Roni Mitra

A Combinatorial Approach to the Geometry of Shimura Curves over Discrete Valuation Rings

Thesis Advisor: Dr. Pierre Parent

Introduction

The aim of this thesis is to introduce important objects in arithmetic geometry like modular forms, modular curves, Shimura curves, etc., and to study some of their geometric properties. More precisely, for X a Shimura curve over $\mathbb{Q}$ and $X \to J$ an Albanese morphism to its Jacobian, consider the extension: $X^{\mathrm{sm}} \to \mathcal{J}$ from the smooth locus X^{sm} of the Cerednik-Drinfeld model of X over $\mathbb{Z}_p$, to the Néron model $\mathcal{J}$ of J over $\mathbb{Z}_p$. A natural question to ask is: "When is this extended morphism a closed immersion?"

Thanks to a theorem of Edixhoven, we can in fact reduce this abstract question to a just a combinatorial problem. Indeed, we will see that there is a notion of "dual graph" associated to our Shimura curve, and Edixhoven's theorem allows us to translate this property of being a closed immersion into a property of "non-disconnectivity" of this graph.

After having defined all these objects, we will qualitatively describe the graphs for the Shimura curves X_{pq} of discriminant equal to a product of two primes p and q, and indicate that "generically", they should be "non-disconnecting". We will support this intuition by a theorem of Parent and Yafaev describing some asymptotic behaviour of these graphs. We will however conclude our work by showing that if $p = 2$, then there are infinitely many q s such that the corresponding graphs are indeed disconnecting.

The Organization of the Thesis

In Chapter 1, we will recall some basic concepts about abelian varieties, divisors on curves, jacobians and modular forms.

In Chapter 2, we will introduce the notion of the "dual graph" $\mathcal{G}$ attached to "good" models of "good" curves. There is a torus T associated to such curves also, and the character group X of this torus turns out to be equal to $H_1(\mathcal{G}, \mathbb{Z})$. Then we will show that we get the same result even under the weaker assumption that the curve is "admissible" in the sense of Jordan-Livné.

In Chapter 3, we will first review some concepts from quaternion algebras. We will show that there is a way by which Eichler orders in quaternion algebras can be linked to "enhanced elliptic curves". Then we will proceed to discuss about the action of Hecke operators on the character group of $X_0(M)_{\overline{\mathbb{F}}_q}$.

In Chapter 4, we will first explain what Shimura curves are. Using the results found in Chapter 3, we will then qualitatively determine what $\mathcal{G}$ is for a given Shimura curve. In particular, for the Shimura curves X_{pq}, it turns out that there is a theoretically simple fomulation of the corresponding

dual graph $\mathcal{G}(X_{pq}/\overline{\mathbb{F}_p})$ in terms of p-isogenies between isomorphism classes of supersingular elliptic curves in characteristic q and supersingular j-invariants.

In Chapter 5, the final chapter, we will finally come to the heart of the thesis. We will try to answer the question regarding whether the extended Albanese morphism ${X_{pq}}^{\mathrm{sm}} \longrightarrow \mathcal{J}$ that we posed above is a closed immersion or not. As was previously told, it turns out by Edixhoven's theorem that to answer this question, it is enough to look at the dual graph $\mathcal{G}(X_{pq}/\overline{\mathbb{F}_p})$ and examine its non-disconnectivity. Parent-Yafaev theorem indicates that for $p > 3$, the answer aymptotically tends to be "Yes". We will prove that for $p = 2$, the answer is "No" for infinitely many q s.

Contents

1 Some Background Material

This chapter aims at familiarizing the readers with a few concepts from abelian varieties and modular forms that we will need for understanding the rest of the material in this thesis, assuming them to possess only some basic scheme-theoretic vocabulary.

1.1 Some Algebraic Geometry.

In this section we will quickly review the definitions of some objects in algebraic geometry beyond schemes-everything from group schemes to Néron models.

Definition. Group Scheme. A group scheme over S, or an S-group scheme, is an S-scheme $\pi : G \longrightarrow S$ together with S-morphisms $m : G \times_S G \longrightarrow G$ (group law, or multiplication), $i : G \longrightarrow G$ (inverse) and $e : S \longrightarrow G$ (identity section), such that the following identities of morphisms hold:

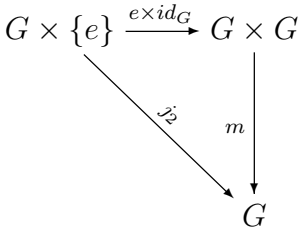
i)Associativity: $m \circ (m \times id_G) = m \circ (id_G \times m) : G \times_S G \times_S G \longrightarrow G$.

$$\begin{array}{ccc} G \times_S G \times_S G & \xrightarrow{id_G \times m} & G \times_S G \\ \downarrow{\scriptstyle m \times id_G} & & \downarrow{\scriptstyle m} \\ G \times_S G & \xrightarrow{m} & G \end{array}$$

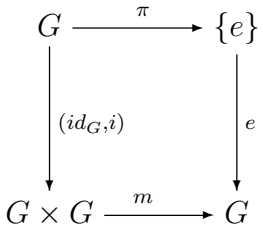
ii)Identity element: $m \circ (e \times id_G) = j_1 : S \times_S G \longrightarrow G$

$$\begin{array}{ccc} \{e\} \times G & \xrightarrow{e \times id_G} & G \times G \\ & \searrow^{j_1} & \downarrow{\scriptstyle m} \\ & & G \end{array}$$

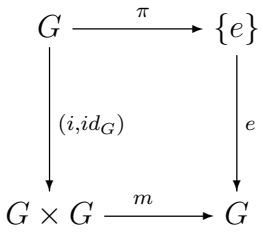
and $m \circ (id_G \times e) = j_2 : G \times_S S \longrightarrow G$.



iii)Two-sided inverse: $e \circ \pi = m \circ (id_G \times i) \circ \Delta_{G/S} = m \circ (i \times id_G) \circ \Delta_{G/S} : G \longrightarrow G$.



and



where $j_1 : S \times_S G \longrightarrow G$ and $j_2 : G \times_S S \longrightarrow G$ are the canonical isomorphisms.

A group scheme G is said to be *commutative* if, writing $s : G \times_S G \longrightarrow G \times_S G$ for the isomorphism switching the two factors, we have the identity $m = m \circ s : G \times_S G \longrightarrow G$.

Let $(\pi_1 : G_1 \longrightarrow S, m_1, i_1, e_1)$ and $(\pi_2 : G_2 \longrightarrow S, m_2, i_2, e_2)$ be two group schemes over S. A *homomorphism* of S-group schemes from G_1 to G_2 is a morphism of schemes $f : G_1 \longrightarrow G_2$ over S such that $f \circ m_1 = m_2 \circ (f \times f) : G_1 \times_S G_1 \longrightarrow G_2$. (This condition implies that $f \circ e_1 = e_2$ and $f \circ i_1 = i_2 \circ f$.)

Example of a Group Scheme. Given a scheme S, $\mathbb{G}_{\mathbf{m},S} := \mathbb{G}_{\mathbf{m},\mathbb{Z}} \times_{\mathrm{Spec}(\mathbb{Z})} S$ is a group scheme, where $\mathbb{G}_{\mathbf{m},\mathbb{Z}} = \mathrm{Spec}\mathbb{Z}[t, \frac{1}{t}]$. When we write $\mathbb{G}_{\mathbf{m}}$, it is understood that we are talking about $\mathbb{G}_{\mathbf{m},\mathbb{Z}}$.

Definition. Variety. For us, a variety over a field k will be a k-scheme which is separated, of finite type and geometrically integral over $\mathrm{Spec}(k)$.

Definition. Abelian Variety. An abelian variety over a field k is a proper k-variety which is a k-group scheme.

Notation. Given an abelian variety G over k, we define $G^{\mathbf{0}}$ to be the connected component of G containing 0, i.e., the image of $\varepsilon : \mathrm{Spec}(k) \longrightarrow G$.

Definition. Abelian Scheme. For S any scheme, an abelian scheme over S is a S-group scheme A which is proper, smooth and geometrically connected over S.

Definition. Isogeny. An isogeny between two S-abelian schemes is an S-homomorphism (i.e. a morphism as S-group schemes) which is finite, flat and surjective.

Definition. Semiabelian Scheme. A group scheme which is separated, smooth, commutative, such that each fiber is an extension of an abelian variety by a torus is called a semiabelian scheme.

Definition. Polarization. A polarization of an abelian variety is an isogeny from an abelian variety to its dual. A principal polarization is an isomorphism between an abelian variety and its dual.

Definition. Model. If S is a scheme, T a scheme over S, and X a scheme over T, what we call a model for X over S will be a S-scheme $\mathcal{X}$ such that $X \simeq \mathcal{X} \times_S T$.

So $X_{/T}$ has a model over S if "X can be defined over S". Of course models need not be unique. The question then is to find "good" models. This may have a geometric sense: for instance, if X/T is smooth, proper, or so, it makes sense to ask the same for its model over S. The notion of a good model can also have a structural sense, for example, if X/T is a group scheme, we may want this structure to come from the one already defined over S. Still, the notion of a good model may have a functorial meaning: if X represents an interesting functor on $\underline{\mathrm{Sch}}_{/T}$, one can ask for $\mathcal{X}$ to represent "the same functor" on $\underline{\mathrm{Sch}}_{/S}$.

Definition. Néron model. Let R be a Dedekind domain with fraction field K, and let A_K be an abelian variety. A Néron model $A_R = N(A_K)$ for A_K is a smooth group scheme over R whose generic fiber is A_K and which satisfies the following universal property (Néron Mapping Property):
Let $\mathcal{X}_R$ be a smooth R-scheme, and let $\phi_K : X_K \to A_K$ be a rational map defined over K. Then there exists a unique R-morphism $\phi_R : \mathcal{X}_R \to \mathcal{A}_R$ extending ϕ_K.

Clearly, this universal property characterizes the Néron model. It is a deep theorem that Néron models exist.

1.2 Divisors on Curves and Linear Equivalence.

Let X be a projective nonsingular curve over an algebraically closed field k. A *divisor* on X is a formal finite $\mathbb{Z}$-linear combination of $\sum_{i=1}^{m} n_i P_i$ closed points of X. Let $\mathrm{Div}(X)$ be the set of all divisors on X. The degree of a divisor $\sum_{i=1}^{m} n_i P_i$ is the integer $\sum_{i=1}^{m} n_i$. Let $\mathrm{Div}^0(X)$ denote the subgroup of divisors of degree 0.

Suppose k is a perfect field (for example, k has characteristic 0 or is a finite field), but not necessarily algebraically closed. We define the group of divisors of X over k be the subgroup

$$\mathrm{Div}(X) = \mathrm{Div}(X/k) = H^0(\mathrm{Gal}(\overline{k}/k), \mathrm{Div}(X/\overline{k}))$$

of elements of $\mathrm{Div}(X/\overline{k})$ that are fixed by every automorphism of $\overline{k}/k$. Likewise, we define $\mathrm{Div}^0(X/\overline{k})$ to be the elements of $\mathrm{Div}(X/\overline{k})$ of degree 0.

A *rational function* on an algebraic curve X is a function $X \longrightarrow {\mathbb{P}_k}^1$, which is locally defined by polynomials which have only a finite number of poles. For example, if X is the elliptic curve over k defined by $y^2 = x^3 + ax + b$, then the field of rational functions on X is the fraction field of the integral domain $k[x,y]/(y^2 - (x^3 + ax + b))$. Let $K(X)$ denote the field of all rational functions on X.

There is a natural homomorphism $K(X)^* \longrightarrow \mathrm{Div}(X)$ which associates to a rational function f its divisor

$$(f) = \mathrm{ord}_P(f).P$$

where $\mathrm{ord}_P(f)$ is the order of vanishing of f at P. Since X is nonsingular, the completed local ring of X at P is isomorphic to $k[[t]]$. We can thus write $f(t) = t^r g(t)$ for some $g(t) \in k[[t]]$. Then $R = \mathrm{ord}_P(f)$.

It is a standard fact in the theory of algebraic curves that if f is a non-zero rational function, then $(f) \in \mathrm{Div}^0(X)$, i.e., the number of zeroes of f counted with multiplicity equals the number of poles of f. The *Picard group* $\mathrm{Pic}(X)$ of X is the group of divisors on X modulo linear equivalence, i.e., a divisor $D \in \mathrm{Div}(X)$ represents the same class of divisors in $\mathrm{Pic}(X)$ as $D + (f)$, for any $f \in K(X)^*$. Since divisors of the form (f) have degree 0, the subgroup $\mathrm{Pic}^0(X) \in \mathrm{Pic}(X)$ of divisors on X of degree 0, modulo linear equivalence, is well-defined. Moreover, we have an exact sequence of abelian groups
$0 \longrightarrow K(X)^* \longrightarrow \mathrm{Div}^0(X) \longrightarrow \mathrm{Pic}^0(X) \longrightarrow 0$.

Thus, for any algebraic curve X we have associated to it an abelian group $\mathrm{Pic}^0(X)$. Suppose $\pi : X \longrightarrow Y$ is a morphism of algebraic curves. If $P \in \mathrm{Div}(Y/\overline{k})$ is a point, let $\pi^*(P)$ be the sum $\sum e_{Q/P} Q$ where $\pi(Q) = P$ and $e_{Q/P}$ is the ramification degree of Q/P. So, if D is a divisor on Y, the pullback $\pi^*(D)$ (which is defined linearly from the definition of π^P) is a divisor on X. We can show that $\mathrm{Div}(Y) \longrightarrow \mathrm{Div}(X)$ induces a homomorphism $\mathrm{Pic}^0(Y) \longrightarrow \mathrm{Pic}^0(X)$. Furthermore, we obtain the contravariant *Picard functor* from the category of algebraic curves over a fixed base field to the category of abelian groups, which sends X to $\mathrm{Pic}^0(X)$ and $\pi : X \longrightarrow Y$ to $\pi^* : \mathrm{Pic}^0(Y) \longrightarrow \mathrm{Pic}^0(X)$.

Alternatively, instead of defining morphisms by pullback of divisors, one can define the push forward. Suppose $\pi : X \longrightarrow Y$ is a morphism of algebraic curves and D is a divisor on X. If $P \in \mathrm{Div}(X/\overline{k})$ is a point, let $\pi_*(P) = \pi(P)$. Then π_* induces a morphism $\mathrm{Pic}^0(X) \longrightarrow \mathrm{Pic}^0(Y)$. We again obtain a functor, called the covariant *Albanese functor* from the category of algebraic curves to the category of abelian groups, which sends X to $\mathrm{Pic}^0(X)$ and $\pi : X \longrightarrow Y$ to $\pi_* : \mathrm{Pic}^0(X) \longrightarrow \mathrm{Pic}^0(Y)$.

1.3 An Algebraic Definition of the Jacobian.

First, we describe some universal properties of the Jacobian of an algebraic curve X over a field k under the hypothesis that $X(k) \neq \emptyset$. The Jacobian variety of X is an abelian variety J such that for an extension k'/k, there is

a (functorial) isomorphism $J(X/k') \longrightarrow \mathrm{Pic}^0(X/k')$.

Fix a point $P \in X(k)$. Then we obtain a map $f : X(k) \longrightarrow \mathrm{Pic}^0(X/k)$ by sending $Q \in X(k)$ to the divisor class of $Q - P$. One can show that if X has positive genus, then this map is induced by an injective morphism of algebraic varieties $X \hookrightarrow J$. This morphism has the following universal property: if A is an abelian variety and $g : X \longrightarrow A$ is a morphism that sends P to $0 \in A$, then there is a unique homomorphism $\psi : J \longrightarrow A$ of abelian varieties such that $g = \psi \circ f$.

This condition uniquely characterizes J, since if some other pair $(J', f' : X \longrightarrow J')$ has this universal property too, then there will be unique maps $J \longrightarrow J'$ and $J' \longrightarrow J$ whose composition in both directions must be the identity (use the universal property with $A = J$ and $f = g$).

The property $J \approx \mathrm{Pic}^0(J)$ (Abel-Jacobi) of Jacobians is used very often.

1.4 Modular Forms.

Let N be a positive integer. The *principal congruence subgroup of level N* is defined as:

$$\Gamma(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} (\mathrm{mod} \quad N) \right\}$$

Definition. Congruence Subgroup. A subgroup Γ of $\mathbf{SL}_2(\mathbb{Z})$ is a *congruence subgroup* if $\Gamma(N) \subset \Gamma$ for some $N \in \mathbb{Z}^+$, in which case Γ is a congruence subgroup of **level** N.

Examples of Congruence Subgroups:

$$(1)\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} (\mathrm{mod} \quad N) \right\}$$

$$(2)\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} (\mathrm{mod} \quad N) \right\}$$

One has an isomorphism: $\Gamma_0(N)/\Gamma_1(N) \simeq (\mathbb{Z}/N\mathbb{Z})^*$
defined by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto d (\mathrm{mod}\ N)$

The *upper-half plane* is $\mathcal{H} := \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$. We write: $\mathcal{H}^* := \mathcal{H} \cup \{\infty\} \cup \mathbb{Q}$.

Definition. Modular Curve. A modular curve is given as a quotient: $\Gamma\backslash(\mathcal{H} \cup \infty \cup \mathbb{Q})$ for some congruence subgroup Γ.

Examples of Modular Curves: People frequently work with the classical modular curves $X_0(N)$ and $X_1(N)$, which correspond to the congruence subgroups $\Gamma = \Gamma_0(N)$ and $\Gamma = \Gamma_1(N)$ respectively.

Important Fact. Modular curves over $\mathbb{C}$ define Riemann surfaces.

If $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ and $f : \mathcal{H} \longrightarrow \mathbb{C}$ is a function, we define

$$f_{|[g_k]}(z) := (cz + d)^{-k} f(gz).$$

Definition. Modular form. Let k be a non-negative integer and Γ be a congruence subgroup. A modular form f of weight k for Γ is a function $f : \mathcal{H} \longrightarrow \mathbb{C}$ such that

1. f is holomorphic on $\mathcal{H}$;

2.$f_{|[g_k]}(z) = f(z)$for all$z \in \mathcal{H}, g \in \Gamma$;

3. f is holomorphic at the "cusps" (see below for a discussion of this notion).

If N is an integer such that Γ contains the full congruence group $\Gamma(N)$, then f is said to have *level* N.

We note that with this definition, the level of a modular form is not uniquely determined. We also need to explain the holomorphy condition (3) at the "cusps" (i.e, the points in $\mathcal{H}^*$ that can be written in the form $\gamma.\infty$ for some $\gamma \in \mathbf{SL}_2(\mathbb{Z})$). To see this, we remark that Γ contains an element of the form $\begin{pmatrix} 1 & A \\ 0 & 1 \end{pmatrix} : z \mapsto z + A$, where A can be chosen to be the minimal positive integer satisfying this property. For an open neighbouhood $U = \{z \in \mathcal{H},\ \mathrm{Im}(z) > M\}$ (M some large enough positive integer) of ∞ in $\Gamma\backslash\mathcal{H}^*$, the map $q_A(z) := e^{2i\pi z/A} : U \longrightarrow \mathbb{C}$ is well-defined, and even a biholomorphism to a center-free disk $D\backslash\{0\}$. Now, any f verifiying condition 2 in the above definition satisfies $f(z + A) = f(z)$, so it induces a holomorphic function $\mathcal{F}$ on $D\backslash\{0\}$. By definition, holomorphy of f at ∞ means holomorphy of $\mathcal{F}$ at 0. The other cusps can be written $c = \gamma.\infty$ and it follows from the definitions that for $\gamma \in \mathbf{SL}_2(\mathbb{Z})$ and g in $\gamma^{-1}\Gamma\gamma$,

$$f|_{[\gamma]_k}\Big|_{[g]_k} = f|_{[\gamma]_k}\,.$$

So $f_{|[\gamma_k]|[g_k]}$ also induces a function on $D\backslash\{0\}$. We then say that f is holomorphic at the cusps if every $f_{|[\gamma_k][g_k]}$ above is holomorphic at ∞. Actually such an f admits an expansion:

$f(z) = \sum_{n=-\infty}^{\infty} a_n {q_A}^n$

such that holomorphy at ∞ means $a_n = 0$ for $n < 0$. One similarly says that f vanishes at ∞ if $a_n = 0$ for $n \leq 0$.

Definition. Cusp form. A cusp form is a modular form which vanishes at all the cusps of $\Gamma\backslash\mathcal{H}$ where Γ is a congruence subgroup.

Notations. One denotes by $\mathcal{M}_k(\Gamma)$ the $\mathbb{C}$-vector space of modular forms of weight k for Γ, and by $\mathcal{S}_k(\Gamma)$ its subspace of cusp-forms.

The space $\mathcal{M}_k(\Gamma)$ can be identified with the space of "weight-k" differentials on $\Gamma\backslash\mathcal{H}$.

2 The Dual Graph $\mathcal{G}$ of a Curve

2.1 The Case of Regular Curves

Let p be a prime. We consider a curve C over a p-adic field K, with uniformizer π and residue field k. We denote by P the Jacobian $\mathrm{Pic}^0(C)$ of C. We first suppose that we have a regular minimal model $\mathcal{C}$ of C over the integer ring O_K of K, i.e., $\mathcal{C}$ is a model of C over O_K which is regular and posesses all other technically "good" properties that we will not discuss here. We also assume that the multiplicities of all the irreducible components of $\mathcal{C}_k := \mathcal{C} \times_{O_k} k$ have 1 as their greatest common divisor. Let $P_k := P \times_{O_k} k$ be the special fiber of the Néron model of P. Let $P^0 = (P_k)^0$ denote the connected component of 0 in this special fiber. Let $\mathrm{Pic}^0(\mathcal{C}_k)$ be the set of classes of divisors on $\mathcal{C}_k$ having degree 0 on *each* of its connected components.

Lemma 2.1 *There is a canonical isomorphism:* $P^0 \approx \mathrm{Pic}^0(\mathcal{C}_k)$

Proof. The lemma is quite difficult to prove, and the interested reader is referred to to [SGA7 I](12.1.12).

■

We know that all singular points of the curve $\mathcal{C}_k$ are ordinary double points, i.e., they have local equation $xy = 0$. Then P^0 is a semiabelian scheme over k, i.e., an extension of an abelian variety A by a torus. To be precise, we write the normalization of $\mathcal{C}_k$ as the disjoint union of non-singular curves D_j. The normalization map $\amalg_j D_j \to \mathcal{C}_k$ induces an obvious morphism

$\mathrm{Pic}^0(\mathcal{C}_k) \to \prod_j \mathrm{Pic}^0(D_j) = A$

as the Picard functor is a contravariant functor and $\mathrm{Pic}^0(\amalg_j D_j) \approx \prod_j \mathrm{Pic}^0(D_j)$. It turns out that the kernel of the above morphism is a torus which we denote by T (cf.[EGA IV](21.8.5)). Now, to make things easier, we introduce the notion of a "dual" graph $\mathcal{G}$ associated to $\mathcal{C}_k$. $\mathcal{G}$ is defined as the graph with the following properties:

◇ The set J of irreducible components of $\mathcal{C}_k$ form the set of vertices of $\mathcal{G}$.

◇ The set I of singular points of $\mathcal{C}_k$ form the set of edges of $\mathcal{G}$.

◇ The edge corresponding to a singular point $i \in I$ connects the two vertices corresponding to the two components of $\mathcal{C}_k$ which meet at i.

◇ $\mathcal{G}$ is an unoriented graph.

Remark. We assumed that all singular points have local equation $xy = 0$. This means that each singular point involves exactly two connected components. In other words, our graph is well-defined, i.e. "every edge links exactly

two vertices" in $\mathcal{G}$. Also, the implicit "good" properties of $\mathcal{C}_k$ ensure that the graph $\mathcal{G}$ is connected.

Proposition 2.2 *There is a canonical isomorphism:*

$$X(T) \approx H_1(\mathcal{G}, \mathbb{Z})$$

where $X(T)$ is the character group of T.

Proof. For the proof, see [SGA 7 I](12.3.7).

■

We try to calculate $H_1(\mathcal{G}, \mathbb{Z})$ next. We first consider the bouquet $\overline{\mathcal{G}}$ of circles obtained by identifying all the vertices of $\mathcal{G}$. The quotient map $\mathcal{G} \to \overline{\mathcal{G}}$ induces an inclusion:

$$\imath : X := H_1(\mathcal{G}, \mathbb{Z}) \hookrightarrow H_1(\overline{\mathcal{G}}, \mathbb{Z}) \qquad (1)$$

(It is clear that an equivalence class of loops in $\mathcal{G}$ goes to equivalence class(es) of loops in $\overline{\mathcal{G}}$ when all the vertices of $\mathcal{G}$ are identified, showing that $\imath$ is well-defined. Further, no non-nullhomotopic loop in $\mathcal{G}$ becomes nullhomotopic in $\overline{\mathcal{G}}$, which explains the injectivity of $\imath$.)

For each $i \in I$, we give the corresponding edge of $\mathcal{G}$ an orientation, i.e., we specify one of its end-points as its initial point $j_1(i)$ and the other one as its final point $j_2(i)$. Equivalently, we give an ordering $(j_1(i), j_2(i))$ of the two irreducible components which pass through i. The resulting orientation of the edges of $\overline{\mathcal{G}}$ give rise to an isomorphism :

$$H_1(\overline{\mathcal{G}}, \mathbb{Z}) \approx \mathbb{Z}^I \qquad (2)$$

$$\gamma_1^{a_1} * \ldots\ldots\ldots * \gamma_1^{a_I} \longleftrightarrow (a_1, \ldots\ldots\ldots, a_I)$$

where γ_i is the image of $i \in I$ under $\imath$. It is clear that the γ_is form a minimal set of generators of $H_1(\overline{\mathcal{G}}, \mathbb{Z})$.

By composing the inclusion of (1) and the isomorphism of (2), one gets a non-canonical inclusion:

$$e : X \hookrightarrow \mathbb{Z}^I \qquad (3)$$

We would like to identify X with a subgroup of of $\mathbb{Z}^I$. For doing this, we define

$$D := \{\sum_{j=1}^{J} n_j V_j | \sum n_j = 0 \text{ and } n_j \in \mathbb{Z}\}$$

.

where $V_1, V_2, ..., V_J$ are the vertices of $\mathcal{G}$. We call $\sum n_j$ the *degree* of $\sum n_j V_j$. It can be easily verified that D is indeed a group and by identifying $\sum_{j=1}^{J} n_j V_j$ with $(n_1, ..., n_J) \in \mathbb{Z}^J$, we can view it as a subgroup of $\mathbb{Z}^J$.

Proposition 2.3 *The group X corresponds to the kernel of the homomorphism $\alpha : \mathbb{Z}^I \to D$ defined by $\alpha(e_i) = j_1(i) - j_2(i)$, where e_i is the $\mid I \mid$-tuple with 1 at the ith place and 0s everywhere else, with the identification between vectors in $\mathbb{Z}^I$ and loops in $H_1(\overline{\mathcal{G}}, \mathbb{Z})$ as in (2).*

Proof. That α is well-defined is clear:

$$\alpha(\sum_{i=1}^{I} a_i e_i) = \sum a_i (j_1(i) - j_2(i))$$

.

Also, it is trivial to check that α is indeed a homomorphism, i.e.,
$\alpha(v_1 + v_2) = \alpha(v_1) + \alpha(v_2)$ for all vectors v_1 and v_2 in $\mathbb{Z}^I$ and $\alpha(0) = 0$.

Further, the image of α does indeed land inside D too because the degree of any element $\sum_{i=1}^{I} a_i e_i$ in the image is equal to $\deg(\alpha(\sum_{i=1}^{I} a_i e_i)) = \sum_{i=1}^{I} a_i \deg(\alpha(e_i)) = \sum_{i=1}^{I} a_i \ (\deg(j_1(i)) - \deg(j_2(i))) = \sum_{i=1}^{I} a_i (1 - 1) = 0$.

Now for the main part of the proof.

First let $\Gamma \in X = H_1(\mathcal{G}, \mathbb{Z})$, i.e., Γ is a loop in $\mathcal{G}$.
Suppose that Γ is formed by taking the edges $n_1, n_2, ..., n_m$ in order. In other words, $j_2(n_l) = j_1(n_{l+1})$ for $l = 1, ..., (m-1)$ and $j_2(n_m) = j_1(n_1)$. Then,
$\alpha(\Gamma)$
$= \sum_{i=1}^{m} (j_1(n_i) - j_2(n_i))$
$= j_1(n_1) + (-j_1(n_1) + j_1(n_2)) + ... + (-j_1(n_{m-1}) + j_1(n_m)) - j_2(n_m)$
$= j_1(n_1) + 0 + 0 + ... + 0 - j_2(n_m) = 0.$
This proves that $X \subset \text{Kernel}(\alpha)$.

Now, for the other inclusion, let $\Gamma \in \mathbb{Z}^I \backslash H_1(\mathcal{G}, \mathbb{Z})$, i.e., Γ is not a loop in $\mathcal{G}$. It is quite clear that we can decompose Γ as a union of a set L of loops and a set N of non-loops in such a way that in N, all elements are connected non-loops and no non-loop is a subset of a loop and the various non-loops are disjoint from one-another. As α is a homomorphism and image of every loop under α is 0 by the first part of the proof, it follows that $\alpha(L) = 0$.

Thus, $\alpha(s) = \alpha(L \cup N) = \alpha(L) + \alpha(N) = \alpha(N)$. As Γ is a non-loop by assumption, N is non-empty. In particular, N has a free-end, i.e., a vertex which is an end-point of just one edge, say s occuring with multiplicity $n_s \neq 0$ in N. Then in the expression $\alpha(N) = \sum_{j=1}^{J} b_j E_j$, where E_j is the j-th $\mid J \mid$-tuple (has 1 at the jth place and 0s everywhere else) the coefficient of e_s is $\pm n_s \neq 0$, implying that $\alpha(N) \neq 0$, i.e., $\Gamma \in \mathbb{Z}\backslash\text{Kernel}(\alpha)$. This proves the other inclusion $\text{Kernel}(\alpha) \subset X$.

This completes the proof.

■

2.2 The Case of Admissible Curves.

Next, we relax the condition that $\mathcal{C}$ is regular. Instead, we assume that $\mathcal{C}$ is an admissible curve in the sense of Jordan-Livné [Jor-Liv]. This assumption implies that the special fiber of $\mathcal{C}$ has only ordinary double points as singularities, as in the regular case, but the local equation of the singularities are now $xy = \pi^{\epsilon}$. More precisely, still using our previous definition of I and J in this discussion, there is a collection of positive integers ε_i associated to each $i \in I$, called the "width" of the corresponding singularity. It turns out that the special fiber of a regular minimal model for $\mathcal{C}$ may be obtained from $\mathcal{C}_k$ by replacing each singular point $i \in I$ with $\varepsilon_i > 1$ by a chain of $n_i := (\varepsilon_i - 1)$ copies of the projective line $\mathbb{P}^1$. We will call the model thus obtained the "derived" regular model corresponding to $\mathcal{C}$.

Proposition 2.4 *Let C be a curve such that its minimal model $\mathcal{C}$ is an "admissible curve" in the sense of Jordan-Livné. Let $\mathcal{G}$ and $\mathcal{G}_{\text{new}}$ be the dual graphs of $\mathcal{C}$ and the "derived" regular model corresponding to $\mathcal{C}$ respectively. Then,*
$H_1(\mathcal{G}, \mathbb{Z}) = H_1(\mathcal{G}_{new}, \mathbb{Z})$.
Thus, we can continue using the recipe that we used in the last section under the weaker assumption that $\mathcal{C}$ is an "admissible curve", but not necessarily regular.

Proof. The above construction results in a "blow-up" of $\mathcal{C}_k$ where the sets I and J are replaced by their analogues $\tilde{I}$ and $\tilde{J}$. There is an obvious surjective map:

$$\tilde{I} \longrightarrow I \qquad (4)$$

defined by

$$e(i,k) \mapsto e_i$$

for $i = 1, 2, ..., I$ and $k = 1, ..., n_i$
where the "e(i,k)"s, $k = 1, ..., n_i$ are the singularities arising from the desingularizations of the singular point i.

Note. *By abuse of notation, we will often be writing e_i for i and (i,k) for $e(i,k)$ and vice-versa. Also, we will sometimes use the notations $I, J, \tilde{I}$ and $\tilde{J}$ both for these sets and their respective cardinalities. Optimally, no confusion should arise.*

We can get a map Φ associated to the map of (4) also:

$$\Phi : \mathbb{Z}^I \longrightarrow \mathbb{Z}^{\tilde{I}}$$

being defined by

$$e_i \mapsto \sum_{k=1}^{n_i} e(i,k)$$

$i = 1, ..., I$;
where $e(i_0, k_0)$ is the $|\tilde{I}|$-tuple with 1 at the $(\#\{(i,k) \text{ with } i < i_0\} + k_0)$ th place and 0s everywhere else.
As all the $e(i,k)$ s are "linearly independent", so any non-trivial element $\sum_{i=1}^{I} m_i e_i$ of $\mathbb{Z}^I$ goes to the non-trivial element $\sum_{i=1}^{I} \sum_{k=1}^{n_i} m_i e(i,k)$ of $\mathbb{Z}^{\tilde{I}}$. This means that the map Φ is injective.
Now, let us look at $K := \text{Coker}(\Phi) = \mathbb{Z}^{\tilde{I}}/\text{Image}(\Phi)$. Now, K is clearly torsion-free because for any vector $v \in \mathbb{Z}^{\tilde{I}}$, $v \in \text{Image}(\Phi) \Leftrightarrow nv \in \text{Image}(\Phi)$ for all $n \in \mathbb{Z}\backslash\{0\}$. On the other hand, $J \subset \tilde{J} = J \cup \{$ all the adjoined $\mathbb{P}^1$s$\}$. So we have a natural injection:

$$\mathbb{Z}^J \longrightarrow \mathbb{Z}^{\tilde{J}} \qquad (5)$$

$$\sum_{j=1}^{J} m_j V_j \mapsto \sum_{j=1}^{J} m_j \tilde{V}_j,$$

where $\tilde{V_j}$ is the irreducible component of $\mathcal{C}_k$ containing V_j. (This map makes sense as $J < \tilde{J}$)
As before, in analogy with D, we define $\tilde{D}$ to be

$$\tilde{D} := \{\sum_{j=1}^{\tilde{J}} m_j \tilde{V_j} | \sum_{j=1}^{\tilde{J}} m_j = 0\}.$$

Thus, restricting the map in (5) to the subgroup D of $\mathbb{Z}^J$, one gets an injective map:

$$D \longrightarrow \tilde{D}$$

$$\sum_{j=1}^{J} m_j V_j \mapsto \sum_{j=1}^{J} m_j \tilde{V_j}$$

Next, we define a map $\tilde{\alpha}$ analogous to the map α defined before. That is, the map

$$\tilde{\alpha} : \mathbb{Z}^{\tilde{I}} \longrightarrow \tilde{D}$$

is defined by:

$$e(i,k) \mapsto j_1((i,k)) - j_2((i,k))$$

where the $j_1((i,k))$ and $j_2((i,k))$ are the initial and final points of the edge corresponding to $e(i,k)$.
We can prove as before that $X = \text{Kernel}(\tilde{\alpha})$, i.e., there is an exact sequence:

$$0 \longrightarrow X \xrightarrow{\tilde{\varepsilon}} \mathbb{Z}^{\tilde{I}} \xrightarrow{\tilde{\alpha}} \tilde{D} \longrightarrow 0.$$

In the above sequence, $\tilde{\varepsilon}$ is just the inclusion map. Let Y be the kernel of the surjective map $\alpha : \mathbb{Z}^I \longrightarrow D$ and $\varepsilon : Y \longrightarrow \mathbb{Z}^I$ be the inclusion map. Then we have an exact sequence:

$$0 \longrightarrow Y \xrightarrow{\varepsilon} \mathbb{Z}^I \xrightarrow{\alpha} D \longrightarrow 0.$$

Remark. α is surjective because every element $\sum_{j=1}^{J} a_j V_j \in D$ (implying that $\sum_{j=1}^{J} a_j = 0$) can be written in the form: $\sum_{i=1}^{I} b_i(j_1(i) - j_2(i)) = \alpha(\sum_{i=1}^{I} b_i e_i)$. To see this, first notice that $\sum_{j=1}^{J} a_j V_j = \sum_{j=1}^{J-1} \tilde{a}_j (V_j - V_{j+1})$ for some integers $\tilde{a}_j$ because $\sum_{j=1}^{J-1} a_j = 0$. Thus, as α is a homomorphism,to show that $\tilde{\alpha}$ is surjective, it suffices to show that given any two elements V_j and V_k belonging to J, it is possible to find an element $z \in \mathbb{Z}^{\tilde{I}}$ such that

$\alpha(z) = V_j - V_k$. Now, by the previous remark, we know that the graph $\mathcal{G}$ is connected. So, it must must be possible to find a path from the vertex V_j to the vertex V_k, composed by taking the edges $m_1, ..., m_l$ in order, say. This implies that $j_2(m_n) = j_{1(}m_{n+1})$ for $n = 1, 2, ..., (l-1)$ and $j_1(m_1) = V_j$ and $j_2(m_l) = V_k$. Then, $\alpha(\sum_{r=1}^{l} e_{m_r}) = \sum_{r=1}^{l}(j_1(m_r) - j_2(m_r)) = V_j - V_k$. Thus, α is surjective. Similarly, one can prove that $\tilde{\alpha}$ is surjective.

Now we have a commutative diagram:

$$\begin{array}{ccc} \mathbb{Z}^I & \xrightarrow{\alpha} & \mathrm{D} \\ \downarrow{\scriptstyle \tau} & & \downarrow{\scriptstyle \iota} \\ \mathbb{Z}^{\tilde{I}} & \xrightarrow{\tilde{\alpha}} & \tilde{\mathrm{D}} \end{array}$$

(The diagram is commutative because α is a homomorphism and for the basis vectors e_i, we have
$\iota(\alpha(e_i)) = \iota(j_1(e_i) - j_2(e_i)) = \sum_{k=1}^{n_i} j_1((i,k)) - \sum_{k=1}^{n_i} j_2((i,k))$
and
$\tilde{\alpha}(\tau(e_i)) = \sum_{k=1}^{n_i} e(i,k) = \sum_{k=1}^{n_i}(j_1((i,k)) - j_2((i,k))$ making $\iota(\alpha(e_i)) = \tilde{\alpha}(\tau(e_i))$.)

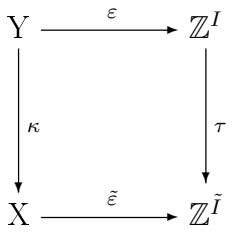
Recall that $Y := \text{Kernel}(\alpha)$ and $X := \text{Kernel}(\tilde{\alpha})$. Now, let $z \in Y$, i.e.,
$\alpha(z) = 0 \Rightarrow \iota(\alpha(z)) = \iota(0) = 0$ (since ι is a homomorphism)
$\Rightarrow \tilde{\alpha}\tau(z) = 0$ (since the above diagram is commutative)
$\Rightarrow \tau(z) \in \text{Kernel}(\tilde{\alpha}) = X$
Thus, we have an induced map:

$$\kappa : Y \longrightarrow X$$

defined by

$$z \mapsto \tau(z),$$

i.e., κ is the restriction of τ to Y. Since the maps $\varepsilon : Y \longrightarrow \mathbb{Z}^I$ and $\tilde{\varepsilon} : X \longrightarrow \mathbb{Z}^{\tilde{I}}$ are inclusion maps, the following diagram commutes by the definition of κ.



Since τ and ε are injective(clearly!), so is $\tau \circ \varepsilon$. Then as the above diagram is commutative, so is $\tilde{\varepsilon} \circ \kappa (= \tau \circ \varepsilon)$, implying that κ is injective too. Now, let us look at the cokernel of κ. As we are dealing with abelian groups only, so $\text{Coker}(\kappa) = X/\text{Image}(\kappa)$ is also an abelian group. Now,
$\text{rank}(\text{Coker}(\kappa)) = \text{rank}(X) - \text{rank}(\text{Image}(\kappa)).$ $= \text{rank}(X) - \text{rank}(Y)$ (since κ is injective)
$= |\tilde{I}| - \text{rank}(\tilde{D}) - |I| + \text{rank}(D)$ (because of the above exact sequences)
$= |\tilde{I}| - (|\tilde{J}| - 1) - |I| + (|J| - 1)$ (see the definitions of D and $\tilde{D}$)
$= (|\tilde{I}| - |I|) - (|\tilde{J}| - |J|) = 0.$ (as the number of new singular points=the number of new irreducible components).

This means that $\text{Coker}(\kappa)$ is a torsion abelian group. On the other hand, we have seen that $\text{Coker}(\tau)$ is torsion-free (abelian group). Now, the *Snake Lemma* implies that $\text{Coker}(\kappa)$ injects into $\text{Coker}(\tau)$. Thus, $\text{Coker}(\kappa)$ is both torsion-free and a torsion abelian group, which is possible if and only if $\text{Coker}(\kappa) = 0$.

$\Leftrightarrow X/\text{Image}(\kappa) = 0$

$\Leftrightarrow X = \text{Image}(\kappa)$

$\Leftrightarrow \kappa$ is a surjection.

We had seen before that κ is an injective homomorphism too. Combining this with the result about surjectivity of κ found above, we conclude that κ is an isomorphism. That is, $X \approx Y$, which means that $H_1(\mathcal{G}, \mathbb{Z}) = H_1(\mathcal{G}_{new}, \mathbb{Z})$, where $\mathcal{G}_{new}$ is the new graph of the curve.
This means that we can continue to work using our old recipe without worrying about the regularity of $\mathcal{C}$.

■

3 A Quaternion Viewpoint of Modular Curves

As the name of the chapter suggests, we are going to understand modular curves from the point of view of quaternions in this chapter. In order to do this, we need a few basic concepts which we introduce below.

3.1 Some Basic Concepts.

Recall that the modular curve $X_0(N)_{\mathbb{C}}$ was defined as

$X_0(N)_{\mathbb{C}} := \Gamma_0(N)\backslash\mathcal{H}^*$

where $\mathcal{H}^* := \{$ Upper-half plane $\} \cup \mathbb{Q} \cup \{\infty\}$

and $\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} (\text{mod } N) \right\}$

We now state the following theorem without proof:

Theorem 3.1 *The curve $X_0(N)_{\mathbb{C}}$ has a proper modular model $X_0(N)_{\mathbb{Z}}$ over $\mathbb{Z}$, which is smooth over $\mathbb{Z}[\frac{1}{N}]$.*

In particular, it makes sense to define a curve $X_0(N)_{\mathbb{Q}_q} = X_0(N)_{\mathbb{Z}} \times_{\mathbb{Z}} \mathbb{Q}_q$ over $\mathbb{Q}_q$.

Definition. Quaternion Algebra. A quaternion algebra B over a field K is a *central simple algebra* with center K, which is 4-dimensional as a vector space over K. (Recall that a central simple algebra is a simple algebra which has finite dimension over its center).

Examples:

For any field K, the ring of matrices $\mathbf{M}_2(K)$ with entries in K is a quaternion algebra over K. If K is algebraically closed, then all quaternion algebras over K are isomorphic to $\mathbf{M}_2(K)$.

For $K = \mathbb{R}$, the well known algebra $\mathbb{H}$ of Hamiltonian quaternions is a quaternion algebra over $\mathbb{R}$. The two algebras $\mathbb{H}$ and $\mathbf{M}_2(K)$ are the only quaternion algebras over $\mathbb{R}$, up to isomorphism.

When K is a number field, there are infinitely many non-isomorphic quaternion algebras over K. In fact, there is one such quaternion algebra for every even sized finite collection of finite primes or real primes of K.

One can show that every quaternion algebra over K other than $\mathbf{M}_2(K)$ is always a division ring.

The Quaternion algebra "$\mathbf{B_D}$":

Let $D = p_1 p_2 ... p_{2m}$ be the product of an even number of primes in $\mathbb{Z}$ (including ∞), the various 'p_i's being distinct. By the theory of quaternion algebras over $\mathbb{Q}$, there is a quaternion algebra B_D over $\mathbb{Q}$, which up to isomorphism is characterized by:

$$\begin{cases} B_D \otimes_{\mathbb{Q}} \mathbb{Q}_l \approx & \mathbf{M}_2(\mathbb{Q}_l) & \text{if } l \nmid D; \\ B_D \otimes_{\mathbb{Q}} \mathbb{Q}_l \approx & H_l & \text{if } l \mid D. \end{cases}$$

where H_l is the *unique* quaternion algebra over $\mathbb{Q}_l$.

The 'p_i's are called the *ramification primes*, and D is called the *discriminant* of B_D.

If the p_is are finite, then $B_D \otimes \mathbb{R} \approx \mathbf{M}_2(\mathbb{R})$. So, picking a maximal order O_D in B_D, one gets an injection:

$$O_D{}^* \hookrightarrow (O_D \otimes_{\mathbb{Z}} \mathbb{Q})^* = B_D{}^* \hookrightarrow (B_D \otimes_{\mathbb{Q}} \mathbb{R})^* \approx \mathbf{GL}_2(\mathbb{R}).$$

We also write $O_D{}^+$ for the inverse image in $O_D{}^*$ of the composed map $O_D{}^* \hookrightarrow GL_2^+(\mathbb{R})$, where $GL_2^+(\mathbb{R})$ is the set of matrices in $\mathbf{GL}_2(\mathbb{R})$ with positive determinant. Thus we get an inclusion $O_D{}^+ \hookrightarrow GL_2^+(\mathbb{R})$.

Review of Elliptic Curves.

Let E be an elliptic curve over a field k of characteristic q. Let $E[q]$ denote the group of q-torsion points of E. Only one of the following two cases can occur:

1)**The Ordinary Case**.

$$E[q](\overline{k}) \approx \mathbb{Z}/q\mathbb{Z}$$

2)**The Supersingular Case**.

$$E[q](\overline{k}) = \{0\}$$

There are only a finite number of isomorphism classes of supersingular elliptic curves over k and an infinite number of isomorphism classes ordinary elliptic curves over k.

In general, there are only two q-isogenies on E/k:

1)Case (a). $\mathrm{Frob}_q : E \longrightarrow E^{(q)}$ (**Frobenius**).

2)Case (b). $\mathrm{Ver}_q : E \longrightarrow E^{(q^{-1})}$ (**Verschiebung**, the dual of Frobenius)

The isogeny Frob_q is purely radicial *radicial*, i.e., its kernel has no non-trivial physical point. If E is ordinary, Ver_q is *étale*, and

$\mathrm{Kernel}(\mathrm{Ver}_q)(\overline{k}) = E[q](\overline{k}) = \mathbb{Z}/q\mathbb{Z}$

If E is supersingular, $\mathrm{Ver}_q = \mathrm{Frob}_q$.

Upshot. To give $(E, C_{Mq}) = (E, C_M, C_q) \in X_0(Mq)(\overline{k})$ is equivalent to giving $(E, C_M) \in X_0(M)$ and

$$\begin{cases} C_q = & \mathrm{Ker}(\mathrm{Frob}_q) & \text{(Case (a))}; \\ C_q = & \mathrm{Ker}(\mathrm{Ver}_q) & \text{(Case(b))}. \end{cases}$$

If E is supersingular, Case(a)=Case(b).

Definition. Eichler Order. Let B_D be the unique (up to isomorphism) quaternion algebra over $\mathbb{Q}$ with discriminant D. We take a maximal order S in B_D, i.e., S is a maximal free rank-4 subalgebra of B_D. Then, $S \otimes \mathbb{Q} \approx B_D$. An *Eichler Order of level* M is a subalgebra $R \subset S$ such that after fixing an isomorphism $\Phi : S \otimes \mathbb{Z}_l \longrightarrow \mathbf{M}_2(\mathbb{Z}_l)$ for primes l not dividing D, we get an isomorphism: $\Phi|_{R \otimes \mathbb{Z}_l} : R \otimes \mathbb{Z}_l \longrightarrow \left\{ \mathcal{M} \in \mathbf{M}_2(\mathbb{Z}_l) : \mathcal{M} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} (\text{mod } l^n) \right\}$ where l^n is the largest power of l dividing M and $B_D \otimes \mathbb{Z}_l \simeq S \otimes \mathbb{Z}_l$ is the maximal order of $B_D \otimes \mathbb{Z}_l$ if $l \mid D$.

It turns out that every Eichler order can be expressed as the intersection of two maximal orders, though not necessarily in a unique way.

Theorem 3.2 ***The Skolem-Noether Theorem.*** *Let A and B be simple rings, and $K = Z(B)$ be the centre of B. Suppose that the dimension of B over the field K is finite, that is, B is a central simple algebra (K is a field since any $x \in K$, by centrality, generates a two-sided ideal $I \neq 0$ so simplicity of B implies that $I = B$ and hence x is invertible).*

Then if $f, g : A \longrightarrow B$ are K-algebra homomorphisms, there exists a unit b in B such that $g(a) = bf(a)b^{-1}$ for all a in A.

Definition. Adelization of a Ring. Given a ring R, its adelization R_f is defined to be:

$$R_f = R \otimes \widehat{\mathbb{Z}}$$

where $\hat{\mathbb{Z}} = \prod_{l \text{ prime}} \mathbb{Z}_l$ is the profinite completion of $\mathbb{Z}$.

Definition. $\boldsymbol{T_l(A)}$. Let A be an abelian variety of dimension g over a field K and l a prime number. Let $A[l^n]$ be the kernel of multiplication by l^n on A for all integers $n \geq 1$. Then we define $T_l(A)$ as the inverse limit of the abelian groups $A[l^n]$. Assuming we have a fixed separable closure of K, the absolute Galois group G of K acts on $T_l(A)$, which is a profinite group. In fact it is more, being also a module over the ring of l-adic integers $\mathbb{Z}_l$.

Classical results on abelian varieties show that if K has characteristic zero, or characteristic p where the prime number $p \nmid l$, then $T_l(A)$ is a free module over $\mathbb{Z}_l$ of rank $2d$, where d is the dimension of A. In the other case, it is still free, but the rank may take any value from 0 to d.

Definition. The q-adelic Tate module. Given an enhanced elliptic curve $\mathbf{E} = (E, B)$ (i.e., B is a subgroup of the elliptic curve E) over $\overline{\mathbb{F}_q}$, we define:

$$T(\mathbf{E}) := T_q(E) \times \prod_{l \neq q \text{ is prime}} T_l(E)$$

Definition. The Bruhat-Tits Tree. Given any prime p, there is a notion of a tree $\mathcal{T}$ of $\mathbf{PGL}(\mathbb{Q}_p)$ associated to the set $\mathcal{L}$ of homothety classes of lattices in ${\mathbb{Q}_p}^2$. The vertices of $\mathcal{T}$ are simply the elements of $\mathcal{L}$. Given two elements $\overline{L_1}, \overline{L_2} \in \mathcal{L}$, we may assume that $L_1 \supset L_2$ after lifting L_1 and L_2 as real lattices and multiplying L_2 by a suitable $\alpha = p^k$, with $k \in \mathbb{Z}$ and with k being of minimal absolute value. Now $\sharp(L_1/L_2) = p^n$ for some $n \in \mathbb{N}$. We call n the *distance* between L_1 and L_2. $\overline{L_1}$ and $\overline{L_2}$ are said to be connected by an edge $\overline{L_1 L_2}$ if $d(\overline{L_1}, \overline{L_2}) = 1$.

As any lattice L_0 in ${\mathbb{Q}_p}^2$ is isomorphic to ${\mathbb{Z}_p}^2$, there are exactly $\sharp\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z}) = (p+1)$ sublattices of index p. So, there are exactly $(p+1)$ vertices which are at a distance of 1 from it. Equivalently, every vertex of T is connected to exactly $(p+1)$ other vertices by means of edges.

Definition. Dual and Inverse of an Isogeny. Let E and E_0 be elliptic curves. If $\lambda : E \longrightarrow E_0$ is an isogeny, then there is an isogeny $\mu : E_0 \longrightarrow E$ such that $\mu \circ \lambda : E \longrightarrow E$ is just the multiplication map by a minimum positive integer $deg(\lambda)$ called the degree of λ. We call μ the dual isogeny of λ.

We define the inverse λ as $\lambda^{-1} := \frac{1}{deg(\lambda)} \times \mu \in \mathrm{Hom}(E_0, E) \otimes \mathbb{Q}$.

So, if $\sigma \in \mathrm{End}(E_0)$, then $\lambda^{-1}\sigma\lambda \in \mathrm{End}(E) \otimes \mathbb{Q}$.

3.2 Our Setting

Given.

Let p and q be distinct prime numbers, and M be a positive integer prime to pq. We will consider the mod q reduction of the curve $X_0(qM)$ in the sections 3.2-3.5. In 3.6., we will deduce that some analogous facts hold for $X_0(pqM)$ too, by analogy. Let C be the modular curve $X_0(qM)$ over $\mathbb{Q}_q$ and let $\mathcal{C}$ be the regular minimal model of C over $\mathbb{Z}_q$. Using the machinery and terminology developed above, we will study the dual graph $\mathcal{G}$ in terms of $\mathcal{C}_{\mathbb{F}_q}$ in terms of quaternions.

The Dual Graph of $\mathcal{C}_{\mathbb{F}_q}$

We know that the curve $\mathcal{C}_{\mathbb{F}_q}$ is just the set of qM-isogenies, i.e., pairs (E, C_{Mq}) of elliptic curves enhanced by a subgroup C_{Mq} of order Mq [Deligne-Rapoport]. By the "upshot" in the review of elliptic curves given above, we know that $\mathcal{C}_{\mathbb{F}_q}$ is composed of just two copies of the curve $X_0(M)_{\mathbb{F}_q}$ attached at the supersingular points (i.e.,those supersingular points which arise from supersingular elliptic curves over $\overline{\mathbb{F}_q}$), a supersingular point on the first copy being identified with its Frobenius transform on the second.

We continue using the same notation as in Chapter 2. Then J, the set of irreducible components of $\mathcal{C}_{\mathbb{F}_q}$ has two elements. I, the set of singular points of $\mathcal{C}_{\mathbb{F}_q}$ is clearly the set $\Sigma(M)$ of $\mathbb{F}_q$-isomorphism classes of "enhanced elliptic curves" $\mathbf{E} = (E, B)$, where E is a supersingular elliptic curve over $\overline{\mathbb{F}_q}$ and B is a cyclic subgroup of E of order M.

For each $i \in I$, the elements $j_1(i)$ and $j_2(i)$ are the (only) two distinct elements of J. For our convenience, we will orient the $i \in I$ in such a way that $j_1(i)$ and $j_2(i)$ are independent of i. The graph of $\mathcal{G}$ in this case has precisely two vertices and all the edges connect the two distinct vertices and are oriented in the same direction.

3.3 Relating the Character Group corresponding to $X_0(qM)$ with $\mathbf{Div}^0(\Sigma(M))$

Using the above convention, we get that:

Proposition 3.3 *The character group X in the case $C = X_0(Mq)$ is the group of degree 0-divisors on the set $\Sigma(M)$ of supersingular points of $X_0(M)_{\overline{\mathbb{F}_q}}$.*

Proof. From Proposition 2.3 of the previous chapter, we know that $X = \mathrm{Ker}(\alpha)$, where

$\alpha : \mathbb{Z}^I \longrightarrow D$ is defined by $\alpha(i) = j_1(i) - j_2(i)$.

Let $\mathbf{v} = \sum_{i=1}^{|I|} n_i e(i) \in Ker(\alpha) \subset \mathbb{Z}^I$.

$\Leftrightarrow \alpha(\sum_{i=1}^{|I|} n_i e(i)) = 0$

$\Leftrightarrow \sum_{i=1}^{|I|} n_i (j_1(i) - j_2(i)) = 0$

$\Leftrightarrow (\sum_{i=1}^{|I|} n_i)(j_1(i) - j_2(i)) = 0$ (since $j_1(i)$ and $j_2(i)$ are independent of i)

$\Leftrightarrow \sum_{i=1}^{|I|} n_i = 0$ (since $j_1(i) \neq j_2(i)$ as the two concerned copies of $X_0(M)_{\mathbb{F}_q}$ are distinct.)

$\Leftrightarrow \sum_{i=1}^{|I|} n_i e(i)$ is a degree-0 divisor on $\mathbb{Z}^I$.

$\Leftrightarrow \sum_{i=1}^{|I|} n_i e(i)$ is a degree-0 divisor on $\mathbb{Z}^{\Sigma(M)}$, where $\Sigma(M)$ is the set of supersingular points of $X_0(M)_{\overline{\mathbb{F}_q}}$. (since from the previous paragraph, $I = \Sigma(M)$ in this case)

■

3.4 Linking Eichler Orders with Enhanced Elliptic Curves

We continue using the same notations as in the previous two sections.

Now for each supersingular E, it is known that the $\mathbb{Q}$-algebra $H := (\mathrm{End}(E)) \otimes \mathbb{Q}$ is the unique (upto isomorphism) quaternion algebra over $\mathbb{Q}$ which is ramified precisely at q and at ∞. Since E is supersingular, the ring $\mathrm{End}(E)$ is a maximal order in H, while its subring $\mathrm{End}(\mathbf{E})$ is an Eichler order of level M in $\mathrm{End}(E)$.(accept these statements as facts)

Consider the canonical quotient map $\lambda : E \longrightarrow E/B$. There is a natural inclusion:

$$\mathrm{End}(E/B) \hookrightarrow H \text{ given by:}$$

$$\sigma \mapsto \lambda^{-1}\sigma\lambda.$$

Now,

$$\mathrm{End}(\mathbf{E}) = \{\sigma \in \mathrm{End}(E) | \sigma(B) = B\} = \mathrm{End}(E) \cap \mathrm{End}(E/B).$$

So, $\mathrm{End}(\mathbf{E})$ is an (oriented) Eichler order.

Next, we describe the set $I = \Sigma(M)$ in terms of the arithmetic of the quaternion algebra H. Since all supersingular elliptic curves over $\overline{\mathbb{F}_q}$ are isogenous, we can start with a fixed $\mathbf{E}_0$ and keep track of the isomorphism classes of enhanced elliptic curves gotten by isogenies from $\mathbf{E}_0$.

We consider $T(\mathbf{E})$ as "enhanced" by the distinguished cyclic subgroup B of $T(\mathbf{E})/MT(\mathbf{E})$. We fix $\mathbf{E}_0 = (E_0, B_0)$, and define

$$R = \mathrm{End}(\mathbf{E}_0), \quad H = R \otimes_{\mathbb{Z}} \mathbb{Q}.$$

Let R_f and H_f be the adelizations of these rings. Given any enhanced supersingular curve $\mathbf{E} = (E, B)$, we select a non-zero $\lambda \in \mathrm{Hom}(E, E_0) \otimes_{\mathbb{Z}} \mathbb{Q}$. This homomorphism identifies $T(\mathbf{E})$ with a sublattice of $V(\mathbf{E}_0) := T(\mathbf{E}_0) \otimes_{\mathbb{Z}} \mathbb{Q}$. This is because every element $\lambda \in \mathrm{Hom}(E, E_0) \otimes_{\mathbb{Z}} \mathbb{Q}$ can be written as $\tilde{\lambda} \otimes \frac{r}{s}$ where $\tilde{\lambda} \in \mathrm{Hom}(E, E_0)$ and $\frac{r}{s} \in \mathbb{Q}$. We define $\lambda(T(\mathbf{E})) := T(\tilde{\lambda}(\mathbf{E})) \otimes \frac{r}{s}$. By the definition of $\tilde{\lambda}$, we know that $\tilde{\lambda}(\mathbf{E})$ does indeed land inside $\mathbf{E}_0$ and it is also clear that $\tilde{\lambda}(\mathbf{E})$ is an elliptic curve, so $T(\tilde{\lambda}(\mathbf{E}))$ makes sense. Thus the definition of $\lambda(T(\mathbf{E}))$ makes sense and so it identifies $T(\mathbf{E})$ with the sublattice $T(\tilde{\lambda}(\mathbf{E})) \otimes \frac{r}{s}$ of $V(\mathbf{E}_0) := T(\mathbf{E}_0) \otimes_{\mathbb{Z}} \mathbb{Q}$. Now, we can find a unique element (see below for knowing the reason)

$g \in {H_f}^*/{R_f}^*$

such that one has the equality of enhanced lattices $g.T(\mathbf{E}) = T(\mathbf{E}_0)$(after identifying $T(\mathbf{E})$ with $\lambda(T(\mathbf{E})$, of course!). This means that $g.T(\mathbf{E})$ and $T(\mathbf{E}_0)$ coincide as lattices of $V(\mathbf{E}_0)$ and the induced isomorphism

$g : T(\mathbf{E})/MT(\mathbf{E}) \approx T(\mathbf{E}_0)/MT(\mathbf{E}_0)$

carries B to B_0.

(From the definition of the adelic Tate module and the fact that both $T(\mathbf{E})$ and $T(\mathbf{E}_0)$ are sublattices of $T(\mathbf{E}) \otimes_{\mathbb{Z}} \mathbb{Q}$, it is clear that there should be an element $g \in {H_f}^*$ such that as sets,

$$g.T(\mathbf{E}) = T(\mathbf{E}_0) \qquad (6)$$

If there are two 'g's, say g_1 and g_2 satisfying (6), then we should have:
${g_1}^{-1}.T(\mathbf{E}_0) = {g_2}^{-1}T(\mathbf{E}_0)$.

$\Leftrightarrow {g_2}^{-1}g_1 \in {R_f}^* = (\mathrm{End}(\mathbf{E}_0) \otimes \hat{\mathbb{Z}})^*$.

$\Leftrightarrow$ There exists a unique $g \in {H_f}^*/{R_f}^*$ such that (6) holds.

The assertion about the induced isomorphism carrying B to B_0 is obvious.)

Now, two distinct 'λ's in $\mathrm{Hom}(E, E_0) \otimes_{\mathbb{Z}} \mathbb{Q}$ can give rise to the same sublattice in $V(\mathbf{E}_0) := T(\mathbf{E}_0) \otimes_{\mathbb{Z}} \mathbb{Q}$(corresponding to a unique $g \in {H_f}^*/{R_f}^*$) if and only if they differ by an element of $(\mathrm{End}(T(\mathbf{E}_0) \otimes_{\mathbb{Z}} \mathbb{Q}))^* = H^*$. So, because of the ambiguilty in the choice of λ, g is well-defined only in

$H^* \backslash {H_f}^*/{R_f}^*$. Hence, we have the following theorem:

Proposition 3.4 *This construction provides a bijection $\Phi_{\mathbf{E}_0}$ from the set $\Sigma(M)$ of supersingular points of $X_0(M)_{\overline{\mathbb{F}_q}}$ to the coset space $H^* \backslash {H_f}^*/{R_f}^*$.*

Proof. It was seen above that a given element $\mathbf{E} \in \Sigma(M)$ corresponds to a unique Tate-adelic module $T(\mathbf{E})$ (follows from the definition of $T(\mathbf{E})$), which

in turn, corresponds to a unique sublattice of $V(\mathbf{E}_0)$. Now this sublattice is uniquely determined by a unique $g \in H^* \backslash {H_f}^* / {R_f}^*$. This completes the proof.

■

Variant. *The set $\Sigma(M)$ is naturally isomorphic to the set of right ideal classes of the Eichler order R of level M in H.*

Proof. It is possible to identify the indicated set of ideal classes with the coset space above. For a proof, see [Vig,p.87]. So, the above assertion then becomes just a reassertion of the statement of Proposition 3.4 above, which we proved just now.

Proposition 3.5 *Let B and $B^{'}$ be maximal orders of a quaternion algebra of discriminant q (i.e., it is ramified at q and ∞) such that $S = B \cap B^{'}$ is an Eichler order of level M in B. Then there is an enhanced elliptic curve $\mathbf{E}$ over $\overline{\mathbb{F}_q}$ and an isomorphism*

$$\kappa : (S, B) \approx (\mathrm{End}(\mathbf{E}), \mathrm{End}(E)),$$

i.e., an isomorphism $B \approx \mathrm{End}(E)$ which carries S to $\mathrm{End}(\mathbf{E})$. Moreover, let $\mathbf{E}^{'}$ be another such enhanced elliptic curve and let $\kappa^{'} : (S, B) \approx (\mathrm{End}(\mathbf{E}^{'}), \mathrm{End}(E^{'}))$ be be another such isomorphism. Then, the pair $(\mathbf{E}^{'}, \kappa^{'})$ is isomorphic to either $(\mathbf{E}, \kappa)$ or to $(\mathbf{E}^{(\mathrm{q})}, \kappa^{(q)})$.

[We say that $(\mathbf{E}, \kappa)$ and $(\mathbf{E}^{'}, \kappa^{'})$ are isomorphic if there is an isomorphism $\mathbf{E} \approx \mathbf{E}^{'}$ for which the induced isomorphism $\iota : \mathrm{End}(\mathbf{E}) \approx \mathrm{End}(\mathbf{E}^{'})$ satisfies $\kappa = \kappa^{'}\iota$. The '(q)'s in superscripts stand for the image under the Frobenius map, of course.]

Proof. As before, we fix an enhanced supersingular curve $\mathbf{E}_0$. Let

$$R = \mathrm{End}(\mathbf{E}_0),\ A = \mathrm{End}(E_0) \text{ and } H = R \otimes \mathbb{Q}.$$

After choosing and fixing an isomorphism $B \otimes \mathbb{Q} \approx H$, we assume that B, $B^{'}$ and S are orders in H.

We divide the proof into various steps:

Step 1: Constructing an injection $\kappa : \mathrm{End}(\mathbf{E}) \otimes \mathbb{Q} \longrightarrow H$.

We first consider all pairs $(\mathbf{E}, \kappa)$ consisting of an enhanced elliptic curve $\mathbf{E}$ and an injection $\kappa : \mathrm{End}(\mathbf{E}) \otimes \mathbb{Q} \longrightarrow H$ (which doesn't necessarily map

End($\mathbf{E}$) to S and End(E) to B). For every non-zero $\lambda \in \mathrm{Hom}(E, E_0) \otimes_{\mathbb{Z}} \mathbb{Q}$, we get such an injection κ_λ which maps $e \in \mathrm{End}(\mathbf{E}) \otimes \mathbb{Q}$ to $\lambda e \lambda^{-1}$. It follows from the Skolem-Noether Theorem that every κ is of the form κ_λ. Also, the choice of λ is unique upto multiplication by an element of $\mathbb{Q}^*$: $\lambda_1 \in \mathrm{Hom}(E, E_0) \otimes_{\mathbb{Z}} \mathbb{Q}$ and $\lambda_2 \in \mathrm{Hom}(E, E_0) \otimes_{\mathbb{Z}} \mathbb{Q}$ give isomorphic pairs $(\mathbf{E}_1, \kappa_1)$ and $(\mathbf{E}_2, \kappa_2)$ iff there exists an isomorphism $\iota : \mathbf{E}_1 \longrightarrow \mathbf{E}_2$ such that λ_1 and λ_2 differ (multiplicatively) by an element of $\mathbb{Q}^*$.

Now, we just saw that the construction

$$(\mathbf{E}, \lambda) \mapsto T(\mathbf{E}) \subset V(\mathbf{E}_0)$$

gives rise to a one-one correspondence between the set of isomorphism classes of pairs $(\mathbf{E}, \lambda)$ and the set ${H_f}^*/{R_f}^*$ of "enhanced" lattices in $V(\mathbf{E}_0)$. If we mod out by $\mathbb{Q}^*$, we obtain a 1-1 correspondence between ${H_f}^*/{R_f}^*\mathbb{Q}^*$ and the set of isomorphism classes of pairs $(\mathbf{E}, \kappa)$ with $\mathbf{E}$ an elliptic curve and κ an injection $\mathrm{End}(\mathbf{E}) \otimes \mathbb{Q} \hookrightarrow H$.

Step 2 : A Necessary and Sufficient Condition (*).
We take $g \in {H_f}^*$ and look at the associated pair $(\mathbf{E}, \kappa)$. Under κ, End($\mathbf{E}$) and End(E) go to the orders $H \cap (gR_f g^{-1})$ and $H \cap (gA_f g^{-1})$ of H respectively. Thus, κ maps End($\mathbf{E}$) to R and End(E) to A iff both the equalities below hold:

$$H \cap (gA_f g^{-1}) = B_f \text{ and } H \cap (gR_f g^{-1}) = S_f. \qquad (*)$$

Step 3 : Verification that condition (*) holds.
We examine these equalities locally at each prime l, i.e., for g now in ${H_l}^*$, we verify for which gs, if any, the following two equalities hold:

$$H \cap (gA_l g^{-1}) = B_l \text{ and } H \cap (gR_l g^{-1}) = S_l. \qquad (**)$$

$(*)$ holds iff $(**)$ holds. We divide the set of all primes into three disjoint sets for this purpose:

Case(a) : $l = q$.
When $l = q$, $(**)$ is satisfied trivially. This is because the quaternion algebra H_q over $\mathbb{Q}_q$ has a unique maximal order [Vig.,Lemme 1.5,p.34] and so every $g \in {H_q}^*$ takes A_q to B_q and R_q to S_q.

Notice that there are two classses in ${H_q}^*/({R_q}^*{\mathbb{Q}_q}^*)$: On ${H_q}^*$, we have a valuation $v : H_q^* \longrightarrow \mathbb{Z}$. By definition, $R_q^* = \{a \in {H_q}^* \mid v(a) = 0\}$. So, it makes sense to define a quotient map: $\overline{v} : {H_q}^*/{R_q}^* \longrightarrow \mathbb{Z}$, defined by $\overline{a} \longmapsto v(a)$. $\mathbb{Z}_q \subset R_q$ is ramified in R_q, i.e., there exists $\pi \in R_q$ such that $\pi^2 = \pm q$, so $v(q) = 0 \pmod 2$ (actually, $v(q) = 2$). So $v({\mathbb{Z}_q}^*) =$

$2\mathbb{Z}$ and $v(\mathbb{Q}_q{}^*) = 2\mathbb{Z}$. Therefore, $\overline{v}$ induces $H_q{}^*/(R_q{}^*\mathbb{Q}_q{}^*) \approx \mathbb{Z}/2\mathbb{Z}$. So, $\mid H_q{}^*/(R_q{}^*\mathbb{Q}_q{}^*) \mid = \mid \mathbb{Z}/2\mathbb{Z} \mid = 2$.

Case(b) : $(l, qM) = 1$.
When l is prime to qM,

$$A_l = R_l \text{ and } B_l = S_l.$$

So the two equalities in $(*)$ become the one and the same equality and this equality can be satisfied because all maximal orders in $\mathbf{M}_2(\mathbb{Q}_l)$ are conjugate [Vig.,2.4.,p.39]. Also, the set of 'g's for which the equality is satisfied form a single class in $H_l{}^*/(R_l{}^*\mathbb{Q}_l{}^*)$. This is because the normalizer of $\mathbf{M}_2(\mathbb{Z}_l)$ in $\mathbf{GL}(2, \mathbb{Q}_l)$ is $\mathbf{GL}(2, \mathbb{Z}_l)\mathbb{Q}_l{}^*$.

Case(c) : $l \mid M$.
Lastly, let $l \mid M$, and let $n > 0$ be such that l^n is the largest power of l dividing M. Then the two Eichler orders R_l and S_l are each intersections of a unique pair of maximal orders of $H_l \approx \mathbf{M}_2(\mathbb{Q}_l)$ [Vig.,2.4,39]: $S_l = B_l \cap B_l{}^*$ and $R_l = A_l \cap A_l{}'$, where $A' = \text{End}(E/B)$. So, $g \in H_l{}^*$ thus conjugates A_l to B_l and R_l to S_l iff it conjugates A_l to B_l and $A_l{}'$ to $B_l{}'$.

We may think of A_l, B_l, $A_l{}'$ and $B_l{}'$ as vertices a, b, a', b' of the tree Δ associated to $\mathbf{SL}_2$ over $\mathbb{Q}_l$. To do so, we notice that the vertices of Δ are the lattices in $\mathbb{Q}_l \oplus \mathbb{Q}_l$, taken modulo homothety. The map sending the lattice $L \subset \mathbb{Q}_l \oplus \mathbb{Q}_l$ to the maximal order $\text{End}(L)$ of $\mathbf{M}_2(\mathbb{Q}_l)$ sets up a 1-1 correspondence between the vertices of Δ and the maximal orders in $\mathbf{M}_2(\mathbb{Q}_l)$ [Vig.,p.41].

As R and S are Eichler orders of level M and $l^n \mid\mid M$, the vertices a and b are at a distance n from each other, as are the vertices a' and b'. We know from the Elementary Divisor Theorem that it is possible to find a basis e_1, e_2 of $\mathbb{Q}_l \oplus \mathbb{Q}_l$ so that a is represented by the lattice $\mathbb{Z}_l e_1 \oplus \mathbb{Z}_l e_2$ and b by the lattice $\mathbb{Z}_l e_1 \oplus l^n \mathbb{Z}_l e_2$. Similarly, there is a basis f_1, f_2 of $\mathbb{Q}_l \oplus \mathbb{Q}_l$ such that a' is represented by the lattice $\mathbb{Z}_l f_1 \oplus \mathbb{Z}_l f_2$ and b' is represented by the lattice $\mathbb{Z}_l f_1 \oplus l^n \mathbb{Z}_l f_2$. If $g \in \mathbf{GL}(2, \mathbb{Z}_l)$ maps e_1 to f_1 and e_2 to f_2, then g conjugates A_l to B_l and $A_l{}^*$ to $B_l{}^*$. On the other hand, if h also conjugates A_l to B_l and $A_l{}^*$ to $B_l{}^*$, we have

$h^{-1}g \in N(A_l) \cap N(B_l) = (A_l{}^*\mathbb{Q}_l{}^*) \cap (B_l{}^*\mathbb{Q}_l{}^*) = (A_l{}^* \cap B_l{}^*)\mathbb{Q}_l{}^* = R_l{}^*\mathbb{Q}_l{}^*$.

Hence, the set of 'g's conjugating A_l to B_l and $A_l{}^*$ to $B_l{}^*$ again make up a single class in $H_l{}^*/(R_l{}^*\mathbb{Q}_l{}^*)$.

Step 4 : The Conclusion. After examining each local classs, we conclude that the g in $H_f{}^*$ which conjugate A_f to B_f and R_f to S_f form exactly two classes in $H_f{}^*/(R_f{}^*\mathbb{Q}^*)$. These classes are interchanged by left multiplication

by any element of $H_f{}^*$ which is trivial outside the prime q and has odd valuation at q. It is a fact that this multiplication corresponds to the Frobenius map.

■

3.5 The Action of Hecke Operators on the Character Group X.

Definition. The $\mathbf{n^{th}}$ Hecke correspondence T_n. For an integer N, we consider a model of the curve $X_0(N)$ (over $\mathbb{Q}$). If n is an integer which is coprime to N, we define the correspondence T_n (which is an endomorphisn on the set of divisors of $X_0(N)$) on this curve by the following recipe:

$$T_n(E, C_N) := \sum_{C_n}(E/C_n, C_N + C_n/C_n) = \sum_{C_n}(E/C_n, C_N(\text{mod} \quad C_n))$$

where the sum is taken over all cyclic isogenies of degree n in E. If $\gcd(n, N) > 1$, T_n is defined by a similar sum, but now the C_ns have no other choice than running through the set of isogenies such that $C_n \cap C_N = \{0\}$.

Note that as $C_N + C_n/C_n$ is again a cyclic isogeny of degree n in E, it makes sense to define ${T_n}^r$ for $r \geq 1$ using linearity of T_n. Let $J_0(N)$ be the jacobian of $X_0(N)$. By Albanese functoriality, the T_n as defined above induces an operator on $J_0(N)$, which by abuse of notation, we will call T_n too. Abel-Jacobi theorem tells us that $J_0(N)$ can be idetified with $\text{Pic}^0(X)$. Under this identification, we now define what the "induced" T_ns turn out to be.

If $x \in J_0(N)$, then $x = \sum n_i(P_i)$ for some closed points P_i in $X_0(N)$ with $\sum n_i = 0$. We define

$$T_n(x) := \sum n_i T_n(P_i).$$

The T_ns on the right hand side of the equation are the usual T_ns on $X_0(N)$ as defined in above. Let $\mathbb{T}$ be the subalgebra of $\text{End}(J_0(N))$ generated by the T_ns. It is clear that one may extend the actions of individual T_n to $\mathbb{T}$ by linearity. Thus $\mathbb{T}$ acts on $J_0(N)$ and hence on its Néron model $\mathcal{J}_0(N)$ at each prime dividing N. As before, we concentrate on the case $N = qM$, with q a prime and M coprime to q. It is a fact that there is an exact sequence

$$0 \longrightarrow T \longrightarrow \mathcal{J}_0(N) \longrightarrow \mathcal{A} \longrightarrow 0,$$

where T is a torus and $\mathcal{A}$ is an abelian variety. So $\mathbb{T}$ acts on T too and by functoriality, it acts on its character group $X = X(T) = \mathrm{Hom}(T, \mathrm{G}_{\mathbf{m}})$. Using the same notations as before, we recall that there is an isomorphism $X \approx H_1(\mathcal{G}, \mathbb{Z})$ and an incusion $X \hookrightarrow \mathbb{Z}^I$. Also, $I = \Sigma(M)$ in our case, i.e., the set of isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}_q}$ enhanced by a cyclic subgroup of order M. So, let us try to determine the induced action of T_ns on $\Sigma(M)$.

We first consider the case when n is prime to q. The T_ns operate on $\Sigma(M)$ in the evident way, i.e., via the same "modular rules" which define the T_ns over $\mathbb{Q}$. We give here the rule for T_n when n is a prime number $r \neq q$; we give the expression for $T_r(\mathbf{E})$, where $\mathbf{E}$ is an elliptic curve E which is enhanced by a cyclic of subgroup M.

We distinguish cases according as r is prime to M or a divisor of M. In the former case, we have the standard expression

$$T_r(\mathbf{E}) = \sum_C \mathbf{E}/C$$

,

where the sum is taken over all the subgroups C of order r in E and where $\mathbf{E}/C$ is the elliptic curve E/C with the evident subgroup of order M. In the case where r divides M, the enhancement of E provides E, in particular, with a subgroup D of order r. We have

$$T_r(\mathbf{E}) = \sum_{C \neq D} \mathbf{E}/C$$

Now, if $\omega \in H^0(J_0(N), \Omega^1)$, then one defines $T_n(\omega)$ as follows:

$$T_n\omega(x) = \sum_{T_n(x) = \sum y} \omega(y) \in H^0(J_0(N), \Omega^1).$$

Therefore T_n defines an element in $\mathrm{End}(H^0(J_0(N), \Omega^1))$=$\mathrm{End}(S_2(\Gamma_0(N)))$. Thus $\mathbb{T}$ acts on $\mathrm{End}(S_2(\Gamma_0(N)))$.

3.6 Comparison with the Curve $X_0(pqM)$.

We recall that p is a prime number which is coprime to qM. Also, we will continue to understand that "enhanced elliptic curves " are elliptic curves which are enhanced by cyclic subgroups of order M. We will compare $X_0(pqM)$ with $X_0(qM)$ by replacing the M in sections 3.2-3.5 with a pM. (We can

clearly do this because we assumed that p and q are distinct primes and $(M, pq) = 1$.)

We again use X to denote the group $\mathrm{Div}(\Sigma(M))$ of degree-0 divisors on the set of supersingular points of $X_0(qM)_{\overline{\mathbb{F}_q}}$. Let L be the analogue of X with qM replaced by pqM, i.e., the character group associated to $X_0(pqM)_{\overline{\mathbb{F}_q}}$. The analogue of Proposition (3.3) for $X_0(pqM)$ describes L in terms of supersingular elliptic curves which are enhanced by cyclic subgroups of order pM. We can regard such objects as p-isogenies

$\mathbf{E}_1 \longrightarrow \mathbf{E}_2$,

where $\mathbf{E}_1$ and $\mathbf{E}_2$ are enhanced by subgroups of order M.

We have two natural degenracy maps $\tilde{\alpha}, \tilde{\beta} : X_0(pqM) \rightrightarrows X_0(qM)$,

defined by :

$$\tilde{\alpha} : (E, C_{qM}, C_p) \longmapsto (E, C_{qM}),$$

and

$$\tilde{\beta} : (E, C_{qM}, C_p) \longmapsto (E/C_p, (C_{qM} + C_p)/C_p).$$

These two induce maps $\tilde{\alpha}_*, \tilde{\beta}_* : L \rightrightarrows X$, which can be realized explicitly by the maps sending $\mathbf{E}_1 \longrightarrow \mathbf{E}_2$ to $\mathbf{E}_1$ or $\mathbf{E}_2$. These two combine to make a single degeneracy map

$$\delta : L \longrightarrow (X \oplus X).$$

Let Y be the kernel of δ. Then we have an exact sequence:

$$0 \longrightarrow Y \longrightarrow L \longrightarrow (X \oplus X) \longrightarrow 0.$$

We will try to find relations between the above sets and the above maps in the next chapter.

4 Bad Reduction of Shimura Curves

In this chapter, we will introduce Shimura curves, and we will make a "quaternionic description of their dual graphs" anologous to that of Chapter 3 for modular curves. We will describe those graphs in terms of supersingular elliptic curves (see Theorem 3.3). That will allow us to make a concrete study of those graphs in Chapter 5. We will also describe Ribet's theorem, linking character groups in the Shimura curves setting to the more familiar analogue in the case of modular curves.

4.1 Basic Definitions.

Let $D = p_1 p_2 ... p_{2m}$ be the product of an even number of (finite) primes in $\mathbb{Z}$, the various 'p_i's being distinct. As we saw in Chapter 3, $B_D \otimes \mathbb{R} \approx \mathbf{M}_2(\mathbb{R})$. So, picking a maximal order O_D in B_D, one gets an injection:

${O_D}^+ \hookrightarrow {O_D}^* \hookrightarrow (O_D \otimes_{\mathbb{Z}} \mathbb{Q})^* = {B_D}^* \hookrightarrow (B_D \otimes_{\mathbb{Q}} \mathbb{R})^* \approx GL_2(\mathbb{R})$ (see 3.1).

We denote the composition of the above maps ${O_D}^* \hookrightarrow \mathbf{GL}_2(\mathbb{R})$ by i.

Now, consider the Riemann surface $i(O_D^+)\backslash\mathcal{H}$. Shimura has proved that this is a compact Riemann surface. (Thinking of the case $B_D \approx \mathbf{M}_2(\mathbb{Q}), {O_D}^+ = \mathbf{SL}_2(\mathbb{Z})$, one obtains the classical modular curves over $\mathbb{C}$, which are not compact.) We define $X^D/\mathbb{C}$, the **Shimura Curve** associated to B_D to be this compact Riemann surface $i(O_D^+)\backslash\mathcal{H}$. This Riemann surface has the following modular interpretation: it parameterizes principally polarized abelian surfaces whose ring of endomorphisms contains a maximal order in the quaternion algebra B_D.

It is a fact that such a $X^D/\mathbb{C}$ has a "modular" model over $\mathbb{Q}$ (proved by Shimura), and also over $\mathbb{Z}[1/D]$ (proved by Deligne-Rapoport) and even over $\mathbb{Z}$ (proved by Cerednik-Drinfeld).

Variation. We take B_D as above. For N coprime to D, we define ${O_D}^0(N)$ to be the set of $x \in O_D$, for which upon identifying $O_D \otimes \mathbb{Z}_l$ with $M_2(\mathbb{Z}_l)$ for $l \nmid D$, one gets $x \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} (\text{mod } l^n)$, $\forall l \nmid D$, $l^n \parallel N$.

Again, one builds in the same way as above, a curve ${X_0}^D(N)/\mathbb{Q}$ (by replacing O_D by ${O_D}^0(N)$, which we will call a **Shimura curve** of **discriminant** D and **level** N.

We finally note that $\text{Jac}({X_0}^D(N))_{\mathbb{Q}} \approx (J_0(ND))^{D\text{-new}}$. (Recall that $J_0(ND)$ is isogenous to $\prod (J_f)^{e_f}$, where f runs through the (finite) set of newforms of some level M dividing ND, and J_f is the sub-abelian variety of $J_0(ND)$ corresponding to f as defined by Shimura. Then, $J_0(ND)^{D\text{-new}}$ is

isogenous to $\prod(J_\phi)^{e_\phi}$, where ϕ runs through the newforms of some level M divisible by D (and dividing ND, of course).)

4.2 Our Setting.

Let p and q be distinct primes, and let M be an integer prime to pq. Let B be an indefinite quaternion algebra over $\mathbb{Q}$ of discriminant pq. (Up to isomorphism, B is unique.) Let $\mathcal{O}$ be an Eichler order of level M (i.e., reduced discriminant Mpq) in B. Let Γ_∞ be the group of elements of $\mathcal{O}$ with reduced norm 1. After fixing an embedding $B \to \mathbf{M}_2(\mathbb{R})$, we obtain in particular an embedding $\Gamma_\infty \to \mathbf{SL}_2(\mathbb{Z})$ and therefore an action of Γ_∞ on the Poincare upper half- plane $\mathcal{H}$. Let C be the standard model over $\mathbb{Q}$ of the compact Riemann surface $\Gamma_\infty\backslash\mathcal{H}$, and let J be the Jacobian $\mathrm{Pic}^0(C)$. The curve C is furnished with Hecke correspondences T_n with $n \geq 1$. In analogy with the situation in Chapter 3, we again write T_n for the endomorphism of J induced by T_n via Pic functoriality.

For simplicity, we simply write C for the curve $C_{\mathbb{Q}_p}$ and J for $J_{\mathbb{Q}_p}$. A model $\mathcal{C}$ for C over $\mathbb{Z}_p$ as considered in Chapter 2 was constructed by Cerednik in [Cer]; and by Drinfeld in [Drin]. Drinfeld gave a modular-theoretic interpretation of Cerednik's construction. It follows, in particular, from their work, that J has purely toric reduction at p. Let Z be the character group of the torus at $(J_{\mathbb{F}_p})^0$.

Recall that we can define the dual graph $\mathcal{G}$ of the fiber at p of $\mathcal{C}$, and that Z is isomorphic to $H_1(\mathcal{G}, \mathbb{Z})$ (cf. Proposition 2.2).

Let $\tilde{\mathbb{T}}$ be the formal polynomial ring $\mathbb{Z}[T_1, T_2, ...]$ generated by the commuting indeterminates T_n. There is a standard action of $\tilde{\mathbb{T}}$ on J, in which $T_n \in \tilde{\mathbb{T}}$ acts as T_n on J.

The objective of this section is, as we said in the forewords, to to relate Z to the $\mathbb{T}$-modules L, $X \oplus X$, Y, etc. of Chapter 3 (Since the Hecke operators T_n on $J_0(Mpq)$ make $\mathbb{T}$ a quotient of $\tilde{\mathbb{T}}$, every $\mathbb{T}$ module is naturally a $\tilde{\mathbb{T}}$-module.)

4.3 Figuring out $\mathcal{G}$

Now let H be the quaternion algebra over $\mathbb{Q}$ with discriminant q. Let R be a Eichler order of level M in H. Let $S \subset R$ be the Eichler order of level Mp in H gotten by intersecting R with the evident Eichler order in $M(2, \mathbb{Z}_p)$:

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(2, \mathbb{Z}) | p \text{ divides } c \right\}.$$

Let $\mathcal{V}$ be the set of isomorphism classes of locally free rank-1 left R-modules, and let $\mathcal{E}$ be the set of isomorphism classes of locally free rank-1 left S-modules. We have canonically

$\mathcal{V} = {R_f}^* \backslash {H_f}^* / H^*$,

$\mathcal{E} = {S_f}^* \backslash {H_f}^* / H^*$.

The inclusion of S into R defines a degeneracy map

$\alpha : \mathcal{E} \longrightarrow \mathcal{V}$.

A second degeneracy map

$\beta : \mathcal{E} \longrightarrow \mathcal{V}$

is obtained by considering the Eichler order T of H which has level M, contains S, agrees with R locally at all places except for p, and is distinct from R. The order T is given adelically as mRm^{-1}, where m is trivial except at p, where it is the diagonal matrix diag(1,p). The analogue of α for T is a map from $\mathcal{E}$ to the double coset space

$m{R_f}^* m^{-1} \backslash {H_f}^* / H^*$.

We get β by identifying this space with $\mathcal{V}$ via multiplication by m^{-1} on $(H_f)^*$. Hence β maps the class of x in the double-coset space defining $\mathcal{V}$ to the class of $m^{-1}x$ in the double-coset space defining $\mathcal{V}$. Then we get the following theorem,which we state without proof, and that will be our main result for this chapter:

Theorem 4.1 *The set of edges of $\mathcal{G}$ is canonically the set $\mathcal{E}$. The set of vertices of $\mathcal{G}$ is the disjoint union $\mathcal{V} \times \{1, 2\}$ of two copies of $\mathcal{V}$. A given edge $e \in \mathcal{E}$ connects the vertex $(\alpha(e), 1)$ with the vertex $(\beta(e), 2)$.*

It follows from the above theorem that the character group Z, a priori the group $H_1(\mathcal{G}, \mathbb{Z})$ is the kernel of the map $\omega : \mathbb{Z}^{\mathcal{E}} \longrightarrow \mathbb{Z}^{\mathcal{V}} \times \mathbb{Z}^{\mathcal{V}}$ induced by $(\alpha, \beta) : \mathcal{E} \longrightarrow \mathcal{V} \times \mathcal{V}$. An element of Kernel($\omega$) visibly has degree 0 as a formal linear combination of elements of $\mathcal{E}$. Writing $(\mathbb{Z}^{\mathcal{E}})_0$ and $\mathbb{Z}_0^{\mathcal{V}}$ for the group of degree-0 divisors on $\mathcal{E}$ and $\mathcal{V}$, we get:

Corollary 4.2 *The character group Z is the kernel of the degeneracy map*

$\omega_0 : \mathbb{Z}_0^{\mathcal{E}} \longrightarrow \mathbb{Z}_0^{\mathcal{V}} \times \mathbb{Z}_0^{\mathcal{V}}$

induced by (α, β).

Now, we compare the groups Z and Y (see Chapter 3). By definition, Y is the kernel of a natural degeneracy map $\delta : L \longrightarrow X \oplus X$, where L and X are the groups of degree-0 divisors on the sets $\Sigma(Mp)$ and $\Sigma(M)$ of supersingular points on $X_0(Mp)$ and $X_0(M)$ in characteristic q. Z has an analogous description (Corollary 4.2) with $\mathbb{E}_0$ replaced by $\mathcal{E}$ and $\Sigma(M)$ replaced by $\mathcal{V}$. Taking first $M = Mp$ and then $M = M$ in Proposition 3.4, we

find that $\Sigma(Mp)$ and $\Sigma(M)$ are double-coset spaces of the type defining $\mathcal{E}$ and $\mathcal{V}$, but with the orders S and R replaced by orders of the form $\mathrm{End}(\mathbb{E}_0, C_p)$ and $\mathrm{End}(\mathbb{E}_0)$. Hence, $\mathbb{E}_0$ is (as usual) a supersingular elliptic curve E_0 in characteristic q which has been enhanced by a cyclic subgroup of E_0 having order p. To compare the pairs $(\mathcal{E}, \mathcal{V})$ and $(\Sigma(Mp), \Sigma(M))$, Ribet shows that there exists a $\mathbb{E}_0$, C_p such that $\mathrm{End}(\mathbb{E}_0, C_p) = S$ and $\mathrm{End}(\mathbb{E}_0) = R$, hence proving that there are $(\mathcal{E}, \mathcal{V}) = (\Sigma(Mp), \Sigma(M))$. This leads to:

Theorem 4.3 *There is a $\tilde{\mathbb{T}}$-isomorphism $Z \approx Y$.*

In the statement of this theorem, we understand that the actions of $\tilde{\mathbb{T}}$ on Z and on Y to be the standard (Pic) actions.

Define $\overline{\mathbb{T}}$ to be the quotient of the torus cut out by the space $S_{pq-\mathrm{new}}$ of forms on $\Gamma_0(pqM)$ which are new relative to p and q(i.e., forms in $S_2(\Gamma_0(pqM))$ whose *exact* level is a multiple of pq). It can be proved that it is also the quotient of $\mathbb{T}$ cut out by Y. Also, since J has purely toric reduction, $\mathrm{End}_{\mathbb{Q}}(J)$ operates faithfully on Z. Therefore, the above Theorem implies:

Corollary 4.4 *There is a unique injection $\overline{\mathbb{T}} \longrightarrow End(J)$ mapping the n^{th} Hecke operator in $\overline{\mathbb{T}}$ to the n^{th} Hecke operator on J.*

4.4 Definition of $\mathcal{G}(X_{pq}/\overline{\mathbb{F}_p})$.

Now, to make things easier for us in the next chapter, we sum up the various results that we obtained in this chapter and which are going to be useful for understanding the material of the next chapter.

Consider the special case $M = 1$From what we have said above, one sees that $\mathcal{V} \approx \Sigma(1)$ and $\mathcal{E} \approx \Sigma(p)$. By Proposition 4.4, we know that $\mathcal{G}$ in this case has two copies of $\mathcal{V}$ as its set of vertices and the set $\mathcal{E}$ as its set of edges. We define X_{pq} to be the Shimura curve associated to the quaternion algebra B_{pq}. It is a fact that at p, $X_{pq}/\overline{\mathbb{F}_p}$ is a union of projective lines with ordinary double points as singularities, so $J(X)^0_{\overline{\mathbb{F}_p}}$ is purely toric, i.e., it is a torus: $J(X)^0_{\overline{\mathbb{F}_p}} \approx {G_m}^g/\overline{\mathbb{F}_p}$, where g is the dimension of the torus. We define $\mathcal{G}(X_{pq}/\overline{\mathbb{F}_p})$ to be the "dual graph" associated to this Shimura curve X_{pq}. Recalling the definition of $\Sigma(1)$ and $\Sigma(p)$, from what we said just now, it follows that:

Theorem 4.5 *Let $\mathcal{V}_{pq}$ and $\mathcal{E}_{pq}$ be the set of vertices and edges of the graph $\mathcal{G}(X_{pq}/\overline{\mathbb{F}_p})$. Then we have:*

$\mathcal{V}_{pq} \approx \mathcal{V}_1 \cup \mathcal{V}_2$

where $\mathcal{V}_1 = \{$supersingular elliptic curves in characteristic $q\}/\approx$.

$\mathbb{E}_1 \in \mathcal{V}_1$ *and* $\mathbb{E}_2 \in \mathcal{V}_2$ *are linked by an edge if and only if there is an isogeny* $\mathbb{E}_1 \longrightarrow \mathbb{E}_2$ *of degree* p*, i.e.,*

$\mathcal{E}_{pq} = \{(\mathbb{E}, C_p) \mid \mathbb{E}$ *is a supersingular elliptic curve in characteristic* $q, C_p \subset \mathbb{E}$ *is a* p*-isogeny*$\}/\approx$

Remark. Remembering the concept of *dual isogenies*, we see that there is a p-isogeny $\mathbb{E}_1 \longrightarrow \mathbb{E}_2$ if and only if there is a p-isogeny $\mathbb{E}_2 \longrightarrow \mathbb{E}_1$. So, this graph $\mathcal{G}(X_{pq}/\overline{\mathbb{F}_p})$ is symmetric or bipartite.

5 Is $\mathcal{G}(X_{pq}/\overline{\mathbb{F}_p})$ non-disconnecting?

5.1 Edixhoven's Theorem.

Now, it's time that we come back to the question that we promised to attempt to answer in our "Introduction":

Question. *Let X be a Shimura curve over $\mathbb{Q}$ and $X \to J$ be an Albanese morphism to its Jacobian. Consider the extension: $X^{\mathrm{sm}} \to \mathcal{J}$ from the smooth locus X^{sm} of the Cerednik-Drinfeld model of X over $\mathbb{Z}_p$, to the Néron model $\mathcal{J}$ of J over $\mathbb{Z}_p$. When is this extended morphism a closed immersion?*

Thanks to a theorem of Edixhoven, we can translate this abstract question into the simple combinatorial language of graphs and the property of their being "non-disconnecting". To answer this question (or even understand it properly), we first need to introduce and recall a few concepts.

Definition. Albanese Morphism. Let X be a curve over a field k, and suppose that $X(k) \neq \varnothing$. Let $P \in X(k)$ be arbitrary. Then the Albanese morphism $\Phi(P)$ from X to its jacobian J is defined as the morphism sending Q to the divisor class $(Q - P)$. (Recall that $\mathrm{Jac}(X) \approx \mathrm{Pic}^0(X)$.)

For the rest of this section, we fix a discrete valuation ring D with fraction field K, uniformizer π and residue field k.

Definition. Nodal Curve. Let X be a flat curve over $\mathrm{Spec}(D)$. We will say that X/D is a nodal curve if all the singularities are ordinary double points, i.e., if the point of X outside the smooth locus have local equation $xy = 0$ in the their fiber.

Definition. Non-disconnecting. A graph G is *non-disconnecting* if even after removing any arbitrarily chosen edge E from it, the graph $G\backslash E$ is connected. It is *disconnecting* otherwise.

Now, we have necessary vocabulary to understand our original question and Edixhoven's result which answers when and to what extent the concerned extended morphism is a closed immersion.

Theorem 5.1 ***(Edixhoven.)*** *Let X be a proper and flat curve over $\mathrm{Spec}(D)$, which is regular, generically smooth, and nodal. Suppose that the fibre X_K*

of X is smooth over K, geometrically irreducible and has non-zero genus. Let P be a given point in $X(K)$. Let $f_K : X_K \longrightarrow J_K$ be the usual closed immersion sending Q to $(Q - P)$. Let $f : X^{\mathrm{sm}} \longrightarrow \mathcal{J}$ be the induced morphism from the smooth locus X^{sm} of X to the Néron model $\mathcal{J}$ over D of J_K. Then f is a closed immersion if and only if the dual graph of the curve $X_{\overline{k}}$ is non-disconnecting where $\overline{k}$ is some algebraic colsure of k.

Note that if X/D is as in the above definition, then its smooth locus (that is, the largest open subscheme of X which is smooth over D) is the complement in X of a finite set of singular points of X_k. (Recall that $X_k \subset X$.)

Let us restrict ourselves to the case when X is a Shimura curve X_{pq}, where X_{pq} is defined as in the previous chapter. So, now, we have a new motivation for looking at the graph $\mathcal{G}(X_{pq}/\overline{\mathbb{F}_p})$ and examining its disconnectivity properties, and that's what we precisely intend to do next, as the name of this chapter indicates. In the light of Edixhoven's theorem, determining whether this graph is non-disconnecting or not, would give us the answer to the following quesion too:

Question. *Let X_{pq} be the Shimura curve associated to the quaternion algebra B_{pq}. If $P \in X(\mathbb{Z}_p)$,look at the closed immersion $f_P/\mathbb{Q}_p : X \longrightarrow J$ sending Q to $(Q) - (P)$. Send this map to the naturally "derived" map $f_P/\mathbb{Z}_p : X/\mathbb{Z}_p \longrightarrow J/\mathbb{Z}_p$ where J, of course, is defined as above. When is $f_P/\mathbb{Z}_p$ a closed immersion?*

5.2 Some Basics.

We still focus on the dual graph $\mathcal{G}(X_{pq}/\overline{\mathbb{F}}_p)$ of the Shimura curve X_{pq}, where p and q are some finite primes. We concluded our last chapter by saying that the set of vertices of the bipartite graph $\mathcal{G}(X_{pq}/\overline{\mathbb{F}}_p)$ is given by two copies $\mathcal{V}_1$ and V_2 of supersingular elliptic curves in characteristic q and its set of edges is given by the set of p-isogenies between these classes of elliptic curves. Here we are going to talk about *how* exactly we determine whether there is the number of edges,if any, between any two vertices in the two different copies of the graph.

At first, we recall some basic facts about elliptic curves that we again need here. First, there are finitely many supersingular elliptic curves over a field, as they all belong to $\mathbb{F}_{p^2}$ (if p is the characteristic of this field). Second, the j-invariants $j = 0$ and $j = 1728$ are special. The only elliptic curves

which may have some special automorphism (i.e., some automorphism other than multiplication by ± 1) are the elliptic curves with *j-invariant* equal to 0 or 1728. If E has *j-invariant* 0, then $\mathrm{End}(E)$ contains a non-trivial third root of unity. And if E has *j-invariant* 1728, then $\mathrm{End}(E)$ contains a non-trivial fourth root of unity.

Now, given a q, let $j_0, j_2, ..., j_g$ be the set J of j-invariants representing the classes of supersingular elliptic curves over $\overline{\mathbb{F}_q}$. As we saw in the last chapter, the set of vertices of $\mathcal{G}(X_{pq}/\overline{\mathbb{F}_p})$ is given by two copies, say $\mathcal{V}_1$ and $\mathcal{V}_2$, of the elements of J. Let E_{j_i} denote the isomorphism class of supersingular elliptic curves corresponding to the j-value j_i. Let $C_{r,l}$ be the vertex corresponding to the j-value j_l in the copy $\mathcal{V}_r; r = 1, 2$ of J. We outline here a method to determine whether there is an edge between $C_{1,l}$ and $C_{2,m}$, or equivalently, detemining whether there is a p-isogeny between the isomorphism classes E_{j_l} and E_{j_m}. Due to the symmetry of the dual graph $\mathcal{G}(X_{pq}/\overline{\mathbb{F}_p})$, it is clear that it is sufficient to look at the *Mestre-Oesterlé graph* $G(X_{pq}/\overline{\mathbb{F}_p})$ with V and E as its set of vertices and edges respectively, where V is defined as the set J of supersingular j-invariants in characteristic q, and there is an edge $e \in E$ connecting j_l and j_m if and only if there is a p-isogeny between the isomorphism classes E_{j_l} and E_{j_m}.

We want to know about the edges emanating from the vertex j_l of $G(X_{pq}/\overline{\mathbb{F}_p})$. The idea is to look at the modular polynomial $\Phi_p(X, Y)$ and consider its reduction modulo q when $Y = j_l$ is substituted. (Recall that $\Phi_p(X, Y)$ is the bivariate symmetric polynomial such that $\Phi_p(X, j_l)$ is the polynomial whose roots are the j-invariants of elliptic curves linked by a p-isogeny to an elliptic curve with j-invariant equal to j_l). Suppose that $j_l \neq 0, 1728$. Let $j_{l,1}, ..., j_{l,(p+1)}$ be the roots of $\Phi_p(X, j_l)$ in $\mathbb{F}_{q^2}$ occuring with multiplity $\alpha_1, ..., \alpha_{p+1}$ respectively. It is a fact that there are α_k edges from j_l to $j_{l,k}$; $k = 1, ..., (p + 1)$, in $G(X_{pq}/\overline{\mathbb{F}_p})$. If there happens to be multiple number of p-isogenies $\phi\colon \mathbb{E}_1 \longrightarrow \mathbb{E}_2$ between the corresponding classes of supersingular elliptic curves which are isomorphic (that is, $(\mathbb{E}_1, \phi) = (\mathbb{E}_1, \phi \circ \iota)$, for $\iota \in \mathrm{Aut}(\mathbb{E}_1)$), then they will be counted as just one single edge in $G(X_{pq}/\overline{\mathbb{F}_p})$ and the derived graph $\mathcal{G}(X_{pq}/\overline{\mathbb{F}_p})$.

Note that the p-isogenies in a elliptic curve E over $\overline{\mathbb{F}}_q$ lie in $E[p](\overline{\mathbb{F}_q}) \approx {\mathbb{F}_p}^2$ if $p \neq q$. So,it is clear that the number of p-isogenies is given by the number of elements in $\mathbb{P}(E[p]) \approx \mathbb{P}^1(\mathbb{F}_p)$ which is equal to $(p + 1)$. So, if there is no special automorphism on E, i.e. if $j \neq 0, 1728$, then we must have $p + 1$ edges emanating from each vertex and the same number of edges going into it.

As the name of this chapter indicates, we aim to examine the property of non-disconnectivity of the graph $\mathcal{G}(X_{pq}/\overline{\mathbb{F}_p})$ in this chapter.

5.3 The Asymptotic Case.

We give here a theorem which lets us guess something about the asymptotic behaviour of $\mathcal{G}(X_{pq}/\overline{\mathbb{F}_p})$ when p is sufficiently large compared to q. We continue using the same notations as before and introduce some more. We write the bipartite graph $\mathcal{G}(X_{pq}/\overline{\mathbb{F}_p})$ as a union $\mathcal{V}_1 \cup \mathcal{V}_2$ and enumerate the vertices of $\mathcal{V}_r$ as $\{C_{r,0}, ..., C_{r,g}\}$ for $r = 1, 2$ as before. Each $j_s \in J$ corresponds to an elliptic curve E_{j_s} and we set $w(j_s) := card(\mathrm{Aut}(E_s)/\{\pm 1\})$. One knows that at most two $w(j_s)$ s are different from 1, in which case they are equal to 2 or 3 (at least if p and q do not divide 6, see previous section). The Eisenstein vector Eis for $X_0(q)_{\mathbb{F}_q}$ is defined to the vector $(w(j_0)^{-1}, ..., w(j_g)^{-1})^t \in \frac{1}{12}\mathbb{Z}^S$. For $v = (v_i)_{i\in S} \in \mathbb{C}^S$, we define the weight $W(v)$ as $\sum_{i\in S}(v_i)$. The weight $W(\mathrm{Eis}) = \sum(w(C_r))^{-1}$ is approximately equal to $q/12$.

Theorem 5.2 *(**Parent-Yafaev**) Fix a prime $q > 3$. As the prime p tends to infinity, the edges of $\mathcal{G}(X_{pq}/\overline{\mathbb{F}_p})$ are equidistributed in the following sense. If $C_{1,l}$ and $C_{2,m}$ are elements of $\mathcal{V}_1$ and $\mathcal{V}_2$ respectively, the number of edges from $C_{1,l}$ to $C_{2,m}$ is:*

$\frac{(p+1)}{W(\mathrm{Eis})} \times \frac{1}{w(C_{1,l})w(C_{2,m})} + O_q(\sqrt{p})$.

Now, from the preceeding paragraph, we know that $W(Eis) \approx \frac{q}{12}$ and that each of $w(C_{1,l})$ and $w(C_{2,m})$ are lesser than or equal to 3. Thus, if $p >> q$, then the number of edges from $C_{1,l}$ to $C_{2,m}$ is $\geq \frac{12(p+1)}{q} \times \frac{1}{3\times 3} + O_q(\sqrt{p})$, which in turn is greater than $\frac{4(p+1)}{3q}$, which in particular is greater than 1. So,if $p >> q$, then there are multiple edges between each pair of vertices $C_{1,l}$ and $C_{2,m}$,$0 \leq l, m \leq g$. And it is clear that removing one edge from such a graph $\mathcal{G}(X_{pq}/\overline{\mathbb{F}_p})$ will not affect its disconnectivity properties. Thus the graph formed by removing one of its edges will also be connected in such a case. In other words, $\mathcal{G}(X_{pq}/\overline{\mathbb{F}_p})$ is non-disconnecting when p is sufficiently larger than q.

5.4 Guessing about the behaviour of $\mathcal{G}(X_{pq}/\overline{\mathbb{F}_p})$ for odd p and q

The asymptotic behaviour leads us to guess that the graph $G(X_pq/\overline{\mathbb{F}_p})$ is always non-disconnecting when p and q are odd and large enough. It would be interesting if one can really prove or disprove this conjecture.

5.5 The Answer to the $p = 2$ Case.

In this section, we will settle the question of connectivity for graphs of the form $\mathcal{G}(X_2q/\overline{\mathbb{F}_2})$, q being an odd prime. We first claim that the following proposition holds and then proceed to prove it.

Proposition 5.3 *The graph $\mathcal{G}(X_{2q}/\overline{\mathbb{F}_2})$ is disconnecting whenever $q \equiv -1 (mod\ 3)$ or $q = 3$ and is hence disconnecting for infinitely many primes q.*

Let us see what the general method for determining edges outlined in Section 2 yeilds for the particular case $p = 2$.

The modular polynomial $\Phi_2(X, Y)$ is given by:

$\Phi_2(X,Y) = X^3 + Y^3 - X^2Y^2 + 2^4.3.31.XY(X+Y) - 2^4.3^4.5^3(X^2+Y^2) + 3^4.5^3.4027.XY + 2^8.3^7.5^6(X+Y) - 2^{12}.3^9.5^9$.

In this case, the number of edges emanating from each vertex and going into it $= 2 + 1 = 3$. Mestre and Oesterlé made the following computations for the case $p = 2$ for determining whether the edges emanating from $j_l \in J$ and ending at $j_m \in J$ in $G(X_{2q}/\overline{\mathbb{F}_2})$ (This method doesn't take special automorphisms into account):

Case 1:If j_l and j_m are both distinct from 0 and 1728, then the multiplicity (possibly 0) of edges between them is equal to the multiplicity of the the factor $(X - j_m)$ in the factorisation of the polynomial $\Phi_2(X, j_l)$ (mod q).

Case 2: If $j_l = 0 (\text{mod } q)$, then we have $\Phi_2(X, j_l) = \Phi_2(X, 0) = (X - 54000)^3$ (mod q) and so there are three edges from $0 \longrightarrow 54000$. Also, $\Phi_2(X, 54000) = XP(X)$, where $P(X) = X^2 - 2835810000X + 6549518250000$. So, there is one edge $54000 \longrightarrow 0$ (and only one if q does not divide the constant term of P). The other 2 edges emanating from $j = 54000$ end at the root(s)of $P(X)$ mod q.

Case 3: If $j_m = 1728 (\text{mod } q)$, then we have $\Phi_2(X, j_m) = \Phi_2(X, 1728) = (X - 1728)(X - 66^3)^2$ (mod q) and there is one edge from $j_m = 1728$ to $j_l = 1728$ and another two edges from $j_m = 1728$ to $j_l = 66^3$. Also, $\Phi_2(X, 66^3) = (X - 1728)Q(X)$, where $Q(X) = X^2 - 82226316240X - 7367066619912$. So, there is one edge from $j_m = 66^3$ to $j_l = 1728$. The other 2 edges emanating from $j = 66^3$ end at the root(s) of $Q(X)$ mod q.

Proof. With the above information at hand, we try to see whether the graph $\mathcal{G}(X_{2q}/\overline{\mathbb{F}_2})$ is disconnecting or not, for an arbitrary but fixed q. Notice that a graph is necessarily disconnecting if it has a vertex which is the end-point of just one edge. Can we use this obvious fact in our case? Well, we know that there are 3 edges emanating and going into each vertex. So this situation would be possible iff we can find an edge $j_r \longrightarrow j_s$ in $\mathcal{G}(X_{2q}/\overline{\mathbb{F}_2})$ which has three 2-isogenies associated to it which are all isomorphic. In particular, we will have $\Phi_2(X, j_r) = (X - j_s)^3 \pmod q$. We try to find some similar equation above and see that $\Phi_2(X, 0) = (X - 54000)^3 \pmod q$. If we will succeed in showing that the three 2-isogenies associated to the three edges $0 \longrightarrow 54000$ found by the above method in $G(X_{2q}/\overline{\mathbb{F}_2})$ are indeed isomorphic, then we will have proved that the graph $\mathcal{G}(X_{2q}/\overline{\mathbb{F}_2})$ is always disconnecting when it has a vertex corresponding to the j-value 0.

For a supersingular elliptic curve E corresponding to the j-value 0, we know that $\mathrm{End}(E)$ contains $\mathbb{Z}[\omega]$, with ω a primitive third root of unity. So, if $\Phi : E \longrightarrow E'$ is a 2-isogeny, then so are $\Phi \circ \omega$ and $\Phi \circ \omega^2$. Now, $\mathbb{Z}[\omega] \otimes \mathbb{F}_2 \simeq \mathbb{F}_4$ defines a subring of $\mathrm{End}(E[2]) \simeq M_2(\mathbb{F}_2)$ and ω has no nontrivial eigenspace in $E[2]$, so it acts without fixed point on $\mathbb{P}^1(E[2]) \simeq \mathbb{P}^1(\mathbb{F}_2)$. In other words, (E, Φ), $(E, \Phi \circ \omega)$ and $(E, \Phi \circ \omega^2)$ are *the* 2-isogenies emanating from E. Therefore, they are isomorphic and the three edges $0 \longrightarrow 54000$ are actually counted as 1 in $\mathcal{G}(X_{2q}/\overline{\mathbb{F}_2})$. Hence, $\mathcal{G}(X_{2q}/\overline{\mathbb{F}_2})$ is disconnecting whenever 0 occurs as j-value.

So let's see for which values of q, we get 0 as a j-value.
$\mathbb{Z}[\omega] = \mathbb{Z}[x]/(x^2 + x + 1)$,
$\Rightarrow \mathbb{Z}[\omega] \otimes \mathbb{F}_q \approx \mathbb{F}_q[x]/(x^2 + x + 1)$.
Now, $j = 0$ represents a class of supersingular elliptic curves in characteristic q.
$\Leftrightarrow q$ is inert or ramified in $\mathbb{Z}[\xi_3]$.
$\Leftrightarrow 3 \nmid (q - 1)$.
$\Leftrightarrow q \not\equiv 1 \pmod 3$.
So, whenever $q \not\equiv 1 (\mathrm{mod}\ 3)$, the graph $\mathcal{G}(X_{2q}/\overline{\mathbb{F}_2})$ is disconnecting. So, it is always disconnecting for $q \equiv -1 \pmod 3$and for $q \equiv 3$. By Dirichlet's theorem, we know that there are infinite number of 'q's such that $q \equiv -1 \pmod 3$. Hence, $\mathcal{G}(X_{2q}/\overline{\mathbb{F}_2})$ is disconnecting for infinite number of primes q.

■

Acknowledgements

I am grateful to Dr. Pierre Parent, who acted as my supervisor for this thesis, for useful discussions and helpful suggestions. I would like to thank Prof. Bas Edixhoven for agreeing to read my thesis and some of my friends for giving me tips on latexing. Also, I would like like to express my gratitude to the various authors whose names appear in the "Reference" section of my thesis and whose works and ideas I have used, in particular to K. A. Ribet, B. Edixhoven, Mestre, J.Oesterlé, P.Parent and A. Yafaev. These is a long list of people who helped me indirectly, but unfortunately it is not possible to give the complete list of these people due to space considerations.

Bibliography