Università degli Studi di Padova

DIPARTIMENTO DI MATEMATICA "TULLIO LEVI-CIVITA"
Corso di Laurea Magistrale in Matematica

Abelian variety with Tate-Shafarevich group of non-square order

Candidato:
Daniele Troletti
Matricola 1176553

Relatore:
Remke Nanne Kloosterman

Anno Accademico 2018-2019
5 Luglio 2019

Contents

Introduction

One of the classical problem in mathematics was studying diophantine equations, i.e. polynomial equation in one or more variables with integer (or sometimes rational) coefficients. The aim was to find rational solution to these equations. First they wanted to know if there were rational solution at all. Then they wanted to find whether the number of solution was finite or infinite. Finally they aimed to find all the solutions if they were finite or an algorithm to produce all the infinite solutions.

The case of equations in one or two variables was thoroughly studied and understood by number theorists of the last three centuries. The next logical case to study was cubic equation in three variables. This started the research on elliptic curves. These researches were then extended to abelian varieties, which are objects that generalise the elliptic curves in higher dimension.

An abelian variety over a number field K is a projective variety with a group structure on its K-rational points. We denote by $A(K)$ the set of the K-rational points.

One of the most important theorem about the structure of $A(K)$ was conjectured by Poincaré in 1901 and proved later by Mordell and Weil: $A(K)$ is a finitely generated abelian group. So $A(K)$ is composed of a finite abelian group $A(K)_{tors}$ consisting of the torsion elements and a free group of rank r. This number r is called the Mordell-Weil rank, or arithmetic rank, or simply rank, of A. Even after more than 100 years of research the study of $A(K)$ is an active research area.

The proof of the Mordell-Weil theorem is not effective, meaning that it does not provide an algorithm to find the rank of A. An algorithm was developed but it is not even known whether it terminates or not. The reason is that the algorithm does not calculate the rank but only an upper bound. The difference between the upper bound and the rank is measured by the Tate-Shafarevich group $Ш(A/K)$, which is defined using Galois cohomology:

$$Ш(A/K) = \ker\left(H^1(K, A(\overline{K})) \longrightarrow \prod_{v \in M_K} H^1(K_v, A(\overline{K_v}))\right)$$

where M_K is the set of all places of K and K_v is the completion of K with respect to v.

The Tate-Shafarevich group is a very complicated object, even though it turns out that it is often the trivial group. From its definition one easily derives that it is an abelian torsion group.

The Tate-Shafarevich group comes with two very important conjectures. The first one says that the size of the Tate-Shafarevich group is always finite. This conjecture is known to hold true only in the case of elliptic curve of rank 0 or 1 thanks to the works of Kolyvagin, Wiles and others. The second conjecture concerning the Tate-Shafarevich group is the Birch and Swinnerton-Dyer conjecture. It describes a relationship between all the arithmetic and analytic invariants associated to an abelian variety, including the conjectured finiteness of its Tate-Shafarevich group. In 1974 Tate said about this conjecture: "this remarkable conjecture relates the behaviour of a function, L, at a point where it is not at present known to be defined to the order of a group, Ш, which is not known to be finite!". We now know that the L function is defined at that point but not whether the order of the group is finite in general.

When we consider an elliptic curve its Tate-Shafarevich group has square order due to a result of Cassels and Tate. They defined a bilinear pairing between the Tate-Shafarevich group of a variety A over K and that of the dual variety $A^\vee$:

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

Since elliptic curves are isomorphic to their dual variety and in this case the pairing is alternating, and so we find that if the group is finite then its order has to be a square. Following this results several mathematicians were mislead into believing that the order of the Tate-Shafarevich group of every abelian variety should have been a square but they were wrong.

In 1996 Michael Stoll constructed the first example of a variety whose Tate-Shafarevich group has order 2 times a square. He used the Jacobian of a genus 2 curve over $\mathbb{Q}$. Later works of William Stein and other provided more varieties of high dimension with this property. For every prime p Stein constructed a variety of dimension $p-1$ whose Tate-Shafarevich group has order p times a square. Stein had also conjectured that every square-free natural number should appear as the non-square factor of the order of the Tate-Shafarevich group of an abelian variety.

A useful tool to study the order of the Tate-Shafarevich group is an equation of Cassels and Tate. Given two abelian varieties A and B over K and an isogeny φ between them, the Cassels-Tate equation determines the

order of $Ш(A/K)$ relatively to the order of $Ш(B/K)$ in terms of the number of local and global points in the kernel and the cokernel of φ and global points in the kernel and the cokernel of $\varphi^\vee$. Let M_K define the set of all places of K, then

$$\frac{\#Ш(A/K)}{\#Ш(B/K)} = \frac{\#\ker\varphi_K}{\#\operatorname{coker}\varphi_K}\frac{\#\operatorname{coker}\varphi_K^\vee}{\#\ker\varphi_K^\vee}\prod_{v\in M_K}\frac{\#\operatorname{coker}\varphi_v}{\#\ker\varphi_v}$$

They discovered this relation during the proof of the invariance under isogeny of the Birch and Swinnerton-Dyer conjecture, i.e. if two abelian varieties are isogenous then if the conjecture holds true for one then it holds true also for the other one.

Using this technique Stefan Keil constructed some abelian surfaces isogenous to a product of two elliptic curves with Tate-Shafarevich group of order k times a square with $k \in \{2, 3, 5, 6, 7, 10, 13, 14\}$.

When classifying the elliptic curves with some special property up to isomorphism we encounter the so-called modular curve. They represent moduli space of these problems. In order to work with them we can also construct the modular curves as Riemann surfaces. They can be defined as the compactification of a quotient of the complex upper semi-plane $\{z \in \mathbb{C} | \Im(z) > 0\}$ by some subgroups of the linear group $SL_2(\mathbb{Z})$. In particular one of this problem is to classify elliptic curves with a point of exact order p up to isomorphism. This problem gives rise to the modular curve $X_1(p)$.

In this thesis we are exploring the possibility of finding new examples of abelian varieties with Tate-Shafarevich group of non-square order inspecting the modular Jacobian $J_1(p)$ of the modular curve $X_1(p)$ for the prime 13 and 17. We are going to take the quotient by a cyclic subgroup generated by a $\mathbb{Q}$-rational torsion point and analyse the resulting variety. This is interesting since it may provide further examples of abelian varieties with Tate-Shafarevich group of non-square order in low dimension. Many of the examples with high non-square factor in the order of the group have also high dimension.

After an introductory chapter where we fix the notation we define rigorously the Tate-Shafarevich group and prove some of its property in chapter 2. In chapter 3 we focus on the Cassels-Tate equation, analysing all parts of the quotient and providing the right tool to use in order to calculate it. In chapter 4 we introduce the modular curves and their Jacobians. In the last chapter we apply the theorems of the preceding ones in order to calculate the non-square part of the order of the Tate-Shafarevich group of the quotient of the modular Jacobian $J_1(p)$ by a cyclic subgroup generated by a $\mathbb{Q}$-rational torsion point.

Chapter 1

Abelian Variety

The simplest way to introduce abelian variety is as generalization of elliptic curves which allows higher dimension variety.

We start by fixing some basic definitions. A variety over a field K is a scheme of finite type over K, separated and geometrically integral, that is reduced and irreducible over $\overline{K}$. In particular, varieties are geometrically connected.

1.1 Definition

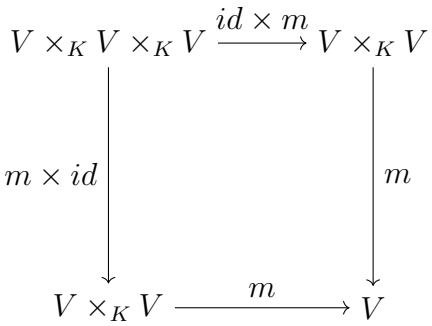
Let K be a field.

Definition 1.1.1. *A **group variety** over K is an algebraic variety V over K together with regular maps*

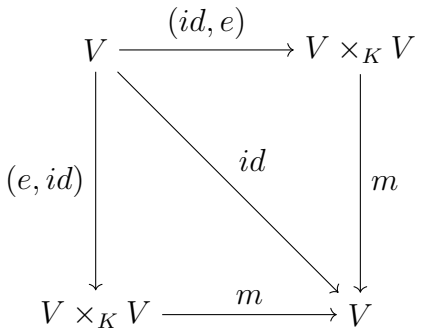
$$m\colon V \times_K V \to V \text{ (addition)}$$
$$inv\colon V \to V \text{ (inverse)}$$

and an element $e \in V(K)$ such that the structure on $V(\overline{K})$ defined by m and inv is a group with identity element e.

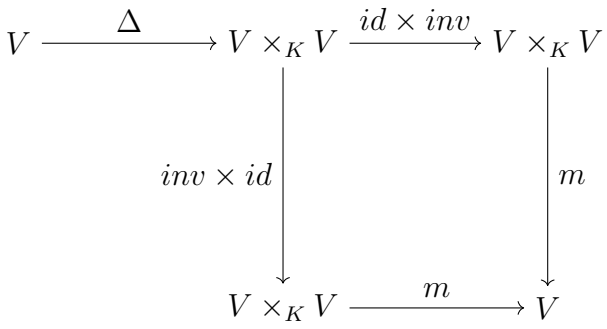
The following commutative diagrams encode this information about the maps. The map id is the identity and Δ is the diagonal immersion.



This is the associativity of the addition, the following is the property of the identity element e:



Last we have the inverse map. In the following diagram every element of the upper left V is mapped to e in the lower right V, so the map inv takes every element to its inverse with respect to m.



Proposition 1.1.2. *Every algebraic group is nonsingular.*

Proof. For any variety we can find an open dense subset U in which the variety is non singular. For every point a in the variety we can consider the translation isomorphism $t_a \colon P \mapsto m(P, a)$. Then the translates of U cover the whole variety, hence it is nonsingular. □

Definition 1.1.3. *A complete connected algebraic group is called an* ***abelian variety****.*

Remark. *A complete connected algebraic group is automatically projective. Moreover projectivity implies that the group law is commutative.*

1.2 Isogenies

Theorem 1.2.1 (Rigidity theorem)**.** *Let U, V and W be abelian varieties and $\alpha\colon U \times V \to W$ a regular map. If there exists points $u \in U$, $v \in V$ and $w \in W$ such that $\alpha(U \times \{v\}) = \alpha(\{u\} \times V) = \{w\}$ then $\alpha(U \times V) = \{w\}$.*

Proof. Since the hypothesis continue to hold after extending scalars from K to $\overline{K}$ we assume K to be algebraically closed.
Let W_0 be an open affine neighborhood of w. Since U is complete the projection map $q\colon U \times_K V \to V$ is closed and so the set $Z = q\left(\alpha^{-1}\left(W \backslash W_0\right)\right)$ is closed in V. This set consists of the second coordinates of points of $U \times V$ not mapping to W_0, so a point $v_0 \in V$ lies outside of Z if and only if $\alpha(U \times \{v_0\}) \subset W_0$. In particular v lies outside of Z and so $V \backslash Z$ is not empty. As $U \times \{v_0\}$ is isomorphic to U, it is complete and from the fact that W_0 is affine it follows that $\alpha(U \times \{v_0\})$ is a point when v_0 is not in Z (this holds because maps from a complete connected variety to an affine one have image equal to a point). Hence $\alpha(U \times \{v_0\}) = \alpha(u, v_0) = \{w\}$. Thus α is constant on the subset $U \times (V \backslash Z)$ of $U \times V$. This subset is non empty and open in the irreducible variety $U \times V$, hence it is dense. As W is separated then α must agree with the constant map on the whole $U \times V$. □

This theorem has an immediate implication on the structure of the maps between abelian varieties.

Corollary 1.2.2. *Let A and B be abelian varieties. Then every regular map $\alpha\colon A \to B$ is the composite of an homomorphism with a translation.*

Proof. The map α will send the identity element e_A of A to a K-rational element b of B. Hence after composing with a translation of $inv(b)$ we may assume that $\alpha(e_A) = e_B$, the identity element of B. Now we want to prove that α is an homomorphism. Consider the map

$$\begin{aligned} \phi\colon A \times A &\to B \\ (a, a') &\mapsto m(\alpha(m(a, a')), inv(m(\alpha(a), \alpha(a')))) \end{aligned}$$

This map is the difference of the two regular maps in the following diagram and so it is a regular map.

$$\begin{array}{ccc} A \times A & \xrightarrow{m} & A \\ {\scriptstyle (\alpha,\alpha)}\downarrow & & \downarrow{\scriptstyle \alpha} \\ B \times B & \xrightarrow{m} & B \end{array}$$

Then since $\phi(A \times \{e_A\}) = \phi(\{e_A\} \times A) = e_B$, by the rigidity theorem ϕ is the zero map. Hence α is an homomorphism. □

We are finally able to prove the following corollary.

Corollary 1.2.3. *The group law on an abelian variety is commutative.*

Proof. A group is abelian if and only if the inverse map is an homomorphism. Since the inverse map takes the identity element e to itself the previous corollary shows that it is an isomorphism. □

Since we have proved that every abelian variety is commutative from now on we will use the additive notation to write the group law (so $+_A$ for the operation and $-_A$ for the inverse) and will denote by 0_A the identity element of A. We will also drop the index whenever the variety is clear from the context.

Definition 1.2.4. *An **isogeny** is a surjective homomorphism of abelian varieties with finite kernel.*

Proposition 1.2.5. *Let $\alpha\colon A \to B$ be an homomorphism of abelian varieties, then the following are equivalent:*

1. *α is an isogeny;*
2. *$\dim A = \dim B$ and α is surjective;*
3. *$\dim A = \dim B$ and $\ker \alpha$ is finite.*

Proof. See [13, Proposition 7.1]. □

The **degree** of an isogeny $\alpha\colon A \to B$ is the degree as a regular map, i.e. $[K(A) : \alpha^*(K(B))]$. If α is separable, i.e. $K(A)/\alpha^*(K(B))$ is a separable extension, then α is unramified. If moreover K is algebraically closed, then every fibre has exactly $\deg \alpha$ points.

Definition 1.2.6. *Let $n \in \mathbb{N}$, we define the multiplication-by-n map as*

$$\begin{aligned}[n]\colon A &\to A \\ a &\mapsto na = a + ... + a \ \textit{(n times)}\end{aligned}$$

and its kernel $A[n]$. The element of the kernel are called the n-torsion points *of A.*

Theorem 1.2.7. *Let A be an abelian variety of dimension d. The integer multiplication $[n]$ is an isogeny of degree n^{2d}.It is separable, hence it is unramified, if K has characteristic 0 or if the characteristic does not divide n. In these case we have $A[n](\overline{K}) \cong (\mathbb{Z}/n\mathbb{Z})^{2d}$.*

Proof. See [13]. □

1.3 Dual varieties and maps

The formal definition of the dual variety uses the moduli space of line bundles, but in the case of varieties defined over a field this definition becomes much simpler. We will give only this second definition.

We recall that $Pic(A)$ is the quotient of the set of divisors on A modulo principal divisor, i.e. those arising from a rational function. We define $Pic^0(A)$ as the subset of $Pic(A)$ of the element of degree zero. Equivalently we can define $Pic^0(A)$ as the set of isomorphism classes of line bundles on A invariant under the pullback by a translation ($t_a^*\mathcal{L} = \mathcal{L} \ \ \forall\, a \in A$).

Definition 1.3.1. *Let A be an abelian variety, then the* ***dual variety*** *is $A^\vee = Pic^0(A)$.*

For the definition in the general case and a proof of the existence see [15].

This duality acts also on the isogenies between abelian variety in a good way.

Proposition 1.3.2. *Let A/K and B/K be abelian variety. Given an isogeny $\phi\colon A \to B$ there is a unique dual homomorphism $\phi^\vee\colon A^\vee \to B^\vee$. If we see $Pic^0(B)$ as line bundles this map is simply the pullback ϕ^* from B to A.*

Theorem 1.3.3. *Let A/K and B/K be abelian variety and $\phi\colon A \to B$ an isogeny. Let N be the kernel of ϕ. Then the dual map is an isogeny and its kernel is the dual of N in the sense of Cartier duality. In particular both isogenies have the same degree.*

We define some special maps between a variety and the dual. We will see $Pic^0(A)$ always as class of line bundles.

Definition 1.3.4. *Let $\mathcal{L}$ be a line bundle on $A(\overline{K})$. We define the map*

$$\begin{aligned} \lambda_{\mathcal{L}} \colon A(\overline{K}) &\to A^{\vee}(\overline{K}) \\ a &\mapsto \tau_a^* \mathcal{L} \otimes \mathcal{L}^{-1} \end{aligned}$$

where τ_a is the translation by a.

Remark. *This map is well defined, in fact its image is always in $Pic^0(A)$. Furthermore this map is an homomorphism.*

Definition 1.3.5. *A **polarization** of the abelian variety A over K is an isogeny $\phi \colon A \to A^{\vee}$ such that over $\overline{K}$ is of the form $\lambda_{\mathcal{L}}$ for some ample line bundle $\mathcal{L}$.*

*A **principal polarization** is a polarization which induces an isomorphism between A and $A^{\vee}$. If A admits a principal polarization the the variety is called a **principally polarized abelian variety**.*

Remark. *This requirement on the form of ϕ is not the same as requiring that it is already of the form $\lambda_{\mathcal{L}}$ for some ample line bundle $\mathcal{L}$ over K.*

1.4 Jacobians

The Jacobian variety is defined only for curves. We now restate the definitions of divisors and Picard group in the case of curves.

Let K be a perfect field and C a curve over it. The group of divisors $Div(C)$ is the free abelian group generated by the elements of $C(\overline{K})$, i.e a divisors is a formal linear combination with integral coefficients. A divisor is effective if all its coefficients are non negative. We will write a divisor as $\sum_{i=1}^{k} n_i P_i$ where $k \in \mathbb{N}$, $n_i \in \mathbb{Z}$ and $P_i \in C(\overline{K})$ for all i.

We are interested in studying the arithmetic of K but this definition of divisor uses its algebraic closure. The absolute Galois group $G_{\overline{K}/K}$ of K acts naturally on $C(\overline{K})$ and so it acts also on $Div(C)$. We define a divisor to be defined over K if it is fixed by the action of $G_{\overline{K}/K}$.

Remark. *If $D = \sum_{i=1}^{k} n_i P_i$ is defined over K then it is not true that necessarily $P_i \in K$ for all i. It is enough that the action of the Galois group swaps the points.*

The degree of a divisor $D = \sum_{i=1}^{k} n_i P_i$ is $deg(D) = \sum_{i=1}^{k} n_i$. We can see the deg map as a group homomorphism $Div(C) \to \mathbb{Z}$. The kernel of this map (i.e. the divisors of degree zero) is denoted by $Div^0(C)$.

Let $f \in \overline{K}(C)$ be a rational function then its divisor is

$$div(f) = \sum_{P \in C(\overline{K})} ord_P(f)P$$

where $ord_P(f)$ is the order of vanishing of f at P (if f has a pole then the order will be negative). It is easy to check that these divisors have degree zero. We define a divisor to be principal if it is $div(f)$ for some $f \in \overline{K}(C)$. We define $PDiv(C)$ the subgroup of principal divisors.

We say that two divisors D_1 and D_2 are linearly equivalent $D_1 \sim D_2$ if their difference is a principal divisor. We define the Picard group

$$Pic(C) = Div(C)/PDiv(C) \text{ and } Pic^0(C) = Div^0(C)/PDiv(C)$$

We would like to define the subgroup of the Picard group of elements fixed by $G_{\overline{K}/K}$ but to do this we need to be able to take quotient in the category of Galois module. We can easily see that $div(f^\sigma) = div(f)^\sigma$ for all $\sigma \in G_{\overline{K}/K}$ and so $PDiv(C)$ is a Galois submodule of $Div^0(C)$ which is a submodule of $Div(C)$. Hence we can take quotient and define

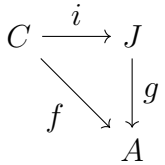
$$Pic^0_K(C) = \left(\frac{Div^0(C)}{PDiv(C)}\right)^{G_{\overline{K}/K}} \quad \text{and} \quad Pic^0_K(C) = \left(\frac{Div^0(C)}{PDiv(C)}\right)^{G_{\overline{K}/K}}$$

We can now define the Jacobian variety and some of its main property.

Theorem 1.4.1. *Let C be a smooth curve over K. Then there is an abelian variety J over K, called the **Jacobian variety** of C, such that there is an isomorphism of $G_{\overline{K}/K}$-modules $Pic^0(C) \cong J(\overline{K})$. The dimension of J is equal to the genus of C. The Jacobian variety is principally polarized.*

If $C(K)$ is non empty we can always embed the variety C into its Jacobian. Fix a point $P \in C(K)$. Identifying the Jacobian with $Pic^0(C)$ we can associate a map to P that sends a point $Q \in C$ to the divisor class $[Q - P]$.

Proposition 1.4.2 (Universal property of the Jacobian)**.** *Let C/K be a curve with Jacobian J. Fix a rational point $P \in C(K)$ and denote by $i\colon C \to J$ the corresponding embedding of C into its Jacobian. Then J satisfies the following universal property: for any abelian variety A and for any algebraic morphism $f\colon C \to A$ such that $f(P) = 0_A$ there is a unique homomorphism of abelian varieties $g\colon J \to A$ such that the following diagram commutes:*



1.5 The Neron model

Let K be a number field or a p-adic field, R its ring of integers and π a maximal ideal (unique if K is a discrete valuation field). Let X and Y be variety over K, then we can fix flat morphism $\pi_1 \colon X \to Spec(R)$ and $\pi_2 \colon Y \to Spec(R)$. If the fibres of these morphisms over the ideal (0) (the generic fibre) are isomorphic we say that they are different models for the same variety.

In general a variety can have many models but in the case of abelian variety there is a special model which we will use in the rest of this thesis: the Neron model.

Definition 1.5.1. *Let A be an abelian variety over K as above. A **Neron model** for A/K is a smooth group R-scheme $\mathcal{A}$ whose generic fibre is A and which satisfies the following universal property (called Neron mapping property):*

> *Let $\mathcal{X}$ be a smooth R-scheme with generic fibre X over K and let $\phi_K \colon X_{/K} \to A_{/K}$ be a rational map defined over K. Then there exists a unique R-morphism $\phi_R \colon \mathcal{X}_{/R} \to \mathcal{A}_{/R}$ extending ϕ_K.*

Remark. *An important instance of the Neron mapping property is the case where $\mathcal{X} = Spec(R)$ and $X = Spec(K)$. Then the set of K-maps $X \to A$ is precisely the group of K-rational points of $A(K)$ and the set of R-morphism $\mathcal{X} \to \mathcal{A}$ is the group of sections of $\mathcal{A}(R)$. Hence the Neron mapping property shows that the natural inclusion $\mathcal{A}(R) \hookrightarrow A(K)$ is a bijection.*

We now prove that the Neron model of an abelian variety is unique up to isomorphism and that it behaves well under base change.

Proposition 1.5.2. *Let R be a Dedekind domain with fraction field K and let A/K be an abelian variety.*

1. *Suppose that $\mathcal{A}_1$ and $\mathcal{A}_2$ are Neron model for A. Then there exists a unique R-isomorphism $\psi \colon \mathcal{A}_1 \to \mathcal{A}_2$ whose restriction to the generic fibre is the identity map of A. In other words the Neron model is unique up to isomorphism.*

2. *Let K'/K be a finite unramified extension and let R' be the integral closure of R in K'. Let $\mathcal{A}$ be a Neron model for A. Then $\mathcal{A} \times_R R'$ is a Neron model for A over K'.*

Proof. (1) The identity map $A/K \to A/K$ is a rational map from the generic fibre of $\mathcal{A}_1$ to the that of $\mathcal{A}_2$ and $\mathcal{A}_1$ is smooth over R by definition, hence the

Neron mapping property for $\mathcal{A}_2$ says that the identity map extends uniquely to a R-morphism $\psi\colon \mathcal{A}_1 \to \mathcal{A}_2$. In the same way we get $\phi\colon \mathcal{A}_2 \to \mathcal{A}_1$ which is the identity map on the generic fibre. Then $\phi \circ \psi\colon \mathcal{A}_1 \to \mathcal{A}_1$ and the identity map of $\mathcal{A}_1$ are R-morphism which are the same on the generic fibre hence by the uniqueness part of the Neron mapping property we get that $\phi \circ \psi$ is the identity map. Again in the same way we get that $\psi \circ \phi$ is the identity map, so ψ is an isomorphism.

(2) Let $\mathcal{X}'/R$ be a smooth R'-scheme with generic fibre X'/K' and let $\phi_{K'}\colon X'/K' \to A/K'$ be a rational map. The composition

$$\mathcal{X}' \to Spec(R') \to Spec(R)$$

makes $\mathcal{X}'$ into an R-scheme. Further our assumptions on K' imply that the map $Spec(R') \to Spec(R)$ is a smooth morphism. Hence the composition is a smooth morphism so $\mathcal{X}'$ is a smooth R-scheme. Now the Neron mapping property for $\mathcal{A}$ tells us that there is an R-morphism $\mathcal{X}' \xrightarrow{\phi_R} \mathcal{A}$ whose restriction to the generic fibre is the composition $X' \xrightarrow{\phi_{K'}} A \times_K K' \xrightarrow{p_1} E$. The two R-morphism ϕ_R and $\mathcal{X}' \to Spec(R')$ determine an R-morphism (and thus an R'-morphism) to the fibre product $\phi_{R'}\colon \mathcal{X}' \to \mathcal{A} \times_R R'$. Further the restriction of $\phi_{R'}$ to the generic fibre is $\phi_{K'}$. This gives the existence part of the Neron mapping property, the uniqueness one follows easily from that of the Neron mapping property of $\mathcal{A}/R$. This completes the proof that $\mathcal{A} \times_R R'$ is a Neron model for A/K'. □

1.6 Invariants

In this section we are going to define some geometric invariant of the abelian varieties.

Regulator

In order to define the regulator we need to introduce a bilinear pairing on the points of the variety. We start defining the height functions. A height is a map from the points of X to $\mathbb{R}$.

The height of a number $a/b \in \mathbb{Q}$, written in lowest terms, is

$$H\left(\frac{a}{b}\right) = \max\{|a|, |b|\}$$

More generally the height of a point $P \in \mathbb{P}^n(\mathbb{Q})$ is defined by writing the point $P = [x_0, ..., x_n]$ with $x_i \in \mathbb{Z}$ for all i and $\gcd(x_0, ..., x_n) = 1$ and then

setting

$$H(P) = \max\{|x_0|, ..., |x_n|\}$$

Let $K/\mathbb{Q}$ be a number field and M_K the set of all places of K. Then the height of a point $P \in \mathbb{P}^n(K)$ is defined by

$$H_K(P) = \prod_{v \in M_K} \max\{v(x_0), ..., v(x_n)\}$$

It is often more useful to use the absolute logarithmic height since we want the function to be additive and not multiplicative

$$h(P) = \frac{1}{[K:\mathbb{Q}]} \log H_K(P)$$

This height is well defined for every $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$.

Let now X be a projective variety and $\phi\colon X \hookrightarrow \mathbb{P}^n$ be a projective embedding. We define the height as

$$h_\phi(P) = h(\phi(P))$$

More intrinsically, a projective embedding corresponds to a very ample divisor D and choice of sections generating $\mathcal{L}(D)$. So for each very ample divisor D we can choose an embedding $\phi_D\colon X \to \mathbb{P}^n$ and get a height function

$$h_D(P) = h(\phi_D(P))$$

We now define the canonical Neron-Tate height on abelian variety.

Theorem 1.6.1 (Neron, Tate)**.** *Let $D \in Div(A)$ be a symmetric divisor (i.e. $[-1]^*D = D$), then the limit*

$$\hat{h}_D(P) = \lim_{n\to\infty} \frac{1}{n^2} h_D(nP)$$

exists and respect the parallelogram law.

We define the inner product

$$\langle P, Q\rangle_D = \hat{h}_D(P+Q) - \hat{h}_D(P) - \hat{h}_D(Q)$$

which is by the previous theorem a bilinear pairing. One can show the it does not depends on the choice of the divisor D.

Definition 1.6.2. *Let $P_1, ..., P_r$ be a basis for the free part of the group of K-rational points $A(K)$, then the* ***regulator*** *of A is the volume of a fundamental domain for the lattice $A(K)/A(K)_{tors}$:*

$$R_{A/K} = \det\left(\langle P_i, P_j\rangle\right)_{1\le i,j\le r}$$

The local Tamagawa number

Let M_K^0 the set of all finite place of the number field K. Let $v \in M_k^0$, K_v the completion of K at v and k_v its residue field. Let A be an abelian variety then we can consider its reduction at v, i.e. the special fibre of the Neron model at v. We call it $\tilde{A}$. We consider the set of nonsingular point $\tilde{A}_{ns}$ of $\tilde{A}$ and define A_0 the set of points of A whose reduction is nonsingular and A_1 the kernel of the reduction map $A_0(K_v) \to \tilde{A}_{ns}$. There is an obvious exact sequence

$$0 \to A_1(K_v) \to A_0(K_v) \to \tilde{A}_{ns}(k_v) \to 0$$

Proposition 1.6.3. *The set $A_0(K_v)$ has finite index in $A(K_v)$.*

Definition 1.6.4. *The **local Tamagawa number** at v is the index*

$$c_v = [A(K_v) \colon A_0(K_v)]$$

If A has good reduction at v then by definition the local Tamagawa number will be 1.

Chapter 2

The Tate-Shafarevich group

One of the most important theorem about abelian varieties is the following.

Theorem 2.0.1 (Mordell-Weil)**.** *Let A/K an abelian variety over a number field K. Then the group $A(K)$ of K-rational points of A is finitely generated.*

This theorem and its proof are not effective: they do not provide an actual way to compute the rank. Some methods have since been developed in order to calculate the rank but they can just provide an upper-bound. How much these methods fail is measured by the Tate-Shafarevich group.

The Tate-Shafarevich group is defined using Galois cohomology and it is a very complicated group to work with. However it turns out to be trivial in many case. This group is conjectured to be finite but a general proof is still missing.

2.1 Galois cohomology

We will define only the cohomology groups H^0 and H^1 since we need only those in this thesis.

Let K be a perfect field, $\overline{K}$ be an algebraic closure of K and $G_{\overline{K}/K}$ be the absolute Galois group of K. We recall that this is a profinite group (i.e. the inverse limit of a system of finite groups) and as such it comes equipped with the profinite topology. A basis of open sets around the identity consists of the collection of normal subgroups of finite index.

Definition 2.1.1. *A **(discrete)** $G_{\overline{K}/K}$**-module** is an abelian group M on which $G_{\overline{K}/K}$ acts such that the action is continuous for the profinite topology on $G_{\overline{K}/K}$ and the discrete topology on M.*

Definition 2.1.2. *The* 0***-th cohomology group*** *of the* $G_{\overline{K}/K}$*-module* M *is the group of* $G_{\overline{K}/K}$*-invariant element of* M*:*

$$H^0(G_{\overline{K}/K}, M) = M^{G_{\overline{K}/K}} = \left\{ m \in M \mid m^\sigma = m \ \forall \sigma \in G_{\overline{K}/K} \right\}$$

Now we introduce the required elements to define the first cohomology group.

Definition 2.1.3. *Let* M *a* $G_{\overline{K}/K}$*-module. The group of* 1*-cochains (from* G *to* M*) is defined by*

$$C^1(G_{\overline{K}/K}, M) = \{ \text{maps } \xi \colon G \to M \}$$

The group of 1*-cocycles is given by*

$$Z^1(G_{\overline{K}/K}, M) = \left\{ \xi \in C^1(G_{\overline{K}/K}, M) \mid \xi_{\tau\sigma} = \xi_\sigma^\tau + \xi_\tau \text{ for all } \sigma, \tau \in G_{\overline{K}/K} \right\}$$

We further define the group $Z^1_{cont}(G_{\overline{K}/K}, M)$ *of the continuous* 1*-cocycles as the subgroup of* $Z^1(G_{\overline{K}/K}, M)$ *consisting of only the continuous map for the profinite topology on* $G_{\overline{K}/K}$ *and the discrete one on* M*.*

The group of 1*-coboundaries is defined by*

$$B^1(G_{\overline{K}/K}, M) = \left\{ \xi \in C^1(G_{\overline{K}/K}, M) \;\middle|\; \begin{array}{c} \exists m \in M \text{ such that} \\ \xi_\sigma = m^\sigma - m \text{ for all } \sigma \in G_{\overline{K}/K} \end{array} \right\}$$

The 1*-coboundaries are always continuous for the discrete topology on* M*.*

It is easy to check that the group of 1-coboundaries is a subgroup of the continuous 1-cocycles.

Definition 2.1.4. *The* ***first cohomology group*** *is the quotient group*

$$H^1(G_{\overline{K}/K}, M) = \frac{Z^1_{cont}(G_{\overline{K}/K}, M)}{B^1(G_{\overline{K}/K}, M)}$$

Remark. *This definition does not make sense in the case where* M *is non commutative since the* 1*-cocycles does not form a group in general. In this case, using the multiplicative notation, we rewrite the cocycles condition as* $\xi_{\tau\sigma} = (\xi_\sigma)^\tau \xi_\tau$ *and we define two cocycles* ξ *and* ζ *to be* cohomologous *if there exists* $m \in M$ *such that* $m^\sigma \xi_\sigma = \zeta_\sigma m$ *for all* $\sigma \in G_{\overline{K}/K}$*. This is an equivalence relation and we define the first cohomology pointed set (and not group) to be the quotients of the continuous* 1*-cocycles by this equivalence relation.*

Form now on we will use the following shorter notation for the Galois cohomology: $H^*(G_{\overline{K}/K}, M)$ will be simply written as $H^*(K, M)$.

Proposition 2.1.5. *Let M, N, P be $G_{\overline{K}/K}$-module and*

$$0 \to P \xrightarrow{\phi} M \xrightarrow{\psi} N \to 0$$

be an exact sequence. Then there is a long exact sequence in cohomology

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^0(K,P) & \longrightarrow & H^0(K,M) & \longrightarrow & H^0(K,N) \\ & & & & & \overset{\delta}{\searrow} & \\ & & H^1(K,P) & \longrightarrow & H^1(K,M) & \longrightarrow & H^1(K,N) \end{array}$$

where the connecting homomorphism δ is defined as follows: let $n \in H^0(K,N)$, choose an $m \in M$ such that $\psi(m) = n$ and define a cochain $\xi \in C^1(G_{\overline{K}/K}, M)$ by $\xi_\sigma = m^\sigma - m$. Then the value of ξ are in $\ker\psi$ and so in P, hence by a simple calculation we find that $\xi \in Z^1_{cont}(G_{\overline{K}/K}, M)$. We finally define $\delta(n)$ to be the cohomology class of ξ in $H^1(K,P)$.

Proof. See [21, Proposition 1.2 of appendix B]. □

Let M be a $G_{\overline{K}/K}$-module and let L/K be a Galois extension. Then $G_{\overline{K}/L}$ is a subgroup of finite index in $G_{\overline{K}/K}$ so M is naturally a $G_{\overline{K}/L}$-module. Further if ξ is a cochain from $G_{\overline{K}/K}$ to M then restricting the domain to $G_{\overline{K}/L}$ we obtain a cochain from $G_{\overline{K}/L}$ to M. It is clear that this process takes cocycles to cocycles and coboundaries to coboundaries. In this way we get a *restriction homomorphism*

$$Res\colon H^1(K,M) \to H^1(L,M)$$

Further $G_{\overline{K}/L}$ is a normal subgroup and the quotient $G_{\overline{K}/K}/G_{\overline{K}/L}$ is the finite group $G_{L/K}$. Then the submodule of invariant elements $M^{G_{\overline{K}/L}}$ has a natural structure as a $G_{L/K}$-module. Then composing with the projection from $G_{\overline{K}/L}$ and the inclusion $M^{G_{\overline{K}/L}} \hookrightarrow M$ gives a cochain from $G_{\overline{K}/K}$ to M:

$$G_{\overline{K}/K} \to G_{L/K} \xrightarrow{\xi} M^{G_{\overline{K}/L}} \hookrightarrow M$$

This gives a *inflation map*

$$Inf\colon H^1(G_{L/K}, M^{G_{\overline{K}/L}}) \to H^1(K,M)$$

Proposition 2.1.6 (Inflation-Restriction Sequence)**.** *With notations as above there is an exact sequence*

$$0 \to H^1(G_{L/K}, M^{G_{\overline{K}/L}}) \xrightarrow{Inf} H^1(K, M) \xrightarrow{Res} H^1(L, M)$$

Proof. From the definition it is clear that $Res \circ Inf = 0$.

Let $\xi\colon G_{L/K} \to M^{G_{L/K}}$ be a 1-cocycle with $Inf\{\xi\} = 0$, where we use the braces to indicate the cohomology class.Thus there is an $m \in M$ such that $\xi_\sigma = m^\sigma - m$ for all $\sigma \in G_{\overline{K}/K}$. But ξ depends only on $\sigma \pmod{G_{\overline{K}/L}}$, so $m^\sigma - m = m^{\sigma\tau} - m$ for all $\tau \in G_{\overline{K}/L}$. Taking $\sigma = 1$ we find that $m^\tau - m = 0$ for all $\tau \in G_{\overline{K}/L}$, so $m \in M^{G_{\overline{K}/L}}$ and hence ξ is a coboundary from $G_{L/K}$ to $M^{G_{\overline{K}/L}}$.

Finally suppose that $\xi\colon G_{\overline{K}/K} \to M$ is a 1-cocycle with $Res\{\xi\} = 0$. Thus there is an $m \in M$ such that $\xi_\tau = m^\tau - m$ for all $\tau \in G_{\overline{K}/L}$. Subtracting the coboundary from $G_{\overline{K}/K}$ to M defined by $\sigma \mapsto m^\sigma - m$ from ξ we may assume that $\xi_\tau = 0$ for all $\tau \in G_{\overline{K}/L}$. Then the coboundary condition applied to $\sigma \in G_{\overline{K}/K}$ and $\tau \in G_{\overline{K}/L}$ yields $\xi_{\tau\sigma} = \xi_\tau^\sigma + \xi_\sigma = \xi_\sigma$. Thus ξ_σ depends only on the class of σ in $G_{L/K}$. Since $G_{\overline{K}/L}$ is a normal subgroup there is a $\tau' \in G_{\overline{K}/L}$ such that $\sigma\tau = \tau'\sigma$. Using the cocycle condition again, together with the fact that ξ is a map on $G_{L/K}$, gives $\xi_\sigma = \xi_{\tau'\sigma} = \xi_{\sigma\tau} = \xi_\sigma^\tau + \xi_\tau = \xi_\sigma^\tau$. This proves that ξ gives a map from $G_{L/K}$ to $M^{G_{\overline{K}/L}}$, hence $\{\xi\} \in H^1(G_{L/K}, M^{G_{\overline{K}/L}})$. □

The next proposition is a collection of important property of the cohomology groups.

Proposition 2.1.7. *Let K be a field.*

1. $H^1(K, \overline{K}^+) = 0$
2. $H^1(K, \overline{K}^*) = 0$ *[Hilbert's Theorem 90]*
3. *Assume that either $char(K) = 0$ or that $char(K)$ does not divide m. Then $H^1(K, \mu_m) \cong K^*/(K^*)^m$*

2.2 The Selmer and Tate-Shafarevich groups

Let A and A' be abelian varieties and $\phi\colon A \to A'$ be a nonzero isogeny. Let us denote by $A[\phi]$ the kernel of this isogeny. Then there is an exact sequence of $G_{\overline{K}/K}$-module

$$0 \to A[\phi] \to A \xrightarrow{\phi} A' \to 0$$

Taking the Galois cohomology we get the following exact sequence

$$0 \longrightarrow A(K)[\phi] \longrightarrow A(K) \longrightarrow A'(K) \xrightarrow{\delta} H^1(K, A[\phi]) \longrightarrow H^1(K, A) \longrightarrow H^1(K, A')$$

and from this we form the fundamental short exact sequence

$$0 \to \frac{A'(K)}{\phi(A(K)))} \to H^1(K, A[\phi]) \to H^1(K, A)[\phi] \to 0$$

We now make some local consideration. Let M_K denote the set of all place of K and for a fixed $v \in M_K$ we define $\overline{K}_v$ the completion with respect to v of $\overline{K}$. We then fix an extension of v to $\overline{K}$ which in turn fixes an embedding $\overline{K} \subset \overline{K}_v$ of $\overline{K}$ and a decomposition group $G_v \subset G_{\overline{K}/K}$. G_v acts on $A(\overline{K}_v)$ and $A'(\overline{K}_v)$ and repeating the above argument we get the analogous exact sequence:

$$0 \to \frac{A'(K_v)}{\phi(A(K_v)))} \to H^1(G_v, A[\phi]) \to H^1(G_v, A)[\phi] \to 0$$

The natural inclusions listed above give restriction maps on cohomology and thus we end up with the following commutative diagram:

$$\begin{array}{ccccccc}
0 & \longrightarrow & \dfrac{A'(K)}{\phi(A(K)))} & \longrightarrow & H^1(K, A[\phi]) & \longrightarrow & H^1(K, A)[\phi] \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \to & \displaystyle\prod_{v \in M_K} \frac{A'(K_v)}{\phi(A(K_v)))} & \longrightarrow & \displaystyle\prod_{v \in M_K} H^1(G_v, A[\phi]) & \longrightarrow & \displaystyle\prod_{v \in M_K} H^1(K_v, A)[\phi] \to 0
\end{array}$$

Definition 2.2.1. *Let $\phi\colon A/K \to A'/K$ be an isogeny. The* ***ϕ-Selmer group of*** *A/K is the subgroup of $H^1(K, A[\phi])$ defined by*

$$S^{(\phi)}(A/K) = \ker\left(H^1(K, A(\overline{K})[\phi]) \to \prod_{v \in M_K} H^1(K_v, A(\overline{K}_v))\right)$$

and the ***Tate-Shafarevich group of*** *A/K is the subgroup of $H^1(K, A)$ defined by*

$$Ш(A/K) = \ker\left(H^1(K, A(\overline{K})) \to \prod_{v \in M_K} H^1(K_v, A(\overline{K}_v))\right)$$

Remark. *In the definition of the Tate-Shafarevich group we make a choice: how we extend v to $\overline{K}$. We need to prove that the definition does not depends on such choice. This can be done using only cocycle but it can be don easier using a different interpretation of the Tate-Shafarevich group that uses homogeneous spaces.*

Proposition 2.2.2. *Let $\phi\colon A/K \to A'/K$ be a nonzero isogeny of abelian varieties defined over K. There is an exact sequence*

$$0 \to A'(K)/\phi(A(K)) \to S^{(\phi)}(A/K) \to Ш(A/K) \to 0$$

Proof. This is immediate from the previous diagram and the definition of the groups. □

It is a known fact that the Selmer group is finite, on the other hand whether the Tate-Shafarevich group is finite or not is an open question. Some evidences leaded Tate and Shafarevich to believe in the following:

Conjecture 2.2.3. *The Tate-Shafarevich group $Ш(A/K)$ is finite.*

From the works of Kolyvagin we know that this is true for elliptic curves of rank at most 1.

This group is strictly related to the Mordell-Weil theorem since it measure how much the algorithm used to find the rank of the group of K-rational points fails. This group appears also in the famous Birch and Swinnerton-Dyer conjecture: they gave a formula relating some geometric invariant to some analytic ones. The Ш group is very complicated, even for the simple elliptic curves, although it turn out to be the trivial group in many cases.

2.3 Cassels and Tate pairing

In 1962 Cassels showed the existence of a pairing on this group for elliptic curves which forces the order of the group to be a perfect square, provided it is finite. Tate later generalized it to abelian varieties but it does not imply anymore that the order is a perfect square. Let A be an abelian variety over a number fields. Then from [1] and [23] we have the pairing

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

which is non-degenerated in case $Ш(A/K)$ is finite.

This pairing has mislead several mathematicians into believing that the order was always a square even for abelian varieties in general until 1996

when Michael Stoll constructed the first example of an abelian variety with Tate-Shafarevich group of non-square order.

However this pairing gives a strong restriction on the non-square part of the order as proved by W. Stein in [22] using results of M. Flach [5].

Theorem 2.3.1. *Assume* $Ш(A/K)$ *is finite. If an odd prime* p *divides the non-square part of the order of* $Ш(A/K)$ *then* p *divides the degree of every polarization of* A/K*.*

Corollary 2.3.2 (Poonen, Stoll)**.** *If* A/K *is a principally polarized abelian variety then*

$$\#Ш(A/K) = k^2 \text{ or } 2k^2$$

for some $k \in \mathbb{Z}$*.*

In 1996 M. Stoll constructed the first example of a principally polarized abelian variety with $\#Ш(A/K) = 2k^2$. It was the Jacobian of a genus 2 curve over $\mathbb{Q}$. Other examples have since been constructed, many of which in high dimension.

Chapter 3

The Cassels-Tate equation

In this chapter we will introduce the main tool we will use in studying the order of the Tate-Shafarevich group. Then we will analyse the terms of this equation in order to find a way to compute them. This equation gives a formula for computing the quotient of the order of the Tate-Shafarevich group of two isogenous abelian varieties.

3.1 The equation

In the mid 1960s Cassels and Tate found this equation in order to prove the invariance of te Birch and Swinnerton-Dyer conjecture under isogeny (see [2] and [24]).

Let A be an abelian variety over a number field K and denote by R_A the regulator of A, P_A the period of A (integral of a holomorphic differential) and $c_{A,v}$ the local Tamagawa number at a finite place v.

Theorem 3.1.1 (Cassels, Tate)**.** *Let $\varphi\colon A \to B$ be an isogeny between two abelian varieties over a number field K. Assume that al least one of $Ш(A/K)$ or $Ш(B/K)$ is finite then both are finite and*

$$\frac{\#Ш(A/K)}{\#Ш(B/K)} = \frac{R_B}{R_A}\frac{\#A(K)_{tors}\#A^\vee(K)_{tors}}{\#B(K)_{tors}\#B^\vee(K)_{tors}}\frac{P_B}{P_A}\prod_{v\in M_K^0}\frac{c_{B,v}}{c_{A,v}}$$

The product over the Tamagawa number is actually finite since $c_{A,v} = 1$ if v is a place of good reduction. Define $A(K)_{free}$ to be the quotient group $A(K)/A(K)_{tors}$ and consider the following induced group homomorphisms:

$$\varphi_K\colon A(K) \to B(K), \quad \varphi_K^\vee\colon B^\vee(K) \to A^\vee(K), \quad \varphi_v\colon A(K_v) \to B(K_v)$$

$$\varphi_{K,tors}\colon A(K)_{tors} \to B(K)_{tors}, \quad \varphi_{K,tors}^\vee\colon B^\vee(K)_{tors} \to A^\vee(K)_{tors}$$

$$\varphi_{K,free}\colon A(K)_{free} \to B(K)_{free}, \quad \varphi^\vee_{K,free}\colon B^\vee(K)_{free} \to A^\vee(K)_{free}$$

We may now reformulate the above quotients in terms of these induced group homomorphisms. This reformulation, which is part of the proof of the above theorem, turns out to be easier to handle for computational purposes, and we use the Cassels-Tate equation only in this description. There are two trivial equalities, namely

$$\frac{\#A(K)_{tors}}{\#B(K)_{tors}} = \frac{\#\ker\varphi_K}{\#\operatorname{coker}\varphi_{K,tors}} \quad \text{and} \quad \frac{\#A^\vee(K)_{tors}}{\#B^\vee(K)_{tors}} = \frac{\#\operatorname{coker}\varphi^\vee_{K,tors}}{\#\ker\varphi^\vee_K}$$

and two more interesting ones, see the proof of [14, Theorem I.7.3];

$$\frac{R_B}{R_A} = \frac{\#\operatorname{coker}\varphi^\vee_{K,free}}{\#\operatorname{coker}\varphi_{K,free}} \quad \text{and} \quad \frac{P_B}{P_A}\prod_{v\in M_K^0}\frac{c_{B,v}}{c_{A,v}} = \prod_{v\in M_K}\frac{\#\operatorname{coker}\varphi_v}{\#\ker\varphi_v}$$

Hence the Cassels-Tate equation becomes

$$\frac{\#Ш(A/K)}{\#Ш(B/K)} = \frac{\#\ker\varphi_K}{\#\operatorname{coker}\varphi_K}\frac{\#\operatorname{coker}\varphi^\vee_K}{\#\ker\varphi^\vee_K}\prod_{v\in M_K}\frac{\#\operatorname{coker}\varphi_v}{\#\ker\varphi_v}$$

In particular

$$\frac{R_B}{R_A}\frac{\#A(K)_{tors}\#A^\vee(K)_{tors}}{\#B(K)_{tors}\#B^\vee(K)_{tors}} = \frac{\#\ker\varphi_K}{\#\operatorname{coker}\varphi_{K,tors}}\frac{\#\operatorname{coker}\varphi^\vee_K}{\#\ker\varphi^\vee_K}$$

and we call the right-hand side of this equation the **global quotient**. The global quotient clearly breaks into the regulator quotient and the torsion quotient. The product

$$\prod_{v\in M_K}\frac{\#\operatorname{coker}\varphi_v}{\#\ker\varphi_v}$$

runs over all places V of K and is called the local quotient. It is in fact a finite product, since $\#\operatorname{coker}\varphi_v = \#\ker\varphi_v$ for all but finitely many v, as we will prove shortly. In the next sections we will study the local quotient.

3.2 The local quotient

In this section we use the following notation. Let $\varphi\colon A \to B$ be an isogeny between two abelian varieties A and B over a number field K. Let M_K^0 be the set of all finite place of K and $v \in M_K^0$. Consider the induced group homomorphism on K_v-rational points

$$\varphi_v\colon A(K_v) \to B(K_v)$$

Our aim is to compute the quotient $\#\operatorname{coker}\varphi_v/\#\ker\varphi_v$, which mainly consists in determining the cardinality of $\operatorname{coker}\varphi_v$, as the size of the kernel is usually obvious by the definition of φ_v. On a few occasions we focus on isogenies having a K_v-kernel, i.e. $A(\overline{K}_v)[\varphi] = A(K_v)[\varphi_v]$, and thus $\#\ker\varphi_v = \deg\varphi$ and $G_{\overline{K}_v/K_v}$ acts trivially on $A(K_v)[\varphi]$. In general, the cokernel of φ_v can naturally be identified with a subgroup of $H^1(K_v, A(K_v)[\varphi])$ since the short exact sequence

$$0 \to A(\overline{K}_v)[\varphi] \to A(\overline{K}_v) \xrightarrow{\varphi} B(\overline{K}_v) \to 0$$

gives the long exact Galois cohomology sequence

$$0 \to \operatorname{coker}\varphi_v \to H^1(K_v, A(\overline{K}_v)[\varphi]) \to \dots$$

The next lemma determines the size of $H^1(K_v, A(K_v)[\varphi])$ and in particular shows that it is finite, hence $\operatorname{coker}\varphi_v$ is also finite.

Lemma 3.2.1. *Let K_v be a p-adic field and let M be a finite K_v-Galois module of order $\#M$ and with dual $M^\vee = Hom(M, \mathbb{G}_m(K_v))$. The size of the first cohomology group of M can be computed as follows:*

$$\#H^1(K_v, M) = \#H^0(K_v, M) \cdot \#H^0(K_v, M^\vee) \cdot p^{v_p(\#M)[K_v\colon \mathbb{Q}_p]}$$

where v_p is the p-adic valuation.

Proof. This follows from [18, Theorems 2 and 5 in Chapter II.5]. Define the Euler-Poincaré characteristic by

$$\chi(K_v, M) = \frac{\#H^0(K_v, M)\#H^2(K_v, M)}{\#H^1(K_v, M)}$$

By the two cited theorems, we get that $\#H^2(K_v, M) = \#H^0(K_v, M^\vee)$ and that $\chi(K_v, M) = (\mathcal{O}_v\colon \#M\mathcal{O}_v)^{-1}$, where $\mathcal{O}_v$ is the valuation ring of K_v. Hence $\chi(K_v, M) = p^{-v_p(\#M)[K_v\colon \mathbb{Q}_p]}$, which finishes the proof. □

Corollary 3.2.2. *Let φ be of prime degree ℓ. If φ or $\varphi^\vee$ has a K_v-kernel, the*

$$H^1(K_v, A(\overline{K}_v)[\varphi]) = \begin{cases} \mathbb{Z}/\ell\mathbb{Z} & v \nmid \ell,\ \mu_\ell \nsubseteq K_v \\ (\mathbb{Z}/\ell\mathbb{Z})^2 & v \nmid \ell,\ \mu_\ell \subseteq K_v \\ (\mathbb{Z}/\ell\mathbb{Z})^{[K_v\colon Q_p]+1} & v \mid \ell,\ \mu_\ell \nsubseteq K_v \\ (\mathbb{Z}/\ell\mathbb{Z})^{[K_v\colon Q_p]+2} & v \mid \ell,\ \mu_\ell \subseteq K_v \end{cases}$$

And if neither φ nor $\varphi^\vee$ has a K_v-kernel, then

$$H^1(K_v, A(\overline{K}_v)[\varphi]) = \begin{cases} 0 & v \nmid \ell \\ (\mathbb{Z}/\ell\mathbb{Z})^{[K_v\colon Q_p]} & v \mid \ell \end{cases}$$

Proof. By definition $H^1(K_v, A(K_v)[\varphi])$ is abelian and has exponent ℓ. By the previous lemma, for $M = A(K_v)[\varphi]$, we have

$$\#H^1(K_v, M) = \begin{cases} \#H^0(K_v, M) \cdot \#H^0(K_v, M^\vee) & v \nmid \ell \\ \#H^0(K_v, M) \cdot \#H^0(K_v, M^\vee) \cdot \ell^{[K_v\colon \mathbb{Q}_p]} & v \mid \ell \end{cases}$$

If φ, respectively $\varphi^\vee$, has a K_v-kernel, then $A(K_v)[\varphi] \cong \mathbb{Z}/\ell\mathbb{Z}$, respectively μ_ℓ, as Galois modules. Since

$$H^0(K_v, \mathbb{Z}/\ell\mathbb{Z}) \cong \mathbb{Z}/\ell\mathbb{Z} \text{ and } H^0(K_v, \mu_\ell) = \begin{cases} 0 & \mu_\ell \nsubseteq K_v \\ \mathbb{Z}/\ell\mathbb{Z} & \mu_\ell \subseteq K_v \end{cases}$$

and $\mathbb{Z}/\ell\mathbb{Z}$ and μ_ℓ are dual to each other, we get the first statement. If neither φ nor $\varphi^\vee$ has a K_v-kernel, then neither $A(K_v)[\varphi]$ nor its dual is isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$. Therefore

$$H^0(K_v, A(K_v)[\varphi]) = H^0(K_v, A(K_v)[\varphi]^\vee) = 0$$

which completes the proof. □

Corollary 3.2.3. *For p and ℓ being prime, we have*

$$H^1(\mathbb{Q}_p, \mathbb{Z}/\ell\mathbb{Z}) \cong H^1(\mathbb{Q}_p, \mu_\ell) \cong \begin{cases} \mathbb{Z}/\ell\mathbb{Z} & p \neq \ell \neq 2, p \not\equiv 1 \mod \ell \\ (\mathbb{Z}/\ell\mathbb{Z})^3 & p = \ell = 2 \\ (\mathbb{Z}/\ell\mathbb{Z})^2 & \textit{otherwise} \end{cases}$$

Proof. This is immediate from corollary 3.2.2 upon observing that $\mu_2 \subseteq \mathbb{Q}_p$ for all p, and $\mu_\ell \nsubseteq \mathbb{Q}_p$ if and only if $p \not\equiv 1 \mod \ell$ and $\ell \neq 2$. □

For a finite K_v-module M we introduce now the unramified Galois cohomology group which is an important subgroup of $H^1(K_v, M)$. Denote by K_v^{nr} the maximal unramified extension of K_v. We have that the inertia group $I_v = G_{\overline{K}_v/K_v^{nr}}$ is a normal subgroup of $G_{\overline{K}_v/K_v}$. Hence, the usual restriction homomorphism

$$Res_{nr}\colon H^1(K_v, M) \to H^1(K_v^{nr}, M)$$

is defined, and by the inflation-restriction sequence its kernel is isomorphic to $H^1(G_{K_v^{nr}/K_v}, M^{I_v})$. We denote the kernel of Res_{nr} by $H^1_{nr}(K_v, M)$ and call it the **unramified subgroup** of $H^1(K_v, M)$.

Consider again the following Galois cohomology sequence with respect to an isogeny $\varphi\colon A \to B$.

$$0 \to \operatorname{coker} \varphi_v \xrightarrow{\delta_v} H^1(K_v, A(\overline{K}_v)[\varphi]) \to \dots$$

We say that $\operatorname{coker}\varphi_v$ is maximal, respectively maximally unramified, respectively trivial, if δ_v is an isomorphism, respectively if δ_v induces an isomorphism between coker φ_v and the unramified subgroup $H^1_{nr}(K_v, A(\overline{K}_v)[\varphi])$, respectively if $\operatorname{coker}\varphi_v = 0$. Besides merely determining the size of $\operatorname{coker}\varphi_v$, our goal is further to specify it as a subgroup of $H^1(K_v, A(\overline{K}_v)[\varphi])$, and hence the main purpose of this subsection is to give criteria to check whether $\operatorname{coker}\varphi_v$ is maximally unramified.

Remark. *If $K = \mathbb{Q}$ and $(p, \ell) \neq (2, 2)$, the last two corollaries show that if the isogeny $\varphi\colon A \to B$ is of prime degree ℓ and has a $\mathbb{Q}_p$-kernel, then $H^1(\mathbb{Q}_p, A(\overline{\mathbb{Q}}_p)[\varphi])$ is either isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$ or $(\mathbb{Z}/\ell\mathbb{Z})^2$. In the former case, $\operatorname{coker}\varphi_p$ is either trivial or maximal. In the latter case, there is a third possibility, namely that $\operatorname{coker}\varphi_p$ is one of the $\ell + 1$ subgroups of $H^1(\mathbb{Q}_p, A(\overline{\mathbb{Q}}_p)[\varphi])$ of order ℓ. By the next lemma, the unramified subgroup is one of these $\ell + 1$ subgroups of order ℓ.*

Lemma 3.2.4. *Let K_v be a p-adic field and let M be a finite K_v-module. Then the order of $H^1_{nr}(K_v, M)$ equals the order of $H^0(K_v, M)$.*

Proof. For a prime ℓ let us denote by $M[l^\infty]$ the ℓ-primary part of M, thus $M = \oplus_\ell M[\ell^\infty]$. As the Galois group acts on the individual $M[\ell^\infty]$ we get

$$H^0(K_v, \oplus_\ell M[\ell^\infty]) = \oplus_\ell H^0(K_v, M[\ell^\infty])$$

and

$$H^1_{nr}(K_v, \oplus_\ell M[\ell^\infty]) = \oplus_\ell H^1_{nr}(K_v, M[\ell^\infty])$$

Now apply [17, Lemma 4.2] to get that the order of $H^1_{nr}(K_v, M[\ell^\infty])$ equals the order of $H^0(K_v, M[\ell^\infty])$. □

We introduce some more notation. By $\tilde{A}$ we denote the reduction of A modulo v, i.e. the special fibre at v of the Néron model $A/\mathcal{O}_K$ of A, and by $\tilde{A}_0(k_v)$ we denote the smooth part of the k_v-rational points of the reduction at v, i.e. the k_v-rational points of the connected component of $\tilde{A}$ intersecting the zero-section. Denote by $A_0(K_v)$ the preimage of $\tilde{A}_0(k_v)$ under the reduction-mod-v map, and by $A_1(K_v)$ the kernel of $A_0(K_v) \to \tilde{A}_0(k_v)$. We have the following two commutative diagrams with exact rows and induced group homomorphisms as vertical arrows.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_1(K_v) & \longrightarrow & A_0(K_v) & \longrightarrow & \tilde{A}_0(k_v) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi_v^1} & & \downarrow{\scriptstyle \varphi_v^0} & & \downarrow{\scriptstyle \tilde{\varphi}_v^0} & & \\ 0 & \longrightarrow & B_1(K_v) & \longrightarrow & B_0(K_v) & \longrightarrow & \tilde{B}_0(k_v) & \longrightarrow & 0 \end{array} \tag{3.2.5}$$

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_0(K_v) & \longrightarrow & A(K_v) & \longrightarrow & A(K_v)/A_0(K_v) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi_v^0} & & \downarrow{\scriptstyle \varphi_v} & & \downarrow{\scriptstyle \overline{\varphi}_v} & & \\ 0 & \longrightarrow & B_0(K_v) & \longrightarrow & B(K_v) & \longrightarrow & B(K_v)/B_0(K_v) & \longrightarrow & 0 \end{array} \tag{3.2.6}$$

The vertical maps on the right, i.e. $\tilde{\varphi}_v^0$ and $\overline{\varphi}_v$, are group homomorphisms between finite groups, which follows from the theory of Néron models. Therefore, the kernels and cokernels of $\tilde{\varphi}_v^0$ and $\overline{\varphi}_v$ are finite groups. The kernels of φ_v^0 and φ_v^1 are finite as they are subgroups of $\ker \varphi_v$, which is finite by definition. The cokernels of φ_v^0 and φ_v^1 are finite by the snake lemma, since $\operatorname{coker} \varphi_v$ is, as seen in corollary 3.2.2. Hence, all kernels and cokernels of the vertical maps in the above two diagrams are finite groups.

In the unramified case we get the following commutative diagram with exact rows.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_1(K_v^{nr}) & \longrightarrow & A_0(K_v^{nr}) & \longrightarrow & \tilde{A}_0(\overline{k}_v) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi_{v,nr}^1} & & \downarrow{\scriptstyle \varphi_{v,nr}^0} & & \downarrow{\scriptstyle \tilde{\varphi}_{\overline{k}_v}^0} & & \\ 0 & \longrightarrow & B_1(K_v^{nr}) & \longrightarrow & B_0(K_v^{nr}) & \longrightarrow & \tilde{B}_0(\overline{k}_v) & \longrightarrow & 0 \end{array} \tag{3.2.7}$$

We recall a basic fact, which follows from Lang's Theorem (see [11, Theorem 1]).

Lemma 3.2.8. *With notation as above, $\tilde{A}_0(k_v)$ and $\tilde{B}_0(k_v)$ are finite groups of same cardinality.*

Proof. The proof is given [11, page 561]. From the theory of Néron models it follows that $\tilde{A}_0$ and $\tilde{B}_0$ are isogenous connected algebraic groups over the finite field k_v. Let G/k be a connected algebraic group over the finite field k of size q. Denote the group law by multiplication and define the Lang isogeny $f_G(g) = g^{-1}g^{(q)}$, for $g \in G(\overline{k})$, where $g^{(q)}$ is the image of g under the Frobenius morphism. Lang's Theorem [11, corollary of theorem 1] says that $f_G \colon G(k) \to G(k)$ is indeed an isogeny with kernel equal to the k-rational points of G. Now let $\varphi \colon G \to H$ be an isogeny between connected algebraic groups G and H over k. Then $f_H \circ \varphi = \varphi \circ f_G$, and hence the kernels of f_G and f_H have the same cardinality, which proves the lemma. □

Now we apply the snake lemma on diagrams 3.2.5 and 3.2.6 to get a basic lemma. Recall, that the local Tamagawa number $c_{A,v}$ of A at v is defined as the order of the quotient group $A(K_v)/A_0(K_v)$.

Lemma 3.2.9. *With notation as above we have the equality*

$$\frac{\#\operatorname{coker}\varphi_v}{\#\ker\varphi_v} = \frac{\#\operatorname{coker}\varphi_v^1}{\#\ker\varphi_v^1}\cdot\frac{c_{B,v}}{c_{A,v}}$$

Proof. We have already seen the finiteness of all appearing kernels and cokernels. Applying the snake lemma on the kernels and cokernels in diagram 3.2.5 we get

$$\frac{\#\ker\varphi_v^1}{\#\operatorname{coker}\varphi_v^1}\cdot\frac{\#\ker\tilde{\varphi}_v^0}{\#\operatorname{coker}\tilde{\varphi}_v^0} = \frac{\#\ker\varphi_v^0}{\#\operatorname{coker}\varphi_v^0}$$

Since $\#\tilde{A}_0(k_v) = \#\tilde{B}_0(k_v)$, by lemma 3.2.8, we get $\#\ker\tilde{\varphi}_v^0 = \#\operatorname{coker}\tilde{\varphi}_v^0$. It follows that

$$\frac{\#\ker\varphi_v^1}{\#\operatorname{coker}\varphi_v^1} = \frac{\#\ker\varphi_v^0}{\#\operatorname{coker}\varphi_v^0}$$

Applying the snake lemma on diagram 3.2.6 gives

$$\frac{\#\operatorname{coker}\varphi_v}{\#\ker\varphi_v} = \frac{\#\operatorname{coker}\varphi_v^0}{\#\ker\varphi_v^0}\cdot\frac{\#\operatorname{coker}\overline{\varphi}_v}{\#\ker\overline{\varphi}_v}$$

By definition, we have $\#\operatorname{coker}\overline{\varphi}_v/\#\ker\overline{\varphi}_v = c_{B,v}/c_{A,v}$, which completes the proof. □

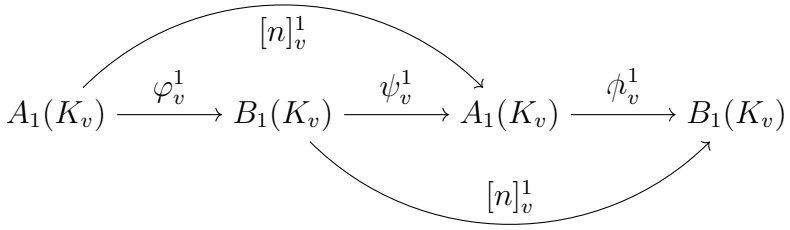
We continue by examining the quotient $\#\operatorname{coker}\varphi_v^1/\#\ker\varphi_v^1$. We start by recalling two basic lemmas, and then we deduce the well known fact that this quotient is almost always trivial, since φ_v^1 is an isomorphism for all but finitely many places v.

Lemma 3.2.10. *The kernel of reduction $A_1(K_v)$ is a pro-p-group.*

Proof. We have that $A_1(K_v)$ is isomorphic to the group $\hat{A}(\mathfrak{m}_v)$ associated to the formal group $\hat{A}$ of A defined over the valuation ring $\mathcal{O}_v$ of K_v with maximal ideal $\mathfrak{m}_v$. If an integer n is coprime to the characteristic p of the residue field k_v, then the multiplication-by-n endomorphism on $\hat{A}(\mathfrak{m}_v)$ is an isomorphism. It is an easy exercise to check that a profinite group is in fact a pro-p-group provided that the multiplication-by-ℓ map is an isomorphism for all primes $\ell \neq p$. Hence $A_1(K_v)$ is a pro-p-group. □

Lemma 3.2.11. *If $v \nmid \deg\varphi$ then φ_v^1 and $\varphi_{v,nr}^1$ are isomorphisms.*

Proof. Denote the degree of φ by n. There exist isogenies $\psi\colon B \to A$ and $\phi\colon A \to B$, such that $\psi\circ\varphi\colon A \to A$ and $\phi\circ\psi\colon B \to B$ are the multiplication-by-n maps $[n]$. Hence we get the following induced group homomorphisms on the kernels of reduction.



Since $v \nmid \deg\varphi$, we have by the previous lemma that both maps $[n]_v^1$ are isomorphisms. Hence it follows that all three homomorphisms ψ_v^1, ϕ_v^1 and φ_v^1 are isomorphisms. Now for any finite unramified extension L_w/K_v, we get by the same argument that φ_w^1 is an isomorphism, and so also is $\varphi_{v,nr}^1$. □

Corollary 3.2.12. *If a prime ℓ divides the cardinality of a kernel or cokernel of one of the induced group homomorphisms φ_v, φ_v^0, φ_v^1, $\overline{\varphi}_v$ or $\tilde{\varphi}_v^0$ appearing in diagrams 3.2.5 and 3.2.6, or ℓ divides the Tamagawa quotient $c_{B,v}/c_{A,v}$, then $\ell \mid \deg\varphi$. Further, if $\gcd(\deg\varphi, c_{A,v}\cdot c_{B,v}) = 1$, then $\overline{\varphi}_v$ is an isomorphism.*

In particular, if φ is of prime degree ℓ, then the cardinalities of all kernels and cokernels of φ_v, φ_v^0, φ_v^1, $\overline{\varphi}_v$ or $\tilde{\varphi}_v^0$, as well as the Tamagawa quotient $c_{B,v}/c_{A,v}$, are powers of ℓ.

Proof. By construction, the claim is clear for all the kernels. If φ is the multiplication-by-n endomorphism of A for a positive integer n, then this is also clear for the cokernels. For a general isogeny φ of degree n, as mentioned in the proof of the above lemma, there is an isogeny $\psi\colon B \to A$, such that $[n] = \psi\circ\varphi$. From the exact sequence

$$0 \to \ker\psi/\varphi(\ker[n]) \to \operatorname{coker}\varphi \to \operatorname{coker}[n]\operatorname{coker}\psi \to 0$$

we derive the statement about the cokernels of the homomorphisms induced by φ. Use lemma 3.2.9 to get the statement about the Tamagawa quotient.

Now assume that $\gcd(\deg\varphi, c_{A,v}\cdot c_{B,v}) = 1$. If a prime ℓ divides the Tamagawa quotient $c_{B,v}/c_{A,v}$ then $\ell \mid \deg\varphi$ by the above part of this lemma, hence ℓ does not divide the product $c_{A,v}\cdot c_{B,v}$. Therefore there are no primes ℓ dividing $c_{B,v}/c_{A,v}$ and thus $c_{B,v} = c_{A,v}$. This implies $\#\ker\varphi_v = \#\operatorname{coker}\varphi_v$. If a prime ℓ divides $\#\ker\varphi_v$, then ℓ divides $\deg\varphi$ and $c_{A,v}$, hence there are no such primes ℓ and $\overline{\varphi}_v$ is an isomorphism. □

We conclude that the product over all quotients $\#\operatorname{coker}\varphi_v/\#\ker\varphi_v$ is actually a finite product. Let S be a finite subset of M_K containing the infinite places, the places of bad reduction of A and B and the places dividing the degree of the isogeny φ.

Corollary 3.2.13. *If $v \nmid \deg \varphi$ and v is a place of good reduction then*

$$\frac{\#\operatorname{coker}\varphi_v}{\#\ker\varphi_v} = 1$$

thus

$$\prod_{v\in M_K} \frac{\#\operatorname{coker}\varphi_v}{\#\ker\varphi_v} = \prod_{v\in S} \frac{\#\operatorname{coker}\varphi_v}{\#\ker\varphi_v}$$

Proof. Use lemmas 3.2.9 and 3.2.11 and the fact that the Tamagawa quotient equals 1 in case of good reduction. □

In view of the corollary, our goal is to provide methods to compute the quotient $\#\operatorname{coker}\varphi_v/\#\ker\varphi_v$, in case v is a place of bad reduction or $v \mid \deg\varphi$. If we stick to good reduction, but do not care whether v divides the degree of φ, then the next lemma gives a very nice criterion to check whether $\operatorname{coker}\varphi_v$ is maximally unramified. The notation used in part (i) of the lemma comes from the following diagram.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_1(\overline{K}_v) & \longrightarrow & A_0(\overline{K}_v) & \longrightarrow & \tilde{A}_0(\overline{k}_v) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi^1_{\overline{K}_v}} & & \downarrow{\scriptstyle \varphi^0_{\overline{K}_v}} & & \downarrow{\scriptstyle \tilde{\varphi}^0_{\overline{k}_v}} & & \\ 0 & \longrightarrow & B_1(\overline{K}_v) & \longrightarrow & B_0(\overline{K}_v) & \longrightarrow & \tilde{B}_0(\overline{k}_v) & \longrightarrow & 0 \end{array}$$

Lemma 3.2.14 (Criterion for maximal unramifiedness of $\operatorname{coker}\varphi_v$ in case v is a place of good reduction)**.** *Assume that v si a place of good reduction.*

1. *If $\ker\varphi^1_{\overline{K}_v}$ is trivial then $\operatorname{coker}\varphi_v$ is maximally unramified.*
2. *If φ has a K_v-kernel and φ^1_v is injective then $\operatorname{coker}\varphi_v$ is maximally unramified.*

Proof. Statement (2) follows directly from (1), as the assumptions imply that $\ker\varphi^1_{\overline{K}_v} = \ker\varphi^1_v = 0$.

For part (1) note, that if $[\xi] \in H^1(K_v, A[\varphi])$ is an element of $\operatorname{coker}\varphi_v$, then $[\xi]$ lies in the kernel of $H^1(K_v, A[\varphi]) \to H^1(K_v, A)$. This means that there is a point $P \in A(K_v)$ such that $\xi(\sigma) = P^\sigma - P$, for all $\sigma \in G_{\overline{K}_v/K_v}$. As v is a place of good reduction we get that $P \in A_0(K_v)$. Consider the reduction-mod-v map $A_0(K_v) \to \tilde{A}_0(k_v)$, which is a group homomorphism. Hence, $\overline{P^\tau - P} = \overline{P}^\tau - \overline{P} = \mathcal{O}$, for all $\tau \in I_v$, as I_v acts trivially on $A_0(\overline{k}_v)$. Therefore for all $\tau \in I_v$, $P^\tau - P$ lies in the kernel of reduction $\varphi^1_{\overline{K}_v}$. As $\varphi^1_{\overline{K}_v}$ is assumed to be trivial we immediately deduce that $P^\tau - P = \mathcal{O}$, for all $\tau \in I_v$,

which is equivalent to $P \in A_0(K_v^{nr})$. By definition, $[\xi]$ lies in $H^1_{nr}(K_v, A[\varphi])$ if it is in the kernel of Res_{nr}. This is clearly the case if $P \in A(K_v^{nr})$, because this makes the restriction of ξ to I_v to be the zero map, and thus $\operatorname{coker} \varphi_v$ injects into $H^1_{nr}(K_v, A[\varphi])$. By lemmas 3.2.4 and 3.2.9, $\operatorname{coker} \varphi_v$ also surjects onto $H^1_{nr}(K_v, A[\varphi])$, as its order is at least the order of $H^1_{nr}(K_v, A[\varphi])$. □

We continue with presenting a reinterpretation given by Schaefer in [16] of the quotient $\#\operatorname{coker} \varphi_v^1 / \#\ker \varphi_v^1$. Using these results, it is very easy to compute $\#\operatorname{coker} \varphi_v^1 / \#\ker \varphi_v^1$ for elliptic curves. First we need some notation. Assume that the abelian varieties A and B are of dimension d and let $v \in M_K^0$ be a finite place. It is possible to write the isogeny $\varphi\colon A \to B$ as a d-tuple of power series in d-variables in a neighbourhood of the identity element $\mathcal{O}$. Let $|\varphi'(0)|_v$ be the normalised v-adic absolute value of the determinant of the Jacobian matrix of partial derivatives of such a power series representation of φ evaluated at 0. Note that $|\varphi'(0)|_v$ is well defined.

Proposition 3.2.15. *With notation as above,*

$$|\varphi'(0)|_v^{-1} = \frac{\#\operatorname{coker} \varphi_v^1}{\#\ker \varphi_v^1}$$

hence

$$|\varphi'(0)|_v = 1 \text{ if } v \nmid \deg \varphi$$

Proof. This is [16, Lemma 3.8] with the previous lemmas. □

Corollary 3.2.16. *With notation as above,*

$$\frac{\#\operatorname{coker} \varphi_v}{\#\ker \varphi_v} = |\varphi'(0)|_v \cdot \frac{c_{B,v}}{c_{A,v}}$$

Before we present our main criterion for checking that $\operatorname{coker} \varphi_v$ is maximally unramified, we give a basic lemma about $|\varphi'(0)|_v$ and the maps φ_v^1 and $\varphi_{v,nr}^1$. The aim of the lemma is to provide a way to replace $v \nmid \deg \varphi$ with the weaker assumption $e_v < p-1$, where e_v is the ramification index of the place v of K. Note, that if $K_v = Q_p$ and $p \neq 2$, then the condition about the ramification index is fulfilled, i.e. we have $e_v < p-1$.

Lemma 3.2.17. *With notation as above the following holds.*

1. *If $|\varphi'(0)|_v = 1$ and $\varphi_{v,nr}^1$ is injective, then φ_v^1 and $\varphi_{v,nr}^1$ are isomorphisms. Hence, if φ_v^1 and $\varphi_{v,nr}^1$ are injective, then φ_v^1 and $\varphi_{v,nr}^1$ are isomorphisms if and only if $|\varphi'(0)|_v = 1$.*

2. *If the ramification index $e_v < p-1$, then φ_v^1 and $\varphi_{v,nr}^1$ are injective.*

3. *If $K = \mathbb{Q}$, then φ_p^1 and $\varphi_{p,nr}^1$ are injective, unless $p = 2$ and $2 \mid \deg \varphi$.*

4. *If $K = \mathbb{Q}$ and $|\varphi'(0)|_v = 1$ then φ_v^1 and $\varphi_{v,nr}^1$ are isomorphisms, unless $p = 2$ and $2 \mid \deg \varphi$.*

Proof. Assume $|\varphi'(0)|_v = 1$, thus $|\varphi'(0)|_w = 1$ for all unramified finite field extensions L_w/K_v. Since $\varphi_{v,nr}^1$ is injective, the maps $\varphi_w^1 \colon A_1(L_w) \to B_1(L_w)$ are also injective. By proposition 3.2.15, the size of the kernels and cokernels of φ_w^1 agree and therefore all φ_w^1 are isomorphisms. Hence $\varphi_{v,nr}^1$ is an isomorphism, which proves (1).

For (2) use the isomorphism $A_1(K_v) \cong \hat{A}(\mathfrak{m}_v)$. Then use [21, IV, theorem 6.1] or the next lemma to conclude that φ_w^1 is injective for any finite unramified field extension L_w/K_v. Hence $\varphi_{v,nr}^1$ is injective. For (3) apply (2) in case $p \neq 2$. In case $2 \nmid \deg \varphi$, this is due to Lemma 3.2.11. Combing part (1) and part (3) gives part (4). □

Lemma 3.2.18. *With notation as above, if the ramification index $e_v < p-1$ then the reduction-mod-v map $A_0(K_v) \to \tilde{A}_0(k_v)$ has torsion-free kernel, i.e. $A_1(K_v)$ is torsion-free.*

In particular, this gives an injection $A(K)_{tors} \hookrightarrow \tilde{A}_0(k_v)$, thus if in addition v is a place of good reduction there is an injection $A(K)_{tors} \hookrightarrow \tilde{A}(k_v)$.

Proof. This is in the appendix of [8]. □

Theorem 3.2.20 provides our main criterion to check whether $\operatorname{coker} \varphi_v$ is maximally unramified. To state the next lemma we introduce the map

$$\delta_v^0 \colon \operatorname{coker} \varphi_v^0 \to H^1(K_v, A(\overline{K}_v)[\varphi])$$

it is obtained by composing the natural map $\operatorname{coker} \varphi_v^0 \to \operatorname{coker} \varphi_v$ with the connecting homomorphism $\delta_v \colon \operatorname{coker} \varphi_v \to H^1(K_v, A(\overline{K}_v)[\varphi])$. Since $\operatorname{coker} \varphi_v^0 \to \operatorname{coker} \varphi_v$ need not be injective, δ_v^0 may also not be injective. Similarly one defines the map

$$\delta_{v,nr}^0 \colon \operatorname{coker} \varphi_{v,nr}^0 \to H^1(K_v^{nr}, A(\overline{K}_v)[\varphi])$$

Lemma 3.2.19. *If $\varphi_{v,nr}^1$ is surjective, then the image of $\operatorname{coker} \varphi_v^0$ under δ_v^0 lies in $H_{nr}^1(K_v, A(\overline{K}_v)[\varphi])$.*

Proof. In the above diagram 3.2.7, the first vertical map $\varphi_{v,nr}^1$ is surjective by assumption. The third vertical map $\tilde{\varphi}_{\overline{k}_v}^0$ is surjective, since $\overline{k}_v$ is algebraically closed, therefore the middle vertical map $\varphi_{v,nr}^0$ is also surjective, i.e. $\operatorname{coker} \varphi_{v,nr}^0$ is trivial. The following diagram commutes.

$$\begin{array}{ccc} \operatorname{coker}\varphi_v^0 & \xrightarrow{\delta_v^0} & H^1(K_v, A(\overline{K}_v)[\varphi]) \\ \downarrow & & \downarrow Res_{nr} \\ \operatorname{coker}\varphi_{v,nr}^0 & \xrightarrow{\delta_{v,nr}^0} & H^1(K_v^{nr}, A(\overline{K}_v)[\varphi]) \end{array}$$

As the lower left group is trivial, the image of the upper left group in the lower right group must be trivial, i.e. the image of δ_v^0 lies in $H^1_{nr}(K_v, A(\overline{K}_v)[\varphi])$. □

Theorem 3.2.20 (Main criterion for maximal unramifiedness of $\operatorname{coker}\varphi_v$)**.** *Let $\varphi\colon A \to B$ be an isogeny between two abelian varieties A and B over a number field K, and let $v \in M_K^0$ be a finite place of K. If $\varphi^1_{v,nr}$ is surjective and φ_v^1 and $\overline{\varphi}_v$ are isomorphisms, then $\operatorname{coker}\varphi_v$ is maximally unramified.*

Proof. As $\overline{\varphi}_v$ is an isomorphism, $\operatorname{coker}\varphi_v^0 \to \operatorname{coker}\varphi_v$ is also an isomorphism. Hence by the above lemma, $\operatorname{coker}\varphi_v$ maps injectively onto a subgroup of $H^1_{nr}(K_v, A(\overline{K}_v)[\varphi])$. We complete the proof by showing that these two groups have same cardinality. By lemmas 3.2.4 and 3.2.9 we get

$$\#H^1_{nr}(K_v, A(\overline{K}_v)[\varphi]) = \#\ker\varphi_v = \#\operatorname{coker}\varphi_v$$

and this completes the proof. □

Corollary 3.2.21 (Criterion for maximal unramifiedness of $\operatorname{coker}\varphi_v$ in case $v \nmid \deg\varphi$)**.** *If $v \nmid \deg\varphi$ and $\gcd(\deg\varphi, c_{A,v}\cdot c_{B,v}) = 1$ then $\operatorname{coker}\varphi_v$ is maximally unramified.*

Proof. The corollary follows directly from theorem 3.2.20 together with lemma 3.2.11 and corollary 3.2.12. □

We also want to apply theorem 3.2.20 in case $v \mid \deg\varphi$. As seen in lemma 3.2.17, we may replace $v \nmid \deg\varphi$ with the conditions $e_v < p-1$ and $|\varphi'(0)|_v = 1$.

Corollary 3.2.22 (Criteria for maximal unramifiedness of $\operatorname{coker}\varphi_v$ in case $v \mid \deg\varphi$)**.** *Assume that the ramification index $e_v < p-1$.*

1. *If $|\varphi'(0)|_v = 1$ and $\gcd(\deg\varphi, c_{A,v}\cdot c_{B,v}) = 1$ then $\operatorname{coker}\varphi_v$ is maximally unramified.*

2. *If v is a place of good reduction, then $\operatorname{coker}\varphi_v$ is maximally unramified if and only if $|\varphi'(0)|_v = 1$.*

3. *If v is a place of good reduction and φ has a K_v-kernel, then $|\varphi'(0)|_v = 1$ and $\operatorname{coker}\varphi_v$ is maximally unramified.*

Proof. For part (1) combine lemma 3.2.17 with theorem 3.2.20 and corollary 3.2.12. For part (2) note, that $c_{A,v} = c_{B,v} = 1$. Hence, if $|\varphi'(0)|_v = 1$, then by (1) we get that $\operatorname{coker}\varphi_v$ is maximally unramified. Now assume that $\operatorname{coker}\varphi_v$ is maximally unramified,hence $\#\operatorname{coker}\varphi_v = \#\ker\varphi_v$. By corollary 3.2.16 we get that

$$|\varphi'(0)|_v = 1 = c_{B,v}/c_{A,v} = 1$$

which completes (2). For (3), combine (2) with lemmas 3.2.14 and 3.2.17. □

We summarise all the criteria for maximal unramifiedness for the case that $K = \mathbb{Q}$. The first one is easily applicable when A and B are elliptic curves.

Corollary 3.2.23 (Criteria for maximal unramifiedness of $\operatorname{coker}\varphi_p$ in case $K = \mathbb{Q}$)**.** *Let $\varphi\colon A \to B$ be an isogeny between two abelian varieties A and B over $\mathbb{Q}$ and let p be a prime such that $p \neq 2$ if $2 \mid \deg\varphi$.*

- *If $|\varphi'(0)|_p = 1$ and $\gcd(\deg\varphi, c_{A,v}\cdot c_{B,v}) = 1$ then $\operatorname{coker}\varphi_p$ is maximally unramified.*

- *If p is a place of good reduction and φ has a $\mathbb{Q}_p$-kernel, then $|\varphi'(0)|_p = 1$ and $\operatorname{coker}\varphi_p$ is maximally unramified.*

We end this section with a basic lemma about the infinite places.

Lemma 3.2.24. *Let L be either $\mathbb{R}$ or $\mathbb{C}$ and let A and B be abelian varieties over L. For an isogeny $\varphi\colon A \to B$ denote with $\varphi_\infty\colon A(L) \to B(L)$ the induced group homomorphism on L-rational points.*

1. *If $L = \mathbb{C}$, then $\#\operatorname{coker}\varphi_\infty/\#\ker\varphi_\infty = 1/\deg\varphi$.*

2. *If $L = \mathbb{R}$, then $\#\operatorname{coker}\varphi_\infty = 1$, if $2 \nmid \deg\varphi$.*

Proof. Part (1) is obvious, as $\mathbb{C}$ is algebraically closed and of characteristic 0, hence φ_∞ is surjective and the size of the kernel equals the degree. For (2) note, that $\operatorname{coker}\varphi_\infty$ embeds into $H^1(\mathbb{R}, A[\varphi])$, which is trivial if the order of $G_{\mathbb{C}/\mathbb{R}}$ is coprime to $A[\varphi]$. □

3.3 Isogenies of quotients of abelian varieties

In this section we will discuss the use of the uniformization of abelian varieties in order to calculate the local quotient of the Cassels-Tate equation. Let K be the field $\mathbb{Q}$ and K_v a p-adic completion with residue filed k_v. The two following theorem are [6, Theorem 6.7.6 and 6.7.8].

Theorem 3.3.1 (Stable reduction of abelian varieties)**.** *After a finite extension of the base field, the Neron model Y of the abelian variety A over K has the following property: Y_v, the component of the identity of the special fibre of Y at v, is an extension of an abelian variety over k_v by a split algebraic torus over k_v. Hence we have*

$$0 \to T(k_v) \to \tilde{A}_v(k_v) \to D(k_v) \to 0 \tag{3.3.2}$$

Theorem 3.3.3 (Uniformization of an abelian variety)**.** *Suppose that the abelian variety A over the field K_v (complete with respect to a discrete valuation v) has a Neron model Y such that Y_v is an extension of an abelian variety D over k_v by a split torus over k_v. Then the following data exists:*

1. *An abelian variety C over K_v and an extension G of C by a split torus T over K_v,*
2. *A lattice $\Lambda \subset G(K_v)$,*

such that G/Λ is an abelian variety and $A \cong G/\Lambda$. Moreover G and Λ are uniquely determined by A. Further D is canonically isomorphic to $\tilde{C}_v$ and the G is simply connected.

Definition 3.3.4. *The exact sequence*

$$0 \to \Lambda \to G \to A \to 0$$

is called the ***uniformization*** *of A.*

The previous theorem imply that $G \to A$ is the universal analytic covering of the abelian variety A.

Remark. *This theorem only holds on K_v. The group G and T greatly depends on the choice of the place.*

Let P be a point of $A(K)$ of prime order ℓ such that its reduction modulo v is not in the image of the torus of the sequence 3.3.2. We define the abelian variety $B = A/\langle P \rangle$ and the quotient isogeny $\varphi\colon A \to B$. From now on we assume that the place $v \nmid \ell$. By the uniformization theorem we can get for $A(K_v)$, respectively $B(K_v)$, the data (T, D, G, Λ, C), respectively $(T', D', G', \Lambda', C')$. Hence we have

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Lambda & \longrightarrow & G & \longrightarrow & A(K_v) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi_\Lambda} & & \downarrow{\scriptstyle \varphi_G} & & \downarrow{\scriptstyle \varphi_v} & & \\ 0 & \longrightarrow & \Lambda' & \longrightarrow & G' & \longrightarrow & B(K_v) & \longrightarrow & 0 \end{array}$$

Since G and G' are simply connected we have that the map φ_v can be lifted to a map $\varphi_G \colon G \to G'$ that induce a map $\varphi_\Lambda \colon \Lambda \to \Lambda'$.

Proposition 3.3.5. *One of the following two options holds:*

1. *φ_G is injective and $\#\operatorname{coker}\varphi_\Lambda = \ell$.*
2. *φ_G has kernel of order ℓ and φ_Λ is a bijection.*

Proof. Clearly $\ker\varphi_G$ can't have a higher order. If φ_G is injective then by the snake lemma we have $0 \to \ker\varphi_\Lambda \to 0$, hence φ_Λ is injective. Furthermore $\ker\varphi_v$ injects into $\operatorname{coker}\varphi_\Lambda$. The map φ_G is injective and by our assumption it is also injective over $\overline{K}_v$, so its image is a subvariety of G'. Since G and G' have the same dimension by construction the induced map $G_{\overline{K}_v} \to G'_{\overline{K}_v}$ is an isomorphism. Since the isogeny φ_v commutes with the Galois group (it is defined over K_v) then also the induced map φ_G commutes with the absolute Galois group hence by descent theory the map and its inverse is defined over K_v, so the map φ_G is surjective. Hence $\#\operatorname{coker}\varphi_\Lambda = \#\ker\varphi_v = \ell$.

If φ_G has kernel of order ℓ then both $\ker\varphi_G$ and $\ker\varphi_v$ have order ℓ, so they are both isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$ hence every map between them is a bijection (it will be $x \mapsto x^n$ for some n such that $\gcd(n,\ell) = 1$). Hence by the snake lemma we get $\ker\varphi_\Lambda = \operatorname{coker}\varphi_\Lambda = 0$. □

Furthermore since P is not in the kernel of the map $A \to C$ then the quotient by $\langle P \rangle$ induce also an isogeny $\varphi_C \colon C \to C'$ of the same degree. Hence again φ_C induces isogeny φ_G and φ_T as in the following diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & T & \longrightarrow & G & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi_T} & & \downarrow{\scriptstyle \varphi_G} & & \downarrow{\scriptstyle \varphi_C} & & \\ 0 & \longrightarrow & T' & \longrightarrow & G' & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

Now we start by analyzing the situation aver finite fields.

Lemma 3.3.6. *Maps between abelian varieties over finite fields have kernels and cokernels of the same order.*

Proof. This is the corollary on page 3 of [12]. □

Similarly we can show that also the maps between tori over finite fields have the same property. Hence from the previous diagram if K_v is a finite field then by the snake lemma $\#\operatorname{coker}\varphi_G = \#\ker\varphi_G$.

In the previous section we have already shown that the map φ_C has kernel and cokernel of the same order even over K_v since $v \nmid \ell$ and C has good reduction.

Now from the diagram 3.2.5 we get that the map $A_1(K_v) \to B_1(K_v)$ is an isomorphism and so the order of the kernel and cokernel of the map $A_0(K_v) \to B_0(K_v)$ is determined at the level of the reduction. In particular if the reduction is good then they have the same order. From theorem 3.3.1 there exists an extension L_w/K_v, tori T and T' and abelian varieties D and D' such that

$$\begin{array}{ccccccccc} 0 & \longrightarrow & T & \longrightarrow & \tilde{A}_w(l_w) & \longrightarrow & D & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & T' & \longrightarrow & \tilde{B}_w(l_w) & \longrightarrow & D' & \longrightarrow & 0 \end{array}$$

is a commutative diagram. Since D and D' have good reduction then kernel and cokernel of $D \to D'$ have the same cardinality. Hence we have the equality

$$\frac{c_{B,w}}{c_{A,w}} = \frac{\#\operatorname{coker}(T \to T')}{\#\ker(T \to T')}$$

Now returning to G and Λ we know that $G/\Lambda \cong A$ so

$$\#\ker(G/\Lambda \to G'/\Lambda') = \#\ker(A \to B) = \#\ker\varphi_v = \ell$$

Proposition 3.3.7. *If φ_G is injective then $\#\operatorname{coker}\varphi_v/\#\ker\varphi_v = 1/\ell$.*

Proof. If φ_G is injective as in the previous theorem it is also surjective, hence $G/\Lambda \to G'/\Lambda'$ is surjective. This completes the proof. □

Proposition 3.3.8. *If φ_G is not injective and $\mu_\ell \nsubseteq K_v$ then $\#\operatorname{coker}\varphi_v = \ell$.*

Proof. By corollary 3.2.2 we have that $H^1(K_v, A(\overline{K}_v)[\varphi]) = \mathbb{Z}/\ell\mathbb{Z}$ hence the cokernel must be of order ℓ. □

Chapter 4

Modular curves

The main examples of this thesis are quotients of Jacobian of modular curves. Modular curves are moduli space for moduli problem of elliptic curves (such as classify elliptic curves with a point of exact order N up to isomorphisms) but can also be defined as quotient of subspace of $\mathbb{C}$. They have a structure of Riemann varieties.

4.1 Congruence subgroup

Let R be a ring, we can define its linear subgroup of degree 2

$$GL_2(R) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in R, ad - bc \in R^* \right\} \tag{4.1.1}$$

where R^* is the multiplicative subgroup of R. Since the determinant map is multiplicative, $GL_2(R)$ is a group with respect to the matrix multiplication. We can further define the subgroup of $GL_2(R)$ of matrices with determinant equal to the identity of R, we call this group $SL_2(R)$.

From now on let $R = \mathbb{Z}$, we denote $SL_2(\mathbb{Z})$ with Γ, let I be the identity matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. We define some important subgroup of Γ.

Definition 4.1.2. *Let $N \in \mathbb{N}$, $N \geq 2$ then:*

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \;\middle|\; c \equiv 0 \,(mod\, N) \right\}$$

$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \;\middle|\; a \equiv d \equiv 1 \,(mod\, N) \;\mid c \equiv 0 \,(mod\, N) \right\}$$

$$\Gamma(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \;\middle|\; a \equiv d \equiv 1 \,(mod\, N)\,, b \equiv c \equiv 0 \,(mod\, N) \right\}$$

We always have

$$\Gamma \geq \Gamma_0(N) \geq \Gamma_1(N) \geq \Gamma(N)$$

Definition 4.1.3. *A **congruence subgroup** of level N is a subgroup Γ of $SL_2(\mathbb{Z})$ such that $\Gamma(N) \subseteq \Gamma$.*

We now consider the map $SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/N\mathbb{Z})$ given by the canonical reduction of the coefficients modulo N and we can easily check that the kernel is $\Gamma(N)$ and that this map is surjective. From the isomorphism theorem follows that $\frac{SL_2(\mathbb{Z})}{\Gamma(N)} \cong SL_2(\mathbb{Z}/N\mathbb{Z})$, and then

$$[SL_2(\mathbb{Z})\colon \Gamma(N)] = \#SL_2(\mathbb{Z}/N\mathbb{Z}) = N^3 \prod_{p|N}(1-p^{-2})$$

where p are primes.

Given a matrix $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$, the reduction of d modulo N belongs to $(\mathbb{Z}/N\mathbb{Z})^*$ because $ad - bc \equiv ad \equiv 1$ modulo N. We define the map $\Gamma_0(N) \to (\mathbb{Z}/N\mathbb{Z})^*$ given by $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto d$. It is well defined with respect to the product in $(\mathbb{Z}/N\mathbb{Z})^*$. Indeed $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} e & f \\ g & h \end{smallmatrix}\right) \mapsto (cf + dh) \equiv dh$ because $c = Nt$ for some $t \in \mathbb{Z}$. This map is also surjective: given $x \in (\mathbb{Z}/N\mathbb{Z})^*$ there is y such that $xy = 1$, and the matrix $\left(\begin{smallmatrix} y & 0 \\ 0 & x \end{smallmatrix}\right)$ will be in $\Gamma_0(N)$. The subset of $\Gamma_0(N)$ with $d = 1$ is $\Gamma_1(N)$ and it is the kernel of this map. From the isomorphism theorem follows that

$$[\Gamma_0(N)\colon \Gamma_1(N)] = \#(\mathbb{Z}/N\mathbb{Z})^* = \varphi(N) = N \prod_{p|N}(1-p^{-1})$$

where p are primes.

In the same way we define the map $\Gamma_1(N) \to \mathbb{Z}/N\mathbb{Z}$ given by $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto b$. This map is well defined with respect to $\mathbb{Z}/N\mathbb{Z}$. We have that $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} e & f \\ g & h \end{smallmatrix}\right)$ maps to $(af + bh) \equiv f + b$ since $a \equiv h \equiv 1$ modulo N. The kernel is given by $\Gamma_1(N)$ with $b \equiv 0 \pmod{N}$, i.e. $\Gamma(N)$. This map is easily proven to be surjective. Then by the isomorphism theorem follows that

$$[\Gamma_1(N)\colon \Gamma(N)] = \#\mathbb{Z}/N\mathbb{Z} = N$$

We have proven the following result.

Proposition 4.1.4.

$$[SL_2(\mathbb{Z}) : \Gamma(N)] = N^3 \prod_{p|N}(1-p^{-2})$$

$$[SL_2(\mathbb{Z}) : \Gamma_1(N)] = N^2 \prod_{p|N}(1-p^{-2})$$

$$[SL_2(\mathbb{Z}) : \Gamma_0(N)] = N \prod_{p|N}(1+p^{-1})$$

If Γ is a congruence subgroup of $SL_2(\mathbb{Z})$ then the index $[SL_2(\mathbb{Z}) : \Gamma]$ will be finite since $[SL_2(\mathbb{Z}) : \Gamma(N)]$ is.

Let $\mathcal{H} := \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$ be upper half plane of the complex plane, $\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$ and $\mathbb{P}^1_{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ be the Riemann sphere.

Definition 4.1.5. *We define an action of $GL_2(\mathbb{R})$ on $\mathbb{P}^1_{\mathbb{C}}$*

$$\begin{aligned} GL_2(\mathbb{R}) \times \mathbb{P}^1_{\mathbb{C}} &\to \mathbb{P}^1_{\mathbb{C}} \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} z &\mapsto \frac{az+b}{cz+d} \end{aligned} \tag{4.1.6}$$

where by convention we have $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\infty = \frac{a}{c}$ and $\frac{a}{0} = \infty$.

This is a group action, i.e. $(\gamma_1\gamma_2)(z) = \gamma_1(\gamma_2(z))$ and $Iz = z$. It is easy to check that $\gamma z = (-\gamma)z$ for all $\gamma \in GL_2(\mathbb{R})$.

We find that every point of $\mathcal{H}$ is mapped in a point of $\mathcal{H}$. Let $z \in H$ and $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$, we have

$$\mathrm{Im}(\gamma z) = \mathrm{Im}\frac{az+b}{cz+d} = \mathrm{Im}\frac{(az+b)(c\overline{z}+d)}{|cz+d|^2} = |cz+d|^{-2}\,\mathrm{Im}(adz+bc\overline{z})$$

Since $(adz + bc\overline{z}) = (ad - bc)\,\mathrm{Im}\, z = \det\gamma\,\mathrm{Im}\, z = \mathrm{Im}\, z$ because $\det\gamma = 1$, we get that $\mathrm{Im}\,\gamma z = |cz+d|^{-2}\mathrm{Im}\, z$. In particular if $\mathrm{Im}\, z > 0$ then $\mathrm{Im}\,\gamma z > 0$.

Now consider the set $\mathbb{P}^1(\mathbb{Q})$ called the set of the cusps. Γ acts transitively on it, since fo every fraction at its lowest terms $\frac{a}{c}$ we can find a matrix $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ solving $ad - bc = 1$ such that $\alpha\infty = \frac{a}{c}$. For a congruence subgroup $\Gamma' \subseteq \Gamma$ this is no longer true.

Definition 4.1.7. *A **cusp** of a congruence subgroup $\Gamma \subseteq SL_2(\mathbb{Z})$ is a class of equivalence the set of cusps under the action of Γ.*

4.2 Modular curves

There are three different ways to define a modular curves: the complex analytic, the algebraic and the moduli space setting. We use the first.

Definition 4.2.1. *Let $\mathcal{H}^*$ the extended upper half-plane of $\mathbb{C}$ and Γ a conguence subgroup of level N. We define the **modular curves***

$$X(\Gamma) = \Gamma\backslash\mathcal{H}^*$$

$$Y(\Gamma) = \Gamma\backslash\mathcal{H}$$

If Γ is respectively $\Gamma(N)$, $\Gamma_0(N)$ or $\Gamma_1(N)$ then we denote the curves above $X(N)$, $X_0(N)$, $X_1(N)$, $Y(N)$, $Y_0(N)$ and $Y_1(N)$ respectively.

The upper half plane $\mathcal{H}$ inherits the Euclidean topology as a subspace of $\mathbb{R}^2$. The natural surjection $\pi\colon \mathcal{H} \to Y(\Gamma)$ gives $Y(\Gamma)$ the quotient topology, meaning a subset of $Y(\Gamma)$ is open if its inverse image under π in $\mathcal{H}$ is open. Since $\mathcal{H}$ is connected and π is continuous, the quotient $Y(\Gamma)$ is also connected.

Proposition 4.2.2. *For any congruence subgroup Γ of $SL_2(\mathbb{Z})$, the modular curve $Y(\Gamma)$ is a connected and Hausdorff Riemann surface.*

Proof. This is [4, Corollary 2.1.2]. □

The topology on $\mathcal{H}^*$ consisting of its intersections with open complex disks (including disks $\{z \mid |z| > r\} \cup \infty$) contains too many points of $\mathbb{P}^1(\mathbb{Q})$ in each neighbourhood to make the quotient $X(\Gamma)$ Hausdorff. Instead, to put an appropriate topology on $X(\Gamma)$ start by defining for any $M > 0$ a neighbourhood

$$\mathcal{N}_M = \{\tau \in \mathcal{H} \mid \Im(\tau) > M\}$$

Adjoin to the usual open sets in $\mathcal{H}$ more sets in $\mathcal{H}^*$ to serve as a base of neighbourhoods of the cusps, the sets

$$\alpha(\mathcal{N}_M \cup \infty) \mid M > 0, \alpha \in SL_2(\mathbb{Z})$$

and take the resulting topology on $\mathcal{H}^*$. Since fractional linear transformations are conformal and take circles to circles, if $\alpha(\infty) \in \mathbb{Q}$ then $\alpha(\mathcal{N}_M \cup \infty)$ is a disk tangent to the real axis. Under this topology each $\gamma \in SL_2(\mathbb{Z})$ is a homeomorphism of $\mathcal{H}^*$. Finally, give $X(\Gamma)$ the quotient topology and extend natural projection to $\pi\colon \mathcal{H}^* \to X(\Gamma)$.

Proposition 4.2.3. *The modular curve $X(\Gamma')$ is a Hausdorff, connected, and compact Riemann surface.*

Proof. This is [4, Proposition 2.4.2]. □

The modular curve $X_1(N)$ has good reduction at every the prime but those dividing N.

Theorem 4.2.4. *The modular curve $X_1(p)$ for a prime p has bad reduction only at the prime p. The reduction is the disjoint union of 2 curves crossing at the supersingular points which over the algebraic closure are*

$$\frac{(p-1)^2(p+1)}{48}$$

Proof. See [9, Theorem 13.5.4 and 12.4.5]. □

4.3 The genus

It is important to know the genus of a modular curve since it is the dimension of its Jacobian variety.

We start giving the following definition.

Definition 4.3.1. *Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$. For each point $\tau \in \mathcal{H}$ let Γ_τ denote the isotropy subgroup of τ , i.e., the τ-fixing subgroup of Γ,*

$$\Gamma_\tau = \{\gamma \in \Gamma \mid \gamma(\tau) = \tau\}$$

*A point $\tau \in \mathcal{H}$ is an **elliptic point** for Γ (or of Γ) if Γ_τ is nontrivial as a group of transformations, that is, if the containment $\{\pm I\}\Gamma_\tau \supset \{\pm I\}$ of matrix groups is proper. The corresponding point $\pi(\tau) \in Y(\Gamma)$ is also called elliptic.*

The following theorem gives a formula to calculate the genus of modular curves.

Theorem 4.3.2. *Let Γ be a congruence subgroup containing $\Gamma(N)$ for some $N \in \mathbb{N}$. Let ϵ_2 and ϵ_3 denote the number of elliptic points of period 2 and 3 respectively. Let s be the number of cusps and g be the genus of $X(\Gamma)$. Then we have*

$$g = 1 + \frac{[SL_2(\mathbb{Z}) \colon \Gamma]}{12} - \frac{\epsilon_2}{4} - \frac{\epsilon_3}{3} - \frac{s}{2}$$

Let φ denote the Euler functions and p a prime number. In the case $\Gamma_0(N)$ we have

1. $[SL_2(\mathbb{Z}) \colon \Gamma_0(N)] = N \prod_{p|N} \left(1 + \frac{1}{p}\right)$
2. $\epsilon_2 = \begin{cases} 0 & \text{if } 4 \mid N \\ \prod_{p|N} \left(1 + \left(\frac{-1}{p}\right)\right) & \text{otherwise} \end{cases}$
3. $\epsilon_3 = \begin{cases} 0 & \text{if } 9 \mid N \\ \prod_{p|N} \left(1 + \left(\frac{-3}{p}\right)\right) & \text{otherwise} \end{cases}$
4. $s = \sum_{d|N, d>0} \varphi(\gcd(d, N/d))$

In the case $\Gamma_1(N)$ with $N \geq 4$ we have

1. $[SL_2(\mathbb{Z}) \colon \Gamma_1(N)] = \frac{1}{2} N^2 \prod_{p|N} \left(1 - \frac{1}{p^2}\right)$

2. $\epsilon_2 = 0$

3. $\epsilon_3 = 0$

4. $s = \begin{cases} \frac{1}{2}\sum_{d|N,d>0} \varphi(d)\varphi(N/d) & \text{if } N \geq 5 \\ 3 & \text{if } N = 4 \end{cases}$

In the case $\Gamma(N)$ *with* $N \geq 2$ *we have*

1. $[SL_2(\mathbb{Z})\colon \Gamma(N)] = \begin{cases} \frac{1}{2}N^3 \prod_{p|N}\left(1 - \frac{1}{p^2}\right) & \text{if } N > 2 \\ 6 & \text{if } N = 2 \end{cases}$

2. $\epsilon_2 = 0$

3. $\epsilon_3 = 0$

4. $s = \begin{cases} \frac{1}{2}N^2 \prod_{p|N}\left(1 - \frac{1}{p^2}\right) & \text{if } N > 2 \\ 3 & \text{if } N = 2 \end{cases}$

Proof. This is [4, Theorem 3.1.1] and [7, Theorem 3.1.2]. □

Corollary 4.3.3. *Let* $p \geq 5$ *be a prime number, then*

$$g(X_1(p)) = \frac{(p-5)(p-7)}{24}$$

4.4 The modular Jacobian

The Jacobian variety associated to the modular curve $X_*(N)$ is denoted by $J_*(N)$. In the case $N = p$ a prime we get that $J_1(p)$ has good reduction at all prime but p and from [3] its Neron model has connected fibres.

Proposition 4.4.1. *The primes* p *such that* $J_1(p)$ *has positive rank are*

$$p = 37, 43, 53, 61, 67 \text{ and all } p \geq 73$$

Proof. See [3, Proposition 6.2]. □

Proposition 4.4.2. *The quotient of* $J_1(p)$ *modulo a subgroup generated by a* $\mathbb{Q}$*-rational point has good reduction at every prime but* p*.*

Proof. The canonical quotient map $\pi\colon J_1(P) \to J_1(p)/\langle P\rangle$ is a surjective homomorphism, then apply [19, Corollary 2]. □

Chapter 5

Quotients of $J_1(p)$

In this last chapter we will study the order of the Tate-Shafarevich group for quotients of $J_1(p)$ modulo a cyclic subgroup generated by a $\mathbb{Q}$-rational point P. We will focus our attention on $p = 13$ and $p = 17$. In these cases there exist points of order 19 and 73 respectively. For these two primes the rank of $J_1(p)$ is zero, so there is only torsion over $\mathbb{Q}$. From the formulas for the genus of $X_1(p)$ we get the dimension of the Jacobian varieties:

$$\dim J_1(13) = g\left(X_1(13)\right) = 2$$

$$\dim J_1(17) = g\left(X_1(17)\right) = 5$$

Let P be a $\mathbb{Q}$-rational point of $J_1(p)$ of order ℓ. Let φ be the quotient isogeny $J_1(p) \to J_1(p)/\langle P\rangle$ with kernel $\langle P\rangle$ and so $\deg\varphi = \ell$.

5.1 Local quotient

Since the only prime of bad reduction is p we need only to check the local quotient at p, ℓ and at the infinity (the archimedean place).

By lemma 3.2.24 we have that at infinity

$$\frac{\#\operatorname{coker}\varphi_\infty}{\#\ker\varphi_\infty} = \frac{1}{\ell}$$

At the prime ℓ we have good reduction and the map has a $\mathbb{Q}_\ell$ kernel so by corollary 3.2.23 we have that the map φ_ℓ^1 is an isomorphism. Since we have good reduction also the local Tamagawa numbers equal 1, so

$$\frac{\#\operatorname{coker}\varphi_\ell}{\#\ker\varphi_\ell} = 1$$

The last prime to check is p. The special fibre of the Neron model of $J_1(p)$ has only one connected component by [3]. The point P is a torsion point and so by lemma 3.2.18 it does not lies in the kernel of the reduction map, hence the reduced map $\tilde{\varphi}_p^0$ has non-trivial kernel and cokernel. Appling the snake lemma to the diagram 3.2.5 we get that $\operatorname{coker}\varphi_p^0$ surjects into $\operatorname{coker}\tilde{\varphi}_p^0$, so $\operatorname{coker}\varphi_p^0$ cannot be trivial. Since for an abelian variety A the index $[A(\mathbb{Q}_p)_0 \colon A(\mathbb{Q}_p)]$ is equal to the number of connected components of the special fibre we get that

$$[J_1(p)(\mathbb{Q}_p)_0 \colon J_1(p)(\mathbb{Q}_p)] = 1$$

hence $J_1(p)(\mathbb{Q}_p) = J_1(p)(\mathbb{Q}_p)_0$. This shows that $\operatorname{coker}\varphi_p$ is non-trivial. The field $\mathbb{Q}_p$ does not contain any ℓ-th root of the unity in both of our cases and $p \nmid \ell$, so by corollary 3.2.2 we get

$$H^1(\mathbb{Q}_p, J_1(p)(\overline{Q}_p)[\varphi]) = \mathbb{Z}/\ell\mathbb{Z}$$

Putting together these results we have that $\#\operatorname{coker}\varphi_p = \ell$. Since φ_p has a $\mathbb{Q}_p$ kernel we conclude that

$$\frac{\#\operatorname{coker}\varphi_p}{\#\ker\varphi_p} = 1$$

Now we recap the value of the local quotient at the places where it can be different from 1:

Place	$J_1(13)$	$J_1(17)$
p	1	1
l	1	1
∞	1/19	1/73

5.2 Global quotient

By the definition φ has kernel of order ℓ. The kernel of the dual map is the Cartier dual of $\ker\varphi$. Since $\ker\varphi \cong \mathbb{Z}/\ell\mathbb{Z}$ it follows that $\ker\varphi^\vee \cong \mu_\ell$ but $\mathbb{Q}$ does not contains any non trivial ℓ-th root of the unity, so the kernel of the dual map has order 1. The trickiest part to calculate is the order of the cokernels.

In the next table we recap all the order of the pieces of the global quotient:

	$J_1(13)$	$J_1(17)$
$\ker \varphi$	19	73
$\operatorname{coker} \varphi$	?	?
$\ker \varphi^\vee$	1	1
$\operatorname{coker} \varphi^\vee$	?	?

5.3 Order of the Tate-Shafarevich group

We can now calculate the order of the Tate-Shafarevich group of this two varieties. From the previous arguments we have that

$$Ш\left(\frac{J_1(13)}{\langle P\rangle}/\mathbb{Q}\right) = \frac{\#\operatorname{coker}\varphi_K}{\#\operatorname{coker}\varphi_K^\vee}\cdot k^2$$

$$Ш\left(\frac{J_1(17)}{\langle P\rangle}/\mathbb{Q}\right) = \frac{\#\operatorname{coker}\varphi_K}{\#\operatorname{coker}\varphi_K^\vee}\cdot k^2$$

Bibliography

[1] J. W. S. Cassels, "Arithmetic on curves of genus 1. IV. Proof of the Hauptvermutung", in: *Journal Reine Angewandte Mathematik* 211 (1962), pp. 95–112.

[2] J. W. S. Cassels, "Arithmetic on curves of genus 1. VIII. On conjectures of Birch nd Swinnerton-Dyer", in: *Journal Reine Angewandte Mathematik* 217 (1965), pp. 180–199.

[3] B. Conrad, B. Edixhoven and W. Stein, "$J_1(p)$ has connected fibers", in: *Documenta Mathematica* 8 (2003), pp. 331–408.

[4] F. Diamond and J. Shurman, *A First Course in Modular Forms*, Graduate Texts in Mathematics 228, Springer-Verlag New York, 2005.

[5] M. Flach, "A generalization of the Cassels-Tate pairing", in: *Journal Reine Angewandte Mathematik* 412 (1990), pp. 113–127.

[6] J. Fresnel and M. van der Put, *Rigid Analytic Geometry and Its Applications*, Progress in Mathematics 218, Birkhäuser Basel, 2004.

[7] H. Hida, *Geometric Modular Forms and Elliptic Curves*, World Scientific, 2012.

[8] N. M. Katz, "Galois properties of torsion points on abelian varieties", in: *Inventiones mathematicae* 62(3) (1981), pp. 481–502.

[9] N. M. Katz and B. Mazur, *Arithmetic Moduli of Elliptic Curves*, Princeton University Press, 1985.

[10] S. Keil, "On non-square order Tate-Shafarevich groups of non-simple abelian surfaces over the rationals", PhD thesis, Humboldt-Universität zu Berlin, Mathematisch-Naturwissenschaftliche Fakultät II, 2014, DOI: `http://dx.doi.org/10.18452/16901`.

[11] S. Lang, "Algebraic group over finite fields", in: *American Journal of Mathematics* 78 (1956), pp. 555–563.

[12] S. Lichtenstein, *Tate's isogeny theorem for abelian varieties over finite fields*, URL: http://virtualmath1.stanford.edu/~conrad/mordellsem/Notes/L03.pdf.

[13] J. S. Milne, *Abelian Varieties*, version 2.0, 2008, URL: https://www.jmilne.org/math/CourseNotes/AV.pdf.

[14] J. S. Milne, *Arithmetic duality theorem*, 2nd ed., BookSurge LLC, 2006.

[15] D. Mumford, "Abelian varieties", in: *Studies in Mathematics* 5 (1970), Published for the Tata Institute of Fundamental Research.

[16] E. F. Schaefer, "Class group and Selmer group", in: *Journal of Number Theory* 56(1) (1996), pp. 79–114.

[17] E. F. Schaefer and M. Stoll, "How to do a p-descent on an elliptic curve", in: *Transactions of the American Mathematical Society* 356 (2004), DOI: https://doi.org/10.1090/S0002-9947-03-03366-X, URL: http://www.mathe2.uni-bayreuth.de/stoll/papers/p-descent-long.pdf.

[18] J. P. Serre, *Galois cohomology*, Springer Monographs in Mathematics, Berlin: Springer-Verlag, 2002.

[19] J. P. Serre and J. Tate, "Good Reduction of Abelian Varieties", in: *Annals of Mathematics*, Second series 88 (3) (1968), pp. 492–517.

[20] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, 1st ed., Graduate Texts in Mathematics 151, Springer-Verlag New York, 1994.

[21] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Graduate Texts in Mathematics 106, Springer-Verlag New York, 2009.

[22] W. A. Stein, "Shafarevich-Tate Groups of Nonsquare Order", in: *Modular Curves and Abelian Varieties*, Progress in Mathematics, ed. by Birkhäuser, vol. 224, Basel, 2004, pp. 277–289.

[23] J. Tate, "Duality theorem in Galois cohomology over number fields", in: *Proceedings of the international congress of mathematicians (Stockholm 1962)*, Institut Mittag-Leffler, Djursholm, 1963, pp. 288–295.

[24] J. Tate, "On the conjecture of Birch and Swinnerton-Dyer and a geometric analog", in: *Séminaire Bourbaki* 9 (1995), ed. by Paris Societe Mathematique de France, pp. 415–440.