverman 2009, Remark VIII.3.2). Currently there is no effective way of constructing generators for $A(K)/nA(K)$. The *Hasse principle* asserts that one can construct such generators given generators for $A(K_v)/nA(K_v)$ for all valuations v of K. By Hensel's lemma, finding such generators is equivalent to determining whether a given principal homogenous space admits a point over some finite ring (see Silverman 2009, Chapter X.4). Hence determining the structure of $A(K)$ reduces to determining where the Hasse principle fails. Hence consider the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A(K)/\alpha A(K) & \xrightarrow{\delta} & H^1(K, A_\alpha) & \xrightarrow{\iota_*} & H^1(K, A)_\alpha & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \prod_v A(K_v)/\alpha A(K_v) & \xrightarrow{\delta_v} & \prod_v H^1(K_v, A_\alpha) & \xrightarrow{\iota_{v*}} & \prod_v H^1(K_v, A)_\alpha & \longrightarrow & 0. \end{array} \tag{1.2}$$

There are two natural groups associated to this diagram.

Definition 1.1. Let A be an abelian variety over K and let α be an endomorphism of A.
The α-*Selmer group* of A over K is given by

$$S_\alpha(A/K) = \ker\left(H^1(K, A_\alpha) \to \prod_v H^1(K_v, A)_\alpha\right).$$

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

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

Note that the product coincides with the direct sum in this definition as any $d \in H^1(K, A)$ vanishes in $H^1(K_v, A)$ for all but finitely many v. The non-zero elements of the Shafarevich-Tate group correspond to those principal homogenous spaces of A that posess a K_v-rational point for all places v, but no K-rational point. Equivalently, they correspond to classes of $H^1(K, A)$ where the Hasse principle fails to hold. By the snake lemma, the Selmer group and the Shafarevich-Tate group fit in the α-descent sequence

$$0 \to A(K)/\alpha A(K) \to S_\alpha(A/K) \to Ш(A/K)_\alpha \to 0.$$

The Selmer group is finite and can be computed effectively, thus it remains to determine the image of $A(K)/\alpha A(K)$ inside this group. For a rational prime p, Milne 2006b, Remark 5.2 shows that generators of $A(K)/pA(K)$ can be constructed effectively if the the p-primary part of the Shavarevich-Tate group is finite. The p-primary part of this group decomposes as the product of the $\mathfrak{p}$-primary parts, where $\mathfrak{p}$ are the primes of $\mathcal{O}_A$ extending p, as described in the following section.

1.2 $\mathfrak{p}$-adic torsion points

Let p be a prime number that is unramified in F 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

$$A_{p^M} = \prod_{\mathfrak{p}|p} A_{\mathfrak{p}^M}. \tag{1.3}$$

Multiplication by p^M is an isogeny of degree p^{2gM} on 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 a $\mathcal{O}_A/p^M\mathcal{O}_A$-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 a $\mathcal{O}_A/\mathfrak{p}^M$-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. 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- odule 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 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 Ribet 1992, Lemma 3.1 that the determinant of this representation is in fact the p-th cyclotomic character

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

The Shaferevich-Tate group of A carries a natural structure of a $\mathcal{O}_A$-module. When it is is finite, it is a torsion module and hence the structure of this group can be analyzed by analyzing its $\mathfrak{p}$-primary parts, where $\mathfrak{p}$ ranges over the primes of $\mathcal{O}_A$. To this end, we aim to generalize the construction of (1.2) to prime ideals. When $\mathcal{O}_A$ is a principal ideal domain, this is immediate, but this is not the case in general. Similar to the decomposition in (1.3), there is a natural decomposition of $\mathbb{Z}/p^M\mathbb{Z}$-modules

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

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

$$A(K)/\mathfrak{p}^M A(K) \hookrightarrow A(K)/p^M A(K) \xrightarrow{\delta} H^1(K, A_{p^M}) \xrightarrow{\text{proj}} H^1(K, A_{\mathfrak{p}^M})$$

Explicitly, let $P \in A(K)$ and consider its reduction modulo $\mathfrak{p}^M A(K)$. By the decomposition above, there exists a $Q \in A(K)$ such that $Q \equiv P$ modulo $\mathfrak{p}^M A(K)$ and $Q \in \mathfrak{q}^M A(K)$ 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 $\sigma \in \text{Gal}(\overline{K}/K)$ 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

$$0 \to A(K)/\mathfrak{p}^M A(K) \xrightarrow{\delta} H^1(K, A_{\mathfrak{p}^M}) \to H^1(K, A)_{\mathfrak{p}^M} \to 0. \tag{1.4}$$

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

$$S_{\mathfrak{p}^M}(A/K) = \ker\left(H^1(K, A_{\mathfrak{p}^M}) \to \bigoplus_v H^1(K, A)\right)$$

and retain the short exact sequence

$$0 \to A(K)/\mathfrak{p}^M A(K) \to S_{\mathfrak{p}^M}(A/K) \to Ш(A/K)_{\mathfrak{p}^M} \to 0.$$

Let

$$H^1(K, A_{\mathfrak{p}^\infty}) = \varinjlim H^1(K, A_{\mathfrak{p}^M}), \qquad \text{and} \qquad S_{\mathfrak{p}^\infty}(A/K) = \varinjlim S_{\mathfrak{p}^M}(A/K),$$

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

$$0 \to A(K) \otimes_{\mathcal{O}_A} F_\mathfrak{p}/\mathcal{O}_\mathfrak{p} \to S_{\mathfrak{p}^\infty}(A/K) \to Ш(A/K)_{\mathfrak{p}^\infty} \to 0, \tag{1.5}$$

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

Chapter 2

Pairings on abelian varieties

Pairing on abelian varieties lie at the heart of arithmetic geometry and the study of Shafarevich-Tate groups. Two pairings of particular interest are the Tate pairing and the Cassels-Tate pairing. This chapter is dedicated to constructing these pairings as well as providing the connection between them. A more in depth exposition can be found in Milne 2006a. In this section K will always denote a number field, and v will denote a place of K.

2.1 The Weil pairing

The most well-known example of a pairing on an abelian variety is the Weil pairing. Let E be an elliptic curve defined over K and let n be an integer. The Weil e_n-pairing is the pairing

$$e_n : E_n \times E_n \to \mu_n$$

as constructed in Silverman 2009, Chapter III.8. Here μ_n denotes the collection of n-th roots of unity. This pairing is non-degenerate, alternating and Galois-invariant. Central to the construction of this pairing is the group isomorphism

$$\begin{aligned} \Phi : E &\to \mathrm{Pic}^0(E), \\ P &\mapsto (P) - (0). \end{aligned} \tag{2.1}$$

While this isomorphism is well-defined for elliptic curves, a generalization to abelian varieties of dimension $g > 1$ does not usually exist. In order to generalize the e_n-pairing to abelian varieties we introduce the notion of dual abelian varieties.

Definition 2.1. Let A/K be an abelian variety of dimension g. The *dual abelian variety* $A^\vee$ of A is the connected component $\mathrm{Pic}^0(A)$ of the Picard scheme $\mathrm{Pic}(A)$.

The Picard scheme should be considered as the scheme-theoretic equivalent of the Picard group $H^1(X, \mathcal{O}_X^*)$ of a scheme X. If X is a smooth projective variety, its connected

component $\mathrm{Pic}^0(X)$ is indeed an abelian variety. Its dimension as a variety is equal to the arithmetic genus of the variety X.

The map in (2.1) is not only an isomorphism of groups, it is also a degree 1 isogeny between an abelian variety and its dual. An isogeny $\phi : A \to A^\vee$ from an abelian variety to its dual is called a *polarization* on A. If ϕ is a degree 1 isogeny, it is called a *principal polarization* and A is said to admit a principal polarization. It can be shown that every polarization arises from an ample line bundle on A (see Conrad 2005, Corollary 5.1.5.). If A has multiplication by an order in a number field then $A^\vee$ has multiplication by the same order. To generalize the e_n-pairing to abelian varieties the natural question arises whether every abelian variety admits a principal polarization. This is not the case in general, however it is still possible to construct a natural generalization of the e_n-pairing to abelian varieties. With the concession of replacing A with its dual, there exists a pairing

$$e_n : A_n \times A_n^\vee \to \mu_n.$$

Following Milne 2008, the pairing is constructed as follows. Assume for simplicity that K is algebraically closed and let $a \in A_n(K)$, and $b \in A_n^\vee(K)$. Using the identification $A_n^\vee(K) = \mathrm{Pic}^0(A)(K)$, let $D \in \mathrm{Div}^0(A)$ be a divisor on A corresponding to b. If n_A denotes multiplication by n on A, then multiplication by n on $\mathrm{Pic}^0(A)$ coincides with the map n_A^*. Hence $n_A^* D$ is linearly equivalent to nD, which is linearly equivalent to zero as b is n-torsion. In particular, there exist rational functions f and g such that $n_A^* D = \mathrm{div}(g)$ and $nD = \mathrm{div}(f)$. Using the equality

$$\mathrm{div}(f \circ n_A) = n_A^* \mathrm{div}(f) = n_A^* nD = n n_A^* D = n \cdot \mathrm{div}(g) = \mathrm{div}(g^n)$$

we conclude that $g^n/(f \circ n_A) = c$ is constant on A. As a is n-torsion it follows that

$$g(X+a)^n = cf(nX+na) = \frac{g(X)^n}{f(nX)} f(nX) = g(X)^n.$$

Hence $g(X)/g(X+a)$ is a function in the field $K(A)$ whose n-th power is 1. It is therefore an n-th root of unity and is contained in K. The e_n-pairing is now defined by sending a and b to this root. For abelian varieties whose endomorphism ring is an order in a number field the e_n-pairing naturally generalizes to an $e_{\mathfrak{p}^M}$-pairing as follows:

Lemma 2.2. For any abelian variety A/K whose endomorphism ring is an order $\mathcal{O}_A$ in a finite extension $F/\mathbb{Q}$, and for any unramified, invertible prime $\mathfrak{p}$ of $\mathcal{O}_A$, the restriction of the e_{p^M}-pairing to the $\mathfrak{p}^M$-torsion of A defines a non-degenerate pairing

$$e_{\mathfrak{p}^M} : A_{\mathfrak{p}^M} \times A_{\mathfrak{p}^M}^\vee \to \mu_{p^M}.$$

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 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 $\mathfrak{q}^M$-torsion points of $A^\vee$ for all primes $\mathfrak{p} \neq \mathfrak{p}$. 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. □

If a finite abelian group G admits a non-degenerate pairing $\alpha : G \times G \to \mathbb{Q}/\mathbb{Z}$, we can define the orthogonal complement $H^\perp$ of any subgroup H of G, as the collection of elements of G that are orthogonal to all elements of H under this pairing. This group fits in a natural short exact sequence

$$0 \to H^\perp \to G \to H^* \to 0,$$

where H^* denotes the Pontryagin dual of H, and the second map is given by evaluation. If in addition, the pairing is alternating, and H is generated by a set of pairwise orthogonal elements, there is a natural inclusion $H \subset H^\perp$. Subgroups satisfying this inclusion are called *isotropic subgroups* of G. Because G is finite, all of its subgroups are isomorphic to their duals. Hence if H is an isotropic subgroup, we must have $|H| \leq |G|^{1/2}$. Consequently, a *maximal isotropic subgroup* is an isotropic subgroup of maximal order, or equivalently a subgroup satifying $H = H^\perp$. If G contains a maximal isotropic subgroup, its order is necessarily a perfect square. It can be shown that such a subgroup always exists, and in fact the following stronger statement holds.

Lemma 2.3. (Lemma 5.2 Davydov 2007) Let G be a finite group admitting an alternating, non-degenerate pairing. Then G contains a maximal isotropic subgroup H such that the sequence

$$0 \to H \to G \to H^* \to 0$$

splits. In particular, the order of G is a perfect square.

2.2 Cup products

Cup products are a method of connecting two cohomology classes of degree p and r together to construct a new cohomology class of degree $p + r$. They are integral to the construction of dualities in Galois cohomology and various other cohomological topics.

Let G be a group and let M and N be two G-modules. The cup product is then defined as the pairing

$$H^p(G,M) \times H^r(G,N) \to H^{p+r}(G, M \otimes N),$$
$$(\zeta, \alpha) \mapsto \zeta \smile \alpha,$$

where

$$(\zeta \smile \alpha)(\sigma_1, ..., \sigma_{p+r}) = \zeta(\sigma_1, ..., \sigma_p) \otimes \alpha(\sigma_{p+1}, ..., \sigma_{p+r}),$$

with $\sigma_1, ..., \sigma_{p+r} \in G$. The cup product satisfies the following properties

1. $(a \smile b) \smile c = a \smile (b \smile c)$,
2. $a \smile b = (-1)^{\deg(a)\deg(b)}(b \smile a)$,
3. $\inf(a \smile b) = \inf(a) \smile \inf(b)$,
4. $\mathrm{res}(a \smile b) = \mathrm{res}(a) \smile \mathrm{res}(b)$.

Here res and inf denote the usual inflation and restriction maps. Recall that giving a bilinear pairing of G-modules $e : M \times N \to P$ is equivalent to giving a linear map $e' : M \otimes N \to P$. If the pairing e is G-equivariant, that is $e(ga, gb) = g(e(a, b))$ for all $g \in G$, one can compose e' with the cup product to create a new family of cup products

$$H^p(G, M) \times H^r(G, N) \to H^{p+r}(G, P).$$

This observation has important consequences; Given an A be an abelian variety over a number field K, an integer n, and a non-archimedean valuation v of K. One can view μ_n as a group subscheme of the multiplicative group $\mathbb{G}_m$, and consider the e_n-pairing (resp. $e_{\mathfrak{p}^M}$-pairing) as a pairing

$$A_n \times A_n^\vee \to \mathbb{G}_m.$$

Taking Galois cohomology, gives a pairing

$$H^1(K_v, A_n) \times H^1(K_v, A_n^\vee) \to H^2(K_v, \mathbb{G}_m).$$

The latter group is occasionally referred to as the Brauer group of K_v and is denoted $\mathrm{Br}(K_v)$[1]. Since K_v is a non-archimedean local field, the Hasse-invariant determines an isomorphism

$$\mathrm{inv}_v : H^2(K_v, \mathbb{G}_m) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}.$$

And we obtain an alternating pairing

$$H^1(K_v, A_n) \times H^1(K_v, A_n^\vee) \to \mathbb{Q}/\mathbb{Z}. \tag{2.2}$$

It can be shown that this pairing is non-degenerate (see Poonen et al. 1999). The Brauer group of K fits in a short exact sequence

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

[1]The Brauer group itself is in fact defined as the set of Morita equivalence classes of central simple K-algebras endowed with a group structure via the tensor product. It can however be shown that these groups are isomorphic for any field K.

In this direct sum, v ranges over all places of K and the second map is given by taking the sum of the Hasse invariants. The completions at the archimedean primes correspond to either $\mathbb{R}$ or $\mathbb{C}$, for the real numbers we have that $\mathrm{Br}(\mathbb{R}) = \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ and the Brauer group of the complex numbers is trivial. From the exact sequence we deduce the following for $c \in H^1(K, A_n)$ and $c' \in H^1(K, A_n^\vee)$

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

Assume that A has multiplication by an order $\mathcal{O}_A$ in a finite extension $F/\mathbb{Q}$. Assume moreover that A admits a principal polarization. The cup product in (2.2) then becomes a pairing on $H^1(K, A_{\mathfrak{p}^M})$, which by (1.4) acts on $A(K)/\mathfrak{p}^M A(K)$.

Proposition 2.4. Assume that A admits a principal polarization, and let v be a non-archimdean place of K, coprime to p, such that A has good reduction at v. Then the image of $A(K_v)/\mathfrak{p}^M A(K_v)$ under δ is a maximal isotropic subgroup of $H^1(K_v, A_{\mathfrak{p}^M})$. In particular, it gives rise to a non-degenerate pairing

$$\langle \cdot, \cdot \rangle_v : H^1(K_v, A)_{\mathfrak{p}^M} \times A(K_v)/\mathfrak{p}^M A(K_v) \to \mathbb{Q}/\mathbb{Z}. \tag{2.3}$$

Proof. Let v be such a place of K. By Silverman 2009, Lemma VIII.2.1, the image of δ is unramified. In particular, the sequence in (1.4) reduces to

$$0 \to A(K_v)/\mathfrak{p}^M A(K_v) \xrightarrow{\delta} H^1(K_v^{\mathrm{ur}}/K_v, A_{\mathfrak{p}^M}) \to H^1(K_v^{\mathrm{ur}}/K_v, A)_{\mathfrak{p}^M} \to 0,$$

where $H^1(K_v^{\mathrm{ur}}/K_v, A_{\mathfrak{p}^M})$ is embedded into $H^1(K_v, A_{\mathfrak{p}^M})$ via the inflation map. As A has good reduction at v, the group $H^1(K_v^{\mathrm{ur}}/K_v, A)$ vanishes (see Milne 2006a, 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 $H^1(K_v^{\mathrm{ur}}/K_v, A_{\mathfrak{p}^M})$ is given by a pairing

$$H^1(K_v^{\mathrm{ur}}/K_v, A_{\mathfrak{p}^M}) \times H^1(K_v^{\mathrm{ur}}/K_v, A_{\mathfrak{p}^M}) \to H^2(K_v^{\mathrm{ur}}/K_v, \mu_{p^M}).$$

But as v is coprime to p, it can be deduced from the Hochschild-Serre spectral sequence, that latter group vanishes (see Milne 2006a, Lemma 2.9). It follows that the inflated group us isotropic and hence so $\delta(A(K_v)/\mathfrak{p}^M A(K_v))$.

To prove maximality, it suffices to show that $H^1(K_v, A)_{\mathfrak{p}^M}$ is isomorphic to $A(K_v)/\mathfrak{p}^M A(K_v)$. As $H^1(K_v^{\mathrm{ur}}/K_v, A)$ vanishes, it follows from inflation-restriction that restriction induces an isomorphism $H^1(K_v, A)_{\mathfrak{p}^M} \xrightarrow{\sim} H^1(K_v^{\mathrm{ur}}, A)^{\mathcal{G}}_{\mathfrak{p}^M}$, where $\mathcal{G}$ denotes the Galois group of K_v^{ur}/K_v. Moreover, as $A(K_v^{\mathrm{ur}})$ is p-divisible, the sequence in (1.4) induces an isomorphism $H^1(K_v^{\mathrm{ur}}, A_{\mathfrak{p}^M}) \cong H^1(K_v^{\mathrm{ur}}, A)_{\mathfrak{p}^M}$, and hence an isomorphism of their $\mathcal{G}$-invariant subgroups. Since the $\mathfrak{p}^M$-torsion points of A are unramified over K_v, the action of the inertia group I of K_v on $A_{\mathfrak{p}^M}$ is trivial. This gives rise to the natural identification $H^1(K_v^{\mathrm{ur}}, A_{\mathfrak{p}^M}) = \mathrm{Hom}(I, A_{\mathfrak{p}^M})$. Let l denote the characteristic of the residue field of K_v. It follows from ramification theory that the wild ramification group I^{wild} of K_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 $\mathbb{Z}_q(1) := \varprojlim \mu_{q^n}$. As any homomorphism f as above factors through this group, we conclude that $H^1(K_v, A)_{\mathfrak{p}^M}$ is isomorphic to the group $\text{Hom}(\mu_{p^M}, A_{\mathfrak{p}^M})^{\mathcal{G}}$. The group of p^M-roots of unity is cyclic, hence this group of homomorphisms is naturally isomorphic to $A_{\mathfrak{p}^M}(K_v)$, and since multiplication by p is an isomorphism on $\mathcal{O}_v$, it follows from Milne 2006a, Lemma 3.3 that $A(K_v)/\mathfrak{p}^M A(K_v)$ is isomorphic to $A_{\mathfrak{p}^M}(K_v)$ as well. It follows that $\delta(A(K_v)/\mathfrak{p}^M A(K_v))$ is maximal isotropic.

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

$$0 \to \delta(A(K_v)/\mathfrak{p}^M A(K_v)) \to H^1(K_v, A_{\mathfrak{p}^M}) \xrightarrow{\text{ev}} \delta\left(A(K_v)/\mathfrak{p}^M A(K_v)\right)^* \to 0.$$

Hence consider the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A(K_v)/\mathfrak{p}^M A(K_v) & \xrightarrow{\delta} & H^1(K_v, A_{\mathfrak{p}^M}) & \xrightarrow{\iota_*} & H^1(K_v, A)_{\mathfrak{p}^M} & \longrightarrow & 0 \\ & & \| & & \| & & \uparrow \varphi & & \\ 0 & \longrightarrow & A(K_v)/\mathfrak{p}^M A(K_v) & \xrightarrow{\delta} & H^1(K_v, A_{\mathfrak{p}^M}) & \xrightarrow{\text{ev}} & \delta\left(A(K_v)/\mathfrak{p}^M A(K_v)\right)^* & \longrightarrow & 0. \end{array}$$

Here φ is the map making this diagram commutative. It is given by the composition $\iota_* \circ \text{ev}^{-1}$, which is well-defined by exactness. Because all groups are finite, φ is an isomorphism. For any $y \in A(K_v)/\mathfrak{p}^M A(K_v)$ and $d \in H^1(K_v, A)_{\mathfrak{p}^M}$, 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. □

The pairing in equation (2.3) is also known as the Tate-pairing. In proving Proposition 2.4, we have also shown the following useful relation between the cup-product and the Tate pairing:

$$\langle \iota_{v*}(c), x \rangle_v = c \smile \delta(x) \tag{2.4}$$

Remark. In Chapter I, Section 3 of his book "Arithmetic Duality Theorems", Milne provides a more profound argument to show that maximality of $A(K_v)/\mathfrak{p}^M A(K_v)$. Any triple (M, N, P) of $\text{Gal}(\overline{K_v}/K_v)$-modules comes equipped with a canonical family of Ext-pairings. For an abelian variety A, the group $\text{Ext}^r_{K_v}(\mathbb{Z}, A)$ is simply the cohomology group $H^r(K_v, A)$. Hence for the triple $(A, \mathbb{Z}, \mathbb{G}_m)$ these pairings are given by

$$\text{Ext}^r_{K_v}(A, \mathbb{G}_m) \times H^{2-r}(K_v, A) \to H^2(K_v, \mathbb{G}_m).$$

The latter is isomorphic to $\mathbb{Q}/\mathbb{Z}$, and it can be shown that these pairings are in fact perfect. The Ext-groups of an abelian variety are closely related to the dual abelian variety by the isomorphisms

$$H^r(K_v, A^\vee) \xrightarrow{\sim} \text{Ext}^{r+1}_{K_v}(A, \mathbb{G}_m).$$

For $r = 1$, this isomorphism along with the pairing above, add up to an isomorphism of compact groups

$$A^\vee(K_v) \xrightarrow{\sim} H^1(K_v, A)^*.$$

The group of $\mathfrak{p}^M$-torsion of $H^1(K_v, A)$ is isomorphic to the group of $\mathfrak{p}^M$-torsion of its Pontryagin dual, and since A admits a principal polarization, this module is therefore isomorphic to the group $A_{\mathfrak{p}^M}(K_v)$. As multiplication by p is an isomorphism on $\mathcal{O}_v$, this module has the same rank as $A(K_v)/\mathfrak{p}^M A(K_v)$.

This construction by Milne allows a more universal definition of the Tate pairing. Since the Ext-pairing and the isomorphisms above only depend on the fact that v is non-archimidean, they give rise to a canonical perfect pairing

$$\langle \cdot, \cdot \rangle_v : H^1(K_v, A) \times A^\vee(K_v) \to \mathbb{Q}/\mathbb{Z}.$$

This definition can be extended to the archimedean places (see Milne 2006a, Remark 3.7).

2.3 The Cassels-Tate pairing

The Tate pairing allows us to construct a pairing on the Shafarevich-Tate groups, known as the Cassels-Tate pairing. The Cassels-Tate pairing is fundamental in understanding the structure of the Shafarevich-Tate group and hence the the structure of the abelian variety A itself. They were first introduced by Cassels for elliptic curves and were later generalized by Tate to a pairing

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

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' be two positive integers, and let $d \in Ш(A/K)_{\mathfrak{p}^M}$ and $d' \in Ш(A^\vee/K)_{\mathfrak{p}^{M'}}$ be two cohomology classes. Let $c' \in S_{\mathfrak{p}^{M'}}(A^\vee/K)$ 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 K. Hence via the Kummer sequence (1.4), we can choose a set $\{y'_v \in A(K_v)\}$ such that

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

Next assume that there exists a $d_1 \in H^1(K, A)_{\mathfrak{p}^{M+M'}}$ 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 K, the reduction $d_{1,v}$ must necessarily be a $\mathfrak{p}^{M'}$-torsion point of $H^1(K_v, A)$. 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 K and assume that $y_v \in A(K_v)$ is another point such that $\delta(y_v) = c'_v$. Then $y'_v - y_v$ vanishes under δ and is therefore contained in $\mathfrak{p}^{M'}A(K_v)$. 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 $d_2 \in H^1(K, A)_{\mathfrak{p}^{M+M'}}$ in the pre-image of d. The difference $d_1 - d_2$ is contained in $H^1(K, A)_{\mathfrak{p}^{M'}}$, and hence originates from a global cocycle $c \in H^1(K, A_{\mathfrak{p}^{M'}})$. Using the relation described in (2.4), this implies that

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

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

Remark. 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 Milne 2006a, Proposition 6.9 and the corresponding remarks. Other constructions can also be found in Poonen et al. 1999. For the classes d considered in this thesis, such a d_1 always exists.

For elliptic curves, Cassels showed that this pairing is non-degenerate and alternating after dividing by maximal divisible subgroups (see Poonen et al. 1999). In particular, if the Shafarevich-Tate group is finite, its order must be a perfect square. This was later generalized by Tate for abelian varieties over K, who showed that the pairing is non-degenerate after dividing by maximal divisible subgroups. Note that any polarization ϕ on A gives rise to a pairing

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

Tate also showed that this pairing is alternating if ϕ was a polarization arising from K-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 Poonen et al. 1999). Flach later showed that such a pairing is anti-symmetric if ϕ is a principal polarization. Note that anti-symmetry and skew-symmetry are equivalent whenever $2 \neq 0$. Hence for principally polarized abelian varieties A with finite Shafarevich-Tate group, the order of its p-primary part will always be a perfect square when p is an odd prime, and the order of the entire group will either be a perfect square or twice a perfect square. In their 1999 paper, Poonen and Stoll associated a class $c \in H^1(K, A)$ to any principal polarization, and showed that the order of $Ш(A/K)_{2^\infty}$ is a perfect square if and only if $\langle c, c \rangle = 0$. Moreover, by using this c they constructed a modified pairing $\langle \cdot, \cdot \rangle^c$ which is non-degenerate and alternating if and only if $\langle c, c \rangle = 0$.

Chapter 3

Modular abelian varieties

This chapter serves as a brief introduction to modular forms, Hecke operators, newforms and the abelian varieties associated to newforms. Additionally notation is introduced at the end of the section, and several propositions are formulated which will prove fruitfull in later sections. Most propositions and proofs originate from Diamond et al. 2005, and the reader is encouraged to read this book for a broader exposition of the topic.

3.1 Modular forms

Consider the complex upper half plane

$$\mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$$

with the natural topology. Define an action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$, by letting

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\tau + b}{c\tau + d} \text{ for all } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

For any $\tau \in \mathbb{H}$, define the lattice $\Lambda_\tau = \mathbb{Z} + \tau\mathbb{Z}$, and consider the corresponding elliptic curve $E_\tau = \mathbb{C}/\Lambda_\tau$. Then $\tau_1, \tau_2 \in \mathbb{H}$ give rise to $\mathbb{C}$-isomorphic elliptic curves if and only if there exists a $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma\tau_1 = \tau_2$ (see Silverman 1994, Lemma 1.2) . As $-I$ acts trivally on $\mathbb{H}$, we can further impose that $\gamma \in \Gamma_0(1) = \mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$, and we define $Y_0(1) = \Gamma_0(1)\backslash\mathbb{H}$. In greater generality, for integers $N > 1$, define the congruence subgroup

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \mod N \right\},$$

and let $Y_0(N) = \Gamma_0(N)\backslash\mathbb{H}$. This space is Hausdorff, and can be compactified by adding a finite number of points of $\mathbb{P}^1(\mathbb{Q})$, known as the cusps of $\Gamma_0(N)$. This compactification is called the *classic modular curve of level* N and is denoted $X_0(N)$. It carries the

structure of a Riemann Surface. Let $\{\alpha_1, ..., \alpha_r\}$ be a set of coset representatives of $\Gamma_0(N)$ in $\mathrm{SL}_2(\mathbb{Z})$. The cusps of $\Gamma_0(N)$ are then given by the orbits of $\alpha_r(\infty)$ under the action of $\Gamma_0(N)$. It can occur that two corepresentatives correspond to the same cusp of $\Gamma_0(N)$.

Intuitively, the classical modular curve parametrizes isogenies between elliptic curves with cyclic kernel isomorphic to $\mathbb{Z}/N\mathbb{Z}$; Any point in $Y_0(N)$ corresponds to an isomorphism class of elliptic curves, together with a finite cyclic subgroup of order N. Consider the matrix

$$\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}.$$

It acts as multiplication by N on $\mathbb{H}$. For any $\tau \in \mathbb{H}$, the lattices $\Lambda_{N\tau}$ and $\frac{1}{N}\mathbb{Z} + \tau\mathbb{Z}$ are homothetic, hence they give rise to $\mathbb{C}$-isomorphic elliptic curves. The second lattice contains Λ_τ as a sublattice of index N, and therefore gives rise to an isogeny of degree N. Hence to any $\tau \in \mathbb{H}$, we associate the short exact sequence of algebraic groups

$$0 \to \left(\tfrac{1}{N}\mathbb{Z} + \tau\mathbb{Z}\right) \Big/ (\mathbb{Z} + \tau\mathbb{Z}) \to \mathbb{C} \Big/ (\mathbb{Z} + \tau\mathbb{Z}) \to \mathbb{C} \Big/ \left(\tfrac{1}{N}\mathbb{Z} + \tau\mathbb{Z}\right) \to 0.$$

Two points τ_1, τ_2 are then equivalent if there exists some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ inducing an isomorphism between the elliptic curves in this sequence, and this holds if and only if $\gamma \in \Gamma_0(N)$.

Let $f : \mathbb{H} \to \mathbb{C}$ be a continuous function, for any integer $k \geq 0$ and $\gamma \in \mathrm{GL}_2^+(\mathbb{Q})$, the *weight* $2k$ *operator* is defined as

$$f[\gamma]_{2k}(\tau) = \det(\gamma)^{2k-1}(c\tau + d)^{-2k} f(\gamma\tau),$$

where $c = (\gamma)_{21}$ and $d = (\gamma)_{22}$ are the coeffcients of γ.

Definition 3.1. Let $k \geq 0$ be an integer. A *weakly modular function* of weight $2k$ and level N is a meromorphic function $f : \mathbb{H} \to \mathbb{C}$ that f remains meromorphic when extended to all the cusps of $\Gamma_0(N)$ and satisfies the level N modularity condition:

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^{2k} f(\tau) \text{ for all } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N).$$

A *modular form* is a weakly modular function that is holomorphic on $\mathbb{H}$ and all the cusps of $\Gamma_0(N)$. If it moreover vanishes at all the cusps of $\Gamma_0(N)$, it is said to be a *cusp form.*

A modular form can eqivalently be defined as a holomorphic function that is weight $2k$ invariant for all $\gamma \in \Gamma_0(N)$, that is $f[\gamma]_{2k} = f$. Consider the matrix given by $a = b = d = 1$ and $c = 0$. It is contained in $\Gamma_0(N)$ and acts on $\mathbb{H}$ by addition of 1. Hence by the modularity condition any modular form f must be periodic. In particular, it can be expressed as a Fourier series

$$f = \sum_{n=0}^{\infty} a_n q^n$$

where $q^n = e^{2\pi i\tau}$. A modular form then vanishes at infinity, if and only if $a_0 = 0$. Consider the set of coset representatives $\{\alpha_1, ..., \alpha_r\}$ of $\Gamma_0(N)$ in $\mathrm{SL}_2(\mathbb{Z})$. Since f is a modular form with respect to $\Gamma_0(N)$, its weight $2k$ conjugates $f_j = f[\alpha_j]_{2k}$ are modular forms with respect to the groups $\alpha_j^{-1}\Gamma_0(N)\alpha_j$. Moreover they satisfy $f_j(\infty) = f(y_j)$, where y_j is the cusp corresponding to α_j. Hence f is a cusp form if and only if $a_0 = 0$ in the fourier expansion of f_j for all j. A typical example of a modular form is the modular discriminant

$$\Delta(\tau) = q\prod_{n=1}^{\infty}(1-q^n)^{24}$$

which sends τ to the discriminant of the Weirestraß equation of the elliptic curve associated to τ. The collection of cusp forms of weight $2k$ carry a natural structure of a $\mathbb{C}$-vector space and is denoted $\mathcal{S}_{2k}(N)$. This space admits the following inner product.

Definition 3.2. Let $N \geq 1$ and$k \geq 0$ be two positive integers. The *Petersson inner product* is defined as the pairing

$$\begin{aligned}\langle\cdot,\cdot\rangle : \mathcal{S}_{2k}(N)\times\mathcal{S}_{2k}(N) &\to \mathbb{C},\\ (f,g) &\mapsto \frac{1}{[\mathrm{SL}_2(\mathbb{Z}):\Gamma_0(N)]}\int_{X_0(N)} f(\tau)\overline{g(\tau)}\mathrm{Im}(\tau)^{2k}d\nu(\tau),\end{aligned}$$

where $d\nu(x+iy) = \frac{dxdy}{y^2}$ denotes the hyperbolic volume.

Since $X_0(N)$ carries the structure of a Riemann-Surface, the notion of holomorphy is well-defined on it, and we can fix an atlas $\{V_j\}_{j\in J}$ on it. Let $\tau_j \in V_j$ and let $\gamma \in \Gamma_0(N)$ be given. Letting $d\tau_j$ denote the standard differential of τ, simple computation shows that $d(\gamma\tau_j) = (c\tau + d)^{-2}d\tau_j$. Thus, for a modular form $f = (g_j)_j$ of weight $2k$, the object $(g_j(\tau_j)d\tau_j^k)_{j\in J}$ is $\Gamma_0(N)$-invariant, and hence a differential k-form ω_f on $X_0(N)$. It follows from the theory of automorphic forms that this ω_f is a holomorphic k-form if and only if f vanishes at all the cusps of $X_0(N)$ (see Diamond et al. 2005, Chapter 3). Moreover, any holomorphic k-form is induced by a weight $2k$ cusp form, and as distinct modular forms give rise to distinct differentials, this proves that the map

$$\begin{aligned}\mathcal{S}_{2k}(N) &\to H^0\left(X_0(N), \Omega^k_{X_0(N)}\right),\\ f &\mapsto \omega_f\end{aligned} \tag{3.1}$$

is an isomorphism of $\mathbb{C}$-vector spaces.

3.2 Hecke operators

Since the set of modular forms is a $\mathbb{C}$-vector space, one can speak of operators on this space. A type of operator that is of particular interest in the theory of modular forms is the Hecke operator. Let p be a prime number and consider the matrix

$$P = \begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}.$$

This matrix acts as division by p on $\mathbb{H}$, and therefore gives rise to a degree p isogeny $E_\tau \to E_{\tau/p}$, for any $\tau \in \mathbb{H}$. In particular, it shows that the point τ/p is p-isogenous to τ on $Y_0(N)$. Let $\gamma \in \Gamma_0(N)$ be any matrix, as γ does not necessarily commute with P, the points $\gamma\tau/p$ and τ/p need not be congruent modulo $\Gamma_0(N)$ and hence correspond to different points on $Y_0(N)$. In this case the composition $E_\tau \to E_{\gamma\tau} \to E_{\gamma\tau/p}$ is another isogeny of degree p, and hence gives rise to another p-isogenous point on $Y_0(N)$. In fact all p-isogenous points of $Y_0(N)$ are realized by such a composition. This leads to the study of the distinct points of $Y_0(N)$ are p-isogenous to τ.

Any p-isogeny respecting the level N structure is given by an element of $P\Gamma_0(N)$. Two points in $\mathbb{H}$ are in the same class of $Y_0(N)$ if they are in the same $\Gamma_0(N)$ orbit. Hence the distinct p-isogeny classes given a certain point in $Y_0(N)$ are in one to one correspondence with the orbits of $\Gamma_0(N)\backslash\Gamma_0(N)P\Gamma_0(N)$.

Definition 3.3. Let f be a weakly modular function of weight $2k$ and level N, and let p a prime number. Let $\{\beta_j\}_{j\in J}$ be a set of coset representatives of the orbits of $\Gamma_0(N)\backslash\Gamma_0(N)P\Gamma_0(N)$. The *$p$-th Hecke operator* acting on f is defined as

$$T_p(f) = \sum_{j\in J} f[\beta_j]_{2k}.$$

The Hecke operators can be described explicitly if given a set of orbit representatives $\{\beta_j\}$ as in Definition 3.3. By Diamond et al. 2005, Lemma 5.1.2, giving such a set is equivalent to giving a set of orbit representatives $\{\gamma_j\}$ for the action $\Gamma_3\backslash\Gamma_0(N)$, where $\Gamma_3 = (P^{-1}\Gamma_0(N)P) \cap \Gamma_0(N)$, via the identification $\beta_j = P\gamma_j$. Observe that

$$P^{-1}\Gamma_0(N)P = \left\{ \begin{pmatrix} a & pb \\ \frac{c}{p} & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Q}) \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \right\}.$$

Hence

$$\Gamma_3 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \mod N,\ b \equiv 0 \mod p \right\}.$$

Hence Γ_3 is given by all matrices of $\Gamma_0(N)$ subject to the addtional condition that $b \equiv 0 \mod p$. Consequently, a natural choice of coset representatives would be given by

$$\gamma_j = \begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix},\ 0 \le j < p.$$

Clearly the γ_j are in distinct Γ_3 orbits. Let $\gamma \in \Gamma_0(N)$, then γ is contained in the orbit of γ_j if and only if $\gamma\gamma_j^{-1} \in \Gamma_3$. Observe that

$$\gamma\gamma_j^{-1} = \begin{pmatrix} a & b - aj \\ c & jc + d \end{pmatrix},$$

hence γ is contained in the γ_j orbit if and only if $b - aj \equiv 0 \mod p$. Such a j exists if and only if $p \nmid a$, since p cannot divide a and b simultaneously. If $p \mid N$, then p divides c and by the same argument, it follows that $p \nmid a$. In this case it follows that $\{\gamma_j\}$ is a complete set of orbit representatives for $\Gamma_3 \backslash \Gamma_0(N)$. If $p \nmid N$, there exist $m, n \in \mathbb{Z}$ such that $mp - nN = 1$. Define the matrix

$$\gamma_\infty = \begin{pmatrix} mp & n \\ N & 1 \end{pmatrix} \in \Gamma_0(N),$$

and assume that $p \mid a$. Then

$$\gamma\gamma_\infty^{-1} = \begin{pmatrix} a - bN & bmp - an \\ c - dN & dmp - cn \end{pmatrix} \in \Gamma_3,$$

and hence $\{\gamma_j \mid 0 \leq j < p\} \cup \{\gamma_\infty\}$ is a complete set of orbit representatives. By applying Diamond et al. 2005, Lemma 5.1.2, it follows that

$$\beta_j = \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix},\ 0 \leq j < p,\ \beta'_\infty = \begin{pmatrix} m & n \\ N & p \end{pmatrix} \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix},$$

forms a complete set of orbit representatives for $\Gamma_0(N) \backslash \Gamma_0(N) P \Gamma_0(N)$. Note that β'_∞ can be replaced with the multiplication by p-matrix β_∞ as the first matrix in the product is contained in $\Gamma_0(N)$. Hence, the p-th Hecke operator admits the following explicit description

$$T_p f(\tau) = \begin{cases} \frac{1}{p} \sum_{j=0}^{p-1} f\left(\frac{\tau + j}{p}\right) + \frac{1}{p} f(p\tau), & p \nmid N \\ \frac{1}{p} \sum_{j=0}^{p-1} f\left(\frac{\tau + j}{p}\right), & p \mid N \end{cases} \tag{3.2}$$

Working recursively, Hecke operators can be defined for any $n > 0$.

Definition 3.4. The n-th Hecke operator for any $n > 0$ is defined by the relations

1. $T_1 = 1$
2. $T_{mn} = T_m T_n$ if $(m, n) = 1$
3. $T_{p^r} = \begin{cases} T_p T_{p^{r-1}} - p^{2k-1} T_{p^{r-2}}, & p \nmid N \\ T_p T_{p^{r-1}}, & p \mid N \end{cases}$

Since Hecke operators are sums of weight $2k$-operators, they preserve the space of modular forms and the space of cusp forms. Of particular interest are those forms that are eigenvectors for all Hecke operators simultaneously. Such forms are called *Hecke eigenforms*. Hecke operators play an integral role in determining the structure of modular

form. In fact, the fourier transform of a modular form can be described entirely in terms of the fourier transforms of the Hecke operators. Hecke eigenforms allow an even more explicit description.

Theorem 3.5. Let $f = \sum_{n=0}^{\infty} a_n(f)q^n$ be a modular form of level N and weight $2k$. Then for any $n \geq 0$, we have the equality

$$a_n(f) = a_1(T_n f).$$

If f is an eigenform for T_n with eigenvalues λ_n, then

$$a_n(f) = a_1(T_n f) = \lambda_n a_1(f).$$

Proof. A more universal statement and proof can be found in Diamond et al. 2005, most notably Proposition 5.3.1. □

If f is an eigenform for all n coprime to N such that $a_1(f) = 0$, then Theorem 3.5 shows that $a_n(f) = 0$ for all n coprime to N. The main lemma of Atkin-Lehner theory states that any such cusp form can be expressed as a sum

$$f(\tau) = \sum_{p|N} g_p(p\tau), \text{ for some } g_p \in \mathcal{S}_{2k}(N/p).$$

These kinds of cusp forms are examples of *old forms*.

Definition 3.6. The *old subspace* $\mathcal{S}_{2k}(N)^{\text{old}}$ is the subspace of level N cusp forms spanned by all

$$f(\tau) = g(d\tau),$$

where g is a level M cusp form with M a proper divisor of N and $d \mid N/M$. An *oldform* is an element in the old subspace. The *new subspace* $\mathcal{S}_{2k}(N)^{\text{new}}$ is the orthogonal complement of the old subspace in the space of cusp forms under the Petersson inner product . A level N *newform* is a Hecke eigenform in the new subspace such that $a_1 = 1$.

Both spaces are preserved by the Hecke operators (see Diamond et al. 2005, Proposition 5.6.2) Notice that an eigenform can be a newform at atmost one level. This level is called the conductor of f. A strong theorem states that any modular form in the new subspace that is an eigenform for all Hecke operators away from the level, is in fact an eigenform for all Hecke operators (see Diamond et al. 2005, Theorem 5.8.2) This thesis will focus primarily on weight 2 newforms as they retain strong algebraic properties.

Proposition 3.7. Let $f = \sum_{i=1}^{n} a_n q^n$ be a level N newform of weight 2. Then a_n is a real algebraic integer for all n.

Proof. Recall that the Jacobian of $X_0(N)$ is given by

$$J_0(N) = H^0\left(X_0(N), \Omega^1_{X_0(N)}\right)^* \Big/ H_1(X_0(N), \mathbb{Z}) \cdot$$

Hence the isomorphism in (3.1) allows us to identify

$$J_0(N) = \mathcal{S}_2(N)^* \Big/ H_1(X_0(N), \mathbb{Z}). \tag{3.3}$$

Note that the Hecke operators acts on $\mathcal{S}_2(N)^*$ by composition. By Diamond et al. 2005, Proposition 6.3.2, this action of Hecke operators induces an action on the Jacobian of $X_0(N)$. In particular it acts on the finitely generated abelian group $H_1(X_0(N), \mathbb{Z})$. This shows that the characteristical polynomial of T_n has integer coefficients, and as it is monic, all of its eigenvalues are algebraic integers. Hence by Theorem 3.5, a_n is an algebraic integer for all n. The Hecke operators T_n for n coprime to N are self adjoint with respect to the Petersson inner product (Diamond et al. 2005, Theorem 5.5.3). Consequently, their eigenvalues are real and hence so is a_n, for n coprime to N. It now follows from the Strong Multiplicity One theorem that a_n is real for all n. □

3.3 Abelian varieties associated to newforms

Proposition 3.7 shows that all coefficients of a weight 2 newform f are real algebraic integers. In particular, the field of coefficients of f is a real, algebraic extension of $\mathbb{Q}$. Since the Hecke operators act on the finitely generated abelian group $H_1(X_0(N), \mathbb{Z})$, this field satisfies even stronger properties.

Definition 3.8. The *Hecke algebra of level N* is the endomorphism ring of $S_2(N)$ generated by the Hecke operators,

$$\mathbb{T}_N = \mathbb{Z}[T_n \mid n \in \mathbb{N}].$$

As the Hecke algebra acts on $H_1(X_0(N), \mathbb{Z})$, this ring is a finitely generated $\mathbb{Z}$-module of rank at most $4g_N$, where g_N is the genus of $X_0(N)$. Let f be a weight 2 newform of level N, and consider the map

$$\begin{aligned} \lambda_f : \mathbb{T}_N &\to \overline{\mathbb{Q}}, \\ T_n &\mapsto a_1(T_n f). \end{aligned}$$

Denote its kernel by $\mathcal{I}_f$. This homomorphism surjects onto the coefficient ring of f and hence induces an isomorphism

$$\lambda_f : \mathbb{T}_N / \mathcal{I}_f \xrightarrow{\sim} \mathbb{Z}[a_n \mid n \in \mathbb{N}].$$

In particular, this ring is a finitely generated $\mathbb{Z}$-module and its field of fractions is hence a real number field. Moreover, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the space of cusp forms by acting on the coefficients of the fourier expansion of a cusp form. Since this action commutes with the action of the Hecke operators, f^σ is again a newform for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. In particular all its coefficients are real, and hence the field of coefficients $F = \mathbb{Q}(a_n \mid n \in \mathbb{N})$ is a totally real number field.

It follows from the construction of Hecke operators that their action on $J_0(N)$ is given by regular maps. Moreover, as the Hecke operators respect the group law on $J_0(N)$, they are morphisms of abelian varieties. Hence $\mathbb{T}_N$ can be realized as a subring of $\mathrm{End}(J_0(N))$. The image of a morphism $\alpha : A \to B$ between abelian varieties is an abelian subvariety of B. Hence for any $\alpha \in \mathcal{I}_f$, $\alpha(J_0(N)$ is an abelian subvariety of $J_0(N)$, and since $\mathcal{I}_f$ is finitely generated, it now follows that

$$\mathcal{I}_f(J_0(N)) := \sum_{\alpha \in \mathcal{I}_f} \alpha(J_0(N)) \subset J_0(N)$$

is an abelian subvariety of $J_0(N)$ as well. This obervation together with the following proposition allows us to construct the abelian variety A_f associated to f.

Proposition 3.9. Let A be an abelian variety and let B be an abelian subvariety of A. Then there exists a unique abelian variety C together with a surjective morphism of abelian varieties $\varphi : A \to C$ such that $\ker(\varphi) = B$, satisfying the following universal property: For any surjective morphism of abelian varieties $g : A \to D$, with $B \subset \ker(g)$ there exists a unique morphism $g' : C \to D$ such that the following diagram commutes.

$$\begin{array}{ccc} A & \xrightarrow{g} & D \\ \downarrow{\scriptstyle \varphi} & \nearrow_{g'} & \\ C & & \end{array}$$

Moreover, $\dim A = \dim B + \dim C$.

Proof. A proof can be found in Perret-Gentil 2014, Proposition 1.56 and Polishchuk 2003, Section 9.5. □

Thus for any newform f of weight 2 and level N we define the abelian variety A_f as

$$A_f := J_0(N)/\mathcal{I}_f(J_0(N)). \tag{3.4}$$

As $J_0(N)$ is defined over $\mathbb{Q}$, so is A_f. An abelian variety A defined over $\mathbb{Q}$ admitting a surjective morphism $\alpha_f : J_0(N) \to A$ is called a *modular abelian variety*. In fact it can be shown that any modular abelian variety is isogenous to a product of abelian variety A_f associated to newforms f (Ribet 1992, Theorem 4.4). The modularity of A_f gives a strong insight in its structure. An immediate concequence is that A_f has conductor N.

Proposition 3.10. Let $A = A_f$ be an abelian variety associated to a weight 2 newform f of level N, and let $F = \mathbb{Q}(a_n \mid n \in \mathbb{N})$ be the field of coefficients of A The following statements hold.

1. A has dimension $g = [F : \mathbb{Q}]$.
2. A has real multiplication by the order $\mathcal{O}_A = \mathbb{Z}[a_n \mid n \in \mathbb{N}]$.
3. All real multiplications $\alpha \in \mathcal{O}_A$ of A are defined over $\mathbb{Q}$.

Proof. Let g_N denote the dimension of $J_0(N)$. By Proposition 3.9, the first statement is equivalent to the condition that $\dim \mathcal{I}_f(J_0(N)) = g_N - [F : \mathbb{Q}]$. Consider the short exact sequence of free $\mathbb{Z}$-modules

$$0 \to \mathcal{I}_f \to \mathbb{T}_N \to \mathbb{Z}[a_n \mid n \in \mathbb{N}] \to 0.$$

Extension of scalars gives rise to an exact sequence of $\mathbb{C}$-vector spaces

$$0 \to \mathcal{I}_f \otimes \mathbb{C} \to \mathbb{T}_N \otimes \mathbb{C} \to \mathbb{C}^{[F:\mathbb{Q}]} \to 0.$$

Denote $\mathbb{T}_{\mathbb{C}} = \mathbb{T}_N \otimes \mathbb{C}$ and consider the pairing

$$\mathbb{T}_{\mathbb{C}} \times \mathcal{S}_2(N) \to \mathbb{C}, \ (T, g) \mapsto a_1(Tg).$$

This pairing is non-degenerate and hence induces an isomorphism $h : \mathbb{T}_{\mathbb{C}} \to S_2(N)^*$. In particular its dimension as a $\mathbb{C}$-vector space coincides with the dimension of $J_0(N)$ as well as the rank of $\mathbb{T}_N$ (by equation (3.3)). Hence by the exact sequence above, $\dim \mathcal{I}_f \otimes \mathbb{C} = g_N - [F : \mathbb{Q}]$. This vector space acts on $\mathcal{S}_2(N)^*$ by composition on the right. On the other hand, as $\mathcal{I}_f \otimes \mathbb{C}$ is an ideal in $\mathbb{T}_{\mathbb{C}}$, and since h is an isomorphism, this action coincides with ideal action of $\mathcal{I}_f \otimes \mathbb{C}$ on $\mathbb{T}_{\mathbb{C}}$. Hence the image of this action is simply $\mathcal{I}_f(\mathcal{S}_2(N)^*) \otimes \mathbb{C}$, which allows the identification $\mathcal{I}_f \otimes \mathbb{C} = \mathcal{I}_f(\mathcal{S}_2(N)^*) \otimes \mathbb{C}$. By linearity, this is the same space as the space generated by the action of $\mathcal{I}_f$ on $\mathcal{S}_2(N)^*$, whose dimension as a $\mathbb{C}$-vector space coincides with the dimension of the variety $\mathcal{I}_f(J_0(N))$. We conclude that $\dim_{\mathbb{C}} \mathcal{I}_f \otimes \mathbb{C} = g_N - [F : \mathbb{Q}]$ as required.

The action of the Hecke algebra $\mathbb{T}_N$ on $J_0(N)$ decends to an action on A_f. The kernel of this action is precisely the group $\mathcal{I}_f$ and hence the quotient $\mathbb{T}_N/\mathcal{I}_f$ acts faithfully on A_f. As this ring is naturally isomorphic to $\mathbb{Z}[a_n \mid n \in \mathbb{N}]$, we conclude that this order acts on A_f. In particular, this gives an injection $F \hookrightarrow \mathbb{Q} \otimes \mathrm{End}_{\mathbb{Q}}(A)$. Any number field L acting faithfully on A_f, must act faithfully on $\mathrm{Lie}(A/\mathbb{Q})$ by functoriality. As this is a $\mathbb{Q}$-vector space of dimension $\dim A_f = [F : \mathbb{Q}]$, the dimension of L is bounded by $[F : \mathbb{Q}]$. Hence F is the largest field that can act faithfully on A_f, and we conclude that A_f has totally real multiplication by the order $\mathbb{Z}[a_n \mid n \in \mathbb{N}]$. This proves property the second statement.

The third statement follows directly from the fact that the Hecke operators are defined over $\mathbb{Q}$. □

In proving Proposition 3.10, the following useful proposition was also proved.

Proposition 3.11. Let $A = A_f$ be a modular abelian variety associated to a newform $f = \sum_{n=1}^{\infty} a_n q^n$ of conductor N Then for any $p \nmid N$, the following diagram commutes:

$$\begin{array}{ccc} J_0(N) & \xrightarrow{T_p} & J_0(N) \\ \downarrow{\scriptstyle \alpha_f} & & \downarrow{\scriptstyle \alpha_f} \\ A_f & \xrightarrow{a_p} & A_f \end{array}$$

For the rest of this thesis, unless otherwise stated, A will always be a modular abelian variety of the type constructed above, and N will denote its conductor which will henceforth be assumed to be square-free. The notations $\mathcal{O}_A$ and F are used to denote the order and number field as described in Proposition 3.10. Moreover, we a ssume that A admits a principal polarization.

3.4 The Eichler-Shimura relation

Let p be a prime number not dividing N. Since $X_0(N)$ is a projective curve of conductor N, it has good reduction modulo p. Denote the reduced curve by $\tilde{X}_0(N)$, and define the Frobenius map $\mathrm{Fr}_p : \tilde{X}_0(N) \to \tilde{X}_0(N)$, raising all coefficients of a point P to the p-th power. Since $\tilde{X}_0(N)$ is a curve, its divisors are generated by the points on $\tilde{X}_0(N)$, hence the Frobenius map induces a forward map $\mathrm{Fr}_{p,*}$ on the set of divisors via

$$(P) \mapsto (\mathrm{Fr}_p(P)).$$

It also defines a reverse map Fr_p^* via

$$(P) \mapsto \sum_{Q \in \mathrm{Fr}_p^{-1}(P)} e_Q(\mathrm{Fr}_p)(Q),$$

where $e_Q(\mathrm{Fr}_p)$ denotes the ramification degree of Fr_p at Q. As the Frobenius map is bijective and ramified of degree p everywhere, the second expression can be simplified to

$$(P) \mapsto p(\mathrm{Fr}_p^{-1}(P)).$$

Both maps reduce to a map on $\mathrm{Pic}^0(\tilde{X}_0(N))$. Since the Picard group is canonically isomorphic to the Jacobian $\tilde{J}_0(N)$, these two maps give rise to endomorphisms of $\tilde{J}_0(N)$. In particular, the composition satisfies

$$\mathrm{Fr}_p^* \circ \mathrm{Fr}_{p,*} = p \cdot 1_{\mathrm{End}(\tilde{J}_0(N))}$$

Furthermore, the Eichler-Shimura relation states that the diagram

$$\begin{array}{ccc} J_0(N) & \xrightarrow{T_p} & J_0(N) \\ \downarrow & & \downarrow \\ \tilde{J}_0(N) & \xrightarrow{\mathrm{Fr}_p^* + \mathrm{Fr}_{p,*}} & \tilde{J}_0(N) \end{array} \tag{3.5}$$

commutes (see Diamond et al. 2005, Theorem 8.7.2). Finally Proposition 3.11 gives the relation

$$a_p \circ \alpha_f = \alpha_f \circ T_p.$$

By abuse of notation, write Fr_p for the composition $\alpha_f \circ \mathrm{Fr}_{p,*}$. Using the Eichler-Shimura relation and composing with $\mathrm{Fr}_{p,*}$, now gives the following relation in $\mathrm{End}(A(\overline{F_p}))$

$$\mathrm{Fr}_p^2 - a_l \mathrm{Fr}_p + p = 0. \tag{3.6}$$

Fix an extension $\overline{p}$ of p in $\overline{\mathbb{Q}}$, and denote by $\mathrm{Frob}(p)$ its Frobenius element. Observe that its action on $A(\overline{\mathbb{F}_p})$ coincides with the action of Fr_p and therefore satisfies the same characteristical polynomial in $\mathrm{End}(A(\overline{\mathbb{F}_p}))$. Henceforth, we will refer to $\mathrm{Frob}(p)$ as the Frobenius symbol of p in $\overline{\mathbb{Q}}$ and its natural restrictions to all subfields.

3.5 The Fricke involution

Consider the matrix

$$w_N = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$$

It gives rise to the degree 2 map $\tau \mapsto \frac{-1}{N\tau}$ on $X_0(N)$, known as the *Fricke involution*. The associated weight 2 operator $[w_N]_2$ acting on the space of cusp forms $\mathcal{S}_2(N)$ has degree 2, hence its characteristical polynomial is given by $X^2 - 1$. As this operator acts non-trivially, its minimum polynomial coincides with its characteristical polynomial, and its eigenvalues are ± 1.

Proposition 3.12. The Fricke involution $[w_N]_2$ commutes with Hecke operators T_n for any n coprime to N.

Proof. Let $p \nmid N$ be a prime number. Recall that the Hecke operator T_p can be described explicitly in terms of the coset representatives β_j, as described in (3.2). Hence it suffices to show that conjugation by w_N permutes the orbits of the β_j. A direct computation shows that $w_N^{-1}\beta_\infty w_N = \beta_0$, and as $w_N^{-1} = -N^{-1}w_N$, the converse equation holds as well. Hence conjugation by w_N permutes the orbits of β_0 and β_∞. For $j, j' \neq 0, \infty$, a direct computation shows that the equation $w_N\beta_j = A\beta_{j'}w_N$ has a solution $A \in \Gamma_0(N)$ if and only if $p \mid 1 + Njj'$. Hence for any $j \neq 0, \infty$, conjugation by w_N maps the orbit of β_j onto the orbit of $\beta_{j'}$, where $j' \equiv -(Nj)^{-1} \mod p$. It follows that the Hecke operator T_p commutes with the Fricke involution. The statement now follows for general n coprime to N as every Hecke operator can be written uniquely as a composition of Hecke operators of prime degree. □

Let $f \in \mathcal{S}_2(N)$ be a newform. Since $[w_N]_2$ commutes with the Hecke operators T_n coprime to N, the cusp form $f[w_n]_2$ is again an eigenform for these operators with the same eigenvalues as f. It therefore follows by Diamond et al. 2005, Theorem 5.8.2.b) that $f[w_N]_2 = cf$ for some constant $c \in \mathbb{C}$, and hence that f is an eigenform for the Fricke involution, and $c = \pm 1$. The Fricke involution plays an important role in the structure of L-functions associated to newforms. In fact, the eigenvalue ϵ of a newform f is the negative of the sign of the L function of f at 1 (see Ribet and Stein 2011, Theorem 16.1.4) .

Chapter 4

Chebotärev Density Theorem

This short, technical chapter introduces several lemmas, necessary for later chapters. Of particular interest is Corollary 4.3.1 which plays an integral role in the proof of Proposition 6.6.

From now on assume that K is an imaginary quadratic number field of discriminant $D \neq 3, 4$ and that N splits completely in K. Let p be rational prime such that

1. $p \nmid 6DN\varphi(N)$,
2. p is unramified in F and invertible in $\mathcal{O}_A$,
3. For all $\mathfrak{p}$ extending p in $\mathcal{O}_A$, the map $\rho_{\mathfrak{p}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathcal{O}_{\mathfrak{p}})$ surjects onto the subgroup
$$\{g \in \mathrm{GL}_2(\mathcal{O}_{\mathfrak{p}}) \mid \det(g) \in \mathbb{Z}_p^*\}.$$

Note that these conditions hold for all but finitely many primes p, (see Longo et al. 2013, 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 4.1. There is a natural injection of $\mathrm{Gal}(L/\mathbb{Q})$-modules
$$H^1(K, A_{\mathfrak{p}^M}) \hookrightarrow H^1(L, A_{\mathfrak{p}^M}) = \mathrm{Hom}(\mathrm{Gal}(\overline{\mathbb{Q}}/L), A_{\mathfrak{p}^M}).$$

Proof. Let p be the rational prime below $\mathfrak{p}$. 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 $\mathbb{Q}(A_p)$ are disjoint over $\mathbb{Q}$, hence so are the fields K and $\mathbb{Q}(A_{\mathfrak{p}})$. We obtain that $\mathrm{Gal}(K(A_{\mathfrak{p}})/K) \cong \mathrm{Gal}(\mathbb{Q}(A_{\mathfrak{p}})/\mathbb{Q})$. This group naturally injects in $\mathcal{G} = \mathrm{Gal}(L/K)$, and contains the cyclic subgroup $\mathbb{F}_p^*$ of order $p-1$. As $p-1$ is coprime to p it naturally follows that $H^n(\mathbb{F}_p^*, A_{\mathfrak{p}^M}) = 0$ for all $n \geq 1$. For $n = 0$, we have that $H^0(\mathbb{F}_p^*, A_{\mathfrak{p}^M}) = (A_{\mathfrak{p}^M})^{\mathbb{F}_p^*} = 0$. Inflation-restriction, now gives an exact sequence
$$0 \to H^n(\mathcal{G}/\mathbb{F}_p^*, (A_{\mathfrak{p}^M})^{\mathbb{F}_p^*}) \to H^n(\mathcal{G}, A_{\mathfrak{p}^M}) \to H^n(\mathbb{F}_p^*, A_{\mathfrak{p}^M}).$$

By the above, the last term vanishes and as $(A_{p^M})^{\mathbb{F}_p^*} = 0$ 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 4.2. Let $C \subset \mathrm{Hom}(\mathrm{Gal}(\overline{\mathbb{Q}}/L), A_{\mathfrak{p}^M})$ 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

$$\begin{aligned} \mathrm{Gal}(L_C/L) &\xrightarrow{\sim} \mathrm{Hom}_{\mathcal{G}}(C, A_{\mathfrak{p}^M}), \\ \sigma &\mapsto (\alpha \mapsto \alpha(\sigma)). \end{aligned}$$

Proof. Let C be given as in the proposition, let $\alpha_1, ..., \alpha_r$ generate C as an $\mathcal{O}_M$-module, and let $H = \cap \ker(\alpha_i)$. As each of the kernels in the intersection is an open normal subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$ 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

$$\mathrm{Gal}(\overline{\mathbb{Q}}/L) \to \mathrm{Hom}_{\mathcal{G}}(C, A_{\mathfrak{p}^M})$$

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 $\sigma,\ \tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/L)$ 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 $\tau \in \cap_{i>1} \ker(\alpha_i)$. 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 $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/L))$ 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 $\mathrm{Hom}(\mathrm{Gal}(\overline{\mathbb{Q}}/L), A_{\mathfrak{p}^M})$ by Lemma 4.1, and hence find a Galois extension L_C/L with Galois group isomorphic to $\mathrm{Hom}_{\mathcal{G}}(C, A_{\mathfrak{p}^M})$. 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 $c \in C$,

$$c_\lambda = 0 \Leftrightarrow \phi_\sigma(c) = 0 \text{ for all } \sigma \in G(\lambda_L, L_C) \tag{4.1}$$

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. As 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 $\mathbb{Q}$. This is illustrated in the following proposition.

Proposition 4.3. 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 numbers l, unramified in L such that

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

Proof. Note that the second condition is sound as the extension L_C/L is abelian. 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 Čhebotarev 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 $L/\mathbb{Q}$. Thus, for any prime λ' of L above l, there exists a $\eta \in \mathrm{Frob}(l)$ such that $\eta^2 = \mathrm{Frob}(\tilde{\lambda})$. Thus, for appropriate choice of λ', we conclude that $\mathrm{Frob}(\lambda') = \sigma$. □

Corollary 4.3.1. 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 prime numbers l such that

1. $\mathrm{Frob}(l) = \mathrm{Frob}(\infty)$ in $\mathrm{Gal}(L/\mathbb{Q})$,
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 ord $\phi(c_i) = p^{N_i}$. By Proposition 4.3, there exist infinitely many l such that $\mathrm{Frob}(l) = \mathrm{Frob}(\infty)$ in $\mathrm{Gal}(L/\mathbb{Q})$ and $\sigma = \mathrm{Frob}(\lambda')$ for some λ' extending l. By condition 1, 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 (4.1) that ord $c_{i,\lambda}$ = ord $\phi_\sigma(c_i) = p^{N_i}$ which concludes the proof. □

Chapter 5

Heegner points

Since K is an imaginary quadratic field and N is split in K, the abelian variety A comes equipped with a family of Heegner points defined over the ring class fields of K. The Heegner points give rise to a family of cohomology classes $c_M(n)$, which will later be shown to generate the Sharaevich-Tate group.

In the first section the construction of Heegner points is illustrated as well as the cohomology classes associated to them. Moreover, it provides an explicit description of these cohomology classes (Lemma 5.3), and gives an upper bound on the order of said classes. The second section provides a proof of a theorem by Kolyvagin (Theorem 5.5), which expresses strong relations between the cohomology classes $c_M(n)$. This theorem lays the groundwork for the structure theorem in Chapter 6.

5.1 Cohomology classes associated to Heegner points

Let n be a positive square-free integer whose prime factors are inert in K. Let $\mathcal{O}_n = \mathbb{Z} + n\mathcal{O}_K$ be the order of conductor n, and let K_n be the corresponding ring class field. Recall from class field theory that for coprime l and m as above, the ring class fields K_l and K_m are linearly disjoint over K_1 and satisfy $K_lK_m = K_{ml}$. Consequently let $G_n = \mathrm{Gal}(K_n/K_1)$, then $G_n \cong \prod_{l|n} G_l$ where l runs over all primes dividing n. The group G_l is cyclic of order $l+1$, and there is a natural isomorphism $G_l \cong \mathrm{Gal}(K_n/K_{n/l})$. Henceforth these groups will be regarded as the same object.

As N splits completely in K, there exists an ideal $\mathcal{N} \subset \mathcal{O}_K$ such that $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$. For n as above consider the ideal $\mathcal{N}_n = \mathcal{N} \cap \mathcal{O}_n$. Since $(N, n) = 1$, all prime factors of $\mathcal{N}_n$ are invertible, and the residue is given by $\mathcal{O}_n/\mathcal{N}_n \cong \mathbb{Z}/N\mathbb{Z}$. This yields an inclusion

$$\mathcal{O}_n \subset \mathcal{N}_n^{-1} \subset \mathbb{C}$$

and hence a short exact sequence of algebraic groups

$$0 \to \mathcal{N}_n^{-1}/\mathcal{O}_n \to \mathbb{C}/\mathcal{O}_n \xrightarrow{r_n} \mathbb{C}/\mathcal{N}_n^{-1} \to 0.$$

Notice that $r_n : \mathbb{C}/\mathcal{O}_n \to \mathbb{C}/\mathcal{N}_n^{-1}$ is an isogeny of elliptic curves with kernel isomorphic to $\mathbb{Z}/N\mathbb{Z}$. Hence r_n induces a point $x_n \in X_0(N)(\mathbb{C})$. In fact, since $\mathbb{C}/\mathcal{O}_n$ has complex multiplication by $\mathcal{O}_n$, the pointx_n is defined over K_n. Define the *Heegner point of conductor* n on A as

$$y_n = \alpha_f((x_n) - (\infty)) \in A(K_n).$$

Define the *Heegner point associated to* K as

$$y_K = \mathrm{Tr}_{K_1/K}(y_1).$$

For a prime l let σ_l be a generator for G_l, and denote by Tr_l the object $\sum_{\sigma \in G_l} \sigma \in \mathbb{Z}[G_l]$. Let $D_l \in \mathbb{Z}[G_l]$ be given by

$$D_l = \sum_{i=1}^{l} i \cdot \sigma_l^i$$

It satisfies the equation

$$(\sigma_l - 1) \cdot D_l = l + 1 - \mathrm{Tr}_l. \tag{5.1}$$

For n as above define $D_n = \prod D_l$. Let $\mathcal{G}_n = \mathrm{Gal}(K_n/K)$, and let S be a set of coset representatives of G_n in $\mathcal{G}_n$. Observe that there is a bijection $S \leftrightarrow \mathrm{Cl}(\mathcal{O}_K)$. Finally define the *derived Heegner point of conductor* n, to be the point

$$P_n = \sum_{\sigma \in S} \sigma(D_n y_n) \in A(K_n).$$

Observe that

$$P_1 = \sum_{\sigma \in S} \sigma(y_1) = \mathrm{Tr}_{K_1/K}(y_1) = y_K.$$

Definition 5.1. Let $M \geq 1$ be an integer. An *M-Kolyvagin prime* is a prime number l such that

1. l is inert in K,
2. $a_l \equiv l + 1 \equiv 0 \mod \mathfrak{p}^M$.

Further, define $S(M)$ to be the collection of square-free products of such primes. For integers r, let $S_r(M)$ be the subset of $S(M)$ consisting of integers with exactly r prime factors.

An equivalent definition of an M-Kolyvagin prime is any prime number l such that

$$\mathrm{Frob}(l) = \mathrm{Frob}(\infty) \subset \mathrm{Gal}(K(A_{\mathfrak{p}^M})/\mathbb{Q}).$$

To see this, notice that two elements $\sigma, \eta \in \mathrm{Gal}(\mathbb{Q}(A_{\mathfrak{p}^M})/\mathbb{Q})$ are in the same conjugacy class if and only if their characteristical polynomials in $\mathrm{GL}_2(A_{\mathfrak{p}^M})$ are equal. As $A_{\mathfrak{p}^M}$ injects into $A(\overline{\mathbb{F}_l})$, it follows from (3.6) that the characteristical polynomial of $\mathrm{Frob}(l)$ is

given by $T^2 - a_l T + l$, whereas the characteristical polynomial of $\mathrm{Frob}(\infty)$ is known to be $T^2 - 1$. We hence conclude that condition 2 is equivalent to

$$\mathrm{Frob}(l) = \mathrm{Frob}(\infty) \subset \mathrm{Gal}(\mathbb{Q}(A_{\mathfrak{p}^M})/\mathbb{Q})$$

The property that l is inert in K implies that $\mathrm{Frob}(l)|_K = \tau$, proving the equivalence. While it follows from the condtions above, it is useful to point out that N, D and p are pairwise coprime and that any prime l as above will never divide the product NDp. Further notice that there are inclusions $S_r(M+1) \subset S_r(M)$.

Proposition 5.2 (Gross 1991, Proposition 3.6)**.** Let $n \in S(M)$, then $A_{p^M}(K_n) = 0$ and

$$P_n \in (A(K_n)/\mathfrak{p}^M A(K_n))^{\mathcal{G}_n}$$

Proof. The first statement follows directly from Longo et al. 2013, Proposition 3.9 as the Galois group $\mathrm{Gal}(K_n/\mathbb{Q})$ is solvable. To prove the second statement, it suffices to show that $D_n y_n \in (A(K_n)/\mathfrak{p}^M A(K_n))^{G_n}$. Let l be a prime dividing n, and write $n = ml$. Using the equality $D_n = D_l D_m$ and (5.1) we obtain

$$(\sigma_l - 1) \cdot D_n y_n = (l + 1 - \mathrm{Tr}_l) D_m y_n \tag{5.2}$$

It follows from Kolyvagin and Logachëv 1989, Equation 2.1.4 and Proposition 3.10 that $\mathrm{Tr}_l(y_n) = a_l \cdot y_m \in A(K_m)$. Hence it follows from 2 that

$$(\sigma_l - 1) D_n y_n \equiv 0 \in A(K_n)/\mathfrak{p}^M A(K_n)$$

and thus $\sigma_l D_n y_n = D_n y_n \in A(K_n)/\mathfrak{p}^M A(K_n)$. Since G_n is generated by these σ_l we conclude that

$$D_n y_n \in \left(A(K_n) \Big/ \mathfrak{p}^M A(K_n) \right)^{G_n}$$

□

Using these points, Kolyvagin was able to construct cohomology classes in $H^1(K, A_{\mathfrak{p}^M})$ in the following manner. Consider the diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A(K)/\mathfrak{p}^M A(K) & \xrightarrow{\delta} & H^1(K, A_{\mathfrak{p}^M}) & \xrightarrow{\iota_*} & H^1(K, A)_{\mathfrak{p}^M} & \longrightarrow & 0 \\
 & & \downarrow & & \wr \downarrow \mathrm{res} & & \downarrow \mathrm{res} & & \\
0 & \longrightarrow & (A(K_n)/\mathfrak{p}^M A(K_n))^{\mathcal{G}_n} & \xrightarrow{\delta_n} & H^1(K_n, A_{\mathfrak{p}^M})^{\mathcal{G}_n} & \xrightarrow{\iota_{n*}} & H^1(K_n, A)^{\mathcal{G}_n}_{\mathfrak{p}^M} & &
\end{array}$$

Notice that restriction is indeed an isomorphism since $H^1(K_n/K, A_{\mathfrak{p}^M}) = 0$ as a consequence of Proposition 5.2. Define $c_M(n) \in H^1(K, A_{\mathfrak{p}^M})$ to be the unique class such that

$$\mathrm{res}(c_M(n)) = \delta_n(P_n) \tag{5.3}$$

and let $d_M(n)$ be the image of $c_M(n)$ in $H^1(K, A)$.

Lemma 5.3 (McCallum 1991)**.** Let $Q_n \in A(K_n)$ be any point congruent to P_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 representant for $c_M(n)$, where $\frac{(\sigma-1)Q_n}{p^M}$ is the unique p^M-division point of $(\sigma-1)Q_n$ in $A(K_n)$.

Proof. Let Q_n be any such point, and observe that $\delta_n(P_n) \in H^1(K_n, A_{\mathfrak{p}^M})$ is represented by the cocycle

$$\sigma \mapsto \sigma\frac{Q_n}{p^M} - \frac{Q_n}{p^M}.$$

The existence of the p^M-division point of $(\sigma-1)Q_n$ follows from the second statement of Proposition 5.2 and the fact that $Q_n \in \mathfrak{q}^M A(K_n)$ for all other primes $\mathfrak{q} \mid p$. Since two distinct p^M-division points differ by a p^M-torsion point, the first statement of Proposition 5.2 guarantees the uniqueness of the point. The term $\sigma \mapsto -\frac{(\sigma-1)Q_n}{p^M}$ 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 $\sigma \in \mathcal{G}_n$, its restriction to K_n is precisely the representative of $\delta_n(P_n)$ describe above. It follows that this cocycle is a representative of $c_M(n)$ by (5.3). □

Corollary 5.3.1. The class $d_M(n)$ is represented by the cocycle

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

Proof. The map $\sigma \mapsto \sigma\frac{Q_n}{p^M} - \frac{Q_n}{p^M}$ is a coboundary in $H^1(K, A)$. □

Corollary 5.3.2. For all integers $M \geq 2$ and $n \in S(M)$ we have

$$p \cdot c_M(n) = c_{M-1}(n).$$

Proof. Let Q_n be a point as described in Lemma 5.3, and write $c_M(n)$ for the associated cocycle. As $(\sigma-1)Q_n$ has a unique p^M-division point in $A(K_n)$, it 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

$$\begin{aligned}(p \cdot c_M(n))_\sigma &= -\frac{(\sigma-1)Q_n}{p^{M-1}} + p \cdot \sigma\frac{Q_n}{p^M} - p\frac{Q_n}{p^M} \\ &= -\frac{(\sigma-1)Q_n}{p^{M-1}} + \sigma\frac{Q_n}{p^{M-1}} - \frac{Q_n}{p^{M-1}} = c_{M-1}(n)_\sigma.\end{aligned}$$

□

Write $\mathfrak{p}^M \mid P_n$ if $P_n \in \mathfrak{p}^M A(K_n)$, and define

$$\mathrm{ord}_{\mathfrak{p}}(P_n) = \max\{M : \mathfrak{p}^M \mid P_n\}.$$

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

$$\mathrm{ord}\ c_M(n) = p^{M-\mathrm{ord}_{\mathfrak{p}}(P_n)} \tag{5.4}$$

whenever $c_M(n)$ exists. Using this define

$$M_r = \min\{\mathrm{ord}_{\mathfrak{p}}(P_n) \mid n \in S_r(\mathrm{ord}_{\mathfrak{p}}(P_n)+1)\}.$$

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 descripition of the Shafarevich-Tate group (see Corollary 6.3.2).

5.2 Kolyvagin's Theorem

Let $n \in S(M)$, let l be a prime such that $n = ml$, and let λ denote its extension to K. As λ is principal in K it splits completely in K_m by class field theory. Recall that an extension λ' of λ in K_m, induces a local field extension $K_{m,\lambda'}/K_\lambda$ of degree $f(\lambda'/\lambda) = 1$. It therefore induces an embedding $K_m \hookrightarrow K_\lambda$. This observation allows us to embed P_m in $A(K_\lambda)/\mathfrak{p}^M A(K_\lambda)$, and by Proposition 5.2 the class of P_m is independent of the choice of the embedding. Recall that the Hilbert Class field K_1 is the maximal unramified extension of K. In particular since λ is the only prime of K that ramifies in K_l, any prime of K_1 lying above λ must be totally ramified in the extension K_l/K_1. Consequently, any λ' extending λ in K_m must be totally ramified in $K_n = K_m K_l$ by linear disjointness.

Let v be a prime of K dividing N (hence a prime where A has bad reduction), and denote by A_0 the collection of K_v^{ur}-rational smooth points of A. 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 one of the following conditions

1. The prime $\mathfrak{p}$ is principal.
2. If v is a finite place of K where A has bad reduction then v satisfies one of the following conditions:
   (a) v is a principal of K,
   (b) $p \nmid [A : A_0]$.

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 5.4 (Gross 1991)**.** Let $n \in S(M)$, and let v be a valuation of K prime to n, then $c_M(n)_v \in \delta_v(A(K_v))$. Moreover, if $v = v_\lambda$ for some prime l inert in K, we have $c_M(n)_\lambda = \delta_\lambda(P_n)$.

Proof. Notice that the first statement is equivalent to the vanishing of $d_M(n)_v$. Clearly if $v = \infty$, we have $K_v = \mathbb{C}$, and hence $H^1(K_v, A_{\mathfrak{p}^M}) = 0$, thus $d_M(n)_v = 0$. Next assume v is finite, it follows from the construction of $d_M(n)$ that it vanishes when restricted to $H^1(K_n, A)$. It is therefore inflated from a class in $H^1(K_n/K, A)$. As v does not divide n, it is unramified in K_n. This implies that $d_M(n)_v$ acts trivially on the inertia group I_v of K_v, and is therefore contained in the group $H^1(K_v^{\mathrm{ur}}/K_v, A)$. It follows from Milne 2006a, Proposition 3.8 that this group is trivial if v has good reduction.

Assume that A has bad reduction modulo v.
By the same lemma we have $H^1(K_v^{\mathrm{ur}}/K_v, A) = H^1(K_v^{\mathrm{ur}}/K_v, A/A_0)$, where A_0 denotes the open subscheme of smooth points of A. Consider the Heegner point $(x_n) - (\infty)$ on the Jacobian $J_0(N)$, and let w be a valuation of K_n extending v. Then Gross and Zagier 1986, Proposition 3.1 states that either $(x_n) - (\infty)$ or $(x_n) - (0)$ is a smooth point of $J_0(N)(K_{n,w})$. Manin showed that the cusps of $X_0(N)$ reduce to rational torsion points in $J_0(N)$, hence y_n is a smooth point of $A(K_v^{\mathrm{ur}})$ up to addition by a rational torsion point Q. In particular, as $A(\mathbb{Q})$ has no p-torsion, y_n and hence P_n is contained in a group A' containing A_0 with index $[A' : A_0]$ coprime to p. If $\mathfrak{p}$ is principal and generated by π, then multiplication by π is an isomorphism on A'/A_0 and $d_M(n)$ is represented by a cocycle

$$\sigma \mapsto \frac{(\sigma - 1)P_n}{\pi^M}.$$

Since this cocycle is valued in A'/A_0 and the class $d_M(n)$ is killed by π^M, this shows that $d_M(n)_v$ vanishes. Alternatively, if v is not principal, then p does not divide the index $[A : A_0]$. As the order of $d_M(n)$ is a power of p, its restriction to $H^1(K_v^{\mathrm{ur}}/K_v, A/A_0)$ vanishes.

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

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

As Q_n is defined over K_n, the first term of this expression is determined solely by its restriction to $\mathrm{Gal}(K_n/K)$. As a cocycle over K_λ it is therefore determined uniquely by its action on the decomposition group of λ in K_n. But as λ splits completely, its decompostion 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 5.5 (Kolyvagin 2007, Theorem 3)**.** Let $l \in S_1(M)$, with extension λ in K. There exists a homomorphism

$$\chi_l : A(K_\lambda) \to H^1(K_\lambda, A_{\mathfrak{p}^M})$$

such that

1. for all $m \in S(M)$ coprime to l we have

$$c_M(ml)_\lambda = \chi_l(P_m),$$

2. $\ker \chi_l = \mathfrak{p}^M A(K_\lambda)$ and

$$\chi_l(A(K_\lambda)/\mathfrak{p}^M A(K_\lambda)^{\pm}) \subset H^1(K_\lambda, A_{\mathfrak{p}^M})^{\mp},$$

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

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

Proof. Let $l \in S_1(M)$, with extension λ in K and fix an extension $\overline{\lambda} \in \overline{K}$. Recall that $\mathbb{F}_\lambda$ has degree 2 over $\mathbb{F}_l$. In particular, $\text{Frob}(l)^2 = 1$ in $\text{End}(A(\mathbb{F}_\lambda))$. Consequently it follows that

$$a_l - (l+1)\text{Frob}(l) = -\text{Frob}(l)(\text{Frob}(l)^2 - a_l \text{Frob}(l) + l). \tag{5.5}$$

As this is divisible by the characteristical polynomial of $\text{Frob}(l)$, this endomorphism must vanish on $A(\mathbb{F}_\lambda)$. Notice that λ splits completely in $K(A_{\mathfrak{p}^M})$ as l has degree two in the extension $K(A_{\mathfrak{p}^M})/\mathbb{Q}$. 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 $A(\mathbb{F}_{\bar{\lambda}})$ and since the expression in (5.5) vanishes, there exists a unique $\tilde{T}_P \in A_{p^M}$ such that

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

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_l. As λ is principal in K it splits completely in K_1, and hence $K_{\lambda_1} = K_\lambda$. In particular, the extension K_{λ_l}/K_λ is totally ramified with cyclic Galois

group generated by σ_l. Given P as above, define $\chi_l(P)$ to be the inflation of the unique cocycle on $\mathrm{Gal}(K_{\lambda_l}/K_\lambda)$ 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 $n = ml \in S(M)$, let λ_n be the restriction of $\overline{\lambda}$ to K_n, and let λ_m be its restriction to K_m. As λ splits completely in K_m, it follows that $K_{\lambda_m} = K_\lambda$ and that $K_{\lambda_n} = K_{\lambda_l}$. We claim that $P_n \in p^M A(K_{\lambda_n})$. As the extension K_{λ_n}/K_λ is totally ramified and generated by σ_l, this automorphism acts trivially on $\mathbb{F}_{\lambda_n}$, hence D_l acts on $A(\mathbb{F}_{\lambda_n})$ as $l(l+1)/2$. As $\mathfrak{p}^M$ divides $l+1$, so does p^M and it follows that $P_n \in p^M A(\mathbb{F}_{\lambda_n})$. In particular there exists a $Q \in A(K_{\lambda_n})$ such that $p^M Q \equiv P_n \mod \lambda_n$, and therefore $p^M Q - P_n \in A_1(K_{\lambda_n})$. Here A_1 denotes the kernel of the reduction map to the residue field. This group is naturally isomorphic to $\hat{A}(\lambda_n)$, the formal group associated to A over the maximal ideal of K_{λ_n}. As p is coprime to l, multiplication by p is an isomorphism on this group, and hence on $A_1(K_{\lambda_n})$ as well. It follows that $p^M Q - P_n \in p^M A(K_{\lambda_n})$, and thus that $P_n \in p^M A(K_{\lambda_n})$ proving the claim.

Consider the p^M-torsion point

$$-\frac{(\sigma_l - 1)P_n}{p^M} + \sigma_l \frac{P_n}{p^M} - \frac{P_n}{p^M} \in A(K_{\lambda_n}). \tag{5.6}$$

The extension K_{λ_n}/K_λ is totally ramified, hence σ_l acts trivially on $A(\mathbb{F}_{\lambda_n})$. The reduction of ths point modulo $\overline{\lambda}$ is therefore congruent to $-\frac{(\sigma_l-1)P_n}{p^M}$. Recall from (5.2) and Gross 1991, Proposition 3.7.1 that

$$a_l D_m y_m - (l+1) D_m y_n = -(\sigma_l - 1) \cdot D_n y_n.$$

Applying the second part of the same proposition shows that

$$\frac{a_l - (l+1)\mathrm{Frob}(l)}{p^M} P_m \equiv -\frac{(\sigma_l - 1)P_n}{p^M} \mod \overline{\lambda},$$

This shows that $\chi_l(P_m)$ is defined to be the inflation of the cocycle determined by

$$\sigma_l \mapsto \left(-\frac{(\sigma_l - 1)P_n}{p^M} + \sigma \frac{P_n}{p^M} - \frac{P_n}{p^M} \right)_{\mathfrak{p}^M}.$$

Recall that $c_M(n)$ is represented by

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

where Q_n is any point as in Lemma 5.3. As $P_n \in p^M A(K_{\lambda_n})$ so is Q_n. Hence this cocycle vanishes when restricted to $H^1(K_{\lambda_n}, A_{\mathfrak{p}^M})$. The class $c_M(n)$ and is therefore inflated from a class in $H^1(K_{\lambda_n}/K_\lambda, A_{\mathfrak{p}^M})$. In particular, using the same cocycle as representative, we see that the class $c_M(n)_\lambda$ is defined uniquely by

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

But as this $\mathfrak{p}^M$-torsion point is precisely the $\mathfrak{p}^M$-component (5.6), we conclude that $\chi_l(P_m) = c_M(ml)_\lambda$.

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

$$\chi_l(\tau P)^\tau_{\sigma_l} = -\chi_l(P)_{\sigma_l}.$$

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 $-\tau\chi_l(\tau P)_{\sigma_l}$. Since the natural action of τ coincides with the action of $\mathrm{Frob}(l)$, on $\mathbb{F}_\lambda$, it follows that $\tau T_P = T_{\tau P}$. But as $\chi_l(P)_{\sigma_l} = T_P$, 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 $\mathrm{im}\ \chi_l \cap \mathrm{im}\ \delta_\lambda = 0$. 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_m maps to $d_M(ml)_\lambda$ via $c_M(ml)_\lambda$ hence they must all have the same order, (here P_m is viewed as an element of $A(K_\lambda)/\mathfrak{p}^M A(K_\lambda)$). By Lemma 5.4 this order is equal to $\mathrm{ord}\ c_M(m)_\lambda$. □

Theorem 5.5 allows us to relate the classes $c_M(n)$ with the classes of the divisors of n. In particular, for any $m, l \in S(M)$ such that $(m, l) = 1$ define

$$\mathrm{ord}_\mathfrak{p}(P_m)_\lambda = \max\{M : P_m \in \mathfrak{p}^M A(K_\lambda)\}.$$

Notice that this definition is sound as it is indeed possible to inject K_m into K_λ whenever $l \nmid m$. This enables us to formulate several useful consequences of Theorem 5.5.

Corollary 5.5.1. Let $n \in S(M)$. The following statements hold.

1. For all primes $l \mid n$ we have

$$\mathrm{ord}_\mathfrak{p}(P_n) \leq \mathrm{ord}_\mathfrak{p}(P_{n/l})_\lambda,$$

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

$$\text{if } P_{n/l} \notin \mathfrak{p}^M A(K_\lambda), \text{ then } P_n \notin \mathfrak{p}^M A(K_n).$$

2. For any $M > 0$

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

3. If $n \in S_r(M_{r-1})$, then

$$d_{M_{r-1}}(n) \in Ш(A/K).$$

Proof. The second part of the first statement is a direct consequence of the first. Whenever $M \geq \mathrm{ord}_{\mathfrak{p}}(P_{n/l})_\lambda$, the order of $P_{n/l}$ in $A(K_\lambda)/\mathfrak{p}^M A(K_\lambda)$ is naturally given by $p^{M-\mathrm{ord}_{\mathfrak{p}}(P_{n/l})_\lambda}$. By Theorem 5.5 this order is equal to ord $c_M(n)_\lambda$. Hence

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

which proves the first statement. By Lemma 5.4, $d_M(n)$ vanishes at all valuations prime to n. For the valuations dividing n, we have

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

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

In light of Corollary 5.5.1 we can prove a notable property of the M_r defined earlier.

Corollary 5.5.2. Assume that y_K has infinite order in $A(K)$.
Then $M_0 = \mathrm{ord}_{\mathfrak{p}}[A(K) : \mathcal{O}_A y_K]$ 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 Howard 2004, Theorem A, $\mathcal{O}_A y_K$ is of finite index in $A(K)$. Since $S_0 = \{1\}$ and $P_1 = y_K$, we have

$$M_0 = \mathrm{ord}_{\mathfrak{p}}(y_K) = \max\{M : y_K \in \mathfrak{p}^M A(K_1)\}.$$

Simultaneously

$$\mathrm{ord}_{\mathfrak{p}}[A(K) : \mathcal{O}_A y_K] = \max\{M : y_K \in \mathfrak{p}^M A(K)\}.$$

And 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 $m \in S_r(M)$. By Corollary 4.3.1, there exists a prime $l \nmid m$ such that $l \in S_1(M)$ and ord $c_M(m)_\lambda =$ ord $c_M(m)$. In particular, this implies that

$$\mathrm{ord}_{\mathfrak{p}}(P_m) = \mathrm{ord}_{\mathfrak{p}}(P_m)_\lambda \geq \mathrm{ord}_{\mathfrak{p}}(P_{ml})$$

by Corollary 5.5.1. Hence for any $m \in S_r(M)$, there exists an $n \in S_{r+1}(M)$ such that $\mathrm{ord}_{\mathfrak{p}}(P_m) \geq \mathrm{ord}_{\mathfrak{p}}(P_n)$. Which conludes the proof. □

Corollary 5.5.2 allows the formulation of the following simple but important consequence of Theorem 5.5.

Proposition 5.6 (McCallum 1991)**.** Let M and M' be two positive integers. Let $n \in S(M+M')$ and $n' \in S(M')$ be two integers such that $d_M(n), d_{M'}(n') \in Ш(A/K)$. Then the Cassels pairing is given by

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

Proof. Recall the construction of the Cassels pairing in Chapter 2. Indeed $d_{M+M'}(n)$ is a suitable choice for d_1 as $p^{M'} d_{M+M'}(n) = d_M(n)$. By Lemma 5.4, it vanishes for all valuations v prime to n. Hence this sum can be restricted to the primes dividing n. By the same lemma, $P_{n'}$ is a suitable choice for those y_λ, for each of those $l \nmid n'$. If $l \mid n'$, then $d_{M'}(n')_\lambda = 0$ as it is contained in $Ш(A/K)$. Hence by Theorem 5.5, $c_{M'}(n')_\lambda = 0$, and hence there is no contribution to the pairing for this prime. Summing up the remaining terms gives the desired conclusion. □

Chapter 6

Structure of the Shafarevich-Tate group

In this final chapter we generalize McCallum's result for modular elliptic curves to modular abelian varieties arising from weight 2 newforms (Theorem 6.3). Throughout this chapter, $\mathfrak{p}$ is a prime of $\mathcal{O}_A$ satisfying the properties described in Chapters 4 and 5, and y_K is assumed to have infinite order in $A(K)$. In the first section, the Fricke involution (see Section 3.5), and its application to the Shafarevich-Tate group are briefly revisited. The second and final section combines the results from all previous chapters to formulate Theorem 6.3 as well as the provide the lemmas needed to proof it. The chapter concludes with the proof of this theorem, which provides an explicit structure of the $\mathfrak{p}$-primary part of the Shafarevich-Tate group in terms of the M_r introduced in the previous chapter.

6.1 An application of the Fricke involution

Let f be the newform associated to A, and let $\epsilon = \pm 1$ be its eigenvalue under the Fricke involution. For a positive integer r, define $\epsilon_r = (-1)^r \epsilon$.

Lemma 6.1 (Gross 1991)**.** For all integers $n \in S_r(M)$, there exists a $\sigma \in \mathcal{G}_n = \mathrm{Gal}(K_n/K)$ such that

$$\tau y_n = \epsilon \cdot \sigma y_n + Q,$$

for some $\mathbb{Q}$-rational torsion point Q. In particular, P_n is contained in the ϵ_r-eigenspace of $(A(K_n)/\mathfrak{p}^M A(K_n))^{\mathcal{G}_n}$.

Proof. On $X_0(N)$ we have the identity

$$\tau x_n = w_N(\sigma x_n)$$

for some $\sigma \in \mathcal{G}_n$ (see Gross 1984, Section 5). Hence on $J_0(N)$ we have

$$\tau((x_n) - (\infty)) = w_N((\sigma x_n) - (\infty)) + (w_N\infty) - (\infty).$$

Observe that $w_N\infty$ is the cusp 0 on $X_0(N)$ and that the class of $(0 - \infty)$ is torsion on the Jacobian. Hence after applying α_f, we obtain $\tau y_n = \alpha_f((w_N \circ \sigma)(x_n - \infty)) + Q$, on A. But as w_N acts as ϵ on f, we obtain the desired conclusion.

To prove the second statement, recall that $P_n = \sum \sigma' D_n y_n$, where $D_n = \prod_{l|n} D_l$ and $D_l \in \mathbb{Z}[G_l]$ is an element satisfying

$$(\sigma_l - 1)D_l = l + 1 - \mathrm{Tr}_l.$$

Notice that D_l is determined uniquely up to addition by multiples of Tr_l. As $l + 1 - \mathrm{Tr}_l$ is invariant under conjugation by τ, we find that

$$\begin{aligned}(\sigma_l - 1)D_l\tau &= \tau(\sigma_l - 1)D_l \\ &= (\sigma_l^{-1} - 1)\tau D_l \\ &= (\sigma_l - 1)(-\sigma_l^{-1})\tau D_l\end{aligned}$$

Hence $D_l\tau + \sigma_l^{-1}\tau D_l$ vanishes under $(\sigma_l - 1)$ and is therefore a multiple of Tr_l. Applying τ to P_n yields

$$\begin{aligned}\tau P_n &= \sum_{\sigma' \in S} \tau\sigma' D_n y_n \\ &= \sum_{\sigma' \in S} \sigma'^{-1}\tau \prod_{l|n} D_l y_n \\ &= \sum_{\sigma' \in S} \sigma'^{-1} \prod_{l|n} \left(-\sigma_l D_l(\tau y_n) + k_l \mathrm{Tr}_l y_n\right)\end{aligned}$$

Recall that $\mathrm{Tr}_l y_n = a_l y_m$ and that a_l vanishes modulo $\mathfrak{p}^M$. Hence modulo $\mathfrak{p}^M A(K_n)$ we obtain

$$\begin{aligned}\tau P_n &= (-1)^r \sum_{\sigma' \in S} \sigma'^{-1} \prod_{l|n} \sigma_l \prod_{l|n} D_l \tau y_n \\ &= (-1)^r \prod_{l|n} \sigma_l \sum_{\sigma' \in S} \sigma'^{-1} \prod_{l|n} D_l \tau y_n\end{aligned}$$

By the first statement of the lemma, τy_n is equal to $\epsilon \cdot \sigma y_n + Q$, for some $\mathbb{Q}$-rational torsion point Q. By Proposition 5.2 $A_p(\mathbb{Q}) = 0$, hence Q vanishes when restricted to $\mathfrak{p}^M A(K_n)$. Observe that $\{\sigma'^{-1} \mid \sigma' \in S\}$ is another set of representatives of G_n, and as P_n is defined independent of the choice of representatives, it follows that

$$\tau P_n = (-1)^r \epsilon \prod_{l|n} \sigma_l \sigma P_n \text{ modulo } p^M A(K_n).$$

Finally since the class of P_n is $\mathcal{G}_n$-invariant we conclude that $\tau P_n = \epsilon_r P_n$. □

The Fricke involution plays an integral role in analyzing the structure of the Shafarevich-Tate group; Lemma 6.1 shows that it determines the eigenvalues of the Heegner points, which in turn determine the eigenvalues of $c_M(n)$ and $d_M(n)$. Apart from this it also imposes conditions on the groups the groups $A(K)/\mathfrak{p}^M A(K)$. This is ilustrated in the following Lemma.

Lemma 6.2. 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 k. For any integer M, $y_K = P_1$ is contained in the ϵ-eigenspace of $A(K)/\mathfrak{p}^M A(K)$ by Lemma 6.1. The decomposition into eigenspaces

$$A(K)/\mathfrak{p}^M A(K) \cong \Big(A(K)/\mathfrak{p}^M A(K)\Big)^{\epsilon} \oplus \Big(A(K)/\mathfrak{p}^M A(K)\Big)^{-\epsilon},$$

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 5.2, it follows that $A(K)/\mathfrak{p}^M A(K)^{-\epsilon} = 0$. Consequently $A(K)^{-\epsilon} \otimes F_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}}$ vanishes and thus we obtain the desired isomorphism by the $\mathfrak{p}^\infty$-descent sequence (1.5). □

6.2 The Structure Theorem

As the Shafarevich-Tate group is finite, 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 2.3 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 $D^{-\epsilon} = D_1 \times D_3 \times \cdots$ where D_i is a cyclic $\mathcal{O}_A/\mathfrak{p}^{N_i}$-module. Analgously, D^{ϵ} admits a decomposition $D^{\epsilon} = D_2 \times D_4 \times \cdots$. As 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 isotropoic subgroup $D = D_1 \times D_2 \times D_3 \times \cdots$ such that the exact sequence

$$0 \to D \to Ш(A/K)_{\mathfrak{p}^\infty} \to D^* \to 0 \tag{6.1}$$

is split. The rest of this thesis will be dedicated to proving the following relation between the N_r and the earlier defined M_r.

Theorem 6.3. Assume that y_K has infinite order. Then

$$N_r = M_{r-1} - M_r \tag{6.2}$$

for all $r \geq 1$.

Before proving Theorem 6.3 we mention a few direct corollaries.

Corollary 6.3.1. 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 increments $M_r - M_{r+1}$ decrease if we increase r by 2, there need not be the case if we increase r by 1. Additionally, Theorem 6.3 allows us to give an explicit description of the p-torsion order of the Shafarevich-Tate group.

Corollary 6.3.2. Let $m = \min\{M_r, r \geq 0\}$. Then

$$\mathrm{ord}_{\mathfrak{p}}|Ш(A/K)| = 2(M_0 - m).$$

In order to prove Theorem 6.3 several lemmas are needed.

Lemma 6.4. Let $l \in S_1(M)$ be a prime number, then im χ_l is a maximal isotropic subgroup of $H^1(K_\lambda, A_{\mathfrak{p}^M})$.

Proof. Let $x, y \in$ im χ_l. Recall from the proof of Theorem 5.5 that x and y are inflated from cocycles in $H^1(\langle\sigma_l\rangle, A_{\mathfrak{p}^M})$. As the Tate-pairing is a cup-product, it satisfies

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

As σ_l is totally ramified, its second cohomology group injects in the group $H^2(I, \mu_{\mathfrak{p}^M})$, where I is the inertia group of K_λ. But this group is trivial as $l \neq p$ (see Milne 2006a, Lemma 1.2.9). Hence $x \smile y = 0$. Maximality follows from the second statement of Theorem 5.5. □

Lemma 6.5. Let $l \in S_1(M)$ and let $S \subset S_1(M)$ 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 $S \cup \{l\}$,
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 (Milne 2006a, 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 $H_{v_q} = \text{Im } \chi_q$. For all other places $v \in T \backslash \{l\}$, let $H_v = \delta(A(K_v))$. Notice that for all places $v \neq l$ 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

$$\bigoplus_{v \in T \backslash \{l\}} \frac{H^1(K_v, A_{\mathfrak{p}^M})^{\pm}}{H_v^{\pm}}.$$

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 Milne 2006a, Proposition 3.8 that $H^1(K_v^{\text{ur}}/K_v, A) = 0$. Consequently, the map $\delta_v : A(K_v) \to H^1(K_v^{\text{ur}}/K_v, A_{\mathfrak{p}^M})$ is surjective. □

The strategy for proving Theorem 6.3 is the following: Let r be an integer and assume $M_{r-1} > M_r$. Let $n \in S_r(M_{r-1})$, Corollary 5.5.1 imposes that $d_{M_{r-1}}(n) \in Ш(A/K)$. As $\text{ord}_{\mathfrak{p}}(P_n) \geq M_r$, it follows from (5.4) that the order of $d_{M_{r-1}}(n)$ is at most $p^{M_{r-1}-M_r}$. For properly chosen n_r, it will be shown that $d_{M_{r-1}}(n_r)$ attains this order. Proceeding inductively, and choosing the n_r independent of $n_s, s \leq r$, we will show that $N_r = M_{r-1} - M_r$ which will complete the proof. In order to guarantee the independence of the n_r, we need the following proposition.

Proposition 6.6 (McCallum 1991)**.** 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 $n \in S_r(M)$ such that ord $c_M(n) = p^{M-M_r}$ and $\langle c_M(n) \rangle \cap C = \{0\}$.

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

$$p^M \geq \max\{\text{exponent of } C, p^{M_{r-1}}\}.$$

Let $n \in S_r(M_r+1)$ be an integer such that $\mathrm{ord}_{\mathfrak{p}}(P_n) = M_r$, and let $L = K(A_{\mathfrak{p}^M})$. Recall from Chapter 4 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 n. For every $l \in S$, fix an extension λ_L in L. Let $X \subset C^*$ denote the submodule generated by the characters of all $l \in S \cap S(M)$, 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 $S \cap S(M) \backslash \{l_0\}$ generate the image of X, and we can choose a $\psi \in C^*$ such that

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

If $c_{M_r+1}(n) \in C$, we can impose the additional condition that $\psi(c_{M_r+1}(n)) \neq 0$, 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 6.5, we choose a $c \in H^1(K, A_{\mathfrak{p}})^{-\epsilon_r}$ such that

$$\begin{aligned} &c \neq 0, \\ &c_v \in \delta_v(A(K_v)), && \text{for all } v \notin S, \\ &c_\lambda \in \text{im } \chi_l, . && \text{for all } l \in S \backslash \{l_0\} \end{aligned} \tag{6.3}$$

Let $\langle C, c_{M_r+1}(n) \rangle$ denote the subgroup of $H^1(K, A_{\mathfrak{p}^M})$ generated by C and $c_{M_r+1}(n)$. 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 $\phi \in \langle C, c_{M_r+1}(n), c \rangle^*$ such that

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

By Proposition 4.3, there exists an $l' \in S_1(M)$ such that $\phi = \phi_{\mathrm{Frob}(\lambda'_L)}$, and hence that $\psi = \psi_{\mathrm{Frob}(\lambda'_L)}$. Moreover, observe that the sum

$$\sum_v c_{M_r+1}(nl')_v \smile c_v.$$

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 5.4 that $c_{M_r+1}(nl')_v \in \delta_v(A(K_v))$. Equation (6.3) 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 $l \in S \backslash \{l_0\}$, it follows from Theorem 5.5 that $c_{M_r+1}(nl')_\lambda = \chi_l(P_{nl'/l})$. By construction c_λ is contained in im χ_l 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

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

For λ', it follows from (2.4) and (6.3) that

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

for some $x \in A(K_{\lambda'})$. Theorem 5.5 gives the equality

$$\text{ord } d_{M_r+1}(nl')_{\lambda'} = \text{ord } c_{M_r+1}(nl')_{\lambda'} = \text{ord } c_{M_r+1}(n)_{\lambda'}.$$

The choice of ϕ, now guarantees that this cocycle is non-zero by (4.1), and since $\text{ord}_{\mathfrak{p}}(P_n) = M_r$, (5.4) shows that ord $c_{M_r+1}(n) = p$, and hence that $d_{M_r+1}(nl') \in H^1(K, A)_{\mathfrak{p}}^{-\epsilon_r}$. By the choice of c, $c_{\lambda'}$ has order at most p, and as $\phi(c) = \phi_{\text{Frob}(\lambda'_L)}(c) \neq 0$, 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

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

It follows that $c_{M_r+1}(nl')_{\lambda_0} \neq 0$, and by Theorem 5.5 that $P_{nl'/l_0} \notin \mathfrak{p}^{M_r+1}A(K_{\lambda_0})$. By the definition of M_r we must therefore have that $\text{ord}_{\mathfrak{p}}(P_{nl'/l_0}) = M_r$. Thus by replacing n with $n' = nl'/n_0$, 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 $S \subset S_1(M)$, hence $c_M(n)$ exists and has order p^{M-M_r}. Observe that

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

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

$$\text{ord } c_{M_{r-1}}(n)_\lambda = \text{ord } c_{M_{r-1}}(n/l)_\lambda = 1$$

for all $l \in S$. Hence

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

Since $c_{M_{r-1}}(n)$ is a multiple of $c_M(n)$ of order $p^{M_{r-1}-M_r}$, the statement is proved if $M_{r-1} > M_r$. 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 $m \in S_{r-1}(M)$ such that ord $c_M(m) = p^{M-M_{r-1}}$. By Proposition 4.3, there exists an $l \in S_1(M)$ such that $c_{M_r+1}(m)_\lambda \neq 0$. By Theorem 5.5, we hence have that $d_{M_r+1}(ml)_\lambda \neq 0$.

In particular this means that $d_{M_r+1}(ml) \notin Ш(A/K)$ and hence $c_{M_r+1}(ml) \notin S_{\mathfrak{p}^\infty}(A/K)$. As C is contained in this group, we conclude

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

and thus the proposition is proved. □

In the process of proving Proposition 6.6, the following weaker statement has been proven as well.

Corollary 6.6.1. Let r be a square-free integer and let $M' \geq M$ be two integers such that $M \geq M_r$. Then for all $n \in S_r(M)$, there exists an $n' \in S_r(M')$ such that ord $c_{M'}(n') \geq$ ord $c_M(n)$.

Using this, let r be an odd number and let $n \in S_r(M_{r-1})$ be such that $c_{M_{r-1}}(n)$ has order $p^{M_{r-1}-M_r}$. By Corollary 5.5.1 we have that $d_{M_{r-1}}(n) \in Ш(A/K)^{-\epsilon}_{\mathfrak{p}^\infty}$, and hence that $c_{M_{r-1}}(n) \in S_{p^\infty}(A/K)$. By Lemma 6.2 $d_{M_{r-1}}(n)$ has order $p^{M_{r-1}-M_r}$ in this group. As the Cassels-pairing is alternating on the $\mathfrak{p}$-primary part, we conclude that $Ш(A/K)^{-\epsilon}_{p^\infty}$ 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 6.6 that $c_{M_{r-1}}$ is chosen independent of $\{c_{M_{2k}}, \tilde{c}_{M_{2k}} \mid k < m\}$, it follows that $Ш(A/K)^{-\epsilon}_{p^\infty}$ 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 6.3. We proceed by induction on r. By applying Proposition 6.6 to $C = \{0\}$ and $r = 1$, it is shown above that there exists an $l \in S_1(M_0 - M_1)$ such that $d_{M_0-M_1}(l) \in Ш(A/K)^{-\epsilon}_{\mathfrak{p}^\infty}$ 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 (1.5) 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 4.3.1, there exists a prime number l_1 such that

$$\begin{aligned} \text{ord } c_{M_0+N_1}(1)_{\lambda_1} &= p^{N_1}, \\ \text{ord } c_{1,\lambda_1} &= p^{N_1}, \\ c_{i,\lambda_1} &= 0, \text{ for all } i \geq 2. \end{aligned} \tag{6.4}$$

The first condition of Corollary 4.3.1 is equivalent to the property that $l_1 \in S_1(M_0+N_1)$. Therefore by Corollary 5.5.1, it follows that $d_{M_0}(l_1) \in Ш(A/K)$. Thus for all i and for any $0 \leq M \leq N_i - 1$ we have that

$$\langle d_{M_0}(l_1), p^M d_i \rangle = \langle d_{M_0-M}(l_1), d_i \rangle = \langle d_{M_0-M+N_i}(l_1)_{\lambda_1}, y_{i,\lambda_1} \rangle_{\lambda_1}, \tag{6.5}$$

To see that the last equality holds, observe that $d_{M_0-M+N_i}(l_1)$ satisfies the properties of d_1 in the definition of the Cassels-Tate pairing. Moreover, all other terms in this sum vanish by Lemma 5.4. By (2.4) 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 5.5 ord $d_{M_0+N_1-M}(l_1)_{\lambda_1} =$ 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 (6.5) is non-trivial for all $0 \leq M \leq N_1 - 1$. We conclude that the character

$$\mathcal{X}_1 : \ d \mapsto \langle d_{M_0}(l_1), d \rangle \in D^*$$

vanishes on $D_2 \times D_3 \times \cdots$. Observe that this character is the image of $d_{M_0}(l_1)$ in D^* under the map in (6.1). 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 $d_{M_0}(l_1)$ 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 for all $1 \leq j < r$ that $N_j = M_{j-1} - M_j$. Moreover assume that there exist $l_1, ..., l_{r-1} \in S_1(M')$ such that

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

and that the characters

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

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 $n_j = \prod_{i \leq j} l_i$, 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

$$C = \langle \delta(h_1), \delta(h_2), c_1, ..., c_{r-1}, c_{M_0}(n_1), ..., c_{M_{r-2}}(n_{r-1}) \rangle^{\epsilon_k}.$$

This module is generated by at most r independent elements. Using Proposition 6.6, choose any $n \in S_r(M')$ such that ord $c_{M_{r-1}}(n) = p^{M_{r-1}-M_r}$ and $C \cap \langle c_{M_{r-1}}(n) \rangle = 0$. Assume that ord $d_{M_{r-1}}(n) > N_r$. As the sequence in (6.1) splits, we observe that $d_{M_{r-1}}(n)$

is contained in the submodule generated by $d_1, ..., d_{r-1}, d_{M_0}(n_1), ..., d_{M_{r-2}}(n_{r-1})$. Let c denote the lift of $d_{M_{r-1}}(n)$ to $S_{\mathfrak{p}^\infty}(A/K)$. If r is odd, the lift is unique and must therefore equal $c_{M_{r-1}}(n)$, which gives a contradiction as the lift is contained in C. Otherwise, $c_{M_{r-1}}(n) - c$ is contained in the image of $A(K)^\epsilon \otimes F_\mathfrak{p}/\mathcal{O}_\mathfrak{p}$. After multplying by a power of p if necessary, one can assume that $c_{M_{r-1}}(n) - c \in \delta(A(K)/\mathfrak{p}^{M'}A(K))$. As this module is generated by $\delta(h_1)$ and $\delta(h_2)$, we conclude that $c_{M_{r-1}}(n) \in C$. This gives a contradiction, hence ord $d_{M_{r-1}}(n) \leq N_r$. Notice that multiplying $c_{M_{r-1}}(n)$ with the order of $d_{M_{r-1}}(n)$ gives an element in $\langle \delta(h_1), \delta(h_2) \rangle$. By construction this must be 0, hence $c_{M_{r-1}}(n)$ has the same order as $d_{M_{r-1}}(n)$ and therefore

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

Conversely, by Corollary 4.3.1 there exists a prime number $l_r \in S_1(M')$ such that

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

Letting $n_r = l_r n_{r-1}$ and $0 \leq M \leq N_i - 1$, we observe

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

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

$$\begin{aligned} \text{ord } d_{M_{r-1}+N_r-M}(n_r)_{\lambda_r} &= \text{ord } c_{M_{r-1}+N_r-M}(n_r)_{\lambda_r} \\ &= \text{ord } c_{M_{r-1}+N_r-M}(n_{r-1})_{\lambda_r} \\ &= p^{N_r-M} > 1. \end{aligned}$$

Hence by the non-degeneracy of the Tate pairing described in Proposition 2.4, we conclude that this pairing is non-trivial for $i = r$ and all $0 \leq M \leq N_r - 1$. Therefore the character

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

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 $d_{M_{r-1}}(n_r)$ we conclude that $d_{M_{r-1}}(n_r)$ 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

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

□

Bibliography

Conrad, Brian (Aug. 2005). "Abelian varieties: geometry, parameter spaces, and arithmetic". In: *Mathematics Subject Classification. Primary 14G22; Secondary 14H52*.

Davydov, Alexei (2007). "Twisted automorphisms of group algebras". In: arXiv: `0708.2758 [math.RT]`.

Diamond, Fred and Jerry Michael Shurman (2005). *A first course in modular forms*. Vol. 228. Springer Science & Business Media.

Gross, Benedict H. (1984). "Heegner points on $X_0(N)$". In: *Modular forms*, pp. 87–106.

– (1991). "Kolyvagin's work on modular elliptic curves". In: *L-functions and arithmetic (Durham, 1989)* 153, pp. 235–256.

Gross, Benedict H. and Don B. Zagier (1986). "Heegner points and derivatives ofL-series". In: *Inventiones mathematicae* 84.2, pp. 225–320.

Howard, Benjamin (2004). "Iwasawa theory of Heegner points on abelian varieties of GL_2-type". In: *Duke Mathematical Journal* 124.1, pp. 1–45.

Kolyvagin, Victor A. (2007). "Euler systems". In: *The Grothendieck Festschrift*. Springer, pp. 435–483.

Kolyvagin, Victor A. and Dmitry Yu Logachëv (1989). "Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties". In: *Algebra i Analiz* 1.5, pp. 171–196.

Longo, Matteo and Stefano Vigni (2013). "A refined Beilinson-Bloch conjecture for motives of modular forms". In: *arXiv preprint arXiv:1303.4335*.

McCallum, William G. (1991). "Kolyvagin's work on Shafarevich-Tate groups". In: *L-functions and arithmetic (Durham, 1989)* 153, pp. 295–316.

Milne, James S. (2006a). *Arithmetic Duality Theorems*. Second. BookSurge, LLC, pp. viii+339. ISBN: 1-4196-4274-X.

– (2006b). *Elliptic Curves*. BookSurgePublishers, pp. 238+viii. ISBN: 1-4196-5257-5.

– (2008). *Abelian Varieties (v2.00)*. Available at www.jmilne.org/math/.

Perret-Gentil, Corentin (2014). "Associating abelian varieties to weight-2 modular forms: the Eichler-Shimura construction". MA thesis. Ecole Polytechnique Fédérale de Lausanne.

Polishchuk, Alexander (2003). *Abelian varieties, theta functions and the Fourier transform*. Vol. 153. Cambridge University Press.

Poonen, Bjorn and Michael Stoll (1999). "The Cassels-Tate pairing on polarized abelian varieties". In: *Annals of Mathematics* 150.3, pp. 1109–1149.

Ribet, Kenneth A. (1992). "Abelian varieties over Q and modular forms". In: *arXiv preprint alg-geom/9208002*.

Ribet, Kenneth A. and William A. Stein (2011). "Lectures on modular forms and Hecke operators". URL: `http://wstein.%20org/books/ribet-stein/main.%20pdf`.

Silverman, Joseph H. (1994). *Advanced topics in the Arithmetic of Elliptic Curves*. Vol. 151. Springer Science & Business Media.

– (2009). *The arithmetic of elliptic curves*. second. Vol. 106. Springer Science & Business Media.