VISIBLE ELEMENTS OF THE SHAFAREVICH-TATE GROUP

A SENIOR THESIS OF

Dimitar P. Jetchev

THESIS ADVISOR: WILLIAM A. STEIN

SUBMITTED IN PARTIAL FULFILLMENT OF THE HONORS REQUIREMENTS
FOR THE DEGREE OF BACHELOR OF ARTS TO THE

DEPARTMENT OF MATHEMATICS
HARVARD UNIVERSITY

CAMBRIDGE, MASSACHUSETTS
APRIL 2004

To my parents and my grandparents

Table of Contents

Abstract

We study a subgroup of the Shafarevich-Tate group of an abelian variety known as the *visible subgroup*. We explain the geometric intuition behind this subgroup, prove its finiteness and describe several techniques for exhibiting visible elements. Two important results are proved - one what we call the *visualization theorem*, which asserts that every element of the Shafarevich-Tate group of an abelian variety becomes visible somewhere. Although the theorem is not original, the proof is original and is based on the explicit use of principal homogeneous spaces. The second result is the *visibility theorem*, stating that under certain conditions, one can inject a weak Mordell-Weil group into the Shafarevich-Tate group. Finally, we present two applications which provide evidence for the Birch and Swinnerton-Dyer conjecture - one example, in which the visibility theorem applies directly, and one, where visibility occurs only after raising the level of the modular Jacobian.

Acknowledgements

I would like to thank William A. Stein, my supervisor, for his enormous help, advising and enthusiasm on the whole thesis project and for the valuable comments on the draft. Many thanks to Barry Mazur and David Helm for the various discussions and comments.

I should also mention that the senior thesis project was partially funded by Harvard College Research Program.

Cambridge, Massachusetts Dimitar P. Jetchev
April 5, 2004

Introduction

In the 1960s, the British mathematicians Bryan Birch and Peter Swinnerton-Dyer stated several interesting conjectures about the arithmetic of the elliptic curves over $\mathbb{Q}$, after doing some computations at Cambridge University. Later on, John Tate formulated more functorial versions of these conjectures and generalized them to abelian varieties over $\mathbb{Q}$. The most famous version of the Birch and Swinnerton-Dyer conjecture is a relation between analytic and arithmetic invariants of an elliptic curve (more generally, abelian variety).

Conjecture 1 (Birch and Swinnerton-Dyer Conjecture). *Let E be an elliptic curve over $\mathbb{Q}$ of Mordell-Weil rank r and let $L(E,s)$ be the L-series, attached to the elliptic curve, then*

$$ord_{s=1}L(E,s) = r.$$

There is another version of the conjecture, which was described by John Tate in 1974 and is known as the full BSD conjecture. We will state the conjecture for abelian varieties over $\mathbb{Q}$, attached to newforms. The quantities that are included into the conjecture are the real volume Ω_A (or the canonical volume of $A(\mathbb{R})$, the Tamagawa numbers $c_{A,p}$, the order of the Shafarevich-Tate group $\text{Ш}(A/\mathbb{Q})$, the order of the torsion subgroups $A(\mathbb{Q})_{\text{tors}}$ and $A^\vee(\mathbb{Q})_{\text{tors}}$ and the order of vanishing of the L-function of A. All of the quantities will be discussed in more details later.

Let A be an abelian variety over $\mathbb{Q}$, which is attached to a newform $f = \sum_{n\geq 1} a_n q^n$ of level N and let $f^{(\sigma)} = \sum_{n\geq 1} a_n^\sigma q^n$ be the different Galois conjugates of f. We can define the L-function of the variety A as $L(A,s) := \prod_{\sigma: K_f \hookrightarrow \overline{\mathbb{Q}}} \left(\sum_{n\geq 1} \frac{a_n^\sigma}{n^s} \right)$.

Conjecture 2 (Full BSD Conjecture). *Assume that $L(A,s)$ does not vanish at $s = 1$. Then*

$$\frac{L^{(r)}(A,s)}{r! \cdot \Omega_A} = \frac{|\text{Ш}(A/K)| \cdot \prod_{p|N} c_{A,p} \cdot \text{Reg}_A}{|A(\mathbb{Q})_{\text{tors}}| \cdot |A^\vee(\mathbb{Q})_{\text{tors}}|}.$$

The above conjecture assumes that $\text{Ш}(A/\mathbb{Q})$ is finite. In fact, there is a close connection between the Birch and Swinnerton-Dyer conjecture, and the Tate-Shafarevich conjecture (according to which $Ш(A/K)$ is always finite for any abelian variety over a number field).

The main goal of this thesis is to introduce and study a subgroup of the Shafarevich-Tate group, known as the *visible subgroup* and to describe various techniques for producing visible elements of certain order, which in turn could provide evidence for Conjecture 2. We prove a theorem (the *visibility theorem*), which is due to William Stein and Amod Agashe, which exhibits embeddings of certain weak Mordell-Weil group into $Ш(A/K)$ for abelian varieties of rank zero under certain hypothesis. We prove a general statement, according to which every element of $Ш(A/K)$ can be visualized somewhere. The proof of this statement is original and was discovered by William Stein and the author. Finally, we present a technique for visualizing elements by raising the level of the modular Jacobian. This technique is based on a theorem of K. Ribet and can be applied for abelian varieties, for which the visibility theorem fails. We give a computational example to explicitely illustrate the technique.

This thesis project should in no case be considered to be a self-contained presentation, since such an exposition would have been beyond the volume of a senior thesis. As such, we assume basic familiarity with elliptic curves, Galois theory, Galois cohomology, theory of schemes. We also assume that the reader is familiar with the existence and the basic properties of Néron models of abelian varieties. We sometimes sketch the more technical proofs and constructions, omitting the details and refering the reader to more detailed references. We tried, however, to present all the important steps and ideas in the main results of the thesis (the visibility theorem, the visualization theorem, etc.). Some of the chapters (such as Chapter 1 and Chapter 3) require much less background than the others.

Chapter 1

Mordell-Weil Theorem, Shafarevich-Tate Group and Selmer Groups for Elliptic Curves.

We use the proof of the weak Mordell-Weil group as a motivation for introducing the Shafarevich-Tate group and the Selmer group of an elliptic curve. This approach allows us to present a more geometric interpretation of the two groups in terms of principal homogeneous spaces and their relation to Galois cohomology. These ideas are important for the computation of the full Mordell-Weil group $E(K)$, which is still an open problem. It follows from [23, VIII.3] and [23, Exer. 8.18] that by knowing generators for the group $E(K)/mE(K)$, we can obtain generators for $E(K)$ with a finite amount of computation. Thus, we will be interested only in computing the group $E(K)/mE(K)$.

We show how computing the weak Mordell-Weil group $E(K)/mE(K)$ reduces to determining whether there exists at least one rational point on certain homogeneous spaces. The last problem is a particular case of Hilbert's Tenth Problem about deciding the solvability of diophantine equations. In fact, the techniques allow us to describe an algorithm for computing $E(K)/mE(K)$ which terminates if one assumes the Tate-Shafarevich conjecture about the finiteness of $Ш(E/K)$. Finally, we prove that the ϕ-Selmer group for an arbitrary isogeny $\phi : E' \to E$ is always finite and explain how to compute that group.[1]

1.1 Weak Mordell-Weil Group and Kummer Pairing via Galois Cohomology

Suppose that E is an elliptic curve over a number field K and $m \geq 2$ is an integer, such that $E[m] \subseteq E(K)$. We define the weak Mordell-Weil group for E/K to be the

[1] We should make clear that we will not be concerned at all about the computational complexity of the algorithms, i.e. how difficult the computations are.

quotient group $E(K)/mE(K)$, where $E(K)$ is the group of K-rational points on E.

We start by defining a pairing

$$\kappa : E(K) \times \mathrm{Gal}(\overline{K}/K) \to E[m],$$

in the following way: for each $P \in E(K)$ choose $Q \in E(\overline{K})$, such that $[m]Q = P$ and let $\kappa(P, \sigma) := Q^\sigma - Q$.

First of all, this pairing is well-defined. To see this, suppose that Q' is another point, such that $[m]Q = [m]Q' = P$. We need to check that $Q'^\sigma - Q' = Q^\sigma - Q$. But $[m](Q' - Q) = 0$, i.e. $Q - Q' \in E[m] \subseteq E(K)$, which means that $Q' - Q$ is fixed by the action of $\mathrm{Gal}(\overline{K}/K)$. Hence, $(Q' - Q)^\sigma = Q' - Q$, or $Q'^\sigma - Q' = Q^\sigma - Q$. We often call the pairing κ the Kummer pairing.

The basic properties of κ are summarized in the following proposition:

Proposition 1.1.1. *The pairing κ is bilinear, with left kernel equal to $mE(K)$ and right kernel equal to $Gal(\overline{K}/L)$, where L is a field extension of K obtained by adjoining the coordinates of all points in $[m]^{-1}E(K)$ (or $L = K([m]^{-1}E(K))$). In particular, κ induces a perfect bilinear pairing*

$$E(K)/mE(K) \times Gal(L/K) \to E[m].$$

Proof. Bilinearity of κ is obvious from the definition. Suppose that $P \in E(K)$ is in the left kernel of κ. Choose $Q \in E(\overline{K})$, such that $[m]Q = P$. We will show that $Q \in E(K)$ and thus, it will follow that $P \in mE(K)$. But this is clear from the definition, since $\kappa(P, \sigma) = 0$ means precisely that Q is fixed by σ. Conversely, any $P \in mE(K)$ is in the left kernel of κ.

Let $\sigma \in \mathrm{Gal}(\overline{K}/K)(K)$ be in the right kernel. In this case it suffices to show that σ fixes the field extension L/K. Let $P \in E(K)$ and Q be a point, such that $[m]Q = P$. Then $\kappa(P, \sigma) = 0$ implies $Q^\sigma = Q$. Since this is true for any point in $[m]^{-1}E(K)$, then L is fixed by σ, i.e. $\sigma \in \mathrm{Gal}(\overline{K}/L)$. Conversely, any $\sigma \in \mathrm{Gal}(\overline{K}/L)$ is in the right kernel, because it fixes the points in $[m]^{-1}E(K)$.

We obtain the perfect bilinear pairing by moding out by the left and right kernels of κ. $\square$

Next, our goal is to describe the Kummer pairing in terms of Galois cohomology. To begin with, consider the short exact sequence of $\mathrm{Gal}(\overline{K}/K)$-modules for a fixed integer $m > 1$

$$0 \to E[m] \to E(\overline{K}) \xrightarrow{\cdot m} E(\overline{K}) \to 0.$$

This short exact sequence gives a long exact sequence on cohomology

$$\begin{aligned} 0 &\to H^0(\mathrm{Gal}(\overline{K}/K), E[m]) \to H^0(\mathrm{Gal}(\overline{K}/K), E(\overline{K})) \xrightarrow{\cdot m} H^0(\mathrm{Gal}(\overline{K}/K), E(\overline{K})) \\ &\xrightarrow{\delta} H^1(\mathrm{Gal}(\overline{K}/K), E[m]) \to H^1(\mathrm{Gal}(\overline{K}/K), E(\overline{K})) \xrightarrow{\cdot m} H^1(\mathrm{Gal}(\overline{K}/K), E(\overline{K})). \end{aligned}$$

But $H^0(G,M) = M^G$ for any group G and a G-module M, so we rewrite the above sequence as

$$\begin{aligned} 0 &\rightarrow E(K)[m] \rightarrow E(K) \xrightarrow{\cdot m} E(K) \xrightarrow{\delta} H^1(\mathrm{Gal}(\overline{K}/K), E[m]) \\ &\rightarrow H^1(\mathrm{Gal}(\overline{K}/K), E(\overline{K})) \xrightarrow{\cdot m} H^1(\mathrm{Gal}(\overline{K}/K), E(\overline{K})). \end{aligned}$$

Using the fact that $\ker(\delta) = mE(K)$, we obtain the following short exact sequence, known as the *Kummer sequence*:

$$0 \rightarrow E(K)/mE(K) \xrightarrow{\delta} H^1(\mathrm{Gal}(\overline{K}/K), E[m]) \rightarrow H^1(\mathrm{Gal}(\overline{K}/K), E(\overline{K}))[m] \rightarrow 0.$$

Since the left kernel of the pairing κ is $mE(K)$, then κ induces a homomorphism

$$\delta_E : E(K)/mE(K) \rightarrow \mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), E[m]).$$

It follows immediately that δ_E is precisely the connecting homomorphism δ for the above long exact sequence.

1.2 Properties of $L = K([m]^{-1}E(K))/K$

After introducing the Kummer pairing in the previous section, we will to study in a more detail the field extension $L = K([m]^{-1}E(K))$, which appeared in Proposition 1.1.1 in the previous section. The main result that we prove is that this extension is abelian and of exponent dividing m, which is unramified outside of a finite set of places ν. Then, using a general result from algebraic number theory, we will prove that L/K is a finite extension.[2]

The main properties of the field extension L/K are summarized in the following

Proposition 1.2.1. *(i) The field extension L/K is an abelian extension of exponent dividing m. In other words, the Galois group Gal(L/K) is abelian and every element has order dividing m.*
(ii) If S is the finite set of places at which E has bad reduction, together with the infinite places and the places ν, for which $\nu(m) \neq 0$, then L/K is unramified at each $\nu \notin S$.

The following lemma will be used in the proof of the proposition:

Lemma 1.2.2. *Suppose that ν is a discrete valuation, such that $\nu(m) = 0$ and E/K has good reduction at ν. Then the reduction map $E(K)[m] \rightarrow \tilde{E}_\nu(k_\nu)$ is injective.*

Proof. This is proved in [23, VII.3.1] by using formal groups. We will later on refer to a similar statement for abelian varieties. ∎

[2] Note that finite generatedness of $E(K)$ would immediately imply that L/K is finitely generated, because L would be an extension of K, obtained by adjoining finitely many elements. However, we cannot use this, because we are trying to prove finite generatedness for $E(K)$.

We are now ready to prove the proposition:

Proof of Proposition 1.2.1. (i) This is a consequence of proposition 1.1.1. Indeed, the map $\mathrm{Gal}(L/K) \to \mathrm{Hom}(E(K), E[m])$ defines an injection $\sigma \mapsto \kappa(\sigma, \cdot)$, so $\mathrm{Gal}(L/K)$ is abelian and the order of every elements of divides dividing m, since every homomorphism of $\mathrm{Hom}(E(K), E[m])$ has order dividing m.
(ii) Take a point $Q \in [m]^{-1}E(K)$ and let $P = [m]Q$. Consider the extension $L = K(Q)$ over K. It suffices to show that this extension is unramified at each $\nu \notin S$. Let ν' be an extension of ν in $K(Q)$ and $D_{\nu'/\nu}$ and $I_{\nu'/\nu}$ be the inertia and the decomposition groups, respectively. We will be done if we show that each element of $I_{\nu'/\nu}$ acts trivially on $K(Q)$. Indeed, every element of $I_{\nu'/\nu}$ acts trivially on $\tilde{E}_\nu(k'_{\nu'})$, where $k'_{\nu'}$ denote the reduction of $K(Q)$ at ν'. Therefore $(Q^\sigma - Q)^\sim = \tilde{Q}^\sigma - \tilde{Q} = \tilde{0}$ for all $\sigma \in I_{\nu'/\nu}$. But $Q^\sigma - Q \in E[m]$, because $Q \in [m]^{-1}E(K)$. Thus, lemma 1.2.2 implies that $Q^\sigma = Q$, so $I_{\nu'/\nu}$ acts trivially on $K(Q)/K$, which means that the field extension is unramified. This proves the proposition. □

So far, we concluded that L/K is an abelian extension of exponent dividing m which is unramified outside of a finite set of primes. It turns out that these properties are enough to deduce the finiteness of L/K. The next theorem establishes precisely this statement. In the proof, we use several results from algebraic number theory.

Theorem 1.2.3. *Let K be a number field, $m \geq 2$ be an integer, and S be a finite set of places, containing all infinite places in K and all finite places ν, such that $\nu(m) \neq 0$. Consider the maximal abelian extension L/K which has exponent dividing m and which is unramified at all places outside of S. Then L/K is a finite extension.*

Proof. If the proposition is true for a finite extension K'/K, then it is certainly true for K. Indeed, if L/K is the maximal abelian extension of exponent dividing m, which is unramified outside of the finite set S, then LK'/K' is a maximal abelian extension of exponent m, unramified outside of a set S' of extensions of the places in S to LK'. Therefore, LK'/K' is finite, and so L/K would also be finite. Thus, we can assume that K contains the m-th roots of unity μ_m.

We define *the ring of S-integers*

$$R_S = \{a \in K : \nu(a) \geq 0 \text{ for all } \nu \notin S\}.$$

Sine the class number of R_S is finite, we can add finitely many places to S, so that R_S becomes a Dedekind domain with class number 1 (i.e. a principal ideal domain). Making S bigger increases L and so we can assume that R_S is a principal ideal domain.

Next, we use another auxiliary result:

Lemma 1.2.4. *Let K be a number field (more generally, any field of characteristic 0), containing the m-th roots of unity μ_m. Then the maximal abelian extension of K of exponent m is obtained by adjoining m-th roots of the elements of K. In other words, $L = K(a^{1/m} : a \in K)$ is the maximal abelian extension of K of exponent m.*

Proof. Let L be an abelian extension of K of exponent dividing m and let $G = \mathrm{Gal}(L/K)$. Since G is abelian, then $G \cong G_1 \times \cdots \times G_k$, where the groups G_i are all cyclic. Let L_i/K be the fixed field of $G_1 \times \cdots \times \hat{G}_i \times \cdots \times G_n$. The Galois group of L_i/K is G_i, which is cyclic of order $m' \mid m$. The field K contains the primitive m'-th root of unity ε. Since $N_{L_i/K}(\varepsilon) = 1$, then by Hilbert Satz 90, $\varepsilon = \sigma(u_i)/u_i$ for some $u_i \in L_i$ (σ is a generator for the Galois group $\mathrm{Gal}(L_i/K)$). Next, $\sigma(u_i^n) = (\sigma(u_i))^n = (\varepsilon^{-1}u_i)^n = u_i^n$, so $u_i^n \in K$. Since $\sigma^i(u_i) = \varepsilon^{-i}u_i$, then the minimal polynomial of u_i has degree m', so $L_i = K(u_i)$, where $u_i^{m'} \in K$. Therefore, the maximal, abelian extension of K of exponent dividing m is

$$L = K(a^{1/m} : a \in K).$$

□

By lemma 1.2.4 and by the fact that $K([m]^{-1}K)/K$ is abelian, of exponent dividing m and unramified outside the finite set S, then $K([m]^{-1}K)/K$ is the largest subfield of $K(a^{1/m} : a \in K)$, which is unramified outside S.

Suppose that $\nu \notin S$. Then $a^{1/m} \in L$ for some $a \in K$ if and only if $K_\nu(a^{1/m})/K_\nu$ is unramified. But since $\nu(m) = 0$, then this condition is satisfied precisely when $\nu(a) \equiv 0 \pmod{m}$. Finally, we conclude that $L = K(a^{1/m} : a \in T_S)$, where

$$T_S = \{a \in K^*/K^{*m} : \nu(a) \equiv 0 (\mathrm{mod}\ m) \text{ for all } \nu \notin S\}$$

We will be done if we prove that T_S is finite. The idea is to consider the natural map $R_S^* \to T_S$. We claim that this map is surjective. Indeed, the valuations $\nu \notin S$ correspond precisely to the prime ideals of R_S. Thus, if $a \in K^*$ represents an element of T_S, then the ideal aR_S is the m-th power of an ideal of R_S (by the definition of T_S). Since R_S is a principal ideal domain, then $aR_S = b^m R_S$ for some $b \in K^*$. Hence, $a = ub^m$ for some $u \in R_S^*$. But then the images of a and u in T_S are the same and therefore the map $R_S^* \to T_S$ is surjective. Since its kernel contains $(R_S^*)^m$ then we obtain a surjective map $R_S^*/(R_S^*)^m \to T_S$. Finally, using Dirichlet's S-unit theorem [14, V §1], it follows that R_S^* is finitely generated and therefore $R_S^*/(R_S^*)^m$ is finite. Thus, T_S is finite and L/K is a finite extension. □

Thus, L/K is a finite extension, so using the perfect pairing $E(K)/mE(K) \times \mathrm{Gal}(L/K) \to E[m]$, we conclude that $E(K)/mE(K)$ is finite.

1.3 Computing the Weak Mordell-Weil Group and Principal Homogeneous Spaces

Recall that we assumed in the very beginning that $E[m] \subset E(K)$. This assumption implies that $\mu_m \subset K^*$. It follows from Hilbert 90 Satz that each homomorphism $\mathrm{Gal}(\overline{K}/K) \to \mu_m$ has the form $\sigma \mapsto \sigma(\beta)/\beta$ for some $\beta \in \overline{K}^*$ and $\beta^m \in K^*$. Therefore, we have an isomorphism $\delta_K : K^*/K^{*m} \to \mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), \mu_m)$.

The main idea for the computation of the weak Mordell-Weil group $E(K)/mE(K)$ is to use the homomorphisms δ_E (from section 1) and δ_K in order to construct a pairing

$$b : E(K)/mE(K) \times E[m] \to K^*/K^{*m},$$

which is computable.

For the construction of this pairing, we use the Weil pairing $e_m : E[m] \times E[m] \to \mu_m$, defined in [23, III.8]. Define

$$b(P, Q) = \delta_K^{-1}(e_m(\delta_E(P)(\cdot), Q)).$$

The pairing is well-defined, because δ_K is an isomorphism. It is also not hard to check that the pairing is bilinear and nondegenerate on the left. Indeed, if δ_K were degenerate on the left, then there would exist a point P, such that for all $Q \in E[m]$ and all $\sigma \in \mathrm{Gal}(\overline{K}/K)$, $e_m(\kappa(P, \sigma), Q) = 1$. Since the Weil pairing is nondegenerate, then $\kappa(P, \sigma) = 0$, which means that $P \in mE(K)$ by proposition 1.1.1.

The pairing b is easily computable as follows:

Proposition 1.3.1. *Let S be the finite set of places ν at which E has a bad reduction, the infinite places and the primes dividing m. Then the image of the pairing b lies in the subgroup*

$$K(S, m) = \{b \in K^*/K^{*m} : \nu(b) \equiv 0 (mod\ m)\ for\ all\ \nu \notin S\}$$

Moreover, for a point $Q \in E[m]$ if f_Q and g_Q are functions, satisfying $div(f_Q) = m(Q) - m(0)$ and $f_Q \circ [m] = g_Q^m$, then $b(P, Q) \equiv f_Q(P)(mod\ K^{*m})$ for $P \neq Q$. In the case $P = Q$ one can consider any point $P' \in E(K)$, such that $f_Q(-P') \neq 0$ and use bilinearity of the pairing to obtain $b(P, P) = f_Q(P + P')/f_Q(P')$.

Before presenting the proof, we will make the following

Remark 1.3.2. Proposition 1.3.1 is useful for computing the group $E(K)/mE(K)$ in the following way: suppose that one is able to recover the functions f_Q and g_Q from the equation of the curve. Next, take generating points Q_1 and Q_2 for $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. The idea is to consider the finitely many pairs $(b_1, b_2) \in K(S, m) \times K(S, m)$ and for each one to test whether we can solve the equations $b_1 z_1^m = f_{Q_1}(P)$ and $b_2 z_2^m = f_{Q_2}(P)$ and $P \in E(K)$ have a common solution $(P, z_1, z_2) \in K^2 \times K^{*2}$. Since the pairing b is nondegenerate on the left, then for a fixed pair (b_1, b_2), there is at most one possible P, such that there exists a solution (P, z_1, z_2) of the above system. Thus, one can recover this unique P from arbitrary K-rational point on the variety

$$b_1 z_1^m = f_{Q_1}(P),\ b_2 z_2^m = f_{Q_2}(P),\ P \in E(K),$$

so the question of computing the Mordell-Weil group reduces to determining whether or note each of finitely many varieties (each corresponding to a pair (b_1, b_2)) has a K-rational point. We call these auxiliary varieties *homogeneous spaces* for E/K. In that sense, the question of computing the group $E(K)/mE(K)$ is related to Hilbert's Tenth Problem of deciding the solvability of diophantine equations.

Proof of Proposition 1.3.1. Consider the element $\beta = b(P,Q)^{1/m}$ and the field extension $K(\beta)/K$. The proof of the first part is based on two observations. First, the element β is contained in the finite extension $L = K([m]^{-1}E(K))$, as defined in proposition 1.1.1. Since L/K is unramified outside of S by theorem 1.2.1, then $K(\beta)/K$ is unramified as well. But we get from algebraic number theory that $K(\beta/K)$ is unramified at ν if and only if $\nu(\beta^m) \equiv 0 \pmod{m}$. This proves that the image of b is contained in $K(S,m)$.

For the second part of the proposition, recall [23, III.8] that f_Q and g_Q are used for defining the Weil pairing. In other words, $e_m(P,Q) := \dfrac{g_Q(X+P)}{g_Q(X)}$ (the last fraction is the same for all X). Choose a point $P' \in E(\overline{K})$, such that $mP' = P$. Then by the definition of b and e_m for $X = P'$, we have

$$\frac{\beta^\sigma}{\beta} = e_m(P'^\sigma - P', Q) = \frac{g_Q(P'^\sigma)}{g_Q(P')} = \frac{g_Q(P')^\sigma}{g_Q(P')}.$$

By raising to the m-th power and using the fact that δ_K is an isomorphism, we conclude that $g_Q(P')^m \equiv \beta^m \pmod{K^{*m}}$. Hence, $f_Q(P) = f_Q(mP') = g_Q(P')^m \equiv b(P,Q) \pmod{K^{*m}}$, which completes the proof of the proposition. □

We should note at that point that there is a whole theory of principal homogeneous spaces and that they can be defined abstractly as varieties, equipped with a simple transitive action of the elliptic curve (or more generally, the abelian variety). For the later chapters, we assume that the reader is familiar with the basic theory. In fact, all we will need is that the equivalence classes of principal homogeneous spaces (or torsors) form a group (the Weil-Châtelet group $WC(E/K)$) and the elements of that group are in bijective correspondence with the cohomology group $H^1(\mathrm{Gal}(\overline{K}/K), E)$. The basic theory is presented in [23, X.3]

1.4 Applications and Complete 2-descent

Our discussion in the previous section will not be complete without an explicit example, for which we compute the weak Mordell-Weil group, using the described techniques. Since the main technical difficulties arise from the group law on the elliptic curve, derived out of the Weierstrass equation, we restrict ourselves to the case $m = 2$, which can be made explicit using the formulas for the group law on the elliptic curve, out of the Weierstrass equations.

First, take a Weierstrass equation for E of the form

$$y^2 = (x - e_1)(x - e_2)(x - e_3).$$

The 2-torsion point in E are 0 and $Q_i = (e_i, 0)$ for $i = 1, 2, 3$. The first step is to determine the functions f_{Q_i} and g_{Q_i}. In this case, the explicit formulas for the group law on the curve [23, III.2] makes this quite easy. We check that the function $f_{Q_i} = x - e_i$ satisfies $\operatorname{div}(f_{Q_i}) = 2(Q_i) - 2(0)$. Moreover,

$$x \circ [2] - e_i = \frac{(x^2 - 2e_i x - 2e_i^2 + 2(e_1 + e_2 + e_3)e_i - (e_1e_2 + e_1e_3 + e_2e_3))^2}{(2y)^2},$$

so we set $g_{Q_i} = \dfrac{(x^2 - 2e_i x - 2e_i^2 + 2(e_1 + e_2 + e_3)e_i - (e_1e_2 + e_1e_3 + e_2e_3))}{2y}$. Recall that knowing f_{Q_i} means knowing explicitely the equations for the principal homogeneous spaces.

Fix $(b_1, b_2) \in K(S, 2) \times K(S, 2)$. To check whether (b_1, b_2) is in the image of the pairing b means to check whether the system of equations

$$y^2 = (x - e_1)(x - e_2)(x - e_3) \tag{1}$$

$$b_1 z_1^2 = x - e_1 \tag{2}$$

and

$$b_2 z_2^2 = x - e_2 \tag{3}$$

has a solution $(x, y, z_1, z_2) \in K \times K \times K^* \times K^*$ (we are using the fact that Q_1 and Q_2 are generators for $E[2]$). By substituting (2) and (3) into (1), we obtain $y^2 = (x - e_3)b_1b_2z_1^2z_2^2$. Since b_1, b_2, z_1, z_2 are non-zero, we can consider $z_3 = \dfrac{y}{b_1b_2z_1z_2}$. Then the new set of equations is $b_1b_2z_3^2 = x - e_3$, $b_1z_1^2 = x - e_1$ and $b_2z_2^2 = x - e_2$. By eliminating x, we get a pair of equations

$$b_1z_1^2 - b_2z_2^2 = e_2 - e_1,\ \ b_1z_1^2 - b_1b_2z_3^2 = e_3 - e_1.$$

We can use various techniques, such as reduction to determine whether or not this pair of equations has at least one rational point (z_1, z_2). If this happens to be the case, then we recover easily x and y as

$$x = b_1z_1^2 + e_1,\ \ y = b_1b_2z_1z_2z_3$$

The only pairs which we cannot compute using f_{Q_1} and f_{Q_2} are $b(Q_1, Q_1)$ and $b(Q_2, Q_2)$. But we use

$$b(Q_1, Q_1) = b(Q_1, Q_1 + Q_2)/b(Q_1, Q_2) = \frac{(e_1 - e_3)}{e_1 - e_2}.$$

Similarly,

$$b(Q_2, Q_2) = \frac{(e_2 - e_3)}{e_1 - e_2}.$$

We can summarize the whole argument in the following

Theorem 1.4.1 (Complete 2-descent). *Suppose that E/K is an elliptic curve, given by a Weierstrass equation*

$$y^2 = (x - e_1)(x - e_2)(x - e_3), \quad e_i \in K$$

Let S be the set of places at which E has bad reduction, the places dividing 2 and the infinite places. Then there exists an injective homomorphism

$$E(K)/2E(K) \to K(S,2) \times K(S,2),$$

which is given explicitly (by proposition 3.1) as

$$P \mapsto \begin{cases} (x(P) - e_1, x(P) - e_2) & \text{if } x(P) \neq e_1, e_2, \\ ((e_1 - e_3)/(e_1 - e_2), e_1 - e_2) & \text{if } x(P) = e_1, \\ (e_2 - e_1, (e_2 - e_3)/(e_2 - e_1)) & \text{if } x(P) = e_2, \\ (1,1) & \text{if } P = O. \end{cases}$$

If $(b_1, b_2) \in K(S,2) \times K(S,2)$ is not in the image of the three points O, $(e_1, 0)$ and $(e_2, 0)$, then (b_1, b_2) is the image of a point $P \in K$ if and only if the equations $b_1 z_1^2 - b_2 z_2^2 = e_2 - e_1$ and $b_1 z_1^2 - b_1 b_2 z_3^2 = e_3 - e_1$ have a solution $(z_1, z_2, z_3) \in K^* \times K^* \times K$. If such a solution exists, then a representative for the element of $E(K)/mE(K)$ is given by $x(P) = b_1 z_1^2 + e_1$ and $y(P) = b_1 b_2 z_1 z_2 z_3$.

1.5 Definition of the ϕ-Selmer and Shafarevich-Tate Groups

As in the previous section, we are led by the motivation to effectively compute the Mordell-Weil group. The main step is to find generators for the weak Mordell-Weil group $E(K)/mE(K)$.

In the previous section, we obtained the Kummer sequence out of the long exact sequence on group cohomology. Now, we consider a slightly more general setting: suppose that $\phi : E \to E'$ is a non-zero isogeny of elliptic curves over K. Then one has a short exact sequence

$$0 \to E[\phi] \to E \xrightarrow{\phi} E' \to 0.$$

In precisely the same way as for the case $E' = E$ and $\phi = [m]$ from the previous section, we obtain a short exact sequence

$$0 \to E'(K)/\phi(E(K)) \xrightarrow{\delta} H^1(\mathrm{Gal}(\overline{K}/K), E[\phi]) \to H^1(\mathrm{Gal}(\overline{K}/K), E(\overline{K}))[\phi] \to 0.$$

Next, we consider a place ν for the number field K. Extend ν to a place of the algebraic closure $\overline{K}$. This gives us an embedding $\overline{K} \subset \overline{K}_\nu$ and a decomposition group, which we denote by $D_\nu \subset \mathrm{Gal}(\overline{K}/K)$. By the definition of a decomposition group and of the completion $\overline{K}_\nu$, it follows that D_ν acts on $E(\overline{K}_\nu)$ and $E'(\overline{K}_\nu)$. Repeating the same argument as the one in the previous section, we obtain similar Kummer sequences

$$0 \to E'(K_\nu)/\phi(E(K_\nu)) \to H^1(D_\nu, E[\phi]) \to H^1(D_\nu, E(\overline{K}))[\phi] \to 0.$$

Notice that $D_\nu \subset \mathrm{Gal}(\overline{K}/K)$ and $E(\overline{K}) \subset E(\overline{K}_\nu)$. Of course, it is a subtle question on how the local cohomology depends on the choice of ν, but this is discussed in detail in [5, Ch. IV]. Recall from the basic properties of Galois cohomology that these inclusions induce restriction maps on cohomology. We do the same for each place ν and use these restriction maps to obtain the following commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \frac{E'(K)}{\phi(E(K))} \arrow[r, "\delta"] \arrow[d] & H^1(\mathrm{Gal}(\overline{K}/K), E[\phi]) \arrow[r] \arrow[d] & H^1(\mathrm{Gal}(\overline{K}/K), E(K))[\phi] \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \prod_\nu \frac{E'(K_\nu)}{\phi(E(K_\nu))} \arrow[r, "\delta"] & \prod_\nu H^1(D_\nu, E[\phi]) \arrow[r] & \prod_\nu H^1(D_\nu, E(K_\nu))[\phi] \arrow[r] & 0
\end{tikzcd}$$

But in the previous section, we identified the group of equivalence classes of principle homogeneous spaces $WC(E/K)$ with the cohomology group $H^1(\mathrm{Gal}(\overline{K}/K), E)$. Thus, we can replace the upper and lower last terms by $WC(E/K)$ and $WC(E/K_\nu)$ respectively.

Our ultimate goal is computing the image of $E'(K)/\phi(E(K))$ in $H^1(\mathrm{Gal}(\overline{K}/K), E[\phi])$, which is the same as computing the kernel of the map $H^1(\mathrm{Gal}(\overline{K}/K), E[\phi]) \to WC(E/K)[\phi]$. But the following proposition provides a way of testing whether an element is in the kernel, in terms of K-rational points on the homogeneous spaces of $WC(E/K)$.

Proposition 1.5.1. *Suppose that C/K is a homogeneous space for E/K. Then C/K represents the trivial element of $WC(E/K)$ if and only if C has at least one K-rational point.*

Proof. One of the directions is easy. Suppose that C/K represents a trivial element of $WC(E/K)$. Then there is a K-isomorphism $\varphi : E \to C$. Then $\varphi(0) \in C(K)$, so in particular $C(K)$ is non-empty.

Conversely, suppose that $C(K)$ is non-empty, i.e. $P_0 \in C(K)$. Define a morphism $\theta : E \to C$ by $\theta(Q) = P_0 + Q$. We first show that the morphism θ is defined over K. Suppose $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Then

$$\theta(Q)^\sigma = (P_0 + Q)^\sigma = P_0^\sigma + Q^\sigma = P_0 + Q^\sigma = \theta(Q^\sigma).$$

Thus, the morphism is defined over K. We next prove that θ is an isomorphism. Indeed, since E acts simply transitively on C, then for each $P \in C$ there is a unique $Q \in E$, such that $\theta(Q) = P$ and so θ has degree 1. This means that the induced map on function fields $\theta^* : \overline{K}(C) \to \overline{K}(E)$ is an isomorphism of fields. In other words $\theta^*\overline{K}(C) = \overline{K}(E)$. Therefore, θ has an inverse, which we denote by $\theta^{-1} : \overline{K}(E) \to \overline{K}(C)$. This isomorphism gives rise to a rational function $\psi : C \to E$ of degree 1. But such a function is always a morphism, since E is smooth. $\square$

Although we obtained a simple criteria to check if a principal homogeneous space represents the trivial element in the Weil-Châtelet group, it is still a hard question to determine whether a curve C has a K-rational point. In such cases, it is always easier to work over complete local fields, because we can use Hensel's lemma to reduce the problem to checking whether the curve has a point over a finite ring.

To illustrate more precisely the above idea, consider a place ν and the complete local field K_ν. By proposition 1.5.1, computing the kernel of the map

$$H^1(D_\nu, E[\phi]) \to WC(E/K_\nu)[\phi]$$

reduces to the question of determining whether a homogeneous space C has a K_ν-rational point. This idea naturally leads to the following definitions:

Definition 1.5.2. For an isogeny $\phi : E \to E'$ defined over K, consider the ϕ-Selmer group $S^{(\phi)}(E/K)$ to be the subgroup of $H^1(\mathrm{Gal}(\overline{K}/K), E[\phi])$, defined as

$$S^{(\phi)}(E/K) := \ker \left\{ H^1(\mathrm{Gal}(\overline{K}/K), E[\phi]) \to \prod_\nu WC(E/K_\nu) \right\}.$$

We also consider the Shafarevich-Tate group of E/K to be the subgroup of $WC(E/K)$ defined as

$$Ш(E/K) := \ker \left\{ WC(E/K) \to \prod_\nu WC(E/K_\nu) \right\}.$$

Although the above definitions include the choices of the extension of each place ν to the algebraic closure $\overline{K}$, from the more geometric interpretation of homogeneous spaces, it follows that both $S^{(\phi)}$ and Ш depend only on E and K. Indeed, recall that a homogeneous space C represents a trivial element in $WC(E/K_\nu)$ if and only if it has a K_ν-rational point, a condition which is certainly independent of the choice of extension of the places ν. Therefore, both $S^{(\phi)}$ and Ш depend only on E and K.

A famous conjecture about Ш(E/K) for an elliptic is that it is always finite and has order a perfect square.

Conjecture 3 (Tate-Shafarevich). *If E/K is an elliptic curve, then* Ш(E/K) *is finite.*

Remark 1.5.3. Another interesting observation for Ш is that it measures the failure of the *local-to-global principle*, since the nonzero elements in Ш are equivalence classes of homogeneous spaces which have a rational point for every local field K_ν, but do not have a K-rational point. For instance, for quadratic forms we have the Hasse-Minkowski principle, according to which existence of a $\mathbb{Q}_\nu$-rational point for each ν-adic field implies existence of a $\mathbb{Q}$-rational point. This is not always true for arbitrary curves. An example of an obstruction to the local-to-global principle is the curve (see [4, Ch. 18] for details)

$$3X^3 + 4Y^3 + 5Z^3 = 0.$$

The Shafarevich-Tate groups measures the failure of the local-to-global principle. Notice that the Tate-Shafarevich conjecture implies that for all, but finitely many equivalence classes of homogeneous spaces the local-to-global principle still holds.

1.6 Finiteness of the Selmer Group

Unlike Ш, it is not hard to prove that $S^{(\phi)}$ is finite and effectively computable. The main goal of the section is to prove finiteness of $S^{(\phi)}$ for an arbitrary isogeny ϕ.

To begin with, let $\phi : E \to E'$ be an isogeny defined over the number field K. Using only the cohomological definition of the Selmer group and Shafarevich-Tate group and the commutative diagram from the previous section, we obtain the following short exact sequence

$$0 \to E'(K)/\phi(E(K)) \to S^{(\phi)}(E/K) \to \text{Ш}(E/K)[\phi] \to 0.$$

This is going to be helpful for proving the first main result of the section

Theorem 1.6.1. *The ϕ-Selmer group $S^{(\phi)}(E/K)$ is finite. In particular, if one chooses ϕ to be the m-isogeny of E to itself, then the weak Mordell-Weil group $E(K)/mE(K)$ is finite.*

The key idea for the proof of the finiteness of the Selmer group is the nontrivial observation that it consists of cohomology classes of cocycles which are *unramified* outside of finite set of places S. Before proceeding, we give a precise definition for a cocycle to be unramified.

Definition 1.6.2. Suppose that M is a $\mathrm{Gal}(\overline{K}/K)$-module, ν is a discrete valuation for the number field K and $I_\nu \subset \mathrm{Gal}(\overline{K}/K)$ be the inertia group for ν. A cohomology class $\zeta \in H^p(\mathrm{Gal}(\overline{K}/K), M)$ is defined to be *unramified at* ν if has a trivial image in $H^p(I_\nu, M)$ under the restriction map $H^p(\mathrm{Gal}(\overline{K}/K), M) \to H^p(I_\nu, M)$.

First of all, we make one clarification about the above definition. Since we have already fixed a decomposition group D_ν for ν, the inertial group I_ν is determined by the decomposition group as the kernel of the map $D_\nu \to \mathrm{Gal}(\overline{k}_\nu/k_\nu)$, where ν' is the extension of ν to the algebraic closure of K and $\overline{k}_\nu$ and k_ν are the two residue fields for the complete local fields K_ν and $\overline{K}_\nu$ respectively.

Before proving theorem 1.6.1, we need to prove a lemma

Lemma 1.6.3. *For any finite, abelian $Gal(\overline{K}/K)$-module M the group of cohomology classes which are unramified outside a finite set of primes is finite. In other words, the group*

$$H^1(Gal(\overline{K}/K), M; S) := \{\zeta \in H^1(Gal(\overline{K}/K), M) : \zeta \textit{ is unramified outside of } S\}$$

is finite.

Proof. Using the definition of the profinite topology and the finiteness of M, we deduce that there must be a finite index subgroup of $\mathrm{Gal}(\overline{K}/K)$ which acts trivially on M. Therefore, we can assume that $\mathrm{Gal}(\overline{K}/K)$ acts trivially on M by changing K with a finite extension (because the inflation-restriction sequence on Galois cohomology implies that it suffices to prove the statement for the extension of K). This in turn implies that $H^1(\mathrm{Gal}(\overline{K}/K), M; S) = \mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), M; S)$. To complete the proof, denote by m the exponent of M (i.e. the smallest m, such that $mx = 0$ for all $x \in M$). Denote by L the maximal abelian extension of exponent m, which is unramified outside of S. Then the natural map $\mathrm{Hom}(\mathrm{Gal}(L/K), M) \to \mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), M; S)$ is clearly an isomorphism. But theorem 1.2.3 implies that L/K is a finite extension, i.e. $H^1(\mathrm{Gal}(\overline{K}/K), M; S)$ is a finite. □

Proof of theorem 1.6.1. Suppose that $\zeta \in S^{(\phi)}(E/K)$ and ν is a finite place of K which does not divide the degree of the isogeny ϕ and that E' has a good reduction at ν. We will prove that ζ is unramified at ν. Using the definition of $S^{(\phi)}$, we obtain that ζ has a trivial image in $WC(E/K_\nu)$. But $WC(E/K_\nu)$ is identified with $H^1(D_\nu, E)$, so $\zeta(\sigma) = P^\sigma - P$ is a coboundary, where $P \in E(\overline{K}_\nu)$ for all $\sigma \in D_\nu$. Furthermore, the definition implies that $P^\sigma - P \in E[\phi]$. But $E[\phi] \subset E[m]$ and we can use lemma 2.2 to show that $E(K)[m]$ injects into $\tilde{E}_\nu$. But the reduction (mod ν) maps sends $P^\sigma - P \to (P^\sigma - P)^\sim = \tilde{P}^\sigma - \tilde{P}$. The last point is $\tilde{0}$ for any $\sigma \in I_\nu$ by the definition of the inertia group. Therefore $P^\sigma = P$ for every $\sigma \in I_\nu$ and hence the restriction of ζ to $H^1(I_\nu, E[\phi])$ is trivial, i.e. ζ is unramified at ν. Finally, the statement follows from lemma 1.6.2. □

Chapter 2

Abelian Varieties

The purpose of this chapter is to introduce the basic theory of abelian varieties. We prove that the group of points on an abelian variety is always commutative as a consequence of the rigidity lemma. We sketch the construction of the dual abelian variety (a variety that will be used a lot in the next chapters). Finally, we discuss Jacobians of curves.

2.1 Abelian Varieties over Arbitrary Fields

Abelian varieties are the main objects of study of this paper.

Definition 2.1.1. An *abelian variety* over a field K is a smooth, proper, algebraic variety X over K, together with multiplication and inverse morphisms

$$m : X \times X \to X \quad \text{(multiplication)}$$

$$i : X \to X \quad \text{(inverse)},$$

and an identity element $e \in X(K)$, such that the maps m, i and the element e define a group structure on $X(\overline{K})$.

Example 2.1.2. The obvious examples are elliptic curves, since they are smooth as algebraic varieties and have a group structure (the group law is defined by the usual addition of points law on elliptic curves).

It is not clear *à priori* whether multiplication on the group variety is commutative. For elliptic curves, commutativity is straightforward from the definition of the group law. To prove commutativity in general, we use the following

Theorem 2.1.3 (Rigidity Theorem). *Let $f : X \times Y \to Z$ be a morphism of varieties over K. Suppose that X is smooth and there exist $y_0 \in Y(K)$ and $z_0 \in Z(K)$, such that*

$$f(X \times \{y_0\}) = \{z_0\}.$$

Then there exists a morphism $g : Y \to Z$, such that $f = g \circ \pi$, where $\pi : X \times Y \to Y$ is the projection morphism.

Proof. Choose a point $x_0 \in X$ and define $g(y) = f(x_0, y)$. Choose an open affine neighborhood U_0 of z_0 in Z. Since X is proper over K, then π is closed. Then $W = \pi(f^{-1}(Z - U_0))$ is closed in Y. Then $Y - W$ is an open set of Y, which is nonempty, because $y_0 \in Z - W$. Indeed, $y \in Y - W$ if and only if $f(X \times \{y\}) \subset U_0$. Therefore, whenever y is a closed point of X, f maps the complete variety $X \times \{y\}$ to the affine variety U_0, so it must be a constant map. Therefore, for any $x \in X$ and $y \in Y$,

$$f(x, y) = f(x_0, y) = g(y) = (g \circ \pi)(x, y).$$

This means that f and $g \circ \pi$ agree on an open dense subset of $X \times Y$ and so they coincide everywhere. □

Rigidity theorem allows us to express morphisms of abelian varieties as a composition of homomorphisms and translations.

Corollary 2.1.4. *Let X and Y be abelian varieties and $f : X \to Y$ be any morphism. There is a homomorphism $g : X \to Y$ and $a \in Y$, such that $f(x) = g(x) + a$.*

Proof. Let $a = f(0)$. By replacing f with $f - a$, we can assume that $f : X \to Y$ satisfies $f(0) = 0$. We will show that f is a homomorphism. Consider $\phi : X \times X \to Y$, defined by $\phi(x', x'') = f(x' + x'') - f(x') - f(x'')$. For fixed $x'' \in X$, $\phi(x', x'')$ is independent of the choice of x', so $\phi(x', x'') = \phi(0, x') = 0$. Thus, $\phi \equiv 0$ and so f is a homomorphism.[1] □

Finally, we conclude that any abelian varieties are commutative.

Corollary 2.1.5. *If X is an abelian variety, then X is commutative.*

Proof. Consider the morphism $x \mapsto x^{-1}$. It maps the identity element to itself, so by the previous corollary, it must be a homomorphism. Thus, $x^{-1}y^{-1} = y^{-1}x^{-1}$, so X is commutative. □

2.2 The Dual Abelian Variety in Characteristic Zero

One of the main problems from the theory of abelian varieties deals with studying the isomorphism classes of invertible sheaves on the varieties (the structure of the Picard group). The goal of this section is to endow the group of isomorphism classes of invertible sheaves of degree 0 on A, considered over the closure of K (or $\mathrm{Pic}^0(A_{\overline{K}})$) with the structure of an abelian variety over K. We will call this variety $A^\vee$ the dual of A (or the Picard variety A).

[1] Although we used additive notation for the group law, we do not make any use of the commutativity so far.

Definition 2.2.1. The dual (or Picard) variety is an abelian variety $A^\vee$, together with an invertible sheaf $\mathcal{P}$ on $A \times A^\vee$ (called the Poincaré sheaf), such that
(i) $\mathcal{P}|_{\{0\}\times A^\vee}$ is trivial and for each $a \in A^\vee(\overline{K})$, $\mathcal{P}|_{A\times\{a\}}$ represents the element a.
(ii) For every K-scheme T and invertible sheaf $\mathcal{L}$ on $A \times T$, such that $\mathcal{L}|_{\{0\}\times T}$ is trivial and $\mathcal{L}_{A\times\{t\}}$ lies in $\mathrm{Pic}^0(A_{K(t)})$ for all $t \in T(\overline{K})$, there is a unique morphism $f : T \to A^\vee$, such that $(1 \times f)^*\mathcal{P} \cong \mathcal{L}$.

It follows from (i) and (ii) that the pair $(A^\vee, \mathcal{P})$, if it exists, is determined uniquely up to unique isomorphism. Moreover, if we plug in $T = \mathrm{Spec}\ \overline{K}$, then we get $A^\vee(\overline{K}) = \mathrm{Pic}^0(A_{\overline{K}})$.

Next, we will sketch the construction of the dual variety. We start with an important result about invertible sheaves on abelian varieties which is proved in §6 of [16].

Theorem 2.2.2 (Theorem of the Square). *Let A be an abelian variety over K and $\mathcal{L}$ be an invertible sheaf on the variety A. For any point $c \in A$, we denote by $t_c : A \to A$ the translation map $x \mapsto c + x$. Then*

$$t^*_{a+b}\mathcal{L} \otimes \mathcal{L} \cong t^*_a\mathcal{L} \otimes t^*_b\mathcal{L},$$

for arbitrary points $a, b \in A(K)$.[2]

The above theorem is very important, because it can be used to construct a homomorphism $A \to \mathrm{Pic}(A)$ in the following way: fix an invertible sheaf $\mathcal{L}$ on A and define a map

$$\varphi_{\mathcal{L}} : A \to \mathrm{Pic}(A),\ \ a \mapsto t^*_a\mathcal{L} \otimes \mathcal{L}^{-1}.$$

The theorem of the square implies that

$$t^*_{a+b}\mathcal{L} \otimes \mathcal{L}^{-1} \cong (t^*_a\mathcal{L} \otimes \mathcal{L}^{-1}) \otimes (t^*_b\mathcal{L} \otimes \mathcal{L}^{-1}),$$

so $\varphi_{\mathcal{L}}$ is a homomorphism.

Next, we will show that the image of $\varphi_{\mathcal{L}}$ is contained in the subgroup $\mathrm{Pic}^0(A)$ - the subgroup of isomorphism classes of invertible sheaves of degree 0. To check this, it suffices to check for any $a \in A(\overline{K})$ and $b \in A(K)$,

$$t^*_a(\varphi_{\mathcal{L}}(b)) \cong \varphi_{\mathcal{L}}(b).$$

This follows, since

$$t^*_a(\varphi_{\mathcal{L}}(b)) \cong t^*_a(t^*_b\mathcal{L} \otimes \mathcal{L}^{-1}) \cong t^*_{a+b}\mathcal{L} \otimes (t^*_a\mathcal{L})^{-1}.$$

The theorem of the square implies that the last sheaf is isomorphic to $t^*_b\mathcal{L} \otimes \mathcal{L}^{-1} = \varphi_{\mathcal{L}}(b)$. Therefore, $\varphi_{\mathcal{L}}(b) \in \mathrm{Pic}^0(A)$ and we are done.

---

[2] *By $t^*_c\mathcal{L}$ we mean the pullback of the sheaf $\mathcal{L}$ under the map $t_c : A \to A$.*

Our next goal is to view $\mathrm{Pic}^0(A)$ as an abelian variety, which is a quotient of A. So far, we did not make any extra assumptions about the sheaf $\mathcal{L}$. It turns out that if $\mathcal{L}$ is chosen to be an ample invertible sheaf and if K is algebraically closed, then $\varphi_{\mathcal{L}} : A \to \mathrm{Pic}^0(A)$ is surjective. This would allow us to endow $\mathrm{Pic}^0(A)$ with a structure of an abelian variety. The result is contained in the following theorem, which follows from Prop. 10.1 of [16].

Theorem 2.2.3. *If $\mathcal{L}$ is an ample invertible sheaf, then the map $\varphi_{\mathcal{L}} : A_{\overline{K}}(\overline{K}) \to$ $Pic^0(A_{\overline{K}})$ is surjective.*[3]

Since abelian varieties are projective (for a complete proof, see []), then there exists an ample invertible sheaf $\mathcal{L}$ on A. We use $\mathcal{L}$ to define invertible sheaf $\mathcal{L}^*$ on $A \times A$ in the following manner

$$\mathcal{L}^* = m^*\mathcal{L} \otimes \pi_1^*\mathcal{L} \otimes \pi_2^*\mathcal{L}^{-1},$$

where $m : A \times A \to A$ is the multiplication map and π_1 and π_2 are the projections on the first and the second coordinates of $A \times A$, respectively. It follows immediately that $\mathcal{L}^*|_{\{0\}\times A} = \mathcal{L} \otimes \mathcal{L}^{-1}$, which is trivial. Moreover, $\mathcal{L}^*|_{A\times\{a\}} = t_a^*\mathcal{L} \otimes \mathcal{L}^{-1} = \varphi_{\mathcal{L}}(a)$, which (as we already saw) is an element of $\mathrm{Pic}^0(A_{\overline{K}})$. Thus, each element of $\mathrm{Pic}^0(A_{\overline{K}})$ is represented by $\mathcal{L}^*|_{A\times\{a\}}$ for a finitely many a (at least one such a). Thus, if $(A^\vee, \mathcal{P})$ exists, then there is a unique isogeny $\varphi : A \to A^\vee$, such that $(1 \times \varphi)^*\mathcal{P} = \mathcal{L}^*$. Furthermore, $\varphi = \varphi_{\mathcal{L}}$.

If the characteristic of K is zero, then we know precisely the kernel of $\varphi_{\mathcal{L}}$ as a finite group subscheme of A. Indeed, it is determined by its underlying set $K_{\mathcal{L}}$ with its reduced subscheme structure. Therefore, in this case we have $A^\vee \cong A/K_{\mathcal{L}}$. Moreover, $K_{\mathcal{L}}$ acts on $\mathcal{L}^*$ over $A \times A$ by lifting the action on the second factor. If we form the quotient, we obtain a sheaf $\mathcal{P}$, such that $(1 \times \varphi_{\mathcal{L}})^*\mathcal{P} = \mathcal{L}^*$. This is pretty much the construction of $(A^\vee, \mathcal{P})$. A proof that this pair satisfies the conditions in the definitions is presented in [19].

2.3 The Dual Isogeny and the Dual Exact Sequence

In the previous section, we explained how to dualize abelian varieties. The next important construction is the dualization of homomorphisms of abelian varieties.

Suppose that $f : A \to B$ is a homomorphism of abelian varieties and consider the induced map $f^\vee : \mathrm{Pic}\, B \to \mathrm{Pic}\, A$ on isomorphism classes of invertible sheaves on A. Since sheaves of zero degree are mapped to sheaves of zero degree, then we get a natural map on points $f^\vee : A^\vee \to B^\vee$, which is in fact a morphism. To give an argument for the last statement, let $\mathcal{P}_B$ be the Poincaré sheaf on $B \times B^\vee$ and consider the pullback sheaf $(f \times 1)^*\mathcal{P}_B$, which is a sheaf on $A \times B^\vee$. The fact that $f^\vee$ is a

[3] *By $A_{\overline{K}}$ we mean the variety A, considered over $\overline{K}$, i.e. $A_{\overline{K}} \cong A \times_K \overline{K}$.*

morphism follows from the universal mapping property, because $(f \times 1)^*\mathcal{P}_B|_{X\times\{\tilde{y}\}}$ represents $f^\vee(\tilde{y})$ for any $\tilde{y} \in Y^\vee$. Thus, every homomorphism of abelian varieties induces a homomorphism on the dual varieties.

The next proposition provides a description of the dual homomorphisms to isogenies.

Proposition 2.3.1. *Let $f : A \to B$ be an isogeny with finite kernel N. Let $N^\vee$ be the Cartier dual of N. Then the kernel of the dual isogeny $f^\vee : B^\vee \to A^\vee$ is $N^\vee$, i.e. there is a short exact sequence*

$$0 \to N^\vee \to B^\vee \xrightarrow{f^\vee} A^\vee.$$

The proposition is proved in [16, §10]. This is everything that we will need from the theory of dual isogenies for the purpose of this project.

2.4 Jacobians of Curves Over $\mathbb{C}$. The Analytic Construction.

We will motivate the notion of Jacobians by looking at how they were discovered historically. The theory of Jacobian varieties arose from the work of Abel and Jacobi, who were studying integrals of the form

$$I(P) = \int_{P_0}^{P} \omega,$$

where P_0 and P are points on a plane curve $C : g(x, y) = 0$ and ω is a rational differential on C. The main result was the following theorem:

Theorem 2.4.1. *There is an integer g, depending on C, such that if P_0 is a base point and $P_1, P_2, \ldots, P_{g+1}$ are arbitrary points on C, then there exists points $Q_1, Q_2, \ldots, Q_g$, such that*

$$\int_{P_0}^{P_1} \omega + \cdots + \int_{P_0}^{P_{g+1}} \omega = \int_{P_0}^{Q_1} \omega + \cdots + \int_{P_0}^{Q_g} \omega \ \left(\textit{mod periods of } \int \omega\right)$$

Example 2.4.2. Let $C = \mathbb{P}^1$ and $\omega = \dfrac{dx}{x}$. Then $g = 1$ and

$$\int_1^{a_1} \frac{dx}{x} + \int_1^{b_1} \frac{dx}{x} = \int_1^{a_1 b_1} \frac{dx}{x}.$$

The theorem implies that for all $P_1, P_2, \ldots, P_g, Q_1, Q_2, \ldots, Q_g$, there exist $R_1, \ldots, R_g$, such that

$$\sum_{i=1}^{g} \int_{P_0}^{P_i} \omega + \sum_{i=1}^{g} \int_{P_0}^{Q_i} \omega = \sum_{i=1}^{g} \int_{P_0}^{R_i} \omega$$

We recognize a group law in the last equation. The motivation behind the Jacobians is that they will be the objects that will contain the information of how to add two such g-tuples $(P_1, \dots, P_g)$ and $(Q_1, \dots, Q_g)$. To realize this in practice, we will construct a commutative algebraic group J, whose points will correspond to the sums $\displaystyle\sum_{i=1}^{g} \int_{P_0}^{P_i} \omega$ and whose group law will describe precisely how we add two such sums.

To describe precisely the above idea, let ω be a rational differential on C with no poles. Then Abel's theorem (theorem 2.4.1.) can be reduced to the existence of a translation-invariant differential η on J and a morphism of varieties $\phi : C \to J$, such that $\phi^*\eta = \omega$. In other words,

$$\int_{\phi(P_0)}^{\phi(P)} \eta \equiv \int_{P}^{P_0} \omega \;\; (\text{mod periods})\,.$$

If one integrates all holomorphic differentials at once, we will obtain the most important of all J's - the Jacobian of the curve $J(C)$.

Although the above discussion was pretty informal, it is helpful to at least understand the idea behind the analytic construction of the Jacobian. Since we require that J contains information about the addition law for arbitrary holomorphic differential ω, then the map

$$\phi : C \to J(C)$$

should set up a bijection:

$$\phi^* : \{\text{translation invariant 1-forms on } J(C)\} \to \{\text{holomorphic differentials } \omega \text{ on } C\}$$

From here, we can conclude that dim $J(C) = \dim_{\mathbb{C}} H^0(C, \Omega^1) = g$, where g is the genus of C.

In order to construct $J(C)$ analytically, we have to write it as $J(C) = V/L$, where V is a $\mathbb{C}$-vector space and L is a lattice. Let V be the dual space to the space of holomorphic differentials, i.e. $V := H^0(C, \Omega^1)^*$. The lattice L will be the period lattice, i.e.

$$L := \left\{ l \in V \;:\; l(\omega) = \int_\gamma \omega \text{ for some 1-cycle } \gamma \right\}$$

In other words, L can be identified with the integral homology $H_1(C, \mathbb{Z})$. The map $\phi : C \to J(C)$ will be defined as follows: fix a base point P_0 and let $\phi(P)$ be the image in V/L of any $l \in V$, defined by $l(\omega) = \displaystyle\int_{P_0}^{P} \omega$, where we fix a path from P_0 to P.

Since $J(C)$ is a group, it is not hard to verify that

$$V^* \cong \{\text{transl. invariant 1-forms on } J(C)\} \cong H^0(C, \Omega^1),$$

which is precisely what we want. Thus,

$$J(C) := H^0(C(\mathbb{C}), \Omega^1)^*/H_1(C(\mathbb{C}), \mathbb{Z}).$$

For more formal discussion, the reader is suggested to look at Chapter III of [20], or §2 of [18].

2.5 Jacobians of Curves Over Arbitrary Fields. Weil's Construction.

This chapter only sketches Weil's construction of the Jacobian of a curve, since a thorough discussion of then construction would be beyond the volume of this senior thesis. More details are presented in [18].

The formal definition of the Jacobian of a curve is an abelian variety which represents the Picard functor for that curve. More precisely, let C be a complete, nonsingular curve, defined over k with positive genus $g > 0$. One can consider the group of degree 0 divisor classes of C (under linear equivalence), which we denote by $\mathrm{Div}^0(C)$. According to [11, II.6], each invertible sheaf $\mathcal{L}$ on C is of the form $\mathcal{L}(D)$ for some divisor D, and D is uniquely determined up to linear equivalence. The degree of the divisor $D = \sum_{i=1}^{n} n_i P_i$ is defined as $\deg(D) = \sum_{i=1}^{n} n_i [K(P_i) : K]$. Hence, we can define the degree of the invertible sheaf $\mathcal{L}$ as $\deg(\mathcal{L}) = \deg(D)$, where D is a divisor, such that $\mathcal{L} = \mathcal{L}(D)$.

Let T be any connected scheme over the ground field K and $\mathcal{M}$ be an invertible sheaf on T. If $q : C \times T \to T$ is the projection map on the second coordinate, then $q^*\mathcal{M}$ is a trivial sheaf, in the sense that $(q^*\mathcal{M})_t = \mathcal{O}_{C_t}$ for any $t \in T$. Therefore, we can consider the group of all invertible sheaves $\mathcal{L}$ of degree 0 on $C \times T$ modulo the trivial sheaves. Consider the functor

$$P_C^0(T) := \{\mathcal{L} \in Pic(C \times T) | deg(\mathcal{L}_t) = 0 \ \forall t \in T\}/q^*Pic(T).$$

Definition 2.5.1. The Jacobian variety J is an abelian variety defined over K, which represents the functor P_C^0, whenever $C(T) \neq \varnothing$.

Weil's original idea for constructing the Jacobian of a curve C was to consider the g-th symmetric power

$$S^g C = C \times \cdots \times C/S_g$$

and to construct by the Riemann-Roch theorem, a partial group law on $S^g C$, i.e.

$$m : U_1 \times U_2 \to U_3,$$

where $U_i \subset S^g C$ is a Zariski-open set. Then he showed that such a partial group law extends automatically into an algebraic group J with $S^g C \supset U_4 \subset J$ for some Zariski-open U_4.

The formal details of Weil's construction are presented in [18]. One of the main properties of Jacobians that we will be using quite often is that they are self-dual, i.e. $J^\vee = J$.

Chapter 3

Modular Abelian Varieties Attached to Newforms

In this chapter, we provide an important construction of two abelian varieties, associated to a given newform $f \in S_2(\Gamma_0(N))^{\mathrm{new}}$. One of the varieties is a quotient of the modular Jacobian $J_0(N)$ and the other one is a subvariety. In fact, the two abelian varieties are dual to each other. Shimura first associated such abelian varieties to newforms, although his construction is rather different from the one presented here. We describe the construction in a much more explicit way, in terms of the action of the Hecke operator on the modular Jacobian. The subvariety is obtained directly from the dual, using a more general result about optimal quotients.

3.1 Hecke Operators as Correspondences

Consider the modular curve $X_0(N)$ and let $p \nmid N$ be a prime. There are two degeneracy maps $\alpha, \beta : X_0(pN) \to X_0(N)$ which can be defined in two different ways.

One interpretation of the noncuspidal points on the modular curve $X_0(N)$ over $\mathbb{C}$ is as isomorphism classes of pairs (E, C), where E is an elliptic curve and C is a cyclic subgroup of $E(\mathbb{C})$ of order N (see [23, Appendix C §3]). Consider a pair (E, C), where C is a cyclic subgroup of order pN. Since $p \nmid N$, then $C \cong C' \oplus D$, where C' is a cyclic subgroup of order N and D is a cyclic subgroup of order p. Moreover, the subgroups C' and D are unique. Thus, we can define the degeneracy maps

$$\alpha : (E, C) \mapsto (E, C')$$

$$\beta : (E, C) \mapsto (E/D, (C + D)/D)$$

An equivalent construction can be obtained by viewing $X_0(N)$ and $X_0(pN)$ as quotients of the upper-half plane. In this case we will not worry about the cusps, since any rational map between nonsingular curves extends uniquely to a morphism. So, we look at $\Gamma_0(N)\backslash\mathfrak{h}$ and $\Gamma_0(pN)\backslash\mathfrak{h}$.

Since $\Gamma_0(pN) \subset \Gamma_0(N)$, then there is a natural map

$$\alpha' : \Gamma_0(N)\backslash\mathfrak{h} \to \Gamma_0(pN)\backslash\mathfrak{h}.$$

It is not hard to verify (by tracing the definitions) that α and α' represent the same map.

The equivalent way of defining β is as follows: note that there is an inclusion $\Gamma_0(pN) \hookrightarrow \Gamma_0(N)$, defined by

$$X \mapsto \begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix} \cdot X \cdot \begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}^{-1}.$$

We can use this inclusion to construct a map between the quotients of the upper half plane:

$$\Gamma_0(pN)\backslash\mathfrak{h} \simeq \begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix} \Gamma_0(pN) \begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}^{-1} \backslash\mathfrak{h} \to \Gamma_0(N).$$

Again, one checks immediately that this definition agrees with the one given in terms of the parametrization interpretation.

Thus, we have a correspondence

$$\begin{tikzcd} & X_0(pN) \arrow[dl, "\alpha"'] \arrow[dr, "\beta"] & \\ X_0(N) & & X_0(N) \end{tikzcd}$$

We can recover out of this correspondence the pullback and push-forward maps on divisors. Consider the induced map

$$\alpha^* : \mathrm{Div}(X_0(N)) \to \mathrm{Div}(X_0(pN)).$$

The preimages of the prime divisor (E, C) under α are all $(E, C \oplus D)$, where D is a cyclic subgroup of E of order p. Therefore

$$\alpha^* : (E, C) \mapsto \sum_{|D|} (E, C \oplus D),$$

where the above sum runs over all cyclic subgroups of E of order p. Similarly, we recover the push-forward map $\beta_* : X_0(pN) \to X_0(N)$: if (E, C') is a point $X_0(pN)$, then C' can be written uniquely as $C \oplus D$, where C and D are cyclic subgroup of E of orders N and p, respectively. Then

$$\beta_* : (E, C \oplus D) \mapsto (E/D, (C + D)/D).$$

Consider $\varphi := \beta_* \circ \alpha^*$. Then φ is a map $\varphi : \mathrm{Div}(X_0(N)) \to \mathrm{Div}(X_0(N))$. Since φ multiplies the degree of a divisor class by the degree of the map α, then it restricts to a map $\mathrm{Div}^0(X_0(N)) \to \mathrm{Div}^0(X_0(N))$. This is precisely how one obtains the Hecke operator T_p on $J_0(N)$. In other words, we define $T_p := \varphi|_{\mathrm{Div}^0(X_0(N))}$.

Notice that it is possible to define the Hecke operator on modular forms from the above correspondence. Indeed, recall that $S_2(\Gamma_0(N)) \cong H^0(X_0(N), \Omega^1)$, where the isomorphism is given by $f(z) \mapsto f(z)dz$. Indeed, if $f(z)$ is a modular form of weight 2 for $\Gamma_0(N)$, then the differential $f(z)dz$ is $\Gamma_0(N)$-invariant. Since α and β induce maps on differentials, we have a composition

$$H^0(X_0(N), \Omega^1) \xrightarrow{\alpha^*} H^0(X_0(pN), \Omega^1) \xrightarrow{\beta_*} H^0(X_0(N), \Omega^1).$$

Thus, we have an operator T_p on the space of cusp forms $S_2(\Gamma_0(N))$ for all $p \nmid N$. Moreover, the two operators define compatible actions on the space of differentials and on the modular Jacobian, because we can consider the modular curve $X_0(N)$ over $\mathbb{C}$ and since the Jacobian is then

$$J_0(N)(\mathbb{C}) = H^0(X_0(N)(\mathbb{C}), \Omega^1)^*/H_1(X_0(N)(\mathbb{C}), \mathbb{Z}).$$

But $H^0(X_0(N)(\mathbb{C}), \Omega^1)$ is the space of differentials, so we obtain the compatibility of the actions.

3.2 Constructing an Abelian Variety A_f as a Quotient of $J_0(N)$

In the previous section, we defined Hecke operators on the modular Jacobian $J_0(N)$ and on the space of holomorphic differentials $H^0(X_0(N), \Omega_1)$ and showed that the two actions are compatible, i.e the two Hecke algebras are in fact isomorphic. We want to associate an abelian variety to a newform f of level N. Before proceeding, we need one more definition

Definition 3.2.1 (Optimal Quotient). Let J be a Jacobian of a curve, A be an abelian variety and $\pi : J \to A$ be a smooth, surjective morphism. We say that A is an *optimal quotient* of J if the kernel of π is connected.

Suppose now that $f = \sum_{n=1}^{\infty} a_n q^n$ is a newform of level N and weight 2. Consider the ideal $I_f = \ker(\phi)$, where $\phi : \mathbb{T} \to K_f$ sends $T_n \mapsto a_n$. It is not hard to check that I_f is also the annihilator of f. We saw that the Hecke algebra acts on both $S_2(\Gamma_0(N))$ and $J_0(N)$, so the ideal I_f acts on $J_0(N)$.

Proposition 3.2.2. *(i) $I_f J_0(N)$ is strictly contained in $J_0(N)$, so the quotient variety*

$$A_f := J_0(N)/I_f J_0(N)$$

is nonzero.
(ii) The variety A_f is an optimal quotient of $J_0(N)$ of dimension $[K_f : \mathbb{Q}]$.

The key idea for the proof is the following

Lemma 3.2.3. *Let $\mathbb{T}_{\mathbb{C}} = \mathbb{T} \otimes \mathbb{C}$. There exists a perfect Hecke-compatible pairing*

$$\mathbb{T}_{\mathbb{C}} \times S_2(\Gamma_0(N)) \to \mathbb{C}.$$

In particular, $Hom(S_2(\Gamma_0(N)), \mathbb{C})$ and $\mathbb{T}_{\mathbb{C}}$ are isomorphic as $\mathbb{T}_{\mathbb{C}}$-modules.

Proof. Define a pairing

$$\alpha : \mathbb{T}_{\mathbb{C}} \times S_2(\Gamma_0(N)) \to \mathbb{C}$$

as $\alpha(T, f) := a_1(Tf)$, where $a_1(f)$ returns the first coefficient in the Fourier expansion of the modular form f. We claim that this pairing is nondegenerate. Suppose that there is a cusp form f, such that $\alpha(T, f) = 0$ for any operator T in the Hecke algebra $\mathbb{T}_{\mathbb{C}}$. In particular, $\alpha(T_n, f) = 0$ for each n. But one can figure out exactly the Hecke action on q-expansions, namely if $f = \sum_{n=1}^{\infty} a_n q^n$, then

$$T_p f = \begin{cases} \sum_{n=1}^{\infty} a_{pn} q^n + p \sum_{n=1}^{\infty} a_n q^{pn} & \text{if } p \nmid N \\ \sum_{n=1}^{\infty} a_{pn} q^n & \text{if } p \mid N \end{cases}$$

so the formula implies that $a_1(T_n, f) = a_n$. Thus, $a_n = 0$ for each n, so $f = 0$.

To show nondegeneracy on the right, suppose that T is an operator, for which $\alpha(T, f) = 0$ for each $f \in S_2(\Gamma_0(N))$. Then for all n and all cusp forms f, $\alpha(T, T_n f) = 0$. But $\alpha(T, T_n f) = a_1(T(T_n f)) = a_1(T_n(Tf))$, because the Hecke algebra is commutative. By the Hecke action on Fourier expansions, we notice that $a_1(T_n f) = a_n(f)$ for arbitrary cusp form f, so it follows that $0 = \alpha(T, T_n f) = a_n(Tf)$ for all n, i.e. $Tf = 0$. Thus, T kills all cusp forms and so $T \equiv 0$. Therefore α is a nondegenerate pairing. Finally, we have to prove that the pairing α is Hecke equivariant, i.e. $\alpha(T_n T, f) = \alpha(T, T_n f)$. But this follows from the definition, using that the Hecke algebra is commutative.

Finally, it follows from the perfect, Hecke-equivariant pairing α that

$$\mathrm{Hom}(S_2(\Gamma_0(N)), \mathbb{C}) \cong \mathbb{T}_{\mathbb{C}}$$

as $\mathbb{T}_{\mathbb{C}}$-modules. □

Proof of Proposition 3.2.2. (i) The most difficult part is to show that $I_f J_0(N) \subsetneq J_0(N)$. To do this, we consider the variety $J_0(N)$ over $\mathbb{C}$ and then

$$J_0(N)(\mathbb{C}) \cong H^0(X_0(N), \Omega^1)^* / H_1(X_0(N), \mathbb{Z}).$$

The idea is to reduce the statement to showing that $I_f\mathbb{T}_\mathbb{C} \subsetneq \mathbb{T}_\mathbb{C}$, which is easy to prove (in particular, $\mathbb{T}_\mathbb{C}/I_f\mathbb{T}_\mathbb{C} \cong K_f \otimes \mathbb{C}$, where K_f is the Hecke eigenvalue field). The first step in this reduction is to notice that it is enough to check that $I_f H^0(X_0(N), \Omega^1)^* \subsetneq H^0(X_0(N), \Omega^1)^*$ (e.g. by counting dimensions of vector spaces and using the fact that $J_0(N)(\mathbb{C})$ and $I_f J_0(N)(\mathbb{C})$ are obtained by taking modulo one and the same lattice $H_1(X_0(N), \mathbb{Z})$). Next, using the correspondence between differentials on $X_0(N)$ and cusp forms, explained in the previous section, we have $H^0(X_0(N), \Omega^1) \cong S_2(\Gamma_0(N))$ as $\mathbb{T}_\mathbb{C}$-modules, so

$$H^0(X_0(N), \Omega^1)^* \cong \mathrm{Hom}(S_2(\Gamma_0(N)), \mathbb{C}),$$

as $\mathbb{T}_\mathbb{C}$-modules. Finally, by using lemma 3.2.3, $\mathrm{Hom}(S_2(\Gamma_0(N)), \mathbb{C})$ is isomorphic to $\mathbb{T}_\mathbb{C}$ as $\mathbb{T}_\mathbb{C}$-module, so we reduced the question to proving that the $\mathbb{T}_\mathbb{C}$-module $\mathbb{T}_\mathbb{C}/I_f\mathbb{T}_\mathbb{C}$ is nonempty. But $\mathbb{T}_\mathbb{C}/I_f\mathbb{T}_\mathbb{C} \cong K_f \otimes \mathbb{C}$, so the result follows.
(ii) To see that $I_f J_0(N)$ is connected, note that each Hecke operator $T : J_0(N) \to J_0(N)$ defines a morphism. Thus, the image $T(J_0(N))$ is an abelian variety. To see this, note that the image of an abelian variety under a morphism is a group variety. Moreover, since connected sets are mapped to connected sets via continuous maps, then $T(J_0(N))$ is connected and therefore an abelian variety. Finally, the theorem will follow if we show that the sum of two abelian subvarieties of an abelian variety is an abelian subvariety. Indeed, let A and B be abelian subvarieties of $J_0(N)$. Consider the map

$$A \times B \to J_0(N),$$

defined by $(a, b) \mapsto a + b$. Since this map is a morphism then its image is an abelian subvariety, i.e. $A + B$ is an abelian subvariety. Therefore, $I_f J_0(N)$ is an abelian subvariety of $J_0(N)$ which shows that A_f is an optimal quotient. □

3.3 The Dual Abelian Variety as a Subvariety of $J_0(N)$

So far, we constructed an optimal quotient A_f of $J_0(N)$. The dual variety $A_f^\vee$ is an interesting abelian variety. The remarkable property it has is that it can be viewed as a subvariety of $J_0(N)$. Thus, one can associate to each newform f two isogenous abelian varieties - the optimal quotient A_f and the subvariety $A_f^\vee$.

The main goal of this chapter is to construct the morphism, which makes $A_f^\vee$ a subvariety of $J_0(N)$.

First of all, Jacobians of curves are self-dual, i.e. $J^\vee = J$. Moreover, they come equipped with a canonical, principal polarization $\theta_J : J \to J$, which satisfies $\theta_J^\vee = \theta_J$.

Let $\pi : J_0(N) \to A_f$ be the quotient map. Consider the dual map $\pi^\vee : A_f^\vee \to J_0(N)$ and compose it with $\theta_{J_0(N)}$. Thus, we get a morphism

$$A_f^\vee \xrightarrow{\pi^\vee} J_0(N)^\vee \xrightarrow{\theta_{J_0(N)}} J_0(N).$$

The fact that the dual morphism is a closed immersion follows from the following more general statement

Proposition 3.3.1. *Let J/K be a Jacobian and θ_J be the canonical polarization of J. Suppose that $\pi : J \twoheadrightarrow A$ is an optimal quotient. Then the morphism*

$$A^\vee \xrightarrow{\pi^\vee} J^\vee \xrightarrow{\theta_J} J$$

is a closed immersion.

The key idea in the proof of the statement is that for any abelian variety A, the group $A(\overline{K})$ is divisible.

Definition 3.3.2. We say that an abelian group G is *divisible*, if for any element $x \in G$ and any positive integer $n \in \mathbb{Z}$, there exists $y \in G$, such that $x = ny$.

One can see that G is divisible, if and only if the homomorphism $[n] : G \to G$ is surjective for each $n \in \mathbb{N}$.

Example 3.3.3. A nontrivial example of a divisible group is the group of $\overline{K}$-rational points on an elliptic curve E, defined over a number field K, since for any point $P \in E(\overline{K})$ and any integer n, one can choose a point $Q \in E(\overline{K})$, such that $nQ = P$ (because one can recover the group law from the Weierstrass equation of the curve). More generally, for abelian variety A over a number field K, the group $A(\overline{K})$ is a divisible group. This fact is proved in [19].

Example 3.3.4. No nontrivial finite group is divisible. Indeed, if G is a finite group and $x \in G$ is a nontrivial element of order n, then $[n] : G \to G$ has a nontrivial kernel. In particular, it is not surjective and thus G is not divisible.

We will also use the following

Lemma 3.3.5. *Let $f : B \to A$ be a surjective morphism of abelian varieties. The dual morphism $f^\vee : A^\vee \to B^\vee$ has finite kernel.*

Proof. We will use that the "double dual" functor is the identity on the category of abelian varieties. This is a nontrivial result from the theory of abelian varieties. A very ellegant proof, which makes use of the Poincaré sheaves is presented in [].

Consider the abelian variety $C = f^\vee(A) \subset B^\vee$. We have the composition

$$A^\vee \to C \hookrightarrow B^\vee.$$

We can dualize this composition to get

$$B \to C^\vee \to A.$$

Since the double dual is the identity, the composition of the two maps is f, which is surjective. Hence $C^\vee \to A$ is surjective. Hence, $\dim(C) = \dim(C^\vee) \geq \dim(A)$. But $A^\vee \to C$ is surjective, since C is the image of $A^\vee$ under $f^\vee$. Therefore, $\dim(A) = \dim(A^\vee) \geq \dim(C)$. Thus, $\dim(A) = \dim(C)$, so $f^\vee$ has finite kernel. $\square$

Proof of Proposition 3.3.1. It suffices to show that $\pi^\vee$ is injective, since θ_J is an isomorphism and any monomorphism between smooth schemes of finite type is a closed immersion. Since the dual of $\pi^\vee$, which is π is surjective, then $\pi^\vee$ must have a finite kernel, according to lemma 3.3.5. Let $G = \ker(\pi^\vee)$. Let $C = \operatorname{im}(\pi^\vee)$. Then $A^\vee \to C$ is an isogeny. Let G be the kernel of this isogeny. One has the following commutative diagram

$$\begin{tikzcd} G \arrow[r] & A^\vee \arrow[r] \arrow[dr, "\pi^\vee"] & C \arrow[d] \\ & & J \end{tikzcd}$$

After dualizing the diagram, we obtain

$$\begin{tikzcd} G^\vee & A \arrow[l] & C^\vee \arrow[l] \\ & & J \arrow[ul, "\pi"] \arrow[u, "\varphi"'] \end{tikzcd}$$

where $G^\vee$ is the Cartier dual of G. Since G is finite, then $G^\vee$ is also finite, so the kernel of the map $\varphi : J \to C^\vee$ is a finite index subgroup of the kernel of $\pi : J \to A$. But $\ker(\pi)$ is an abelian variety, so it is a divisible group. This means that any quotient of $\ker(\pi)$ is divisible as well. Therefore, the finite quotient $\ker(\pi)/\ker(\varphi)$ is divisible. But no finite group is divisible, so G must be trivial. Therefore, $\pi^\vee : A^\vee \to J^\vee$ is a closed immersion. $\square$

Chapter 4

Visibility Theory

The main goal of this chapter is to introduce and study a subgroup of the Shafarevich-Tate group, which is called the *visible subgroup* and was first introduced by B. Mazur [7]. One of the reasons why this subgroup is interesting to study is that it is always a finite subgroup of the Shafarevich-Tate group, so in particular, it can be used to produce elements of finite order. Another strong motivation to look at the visible subgroup is the fact that every element of the Shafarevich-Tate group can be visualized somewhere (the visualization theorem). We provide a method (the visibility theorem) for producing visible elements of the Shafarevich-Tate group.

4.1 Visible Subgroups of $H^1(K, A)$ and $Ш(A/K)$

Suppose that A and J are abelian varieties, defined over a number field K and let $i : A \to J$ be a morphism of abelian varieties over K.[1]

Definition 4.1.1. The *visible subgroup* of $H^1(K, A)$ with respect to i and J as

$$\mathrm{Vis}_J^{(i)}(H^1(K, A)) := \ker\{H^1(K, A) \to H^1(K, J)\},$$

where $H^1(K, A) \to H^1(K, J)$ is the map on cohomology, induced from i.[2]

The notion is useful, because it relates to the geometric interpretation of the elements of $H^1(K, A)$ as elements of the Weil-Châtelet group in the case when A is a subvariety of J, i.e. when the morphism $i : A \to J$ is a closed immersion. To see the relation, consider the short exact sequence of abelian varieties

$$0 \to A \to J \to C \to 0,$$

[1] Note that J is not necessarily a Jacobian of a curve. The only reason we use the letter J is that in most of the computational examples that we will provide later on, we will be using Jacobians of modular curves.

[2] In some papers, no superscript (i) is used. The only reason we use it here is because we do not necessarily require that the morphism i be an embedding.

where C is the quotient J/A. Write the long exact sequence on Galois cohomology

$$0 \to A(K) \to J(K) \to C(K) \to H^1(K, A) \to H^1(K, J) \to \dots .$$

Using the definition of the visible subgroup, we can extract the following short exact sequence

$$0 \to J(K)/A(K) \to C(K) \to \mathrm{Vis}_J^{(i)}(H^1(K, A)) \to 0.$$

Let c be a visible cohomology class. Then there exists a K-rational point $x \in C(K)$, which maps to c. The fiber over x for the map $J \to C$ is a subvariety of J, which when equipped with the natural action of A becomes a principal homogeneous space, and therefore represents an element of $WC(A/K)$. This element corresponds to the cohomology class c. Thus, the element $x \in C(K)$ *visualizes* the cohomology class c. The following statement follows almost directly from the above remarks.

Corollary 4.1.2. *For any embedding $i : A \to J$, the visible subgroup $Vis_J^{(i)}(H^1(K, A))$ is finite.*

Proof. The group $H^1(K, A)$ is a torsion group, and $C(K)$ is finitely generated, so the surjectivity of the homomorphism $C(K) \to \mathrm{Vis}_J^{(i)}(H^1(K, A))$ implies that $\mathrm{Vis}_J^{(i)}(H^1(K, A))$ must be finite. □

Next, we define the visible subgroup of $Ш(A/K)$ with respect to the morphism $i : A \to J$.

Definition 4.1.3. The *visible subgroup* of $Ш(A/K)$ with respect to the map i is defined as

$$\mathrm{Vis}_J^{(i)}(A) := \mathrm{Vis}_J^{(i)}(H^1(K, A)) \cap Ш(A/K).$$

The above corollary implies that the visible subgroup of $Ш(A/K)$ is always finite.

4.2 The First Property of Visibility

The first interesting property, related to visibility is the fact that each element of $H^1(K, A)$ becomes visible for some abelian variety J and a closed immersion $i : A \hookrightarrow J$.

Theorem 4.2.1 (Visualization Theorem). *Let $c \in H^1(K, A)$ be any cohomology class. Then there exists an abelian variety J and a closed immersion $i : A \hookrightarrow J$, such that $c \in Vis_J^{(i)}(H^1(K, A))$.*

An essential ingrediant of the proof will be the existence of Weil restriction of scalars. We will sketch the important points of the construction. A thorough discussion of this subject is presented in [3, §7.6].

Proposition 4.2.2. *Suppose that L/K is a field extension of number fields.*[3] *Let X' be a scheme of finite type over L. There exists a scheme X of finite type over K, such that the scheme X represents the following contravariant functor*

$$Res_{L/K}(X') : (Sch/K) \to \{Sets\},\ S \mapsto Hom_L(S \times_K L, X).$$

Moreover, smoothness is carried over from the scheme X'/L to X/K, i.e. if X' is smooth, then so is X. We denote the scheme X by $Res_{L/K}(X')$.

Before proceeding further, we will explain the intuition behind the construction of Weil Restriction of scalars. For simplicity, we will work with varieties over fields, and even the simpler case of elliptic curves. Consider the elliptic curve

$$E : Y^2Z = X^3 + XZ^2 + Z^3$$

over the number field $K = \mathbb{Q}(\sqrt{5})$. The goal is to construct a variety over $\mathbb{Q}$, whose $\mathbb{Q}$-rational are in one-to-one correspondence to the K-rational points of E.

First, it suffices to look at the affine patch, corresponding to $Z \neq 0$ and to construct the restriction of scalars only for that patch. So we can assume $Z = 1$, $X = x$ and $Y = y$. One can use the following idea: choose any $\mathbb{Q}$-basis for K, e.g. $\{1, \sqrt{5}\}$ and write $x = x_1 + \sqrt{5}x_2$, $y = y_1 + \sqrt{5}y_2$ for some indeterminates x_1, x_2, y_1, y_2. After plugging x and y into the Weierstrass equation and equating the coefficients in front of the elements of the basis, we get the variety

$$X = \langle x_1^3 + 5x_1x_2^2 - y_1^2 - 5y_2^2 + x_1 + 1,\ 3x_1^2x_2 + 5x_2^3 - 2y_1y_2 - x_2\rangle$$

defined over $\mathbb{Q}$ whose $\mathbb{Q}$-rational points are in one-to-one correspondence with the K-rational points on the affine patch of the elliptic curve E fixed above. Indeed, we have the correspondence $(x, y) \leftrightsquigarrow (x_1, x_2, y_1, y_2)$.

This example strongly suggests how one can generalize the construction for arbitrary schemes of finite type. We will only sketch the construction. For more formal and rigorous treatment of the existence of Weil restriction of scalars, we refer the reader to [3, §7.6].

Sketch of Construction: Let $[L : K] = n$. We can reduce the question to the case when X' is affine (for the general case, we glue local data), i.e.

$$X' = \text{Spec } L[y_1, y_2, \ldots, y_k]/I.$$

Let $I = \langle f_1, f_2, \ldots, f_s\rangle$ for polynomials $f_i \in L[y_1, \ldots, y_k]$. Choose a basis $\{e_1, \ldots, e_n\}$ of L/K and write $y_i = \sum_{j=1}^{n} x_{ij}e_j$, where x_{ij}'s are indeterminates. We express the coefficients of the f_i's as linear combinations of the basis elements. Next, we plug the

[3] *The same argument applies for the general case, but since we will be considering abelian varieties over number fields, we will not worry too much about the general case.*

y_j's into each of the polynomials f_i and after using the multiplication table for the basis $\{e_1, \dots, e_n\}$ and taking the coefficients in front of each of the basis elements, we obtain n polynomials $g_{i1}, g_{i2}, \dots, g_{in}$ from f_i, such that $g_{ij} \in K[x_{11}, \dots, x_{1n}, \dots, x_{kn}]$. Consider the ideal $J = \langle g_{ij} \rangle_{i=1}^{k}{}_{j=1}^{n}$ and look at the scheme

$$X = \text{Spec } K[x_{11}, \dots, x_{kn}]/J.$$

We claim that X represeents the functor $\text{Res}_{L/K}(X')$. All we have to check is that for any K-algebra A, there is a bijection

$$\text{Hom}_L(\text{Spec } A \otimes_K L, X') \to \text{Hom}_K(\text{Spec } A, X),$$

which is functorial in A.[4] But this is easy to check from the definition of X, because it is equivalent to construct a bijection

$$\text{Hom}_L(L[y_1, y_2, \dots, y_k]/I, A \times_K L) \to \text{Hom}_K(K[y_{11}, y_{12}, \dots, y_{1n}, \dots y_{kn}]/J, A),$$

which can be constructed explicitely.[5] □

We are now ready to give a proof of the visualization theorem. This proof was discovered recently by William Stein and the author and makes an explicit use of the simple transitive action of an abelian variety on its principal homogeneous spaces.

Proof of Theorem 4.2.1. Recall that a cohomology class $c \in H^1(K, A)$ is trivial if and only if the corresponding principal homogeneous space C to c has a K-rational point. Intuitively, to trivialize c, it is enough to consider an extension L/K, so that C has an L-rational point. After choosing such an extension L/K, we obtain $\text{res}_{L/K}(c) = 0$, where $\text{res}_{L/K} : H^1(K, A) \to H^1(L, A)$ is the restriction map on Galois cohomology.

Let C/K be a principal homogeneous space (a torsor) for A/K, such that the class $[C] \in WC(A/K)$ corresponds to the element $c \in H^1(K, A)$. Let $A \times C \to C$ be the simple, transitive action of A on C.[6] Let $P \in C(L)$ be the L-rational point. We can define a morphism $\varphi : A_L \to C_L$ be the morphism, defined by $\varphi(a) = a \oplus P$.[7] Since A acts simply transitively on C, then φ is an isomorphism. Let $\psi = \varphi^{-1}$.

The first important step of the proof is to recover the group law on A_L in terms of the morphisms φ and ψ. The main idea for proving this is to use rigidity theorem for abelian varieties. Define a morphism

$$\phi : A_L \times A_L \to A_L$$

by $\phi(a, a') = \psi(a \oplus \varphi(a'))$. We compute $\phi(a, 0) = \psi(a \oplus P) = a$. Also, $\phi(0, a) = \psi(0 \oplus \varphi(a)) = \psi(a \oplus P) = a$. Therefore, if $\mu_L : A_L \times A_L \to A_L$ is the multiplication map, then $\phi - \mu_L$ satisfies the hypothesis for the rigidity theorem, therefore $\phi = \mu_L$.

[4] Hom_K denotes morphisms of schemes over K

[5] In this case Hom_K denotes homomorphisms of K-algebras

[6] In order to avoid confusion with the group law on A, we denote the action of A on C by $\oplus$.

[7] If X is a scheme over K and L is an extension of K, then X_L will denote the scheme $X \times_K L$

Let $J = \mathrm{Res}_{L/K}(A_L)$. The isomorphism $\psi : C_L \to A_L$ induces an inclusion $C(K) \hookrightarrow C(L) \cong A_L(L) \cong J(K)$ and the identity morphism $\mathrm{id} : A_L \to A_L$ induces an inclusion $A(K) \hookrightarrow A_L(L) \cong J(K)$. These inclusions correspond via Yoneda's lemma to injective morphisms $A \to J$ and $C \to J$. Since these morphisms are proper, then [9, §8.11.5] implies that they are closed immersions.

Since A is defined over K, we may view J_L as a product of n copies of A_L, i.e.

$$J_L \cong \prod_{i=1}^{n} A_L.$$

The closed immersion $C \hookrightarrow J$ base extended to L gives a morphism $C_L \to J_L$. This morphism is the map, sending

$$x \mapsto (\psi_1(x), \psi_2(x), \ldots, \psi_n(x)),$$

where $\psi_i : C_L \to A_L$ are the conjugates of $\psi : C_L \to A_L$, obtained by applying the n different embedding $L \hookrightarrow \overline{K}$ to ψ, which fix the field K. Note that each of the ψ_i's is a morphism $C_L \to A_L$, since both C and A are defined over K.

We claim that the image of C_L inside J_L is a translate of A_L. The morphism $A_L \hookrightarrow J_L \cong \prod_{i=1}^{n} A_L$ is precisely the diagonal embedding. To determine the image of C_L, we consider the morphism

$$A_L \xrightarrow{\phi} C_L \to \prod_{i=1}^{n} A_L,$$

which maps $a \mapsto (\psi_1(\varphi(a)), \psi_2(\varphi(a)), \ldots \psi_n(\varphi(a)))$. The image of $a \in A_L(\overline{K})$ is the unique b, such that $b \oplus \sigma_i(P) = a \oplus P$. But the action is transitive, so we get $(-b + a) \oplus P = \sigma_i(P)$, which means that $b = a - \psi(\sigma_i(P))$. This shows that the image of C_L in J_L is a translate of A_L by $(-\psi(\sigma_1(P)), -\psi(\sigma_2(P)), \ldots, -\psi(\sigma_n(P)))$, so we are done. □

4.3 Producing Upper Bound on the Visibility Dimension

The theorem from the previous section gives rise to an interesting question, relating the order of a cohomology class c and the minimal dimension of an abelian variety J, for which c is visible, under a closed immersion $i : A \hookrightarrow J$.

Definition 4.3.1. Let $c \in H^1(K, A)$. The *visibility dimension* of c is the minimal dimension of an abelian variety J, such that $c \in \mathrm{Vis}_J^{(i)}(H^1(K, A))$.

First of all, we produce an upper bound for the visibility dimension of a cohomology class $c \in H^1(K, A)$, in terms of the order n of that element and the dimension of A.

Lemma 4.3.2. *Suppose that G is a group and M is a finite G-module. Let $c \in H^1(G, M)$ be any cohomology class. Then there is a subgroup $H \subseteq G$, such that the restriction of c to $H^1(H, M)$ is trivial and $[G : H] \leq |M|$.*

Proof. Consider $H = \ker(f)$, where $f : G \to M$ is any representative of the cohomology class c. The map f satisfies the cocycle condition

$$f(\sigma\tau) = \sigma f(\tau) + f(\sigma).$$

Clearly, the restriction of c to $H^1(H, M)$ is trivial. To bound the dimension, we construct an injection $G/H \hookrightarrow M$, by sending $\tau H \mapsto f(\tau)$. By the definition of H, this map is well defined. Suppose $f(\sigma) = f(\tau)$. Then, the cocycle condition

$$f(\tau) = f(\sigma(\sigma^{-1}\tau)) = \sigma f(\sigma^{-1}\tau) + f(\sigma).$$

Thus, $\sigma f(\sigma^{-1}\tau) = 0$, i.e. $f(\sigma^{-1}\tau) = 0$, which means that $\sigma^{-1}\tau \in H$. This proves injectivity of the map $G/H \hookrightarrow M$, and so the bound follows. $\square$

Proposition 4.3.3. *The visibility dimension of any $c \in H^1(K, A)$ is at most $d \cdot n^{2d}$, where n is the order of c in $H^1(K, A)$ and d is the dimension of A.*

Proof. It follows from the proof of the Visualization Theorem (Theorem 4.2.1) that the dimension of J, which was constructed using Weil restriction of scalars is at most $[L : K] \cdot \dim A$. Thus, we need an upper bound for the degree of the extension $[L : K]$. To get this, consider the surjective map $H^1(K, A[n]) \to H^1(K, A)[n]$, which is induced from the long exact sequence on Galois cohomology. Since $c \in H^1(K, A)[n]$, it suffices to trivialize one of its preimages. By the above lemma, there exists a finite index subgroup of $\mathrm{Gal}(\overline{K}/K)$ (which by Galois theory corresponds to some field extension L/K), such that c is trivialized in $H^1(L, A[n])$ and the index of the subgroup $[L : K]$ is at most $|A[n]| = n^{2d}$. Thus, one can choose L, so that $[L : K] \cdot \dim A \leq d \cdot n^{2d}$, so we get an upper bound for the dimension. $\square$

4.4 Smooth and Surjective Morphisms

4.4.1 Flat, Smooth and Étale Morphisms

In order to make sense of the notion of continuous family of schemes, we need to introduce the notion of flatness.

Recall from commutative algebra that a morphism $f : A \to B$ of rings is *flat* if the functor $M \mapsto M \otimes_A B$ from A-modules to B-modules is exact. Since *flatness* is a local property, in order to check that f is flat, it suffices to check that the homomorphism of local rings $A_{f^{-1}(\mathfrak{m})} \to B_{\mathfrak{m}}$ is flat for every maximal ideal $\mathfrak{m} \subset B$.

Definition 4.4.1. A morphism $\varphi : Y \to X$ of schemes is *flat*, if the homomorphisms of local rings $\mathcal{O}_{X,\varphi(y)} \to \mathcal{O}_{Y,y}$ is flat for every $y \in Y$.

Example 4.4.2. Any finite, surjective morphism $f : X \to Y$ of nonsingular varieties over algebraically closed fields is flat.

The notion of flatness corresponds to continuous family of manifolds in differential topology. Indeed, $\varphi : Y \to X$ being flat implies that all points $x \in X$, such that $\varphi^{-1}(x)$ is nonempty behave like regular values, i.e. if $Y_x := \varphi^{-1}(x)$, then

$$\dim Y_x = \dim Y - \dim X.$$

Next, we use the notion of flatness to define the relative notion of nonsingular varieties.

Definition 4.4.3. A morphism $\varphi : Y \to X$ of schemes of finite type over a field k is *smooth of relative dimension* n, if:
(1) φ is flat;
(2) if $Y' \subseteq Y$ and $X' \subseteq X$ are irreducible components, such that $\varphi(Y') \subseteq X'$, then

$$\dim Y' = \dim X' + n;$$

(3) for each point $y \in Y$, one has

$$\dim_{k(y)}(\Omega_{Y/X} \otimes k(y)) = n.$$

Example 4.4.4. If $Y = \operatorname{Spec} k$ and k is algebraically closed, then X is smooth over k of relative dimension n if and only if X is regular of dimension n. In particular, if X is irreducible and separated, then X is smooth if and only if X is a variety.

Finally, we can define the notion of an étale morphism.

Definition 4.4.5. A morphism $\varphi : Y \to X$ is called *étale* if it is smooth and of relative dimension zero.

Example 4.4.6. Open immersions are smooth morphisms of relative dimension zero, so they are étale.

4.4.2 Henselian Rings and Strictly Henselian Rings

We start by introducing a special class of rings R, called *henselian* rings. Roughly speaking, those are rings, for which the Hensel lemma is true.

Definition 4.4.7. Let R be a local ring with residue field k. The ring R is called *henselian* if, for every monic polynomial $P \in R[T]$, all k-rational zeros of the residue class $\overline{P} \in k[T]$ lift to R-rational zeros of P. If, in addition, the residue field k is separably closed, the ring R is called *strictly henselian*.

The following statement deals with some properties of strictly henselian rings.

Proposition 4.4.8. *Let R be a local ring. The following are equivalent:*
(1) R is a strictly henselian ring.
(2) For all étale morphisms $f : X \to \mathrm{Spec}\ R$ and for all points $x \in X$, such that $f(x) = s$ is a closed point of Spec R, there exists a section $u : \mathrm{Spec}\ R \to X$ (i.e. S-morphism), such that $u(s) = x$.

Proof. The proposition follows from [10, §18.8.1]. $\square$

4.4.3 Surjectivity of $[n] : G(R) \to G(R)$

The main goal of this whole section is to prove the following theorem:

Proposition 4.4.9. *Let A be an abelian variety over a field K, which is the residue field of a strictly henselian discrete valuation ring R. Let $x \in A(K)$, such that the reduction of x lies in the identity component of the closed fiber of the Néron model $\mathcal{A}$ of A. Then for any integer n, prime to the residue characteristic of R, one has $x \in nA(K)$.*

We start by several technical lemmas which will be used in the proof of the proposition.

Lemma 4.4.10. *Let G be a smooth, commutative group scheme of finite type over an arbitrary base scheme S. Let n be an integer which is not divisible by the residue characteristic of the local ring at every point $s \in S$. Then the multiplication by n morphism $n_G : G \to G$ is étale.*

Proof. The lemma follows from Lemma 2(b) of [3, §7.3]. $\square$

Lemma 4.4.11. *Suppose that $U \subseteq G$ is an open dense group subscheme of G. Then $U = G$.*

Proof. Since the underlying topological spaces for G and $G \times_R K$ are the same, it suffices to prove the statement for a commutative group scheme G over a field K. Let G be a commutative group scheme over a field K. It suffices to prove that $G \times_K \overline{K} = (U \times_K \overline{K}) \cdot (V \times_K \overline{K})$. Therefore, one can assume that K is algebraically closed. In this case, it suffices to prove that U contains all closed points of G. Indeed, U contains all generic points; otherwise U^c will be the closure of a generic point, which is impossible.

Suppose that $x \in G$ is a closed point. Since K is algebraically closed, then x is rational, so U and $U \cdot x$ are both open. Thus, they have at least one common closed point v, so there is $u \in U$, such that $ux = v$, i.e. $x = u^{-1}v \in U$. $\square$

Lemma 4.4.12. *Suppose that G is a finite-type commutative group scheme over a strictly henselian local ring R and the fibers of G over R are geometrically connected.*[8] *The multiplication map by n map*

$$[n] : G(R) \to G(R)$$

[8] *We say that a scheme X over a field K is geometrically connected if $X \times_K \overline{K}$ is connected*

is surjective when $n \in R^\times$*.*

Proof. Choose a point $x \in G(R)$. Then x corresponds to a morphism $x : \text{Spec } R \to G$. Form the following pullback diagram

$$\begin{tikzcd} Y_x \arrow[r, "\psi"] \arrow[d] & \text{Spec } R \arrow[d, "x"] \\ G \arrow[r, "n_G"] & G \end{tikzcd}$$

The surjectivity of $[n] : G(R) \to G(R)$ will follow if we prove that there is a section $\text{Spec } R \to Y_g$. Indeed, note that $\text{Spec } R \to Y_g \to G$ corresponds to a R-rational point on G, which is mapped to $x \in G(R)$ under n_G.

Since R is strictly henselian and by Proposition 4.4.8, it suffices to prove that $Y_g \to \text{Spec } R$ is étale and the closed fiber of Y_g is nonempty. The last two statements would evidently follow if we prove that $n_G : G \to G$ is étale and surjective. Étaleness follows from Lemma 4.4.10. The surjectivity of n_G follows from the fact that the image of n_G must be an open, dense subgroup scheme, so by Lemma 4.4.11 the morphism n_G must be surjective. ☐

Lemma 4.4.13. *Let X be a connected scheme over an arbitrary field K. Suppose that there exists at least one K-rational point of X. Then the scheme X is geometrically connected (i.e. the scheme $X \times_K \overline{K}$ is connected).*

Proof. This is proved in [8, §4.5.13]. ☐

Proof of Proposition 4.4.9. According to the basic properties of the Néron model, $A(K) \cong \mathcal{A}(R)$. The image of $x \in A(K)$ under this isomorphism is a point of $\mathcal{A}^0(R)$. Since $\mathcal{A}^0(R)$ is connected and has a R-rational point, the fibers of A^0 over Spec (R) are geometrically connected by Lemma 4.4.13. Therefore, we can apply Lemma 4.4.12 to obtain that the multiplication by n map $[n] : G(R) \to G(R)$ is surjective. This gives us a point $z \in A(K)$, such that $nz = x$ and we are done. ☐

4.4.4 Surjectivity of the Induced Map on Generic Fibers

Here we discuss the last bit of algebraic geometry that will be needed for the main result in this chapter. Suppose that $\mathcal{A}$ and $\mathcal{B}$ are commutative, smooth, group schemes over strictly Henselian local ring R, which are the Néron models of abelian varieties A and B (both defined over the fraction field K of R) and $\phi : \mathcal{A} \to \mathcal{B}$ is a morphism. We discuss a condition for ϕ, under which the induced map on the generic fibers is always surjective.

Proposition 4.4.14. *Suppose that $\phi : \mathcal{A} \to \mathcal{B}$ is smooth and surjective. Then the induced morphism $\phi_K : A(K) \to B(K)$ is surjective.*

Proof. The idea is very similar to the one that we used in the proof of Lemma 4.4.12. It suffices to show that the induced map $\phi_R : \mathcal{A}(R) \to \mathcal{B}(R)$ is surjective. Choose a point $x \in \mathcal{B}(R)$ and consider the corresponding morphism Spec $R \to \mathcal{B}$. As in the previous proof, form the pullback diagram

$$\begin{tikzcd} Y_x \arrow[r, "\psi"] \arrow[d] & \text{Spec } R \arrow[d, "x"] \\ \mathcal{A} \arrow[r, "\phi"] & \mathcal{B} \end{tikzcd}$$

It will suffice to check that the morphism $\psi : Y_x \to \text{Spec } R$ has a section. To do this, we only need to check that the closed fiber of ψ has a section. But the closed fiber is smooth and nonempty (since ϕ is surjective); also, its base field is separably closed, since R is strictly henselian. Hence, the closed fiber has an R-rational point by [3, §2.2.13]. □

4.5 Producing Visible Elements of the Shafarevich-Tate Group

Suppose that A is an abelian variety over a number field K. We describe a technique which produces visible elements of $Ш(A/K)$. The basic idea is that under certain conditions it will be possible to inject a weak Mordell-Weil group of some abelian variety into $Ш(A/K)$, so we will produce element of finite order of $Ш(A/K)$. The precise statement is the following

Theorem 4.5.1 (Visibility Theorem). *Let A/K and B/K be abelian subvarieties of J/K which have finite intersection.*[9] *Let N be the product of the residue characteristics of the non-archimedian places of bad reduction for B. Suppose that p is a prime number, which satisfies the following conditions:*
(i) $p \nmid N \cdot |(J/B)(K)_{tors}| \cdot |B(K)_{tors}| \cdot \prod_\nu c_{A,\nu} \cdot c_{B,\nu}$, where $c_{A,\nu}$ and $c_{B,\nu}$ are the Tamagawa numbers (or the orders of the component groups of the fibers of the Néron models at ν);
(ii) $B[p] \subset A$;
(iii) If $e_\mathfrak{p}$ is the ramification index of the prime ideal $\mathfrak{p}$, then $e_\mathfrak{p} < p - 1$ for any prime ideal $\mathfrak{p}$ lying above p.
Under these hypothesis, there is a natural map

$$\varphi : B(K)/pB(K) \to Ш(A/K),$$

such that the order of the kernel of φ is at most p^r, where r is the Mordell-Weil rank of A. In particular, the map is injective if the Mordell-Weil rank of A is 0.

[9] *As before, J is not necessarily a Jacobian of a curve; the notation is used only because we will often apply the theorem for J being a Jacobian of a modular curve.*

Proof. There are two major steps for the proof of the theorem. First, we construct a map from the weak Mordell-Weil group $B(K)/pB(K)$ to the visible part of $H^1(K, A)$, using the hypothesis that $B[p] \subset A$. The second step is proving that the image of $B(K)/pB(K)$ in $H^1(K, A)$ consists of locally trivial cohomology classes, which immediately implies that this image is contained in $\mathrm{Vis}_J^{(i)}(\text{Ш}(A/K))$.

Step I: *Constructing a map $B(K)/pB(K) \to H^1(K, A)$.*

The argument we will use is purely algebraic and is based on diagram chasing. Start with the short exact sequence

$$0 \to A \to J \to C \to 0,$$

where C is simply the quotient J/A, considered over K. The associated long exact sequence on Galois cohomology is

$$0 \to A(K) \to J(K) \to C(K) \xrightarrow{\delta} H^1(K, A) \to \cdots . \tag{4.5.1}$$

One can construct a map $\psi : B \to C$ by composing the inclusion map $B \hookrightarrow J$ and the map $J \to C$. Since $B[p] \subset A$ and A is the kernel of the map $J \to C$, then the map $\psi : B \to C$ factors through the multiplication by p map $B \xrightarrow{\cdot p} B$. This gives us the following commutative diagram:

$$\begin{tikzcd}
 & & B \arrow[r, "\cdot p"] \arrow[d] \arrow[dr, "\psi"] & B \arrow[d] \\
0 \arrow[r] & A \arrow[r] & J \arrow[r] & C
\end{tikzcd}$$

We still have not used the fact that $B(K)[p]$ is empty. We take K-rational points and use this fact to get the following diagram, with exact rows and columns:

$$\begin{tikzcd}
 & K_0 \arrow[d] & K_1 \arrow[d] & K_2 \arrow[d] & \\
0 \arrow[r] & B(K) \arrow[r, "\cdot p"] \arrow[d] & B(K) \arrow[r] \arrow[d] \arrow[dr, "\pi"] & B(K)/pB(K) \arrow[r] \arrow[d, "\varphi"] & 0 \\
0 \arrow[r] & J(K)/A(K) \arrow[r] \arrow[d] & C(K) \arrow[r] & \delta(C(K)) \arrow[r] & 0 \\
 & K_3 & & &
\end{tikzcd}$$

By definition, the visible part of $H^1(K, A)$ is the kernel of the map $H^1(K, A) \to H^1(K, J)$, which by the long exact sequence on Galois cohomology is exactly the image of the map $H^0(K, C) \xrightarrow{\delta} H^1(K, A)$, which is $\delta(C(K))$. Now, we apply the snake lemma to get an exact sequence

$$K_0 \to K_1 \to K_2 \to K_3.$$

We can analyze further the sequence, by observing that K_1 is finite. This is because the kernel of $\psi : B \to C$ is $A \cap B$, which is finite. Therefore, $K_1 \subset B(K)_{\text{tors}}$. But $B(K)$ does not contain p-torsion elements. Since $K_2 \subset B(K)/pB(K)$ is a p-group, then $K_1 \to K_2$ must necessarily be the zero map. Therefore, K_2 injects into $K_3 \cong J(K)/(A(K) + B(K)) \cong (J(K)/B(K))/A(K)$. Since torsion of $J(K)/B(K)$ is contained in $(J/B)(K)_{\text{tors}}$, then $J(K)/B(K)$ has no p-torsion. Therefore, if $A(K)$ is a torsion group, then $(J(K)/B(K))/A(K)$ has no p-torsion and so K_2 (which is a p-group) is trivial, i.e. $\varphi : B(K)/pB(K) \to H^1(K, A)$ must be injective.

More generally, suppose that the Mordell-Weil rank of $A(K)$ is r. The order of the kernel of φ is bounded from above by the order of $(J(K)/(A(K) + B(K)))[p]$. The last group is precisely the p-torsion part of the cokernel of the map $\phi : A(K) \to J(K)/B(K)$, so the bound on that kernel follows from

Lemma 4.5.2. *Suppose that G and H are finitely generated abelian groups, G is of rank r, and H has no p-torsion elements. Suppose that $f : G \to H$ is a group homomorphism. Then coker$(f)[p] \leq p^r$.*

Proof. We may consider that H is a torsion-free, since no torsion of order prime to p contributes to the order of $\operatorname{coker}(f)[p]$. Thus, all the torsion of G is mapped to 0 via f and so we might as well assume that G is torsion-free. For free groups, we can see this by considering the Smith normal form of the integer matrix, corresponding ot f. Indeed, the new matrix we obtain consists of at most r diagonal entries $[d_1, d_2, \ldots]$, such that $d_1 \mid d_2 \ldots$, which immediately implies that the order of the p-torsion of the cokernel is at most p^r. $\square$

Step II: *The Local Analysis.*

In the previous step we constructed a map $\varphi : B(K)/pB(K) \to H^1(K, A)$ and proved that the kernel has order at most p^r, where r is the Mordell-Weil rank of A (the last statement follows from Lemma 4.5.2). We should also prove that the image of φ consists of locally trivial cohomology classes in order to conclude that this image lies in Ш(A/K). Consider the composition $\pi : B(K) \to H^1(K, A)$ of the quotient map $B(K) \to B(K)/pB(K)$ and the map φ. Let $x \in B(K)$ be a K-rational point. We want to show that for each place ν, the restriction $\operatorname{res}_\nu(\pi(x)) = 0$.

We prove this by considering the different possibilities for the place ν.

Case 1: *ν is archimedean.*

There is nothing to prove in the case when ν is complex archimedean, because the local cohomology group is trivial.

If ν is real archimedean, we have $H^1(\operatorname{Gal}(\overline{K}_\nu)/K_\nu, A(K_\nu)) = H^1(\operatorname{Gal}(\mathbb{C}/\mathbb{R}), A(\mathbb{R}))$. But $\operatorname{Gal}(\mathbb{C}/\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$ and since the order of the group kills any element of the first cohomology, then $\operatorname{res}_\nu(\pi(x))$ is 2-torsion. But $\pi(x)$ is also p-torsion and p is odd. Therefore, $\operatorname{res}_\nu(\pi(x))$ is both p-torsion and 2-torsion, which means that $\operatorname{res}_\nu(\pi(x)) = 0$.

Case 2: *$p \neq char(\nu)$.*

Let m be the order of the component group $\Phi_{B,\nu}(k_\nu)$ of the closed fiber $\mathcal{B}_{k_\nu}$ at ν of the Neron model $\mathcal{B}$ (i.e. the Tamagawa number $c_{B,\nu}$). Then mx is in the identity component $\mathcal{B}^0_{k_\nu}$. Hence, we can apply Proposition 4.4.9 for the point mx and the local field K_ν^{ur} (whose valuation ring is strictly Henselian) to get that there exists $z \in B(K_\nu^{\mathrm{ur}})$, such that $pz = mx$. Now, look at $\mathrm{res}_\nu(\pi(mx)) \in H^1(K_\nu, A(K_\nu))$. By the discussion of the Kummer pairing in Chapter 1.1, this cohomology class is represented by the 1-cocycle

$$f : \mathrm{Gal}(\overline{K}_\nu/K_\nu) \to A(\overline{K}_\nu),\ \sigma \mapsto \sigma(z) - z.$$

Since $z \in B(K_\nu^{\mathrm{ur}})$, it follows that f is unramified cocycle, i.e. $\mathrm{res}_\nu(\pi(mx))$ is an unramified cohomology class. Thus, $\mathrm{res}_\nu(\pi(mx)) \in H^1(K_\nu^{\mathrm{ur}}/K_\nu, A(K_\nu^{\mathrm{ur}}))$.

Next, we use the following relationship between the unramified cohomology and the the cohomology of the component group.

Lemma 4.5.3. *Let A be an abelian variety over a local field K, which is the fraction field of a discrete valuation ring R with residue field k. Let $\mathcal{A}$ be the Néron model of A and $\Phi(\overline{k})$ be the component group of the closed fiber $\mathcal{A}_k$ of $\mathcal{A}$, i.e. $\Phi(\overline{k}) := \mathcal{A}_k(\overline{k})/\mathcal{A}_k^0(\overline{k})$. Then*

$$H^1(K^{ur}/K, A(K^{ur})) = H^1(K^{ur}/K, \Phi(\overline{k})),$$

where K^{ur} denotes the maximal unramified extension of K.

The lemma is proved in [17, Prop.3.8]. It implies that

$$H^1(K_\nu^{\mathrm{ur}}/K_\nu, A(K_\nu^{\mathrm{ur}})) = H^1(K_\nu^{\mathrm{ur}}/K_\nu, \Phi_{A,\nu}(\overline{k_\nu})).$$

The cohomology of the component group is easier to work with, because the component group is a finite $\mathrm{Gal}(K_\nu^{ur}/K_\nu)$-module and $\mathrm{Gal}(K_\nu^{ur}/K_\nu)$ is a cyclic, so we can apply the following

Lemma 4.5.4. *Suppose that G is a cyclic group and A is a finite G-module. Let*

$$h(A) := |H^0(G, A)|/|H^1(G, A)|$$

be the Herbrand quotient of the G-module A. Then $h(A) = 1$.

Proof. Let g be a generator for G and A^G denote the fixed submodule of A. Let I_G denote the kernel of the homomorphism $\mathbb{Z}[G] \to G$, which maps $g \to 1$. There is an exact sequence

$$0 \to A^G \to A \xrightarrow{\cdot(g-1)} A \to A/I_G A \to 0.$$

Since A is a finite module, it follows that $|A/I_G A| = |A^G|$. Next, let $N : A \to A$ be the homomorphism, obtained by multiplication by $N = \sum_{h \in G} h$. This homomorphism induces a homomorphism $N^* : A/I_G A \to A^G$. Moreover, we have an exact sequence

$$0 \to H^1(G, A) \to A/I_G A \xrightarrow{N^*} A^G \to H^0(G, A) \to 0,$$

which immediately implies that $|H^1(G, A)| = |H^0(G, A)|$, so $h(A) = 1$. □

The lemma implies that the order of $H^1(K_\nu^{\mathrm{ur}}/K_\nu, \Phi_{A,\nu}(\overline{k}_\nu))$ is equal to the order of the component group $\Phi_{A,\nu}(\overline{k}_\nu)$. But $p \nmid c_{A,\nu} = |\Phi_{A,\nu}(\overline{k}_\nu)|$ by assumption. Since the order of $\mathrm{res}_\nu(\pi(mx))$ divides p, it follows that $\mathrm{res}_\nu(\pi(mx))$ is trivial. Therefore, $m\mathrm{res}_\nu(\pi(x)) = 0$. But $p\pi(x) = 0$ and $p \nmid m = c_{B,\nu}$, then it follows that $\mathrm{res}_\nu(\pi(x)) = 0$, i.e. $\pi(x)$ is a locally trivial element.

Case 3: *char*$(\nu) = p$.

Consider the maximal unramified extension K_ν^{ur} of K_ν. Let $\mathcal{A}$, $\mathcal{J}$ and $\mathcal{C}$ be the Neron models of A, J and C respectively.

The first observation is that the induced sequence on the Néron models

$$0 \to \mathcal{A} \to \mathcal{J} \xrightarrow{\psi} \mathcal{C} \to 0$$

is exact, which is a consequence of the following lemma, proved in [3, §7.5, Thm 4.]

Lemma 4.5.5. *Suppose that $0 \to A' \to A \to A'' \to 0$ is an exact sequence of abelian varieties over a field K, which is the fraction field of a discrete valuation ring R. Assume that the ramification index $e = \nu(p)$ satisfies $e < p - 1$, where p is the residue characteristic and ν is the normalized valuation on R. Let $\mathcal{A}'$, $\mathcal{A}$ and $\mathcal{A}''$ be the Néron models of A', A and A'' respectively. If $\mathcal{A}$ has abelian reduction, then the induced sequence*

$$0 \to \mathcal{A}' \to \mathcal{A} \to \mathcal{A}'' \to 0$$

is exact and consists of abelian R-schemes.

Hence, $\psi : \mathcal{J} \to \mathcal{C}$ is a flat morphism, which is surjective and which has a smooth kernel $\mathcal{A}$. This is enough to claim that ψ is smooth [3, §2.4, Prop.8]. Next, using Lemma 4.4.14, it follows that $\mathcal{J}(R) \to \mathcal{C}(R)$ is surjective, and therefore $\mathcal{J}(K_\nu^{\mathrm{ur}}) \to \mathcal{C}(K_\nu^{\mathrm{ur}})$ is surjective. Therefore, $\mathrm{res}_\nu(\pi(x))$ is a unramified cohomology class. Using Lemma 4.5.3, we have

$$H^1(K_\nu^{ur}/K_\nu, A) \cong H^1(K_\nu^{ur}/K_\nu, \Phi_{A,\nu}(\overline{k}_\nu))$$

But A has good reduction at ν, since $p \nmid N$, so $\Phi_{A,\nu}(\overline{k}_\nu)$ is trivial. Therefore $H^1(K_\nu^{\mathrm{ur}}/K_\nu, \Phi_{A,\nu}(\overline{k}_\nu))$ is trivial, so $\mathrm{res}_\nu(\pi(x)) = 0$, which completes the proof of the visibility theorem. $\square$

Chapter 5

Computational Examples and Algorithms

In this chapter we describe specific examples, in which one produces visible elements with the visibility theorem, and therefore provides evidence for the Birch and Swinnerton-Dyer conjecture, by constructing elements of certain finite order of the Shafarevich-Tate group. Two computational examples are provided - one of the examples (a 20-dimensional subvariety of $J_0(389)$) in which we directly produce visible elements using the visibility theorem. The other example is more interesting (18-dimensional subvariety of $J_0(551)$), because no visibility occur at level $N = 551$, but if we raise the level of the modular Jacobian (by mapping $J_0(551) \to J_0(2 \cdot 551)$ by a combination of the degeneracy maps), we can apply the visibility theorem for the image of the variety. We then use a result of K. Ribet to conclude that the Shafarevich-Tate group of the original variety must have elements of certain finite order.

Before presenting the computational example, we describe (or at least give precise reference to) almost all of the computational algorithms that are used for these verifications. For instance, we explain how to compute the modular degree, how to produce upper and lower bounds on the torsion subgroup, how to intersect abelian varieties, how to compute the L-ratios and the orders of the component groups (the Tamagawa numbers).

The examples are not original, so I would like to thank Asst. Prof. William Stein for allowing me to include his examples in my thesis and to use some of the modular abelian algorithms which he came up with in [25].

5.1 Algorithms for Computing with Modular Abelian Varieties

5.1.1 Computing the Modular Degree

Let A_f be an abelian variety attached to a newform f. Then A_f is a quotient of $J_0(N)$, so there is a surjective morphism $J_0(N) \to A_f$. Consider the dual morphism $A_f^\vee \to J_0(N)$ (Jacobians are self-dual), which is an injection. By taking the composition of these two maps, we obtain a finite degree morphism $\theta_f : A_f^\vee \to A_f$. It turns out that the degree of θ_f is a perfect square, which is a consequence of the following

Proposition 5.1.1. *Suppose A is an abelian variety over a field k and let $\lambda : A \to A^\vee$ be a polarization. Suppose that char(k) is either zero, or prime to the degree of λ. There exists a finite abelian group H, such that*

$$ker(\lambda) \cong H \times H,$$

where the above identification is a group isomorphism.

Before proving the proposition, we need a lemma:

Lemma 5.1.2. *Suppose that G is a finite abelian group for which there exists a nondegenerate, alternating, bilinear pairing $\Gamma : G \times G \to \mathbb{Q}/\mathbb{Z}$. There exists a group H, such that $G \cong H \times H$.*[1]

Proof. Using the structure theorem for abelian groups, one can reduce the statement to the case when G is a p-group for some prime number p. Let x be an element of G of maximal order p^h for some integer h. First, we show that there exists $y \in G$, such that $\Gamma(x, y) = 1/p^h$. Indeed, if no such y exists, then $\Gamma(p^{h-1}x, y) = 0$ for each $y \in G$, so Γ is degenerate, which is a contradiction. Notice that every such y still has maximal order p^h, since $0 \neq p^{h-1}\Gamma(x, y) = \Gamma(x, p^{h-1}y)$. Moreover, we show that $\langle x\rangle \cap \langle y\rangle = \varnothing$. Indeed, if $mx = ny$ for some $0 < m, n < p^h$, then

$$0 = m\Gamma(x, x) = \Gamma(x, mx) = n\Gamma(x, y) \neq 0,$$

which is a contradiction. After choosing such y one can define

$$H = \{z : \Gamma(x, z) = \Gamma(y, z) = 0\}.$$

We claim that $G \simeq (\langle x\rangle + \langle y\rangle) \oplus H$. Indeed, for any $g \in G$, the alternating pairing Γ gives us

$$g - (p^h\Gamma(g, y))x - (p^h\Gamma(g, x))y \in H,$$

[1] *It is interesting that this lemma, combined with the existence of the Cassel's pairing for elliptic curves, implies that if the Shafarevich-Tate group of an elliptic curve is finite, then it has a perfect square.*

It is easy to check that this produces a group isomorphism

$$G \simeq (\langle x \rangle + \langle y \rangle) \oplus H.$$

But Γ restricts to an alternating, nondegenerate, bilinear pairing to $H \times H$.

This means that we can use induction on the size of the group G to prove the statement. If G is trivial, there is noting to prove. If not, we construct H and apply the hypothesis for H, i.e. there exists a subgroup H' of H, such that $H \simeq H' \oplus H'$. This means that

$$G \simeq (\langle x \rangle \oplus H') \oplus (\langle y \rangle \oplus H'),$$

because $\langle x \rangle \cap \langle y \rangle = \varnothing$. □

Proof of Proposition 5.1.1. The idea is to prove the existence of a nondegenerate, alternating, bilinear pairing $\beta : \mathrm{Ker}(\lambda) \times \mathrm{Ker}(\lambda) \to \mathbb{Q}/\mathbb{Z}$ and then to use Lemma 5.1.2.

Let m be an integer that kills $\mathrm{Ker}(\lambda)$. Define

$$e^{\lambda} : \mathrm{Ker}(\lambda) \times \mathrm{Ker}(\lambda) \to \mu_m$$

in the following way: suppose that $P, P' \in \mathrm{Ker}(\lambda)$. Choose a point $Q \in A(\overline{k})$, such that $mQ = P'$ and let

$$e^{\lambda}(P, P') := \overline{e}_m(P, \lambda Q),$$

where $\overline{e}_m : A[m] \times A^{\vee}[m] \to \mu_m$ is the Weil pairing. The pairing is well defined, since $m(\lambda Q) = \lambda(mQ) = \lambda(P') = 0$. Moreover, it is nondegenerate, alternating and bilinear, because of the properties of the Weil pairing. Thus, we can apply Lemma 5.1.2 to get $\mathrm{Ker}(\lambda) \cong H \times H$. □

As a consequence of Proposition 5.1.1, we conclude that the degree of the isogeny $\theta_f : A_f^{\vee} \to A_f$. Using the above proposition, we can define the *modular degree.*

Definition 5.1.3. The *modular degree* of A_f is defined as

$$\mathrm{moddeg}(A_f) = \sqrt{\deg(\theta_f)},$$

where $\theta_f : A_f^{\vee} \to A_f$ is the dual isogeny.

There is an explicit algorithm for computing the modular degree of a modular abelian variety, attached to a newform. It is based on Abel-Jacobi's theorem and on the integration pairing[2]

$$\langle , \rangle : S_2(\Gamma_0(N)) \times H_0(X_0(N), \mathbb{Z}) \to \mathbb{C}.$$

[2]From now on, by $S_2(\Gamma_0(N))$ we will mean the complex vector space of modular forms of weight 2 and level N.

Indeed, the pairing induces a natural map

$$\Phi_f : H_0(X_0(N), \mathbb{Z}) \to \mathrm{Hom}(S_2(\Gamma_0(N))[I_f], \mathbb{C}),$$

where I_f is the ideal of the Hecke algebra, which annihilates the form f.

Using Abel-Jacobi's theorem, one can deduce the following commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & H_1(X_0(N),\mathbb{Z})[I_f] \arrow[r] \arrow[d] & \mathrm{Hom}(S_2(\Gamma_0(N)),\mathbb{C})[I_f] \arrow[r] \arrow[d] & A_f^\vee(\mathbb{C}) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & H_1(X_0(N),\mathbb{Z}) \arrow[r] \arrow[d] & \mathrm{Hom}(S_2(\Gamma_0(N)),\mathbb{C}) \arrow[r] \arrow[d] & J_0(N)(\mathbb{C}) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \Phi_f(H_0(X_0(N),\mathbb{Z})) \arrow[r] & \mathrm{Hom}(S_2(\Gamma_0(N))[I_f],\mathbb{C}) \arrow[r] & A_f(\mathbb{C}) \arrow[r] & 0
\end{tikzcd}$$

Finally, since the map $\mathrm{Hom}(S_2(\Gamma_0(N)), \mathbb{C})[I_f] \to \mathrm{Hom}(S_2(\Gamma_0(N))[I_f], \mathbb{C})$ is an isomorphism, then the modular kernel θ_f is isomorphic to the cokernel of the map $H_1(X_0(N), \mathbb{Z})[I_f] \to \Phi_f(H_0(X_0(N), \mathbb{Z}))$ by the snake lemma.

We summarize the algorithm in the following proposition

Proposition 5.1.4. *The kernel of the isogeny $\theta_f : A_f^\vee \to A_f$ is isomorphic to the cokernel of the map*

$$H_1(X_0(N), \mathbb{Z})[I_f] \to \Phi_f(H_0(X_0(N), \mathbb{Z})).$$

Since the Hecke action on the space of modular symbols and the integration pairing are both computable, then the isomorphism allows us to compute ker(θ_f) using modular symbols.

Finally, we explain why the modular degree is important in relation to visibility. We will prove the following result

Proposition 5.1.5. *Let m_A = moddeg(A_f). The visible subgroup of $A_f^\vee \hookrightarrow J_0(N)$ is contained in $Ш(A_f/\mathbb{Q})[m_A]$.*

Proof. The isogeny $\theta_f : A_f^\vee \to A_f$ is a composition of the maps $A_f^\vee \to J_0(N) \to A_f$. Let e_A be the exponent of $\ker(\delta)$. By proposition 5.1.1, $e_A \mid m_A$, so θ_f factors through multiplication by e_A, which means that there is a complementary isogeny $\theta'_f : A_f \to A_f^\vee$, such that $\theta'_f \circ \theta_f = [e_A]$. Let $(\theta_f)_* : Ш(A_f^\vee/\mathbb{Q}) \to Ш(A_f/\mathbb{Q})$ denote the induced map on the Shafarevich-Tate groups. Since $\mathrm{Vis}_{J_0(N)}(Ш(A_f^\vee))$ is contained in $\ker((\theta_f)_*)$, then this visible group is also contained in

$$\ker((\theta'_f \circ \theta_f)_*) = Ш(A_f^\vee/\mathbb{Q})[e_A] \subset Ш(A_f^\vee/\mathbb{Q})[m_A].$$

□

Remark 5.1.6. Note that by considering the complementary isogeny of θ_f one obtains automatically that the visible subgroup of $Ш(A_f^\vee/\mathbb{Q})$ is killed by multiplication by the order of the modular kernel (i.e. the kernel of θ_f). However, using the nontrivial Proposition 5.1.1, we obtain a much stronger statement (the visible Ш is killed by the square of the order of that kernel). In fact, proposition 5.1.5 will be used in the computations in the next section.

5.1.2 Intersecting Complex Tori

In this subsection, we discuss how to compute intersections of abelian varieties. The whole idea is pretty straightforward if one thinks of the varieties as complex tori.

Suppose that V is a finite dimension vector space over $\mathbb{C}$ and Λ be a lattice in V. One can contruct the complex tori $T = V/\Lambda$. Suppose that V_A and V_B are vector subspaces of V. The lattices $\Lambda_A = V_A \cap \Lambda$ and $\Lambda_B = V_B \cap \Lambda$ give us complex subtori $A = V_A/\Lambda_A$ and $B = V_B \cap \Lambda_B$ of T. The following proposition gives us an explicit way to compute the intersection group of A and B, using only the lattices Λ, Λ_A and Λ_B.

Proposition 5.1.7. *Suppose that $A \cap B$ is finite. Then*

$$A \cap B \cong \left(\frac{\Lambda}{\Lambda_A + \Lambda_B}\right)_{tors}.$$

Proof. Since $A \cap B$ is finite, then $V_A \cap V_B = \varnothing$. There is a map $A \oplus B \to T$ given by $(v_A + \Lambda_A) + (v_B + \Lambda_B) \mapsto (v_A - v_B) + \Lambda$. The kernel of consists precisely of pairs (x, x), where $x \in A \cap B$. Indeed, $(v_A + \Lambda_A) + (v_B + \Lambda_B)$ is in the kernel if and only if $v_A - v_B \in \Lambda$, which means precisely that the points $x = v_A + \Lambda_A$ and $y = v_B + \Lambda_B$ viewed as points in T. Therefore, we have an exact sequence

$$0 \to A \cap B \to A \oplus B \xrightarrow{(x,y)\mapsto x-y} T$$

One can construct the following commutative diagram with exact rows and columns:

$$\begin{tikzcd}
 & & 0 \arrow[d] & A \cap B \arrow[d] & \\
0 \arrow[r] & \Lambda_A \oplus \Lambda_B \arrow[r] \arrow[d] & V_A \oplus V_B \arrow[r] \arrow[d] & A \oplus B \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \Lambda \arrow[r] \arrow[d] & V \arrow[r] \arrow[d] & T \arrow[r] \arrow[d] & 0 \\
 & \Lambda/\left(\Lambda_A + \Lambda_B\right) & V/\left(V_A + V_B\right) & T/(A+B) &
\end{tikzcd}$$

Using the snake lemma, we obtain an exact sequence

$$0 \to A \cap B \to \Lambda/(\Lambda_A + \Lambda_B) \to V/(V_A + V_B)$$

Finally, observe that $V/(V_A + V_B)$ is a $\mathbb{C}$-vector space and therefore has no torsion. Therefore, the kernel of $\Lambda/(\Lambda_A + \Lambda_B) \to V/(V_A + V_B)$ contains $\left(\frac{\Lambda}{\Lambda_A + \Lambda_B}\right)_{\text{tors}}$. Conversely, it is easy to check that any element which is not torsion is mapped to a nonzero element of $V/(V_A + V_B)$. Therefore $A \cap B \cong \left(\frac{\Lambda}{\Lambda_A + \Lambda_B}\right)_{\text{tors}}$. □

The proposition can be applied to compute intersections of modular abelian varieties. Indeed, consider the modular Jacobian $J_0(N)$ as an abelian variety over C. The tangent space at the identity is precisely $V = \text{Hom}(S_2(\Gamma_0(N)), \mathbb{C})$. By considering $\Lambda = H_1(X_0(N), \mathbb{Z})$ and the integration pairing, we get $J_0(N)(\mathbb{C}) = V/\Lambda$. Let f and g be newforms, which are not Galois conjugates and let I_f and I_g be the annihilators of f and g in the Hecke algebra $\mathbb{T}$. Let $A = A_f^\vee$ and $B = B_f^\vee$. Then $V_A = V[I_f]$ and $V_B = V[I_g]$ are the tangent spaces at the identity to A and B. According to the above proposition, we have

$$A \cap B \cong \left(\frac{\Lambda}{\Lambda_A + \Lambda_B}\right),$$

where $\Lambda_A = \Lambda[I_f]$ and $\Lambda_B = \Lambda[I_g]$.

5.1.3 Producing a Multiple of the Order of the Torsion Subgroup

We first consider some methods for providing upper bounds on the size of the torsion subgroup of a modular abelian variety $A := A_f$, attached to a newform f, which is a normalized eigenform, i.e. $f = q + \sum_{n=1}^{\infty} a_n q^n$.

The basic idea for bounding the size of the torsion group $A_{tors}(\mathbb{Q})$ is to inject the torsion subgroup into the group of $\mathbb{F}_p$-rational points of the reduction of A for various primes p. We start with the following

Proposition 5.1.8. *Suppose that A is a modular abelian variety, which is a quotient of $J_0(N)$ and $p \nmid 2N$ is a prime. Then there exists an injective map*

$$A(\mathbb{Q})_{tors} \to A_{\mathbb{F}_p}(\mathbb{F}_p).$$

We recognize this statement as a generalization of Lemma 1.2.2. The above proposition is a direct consequence of a more general statement, which is proved in the Appendix of [12]

Using the above proposition, one can get an upper bound on the torsion, by taking the greatest common divisor of all $|A_{\mathbb{F}_p}(\mathbb{F}_p)|$, where p runs over all primes, for which $p \nmid N$. In short,

$$|A(\mathbb{Q})_{\text{tors}}| \leq \gcd\{|A_{\mathbb{F}_p}(\mathbb{F}_p)| \ : \ \forall p \nmid 2N\}.$$

To complete the computation of the upper bound, we need an algorithm for computing the order of the group $A_{\mathbb{F}_p}(\mathbb{F}_p)$. The observation is that the $\mathbb{F}_p$-rational points can be recovered as the fixed points of the Frobenius automorphism, acting on $A_{\mathbb{F}_p}(\overline{\mathbb{F}}_{\shortmid})$. Indeed, the automorphism $\mathrm{Frob}_p : \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p$ that sends $x \mapsto x^p$ induces an automorphism $\mathrm{Frob}_p : A_{\mathbb{F}_p}(\overline{\mathbb{F}}_p) \to A_{\mathbb{F}_p}(\overline{\mathbb{F}}_p)$. Thus,

$$|A_{\mathbb{F}_p}(\mathbb{F}_p)| = |\ker(1 - \mathrm{Frob}_p)|.$$

A useful tool for computing degrees, such as the above one are characteristic polynomials. Since we cannot define characteristic polynomials of an endomorphism of an abelian variety, we should somehow relate this automorphism to an automorphism of vector spaces, or modules of finite rank.

Indeed, it is helpful to introduce the ℓ-adic Tate module. Indeed, it is defined as the inverse limit

$$T_\ell A := \varprojlim_n A[\ell^n],$$

taken with respect to the natural map

$$A[\ell^{n+1}] \xrightarrow{\cdot l} A[\ell^n].$$

Let $\varphi : A \to A$ be any element of $\mathrm{End}(A)$. There is an induced homomorphism $\varphi_l : T_\ell A \to T_\ell A$.

Lemma 5.1.9. *For any $\varphi \in End(A)$,*

$$deg(\varphi) = |det(\varphi_l)|.$$

Proof. This is proved in [16, §12.9]. $\square$

Thus, all we need to do is compute the characteristic polynomial of the Frobenius homomorphism, acting on the ℓ-adic Tate module $T_\ell A$. This is achieved in the following proposition, proved in [22, §7].

Proposition 5.1.10. *Let F_p be the characteristic polynomial of the homomorphism $Frob_p : T_\ell A \to T_\ell A$. Then*

$$F_p(x) = \prod_{\sigma : K_f \hookrightarrow \overline{\mathbb{Q}}} \left(x^2 - \sigma(a_p)x + p\right).$$

Finally, let $G_p(x)$ be the characteristic polynomial of multiplication by a_p on the vector space $K_f/\mathbb{Q}$. Then (e.g. by the Eichler-Shimura relation between T_p and Frob_p, acting on the ℓ-adic Tate module),

$$F_p(x) = x^{[K_f:\mathbb{Q}]} G_p\left(x + \frac{p}{x}\right).$$

But the polynomial $G_p(x)$ is easily computable from the coefficients of f. Therefore, $F_p(x)$ is computable. Finally, we obtain

$$|A_{\mathbb{F}_p}(\mathbb{F}_p)| = |\det(1 - \mathrm{Frob}_p)| = |F_p(1)| = |G_p(1 + p)|.$$

This gives the explicit way of computing the number of $\mathbb{F}_p$-rational points on the reduced variety $A_{\mathbb{F}_p}$.

5.1.4 Producing a Divisor of the Order of the Torsion Subgroup

Producing a lower bound for the order of the torsion subgroup is more subtle than the upper bound. We start by the following

Definition 5.1.11. The *rational cuspidal subgroup* C is defined as the subgroup of $J_0(N)(\mathbb{Q})_{\text{tors}}$, generated by the divisors of the form $(\alpha) - (\infty)$, where α is a rational cusp for $\Gamma_0(N)$ (recall that a divisor is called $\mathbb{Q}$-rational if it is fixed by the action of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$).[3]

Introducing the group C is very useful for our purposes, since the size of its image in $A(\mathbb{Q})_{\text{tors}}$ produces a divisor of the order of the torsion subgroup.

We compute a list of cusp representatives for all the cusps for $\Gamma_0(N)$, using the following

Proposition 5.1.12. *Let $\alpha_1 = \dfrac{p_1}{q_1}$ and $\alpha_2 = \dfrac{p_2}{q_2}$ be two cusps, written in lowest terms. Then $\alpha_1 \sim \alpha_2$ modulo the action of $\Gamma_0(N)$ if and only if*

$$q_2 \equiv uq_1 \ (modN), \ \textit{and}\ up_2 \equiv p_1 \ (mod\ (q_1, N)), \ \textit{for some}\ u, \ (u, N) = 1$$

Proof. Suppose that there is a matrix $M \in \Gamma_0(N)$, such that $M\alpha_1 = \alpha_2$. If $M = \begin{bmatrix} a & b \\ Nc & d \end{bmatrix}$, then $\dfrac{p_2}{q_2} = \dfrac{ap_1 + bq_1}{Ncp_1 + dq_1}$. Since $(ap_1 + bq_1, Ncp_1 + dq_1) = 1$, then it follows that $q_2 = \pm(Ncp_1 + dq_1)$ and $p_2 = \pm(ap_1 + bq_1)$. Hence, we can choose $u = \pm d$ and we get precisely the desired condition.

Conversely, suppose that α_1 and α_2 satisfy the condition. First, choose $s_1', r_1', s_2, r_2 \in \mathbb{Z}$, such that $p_1 s_1' - q_1 r_1' = p_2 s_2 - q_2 r_2 = 1$. Since $q_2 \equiv uq_1 \pmod N$, then $(q_1, N) = (q_2, N) = N_0$. We have $up_2 \equiv p_1 \pmod{N_0}$ which implies that $us_1' \equiv s_2 \pmod{N_0}$. Thus, we can find $x \in \mathbb{Z}$, such that $uxq_1 \equiv us_1' - s_2 \pmod N$. If we set $s_1 = s_1' - xq_1$ and $r_1 = r_1' - xp_1$, then $p_1 s_1 - q_1 r_1 = 1$, $us_1 \equiv s_2 \pmod N$ and $uq_1 \equiv q_2 \pmod N$. Finally, look at the matrices $M_1 = \begin{bmatrix} p_1 & r_1 \\ q_1 & s_1 \end{bmatrix}$ and $M_2 = \begin{bmatrix} p_2 & r_2 \\ s_2 & q_2 \end{bmatrix}$. Since $M_1 M_2^{-1} \in \Gamma_0(N)$ if and only if $s_1 q_2 \equiv s_2 q_1 \pmod N$, then we obtain easily that there is a matrix $M \in \Gamma_0(N)$, such that $M\alpha_1 = \alpha_2$, i.e. the cusps α_1 and α_2 are $\Gamma_0(N)$-equivalent. □

Next, we compute a sublist of all $\mathbb{Q}$-rational cusps. This can be done, provided we know the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the cusps for $\Gamma_0(N)$. Computing this action is possible and is done by G. Stevens [26, Thm. 1.3.1]. The essential result is contained in the following proposition:

[3] The definition we present is not the standard definition of the rational cuspidal subgroup. The standard definition of the rational cuspidal subgroup is the subgroup of the group of cuspidal divisors, which is fixed by $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Proposition 5.1.13. *(i) The cusps of $X_0(N)$ are rational over $\mathbb{Q}(\zeta_N)$ (i.e. they are fixed by the elements of Gal$(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_N))$).*
(ii) The absolute Galois group Gal$(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the cusps for $\Gamma_0(N)$ through the subgroup Gal$(\mathbb{Q}(\zeta_N)/\mathbb{Q}) = (\mathbb{Z}/N\mathbb{Z})^\times$. The element $d \in (\mathbb{Z}/N\mathbb{Z})^\times$ acts on the cusp representative x/y by $x/y \mapsto x/(d'y)$, where d' is the multiplicative inverse of d in $(\mathbb{Z}/N\mathbb{Z})^\times$, i.e. $dd' \equiv 1 \pmod N$.

We can compute the subgroup $\mathcal{C}$ of the space of modular symbols of weight 2 for $\Gamma_0(N)$, generated by the rational cusps. In other words, $\mathcal{C}$ is the space of all symbols $\{\alpha, \infty\}$, where α is a $\mathbb{Q}$-rational cusp. It follows from Abel-Jacobi's theorems that the image of C in $A_f(\mathbb{Q})_{\text{tors}}$ is isomorphic to the image of $\mathcal{C}$ in the quotient group

$$P := \Phi_f(H_1(X_0(N), \mathbb{P}^1(\mathbb{Q}); \mathbb{Z}))/\Phi_f(H_1(X_0(N); \mathbb{Z})),$$

where Φ_f is the integration pairing, defined by

$$\Phi_f : H_1(X_0(N), \mathbb{P}^1(\mathbb{Q}); \mathbb{Z}) \to H_1(X_0(N); \mathbb{Z}),\ \{\alpha, \beta\} \mapsto \left\{ f \mapsto \int_\gamma f \right\},$$

where γ is a path, representing the homology class $\{\alpha, \beta\}$.

5.1.5 Computation of the Tamagawa Numbers

Let A be an abelian variety over a number field K and let $\mathcal{A}$ be its Néron model. The closed fiber of the Néron model at a place ν is a commutative group scheme, which we denote by $\mathcal{A}_{k_\nu}$ (k_ν denotes the residue field at ν). This scheme is not necessarily connected, so we will denote by $\mathcal{A}^0_{k_\nu}$ the connected component of the identity.

Definition 5.1.14. The component group of $\mathcal{A}$ at ν is a finite flat group scheme $\Phi_{A,\nu}$, such that the following sequence is exact

$$0 \to \mathcal{A}^0_{k_\nu} \to \mathcal{A}_{k_\nu} \to \Phi_{A,\nu} \to 0$$

The order $c_{A,\nu}$ of the group of k_ν-rational points on the component group $\Phi_{A,\nu}$ is called the *Tamagawa number* of A at ν. In other words, $c_{A,\nu} = |\Phi_{A,\nu}(k_\nu)|$.

Remark 5.1.15. If A has nonsingular reduction at ν then $c_{A,\nu} = 1$, because $\mathcal{A}_{k_\nu}$ in this case is connected.

There is no general algorithm to compute the Tamagawa numbers. There exists, however, an algorithm for the case of elliptic curves and it is known as Tate's algorithm. We do not present the technical details of the algorithm, since such a presentation would be much longer than the whole chapter. A detailed exposition of this algorithm is given in [27] or [24, IV.§9].

For the case of modular abelian varieties over $\mathbb{Q}$, there is a known algorithm to compute $|\Phi_{A,p}(\overline{\mathbb{F}}_p)|$ in the case when $p \parallel N$ [6]. Furthermore, it is possible to compute $|\Phi_{A,p}(\mathbb{F}_p)|$ up to power of 2 [13]. Computing $c_{A,p}$ in general is still an open problem.

5.1.6 Computing the L-Ratio

To motivate the definition and the interpretation of the L-Ratio, we start with the simpler case of an elliptic curves.

First, suppose that $f \in S_2(\Gamma_0(N))$ is a newform. The L-function $L(f,s)$, associated to f is defined via the Mellin transform

$$L(f,s) := (2\pi)^s \Gamma(s) \int_0^{i\infty} (-iz)^s f(z) \frac{dz}{z}.$$

It is not hard to check (by using the Fourier expansion $f = \sum_{n=1}^{\infty} a_n q^n$) that

$$L(f,s) = \sum_{n=0}^{\infty} \frac{a_n}{n^s}.$$

Next, we look at the special value of the L-function at $s = 1$.

$$L(f,1) = -2\pi i \int_0^{i\infty} f(z)dz = -\langle \{0,\infty\}, f \rangle,$$

where

$$\langle , \rangle : H_1(X_0(N), \mathbb{P}^1(\mathbb{Q}); \mathbb{Z}) \times S_2(\Gamma_0(N)) \to \mathbb{C}$$

is the integration pairing, defined by $\langle [\gamma], f \rangle = 2\pi i \displaystyle\int_\gamma f(z)dz$.

Since the modular symbols $\{0,\infty\}$ is in the rational homology of the curve $X_0(N)$, then $\langle \{0,\infty\}, f \rangle$ is a rational multiple of a period of f. To compute that rational multiple, we use the Hecke operator T_p on modular symbols. Indeed, we have

$$T_p\{0,\infty\} = \{0,\infty\} + \sum_{k=0}^{p-1} \{k/p, \infty\} = (1+p)\{0,\infty\} + \sum_{k=0}^{p-1} \{0, k/p\}.$$

But whenever $p \nmid N$, the symbol $\{0, k/p\}$ is integral, i.e. $\{0, k/p\} \in H_1(X_0(N), \mathbb{Z})$. Thus, $\displaystyle\sum_{k=0}^{p-1} \langle \{k/p, 0\}, f \rangle$ is a period of the modular form f. Another observation is that it is a real period. Indeed,

$$\overline{\langle \{0, k/p\}, f \rangle} = -\langle \{0, k/p\}, f \rangle = \langle \{0, (p-k)/p\}, f \rangle,$$

so after summing all the contribution, we see that the period $\left\langle \displaystyle\sum_{k=0}^{p-1} \{k/p, \infty\}, f \right\rangle$ is real. Now, let $\Omega(f)$ be twice the minimal real part of a period of the lattice. Then

$$\frac{L(f,1)}{\Omega(f)} = \frac{n(p,f)}{2(1+p-a_p)},$$

where $n(p,f)$ is an integer.

For the general case, suppose that $A = A_f$ is a modular abelian variety, attached to a newform f. We want to be able to measure the *volume* of $A(\mathbb{R})$, which will be called *the real volume* and denoted by Ω_A.

To define this notion precisely, let $\mathcal{A}$ be the Néron model for A and $\mathcal{A}_{\mathbb{R}}$ be the generic fiber of $\mathcal{A}$. Consider the space of Néron differentials $H^0(\mathcal{A}, \Omega^1_{\mathcal{A}/\mathbb{Z}})$ and the real vector space

$$V^* = H^0(A_{\mathbb{R}}, \Omega^1_{A_{\mathbb{R}}}) = S_2(\Gamma_0(N), \mathbb{R})[I_f].$$

Indeed, the last identification is a consequence of the definition of A_f is the quotient $J_0(N)/I_f J_0(N)$.

Definition 5.1.16. Suppose that Λ and Λ' are lattices in a real vector space V. The *lattice index* $[\Lambda : \Lambda']$ is defined to be the determinant of the linear transformation of V, which takes Λ to Λ'.

Let Λ^* be the lattice defined by the Néron differentials $H^0(\mathcal{A}, \Omega^1_{\mathcal{A}/\mathbb{Z}})$ in the cotangent space V^*. The dual lattice $\Lambda = \mathrm{Hom}(\Lambda^*, \mathbb{Z})$ is a lattice in the tangent space $V = \mathrm{Hom}(V^*, \mathbb{R})$. We can declare that the real torus V/Λ has measure 1. Since $A(\mathbb{R})^0 = V/H_1(A(R), \mathbb{Z})$, then we can define the volume of $A(\mathbb{R})^0$ using the lattice index $[\Lambda : H_1(A(\mathbb{R}), \mathbb{Z})]$. We write this as

$$\mu_\Lambda(A(\mathbb{R})^0) = [\Lambda : H_1(A(\mathbb{R}); \mathbb{Z})].$$

Since our goal is to measure the volume of $A(\mathbb{R})$, we can use the index $c_\infty = |A(\mathbb{R})/A(\mathbb{R})^0|$ to define

$$\mu_\Lambda(A(\mathbb{R})) = c_\infty \cdot \mu_\Lambda(A(\mathbb{R})^0).$$

Finally, we declare this induced measure $\mu_\Lambda(A(\mathbb{R}))$ to be the real volume Ω_A.

We will be concerned with the computation of the L-ratio, which is $\dfrac{L(A,1)}{\Omega_A}$. It turns out that it is easier to compute the ratio $c_A \cdot L(A,1)/\Omega_A$, where c_A is a special constant, which is known as the Manin constant and is defined as follows

Definition 5.1.17 (Manin Constant). Consider $H^0(\mathcal{A}, \Omega^1_{\mathcal{A}})$ as a submodule of $S_2(\Gamma_0(N), \mathbb{Z})[I_f]$, using

$$H^0(\mathcal{A}, \Omega^1_{\mathcal{A}}) \to H^0(\mathcal{J}, \Omega^1_{\mathcal{J}})[I_f] \to H^0(J_0(N), \Omega^1_{J_0(N)})[I_f] \to S_2(\Gamma_0(N), \mathbb{Z})[I_f],$$

where $\mathcal{J}$ is the Néron model for the Jacobian $J_0(N)$. The Manin constant c_A is defined as

$$c_A = \left| \frac{S_2(\Gamma_0(N), \mathbb{Z})[I_f]}{H^0(\mathcal{A}, \Omega_{\mathcal{A}/\mathbb{Z}})} \right|.$$

There are various results and conjectures about the constant c_A. One result, which will be used in the computations is the following theorem due to B. Mazur [15, §4]

Theorem 5.1.18 (Mazur). *Let p be a prime, such that $p \mid c_A$. Then $p^2 \mid 4N$.*

We will now state the result that allows us to compute the ratio $c_A \cdot \dfrac{L(A,1)}{\Omega_A^1}$.

Theorem 5.1.19. *Let*

$$\Phi : H_1(X_0(N);\mathbb{Q}) \to Hom(S_2(\Gamma_0(N))[I_f],\mathbb{C})$$

be a pairing, obtained from the integration pairing in such a way that $\Phi(\langle 0,\infty\rangle)(f) = L(f,1)$ (as we discussed above, the fact that $\langle 0,\infty\rangle \in H_1(X_0(N),\mathbb{Q})$ follows from the Manin-Drinfeld theorem). Then

$$c_\infty \cdot c_A \cdot \frac{L(A,1)}{\Omega_A} = [\Phi(H_1(X_0(N);\mathbb{Z}))^+ : \Phi(\mathbb{T}\langle 0,\infty\rangle)],$$

where by $\Phi(H_1(X_0(N);\mathbb{Z}))^+$ we mean the positive eigenspace of $Hom(S_2(\Gamma_0(N))[I_f],\mathbb{C})$ with respect to the complex conjugation operator.

The theorem is proved in [1, Thm. 4.5].

5.2 Examples of Visible Elements.

5.2.1 A 20-Dimensional Quotient of $J_0(389)$.

For the purpose of this section, we will be working with the modular Jacobian $J_0(389)$. For clarity, we describe each step of our computation separately.

Step 1: *Decomposing the Jacobian $J_0(389)$ as a product of abelian varieties.*
Consider the cuspidal subspace $S_2(\Gamma_0(389))$. One can use the correspondence between Galois conjugacy classes of newforms and modular abelian varieties, attached to newforms (quotients of $J_0(389)$) to decompose $J_0(389)$ as a product of modular abelian varieties. Using the modular symbols package of the computer algebra system MAGMA, we decompose the new subspace of the cuspidal subspace $S_2(\Gamma_0(389))$ into Galois conjugacy classes. There are five abelian varieties in the decomposition of dimensions 1, 2, 3, 6, 20, which we denote by $A_1, A_2, A_3, A_6, A_{20}$ respectively.

Step 2: *Computing the L-ratio's for the quotients.*
We can apply the algorithm for computing the L-ratio from Section 5.1.6, to verify that $L(A_1,1) = L(A_2,1) = L(A_3,1) = L(A_6,1) = 0$, but $L(A_{20},1) \neq 0$. More precisely, the algorithm, applied to A_{20} gives us

$$\frac{L(A_{20},1)}{\Omega_A} = c_A \cdot \frac{2^{11}\cdot 5^2}{97},$$

where c_A is the Manin constant. But according to Mazur's theorem (Theorem 5.1.16), the Manin constant is $c_A = 2^?$. Moreover, the techniques from [2] produce an upper bound on c_A, i.e. $c_A \leq 2^{20}$. Thus, we recover that

$$\frac{L(A_{20},1)}{\Omega_A} = \frac{2^{11+n} \cdot 5^2}{97},$$

where $0 \leq n \leq 20$.

Step 3: *Computing the modular degree for A_{20}.*
We run the algorithm from section 5.1.1 for the variety A_{20} to compute the kernel of the isogeny $\theta : A_{20}^\vee \to A_{20}$. We obtain $|\ker(\theta)| = 2^{24} \cdot 5^2$.
Computing this kernel is really important for what will follow, because it tells use precisely the primes, for which one can hope to apply the visibility theorem. In this case, the only such prime is $p = 5$.

Step 4: *Computing torsion bounds for A_1 and A_{20}* We use the algorithm from section 5.1.3 to produce upper bounds on the torsion subgroups of A_1 and A_{20}. This computation automatically produces bounds for the order of $A_{20}^\vee(\mathbb{Q})_{\mathrm{tors}}$. This follows from the more general result

Lemma 5.2.1. *Suppose A and B are isogenous abelian varieties. Then the upper bounds for $|A(\mathbb{Q})_{tors}|$ and $|B(\mathbb{Q})_{tors}|$, produced in 5.1.3 are the same. In other words, the upper bounds, produced by the algorithm in 5.1.3 are isogeny invariant.*

Proof. The upper bounds that are produced by algorithm in 5.1.3 depend only on the characteristic polynomial of Frobenius on the ℓ-adic Tate modules $T_\ell A$ and $T_\ell B$. The characteristic polynomials are then determined by $T_\ell A \otimes \mathbb{Q}$ and $T_\ell B \otimes \mathbb{Q}$ respectively. But $T_\ell A \otimes \mathbb{Q} \cong T_\ell B \otimes \mathbb{Q}$, since A and B are isogenous. Hence, the upper bounds are isogeny invariant. □

Next, we can compute the bounds on the order of the torsion subgroup $A_{20}(\mathbb{Q})_{\mathrm{tors}}$. For the upper bound, we try only the primes 3 and 5 to get a bound 97. For the lower bound, we compute the rational cuspidal subgroup, which turns out to be cyclic of order 97. Therefore $|A_{20}(\mathbb{Q})_{\mathrm{tors}}| = |A_{20}^\vee(\mathbb{Q})_{\mathrm{tors}}| = 97$. The algorithm applied for A_1 gives us upper bound 1, and so $|A_1(\mathbb{Q})_{\mathrm{tors}}| = 1$.

Step 5: *Computing Tamagawa Numbers*
Using Tate's algorithm, we compute $c_{A_1,389} = 1$. For A_{20}, we can use the algorithm in [6] to get $c_{A_{20},389} = 97$.

Step 6: *Theorem 4.5.1 for $A = A_{20}^\vee$, $B = A_1$, $J = A + B$ and $p = 5$.*
We will apply the visibility theorem (Theorem 4.5.1) for the abelian variety $A = A_{20}^\vee \subset J_0(N)$ and the elliptic curve $B = A_1 = A_1^\vee \subset J_0(N)$. Let J be the variety $J =$

$A+B$ and $p=5$. We need to check the hypothesis of the theorem. Using the algorithm from Section 5.1.2 we compute $A \cap B = (\mathbb{Z}/20\mathbb{Z}) \times (\mathbb{Z}/20\mathbb{Z})$, which implies that $B[5] \subset A(\overline{\mathbb{Q}})$. In order to apply the visibility theorem for $p=5$, we need to prove that $5 \nmid |B(\mathbb{Q})_{\text{tors}}| \cdot |(J/B)(\mathbb{Q})_{\text{tors}}|$. But $|B(\mathbb{Q})_{\text{tors}}| = 1$. Since A is isogenous to J/B and the kernel of that isogeny is $A \cap B = (\mathbb{Z}/20\mathbb{Z}) \times (\mathbb{Z}/20\mathbb{Z})$, then $|(J/B)(\mathbb{Q})_{\text{tors}}| = |A_{20}^{\vee}(\mathbb{Q})_{\text{tors}}| = 97$. Therefore, $5 \nmid |B(\mathbb{Q})_{\text{tors}}| \cdot |(J/B)(\mathbb{Q})_{\text{tors}}| \cdot c_{A,389} \cdot c_{B,389}$, so we can apply the visibility theorem and get an injection $B(\mathbb{Q})/5B(\mathbb{Q}) \hookrightarrow Ш(A_{20}^{\vee})$. (because A has Mordell-Weil rank zero).

Step 7: *Evidence for the Birch and Swinnerton-Dyer conjecture for* $A_{20}^{\vee}$
The Birch and Swinnerton-Dyer conjecture states that

$$\frac{L(A,1)}{\Omega_A} = \frac{|Ш(A)| \cdot \prod_{p|N} c_{A,p}}{|A(\mathbb{Q})_{\text{tors}}| \cdot |A^{\vee}(\mathbb{Q})_{\text{tors}}|}.$$

We have everything computed precisely, except the Manin constant. We can therefore compute the conjectural order of $Ш(A_{18}^{\vee}/\mathbb{Q})$, because

$$\frac{2^n \cdot 2^1 1 \cdot 5^2}{97} = \frac{97 \cdot |Ш(A/\mathbb{Q})|}{97^2}.$$

Thus, $|Ш(A_{18}^{\vee}/\mathbb{Q})| = 2^{11+n} \cdot 5^2$. Using the injection from Step 6, we get $5^2 | |Ш(A_{18}^{\vee}/\mathbb{Q})|$, which provides evidence for the Birch and Swinnerton-Dyer conjecture.

5.2.2 Evidence for the Birch and Swinnerton-Dyer Conjecture for an 18-Dimensional Quotient of $J_0(551)$.

In this section, we will look at $J_0(551)$. This example is interesting, because the visibility theorem cannot be applied directly, but one needs to embed the variety into a modular Jacobian of level, which is a multiple of 551. Again, for clarity, we sketch the different steps of the computations.

Step 1: *Decomposing the Jacobian* $J_0(389)$ *as a product of abelian varieties.*
Similarly to the case of $J_0(389)$, we compute the newform quotients of $J_0(551)$. There are four elliptic curves E_1, E_2, E_3 and E_4, and abelian varieties A_2, A_3, A_{16} and A_{18} of dimensions 2, 3, 16 and 18. We will be interested in studying the 18-dimensional quotient A_{18}.

Step 2: *Computing the modular degree for* A_{20}.
Let $\theta : A_{18}^{\vee} \to A_{18}$. Using the algorithm from 5.1.1, the modular kernel has order $|\ker(\theta)| = 2^{14} \cdot 13^4$. This shows that the only odd prime p, for which one might get visible elements of $Ш(A_{18}^{\vee})$ in $J_0(551)$ of order p is $p = 13$.

Step 3: *Computing the multiple and the divisor of* $A_{18}(\mathbb{Q})_{tors}$.
The algorithm for the upper bound gives us $|A_{18}(\mathbb{Q})_{\text{tors}}|$ divides 80. The order of

the rational cuspidal subgroup is 40. Therefore, $|A_{18}(\mathbb{Q})_{\mathrm{tors}}| = 40$ or 80. Notice that the order of the modular kernel is not divisible by 5, i.e. the degree of the isogeny $\theta : A_{18}^{\vee} \to A_{18}$ is not divisible by 5. Therefore, the order of the torsion subgroup $|A_{18}^{\vee}(\mathbb{Q})_{\mathrm{tors}}|$ must necessarily be divisible by 5. Thus, we obtain that $5 \mid |A_{18}^{\vee}(\mathbb{Q})_{\mathrm{tors}}| \mid 80$.

Step 4: *Computing the Tamagawa Numbers.*
The most difficult part is to compute the Tamagawa numbers for the abelian variety A_{18}. We can use the techniques from [6]. Since $551 = 19 \cdot 29$ then we need to compute $c_{A_{18},19}$ and $c_{A_{18},29}$. The second number is $c_{A_{18},29} = 40$, but the algorithm does not work for the first one. Instead, we compute the order of the component group order over $\overline{\mathbb{F}}_{19}$, which is $2^2 \cdot 13^2$ and conclude that $c_{A_{18},19} = 2$ or 4 by noting that the Galois generator Frob_{19} acts as -1 (we can verify this in MAGMA using the Atkin-Lehner operator; indeed, Frob_{19} acts on the component group $\Phi_{A,19}(\mathbb{F}_{19})$, so every element of that group must have order 2).

Step 5: *Computing the L-ratio.*
Using the algorithm from 5.1.6, we compute

$$\frac{L(A_{18},1)}{\Omega_{A_{18}}} = c_A \cdot \frac{2^2 \cdot 3^2}{5}.$$

Since $c_A \mid 2^{\dim(A)}$ by [2], then it follows that

$$\frac{L(A_{18},1)}{\Omega_{A_{18}}} = \frac{2^{n+2} \cdot 3^2}{5},$$

for some $0 \le n \le 18$.

Step 6: *Conjectural order of* $\text{Ш}(A_{18}/\mathbb{Q})$
We have all the quantities for the strong Birch and Swinnerton-Dyer conjecture, so we obtain

$$\frac{2^{n+2} \cdot 3^2}{5} = \frac{|\text{Ш}(A_{18}/\mathbb{Q})| \cdot 2^m \cdot (2^3 \cdot 5)}{(2^k \cdot 5) \cdot (2^l \cdot 5)},$$

where $1 \le m \le 2$, $3 \le k \le 4$ and $0 \le l \le 4$. Thus, it follows that $|\text{Ш}(A_{18})| = 2^s \cdot 3^2$ for some $2 \le s \le 24$, so there is no chance to get visible elements for A_{18} inside $J_0(551)$.

We saw that the conjectural order of $\text{Ш}(A_{18}/\mathbb{Q})$ is divisible by 3^2. Although we produced no visible elements, there is a way of proving that $\text{Ш}(A_{18})$ has a subgroup of order 9 by using the following algorithm:

1. Let A be a quotient of $J_0(N)$. Choose a prime number $\ell \nmid N$ and consider the degeneracy maps $\alpha^*, \beta^* : J_0(N) \to J_0(\ell N)$.

2. By Shimura's construction, $A^\vee$ is a subvariety of $J_0(N)$, so we can consider its image in $J_0(\ell N)$ under a linear combination of the degeneracy maps. For instance, look at $C = \alpha^*(A^\vee) + \beta^*(A^\vee)$.

3. Compute explicitely (using modular symbols) the image of the variety $A_{18}^\vee$ in $J_0(\ell N)$.

4. If possible, apply the visibility theorem for C (or some other technique) to prove that C contains a subgroup of the form $B(\mathbb{Q})/pB(\mathbb{Q})$ for some abelian variety B.

5. To prove that $Ш(A)$ has element, whose order is divisible by p, it suffices to show that the degree of the isogeny, which is the composition of the maps

$$A \to A^\vee \to A^\vee \times A^\vee \xrightarrow{\alpha^*+\beta^*} C$$

is not divisible by p (and then to perform analysis on the cochain level to show that the kernel of $Ш(A) \to Ш(C)$ does not have an element of order p). This can be done by noting that the kernel is annihilated by the operators $T_r|_A - (r+1)$ for all primes $r \nmid N$, so it suffices to show that the order of the kernel of some of these operators is not divisible by p.

To justify the last step of the above algorithm, we use a result due to K. Ribet.

Theorem 5.2.2 (Ribet). *(i) Let $\ell \nmid N$ be a prime number. Consider the two degeneracy maps (which we constructed in Chapter 3) $\alpha^*, \beta^* : J_0(N) \to J_0(\ell N)$ and let $\varphi : J_0(N) \times J_0(N) \to J_0(\ell N)$ be the map $\varphi = (\alpha^*, \beta^*)$. Let Σ_N be the kernel of the map $J_0(N) \to J_1(N)$ induced from the covering of modular curves $X_1(N) \to X_0(N)$. Consider the image Σ of Σ_N in $J_0(N) \times J_0(N)$ under the anti-diagonal map $J_0(N) \to J_0(N) \times J_0(\ell N)$ (i.e. the map $x \mapsto (x, -x)$). Then*

$$\Sigma = ker(\varphi).$$

(ii) The subgroup Σ_N (known also as the Shimura subgroup) is annihilated by the endomorphisms $\eta_r = T_r - (r+1)$ of $J_0(N)$ for all primes r which do not divide N.

The statement is proved in [21]. The second part of the theorem is useful for computational purposes. Indeed, note that it is difficult to compute the Shimura subgroup Σ_N, but computing the order of the kernel of the operator $T_r - (r+1)$ is not a problem at all. Since all we need out of this theorem is to show that the prime p do not divide the order of the Shimura subgroup, then it would suffice to check that p do not divide the order of the kernel of η_r.

To illustrate the above algorithm in practice, we choose the prime $\ell = 2$. By decomposing the modular Jacobian $J_0(2 \cdot 551)$ as a product of quotients, we notice that five of the factors are elliptic curves, one of which is the rank 2 elliptic curve E with Weierstrass equation

$$E : y^2 + xy = x^3 + x^2 - 29x + 61.$$

Let C be the image of A_{18} under the composition

$$A_{18} \to A_{18}^{\vee} \hookrightarrow J_0(551) \xrightarrow{\alpha^*+\beta^*} J_0(2 \cdot 551)$$

We can use the techniques from Section 5.1.2 to compute the intersection of E with C and verify that C contains $E[3]$. We wish to apply the visibility theorem for $A = C$ and $B = E$ and $p = 3$. Indeed, the only hypothesis that we have to check is that the Tamagawa numbers for B are not divisible by 3. But Tate's algorithm [27] computes these numbers for elliptic curves. Using this algorithm, one checks that $c_{B,2} = 2$, $c_{B,19} = 2$ and $c_{B,29} = 1$ and we already computed (up to power of 2) those for A. Since the Mordell-Weil rank of C is zero, then there is an injection

$$B(\mathbb{Q})/3B(\mathbb{Q}) \hookrightarrow Ш(C).$$

Finally, we need to check that the degree of the above isogeny $\varphi : A \to C$ is not divisible by 3. To do this, we first compute the kernel of the operator $T_3|_A - (3+1)$. It is possible to perform the last step in practice, because one knows precisely how the Hecke operator acts on the space of modular symbols. The kernel is

$$\ker(T_3|_A - (3+1)) = 126258124029988886400 = 2^{14} \cdot 5^2 \cdot 5552003^2,$$

which is not divisible by 3. Therefore, by Ribet's theorem 3 does not divide the order of the kernel of the isogeny $A_{18} \to C$, so $Ш(A_{18})$ contains an element of order 3, which provides evidence for the Birch and Swinnerton-Dyer conjecture.

Conjectures

The various theorems and examples that we presented illustrate that looking at *visible elements* might be useful for a better understanding of the Shafarevich-Tate group, since rational points on abelian varieties are much easier to understand than cohomology classes.

The visualization theorem, together with the various interesting examples might serve as a good motivation for the following question

Question 1. If A is an abelian variety over K, does there exists a variety J and an embedding $i : A \hookrightarrow J$, such that the whole Shafarevich-Tate group becomes visible, i.e.

$$\mathrm{Vis}_J^{(i)}(Ш(A/K)) = Ш(A/K)?$$

The above question is too general and it is likely that the answer might be negative. However, if we specialize the question to subvarieties of modular Jacobians $J_0(N)$, the level-raising example generates the following question

Question 2. If A is an abelian variety over $\mathbb{Q}$, whose dual is an optimal quotient of $J_0(N)$ (hence A is a subvariety of $J_0(N)$), does there exists $M \in \mathbb{N}$ and a linear combination of degeneracy map $J_0(N) \to J_0(MN)$ [4], such that every element of A becomes visible in $J_0(MN)$, i.e.

$$\mathrm{Vis}_{J_0(MN)}(Ш(A/\mathbb{Q})) = Ш(A/\mathbb{Q})?$$

Why should one even bother to ask these questions? Indeed, there is a very subtle connection between visualizing elements of the Shafarevich-Tate group and what is called *capitulation* of ideal classes.

In fact, suppose that L/K is an extension of number fields and consider the kernel of the natural map $C_K \to C_L$ between the ideal class groups of K and L. The elements of the kernel are those ideal classes of $\mathcal{O}_K$, which become trivial in $\mathcal{O}_L$ (we say that these ideal classes capitulate in C_L). In some sense, capitulation is the analogue of visibility for ideal classes. Class field theory tells us that there exists a Hilbert class field H/K, in which all ideal classes of K become trivial, i.e.

[4] Note that we allow this map to have a kernel - recall that the general definition of visibility did not require that A is embedded in J.

the whole ideal class group C_K capitulates in C_H. It is natural to ask the following

Question 3. Is there some analogue of the Hilbert class field H/K for the case of abelian varieties?

Since abelian varieties are in some sense much more difficult to work with than ideal classes, it might be impossible to answer the above question, or it might as well be that the general answer is negative. However, the connection between *capitulation* and *visibility* might be interesting to study and understand better.

Bibliography

[1] A. Agashe and W. A. Stein, *Visible Evidence for the Birch and Swinnerton-Dyer Conjecture for Modular Abelian Varieties of Analytic Rank* 0, To appear in Math. of Computation.

[2] ______, *The manin constant, congruence primes, and the modular degree*, Preprint,
`http://modular.fas.harvard.edu/papers/manin-agashe/` (2004).

[3] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, Springer-Verlag, Berlin, 1990.

[4] J. W. S. Cassels, *Lectures on elliptic curves*, Cambridge University Press, Cambridge, 1991.

[5] J. W. S. Cassels and A. Fröhlich (eds.), *Algebraic number theory*, London, Academic Press Inc. [Harcourt Brace Jovanovich Publishers], 1986, Reprint of the 1967 original.

[6] Brian Conrad and William A. Stein, *Component groups of purely toric quotients*, Math. Res. Lett. **8** (2001), no. 5-6, 745–766. MR 2003f:11087

[7] J. E. Cremona and B. Mazur, *Visualizing elements in the Shafarevich-Tate group*, Experiment. Math. **9** (2000), no. 1, 13–28. MR 1 758 797

[8] A. Grothendieck, *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. II*, Inst. Hautes Études Sci. Publ. Math. (1965), no. 24, 231. MR 33 #7330

[9] ______, *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. III*, Inst. Hautes Études Sci. Publ. Math. (1966), no. 28, 255. MR 36 #178

[10] ______, *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas IV*, Inst. Hautes Études Sci. Publ. Math. (1967), no. 32, 361. MR 39 #220

[11] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52.

[12] N. M. Katz, *Galois properties of torsion points on abelian varieties*, Invent. Math. **62** (1981), no. 3, 481–502. MR 82d:14025

[13] D. R. Kohel and W. A. Stein, *Component Groups of Quotients of $J_0(N)$*, Proceedings of the 4th International Symposium (ANTS-IV), Leiden, Netherlands, July 2–7, 2000 (Berlin), Springer, 2000.

[14] S. Lang, *Algebraic number theory*, second ed., Springer-Verlag, New York, 1994.

[15] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162.

[16] J. S. Milne, *Abelian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 103–150.

[17] ______, *Arithmetic duality theorems*, Academic Press Inc., Boston, Mass., 1986.

[18] ______, *Jacobian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 167–212.

[19] D. Mumford, *Abelian varieties*, Published for the Tata Institute of Fundamental Research, Bombay, 1970, Tata Institute of Fundamental Research Studies in Mathematics, No. 5.

[20] ———, *Curves and their jacobians*, Ann Arbor, The University of Michigan Press, 1975.

[21] K. A. Ribet, *Raising the levels of modular representations*, Séminaire de Théorie des Nombres, Paris 1987–88, Birkhäuser Boston, Boston, MA, 1990, pp. 259–271.

[22] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton University Press, Princeton, NJ, 1994, Reprint of the 1971 original, Kan Memorial Lectures, 1.

[23] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1992, Corrected reprint of the 1986 original.

[24] ———, *Advanced topics in the arithmetic of elliptic curves*, Springer-Verlag, New York, 1994.

[25] W. A. Stein, *Explicit approaches to modular abelian varieties*, Ph.D. thesis, University of California, Berkeley (2000).

[26] G. Stevens, *Arithmetic on modular curves*, Birkhäuser Boston Inc., Boston, Mass., 1982. MR 87b:11050

[27] J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1975, pp. 33–52. Lecture Notes in Math., Vol. 476. MR 52 #13850