INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps.

ProQuest Information and Learning
300 North Zeeb Road, Ann Arbor, MI 48106-1346 USA
800-521-0600

The Supersingular Locus of Hilbert Modular Surfaces modulo p

by

Marc-Hubert Nicole

Department of Mathematics

McGill University, Montréal

October 2000

A thesis submitted to the Faculty of Graduate Studies and Research
in partial fulfilment of the requirement for M.Sc. degree

Acknowledgments : The two main mathematical projects I tried working on with the best of my energies in the last year and a half have been the book "Lecture Notes on Hilbert Modular Varieties and Modular Forms", assisting Prof. Eyal Z. Goren, and this thesis. Accepting to study and work with Prof. Goren has clearly been the single most labor-inducing decision in my mathematical life. In spite of his occasional despotic surges, I thank him for the great opportunity, for its incredible availability, for his precise and intelligent answers to my often vague, ill-formulated questions, for abundantly sharing his insights and for his extensive editing of this thesis.

On the mathematical level, I would also like to thank my fellow students in number theory, especially Ignazio Longhi for many exchanges and dicussions, including a well-articulated introduction to rigid analytic geometry; and Lassina Dembele, for his enthusiasm and competence at discussing algebraic geometry.

I would also like to thank the organizers and participants of the 1998-1999 Theme Year in Number Theory and Arithmetic Geometry at the Centre de recherches mathématiques for such a challenging and thought-provoking year.

On a more personal tone, I would like to thank all those who made my life easier and sweeter and showed understanding for the numerous ways I made myself unavailable, that is, my family and friends.

On the financial & institutional level, first and foremost I thank the Conseil de recherche en sciences naturelles et génie du Canada (CRSNG) for its support of the two first years of my graduate studies with an ÉS-A scholarship. I thank also the people at the Centre inter-universitaire en calcul mathématique et algébrique (CICMA), especially for supporting my journey to the Park City Summer School in Arithmetic Geometry in July 1999, and for organizing the Québec-Vermont Number Theory Seminar. An authorship bursary from the Centre de recherches mathématiques supported me in the redaction of the above mentioned book. My participation to the latest Oortfest in arithmetic geometry has been made possible by Prof. Eyal Z. Goren and Utrecht Universiteit (Netherlands). Finally, I thank the staff at the department of mathematics, for their kind help.

Résumé :

Nous tentons de généraliser la description du lieu supersingulier de l'espace de modules des surfaces abéliennes polarisées à multiplications réelles par $\mathcal{O}_L$ ([1]) dans le cas où p est inerte dans $\mathcal{O}_L$. Nous présentons des faits probants pour étayer une formule de masse conjecturale pour les points superspéciaux, ainsi (par conséquent) qu'une formule pour le nombre de ces points, généralisant directement un résultat classique de Deuring pour le cas des courbes elliptiques supersingulières. Ce résultat fournirait une interprétation géométrique d'un cas particulier de la correspondance de Jacquet-Langlands. Le reste de la thèse constitue un travail préparatoire aux applications arithmétiques du lieu supersingulier des surfaces modulaires de Hilbert modulo p (p inerte) : formes modulaires de Hilbert, formes modulaires mod p, etc.

Abstract :

We try generalizing the description of the supersingular locus of the moduli space of polarized abelian surfaces with real multiplication by $\mathcal{O}_L$ (see [1]) in the case where p is inert in $\mathcal{O}_L$. We present evidence to support a conjectural mass formula for superspecial points and a counting formula for such points, generalizing a classical result of Deuring on supersingular elliptic curves. This result would provide a geometric interpretation of a special case of the Jacquet-Langlands correspondence. The remaining portion of the thesis is preliminary work with a view toward arithmetical applications of the supersingular locus of Hilbert modular surfaces mod p: Hilbert modular forms, modular forms mod p, etc.

Contents

Introduction 7

Chapter 1. Supersingular Elliptic Curves 9

1. Elliptic curves 9

1.1. Basic properties 9

1.2. Supersingularity 10

1.3. Moduli spaces 12

2. Theta series and modular forms of weight two 15

2.1. Quaternion algebras 15

2.2. Lattices and orders 17

2.3. Geometric interlude 21

2.4. Brandt matrices 25

Chapter 2. Hilbert Modular Surfaces 37

1. Abelian Schemes 37

1.1. Abelian schemes with real multiplication 38

2. Abelian varieties over a finite field 41

2.1. Serre-Tate theorem 43

3. Supersingular and superspecial points 44

3.1. Siegel modular varieties 46

3.2. Hilbert modular surfaces 50

3.3. Components of the supersingular locus 53

3.4. Local structure 53

4. Geometric view on Hecke operators and Brandt matrices 54

4.1. Geometric Brandt Matrices 61

Chapter 3. Structure and numerology of the supersingular locus 67

1. On certain quaternion algebras over $\mathbb{Q}(\sqrt{D})$ 67

1.1. A case study 67

1.2. Class number formula for Eichler orders 70

2. $\zeta_L(-1)$ as a volume of moduli space 72

3. Intersection theory 74

4. Moret-Bailly families with RM 76

4.1. Local picture 82

4.2. Counting points and components 82

Chapter 4. Tensor constructions 85

1. Axiomatics of tensor construction 85

2. Application to superspecial points 90

Chapter 5. Conclusion 93

Bibliography 97

Introduction

The purpose of this thesis is to review what is known about the supersingular locus of modular curves and Hilbert modular surfaces, with an eye to arithmetical applications. The first chapter covers supersingular elliptic curves, the arithmetic of quaternion algebras and the application to modular forms of weight two for $\Gamma_0(p)$. Chapter two studies the moduli spaces of polarized abelian surfaces with real multiplication and level structure, analyzes the supersingular locus of the moduli space mod p and gives a geometric view on Hecke operators, introducing higher-dimensional analogues of Brandt matrices. Chapter three explores evidence towards a class number formula for the number of superspecial points on Hilbert modular varieties mod p and proves various results on components of moduli spaces. Chapter four introduces a technical device (tensor construction) with the goal of systematizing the geometric applications of class number formulae of orders in quaternion algebras over (totally real) number fields to the moduli spaces of abelian varieties with additional structure. We use the conclusion, which is really an introït to greater endeavours, to draw an esquisse of various possible directions for further research; this thesis should therefore be considered as a step in work in progress.

CHAPTER 1

Supersingular Elliptic Curves

The purpose of this chapter is to review succinctly supersingularity of elliptic curves and its connection to the arithmetic of quaternion algebras.

1. Elliptic curves

Our main reference in this section will be [**39**]. The symbol E will always denote an elliptic curve, and we will use the letter p to denote a prime (i.e. a finite place).

1.1. Basic properties. Let us begin with a

DEFINITION 1.1. Let S be scheme. An elliptic curve E over S is a proper, smooth, commutative group scheme of relative dimension one

$$E \xrightarrow{f} S,$$

with geometrically connected fibers all of genus one. Let $s : S \longrightarrow E$ denote the identity section.

Locally in the Zariski topology, we obtain a generalized Weierstrass equation :

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6. \tag{1.1}$$

See [**39**, Section 2.2].

Let us consider the ring of endomorphisms $\mathrm{End}(E) = \mathrm{Hom}(E, E)$ of an elliptic curve defined over an algebraically closed field. It is equipped a positive quadratic degree map and the Rosati involution :

$$\mathrm{End}(E) \longrightarrow \mathrm{End}(E),$$

$$f \mapsto f^* := \lambda^{-1} f^\vee \lambda,$$

where $\lambda : P \mapsto [P] - [0]$ is the canonical principal polarization on E. In characteristic zero, $\mathrm{End}(E)$ is either $\mathbf{Z}$ or an order in an imaginary quadratic field ([**71**, Theorem

9.3, p.100]). We say that the curve E has *complex multiplication* if $\mathrm{End}(E) \neq \mathbf{Z}$. In characteristic p, we have the following

THEOREM 1.2. (Deuring) [17] *An elliptic curve E over a field of characteristic p has complex multiplication if and only if it is defined over a finite field $\mathbf{F}_{p^n}$.*

In this case, there are two possibilities for the endomorphism ring: either $\mathrm{End}(E)$ is an order of conductor prime to p in an imaginary quadratic extension of $\mathbf{Q}$; or $\mathrm{End}(E)$ is a maximal order in the rational definite quaternion algebra $B_{p,\infty}$ ramified at p ([17]).

1.2. Supersingularity. Let E be defined over an algebraically closed field k of characteristic p.

DEFINITION 1.3. An elliptic curve E is called *ordinary* if $E(k)$ has non-trivial points of order p, *supersingular* if not.

The curve E is supersingular precisely when the endomorphism ring $\mathrm{End}(E)$ is a maximal order in a quaternion algebra ([17]).

EXAMPLE 1.4. *The supersingular elliptic curve over $\overline{\mathbf{F}}_2$ ([29, p. 145]).*

The elliptic curve E over $\mathbf{F}_2$ with equation

$$Y^2 + Y = X^3, \tag{1.2}$$

is the unique supersingular curve over $\overline{\mathbf{F}}_2$. Its endomorphism ring has $\mathbf{Z}$-basis

$$\left\{i, j, k, \frac{1+i+j+k}{2}\right\},$$

which is a maximal order in the quaternion algebra $B_{2,\infty}$, that is, the Hamilton quaternion algebra : $\mathbf{Q} + \mathbf{Q}i + \mathbf{Q}j + \mathbf{Q}k$, with

$$i^2 = -1, j^2 = -1, ij = k = -ji.$$

The group $\mathrm{Aut}(E)$ has order 24 and is given by $\left\{\pm 1, \pm i, \pm j \pm k, \frac{\pm 1 \pm i \pm j \pm k}{2}\right\}$.

In the following, we will restrict our study to curves defined over finite fields. Recall that supersingular elliptic curves have models defined over $\mathbf{F}_{p^2}$, hence there is only a finite number of isomorphism classes of supersingular elliptic curves for each p; we shall give

a precise number later on in the moduli context. It is well-known that the supersingular elliptic curves form a unique isogeny class (this follows from Honda-Tate theorem).

DEFINITION 1.5. An abelian scheme A over a scheme S is a group scheme

$$\pi : A \longrightarrow S$$

such that π is smooth and proper, and the geometric fibers are connected.

Let A be an abelian variety over a field k of characteristic p. We denote the Frobenius map by $\mathrm{Fr} : A \longrightarrow A^{(p)}$. The dual morphism is the Verschiebung denoted $\mathrm{Ver} : A^{(p)} \longrightarrow A$. See [**39**, Chapter 12] . Those homomorphisms are "p-elementary" isogenies, that is :

$$\mathrm{Ver} \circ \mathrm{Fr} = [p]_A, \quad \mathrm{Fr} \circ \mathrm{Ver} = [p]_{A^{(p)}}, \tag{1.3}$$

and their kernels are group schemes of order $p^{\dim(A)}$.

There exists a canonical modular form in characteristic p of weight $p-1$ called the Hasse invariant. The vanishing of the Hasse invariant is a criterion for supersingularity. See [**39**, Section 12.4].

THEOREM 1.6. (Igusa) [**39**, Theorem 12.4.3, p.355] *The Hasse invariant has simple zeroes.*

Let us now scrutinize the p-torsion group scheme of elliptic curves. Let k be algebraically closed (of characteristic p).

The multiplication-by-n map $[n] : E \longrightarrow E$ is a proper, flat morphism and its kernel $E[n]$ is an affine group scheme of order n^2. The Weil pairing

$$E[n] \times E[n] \longrightarrow \mu_n,$$

shows that $E[n]$ is a self-dual group scheme; in particular, the largest étale quotient of $E[p]$ is of order $\leq p$. The only simple finite group schemes of order p that can occur in a decomposition series are :

- $\alpha_p = \mathrm{Spec}\Big(k[T]/(T^p)\Big)$; α_p is the kernel of the Frobenius map $\mathrm{Fr} : \mathbb{G}_a \longrightarrow \mathbb{G}_a$. It is a connected self-dual (local-local) group scheme.

- $\mu_p = \mathrm{Spec}\Big(k[T]/(T^p-1)\Big)$; μ_p is the kernel of the Frobenius map $\mathrm{Fr} : \mathbb{G}_m \longrightarrow \mathbb{G}_m$. It is a local-étale group scheme.
- $\mathbf{Z}/p\mathbf{Z} = \mathrm{Spec}\Big(k[T]/(T^p - T)\Big)$; $\mathbf{Z}/p\mathbf{Z}$ is the constant (étale-local) group scheme dual to μ_p.

Since $k = \bar{k}$, there are only two possibilities for $E[p]$:

- Suppose the étale part is of order p: this is the ordinary case. By self-duality

$$E[p] \cong \mu_p \oplus \mathbf{Z}/p\mathbf{Z}. \tag{1.4}$$

  Frobenius acts as zero on μ_p, and identity on $\mathbf{Z}/p\mathbf{Z}$; the Verschiebung acts as zero on $\mathbf{Z}/p\mathbf{Z}$, and identity on μ_p. Hence, the kernel of Frobenius is μ_p, and the kernel of Verschiebung is $\mathbf{Z}/p\mathbf{Z}$.
- Suppose now the étale part is trivial : this is the supersingular case. Since the kernel of Frobenius and Verschiebung is of order p and both act as 0 on α_p, the exact sequence :

$$0 \longrightarrow \alpha_p \longrightarrow E[p] \longrightarrow \alpha_p \longrightarrow 0. \tag{1.5}$$

  is non-split.

It follows that the p-divisible group of an ordinary elliptic curve over an algebraically closed field is

$$\mu_{p^\infty} \times \mathbb{Q}_p/\mathbf{Z}_p. \tag{1.6}$$

In the case of a supersingular elliptic curve, this p-divisible group is isomorphic to the unique 1-parameter formal Lie group of height 2. See [**39**, Theorem 2.9.3, p.93] and [**65**].

1.3. Moduli spaces. In this subsection, we consider the moduli spaces constructed when considering elliptic curves with level structure. The level structures are thrown in to rigidify the problem (i.e. eliminate automorphisms of the curves); in this thesis, we work with schemes rather than algebraic stacks and spaces, under the usual minor technical restriction on the level structure (i.e. $N \geq 3$).

We consider two kinds of level structures for elliptic curves E over a ring R : $\Gamma_0(N)$ and $\Gamma_1(N)$. In the latter case, we shall always assume that N is invertible in R. The general case is treated in [**39**].

DEFINITION 1.7.
- A $\Gamma_0(N)$-level structure is a choice of subgroup scheme $H \subset E[N]$ of order and exponent N defined over R.
- A $\Gamma_1(N)$-level structure is a choice of a point $P \in E[N]$ of exact order N defined over R.

The moduli problem consists in parametrizing elliptic curves with $\Gamma_0(N)$-level structure (resp. $\Gamma_1(N)$-level structure). One may prove that there exist coarse moduli schemes for these moduli problems, which are flat, regular curves over $\mathbf{Z}$ (resp. $\mathbf{Z}[\frac{1}{N}]$) : $Y_0(N)$ (resp. $Y_1(N)$). The terminology stems from the fact that $Y_0(N)(\mathbb{C}) \cong \Gamma_0(N)\backslash\mathcal{H}$, (resp. $Y_1(N)(\mathbb{C}) \cong \Gamma_1(N)\backslash\mathcal{H}$). If $N \geq 4$, $Y_1(N)$ is a fine moduli scheme. We obtain proper morphisms over $\mathbf{Z}$ (resp. $\mathbf{Z}[\frac{1}{N}]$) by adding the cusps, and to keep the moduli theoretic framework, we use the device of generalized elliptic curves (which are essentially cycles of projective lines with adjusted level structure). We then get a regular integral scheme $X_0(N)$ (resp. $X_1(N)$) that is flat and proper over $\mathbf{Z}$ (resp. $\mathbf{Z}[\frac{1}{N}]$), and this construction is still a "continuation" of the complex case (i.e. $X_0(N)(\mathbb{C}) \cong \Gamma_0(N)\backslash\mathcal{H}^*$, resp. $X_1(N)(\mathbb{C}) \cong \Gamma_1(N)\backslash\mathcal{H}^*$). See [**14**] for details, such as a discussion of generalized elliptic curves ("N-gons").

Having good models over $\mathbf{Z}$ (resp. $\mathrm{Spec}(\mathbf{Z}[\frac{1}{N}])$) allows us to consider the reduction mod p of the moduli schemes for any p (resp. p prime to N). The geometric picture is as follows : the reduction of $X_0(p)$ consists of two rational projective curves that intersect precisely at the supersingular points; the number of supersingular elliptic curves h is simply the genus of the intersection graph plus one:

$$h = g + 1. \tag{1.7}$$

We have the following formula for the genus of $X_0(p)$: if $p = 2$, $g = 0$ (since there is a unique supersingular elliptic curve in characteristic two), and otherwise

$$g = \frac{p+1}{12} - \frac{1+(\frac{-1}{p})}{4} - \frac{1+(\frac{-3}{p})}{3}. \tag{1.8}$$

See [32].

THEOREM 1.8. *([39, Corollary 12.4.6, p. 358]) We have the formula :*

$$\frac{p-1}{24} = \sum_{[E]} \frac{1}{|Aut(E)|}. \tag{1.9}$$

where summation is over isomorphism classes of supersingular elliptic curves.

EXAMPLE 1.9. *Supersingular elliptic curves over* $\overline{\mathbf{F}}_{11}$.

There are two supersingular elliptic curves over $\overline{\mathbf{F}}_{11}$, and representatives are given by :

$$E_1 : y^2 = x^3 + 1, \quad E_2 : y^2 = x^3 + x. \tag{1.10}$$

We check that

$$\mathbf{Z}[i] \subset \mathrm{End}(E_2), \quad \mathbf{Z}[\omega] \subset \mathrm{End}(E_1),$$

where ω is a primitive cube root of unity: $\omega^2 + \omega + 1 = 0$. The automorphism group of $E_2 : y^2 = x^3 + x$ thus contains $\mathbf{Z}[i]^\times = \{\pm 1, \pm i\}$; likewise, $\mathbf{Z}[\omega]^\times = \{\pm 1, \pm\omega, \pm\omega^2\} \subset \mathrm{Aut}(E_1)$. The mass formula indicates we don't have to look any further, since $\frac{5}{12} = \frac{1}{4} + \frac{1}{6}$.

N.B. We find in [57] algorithms to compute the orders of endomorphisms associated to supersingular elliptic curves, representatives of the left ideal classes, associated norm forms, etc.

In fact, this is a feature of this connection between supersingular elliptic curves and quaternion algebras: the computational aspect of the latter is sometimes more manageable. Note though, that in [44], supersingular curves are used to compute ideal classes in quaternion algebras.

For example, the maximal order $\mathcal{O}$ associated to E_2 is given by the $\mathbf{Z}$-basis :

$$\left\{\frac{1}{2}(1+j), \frac{1}{2}(i+k), j, k\right\},$$

in the quaternion algebra $B_{11,\infty}$ over $\mathbf{Q}$ given by the relations :

$$i^2 = -1, j^2 = -11, ij = k = -ji.$$

One checks that the only units in this order are ± 1 and $\pm i$, as expected.

2. Theta series and modular forms of weight two

2.1. Quaternion algebras. We recall the main ingredients of the theory of quaternion algebras and their orders, that we apply soon after to Eichler's theorem on the space of weight two modular forms, and later on (in Chapter III) to totally ramified quaternion algebras.

DEFINITION 2.1. A *quaternion algebra* H is a central simple algebra of dimension four over a field K. If char $K \neq 2$, we can pick $(a,b) \in K^2$ nonzero such that H is isomorphic to

$$K \oplus Ki \oplus Kj \oplus Kij,$$

with relations

$$i^2 = a, \quad j^2 = b, \quad ij = -ji.$$

We usually denote ij by k.

A quaternion algebra is equipped with a conjugation $x \mapsto \overline{x}$, a (reduced) trace Tr and a (reduced) Norm with the usual properties :

For char $k \neq 2$, an element u in a quaternion algebra H can be expressed as

$$u = x + yi + zj + wk.$$

Then

- $\overline{u} = x - yi - zj - wk, \quad x,y,z,w \in K$;
- $\mathrm{Tr}(u) = 2x$;
- $\mathrm{Norm}(u) = x^2 - ay^2 - bz^2 + abw^2$.

Note that the (reduced) norm is a quadratic form on H viewed as a K-vector space.

EXAMPLE 2.2. If u is an element of the maximal order corresponding to the ring of endomorphisms of the supersingular elliptic curve, note that its norm is equal to its degree as an endomorphism, because the norm coincides with the degree map.

- $p = 2$. Let $u = x + yi + zj + wk$ be an element. Then its norm is

$$\mathrm{Norm}(u) = x^2 + y^2 + z^2 + w^2,$$

and we check that the elements in Example 1.4 are automorphisms of the supersingular elliptic curve over $\overline{\mathbf{F}}_2$.

- $p = 11$. The norm is :

$$\mathrm{Norm}(u) = x^2 + y^2 + 11z^2 + 11w^2;$$

and the elements $\pm 1, \pm i$ are the units in the order $\mathcal{O}$ of Example 1.9.

A place v of a global field K is said to be *ramified* if

$$H_v = H \otimes K_v,$$

is a division algebra. Let S be the set of ramified places. For $v \notin S$, we have

$$H \otimes K_v \cong M_2(K_v),$$

by Wedderburn's theorem.

We have the following classification:

THEOREM 2.3. (Classification) [**76**, Théorème 3.1]

- *The number of ramified places of a quaternion algebra H over K is finite and even.*
- *For every finite set S of places of K of even order, there exists a quaternion algebra H over K, unique up to isomorphism, such that H is ramified at precisely the places in S.*

EXAMPLE 2.4. Take $S = \{p, \infty\}$. The corresponding quaternion algebra ramified at p and ∞ will be denoted $B_{p,\infty}$. Explicitly, $B_{p,\infty} \otimes \mathbb{Q}_p$ and $B_{p,\infty} \otimes \mathbb{R} \cong \mathbb{H}$ are (central) division algebras, and

$$B_{p,\infty} \otimes \mathbb{Q}_q \cong M_2(\mathbb{Q}_q), \quad \forall q \neq p, \infty.$$

THEOREM 2.5. *([**76**, Chapitre III, Théorème 3.8])*

A quadratic extension L of K can be embedded in a quaternion algebra H over K if and only if $L_p := L \otimes K_p$ is a field for all p ramified in H (i.e. there is no prime ramified in H that is split in L).

THEOREM 2.6. *Let H be a quaternion algebra over $\mathbb{Q}$, let $\infty \neq p$ be a rational prime, and let e_p be the ramification index of p in H ($e_p = 1$ if p is split, and $e_p = 2$ if p is ramified).*

1. *If H_p is a division algebra over $\mathbb{Q}_p$, there there is a unique maximal order*
$$\mathcal{O}_p = \{\alpha \in H_p : \mathrm{Norm}(\alpha) \in \mathbf{Z}_p\}.$$
2. *If H_p is isomorphic to $M_2(\mathbb{Q}_p)$, then all maximal orders are conjugate to $M_2(\mathbf{Z}_p)$ under this isomorphism.*
3. *A maximal order $\mathcal{O}_p$ of H_p has a unique maximal two-sided ideal $\mathfrak{B}$. Every two-sided ideal of $\mathcal{O}_p$ is of the form $\mathfrak{B}^m$ for an integer m, and $\mathfrak{B}^{e_p} = (p)$.*

See [**62**, Theorem 12.8] for item 1, and [**62**, Theorem 17.3] for items 2 and 3.
We will use the following classical theorem a few times. Recall that the inner automorphisms of a quaternion algebra H are given by :
$$k \mapsto hkh^{-1}, \quad k \in H,$$
and $h \in H^\times$.

THEOREM 2.7. (Skolem-Noether) [**33**] *Let H/K be a quaternion algebra. Let L, L' be two (commutative) K-algebras contained in H. All K-isomorphisms from L to L' can be continued to an inner automorphism of H, and all K-automorphisms of H are inner.*

2.2. Lattices and orders. Let K be the quotient field of a Dedekind domain R. Let H be a quaternion algebra over K. A *lattice* is a finitely generated R-module contained in H. We can define the localization of a lattice $\mathfrak{L}$ of K at a place v as
$$\mathfrak{L}_v := \mathfrak{L} \otimes_R R_v.$$
An *ideal* I of H is a complete lattice, i.e. $K \otimes_R I \cong H$. An ideal $\mathcal{O}$ is called an *order* if it is a ring (with identity). By a standard application of Zorn's lemma, there exist maximal orders.

Let $\mathcal{O}$ be a fixed maximal order of a quaternion algebra H. A left ideal of $\mathcal{O}$ is a lattice in H which is stable under left multiplication by $\mathcal{O}$. To any ideal I we can

associate its *left order*

$$\mathcal{O}_l := \{h \in H : hI \subset I\};$$

similarly for a right order $\mathcal{O}_r$. We define the inverse I^{-1} of an ideal I to be :

$$I^{-1} = \{h \in H : IhI \subset I\}.$$

It is a right ideal for $\mathcal{O}$ whose left order is the right order of I.

Recall that the norm of an ideal is the fractional ideal of R generated by the (reduced) norms of its elements. As in the algebraic theory of Dedekind domains, the different of an order $\mathcal{O}$ is the ideal inverse of the dual lattice of $\mathcal{O}$ with respect to the bilinear form induced by the (reduced) trace.

DEFINITION 2.8. The *(reduced) discriminant* $d(\mathcal{O})$ of $\mathcal{O}$ is the norm of the different.

We have a practical criterion to check maximality of orders :

PROPOSITION 2.9.
- *Let $\mathcal{O}$ and $\mathcal{O}'$ be two orders such that $\mathcal{O} \subseteq \mathcal{O}'$. Then $d(\mathcal{O}')$ divides $d(\mathcal{O})$ and $d(\mathcal{O}) = d(\mathcal{O}') \iff \mathcal{O} = \mathcal{O}'$.*
- *An order is maximal iff $d(\mathcal{O})$ is equal to the product of the finite, ramified places of K.*
- *If $\mathcal{O} = \sum_{i=1}^{4} Rx_i$, then*

$$d(\mathcal{O})^2 = R \cdot \det(\mathrm{Tr}(x_i\overline{x_j}))_{1 \le i,j \le 4}.$$

See [**57**, Proposition 1.1], [**76**, Corollaire 5.4] and [**76**, Lemme 4.7, p. 24].

EXAMPLE 2.10. One can easily calculate the discriminants of the maximal orders associated to the supersingular elliptic curves when $p = 2$ and $p = 11$, to obtain that $d(\mathcal{O}_2) = 2$ and $d(\mathcal{O}_{11}) = 11$.

We collect a few facts about projective left ideals of maximal orders.

PROPOSITION 2.11. *([**62**, Theorem 17.3]) Let $\mathcal{O}$ be a maximal order. Then every left ideal of $\mathcal{O}_v$ is principal at all finite places v. A left ideal I of $\mathcal{O}$ is projective if and only if it is locally free at all finite places v.*

PROPOSITION 2.12. *([42, Proposition 40]) Let I be a projective left ideal for a maximal order $\mathcal{O}$. Then the right order $\mathcal{O}'$ of I is also maximal. Moreover, the left order of I (as an ideal of $\mathcal{O}'$) is $\mathcal{O}$.*

DEFINITION 2.13. An *Eichler* order is the intersection of two maximal orders.

Fix a prime number p. Let M and r to be integers, with $(M,p) = 1$, and put $N := p^{2r+1}M$. Let $\tilde{L}$ be the unique unramified quadratic field extension of $\mathbb{Q}_p$, and $\mathcal{O}_{\tilde{L}}$ be the ring of integers of $\tilde{L}$. We denote the conjugation of $\tilde{L}/\mathbb{Q}_p$ by σ.

An order $\mathcal{O}$ of $B_{p,\infty}$ is said to be of level N if, for every q prime, we have

$$\mathcal{O}_q := \mathcal{O} \otimes_{\mathbf{Z}} \mathbf{Z}_q = \text{ is conjugate to } \begin{cases} \begin{pmatrix} \mathbf{Z}_q & \mathbf{Z}_q \\ N\mathbf{Z}_q & \mathbf{Z}_q \end{pmatrix} & \text{if } q \neq p; \\ \left\{ \begin{pmatrix} \alpha & p^r\beta \\ p^{r+1}\beta^\sigma & \alpha^\sigma \end{pmatrix} | \alpha, \beta \in \mathcal{O}_{\tilde{L}} \right\} & \text{if } q = p. \end{cases}$$

The maximal orders form a tree : Let $\mathcal{O}_1$, $\mathcal{O}_2$ be two maximal orders. Define the distance $dist(\mathcal{O}_1, \mathcal{O}_2)$ to be the level of the Eichler order $\mathcal{O}_1 \cap \mathcal{O}_2$. If we put the Eichler orders as vertices, and we connect with an edge vertices $\mathcal{O}_1$, $\mathcal{O}_2$ such that $dist(\mathcal{O}_1, \mathcal{O}_2) = 1$, we obtain a *tree*. See [76, Corollaire 2.6].

We will need the following proposition in Chapter III.

PROPOSITION 2.14. (Hijikata) *Let K be a local field with uniformizer π and ring of integers R. Let $\mathcal{O}$ be an order of $M_2(K)$. The following are equivalent :*

- *The order $\mathcal{O}$ is Eichler;*
- *There exists a unique pair of maximal orders $\mathcal{O}_1$, $\mathcal{O}_2$ such that $\mathcal{O} = \mathcal{O}_1 \cap \mathcal{O}_2$;*
- *There exists an unique integer $n \in \mathbf{N}$ such that $\mathcal{O}$ is conjugate to $\begin{pmatrix} R & R \\ \pi^n & R \end{pmatrix}$;*
- *The order $\mathcal{O}$ contains a subring conjugate to $\begin{pmatrix} R & 0 \\ 0 & R \end{pmatrix}$.*

We will now introduce the class and type numbers.

Two left $\mathcal{O}$-ideals I and J are in the same class if there exists an element $h \in H^\times$ such that $I = Jh$.

PROPOSITION 2.15. *The number of classes of H is finite. For any maximal order $\mathcal{O}$, the number of classes of left ideals is equal to the number of classes of right ideals and is independent of the maximal order of H.*

PROPOSITION 2.16. *([76]) The class number formula for $B_{p,\infty}$*

$$h = \frac{p-1}{12} + \frac{1}{3}\Big(1 - (\frac{-3}{p})\Big) + \frac{1}{4}\Big(1 - (\frac{-1}{p})\Big) \quad \text{when } p > 2, \tag{2.1}$$

where $(\frac{a}{b})$ is the Legendre symbol, and is 1 for $p = 2$.

One will immediately note the equality between this class number and the number of supersingular elliptic curves in characteristic p ! We will come back to this and give an explicit bijection in section 2.3.

There exist a class number formula generalizing Equation (2.1) for any order of level $p^{2r+1}N$, $(N,p) = 1$; in particular, it depends only on the level, and not the specific order. See [**57**, Theorem 1.12, p. 346].

The formula is as follows :

$$H(p^{2r+1}N) = \frac{p^{2r+1}N}{12}(1 - \frac{1}{p})\prod_{\ell|N}(1 + \frac{1}{\ell})$$

$$+ \begin{cases} \frac{1}{4}(1 - (\frac{-4}{p}))\prod_{\ell|N}(1 + (\frac{-4}{\ell})) & \text{if } 4 \nmid N \\ 0 \text{ otherwise} \end{cases}$$

$$+ \begin{cases} \frac{1}{3}(1 - (\frac{-3}{p}))\prod_{\ell|N}(1 + (\frac{-3}{\ell})) & \text{if } 9 \nmid N \\ 0 \quad \text{otherwise} \end{cases}$$

Moreover, (see [**59**]) there are similar formulae for orders of level p^2N :

$$H(p^2N) = \frac{p^2N}{12}(1 - \frac{1}{p^2})\prod_{\ell|N}(1 + \frac{1}{\ell}) + \begin{cases} 0 \text{ if } p \geq 5 \\ \frac{4}{3}\prod_{\ell|N}(1 + (\frac{-3}{\ell})) \text{ if } p = 3 \end{cases}$$

See [**4**], [**5**] for recent developments.

Let $\{I_1, \ldots I_h\}$ be a set of left ideals representing the distinct ideal classes, with $I_1 = \mathcal{O}$; and let $\{\mathcal{O}_1, \ldots \mathcal{O}_h\}$ be the set of right orders of the I_i's. Then each conjugacy class of maximal orders in H is represented (at least once, maybe twice) in this set. We call

the number of distinct conjugacy classes the type number t. See [**42**, Proposition 38, Corollary 39].

COROLLARY 2.17. *The type number t is finite.*

For a more precise statement, see [**42**, Theorem 44].

The following proposition is useful to reduce calculations to local considerations. For example, the following properties can be checked locally : being an order, an Eichler order, a maximal order, an ideal, etc.

PROPOSITION 2.18. *Let X be a lattice in H. Let S be the set of infinite places. There is a bijection between the H-lattices Y and the set of lattices*

$$\{(Y_\mathfrak{p}), Y_\mathfrak{p} \text{ a lattice in } H_\mathfrak{p}, Y_\mathfrak{p} = X_\mathfrak{p} \text{ almost everywhere }\},$$

given by the invertible maps :

$$Y \mapsto (Y_\mathfrak{p})_{\mathfrak{p} \notin S},$$

$$(Y_\mathfrak{p})_{\mathfrak{p} \notin S} \mapsto Y = \{x \in H, x \in Y_\mathfrak{p}, \forall \mathfrak{p} \notin S\}.$$

See [**76**, Proposition 5.1, p. 83] .

2.3. Geometric interlude. Warning: in this subsection, we use R to denote any ring.

We explain in detail the construction of a bijection between the set of supersingular elliptic curves $\{E_1, \ldots, E_h\}$ and the class group of $\mathcal{O} = \mathrm{End}(E_1)$, a maximal order in the quaternion algebra $B_{p,\infty}$. Let $E = E_1$.

The original idea we will use to prove this is due to Serre ([**66**]), with refinements due to Waterhouse ([**79**]).

We give the original results, due to Deuring ([**17**]) and Eichler ([**19**]) (see also [**24**]):

- Let $\mathfrak{A}$ be a left ideal of $\mathcal{O} \subset B_{p,\infty}$, and consider the finite group scheme

$$H(\mathfrak{A}) := \cap \ker(\mathfrak{a}) \subset E,$$

where $\mathfrak{a}$ runs through $\mathfrak{A}$. The quotient $E(\mathfrak{A}) = E/H(\mathfrak{A})$ is a supersingular elliptic curve and $\mathfrak{B} \mapsto E(\mathfrak{B})$ defines a bijection between the set of left ideal classes of $\mathcal{O}$ and the set S of isomorphism classes of supersingular elliptic curves over $\overline{\mathbf{F}_p}$.

- The right order $\mathcal{O}_r(\mathfrak{B})$ is isomorphic to $\mathrm{End}(E(\mathfrak{B}))$.
- The orders $\mathcal{O}_r(\mathfrak{B})$ and $\mathcal{O}_r(\mathfrak{B}')$ are isomorphic iff $E(\mathfrak{B})$ and $E(\mathfrak{B}')$ denote classes in S that are conjugate under the Galois group $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$.
- As a corollary of Skolem-Noether theorem, isomorphic orders are conjugate in $B_{p,\infty}$. Moreover, elements of S are defined over $\mathbb{F}_{p^2}$, hence the types of $B_{p,\infty}$ correspond to orbits in S under the Galois action of $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$.

THEOREM 2.19. *Let S be the category of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ (with isogenies) and let E be an object in S. Let T be the category of locally free rank one left modules over $\mathcal{O} = \mathrm{End}(E)$ (with $\mathcal{O}$-homomorphisms). Then the functor:*

$$F : \mathfrak{A} \mapsto E/H(\mathfrak{A}),$$

from the category of locally free rank one left modules over $\mathcal{O} = \mathrm{End}(E)$ (with $\mathcal{O}$-homomorphisms) is an (anti-)equivalence of categories. More precisely, it yields:

$$\mathrm{Hom}_{\mathcal{O}}(\mathfrak{A}, \mathfrak{B}) \cong \mathrm{Hom}_S(E/H(\mathfrak{B}), E/H(\mathfrak{A})) = \mathfrak{A}^{-1}\mathfrak{B}.$$

DEFINITION 2.20. Let J be a set of isogenies of E. We define $H[J]$ to be the (scheme theoretic) intersection of the kernels of all α in J. A left $\mathcal{O}$-ideal $\mathfrak{A}$ is called a *kernel ideal if* $\mathfrak{A} = \{\alpha \in \mathcal{O} | \alpha(H[\mathfrak{A}]) = 0\}$.

THEOREM 2.21. *Every left $\mathcal{O}$-ideal is a kernel ideal, and every finite subgroup of E is of the form $H[\mathfrak{A}]$ for some left $\mathcal{O}$-ideal $\mathfrak{A}$.*

PROOF. See [**79**, Theorem 3.15, p. 35]. □

LEMMA 2.22. *([**42**, Lemma 47, p. 68]) Let $\phi : E \longrightarrow E'$ and $\psi : E \longrightarrow E''$ be isogenies and suppose that $\psi \ker(\phi) = O_{E''}$. Then there exists an isogeny $\lambda : E'' \longrightarrow E'$ such that $\psi = \lambda\phi$.*

LEMMA 2.23. *([**42**, Proposition 48]) Let $I \subset \mathrm{Hom}(E', E)$ be a left module over $\mathcal{O} = \mathrm{End}(E)$. Then there exists an elliptic curve E'' and an isogeny $\rho : E'' \longrightarrow E$ such that $I = \mathrm{Hom}(E'', E)\rho$.*

PROOF. Taking an isogeny $\phi : E \longrightarrow E'$, we embed I and $\mathrm{Hom}(E', E)$ in $\mathcal{O}$ as integral ideals such that :

$$I\phi \subset \mathrm{Hom}(E', E)\phi \subset \mathcal{O}.$$

Let $E'' = E/H[I\phi]$ for some ϕ and let $\psi : E \longrightarrow E''$ be the isogeny with kernel $H[I\rho]$. By Theorem 2.21 and Lemma 2.22, $I\phi = \{\alpha \in \mathcal{O} : \alpha(H[I\phi]) = O_E\} = \mathrm{Hom}(E'', E_\psi)$, so $I = \mathrm{Hom}(E'', E)\rho$. □

We now proceed : we need to demontrate that F is full, faithfull and generically surjective.

PROOF. • **Faithful.** First, let us quote a lemma:

LEMMA 2.24. *([79, Theorem 3.11]) Let $\mathfrak{A}$ and $\mathfrak{B}$ be kernel ideals. Then*

$$E/H(\mathfrak{A}) \cong E/H(\mathfrak{B}) \iff [\mathfrak{A}] = [\mathfrak{B}],$$

i.e. $\mathfrak{A} = \nu\mathfrak{B}$ for some invertible $\nu \in \mathcal{O}$.

Since every left $\mathcal{O}$-ideal is a kernel ideal, it follows from the lemma that F is faithful.

- **Generically surjective.** Since we know that both sides have the same cardinality of isomorphism classes, and that the functor F is faithful, it follows at once that F is generically surjective.
- **Full.** We know that any supersingular elliptic curve can be written in the form $E/H(\mathfrak{A})$ for some representative $\mathfrak{A}$ of a left ideal class. In Lemma 2.23, take $I := \mathrm{Hom}_S(E/H(\mathfrak{A}), E), E' := E/H(\mathfrak{A})$. From the proof of the lemma, we see that $E'' = E/H[I\phi]$, and thus $I \cong \mathrm{Hom}(E/H[I], E)$, and by faithfulness, letting $\mathfrak{A}$ vary yields all left ideal classes. Similarly, we show that $J^{-1} \cong \mathrm{Hom}(E, E/H[J])$. It follows that

$$\mathrm{Hom}_{\mathcal{O}}(\mathfrak{A}, \mathfrak{B}) \cong (\mathrm{Hom}_S(E/H(\mathfrak{B}), E/H(\mathfrak{A})) \cong \mathfrak{A}^{-1}\mathfrak{B}.$$

Let us compute explicitly the left and right orders of the left $\mathcal{O}$-ideal

$$\mathfrak{A}_i \cong \mathrm{Hom}_S(E/H(\mathfrak{A}_i), E),$$

for $\{\mathfrak{A}_i\}$ a set of representatives of left ideal classes of $\mathcal{O}$.

We have

$$\begin{aligned}\mathcal{O}_\ell(\mathfrak{A}_i) &= \{x \in B_{p,\infty} |\ x\mathfrak{A}_i \subseteq \mathfrak{A}_i\} \\ &= \{x \in B_{p,\infty} |\ x \circ \phi \in \mathfrak{A}_i, \forall \phi \in \mathfrak{A}_i\} \\ &\cong \{x \in \mathbf{Iso}(E,E) |\ x : E \longrightarrow E, x \text{ homomorphism}\} \\ &= \mathrm{End}(E) \\ &= \mathcal{O}\end{aligned}$$

Similarly, we show that $\mathcal{O}_r(\mathfrak{A}_i) \cong \mathrm{End}(E/H(\mathfrak{A}))$.

□

In his Ph.D. thesis ([**42**]), Kohel gives a version of the above correspondence valid over finite fields.

Let $\mathbb{F}_q$ be a finite field of q elements in characteristic p, and let $\mathcal{O} \cong \mathrm{End}(E_0)$ be a maximal order in $B_{p,\infty}$ containing an element of reduced norm q, for E_0 a fixed supersingular elliptic curve defined over $\mathbb{F}_q$.

- Let $\mathcal{S}_{\mathbb{F}_q}$ be the category of supersingular elliptic curves over $\mathbb{F}_q$. The objects of $\mathcal{S}_{\mathbb{F}_q}$ are defined to be pairs (E, π), where E is a supersingular elliptic curve over $\mathbb{F}_q$ and π is the Frobenius endomorphism relative to $\mathbb{F}_q$. A morphism of objects (E_1, π_1) to (E_2, π_2) is defined to be a homomorphism $\psi : E_1 \longrightarrow E_2$ such that $\psi \circ \pi_1 = \pi_2 \circ \psi$.

  DEFINITION 2.25. *Reduced norm*

  Let $\phi : I \longrightarrow J$ be a homomorphism of right modules, I, J projective over $\mathcal{O}$ of rank one.

  Since I, J are locally free, for each prime ℓ there exists $x_\ell \in I_\ell$ and $y_\ell \in J_\ell$ such that $I_\ell = x_\ell \mathcal{O}_\ell$ and $J_\ell = y_\ell \mathcal{O}_\ell$. The image of x_ℓ under $\phi \otimes 1_{\mathbb{Z}_\ell}$ is $y_\ell \alpha_\ell$ for some $\alpha_\ell \in \mathcal{O}_\ell$. We define the *reduced norm of* ϕ to be the product :

  $$N(\phi) = \prod_\ell |\mathbb{Z}_\ell / \mathrm{Norm}(\alpha_\ell)\mathbb{Z}_\ell|.$$

- Let $\mathcal{M}_{\mathcal{O},q}$ be the category of projective right modules of rank one over $\mathcal{O}$. The objects of $\mathcal{M}_{\mathcal{O},q}$ are defined to be pairs (I, ϕ) such that I is a projective right

module of rank one over $\mathcal{O}$ and ϕ is an endomorphism of I of reduced norm q. A morphism of objects (I_1, ϕ_1) and (I_2, ϕ_2) is defined to be a homomorphism $\psi : I_1 \longrightarrow I_2$ such that $\psi \circ \phi_1 = \phi_2 \circ \psi$.

- The functor $I : \mathcal{S}_{\mathbf{F}_q} \longrightarrow \mathcal{M}_{\mathcal{O},q}$ is defined as follows :

$$I : \mathcal{S}_{\mathbf{F}_q} \longrightarrow \mathcal{M}_{\mathcal{O},q}$$

$$(E, \pi) \mapsto (I(E), I(\pi))$$

where $I(E) = \mathrm{Hom}(E_0, E)$ and $I(\pi) = \tau_\pi$ is the homomorphism of $\mathrm{Hom}(E_0, E)$ to itself given by left composition by π. For any morphism ψ of objects (E_1, π_1) to (E_2, π_2) there is a well-defined morphism $I(\psi) = \tau_\psi$ which is the right $\mathcal{O}$-module homomorphism :

$$\tau_\psi : \mathrm{Hom}(E_0, E_1) \longrightarrow \mathrm{Hom}(E_0, E_2)$$

given by left composition by ψ, which satisfies the condition that

$$\tau_\psi \circ \tau_{\pi_1} = \tau_{\pi_1} \circ \tau_\psi.$$

THEOREM 2.26. *([42, Theorem 45, p.67]) The functor I is an equivalence of categories.*

2.4. Brandt matrices. The Brandt matrices give a representation of the Hecke algebra in a space of theta series coming from a quaternion algebra; in fact, Brandt matrices and Hecke operators generate isomorphic semi-simple rings with the same traces. The comparison of the corresponding trace formulae is the main tool to solve the basis problem, that is finding an arithmetically significant generating set for the space of all modular forms of weight k with respect to the group $\Gamma_0(N)$ for some N. We will define Brandt matrices only for $N = p$ a prime number, and apply this to the weight 2 case.

Let $E_1, \ldots E_h$ be representatives for the isomorphism classes of supersingular elliptic curves in characteristic p. Thus $\mathrm{End}(E_i) \cong R_i$ is a maximal order in $B_{p,\infty}$.

DEFINITION 2.27. Let $\mathcal{O} = R_1$ and let $I_1, \ldots, I_h$ be representatives of classes of left ideals, so that the right order of I_i is R_i (and $\mathrm{End}(E_i) \cong R_i$); put $e_i = |R_i^\times|$. The

product $I_j^{-1}I_i$ is a left ideal of R_j. Consider its norm $\mathrm{Norm}(I_j^{-1}I_i)$; there exists a unique positive rational number c such that $(c) = \mathrm{Norm}(I_j^{-1}I_i)$ as fractional ideals. Note that this number is such that $\frac{\mathrm{Norm}(b)}{c}$, where $b \in I_j^{-1}I_i$, are all integers with no common factor. We define the (i,j)-entry of the Brandt matrix $B(m)$ to be :

$$B_{ij}(m) = \frac{\left|\left\{b \in I_j^{-1}I_i | \frac{\mathrm{Norm}(b)}{\mathrm{Norm}(I_j^{-1}I_i)} = m\right\}\right|}{e_j}.$$

Let M_p be the free abelian group on the set $S = \{E_1, \ldots E_h\}$ of supersingular points of $X_0(1)$ in characteristic p, denoted $\mathbf{Z}[S]$.

DEFINITION 2.28. *Hecke operators.* Let $m \in \mathbf{N}$ such that $(m,p) = 1$.

The Hecke operator T_m is the linear map $T_m : M_p \longrightarrow M_p$ determined uniquely by

$$E \mapsto T_m(E) = \sum_C E/C,$$

where C ranges over all subgroups E of order m.

For $m = \prod_i p_i^{a_i}$, we have the decomposition :

$$T_m = \prod_i T_{p_i^{a_i}}.$$

PROPOSITION 2.29. *For ℓ relatively prime to the characteristic of $\overline{k}$, the following relation holds :*

$$T_{\ell^2} + \ell = T_\ell^2.$$

PROOF. Recall that for $\ell \neq p$, $E[\ell] \cong_{\overline{k}} (\mathbf{Z}/\ell\mathbf{Z})^2$. Consider first the modified Hecke operator

$$T_{\ell^2}^{cyc} := \sum_C E/C, \quad |C| = \ell^2, C \text{ cyclic}.$$

Under these conditions, $C \cong \mathbf{Z}/\ell^2\mathbf{Z}$, and this fits uniquely into the exact sequence :

$$0 \longrightarrow \mathbf{Z}/\ell\mathbf{Z} \xrightarrow{\times \ell} \mathbf{Z}/\ell^2\mathbf{Z} \longrightarrow \mathbf{Z}/\ell\mathbf{Z} \longrightarrow 0.$$

Thus, abusing a bit the terminology, the support of $T_{\ell^2}^{cyc}$ is the same as the support of $(T_\ell^2)^{cyc}$. What about non-cyclic subgroups ? Let

$$T_{\ell^2}^{nc} := \sum_C E/C, \quad |C| = \ell^2, C \text{ non cyclic ;}$$

of course, $T_{\ell^2}^{nc} = id$. For $H_1 < E$ of order l, we want to calculate how many $H_2 < E/H_1$ there are such that :

$$E \longrightarrow E/H_1 \longrightarrow (E/H_1)/H_2 \cong E/E[l].$$

By cardinality, there is only one such H_2, that is : $H_2 = E[l]/H_1$. Let us calculate the number of embeddings : $\mathbf{Z}/\ell\mathbf{Z} \hookrightarrow \mathbf{Z}/\ell\mathbf{Z} \oplus \mathbf{Z}/\ell\mathbf{Z}$.

This is geometrically the number of points in $\mathbb{P}^1_{\mathbf{F}_\ell}$, that is : $(\ell^2+1)/(\ell-1) = \ell+1$. Thus, there is only one element in the support of $T_{\ell^2}^{nc}$, and it appears with multiplicity $\ell+1$; this implies that :

$$T_\ell^2 - T_{\ell^2}^{cyc} = \ell + 1.$$

Trivially,

$$T_{\ell^2}^{cyc} + T_{\ell^2}^{nc} = T_{\ell^2},$$

hence

$$T_{\ell^2}^{cyc} + id = T_{\ell^2}.$$

Gathering all formulae, we obtain :

$$T_\ell^2 = T_{\ell^2} + \ell.$$

□

More generally, we have :

PROPOSITION 2.30. *For $\ell \neq p$, we have :*

$$T_\ell \circ T_{\ell^r} = T_{\ell^{r+1}} + \ell \cdot T_{\ell^{r-1}}.$$

PROPOSITION 2.31. *The entry $B_{ij}(m)$ is equal to the number of subgroup schemes C of order m in E_i such that $E_i/C \cong E_j$.*

PROOF. We have an isomorphism

$$I_j^{-1} I_i \cong \mathrm{Hom}(E_i, E_j)$$

as a left R_i and right R_j-module. The degree of an isogeny ϕ_b corresponding to a non-zero element $b \in I_j^{-1} I_i$ is given by $\deg \phi_b = \mathrm{Norm}(b) \cdot \frac{\mathrm{Norm}(I_i)}{\mathrm{Norm}(I_j)}$. So $B_{ij}(m)$ is the number of equivalence classes of isogenies $\phi : E_i \longrightarrow E_j$ of order m, identifying isogenies differing by an an automorphism $\psi \in Aut(E_j) = R_j^\times$, so that two isogenies with the same kernel are identified, hence the result. □

COROLLARY 2.32. *The curves E_i and E_j are conjugate by an automorphism of $\overline{\mathbb{F}}_p$ iff $i = j$ or $B_{ij}(p) = 1$.*

Consider the order $\mathcal{O}$ of (reduced) discriminant d and rank 2 over $\mathbf{Z}$. Let $h(d)$ be the order of the class group, and $u(d)$ the order of the finite group $\mathcal{O}^* / \{\pm 1\}$. If $d > 0$, let $h(d)$ be the class number of binary quadratic forms of discriminant d, and let $u(d) = 1$ unless $d = -3, -4$ when $u(d) = 3, 2$ (respectively). For $D > 0$, we define, following Hurwitz and Gross :

$$H(D) = \sum_{df^2 = -D} \frac{h(d)}{u(d)}.$$

We modify Hurwitz' class number $H(D)$ as follows :

$$H_p(D) = \begin{cases} 0 & \text{if } p \text{ splits in } \mathcal{O}; \\ H(D) & \text{if } p \text{ is inert in } \mathcal{O}; \\ \frac{1}{2} H(D) & \text{if } p \text{ is ramified in } \mathcal{O}, \text{ but does not divide the conductor of } \mathcal{O}; \\ H_p(\frac{D}{p^2}) & \text{if } p \text{ divides the conductor of } \mathcal{O}. \end{cases}$$

Furthermore, we define $H_p(0) = \frac{p-1}{24}$.

REMARK 2.33.
- The trace of $B(0)$ is by definition $\sum_i \frac{1}{e_i}$.
- The trace of $B(1)$ is simply the class number of $B_{p,\infty}$.

THEOREM 2.34. *(*Eichler's trace formula [**29**, Proposition 1.9, p.120])

For all $m \geq 0$,

$$\mathrm{Tr} B(m) = \sum_{s \in \mathbf{Z}, s^2 \leq 4m} H_p(4m - s^2).$$

COROLLARY 2.35. • *Put $m = 0$. Then*

$$\mathrm{Tr}B(0) = \frac{p-1}{24},$$

the mass formula.

• *Put $m = 1$: we get the class number formula for $B_{p,\infty}$ or, as we recall, the number of supersingular elliptic curves in chararacteristic p :*

$$\mathrm{Tr}B(1) = \frac{p-1}{12} + \frac{1}{3}(1 - (\frac{-3}{p})) + \frac{1}{4}(1 - (\frac{-1}{p})).$$

We go ahead and list further properties of the Brandt matrices .

PROPOSITION 2.36. [**29**, Proposition 3.2, p.127] *Let $m \geq 1$.*

• *The row sums $\sum_j B_{ij}(m)$ are independent of i and equal to*

$$\sigma(m)_p := \sum_{d|m,(d,p)=1} d.$$

• *If $(m, m') = 1$, then $B(m)B(m') = B(mm')$.*

• *$B(p)$ is a permutation matrix of order dividing 2 and for $k \geq 1$,*

$$B(p^k) = B(p)^k.$$

• *If $q \neq p$ is prime and $k \geq 2$,*

$$B(q^k) = B(q^{k-1})B(q) - qB(q^{k-2}).$$

• Hecke-Petersson. *The matrices $B(m)$ for $m \geq 1$ generate a commutative subring $\mathbb{T}$ of $M_n(\mathbf{Z})$, which can be identified with the Hecke ring generated by Hecke operators.*

• *Recall that $e_j = |R_j^\times|$. Then*

$$e_j B_{ij}(m) = e_i B_{ji}(m).$$

• *The commutative algebra $\mathbb{T} \otimes \mathbb{Q}$ is semi-simple, and isomorphic to the product of totally real number fields.*

Furthermore, we have a divisibility result, due to the fact that the action of $\mathrm{Aut}(E_i)/\{\pm 1\}$ on the set of subgroups H of E_i of order ℓ such that $E_i/H \cong E_j$ is free, for $i \neq j$:

PROPOSITION 2.37. [**63**, Remark 3.13, p. 450] *For a prime $\ell \neq p$ the entries of the i-th row of the Brandt matrix for a prime ℓ, $B(\ell)_{ij}$ are divisible by $e_i/2$ unless $i = j$.*

We will only consider elliptic modular forms with respect to the group $\Gamma_0(N)$.

DEFINITION 2.38. A *modular form* f of weight k ($k \in \mathbf{Z}, k \geq 0$) on $\Gamma_0(N)$ is a complex-valued function on the complex upper-half plane such that :

- f is holomorphic everywhere;
- f is holomorphic at every cusp of $\Gamma_0(N)$, i.e. on $\mathbb{Q}$ and at infinity;
- $$f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k f(\tau),$$
  for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$.

The complex vector space of all modular forms of weight k on $\Gamma_0(N)$ is denoted by $M_k(N)$. Note that the map $f \mapsto df$ identifies the modular forms of weight 2 on $\Gamma_0(N)$ with meromorphic differentials on $X_0(N)$ with at most simple poles at the cusps. Hence $\dim(S_2(\Gamma_0(N))) = genus(X_0(N))$.

EXAMPLE 2.39. We list here the characteristic polynomials of some Hecke operators T_p acting on $S_2(\Gamma_0(11))$:

p	2	3	5	7	11	13	17	19	23	29	31
P_{T_p}	$x+2$	$x+1$	$x-1$	$x+2$	$x-1$	$x-4$	$x+2$	x	$x+1$	x	$x-7$

We can now state another property of our Brandt matrices, pertaining to their eigenvalues :

Let us now introduce theta series : let $r \in 2\mathbf{N}$, and let $A = (a_{ij})$ be a r-by-r symmetric, positive definite matrix of integers ($a_{ij} \in \mathbf{Z}$) whose diagonal elements a_{ii} are even:

$$Q(X) = \frac{1}{2}{}^t x A x = \frac{1}{2}\sum_{i,j=1}^{r} a_{ij} x_i x_j$$

is a positive definite integral quadratic form, for $x \in \mathbf{R}^n$. The least positive integer n such that nA^{-1} is an integral matrix with diagonal entries is called the *level* or *Stufe* of

the quadratic form. The quadratic form $Q^*(x) = \frac{1}{2}x^t NA^{-1}x$ is the *adjoint* form. The *discriminant* of Q is $(-1)^{r/2} \cdot \det(A)$.

DEFINITION 2.40. The *theta series* associated to Q is defined as :

$$\theta_Q(\tau) = \sum_{v \in \mathbf{Z}^r} e^{2\pi i \cdot Q(v)\tau}$$

$$= \sum_{n=0}^{\infty} a_Q(n) q^n, \quad q = e^{2\pi i \tau},$$

and $a_Q(n)$ is the number of integral solutions of $Q(x) = n$.

See [**53**, Chapter VI] for details.

THEOREM 2.41. *The theta series $\theta_Q(\tau)$ are modular forms for $\Gamma_0(N)$ of weight $r/2$ and trivial character.*

See [**57**, Theorem 2.14].

Define the theta series θ_{ij} by :

$$\theta_{ij}(\tau) = \sum_{m \geq 0} B_{ij}(m) q^m, \quad q = e^{2\pi i \tau}.$$

COROLLARY 2.42. *The θ_{ij} are modular forms of weight 2 on $\Gamma_0(p)$.*

PROOF. The entries of the Brandt matrices are theta series by construction, and it follows from [**53**, Theorem 20, p. VI-22] that they are modular forms of weight 2. We only ought to show that the level is p and the character is trivial.

$$\deg : \mathrm{Hom}(E_1, E_2) \longrightarrow \mathbf{Z}$$

is a positive definite integral quadratic form in four variables of level p and discriminant p^2 (an alternative description is given in [**57**, Proposition 2.11];

Let $\mathcal{O}$ be a maximal order of level p. Consider the left $\mathcal{O}$-ideal $I^{-1}J$, for I, J left $\mathcal{O}$-ideals, and $\mathcal{O}_r(I) = \mathcal{O}$.

Then the quadratic form :

$$x \mapsto \frac{\mathrm{Norm}(x)}{\mathrm{Norm}(I^{-1}J)}, \quad x \in I^{-1}J,$$

is a positive definite quadratic form of Stufe p and discriminant p^2 (note that it coincides with the degree map :

$$\deg : I^{-1}J \cong \mathrm{Hom}(E_J, E_I) \longrightarrow \mathbf{Z}. \quad)$$

For completeness, we reproduce the argument in [**57**, Proposition 2.11]. The quadratic form $Q(x) = \frac{\mathrm{Norm}(x)}{\mathrm{Norm}(I^{-1}J)}$ is positive definite since the quaternion algebra is definite, hence $B_{p,\infty} \otimes \mathbb{R}$ is $\mathbb{H}$, and the norm form there is positive definite. Since by definition $\mathrm{Norm}(I^{-1}J)|\mathrm{Norm}(x), x \in I^{-1}J$, Q is integral. We first show that the level is p. Since the level is a positive integer, we need only determine the level locally at all prime of $q < \infty$. First consider the case $q \neq p$. Then $(I^{-1}J)_q = \mathcal{O}_q\beta$ for some $\beta \in B^{\bullet}_{p,\infty_q} = \mathrm{GL}_2(\mathbb{Q}_q)$. It follows from the definition of the level that :

$$\mathcal{O}_q = \alpha \begin{pmatrix} \mathbf{Z}_q & \mathbf{Z}_q \\ p\mathbf{Z}_q & \mathbf{Z}_q \end{pmatrix} \alpha^{-1},$$

for some $\alpha \in \mathrm{GL}_2(\mathbb{Q}_q)$.

Let $e_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $e_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $e_3 = \begin{pmatrix} 0 & 0 \\ p & 0 \end{pmatrix}$, $e_4 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.

Then $\alpha e_i \alpha^{-1}\beta, i = 1, \ldots, 4$ gives a $\mathbf{Z}_q$-basis for $\mathcal{O}_q\beta$. Further $\mathrm{Norm}(I^{-1}J) = \mathrm{Norm}(\beta) \mod U_q$. Then the matrix A is of the form $A = U^t BU$ where $U \in \mathrm{GL}_2(\mathbf{Z}_q)$ and :

$$\begin{aligned} B &= \frac{1}{\mathrm{Norm}(\beta)} \mathrm{Tr}\Big((\alpha E_i \alpha_i^{-1}\beta)\overline{(\alpha e_j \alpha_i^{-1}\beta)}\Big) \\ &= \frac{1}{\mathrm{Norm}(\beta)} \mathrm{Tr}(\beta\bar{\beta}\alpha^{-1}\overline{\alpha^{-1}}\alpha e_i \bar{e_j}\alpha^{-1}\alpha\bar{\alpha}) \\ &= \mathrm{Tr}(e_i\bar{e_j}) \\ &= \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -p & 0 \\ 0 & -p & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \end{aligned},$$

which has level p in $\mathbf{Z}_q$. Since the Stufe of A is equal to the Stufe of $U^t AU$ for any matrix $U \in \mathrm{GL}_r(\mathbf{Z})$, A has level $p \mod U_q$ in $\mathbf{Z}_q$. For the case $q = p$, we have $(I^{-1}J)_p = \mathcal{O}_p\beta$ for some $\beta \in B^{\times}_{p,\infty_p}$. Since $\mathcal{O}$ has level p, it follows from the definition that $\mathcal{O}_p$ is

conjugate to :

$$\left\{ \begin{pmatrix} \alpha & p^r\beta \\ p^{r+1}\beta^\sigma & \alpha^\sigma \end{pmatrix}, \alpha, \beta \in R \right\}.$$

Thus, using the fact that $R = \mathbf{Z}_p \oplus \mathbf{Z}_p u^{\frac{1}{2}}$, where $u \in \mathbf{Z}$, u a quadratic nonresidue mod p if $p \neq 2$, and $R = \mathbf{Z}_2 \oplus \mathbf{Z}_2(\frac{1+5^{\frac{1}{2}}}{2})$ if $p = 2$, a similar calculation to what we did above shows that A has level p mod U_p in $\mathbf{Z}_p$ also. Thus the level must be p. The discriminant can be calculated in the same local way as the level, and it is p^2. It follows from this discussion that the level of θ_{ij} is p, since the level of Q is p. The character ϵ associated to θ_{ij} is trivial since the discriminant of Q is p^2 and

$$\epsilon = \epsilon(p^2) = (sgn(p^2))^2(p^2/p^2) = 1.$$

□

More importantly,

THEOREM 2.43. *The theta series θ_{ij} of weight 2 on $\Gamma_0(p)$ span the space of modular forms $M_2(\Gamma_0(p))$.*

See [**29**, Section 5].

EXAMPLE 2.44. Take $p = 2$. Let $\mathcal{O} = \mathbf{Z} + \mathbf{Z}i + \mathbf{Z}j + \mathbf{Z}\omega$, $\omega = \frac{1+i+j+k}{2}$. The order $\mathcal{O}$ is a right principal ideal ring, thus any right ideal I is isomorphic to $\mathcal{O}$, and the ring of $\mathrm{End}_{\mathcal{O}}(I) \cong \mathcal{O}$, acting by left multiplication. The norm form is

$$N(x + iy + jz + \omega \cdot w) = x^2 + y^2 + z^2 + (x + y + z + w)w,$$

and its matrix form is :

$$N(x, y, z, w) = \frac{1}{2}\underline{X}M\underline{X}^t = \frac{1}{2}\underline{X}\begin{bmatrix} 2 & 0 & 0 & 1 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 2 & 1 \\ 1 & 1 & 1 & 2 \end{bmatrix}\underline{X}^t,$$

with $\underline{X} = (x, y, z, w)$. The theta series

$$\sum_{\phi \in \mathcal{O}} q^{N(\phi)} = \sum_{x,y,z,w} q^{N(x,y,z,w)}$$

generates $M_2(\Gamma_0(2))$ and is given by the following q-expansion :

$$F_1 = \frac{1}{24} + q + q^2 + 4q^3 + q^4 + 6q^5 + 4q^6 + 8q^7 + q^8 + 13q^9 + \cdots,$$

The Brandt matrices are 1-by-1 arrays, and the list begins as follows :

$$B(0) = \frac{1}{24}, B(1) = 1, B(2) = 1, B(3) = 4, \ldots$$

EXAMPLE 2.45. Take $p = 11$. In this case, the class number is 2. The curve $X_0(11)$ is an elliptic curve with equation:

$$Y^2 + Y = X^3 - X^2 - 10X - 20,$$

and since the genus of $X_0(p)$ is equal to the dimension of the space of cusp forms $S_2(\Gamma_0(p))$, we have a unique normalized cusp form :

$$\begin{aligned} F_1 &= q \prod_{m \geq 1} (1 - q^m)(1 - q^{11m})^2 \\ &= q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} + q^{11} - 2q^{12} + 4q^{13} + \ldots \end{aligned}$$

and the Eisenstein series :

$$\begin{aligned} F_2 &= \frac{5}{12} + \sum_{m \geq 1} \sigma_{11}(m) q^m \\ &= \frac{5}{12} + q + 3q^2 + 4q^3 + 7q^4 + 6q^5 + \ldots, \end{aligned}$$

i.e. the dimension of $M_2(\Gamma_0(11))$ is two. There are four theta series f_{11}, f_{12}, f_{21} and f_{22}; by Theorem 2.43, they generate the space $M_2(\Gamma_0(11))$.

The precise linear relations between them are as follows :

$$F_1 = f_{11} + f_{12} = f_{21} + f_{22} = 3f_{11} - 2f_{22};$$

and

$$F_2 = f_{11} - f_{21} = f_{22} - f_{12} = 3f_{22} - 2f_{11}.$$

So we can easily compute all the Brandt matrices $B(m)$ for m arbitrary high, using a symbolic calculator :

$$B(0) = \begin{pmatrix} 1/4 & 1/6 \\ 1/4 & 1/6 \end{pmatrix}; B(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; B(2) = \begin{pmatrix} 1 & 2 \\ 3 & 0 \end{pmatrix};$$

$$B(3) = \begin{pmatrix} 2 & 2 \\ 3 & 1 \end{pmatrix}; B(4) = \begin{pmatrix} 5 & 2 \\ 3 & 4 \end{pmatrix}; B(5) = \begin{pmatrix} 4 & 2 \\ 3 & 3 \end{pmatrix}, \ldots$$

REMARK 2.46. Let $D(p)$ be the Hecke module spanned by supersingular j-invariants in characteristic p. The subspace of elements of degree 0 is isomorphic to the space of cusp forms of weight 2 for $\Gamma_0(p)$.

CHAPTER 2

Hilbert Modular Surfaces

1. Abelian Schemes

Recall that an abelian scheme A over a scheme S is a group scheme

$$\pi : A \longrightarrow S,$$

such that π is smooth and proper, and the geometric fibers are connected. The abelian scheme X is a commutative group scheme ([**49**, Corollary 6.5]). If A is projective over S, there exists a dual abelian scheme $A^t := \mathrm{Pic}^0_S(A) \subset \mathrm{Pic}_S(A)$, where $\mathrm{Pic}_S(A)$ classifies invertible sheaves trivialized along the section e. A^t is a projective abelian scheme ([**49**, Corollary 6.8]). Put $NS(A) = \mathrm{Pic}(A)/\mathrm{Pic}^0(A)$.

THEOREM 1.1. *([**50**, Theorem 1, Section 15, Chapter III, p. 143])*

Let

$$0 \longrightarrow H \longrightarrow A \xrightarrow{f} B \longrightarrow 0$$

be an exact sequence with A, B are abelian schemes, f an isogeny and H a finite, flat group scheme. Then the dual sequence is exact

$$0 \longrightarrow H^\vee \longrightarrow B^t \xrightarrow{f^t} A^t \longrightarrow 0$$

i.e. $\mathrm{Ker}(f^t) := H^t = H^\vee$, *the Cartier dual of* H.

DEFINITION 1.2. [**49**, Definition 6.3] A *polarization* of $A \longrightarrow S$ is a homomorphism $\lambda : A \longrightarrow A^t$ such that for each geometric point s of S, $\lambda_s = \lambda(\mathcal{L}_s)$ for some ample invertible sheaf $\mathcal{L}_s$ of A_s.

A polarization is finite and faithfully flat, i.e. it is an isogeny. The polarization is called *principal* if it is an isomorphism.

EXAMPLE 1.3. [50, Chapter 3, p. 91] Let $\mathcal{L}$ be an invertible sheaf on A. It defines a group homomorphism:

$$\lambda_{\mathcal{L}} : A \longrightarrow A^t,$$
$$a \mapsto T_a^*(\mathcal{L}) \otimes \mathcal{L}^{-1} \otimes a^*(\mathcal{L})^{-1} \otimes e^*\mathcal{L},$$

where T_a^* is translation-by-a.

FACT 1.4. (1) If f is a polarization, then $f = f^t$ (under $(A^t)^t \cong A$). Hence, the kernel of a polarization is self-dual group scheme. (2) The group scheme $A[n]$ is dual to $A^t[n]$ and one obtains the Weil pairing:

$$A[n] \times A[n]^\vee \longrightarrow \mathbb{G}_m.$$

Let A be defined over a field k of characteristic p. If λ is a polarization, we get a bilinear, antisymmetric, Galois invariant pairing (under $\mathrm{Gal}(\overline{k}/k)$):

$$\langle\ ,\ \rangle_\lambda : A[n] \times A[n] \longrightarrow \mathbb{G}_m,$$
$$\langle x, y\rangle_\lambda = \langle x, \lambda(y)\rangle.$$

It is perfect iff $(\deg\lambda, n) = 1$. One can prove that $A[n]$ is an affine group scheme of order n^{2g} (where $g = \dim A$). If $\mathrm{char(k)} = 0$, then $(\mathrm{char(k)}, n) = 1$, and $A[n]$ is étale, i.e. $A[n] \otimes_k k^{sep} \cong (\mathbf{Z}/n\mathbf{Z})^{2g}$. If $\mathrm{char(k)} = p$ and $n = p$, then $|A[p](\overline{k})| \leq p^g$.

DEFINITION 1.5. An abelian variety A over $\overline{k}$ is *ordinary* if

$$A[p](\overline{k}) \cong (\mathbf{Z}/p\mathbf{Z})^g.$$

For an abelian variety A defined over a field k of characteristic p, we can define the a-number as :

$$a(A) := \dim \mathrm{Hom}_k(\alpha_p, A).$$

1.1. Abelian schemes with real multiplication.

DEFINITION 1.6. An abelian scheme A/S with *real multiplication* (abbreviated RM) by $\mathcal{O}_L$ is an abelian scheme of relative dimension g over S together with a *given* homomorphism of the ring of integers of a totally real field L

$$\iota : \mathcal{O}_L \longrightarrow \mathrm{End}(A),$$

such that $\mathfrak{t}_A$ is a locally (on S) free $\mathcal{O}_L \otimes \mathcal{O}_S$-module of rank 1.

Note that we can define $\mathrm{Lie}(A/S)$ as the S-dual of $\underline{\omega}(A/S)$, the sheaf of invariant 1-forms on A (itself defined as $e^*(\Omega_{A/S})$, $e : S \longrightarrow A$ being the identity section).

EXAMPLE 1.7. 1. For any elliptic curve E, consider:

$$E \otimes_{\mathbf{Z}} \mathcal{O}_L \cong E^g \text{ with a canonical } \mathcal{O}_L\text{-action (multiplication),}$$

the isomorphism being obtained by choosing a $\mathbf{Z}$-basis to $\mathcal{O}_L$. We get an abelian variety over $\mathbb{C}$ by taking

$$(E \otimes_{\mathbf{Z}} \mathcal{O}_L)(\mathbb{C}) = E(\mathbb{C}) \otimes_{\mathbf{Z}} \mathcal{O}_L.$$

We shall discuss this example explicitly in the case $g = 2$ in Chapter III.

2. If an abelian scheme A/S has RM by $\mathcal{O}_L$, so does the dual abelian scheme A^t, under $\iota^t(m) := \iota(m)^t$.

A homomorphism between abelian schemes with real multiplication is a usual homomorphism respecting the $\mathcal{O}_L$-action.

DEFINITION 1.8. An *isogeny* of abelian schemes with real multiplication is a finite homomorphism.

REMARK 1.9. For a separable isogeny f commuting with $\mathcal{O}_L$-action $\mathrm{Ker}f$ is a finite $\mathcal{O}_L$-module, and we define :

$$\deg_{\mathcal{O}_L} f = \mathcal{F}(\mathrm{Ker}f),$$

the Fitting ideal in $\mathcal{O}_L$.

According to Deninger ([**16**]),

$$\deg_{\mathcal{O}_L} f = \det_{L \otimes Q_\ell}(f^*_{|H^1(A,\ell))}), \quad \text{for any } \ell,$$

where $H^1(A, \ell)$ is the first ℓ-adic (resp. crystalline) cohomology group of A with coefficients in $Q_\ell = \mathbb{Q}_\ell$ if $\ell \neq char(k)$ (resp. $Q_\ell = W(k) \otimes \mathbb{Q}$ if $\ell = chark$), hence the ideal $\deg_{\mathcal{O}_L}$ is always ***principal*** .

THEOREM 1.10. *([22, Proposition 1.2.4]) If $f : A \longrightarrow B$ is an isogeny of abelian schemes with RM, then f is faithfully flat, and induces an exact sequence:*

$$0 \longrightarrow \ker f \longrightarrow A \longrightarrow B \longrightarrow 0.$$

DEFINITION 1.11. Let (A, ι) be an abelian scheme with RM by $\mathcal{O}_L$. Let

$$\mathcal{M}_A := \left\{\lambda : A \longrightarrow A^t : \lambda = \lambda^t, \lambda \text{ a } \mathcal{O}_L\text{-linear homomorphism}\right\},$$

(a polarization is $\mathcal{O}_L$-linear if $i^t(r) \circ \lambda = \lambda \circ \iota(r), \quad \forall r \in \mathcal{O}_L$)

$$\mathcal{M}_A^+ := \{\lambda \in \mathcal{M}_A : \lambda \text{ is a polarization } \}.$$

Of course, $\mathcal{M}_A^+ \subseteq \mathcal{M}_A$.

REMARK 1.12. The set $\mathcal{M}_A^+$ is a positive cone.

FACT 1.13. ([61, Proposition 1.17]) $\mathcal{M}_A$ is an $\mathcal{O}_L$-module, projective of rank 1 (i.e. isomorphic to an ideal) i.e.

$$l \in \mathcal{O}_L, \lambda \in \mathcal{M}_A \implies \lambda \circ l \in \mathcal{M}_A.$$

DEFINITION 1.14. A projective rank 1 $\mathcal{O}_L$-module with a notion of positivity is a projective rank 1 $\mathcal{O}_L$-module $\mathcal{M}$ such that for all σ_i an order $<_i$ is chosen on

$$\mathcal{M} \otimes_{\mathcal{O}_L} \mathbb{R} \quad (\cong \mathbb{R} \text{ non canonically}),$$

where the $\mathcal{O}_L$-module structure of $\mathbb{R}$ is given by the embedding σ_i.

DEFINITION 1.15. Let B be a semi-simple algebra with center containing $\mathbb{Q}$. An anti-involution $x \mapsto x^*$ on B is *positive definite* iff $\mathrm{Tr}_{\mathbb{Q}}(xx^*) > 0 \ \forall x \neq 0$.

DEFINITION 1.16. Let λ be a polarization on an abelian scheme A, and put $\mathrm{End}^0(A) = \mathrm{End}(A) \otimes \mathbb{Q}$. The *Rosati involution* associated to λ is the map

$$\mathrm{End}^0(A) \longrightarrow \mathrm{End}^0(A)$$

$$f \mapsto \lambda^{-1} f^t \lambda = f^*$$

FACT 1.17. The Rosati involution is positive definite on $\mathrm{End}^0(A)$ ([50, Chapter IV, Section 21]).

Define a map

$$NS^0(A) \hookrightarrow \mathrm{End}^0(A),$$

$$\phi_\lambda : \mathcal{L}_{(H,\chi)} \mapsto \lambda^{-1}\phi_L.$$

The set $\phi_\lambda(NS^0(A))$ is composed of the symmetric elements of $\mathrm{End}^0(A)$ (under the Rosati involution). In particular, $(\mathcal{M}_A, \mathcal{M}_A^+)$ is naturally an $\mathcal{O}_L$-module with a notion of positivity, since $\mathcal{M}_A^+$ maps to totally positive symmetric elements in $\mathrm{End}^0(A)$)

2. Abelian varieties over a finite field

Let A be an abelian variety of dimension g defined over a perfect field k of characteristic p.

Consider the multiplication-by-ℓ map $[\ell^m] : A \longrightarrow A$. Put $A[\ell^m] := \mathrm{Ker}([\ell^m])$. It is a finite group scheme of order $(\ell^m)^{2g}$.

If $\ell = p$, then $A[p^m]$ is not étale, hence cannot be described by the points in $A(\bar{k})$. Let $A(p)$ be the Barsotti-Tate group (or *p-divisible group*, see [**65**]) of height $2g$ associated to the direct system $\{A[p^m]\}$. Since k is assumed to be perfect and characteristic p, we can use covariant Dieudonné module theory which allows a classification of Barsotti-Tate groups (see [?] for a generalization).

We denote by σ the isomorphism $\sigma : W(k) \longrightarrow W(k)$ on the ring of (infinite) Witt vectors, induced by the Frobenius map $x \mapsto x^p$ on k. We denote by $W(k)[F,V]$ the (non-commutative) ring with variables F, and V, coefficients in $W(k)$ and relations:

$$FV = p = VF, \quad Fa = a^\sigma F \text{ and } aV = Va^\sigma, \text{ for } a \in W(k).$$

Note that $W(k)[F,V]$ is commutative iff $k = \mathbf{F}_p$.

THEOREM 2.1. *There is an equivalence of categories between, on one side, extensions of Barsotti-Tate groups G by finite commutative groups with p-power order over k, and on the other side, left $W(k)[F,V]$-modules M of finite type. Under this equivalence, Barsotti-Tate groups correspond to free modules,*

$$\dim M/FM = \dim G, \quad \dim M/VM = \dim(G^t), \quad \dim M/pM = \textit{height}(G),$$

$$M(G^t) \cong M(G)^\vee := \mathrm{Hom}_{W(k)}(M(G), W(k)).$$

By Dieudonné theorem, we associate to the p-divisible group $A(p)$ the Dieudonné module $\mathcal{D}(A(p))$. We denote by $\mathcal{D}(A(p))$ the contravariant Dieudonné module of $A(p)$ and by $\mathbb{D}(A(p))$ the covariant Dieudonné module.One can check easily that it is the inverse limit of the Dieudonné modules corresponding to $A[p^m]$. We can recover $A[p^m]$ by taking the finite group scheme corresponding to the Dieudonné module $\mathcal{D}(A(p))/p^m\mathcal{D}(A(p))$.

THEOREM 2.2. (Tate)

If k is a finite field, then

$$\mathrm{Hom}_k(A,B)\otimes\mathbf{Z}_p \cong \mathrm{Hom}(\mathcal{D}(B(p)),\mathcal{D}(A(p))),$$

where the r.h.s. denote homomorphisms of $W(k)[F,V]$-modules.

If $\ell \neq p$, then A_{ℓ^m} is étale (i.e. becomes a constant group scheme after base change), hence it is determined by $A_{\ell^m}(\bar{k})$ and the action of the Galois group $\mathrm{Gal}(\bar{k}/k)$ on it. Taking the inverse limit of all $A_{\ell^m}(\bar{k})$, we obtain the Tate module $T_\ell(A)$, which is a free $\mathbf{Z}_\ell$-module of rank $2g$ on which $\mathrm{Gal}(\bar{k}/k)$ acts by $\mathbf{Z}_\ell$-linear maps. Again, $A_{\ell^m}(\bar{k})$ can be recovered from the module since it is isomorphic to $T_\ell(A)/\ell^m T_\ell(A)$ as Galois modules.

THEOREM 2.3. (Tate) *If k is a finite field, then*

$$\mathrm{Hom}(A,B)\otimes\mathbf{Z}_\ell \cong \mathrm{Hom}_{\mathbf{Z}_\ell[\mathrm{Gal}(\bar{k}/k)]}(T_\ell A, T_\ell B).$$

Going back to Barsotti-Tate groups of abelian varieties, we have the classification up to isogeny :

THEOREM 2.4. (Dieudonné) *The category of Barsotti-Tate groups up to isogeny over an algebraically closed field of characteristic p is semi-simple. The simple objects are precisely the p-divisible groups $\mathcal{G}_{m,n}$ for $m,n\in\mathbf{N}$, $(m,n)=1$ or $(m,n)=(1,0)$. The group $\mathcal{G}_{m,n}$ has dimension m and is determined by its $W(k)[F,V]$-module $C_{m,n}=C_p(\mathcal{G}_{m,n})$, where*

$$C_{m,n} = W(k)[F,V]/(F^m - V^n).$$

We complete the picture by putting $\mathcal{G}_{0,1} := \mathbf{Q}_p/\mathbf{Z}_p$.

DEFINITION 2.5. We say that $\mathcal{G}_{m,n}$ has slope $\frac{n}{m+n}$ of length $m+n$, which is the height of $C_{m,n}$. By convention, we give slope 1 and height 1 to $\mathcal{G}_{0,1}$.

Granted the Dieudonné-Manin classification, any p-divisible group $\mathcal{G}$ over k of dimension d and height h can be decomposed, up to isogeny :

$$\mathcal{G} \sim \oplus \mathcal{G}_{m_i,n_i},$$

with $\sum m_i = d, \sum(m_i + n_i) = h$.

We associate to each $\mathcal{G}_{m_i,n_i}$ a segment of slope $\frac{m_i}{m_i+n_i}$ of length $m_i + n_i$. The *Newton polygon* is the unique lower convex polygon starting at $(0,0)$ and ending at $(\text{heigth}(\mathcal{G}), \dim(\mathcal{G}))$ having increasing slopes and constructed from the building blocks associated to $\mathcal{G}_{m_i,n_i}$. All such Newton polygons are symmetric. Note that all the breaking points have integer coordinates.

EXAMPLE 2.6. $g = 1$ An elliptic curve is either ordinary or supersingular. Hence the group $\mathcal{G}_{1,0}$ is isomorphic to the formal group of an ordinary elliptic curve over k, and $\mathcal{G}_{1,1}$ is isomorphic to the formal group of a supersingular elliptic curve over k. The Newton polygon corresponding to an ordinary elliptic curve is a broken line : a segment of slope 0 and a segment of slope 1, and the Newton polygon corresponding to a supersingular elliptic curve is a line of slope $1/2$.

2.1. Serre-Tate theorem. Let k be a field of characteristic p. Let $\Lambda = W_p(k)$ (the infinite Witt vectors). Let $\mathcal{C}_k$ be the category of local artinian rings Λ-algebras $(R, \mathfrak{m}_R)$ together with a given isomorphism $R/\mathfrak{m}_R \cong k$. Morphisms are local isomorphisms of rings inducing the identity on k.

Let A be an abelian variety over k.

THEOREM 2.7. Serre-Tate

For every ring in $\mathcal{C}_k$, the functor :

$$\mathbf{A} \mapsto \mathbf{A}(p)$$

induces an equivalence of categories between the category **A** *of A over R with morphisms of abelian schemes over R, to the category of deformations of $A(p)$ into p-divisible groups*

over R with the morphisms being morphisms of p-divisible groups whose restriction to $A(p)$ comes from an endomorphism of A/k.

3. Supersingular and superspecial points

Let k be an algebraically closed field of characteristic p. We present in this section a number of finiteness results. We begin by Deligne's theorem, which forbids cancellation for products of elliptic curves.

THEOREM 3.1. (Deligne [**70**, p. 580]) *Let $g \geq 2$. Let $E_1, \ldots, E_g, E_{g+1}, \ldots, E_{2g}$ be arbitrary supersingular elliptic curves. Then*

$$E_1 \times \cdots \times E_g \cong E_{g+1} \times \cdots \times E_{2g}.$$

An abelian variety is *supersingular* if it is isogenous to a product of supersingular elliptic curves. If it is *isomorphic* to a product of supersingular elliptic curves, we say it is *superspecial*. Deligne's theorem allows us to restrict ourselves to E^g, for E a fixed supersingular elliptic curve. Furthermore, we may pick a supersingular elliptic curve defined over $\mathbb{F}_p$ such that its (relative) Frobenius $F : E \longrightarrow E$ satisfies $F^2 + p = 0$ (see [**79**, Theorem 4.1.5]).

THEOREM 3.2. (Oort, [**55**, Theorem 2]) *Let A be defined over an algebraically closed field, then*

$$A \cong E_1 \times \cdots \times E_g \iff a(A) = g.$$

Note that if this is the case, A can be defined over a finite field (see [**54**, Lemma 4.5]). It is known ([**31**]) that superspecial abelian surfaces with RM are in fact defined over $\mathbf{F}_{p^2}$.

In all the moduli varieties under consideration in this thesis, the number of superspecial points is finite. The crucial ingredients to show that are Deligne's theorem and the following finiteness result about polarizations :

THEOREM 3.3. ([**51**]) *Let d be a positive integer. An abelian variety A defined over an algebraically closed field k has only* finitely *many possible polarizations of degree d^2, up to isomorphism.*

We will use the following :

COROLLARY 3.4. [**55**, Corollary 7] *Let A be a supersingular abelian surface over k, with $a(A) = 1$; then A is an α_p-covering of a product of two elliptic curves, i.e. A/α_p is isomorphic with a product of two elliptic curves.*

COROLLARY 3.5. ([**36**]) *Let E be a supersingular elliptic curve. Any supersingular abelian surface A is isomorphic to $(E \times E)/\iota(\alpha_p)$, for a suitable immersion $\iota : \alpha_p \hookrightarrow E \times E$.*

PROOF. We show that the two last corollaries are indeed equivalent. If $a(A) = 2$, we can take $\mathrm{Fr} : E \longrightarrow E^{(p)}$ and

$$E \times (E/\alpha_p) \cong E \times E^{(p)} \cong A.$$

Consider a supersingular abelian variety with a-number 1. Suppose Corollary 3.4 is true. Consider the composition :

$$A \longrightarrow A/\alpha_p \longrightarrow A/\mathrm{Ker}[Fr].$$

We have

$$\alpha_p \subseteq \mathrm{Ker}[Fr] \subset A,$$

$$H := \mathrm{Ker}Fr/\alpha_p \subset E_1 \times E_2 \cong A/\alpha_p,$$

and $H \cong \alpha_p$, since it is local-local of rank p, and

$$(E_1 \times E_2)/H \cong A^{(p)}.$$

But

$$(A^{(p)})^{(\frac{1}{p})} \cong A,$$

k being algebraically closed, hence perfect, hence

$$(E_1 \times E_2/H)^{1/p} \cong (E_1)^{1/p} \times (E_2)^{1/p}/\alpha_p \cong A.$$

Hence the result follows.

Now, suppose Corollary 3.5 is true. Then

$$A = E \times E/\alpha_p.$$

Since $H := \alpha_p \cong (E \times E)[\mathrm{Fr}]/\alpha_p$, we have

$$X/H \cong (E \times E)^{(p)} = E^{(p)} \times E^{(p)}.$$

□

COROLLARY 3.6. *([36, Lemma 1.4])* Let $A = E_1 \times E_2$ be an abelian surface with supersingular elliptic curves E_1 and E_2. Let $\iota : \alpha_p \hookrightarrow A$ be an immersion such that $B = A/\iota(\alpha_p)$ is not isomorphic to a product of two elliptic curves. Then, the subgroup scheme which is isomorphic to α_p is *unique* in B.

PROOF. Clear. □

3.1. Siegel modular varieties. Let $\mathcal{A}_{g,n}$ the coarse moduli space of triples (A, λ, η), where A is an abelian variety with a principal polarization λ and full level n-structure α. For $n \geq 3$, it a fine moduli scheme, quasi-projective over $\mathrm{Spec}(\mathbf{Z})$, and smooth over $\mathrm{Spec}(\mathbf{Z}[\frac{1}{n}])$ (see [**49**, Theorem 7.9, p.139]).

We denote by $\mathcal{A}_g \longrightarrow \mathrm{Spec}(\mathbf{Z})$ the coarse moduli space of principally polarized abelian varieties of dimension g. We have :

$$\mathcal{A}_g(\mathbf{C}) \cong \mathbf{Sp}_{2g}(\mathbf{Z})\backslash\mathcal{H}_g;$$

where $\mathcal{H}_g$ is the Siegel upper half plane and where the symplectic group acts on $\mathcal{H}_g$ by:

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} Z = (AZ + B)(CZ + D)^{-1}.$$

Fix a prime p. Since there are only finitely many possibilities for the level n structure, and similarly for polarizations (Theorem 3.3), there are only finitely many superspecial points in the supersingular locus.

PROPOSITION 3.7. *([43, Section 4.9,p.26]) The dimension of the supersingular locus S_g in $A_g \times \overline{\mathbf{F}}_p$ is: $\left[\frac{g^2}{4}\right]$, where $[\cdot]$ denotes the integral part.*

Let $B = B_{p,\infty}$ be the definite quaternion algebra ramified at ∞, and $x \mapsto \overline{x}$ its canonical involution. Let B^n be a left B-module of dimension n. The (non-degenerate) definite quaternion hermitian form $<,>$ on B^n is unique up to change of basis over B

([**68**, Lemma 4.4, p.53]) and may be written in the form $\sum_{i=1}^{n} x_i\overline{y}_i$ for $x, y \in B^n$. Let $\mathcal{O}$ be a maximal order of B.

DEFINITION 3.8. A $\mathbf{Z}$-module M in B^n is called a *left $\mathcal{O}$-lattice* if M is a left $\mathcal{O}$-module and a lattice in B^n.

Two $\mathcal{O}$-lattices M_1 and M_2 are said to be *equivalent* globally (resp. locally at a rational prime q) if $M_1 \cdot g = M_2$ (resp. $(M_1 \otimes \mathbf{Z}_q) \cdot g_p = M_2 \otimes \mathbf{Z}_q)) =$ for g (resp. g_q) in the corresponding group of similitudes of $<,>$ (see [**30**, Section 2.1, p.139]).

DEFINITION 3.9. A *genus* of $\mathcal{O}$-lattices is a set consisting of all (global) $\mathcal{O}$-lattices in B^n which are equivalent locally for every prime q.

The set containing $\mathcal{O}^n$ is called the principal genus. The set of left $\mathcal{O}$-lattices in B^n which are locally equivalent to $\mathcal{O}_q^n$ except for $q = p$ (there is a unique other possibility) is called the non-principal genus. We denote by $H_g(p, 1)$ (resp. $H_g(1, p)$) the number of global equivalence classes in the corresponding genera.

PROPOSITION 3.10. ([**68**, Section 4.4, p.53]) *The class numbers $H_g(p, 1)$ and $H_g(1, p)$ are finite.*

We covered the case $h = H_1(p, 1)$ in the first chapter. The cases $n \geq 2$ contrast by their uniformity and simplicity :

THEOREM 3.11. ([**20**]) *The class number of $M_n(B)$ is equal to one for $n \geq 2$.*

THEOREM 3.12. *(*[**30**, Theorem 2.10, p.144]*) Let $g \geq 2$. The number of superspecial points in A_g is equal to the class number $H_g(p, 1)$ of the principal genus of the quaternion hermitian space B^n.*

THEOREM 3.13. ([**43**, Section 4.9, p.26]) *The number of irreducible components of S_g is given by : $H_g(p, 1)$, if g odd, and by $H_g(1, p)$, if g even. Moreover, for each irreducible component of $S_{g,1}$, the a-number of the generic point is one.*

EXAMPLE 3.14. A general formula has been given in [?] and [?], since it is a bit lenghty, we just quote some values of $H_2(p,1)$ and $H_2(1,p)$ for $g=2$:

p	2	3	5	7	11	13	17	19	23	29	31	37
$H_2(p,1)$	1	1	2	2	5	4	8	10	16	24	26	37
$H_2(1,p)$	1	1	1	1	1	2	2	2	2	3	3	5

We now concentrate on the case $g=2$. As follows from Theorem 3.7, the supersingular locus $\mathcal{S}_2$ has dimension 1. Moreover, all irreducible components are given by rational lines. We shall only sketch briefly the construction of those components, since we will come back to this in chapter 3.

Consider a superspecial abelian variety $A \cong E_1 \times E_2$. Let $\mathfrak{t}_A$ be the tangent space at the origin, and put $\mathbb{P}^1 = \mathbb{P}(\mathfrak{t}_A)$ be the projective line. Set

$$K_{\mathbb{P}^1} = \alpha_p \times \alpha_p \times \mathbb{P}^1; \quad A_{\mathbb{P}^1} = A \times \mathbb{P}^1.$$

Let H be the subgroup scheme H of $K_{\mathbb{P}^1}$ defined by the equation $Y\alpha - X\beta = 0$, where $(X,Y) \in \mathbb{P}^1$. Put $\mathcal{X} = A_{\mathbb{P}^1}/H$.
We have the exact sequence :

$$0 \longrightarrow H \longrightarrow A_{\mathbb{P}^1} \xrightarrow{\pi} \mathcal{X} \longrightarrow 0,$$

with canonical projections $\pi_1 : A_{\mathbb{P}^1} \longrightarrow A$, $\pi_2 : A_{\mathbb{P}^1} \longrightarrow \mathbb{P}^1$, and the induced map $q : \mathcal{X} \longrightarrow \mathbb{P}^1$.
The crucial point is the existence of a symmetric invertible sheaf $\mathcal{L}$ on A ([47, p. 139-140]) such that:

$$K(\mathcal{L}) \cong \alpha_p \times \alpha_p, \tag{3.1}$$

where $K(\mathcal{L})$ is the kernel of the polarization $\phi_{\mathcal{L}} : A \longrightarrow A^t$ defined by $\mathcal{L}$.

Every subgroup of order p of $K(\mathcal{L})$ is isotropic, hence H is fiber-by-fiber isotropic, hence an isotropic subgroup of $K_{\mathbb{P}^1}$. By Mumford's theory, the polarization defined by $\mathcal{L}$ on $A_{\mathbb{P}^1}$ descends to a principal polarization on the abelian scheme

$$q : \mathcal{X} \longrightarrow \mathbb{P}^1.$$

Consider the subscheme $\mathcal{X}[n] = \mathrm{Ker}[n]_{\mathcal{X}}$ over $\mathbb{P}^1$. Since $(n,p) = 1$, $\mathcal{X}[n] \longrightarrow \mathbb{P}^1$ is étale, and this allows us to put level n-structure on $q : \mathcal{X} \longrightarrow \mathbb{P}^1$, and we get morphisms

$$\mathbb{P}^1 \longrightarrow \mathcal{A}_{2,n} \otimes \overline{\mathbf{F}}_p, \quad \mathbb{P}^1 \longrightarrow \mathcal{A}_{2,1} \otimes \overline{\mathbf{F}}_p,$$

where $\mathcal{A}_{2,n} \longrightarrow \mathrm{Spec}(\mathbf{Z}[\frac{1}{n}])$ is the moduli scheme of principally polarized abelian surfaces with full level n structure. Since $q : \mathcal{X} \longrightarrow \mathbb{P}^1$ is non isotrivial ([47, p.131]), the image of this morphism is a component of $\mathcal{S}_{2,n}$ (resp. $\mathcal{S}_{2,1}$). Conversely, one knows that any component of $\mathcal{S}_{2,n}$, $n \geq 2$, $(n,p) = 1$ is a Moret-Bailly family, induced by a divisor satisfying condition 3.1.

We will present formulae for the number of components and the number of superspecial points that occur when we fix the level structure.

For the following, assume $p \geq 3$.

The Galois covering :

$$\mathcal{A}_{2,n} \longrightarrow \mathcal{A}_2,$$

for $(n,p) = 1$ has Galois group isomorphic to $PSp(4, \mathbf{Z}/n\mathbf{Z}) = Sp(4, Z/n\mathbf{Z})/(\pm 1)$.

PROPOSITION 3.15. Number of irreducible components in $\mathcal{S}_{2,q}$ *Let $q \neq p$, q odd. The number of irreducible components in $\mathcal{S}_{2,q}$ is :*

$$\frac{|PSp(4, \mathbf{Z}/q\mathbf{Z})|(p^2-1)}{2880},$$

where $|PSp(4, \mathbf{Z}/q\mathbf{Z})| = \frac{q^4(q^4-1)(q^2-1)}{2}$, $|PSp(4, \mathbf{Z}/2\mathbf{Z})| = 720$.

PROPOSITION 3.16. Number of supersingular points in $\mathcal{S}_{2,q}$. *Let $q \neq p$, q odd. The number of supersingular points in $\mathcal{S}_{2,q}$ is :*

$$|S_{2,q}| = \frac{|PSp(4, \mathbf{Z}/q\mathbf{Z})|(p-1)(p^2+1)}{2880}, \quad |S_{2,2}| = (p-1)(p^2+5p-4).$$

We have a mass formula :

PROPOSITION 3.17.

$$\sum_{i=1}^{H_g(p,1)} \frac{1}{\mathrm{Aut}(A, \lambda_i)} = \frac{(p-1)(p^2+1)}{2880},$$

where the sum runs over superspecial points on A_g.

3.2. Hilbert modular surfaces. We give a description of the works of [72], [13], [1].

Let L be a fixed totally real field of degree $2 = [L : \mathbb{Q}]$. Let $p > 2$ be an inert prime in L, and let $(n, p) = 1$. Denote by $\mathcal{D}_L$ the different ideal of L over $\mathbb{Q}$, and let d_L denote the discriminant of L.

Let $\mathcal{M}_n$ be the moduli space parameterizing abelian surfaces $(A, \iota, (\mathfrak{M}_A, \mathfrak{M}_A^+), \alpha)$ in characteristic p, where $(\mathfrak{M}_A, \mathfrak{M}_A^+)$ is a polarization module, together with a symplectic level $n \geq 3$ structure α and an embedding of rings $\iota : \mathcal{O}_L \longrightarrow \mathrm{End}(A)$.

A few explanations are in order. Let $Cl(L)$ (resp. $(Cl(L)^+)$) denote the (resp. narrow) class group of L, and let h_L (resp. h_L^+) denote its order. The group $Cl(L)^+$ consists of classes of projective, rank one $\mathcal{O}_L$-module $\mathfrak{M}$, endowed with a notion of positivity. Let $\mathfrak{M}^+$ be the positive cone.

DEFINITION 3.18. *Polarization module.* Let (A, ι) be an abelian variety with RM by $\mathcal{O}_L$. Let $\mathfrak{M}_A$ denote the module of $\mathcal{O}_L$-linear, symmetric homomorphisms from A to A^t, and let $\mathfrak{M}_A^+$ denote its natural positive cone, a submodule consisting of polarizations.

The positive cone $\mathfrak{M}_A^+$ is not empty, and $\lambda \in \mathfrak{M}_A^+$ yields an embedding:

$$\mathfrak{M}_A \hookrightarrow \mathbf{Cent}_{End(A)\otimes\mathbb{Q}}(L)^{\lambda}.$$

This embedding identifies $\mathfrak{M}_A$ with a fractional ideal $\mathfrak{A}$ of L, and identifies $\mathfrak{M}_A^+$ with $\mathfrak{A}^+$. By a symplectic level n structure, we mean an isomorphism : $(\mathcal{O}_L/n\mathcal{O}_L)^2 \cong A[n]$ with the standard symplectic pairing on the left hand side corresponding to the Weil pairing on $A[n]$ coming from an $\mathcal{O}_L$-linear polarization of degree prime to p.

The $\mathcal{M}_n$ are fine moduli schemes over $\mathrm{Spec}(\mathbb{Z}[\zeta_n, \frac{1}{n}])$. They are regular 2-dimensional varieties. The coarse moduli space for abelian surfaces with RM is a scheme $\mathcal{M}$ over $\mathrm{Spec}(\mathbb{Z})$; it can be decomposed in a disjoint union of components :

$$\mathcal{M} = \sqcup_{Cl(L)^+} \mathcal{M}(\mathfrak{A}).$$

Over $\mathbb{C}$, we have $\mathcal{M}(\mathfrak{A}) \cong \mathrm{PGL}_2(\mathcal{O}_L \oplus \mathfrak{A})^+ \backslash \mathcal{H}^g$.

DEFINITION 3.19. 1. The group $\mathrm{GL}(\mathfrak{A}\oplus\mathfrak{B})^+$ consists of matrices :

$$\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,d\in\mathcal{O}_L, b\in\mathfrak{A}^{-1}\mathfrak{B}, c\in\mathfrak{A}\mathfrak{B}^{-1}, ad-bc\in(\mathcal{O}_L^\times)^+\right\}.$$

2. The group $\mathrm{SL}(\mathfrak{A}\oplus\mathfrak{B})$ is the subgroup of $\mathrm{GL}(\mathfrak{A}\oplus\mathfrak{B})$ composed of matrices of determinant one.

THEOREM 3.20. 1. *The isomorphism classes of* $(A,\iota)/\mathbb{C}$ *such that there exists an isomorphism :*

$$(\mathfrak{M}_A^+,\mathfrak{M}_A^+)\xrightarrow{\sim}(\mathfrak{C},\mathfrak{C}^+),\mathfrak{C}=(\mathcal{D}_L\mathfrak{A}\mathfrak{B})^{-1},$$

are parameterized by $\mathrm{GL}(\mathfrak{A}\oplus\mathfrak{B})^+\backslash\mathcal{H}^g$.

2. *The isomorphism classes of* $(A,\iota)/\mathbb{C}$ *together with a* given *isomorphism :*

$$m:(\mathfrak{M}_A,\mathfrak{M}_A^+)\xrightarrow{\sim}(\mathfrak{C},\mathfrak{C}^+),\mathfrak{C}=(\mathcal{D}_L\mathfrak{A}\mathfrak{B})^{-1},$$

are parameterized by

$$\mathrm{SL}(\mathfrak{A}\oplus\mathfrak{B})\backslash\mathcal{H}^g.$$

Consider a triple $(A,\iota,(\mathcal{M}_A,\mathcal{M}_A^+)\cong(\mathfrak{A},\mathfrak{A}^+))$. We can change the isomorphism giving the polarization module by an automorphism of the module with a notion of positivity : $\mathrm{Aut}_{\mathcal{O}_L}(\mathfrak{A},\mathfrak{A}^+)=\mathcal{O}_L^{\times+}$. It is also true that for every $\mu\in(\mathcal{O}_L^{\times+})^2$, $(A,\iota,\lambda:(\mathcal{M}_A,\mathcal{M}_A^+)\cong(\mathfrak{A},\mathfrak{A}^+))\cong(A,\iota,\lambda\cdot\mu)$. Summing up, the map :

$$(A,\iota,\lambda)\longrightarrow(A,\iota,(\mathcal{M}_A,\mathcal{M}_A^+))$$

has degree

$$[(\mathcal{O}_L^\times)^+:(\mathcal{O}_L^\times)^2]=[\mathrm{PGL}(\mathfrak{A}\oplus\mathfrak{B})^+:\mathrm{PSL}(\mathfrak{A}\oplus\mathfrak{B})].$$

We define $\mathcal{S}=\mathcal{S}_n$ to be the supersingular locus on $\mathcal{M}_n\otimes\overline{\mathbb{F}}_p$. We can embed the ring of integers $\mathcal{O}_L$ only in finitely many ways in the endomorphism algebra $\mathrm{End}(A)$ of a superspecial abelian variety, up to conjugation by $\mathrm{End}(A)^\times$, hence there are only finitely many superspecial points.

DEFINITION 3.21. ([72]) *A* $\Gamma_0(p)$*-level structure on* $\mathcal{M}_L(\mathfrak{A})$ *is a pair of abelian schemes* $(A,\iota,(\mathfrak{M}_A,\mathfrak{M}_A^+))$, $(A',\iota',(\mathfrak{M}'_A,\mathfrak{M}'^+_A))$ *on* $\mathcal{M}_L(\mathfrak{A})$, *and an* S*-isogeny*

$$f:(A,\iota,(\mathfrak{M}_A,\mathfrak{M}_A^+))\longrightarrow(A',\iota',(\mathfrak{M}'_A,\mathfrak{M}'^+_A))$$

such that the following diagram commutes :

$$\begin{array}{ccc} (\mathfrak{M}'_A, \mathfrak{M}^+_{A'}) & \xrightarrow{m'} & (\mathfrak{A}, \mathfrak{A}^+) \\ \downarrow f^* & & \downarrow \times p \\ (\mathfrak{M}_A, \mathfrak{M}^+_A) & \xrightarrow{m} & (\mathfrak{A}, \mathfrak{A}^+) \end{array}$$

This definition can be equivalently put in (familiar) terms of the kernel group scheme. We have three possibilities for such a subgroup scheme (see [**72**]) :

- μ_p^g;
- $(\mathbf{Z}/p\mathbf{Z})^g$;
- A unipotent group of order p^g.

We explain the equivalence : For an isogeny f, $\mathrm{Ker}(f)$ is an $\mathcal{O}_L$-invariant, isotropic subgroup of $A[p]$ of order p^g . In fact, it is totally isotropic : for we may find an $\mathcal{O}_L$-linear polarization λ of degree prime to p on A (see [**61**]). By assumption $p \cdot \lambda$ descends to $A/\mathrm{Ker}(f)$. Hence $\mathrm{Ker}(f)$ is an isotropic subgroup with respect to the Mumford pairing induced by $p \cdot \lambda$ on $\mathrm{Ker}(p \cdot \lambda)$. Since λ is of degree prime to p, it induces a perfect pairing on $A[p]$, and $\mathrm{Ker}(f)$ is thus isotropic with respect to every $\mathcal{O}_L$-linear polarization. Conversely, let H be an $\mathcal{O}_L$-invariant isotropic subgroup of order p^g of $A[p]$ with respect to every $\mathcal{O}_L$-linear polarization. There exists a unique $\mathcal{O}_L$-structure ι' on $A' = A/H$ such that $\pi : (A, \iota) \longrightarrow (A', \iota')$ is $\mathcal{O}_L$-equivariant. Suppose that $f^*(\mathcal{M}_{A'}) = p\mathcal{M}_A$. Then the isomorphism $(\mathcal{M}_{A'}, \mathcal{M}^+_{A'}) \longrightarrow (\mathfrak{A}, \mathfrak{A}^+)$ makes f into a $\Gamma_0(p)$-level structure. We denote by $\mathcal{M}_0^n(p)$ the corresponding moduli space.

DEFINITION 3.22. *(Deligne-Pappas)* Let S be a scheme. An abelian scheme with real multiplication by $\mathcal{O}_L$ (with RM) is an abelian scheme A over S together with an embedding of rings

$$\iota : \mathcal{O}_L \hookrightarrow \mathrm{End}_S(A),$$

such that the following condition holds :

$$A \otimes_{\mathcal{O}_L} \mathcal{M}_A \cong A^\vee, \quad \textbf{(DP)},$$

where $\mathcal{M}_A = \{\lambda : A \longrightarrow A^\vee : \lambda \circ \iota(r) = \iota(r)^\vee \circ \lambda, \forall r \in \mathcal{O}_L\}$.

Recall that the module $\mathcal{M}_A$ is a projective $\mathcal{O}_L$-module of rank one endowed with a natural notion of positivity determined by the cone of polarizations in $\mathcal{M}_A$.

$$\text{t}^*_{A/k} \text{ is a free } \mathcal{O}_L \otimes_{\mathbf{Z}} \underline{\mathcal{O}}_S\text{-module of rank 1, } \mathbf{(R)}$$
$$\text{and } \mathcal{M}_A \text{ is a projective } \mathcal{O}_L\text{-module of rank 1,}$$

One can show that under the assumption "p is unramified", the conditions **(DP)** and **(R)** are equivalent.

3.3. Components of the supersingular locus. Recall that we assume p is inert. In this case, the non-ordinary locus $\mathcal{V}$ is the supersingular locus $\mathcal{S}$. The components of $\mathcal{S}$ are projective lines, coming from Moret-Bailly families, that is, we consider an abelian surface X with real multiplication such that Rapoport's condition **(R)** fails; using the embedded group $\alpha_p \oplus \alpha_p \hookrightarrow X$ as a pivot to map a family of α_p parameterized by $\mathbb{P}^1$, we construct a non (iso)-trivial abelian scheme $\mathcal{X}$ over $\mathbb{P}^1$ such that Rapoport's condition holds.

The method used to count the number of components is based on [**36**]. The basic idea is the similar, with the extra twist of taking account of the endomorphism structure. The number of components is equal to the number of isomorphism classes of abelian schemes over $\mathbb{P}^1$, with relative polarization, endomorphism and level structure.

THEOREM 3.23. ([**1**]) *Let $\mathcal{S}_{d_L,n}$ be the supersingular locus on the component corresponding to the polarization module $\mathcal{D}_L^{-1}$. The number of components of $\mathcal{S}_{d_L,n}$, $n \geq 3$ is*

$$[\mathcal{M}_{d_L,n} : \mathcal{M}_{d_L,1}]\zeta_L(-1).$$

We have a corresponding mass formula (see [**1**, p.493]).

3.4. Local structure. We describe briefly the type stratification as presented in [**26**]. Let $\underline{A}$ be a point on a Hilbert modular surface $\mathcal{M}_n$. Let $\mathbf{F}$ be a finite field obtained from $\mathbf{F}_{p^2}$ to which we adjoin a primitive n-root of unity (n is the level of the symplectic structure). We denote the embeddings of $\mathcal{O}_L/p$ into $\mathbf{F}$ by $\{\sigma_1, \sigma_2\}$, ordered such that

$\sigma \circ \sigma_i = \sigma_{i+1}$. The kernel of Verschiebung :

$$\ker(V : H^0(\Omega^1_X) \longrightarrow H^0(\Omega^1_X)),$$

is a k-vector space and an $\mathcal{O}_L$-module on which $\mathcal{O}_L$ acts by a set of characters t, each with multiplicity one.

DEFINITION 3.24. The set of characters $t(\underline{A})$ is the *type* of $\underline{A}$.

The stratification follows from the type : for every $t \subseteq \{\sigma_1, \sigma_2\}$ of characters, there exists a closed subscheme W_t of $\mathcal{M}_n$, which is universal with respect to the property: $t \subseteq t(\underline{A})$. We quote, for p inert :

THEOREM 3.25. ([1, Theorem 6.1]) *(See [26] for the case $g > 2$) The set of singular points of S is exactly the set of superspecial points. Every singularity is ordinary with two branches and corresponds to the intersection of different components. The singular points are precisely the superspecial points. To every component one can assign its type in $\{1, 2\}$ such that the intersection graph of S is bipartite. Each component has exactly $p^2 + 1$ intersection points with other components.*

COROLLARY 3.26. ([1, Corollary 6.4]) *Let $n \geq 3$, p inert in L. The number of superspecial points of $S_{d_L,n}$ is*

$$\frac{p^2+1}{2}[\mathcal{M}_{d_L,n} : \mathcal{M}_{d_L}]\zeta_L(-1).$$

4. Geometric view on Hecke operators and Brandt matrices

We shall introduce the Hecke operators from a geometric point of view, using Hecke correspondences.

Let $\mathfrak{A}_1, \ldots, \mathfrak{A}_{h^+}$ be ideal representatives in the narrow class group. Let $\mathcal{M}$ be the moduli space of triples : $\underline{A} := (A, \iota, (\mathcal{M}_A, \mathcal{M}_A^+))$, where $(\mathcal{M}_A, \mathcal{M}_A^+) \cong (\mathfrak{A}_i, \mathfrak{A}_i^+)$ for some i.

We decompose $\mathcal{M}$ according to the narrow ideal classes :

$$\mathcal{M} = \sqcup_{i=1,\ldots,h^+}\mathcal{M}_i.$$

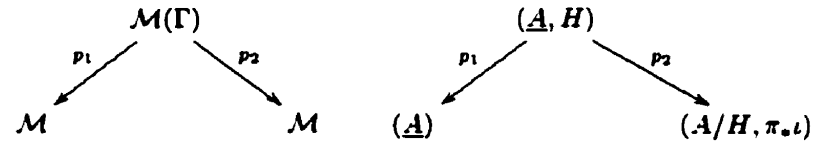
REMARK 4.1. (See [75]) Over $\mathbb{C}$, these components correspond to the groups $\mathrm{GL}_2(\mathcal{O}_L \oplus \mathfrak{a}_i)^+$:

$$\mathcal{M}(\mathbb{C}) \cong \sqcup_{i=1,\dots,n} \mathrm{GL}_2(\mathcal{O}_L \oplus \mathfrak{a}_i)^+ \backslash \mathcal{H}^g.$$

Let Γ be a finite $\mathcal{O}_L$-module of cardinality not divisible by p. Consider the coarse moduli space $\mathcal{M}(\Gamma)$ of pairs $(\underline{A}, H)$, where H is a $\mathcal{O}_L$-invariant, constant, finite subgroup scheme of A isomorphic to Γ as an $\mathcal{O}_L$-module.

Consider the diagram :

(4.1)



where $\pi : A \longrightarrow A/H$ is the natural projection, and the projections p_1, p_2 are finite flat.

The quotient of an abelian scheme with real multiplication by a finite $\mathcal{O}_L$-subgroup is again an abelian scheme with real multiplication : First, it is an abelian scheme with $\mathcal{O}_L$-action by standard facts (see [50, Section 12, Quotient by finite group schemes]). Second, the tangent space $\mathfrak{t}^*$ is locally free, because any isogeny of degree prime to p induces an isomorphism of tangent spaces.

Note that a $\Gamma_0(N)$-level structure for an abelian surface (A, ι) with real multiplication by $\mathcal{O}_L$, is a point in $\mathcal{M}(\Gamma)$, for $\Gamma = \mathcal{O}_L/(N)$.

The Hecke correspondence associated to Γ is $p_{2*} \circ p_1^*$, that is an element of $\mathcal{M}$ (on the left) is sent to the images in $\mathcal{M}$ (on the right) of its preimages in $\mathcal{M}(\Gamma)$.

We now restrict to L real quadratic.

Recall that

$$A[m] \cong_{\bar{k}} (\mathcal{O}_L/m\mathcal{O}_L)^2, \text{ for any } m \in \mathbb{N}.$$

We define Hecke operators as devices reflecting the combinatorics of embeddings of finite $\mathcal{O}_L$-modules into an abelian variety with RM.

Let

$$\mathfrak{M} = \oplus_i \mathcal{O}_L/\mathfrak{G}_i$$

be a finite $\mathcal{O}_L$-module that can be embedded into $(\mathcal{O}_L/m\mathcal{O}_L)^2$ for some m.

We can rewrite $\mathfrak{M}$ in the form :

$$\mathfrak{M} \cong \oplus_i \mathcal{O}_L/\mathfrak{p}_i^{\alpha_i},$$

for suitable prime ideal $\mathfrak{p}_i$.

By the Chinese remainder theorem, we may write $\mathfrak{M}$ using two summands only :

$$\mathfrak{M} \cong \mathcal{O}_L/\mathfrak{A} \oplus \mathcal{O}_L/\mathfrak{B},$$

with $\mathrm{val}_{\mathfrak{p}_i}(\mathfrak{A}) \geq \mathrm{val}_{\mathfrak{p}_i}(\mathfrak{B})$.

To eliminate redundancy, we will assume henceforth that all finite $\mathcal{O}_L$-modules under consideration are given in this canonical form.

DEFINITION 4.2. *(Hecke operators $T_{\mathfrak{A},\mathfrak{B}}$)* For ideals $\mathfrak{A}, \mathfrak{B} \subseteq \mathcal{O}_L$, relatively prime to p, we define the Hecke operator $T_{\mathfrak{A},\mathfrak{B}}$ by the formula :

$$T_{\mathfrak{A},\mathfrak{B}}(A) := \sum_H (A/H), \quad H \cong \mathcal{O}_L/\mathfrak{A} \oplus \mathcal{O}_L/\mathfrak{B},$$

that is, $T_{\mathfrak{A},\mathfrak{B}}$ is the operator defined by diagram (4.1) for $\Gamma = \mathcal{O}_L/\mathfrak{A} \oplus \mathcal{O}_L/\mathfrak{B}$.

We put $T_1 = 1$.

By abuse of notation, we will denote $T_{\mathfrak{A},1}$ simply by $T_{\mathfrak{A}}$.

We will call a Hecke operator $T_{\mathfrak{A},\mathfrak{B}}$ primitive if $\mathcal{O}_L/\mathfrak{A} \oplus \mathcal{O}_L/\mathfrak{B} \hookrightarrow A[\ell]$, where ℓ is a prime.

PROPOSITION 4.3. *The Hecke algebra is generated by primitive $\mathcal{O}_L$-modules:*

$$\mathbb{T} = \mathbf{Z}[T_{\mathfrak{A},\mathfrak{B}}] = \mathbf{Z}[T_{\mathfrak{A},\mathfrak{B}} : T_{\mathfrak{A},\mathfrak{B}} \textit{ primitive}]$$

REMARK 4.4. We can be more precise and give a minimal set of generators, comprised of the following :

- For l inert, $T_{l,1}$.
- For $\mathfrak{p} \cdot \overline{\mathfrak{p}} = l$ split, $T_{\mathfrak{p},1}, T_{\mathfrak{p},\mathfrak{p}}, T_{\overline{\mathfrak{p}},1}, T_{\overline{\mathfrak{p}},\overline{\mathfrak{p}}}$.
- For $\mathfrak{p}^2 = l$ ramified, $T_{\mathfrak{p},1}, T_{\mathfrak{p},\mathfrak{p}}$.

Before proving Proposition 4.3, we give some preliminary lemmas.

LEMMA 4.5. *We have the following identities :*

$$T_{\mathfrak{p},\mathfrak{p}} \circ T_{\mathfrak{p}^n,\mathfrak{p}^m} = T_{\mathfrak{p}^{n+1},\mathfrak{p}^{m+1}} = T_{\mathfrak{p}^n,\mathfrak{p}^m} \circ T_{\mathfrak{p},\mathfrak{p}},$$

and

$$T_{m,m} = id \quad \textit{for any } m \textit{ such that } (m,p) = 1.$$

PROOF. The first identity follows from the unicity of the presentation in the following (non-split) exact sequence :

$$0 \longrightarrow \mathcal{O}_L/\mathfrak{p}^n \oplus \mathcal{O}_L/\mathfrak{p}^m \longrightarrow \mathcal{O}_L/\mathfrak{p}^{n+1} \oplus \mathcal{O}_L/\mathfrak{p}^{m+1} \longrightarrow \mathcal{O}_L/\mathfrak{p} \oplus \mathcal{O}_L/\mathfrak{p} \longrightarrow 0,$$

or

$$0 \longrightarrow \mathcal{O}_L/\mathfrak{p} \oplus \mathcal{O}_L/\mathfrak{p} \longrightarrow \mathcal{O}_L/\mathfrak{p}^{n+1} \oplus \mathcal{O}_L/\mathfrak{p}^{m+1} \longrightarrow \mathcal{O}_L/\mathfrak{p}^n \oplus \mathcal{O}_L/\mathfrak{p}^m \longrightarrow 0,$$

respectively.

For the second, we need to prove that A and $A/A[m]$ are isomorphic as abelian schemes with RM. Let $(m,p) = 1$. The map $[m] : A \longrightarrow A$, is an étale, surjective morphism, hence $A \cong A/A[m]$ as abelian schemes. The natural projection $\pi : A \longrightarrow A/A[m]$ induces a map between abelian schemes with RM :

$$(A,\iota) \xrightarrow{\pi} (A/A[m], j), \quad j = \pi_* i,$$

such that for $r \in \mathcal{O}_L$,

$$j(r)(y) = \pi\iota(r)\pi^{-1}(y) = r(y) + A[m].$$

The isomorphism is given as follows :

$$\phi : (A/A[m], \pi_* i) \cong (A,\iota), \quad \phi(y + A[m]) = m \cdot y.$$

The $\mathcal{O}_L$-actions are clearly conjugate, since for $x \in A$,

$$\iota(r)(x) = \phi j(r)\phi^{-1}(x) \forall r \in \mathcal{O}_L.$$

As we mentioned earlier, since $(m,p) = 1$, there is an induced isomorphism :

$$\mathfrak{t}_A^* \cong \mathfrak{t}_{A/A[m]}^*,$$

and we are done. □

LEMMA 4.6. *Let* $\mathfrak{A} = \prod \mathfrak{p}_i^{\alpha_i}$, $\mathfrak{B} = \prod \mathfrak{p}_i^{\beta_i}$. *Then*

$$T_{\mathfrak{A},\mathfrak{B}} = \prod_i T_{\mathfrak{p}_i^{\alpha_i},\mathfrak{p}_i^{\beta_i}}.$$

PROOF. Put $\mathfrak{A} = \mathfrak{A}'\mathfrak{p}_1^{\alpha_1}$, $\mathfrak{B} = \mathfrak{B}'\mathfrak{p}_1^{\beta_1}$. Again, this sits uniquely in an exact sequence:

$$0 \longrightarrow \mathcal{O}_L/\mathfrak{A}' \oplus \mathcal{O}_L/\mathfrak{B}' \longrightarrow \mathcal{O}_L/\mathfrak{A} \oplus \mathcal{O}_L/\mathfrak{B} \longrightarrow \mathcal{O}_L/\mathfrak{p}_1^{\alpha_1} \oplus \mathcal{O}_L/\mathfrak{p}_1^{\beta_1} \longrightarrow 0,$$

hence

$$T_{\mathfrak{p}_1^{\alpha_1},\mathfrak{p}_1^{\beta_1}} \circ T_{\mathfrak{A}',\mathfrak{B}'} = T_{\mathfrak{A},\mathfrak{B}},$$

and we get the lemma by induction. □

LEMMA 4.7. *For a prime* $\mathfrak{p}$, *we have :*

$$T_{\mathfrak{p}} \circ T_{\mathfrak{p}^\alpha} = T_{\mathfrak{p}^{\alpha+1}} + (\mathrm{Norm}(\mathfrak{p}) + 1) \cdot T_{\mathfrak{p},\mathfrak{p}} \circ T_{\mathfrak{p}^{\alpha-1}},$$

PROOF. The two summands on the right correspond to the decomposition of $T_{\mathfrak{p}} \circ T_{\mathfrak{p}^\alpha}$ in "cyclic" and non-cyclic parts. By unicity of the exact sequence :

$$0 \longrightarrow \mathcal{O}_L/\mathfrak{p}^\alpha \longrightarrow \mathcal{O}_L/\mathfrak{p}^{\alpha+1} \longrightarrow \mathcal{O}_L/\mathfrak{p} \longrightarrow 0,$$

the multiplicity of $T_{\mathfrak{p}^{\alpha+1}}$ is one. Consider $T_{\mathfrak{p}} \circ T_{\mathfrak{p}^\alpha} - T_{\mathfrak{p}^{\alpha+1}}$; there is only one non-cyclic possibility is $T_{\mathfrak{p}^\alpha,\mathfrak{p}}$, and it appears with a certain multiplicity we thus calculate . Since $T_{\mathfrak{p}^\alpha,\mathfrak{p}} = T_{\mathfrak{p},\mathfrak{p}} \circ T_{\mathfrak{p}^{\alpha-1}}$, this amounts to calculate the number of embeddings:

$$\mathcal{O}_L/\mathfrak{p} \hookrightarrow \mathcal{O}_L/\mathfrak{p} \oplus \mathcal{O}_L/\mathfrak{p}.$$

This is the number of points in $\mathbb{P}^1_{\mathcal{O}_L/\mathfrak{p}}$, that is :

$$\frac{\mathrm{Norm}(\mathfrak{p})^2 + 1}{\mathrm{Norm}(\mathfrak{p}) - 1} = \mathrm{Norm}(\mathfrak{p}) + 1.$$

□

We now give the proof of Proposition 4.3 :

PROOF. We see immediately from Lemmas 4.6 and 4.7 that $T_{\mathfrak{p}}$ and $T_{\mathfrak{p},\mathfrak{p}}$ generate the primitive Hecke operators.

We will simply show that any Hecke operator $T_{\mathfrak{A},\mathfrak{B}}$ can be written as a polynomial in those terms :

According to Lemma 4.7, we may reduce to Hecke operators of the form $T_{\mathfrak{p}^\alpha,\mathfrak{p}^\beta}$. Using Lemma 4.6, we get a product of the form :

$$T_{\mathfrak{p}^\alpha,\mathfrak{p}^\beta} = T_{\mathfrak{p},\mathfrak{p}}^{\alpha-\beta} T_{\mathfrak{p}^{\alpha-\beta}}.$$

An easy induction shows that $T_{\mathfrak{p}^{\alpha-\beta}}$ is generated by primitive elements, and we are done. □

COROLLARY 4.8. *For a prime* $\mathfrak{p}$, *we have :*

$$T_{\mathfrak{p}^{\alpha_1},\mathfrak{p}^{\beta_1}} \circ T_{\mathfrak{p}^{\alpha_2},\mathfrak{p}^{\beta_2}} = \sum_{i=0}^{\inf(\alpha_1-\beta_1,\alpha_2-\beta_2)} (\mathrm{Norm}(\mathfrak{p})+1)^i \cdot T_{\mathfrak{p},\mathfrak{p}}^{i+\beta_1+\beta_2} T_{\mathfrak{p}^{\alpha_1+\alpha_2-\beta_1-\beta_2-2i}}.$$

PROOF. The composition is :

$$\begin{aligned} T_{\mathfrak{p}^{\alpha_1},\mathfrak{p}^{\beta_1}} \circ T_{\mathfrak{p}^{\alpha_2},\mathfrak{p}^{\beta_2}} &= T_{\mathfrak{p},\mathfrak{p}}^{\beta_1} \circ T_{\mathfrak{p},\mathfrak{p}}^{\beta_2} \circ T_{\mathfrak{p}^{\alpha_1-\beta_1}} \circ T_{\mathfrak{p}^{\alpha_2-\beta_2}} \\ &= T_{\mathfrak{p},\mathfrak{p}}^{\beta_1+\beta_2} \circ T_{\mathfrak{p}^{\alpha_1-\beta_1}} \circ T_{\mathfrak{p}^{\alpha_2-\beta_2}}, \end{aligned}$$

and since

$$T_{\mathfrak{p}^\alpha} \circ T_{\mathfrak{p}^\beta} = T_{\mathfrak{p}^{\alpha+\beta}} + (\mathrm{Norm}(\mathfrak{p})+1) \cdot T_{\mathfrak{p},\mathfrak{p}}(T_{\mathfrak{p}^{\alpha-1}} \circ T_{\mathfrak{p}^{\beta-1}}), \alpha, \beta \in \mathbb{N},$$

(same proof as Lemma 4.7), an easy induction yields

$$T_{\mathfrak{p}^{\alpha_1-\beta_1}} \circ T_{\mathfrak{p}^{\alpha_2-\beta_2}} = \sum_{i=0}^{\inf(\alpha_1-\beta_1,\alpha_2-\beta_2)} (\mathrm{Norm}(\mathfrak{p})+1)^i \cdot T_{\mathfrak{p},\mathfrak{p}}^{i} T_{\mathfrak{p}^{\alpha_1+\alpha_2-\beta_1-\beta_2-2i}},$$

and thus :

$$T_{\mathfrak{p}^{\alpha_1},\mathfrak{p}^{\beta_1}} \circ T_{\mathfrak{p}^{\alpha_2},\mathfrak{p}^{\beta_2}} = \sum_{i=0}^{\inf(\alpha_1-\beta_1,\alpha_2-\beta_2)} (\mathrm{Norm}(\mathfrak{p})+1)^i \cdot T_{\mathfrak{p},\mathfrak{p}}^{i+\beta_1+\beta_2} T_{\mathfrak{p}^{\alpha_1+\alpha_2-\beta_1-\beta_2-2i}}.$$

□

COROLLARY 4.9. *For Hecke operators* $T_{\mathfrak{A},\mathfrak{B}}$, $T_{\mathfrak{A}',\mathfrak{B}'}$, *we have :*

(4.2)

$$T_{\mathfrak{A},\mathfrak{B}} \circ T_{\mathfrak{A}',\mathfrak{B}'} = \sum_{\mathfrak{C} \mid gcd(\mathfrak{A}\mathfrak{B}^{-1},\mathfrak{A}'\mathfrak{B}'^{-1})} \prod_{\mathfrak{p}\mid\mathfrak{C}} \left(\left((\mathrm{Norm}(\mathfrak{p})+1) \cdot T_{\mathfrak{p},\mathfrak{p}} \right)^{\mathrm{val}_{\mathfrak{p}}(\mathfrak{C})} \cdot T_{\mathfrak{p},\mathfrak{p}}^{\mathrm{val}_{\mathfrak{p}}(\mathfrak{B}\mathfrak{B}')} \right) \cdot T_{\frac{\mathfrak{A}\mathfrak{A}'\mathfrak{B}^{-1}\mathfrak{B}'^{-1}}{\mathfrak{C}^2}},$$

where $\mathfrak{C}$ *is allowed to be the non-proper ideal* $\mathcal{O}_L = (1)$.

PROOF. We decompose the left hand side with respect to the prime decomposition of $\mathfrak{A}$ and $\mathfrak{A}'$ (Lemma 4.6) and we take the product over the primes as in Corollary 4.8. Rearranging with respect to the term $T_{\frac{\mathfrak{A}\mathfrak{A}'\mathfrak{B}^{-1}\mathfrak{B}'^{-1}}{\epsilon^2}}$ yields the above formula. □

Consider the recursion formula :

$$f_{n+1}(x) = x \cdot f_n(x) - \alpha f_{n-1}(x),$$

with $f_0 = 1$, $f_1 = x$.

LEMMA 4.10. (Generating series) *The f_n are given as coefficients of the following generating series :*

$$\sum_{n=0}^{\infty} f_n t^n = \frac{1}{\alpha t^2 - t \cdot x + 1}.$$

PROOF. This is straightforward generatingfunctionology ([**80**]); the recurrence formula :

$$\alpha \cdot f_{n-1}(x) - f_n(x) \cdot x + 1 \cdot f_{n+1}(x),$$

yields the denominator :

$$\alpha t^2 - tx + 1,$$

and the numerator of the form $a + bt$ is determined by the two first terms (the recurrence being of order three). We thus easily get $a = 1$, $b = 0$, and we are done. □

It is a corollary of the proof of Proposition 4.3 that the following holds :

$$\sum_{n=0}^{\infty} T_{\mathfrak{p}^n} t^n = \frac{1}{(\mathrm{Norm}(\mathfrak{p}) + 1)t^2 - t \cdot T_{\mathfrak{p}} + 1}.$$

We note that the degree map on Hecke operators $\deg : \mathbb{T} \longrightarrow \mathbf{Z}$ is a homomorphism. It follows that the degrees satisfy the same relations than the Hecke operators. The first few terms given by the generating series are as follow :

$$T_{\mathfrak{p}} = T_{\mathfrak{p}}$$

$$T_{\mathfrak{p}^2} = T_{\mathfrak{p}}^2 - (\mathrm{Norm}(\mathfrak{p}) + 1)T_{\mathfrak{p},\mathfrak{p}}$$

$$T_{\mathfrak{p}^3} = T_{\mathfrak{p}} \circ T_{\mathfrak{p}^2} - (\mathrm{Norm}(\mathfrak{p}) + 1)T_{\mathfrak{p},\mathfrak{p}} \circ T_{\mathfrak{p}}$$

Note that the degree of $T_{\mathfrak{p}}$ is $\mathrm{Norm}(\mathfrak{p}) + 1$, and the degree of $T_{\mathfrak{p},\mathfrak{p}}$ is 1. The first few terms are thus :

$$\deg(T_{\mathfrak{p}}) = \mathrm{Norm}(\mathfrak{p}) + 1$$

$$\deg(T_{\mathfrak{p}^2}) = (\mathrm{Norm}(\mathfrak{p}))(\mathrm{Norm}(\mathfrak{p}) + 1)$$

$$\deg(T_{\mathfrak{p}^3}) = (\mathrm{Norm}(\mathfrak{p}) - 1)(\mathrm{Norm}(\mathfrak{p}) + 1)^2$$

PROPOSITION 4.11. *The operator $T_{\mathfrak{A},\mathfrak{B}}$ preserve the type. Thus, it maps the supersingular locus to itself, and likewise the superspecial locus to itself.*

PROOF. The main idea is as follows : by construction, the ideals $\mathfrak{A}, \mathfrak{B}$ are prime-to-p, hence the Hecke operators do not modify the p-torsion, that is, a pair A_1, A_2 joined by a Hecke correspondence has isomorphic p-torsion : $A_1[p] \cong A_2[p]$ as polarized group schemes with RM, and by properties of the type, this is equivalent to $t(A_1) = t(A_2)$.

Observe that the above loci can be described by the a-number, which is a p-torsion invariant, of course. More precisely, the locus where the a-number is greater than 0 is the supersingular locus, and the locus where the a-number is greater than 1 is the superspecial locus. □

The reader will have noticed by now that we didn't construct Hecke operators in complete generality, but with a restriction with respect to p. The reason is that the Hecke correspondence T_p is quasi-finite iff p is split. See [1].

4.1. Geometric Brandt Matrices. We define in this section analogues of the classical Brandt (or Brandt-Eichler) matrices. The entries of the Brandt matrices give information on supersingular elliptic curves : the (i,j)-entry is equal to the number of subgroup schemes C of order m in E_i such that the quotient is E_j; two elliptic curves E_i and E_j are conjugate by an automorphism of k iff $i = j$ or $B_{ij}(p) = 1$. We will try to sketch a similar picture, replacing supersingular elliptic curves by superspecial abelian surfaces with RM.

Let $\mathfrak{A}$,$\mathfrak{B}$ be relatively prime to p. We define the geometric Brandt matrices with respect to the Hecke operators $T_{\mathfrak{A},\mathfrak{B}}$.

DEFINITION 4.12. *(Brandt matrix)*

Let $A_i, A_j \in \mathcal{S}$. The entry $\mathfrak{B}_{ij}(T_{\mathfrak{A},\mathfrak{B}})$ is equal to the number of $\mathcal{O}_L$-invariant subgroup schemes C isomorphic to $\mathcal{O}_L/\mathfrak{A} \oplus \mathcal{O}_L/\mathfrak{B}$ (that is, the degree of $T_{\mathfrak{A},\mathfrak{B}}$) in A_i such that $A_i/C \cong A_j$. The Brandt matrix associated to $T_{\mathfrak{A},\mathfrak{B}}$ is thus a $|\mathcal{S}|$-by-$|\mathcal{S}|$ matrix:

$$B(T_{\mathfrak{A},\mathfrak{B}})_{ij} \quad 1 \leq i, j \leq |\mathcal{S}|.$$

Since we do not have a nice Hecke correspondance for $\mathfrak{A}, \mathfrak{B}$ not prime to p, we need to give a ad hoc construction. We define $\mathfrak{B}(p)$ using Frobenius : Fr : $(A, \iota) \mapsto (A^{(p)}, \iota^{(p)}) = (A, \iota^{(p)})$.

DEFINITION 4.13. Put $\mathfrak{B}_{ij}(p) = 1$ if (A, ι_j) and $(A, \iota_i^{(p)})$ are isomorphic, i.e. iff $\iota^{(p)}$ and ι are conjugate, and 0 otherwise.

The trace of $\mathfrak{B}(p)$ is then equal to the number of superspecial abelian surfaces which lie in the prime field. Recall that every superspecial abelian surface with RM has a model over $\mathbb{F}_{p^2}$ (p.42). The matrix $\mathfrak{B}(p)$ is therefore a permutation matrix of order 2. To complete the picture, we put: $\mathfrak{B}(p^k) = \mathfrak{B}(p)^k$. In line with the elliptic case, we suggest:

CONJECTURE 4.14. *The type number of Eichlers orders of the quaternion algebra $B_{p,L}$ is equal to:*

$$t = \mathrm{Tr}\Big(\frac{\mathfrak{B}(1) + \mathfrak{B}(p)}{2}\Big).$$

Properties of the Brandt matrices:

1. • For $\mathfrak{A} = \prod \mathfrak{p}^\alpha$, $\mathfrak{B} = \prod \mathfrak{p}^\beta$, we have :

$$\mathfrak{B}_{ij}(T_{\mathfrak{A},\mathfrak{B}}) = \prod \mathfrak{B}_{ij}(T_{\mathfrak{p}^\alpha,\mathfrak{p}^\beta}).$$

• Moreover,

$$\mathfrak{B}_{ij}(T_{\mathfrak{p},\mathfrak{p}}) \cdot \mathfrak{B}_{ij}(T_{\mathfrak{p}^n,\mathfrak{p}^m}) = \mathfrak{B}_{ij}(T_{\mathfrak{p}^{n+1},\mathfrak{p}^{m+1}}),$$

and

$$\mathfrak{B}_{ij}(T_{m,m}) = Id.$$

PROOF. This is the content of Lemmas 4.6 and 4.7. □

2. The row sums of $\mathfrak{B}_{ij}(T_{\mathfrak{A},\mathfrak{B}})$ are independent of i and equal to

$$\sum_j \mathfrak{B}_{ij}(T_{\mathfrak{A},\mathfrak{B}}) = \prod_{\mathfrak{p}} (\deg T_{\mathfrak{p}^{\alpha-\beta}}),$$

for $T_{\mathfrak{A},\mathfrak{B}} = \prod T_{\mathfrak{p}^\alpha,\mathfrak{p}^\beta}$.

Moreover, $\sum_j \mathfrak{B}_{ij}(T_{\mathfrak{A},\mathfrak{B}})$ depends only on $\mathfrak{A}\mathfrak{B}^{-1}$.

PROOF. We noticed earlier that $\deg T_{\mathfrak{p},\mathfrak{p}} = 1$. □

3. If $p \neq q$ is a prime in $\mathcal{O}_L$ and $k \geq 2$, then

$$\mathfrak{B}(\mathfrak{q}^\alpha) = \mathfrak{B}(\mathfrak{q})\mathfrak{B}(\mathfrak{q}^{\alpha-1}) - (\mathrm{Norm}(\mathfrak{q}) + 1)\mathfrak{B}(\mathfrak{q}^{\alpha-2}).$$

More generally,

(4.3)
$$\mathfrak{B}(T_{\mathfrak{p}^{\alpha_1},\mathfrak{p}^{\beta_1}}) \cdot \mathfrak{B}(T_{\mathfrak{p}^{\alpha_2},\mathfrak{p}^{\beta_2}}) =$$
$$\sum_{i=0}^{\inf(\alpha_1-\beta_1,\alpha_2-\beta_2)} (\mathrm{Norm}(\mathfrak{p}) + 1)^i \cdot \mathfrak{B}(T_{\mathfrak{p},\mathfrak{p}})^{i+\beta_1+\beta_2} \mathfrak{B}(T_{\mathfrak{p}^{\alpha_1+\alpha_2-\beta_1-\beta_2-2i}}),$$

and even :

(4.4)
$$\mathfrak{B}(T_{\mathfrak{A},\mathfrak{B}}) \cdot \mathfrak{B}(T_{\mathfrak{A}',\mathfrak{B}'}) =$$
$$\sum_{\mathfrak{C} | gcd(\mathfrak{A}\mathfrak{B}^{-1},\mathfrak{A}'\mathfrak{B}'^{-1})} \prod_{\mathfrak{p}|\mathfrak{C}} \left((\mathrm{Norm}(\mathfrak{p}) + 1)^{\mathrm{val}_{\mathfrak{p}}(\mathfrak{C})} \cdot \mathfrak{B}(T_{\mathfrak{p},\mathfrak{p}})^{\mathrm{val}_{\mathfrak{p}}(\mathfrak{B}\mathfrak{B}')} \right) \cdot \mathfrak{B}(T_{\frac{\mathfrak{A}\mathfrak{A}'\mathfrak{B}^{-1}\mathfrak{B}'^{-1}}{\mathfrak{C}^2}}),$$

where $\mathfrak{C}$ is allowed to be the non-proper ideal $\mathcal{O}_L = (1)$.

PROOF. The same relations holds for the corresponding Hecke operators. □

4. The matrices $\mathfrak{B}(m)$ for $m \geq 1$ generate a commutative subring $\mathbb{T}$ of a matrix algebra.

5. The abelian surfaces A_i and A_j are conjugate by an automorphism of k iff $i = j$ or $\mathfrak{B}_{ij}(p) = 1$.

PROOF. This is immediate from the definition of the Brandt matrix $\mathfrak{B}(p)$.

□

6. Trace formula for Brandt matrices. Elliptic case :

PROPOSITION 4.15. *(See* [**58**, Proposition 4.9]*) The trace of a Brandt matrix* $B(m)$ *associated to an order of level* $N = pM$ *or* p^2M *is given by :*

$$\mathrm{Tr}B(m) = \sum_s a(s) \sum_f b(s,f) \prod_{\ell | N} c(s,f,\ell) + \delta(\sqrt{m}) Mass(\mathcal{O}),$$

where

$$\delta(\sqrt{m}) = \begin{cases} 1 & \text{if } m \text{ is a perfect square} \\ 0 & \text{otherwise} \end{cases},$$

and

$$Mass(\mathcal{O}) = \frac{p^i M}{12}(1 - \frac{1}{p^i}) \prod_{\ell | M} (1 + \frac{1}{\ell}),$$

for $\mathcal{O}$ *of level* $p^i \cdot M$.

We explain the meaning of the other terms :

Let s *run over all integers such that* $s^2 - 4m$ *is negative. Hence with some* positive *integer* t *and* squarefree *integer* r, $s^2 - 4m$ *has one of the following forms:*

$$s^2 - 4m = \begin{cases} t^2 r & 0 > r \equiv 1 \mod 4 \\ t^2 4r & 0 > r \equiv 2, 3 \mod 4 \end{cases}$$

Put $a(s) = \frac{1}{2}$. *For each fixed* s *let* f *run over all positive divisors of* t.

$$b(s,f) = h((s^2 - 4m)/f^2)\omega((s^2 - 4m)/f^2),$$

where $h(d)$ *(resp.* $(\omega(d))$ *denotes the class number of locally principal ideals (resp. half the cardinality of the unit group) of the order* $\mathcal{O}^d$ *of* $\mathbb{Q}(\sqrt{(d)})$ *of discriminant* d. *Finally,* $c(s,f,\ell)$ *is the number of inequivalent* $\mod U(\mathcal{O}_l)$ *optimal embeddings of* $\mathcal{O}_l^d$ *into* $\mathcal{O}_l$ *where* $d = (s^2 - 4m)/f^2$. *The split order* $\mathcal{O}_l$ *is congruent to* $\begin{pmatrix} \mathbf{Z}_\ell & \mathbf{Z}_\ell \\ \ell^\nu \mathbf{Z}_\ell & \mathbf{Z}_\ell \end{pmatrix}$, *where* $\nu = \mathrm{ord}_\ell(M)$.

One if left to develop a trace formula for geometric Brandt matrices.

REMARK 4.16. An explicit formula for the trace formula for Hecke operators follows from the work of Shimizu (and Selberg). See [**45**] and [**73**].

To develop a trace formula for generalized Brandt matrices, we need to develop a generalized trace formula whose residual term is the class number formula of an order of certain level (related to the congruence subgroup under consideration ($\Gamma_0(p^kN)$), the main term of the trace formulae coming from the optimal embedding theory. To pursue this avenue further, one needs a good knowledge of the Jacquet-Langlands correspondence, which for our purposes, links class numbers to spaces of cusps forms. In particular, it follows from Eichler-Shimizu-Jacquet-Langlands that

$$H(p) = 1 + \dim S_2^0(p),$$

and one can ask a similar question for higher dimensional Hilbert modular varieties. The explicit approach (using theta series) does not transpose directly, since the degree map stemming from geometric Brandt matrices is a *quartic* form, not quadratic.

CHAPTER 3

Structure and numerology of the supersingular locus

1. On certain quaternion algebras over $\mathbb{Q}(\sqrt{D})$

1.1. A case study.

LEMMA 1.1. [6, Lemma 6, p. 464] *Let L be a totally real field. Let (A, ι) be an abelian variety of dimension $g = [F : \mathbb{Q}]$ with multiplication by $\mathcal{O}_L$ over an algebraically closed field k. Then A is isogenous to B^n for some simple abelian variety B over k. Let $D = \mathrm{End}_k(B) \otimes_{\mathbf{Z}} \mathbb{Q}$, so $\mathrm{End}_k(A) \otimes_{\mathbf{Z}} \mathbb{Q} \cong M_n(D)$. Consider the case when D is a totally definite quaternion division algebra over $\mathbb{Q}$, $\dim(B) = 1$ and k has characteristic p. Then the algebra $B_{p,\infty}$ is the quaternion division algebra over $\mathbb{Q}$ ramified at p and ∞, and B is a supersingular elliptic curve over k. The centralizer of L in $\mathrm{End}_k(A) \otimes_{\mathbf{Z}} \mathbb{Q}$, $\mathbf{Cent}_{\mathrm{End}_k \otimes \mathbf{Q}}(L)$, is the quaternion division algebra over L which is ramified at all infinite places of L and all places v of L above p such that $[F_v : \mathbb{Q}_p]$ is odd, and is unramified at all other finite places. We denote it by $B_{p,L}$.*

Put $L = \mathbb{Q}(\sqrt{D})$. Decompose its ring of integers :

$$\mathcal{O}_L = \mathbf{Z} \oplus \mathbf{Z} \cdot \delta,$$

with $\delta = \frac{1+\sqrt{D}}{2}$ if $D \equiv 1 \mod 4$, $\delta = \sqrt{D}$ if $D \equiv 2, 3 \mod 4$. Let E be a supersingular elliptic curve defined over $\overline{\mathbf{F}}_p$. Its endomorphism ring $\mathrm{End}(E)$ is a maximal order in $B_{p,\infty}$. Consider the abelian surface $E \otimes_{\mathbf{Z}} \mathcal{O}_L$, defined canonically by the rule :

$$(E \otimes_{\mathbf{Z}} \mathcal{O}_L)(R) = E(R) \otimes_{\mathbf{Z}} \mathcal{O}_L, \quad R \in \overline{\mathbf{F}}_p - \text{ algebra.}$$

The isomorphism

$$E \otimes_{\mathbf{Z}} \mathcal{O}_L \cong E \times E$$

allows to write an explicit $\mathcal{O}_L$-action :

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$\delta \mapsto \begin{pmatrix} 0 & -\mathrm{Norm}(\delta) \\ 1 & \mathrm{Tr}\delta \end{pmatrix}.$$

In short, we have :

PROPOSITION 1.2. 1. *$E \otimes_{\mathbf{Z}} \mathcal{O}_L$ is a superspecial abelian surface.*

2.

$$\mathrm{End}_k(E \otimes_{\mathbf{Z}} \mathcal{O}_L) \otimes \mathbf{Q} \cong M_2(B_{p,\infty}).$$

3.

$$\mathbf{Cent}_{\mathrm{End}(E \otimes_{\mathbf{Z}} \mathcal{O}_L) \otimes \mathbf{Q}}(L) = B_{p,L} \cong B_{p,\infty} \otimes L.$$

PROOF. Only the last item requires proof : The isomorphism follows from Lemma 1.1. The equality follows from the classification of quaternion algebras over global fields (Theorem 2.3, Chapter II). □

We compute the order :

$$\mathbf{Cent}_{\mathrm{End}(E \otimes_{\mathbf{Z}} \mathcal{O}_L)}(\mathcal{O}_L) \subset B_{p,L}.$$

PROPOSITION 1.3.

$$\mathbf{Cent}_{\mathrm{End}(E \otimes_{\mathbf{Z}} \mathcal{O}_L)}(\mathcal{O}_L) \cong \mathbf{Cent}_{M_2(\mathrm{End}(E))}(\mathcal{O}_L) \cong \mathcal{O}_L \otimes \mathrm{End}(E).$$

PROOF. Let $\begin{pmatrix} \alpha_1 & \beta_1 \\ \delta_1 & \lambda_1 \end{pmatrix} \in M_2(\mathrm{End}(E))$ and $\begin{pmatrix} a & -b\mathrm{Norm}(\delta) \\ b & a + b\mathrm{Tr}\delta \end{pmatrix} \in \mathcal{O}_L \subset M_2(\mathrm{End}(E))$.

Let $\begin{pmatrix} \alpha_1 & \beta_1 \\ \delta_1 & \lambda_1 \end{pmatrix} \in \mathbf{Cent}_{M_2(\mathrm{End}(E))}(\mathcal{O}_L)$, i.e.

$$\begin{pmatrix} \alpha_1 & \beta_1 \\ \delta_1 & \lambda_1 \end{pmatrix} \begin{pmatrix} a & -b\mathrm{Norm}(\delta) \\ b & a + b\mathrm{Tr}\delta \end{pmatrix} = \begin{pmatrix} a & -b\mathrm{Norm}(\delta) \\ b & a + b\mathrm{Tr}\delta \end{pmatrix} \begin{pmatrix} \alpha_1 & \beta_1 \\ \delta_1 & \lambda_1 \end{pmatrix}.$$

Equating both sides, we obtain the following equations :

$$a\alpha_1 + b\beta_1 = a\alpha_1 - b\delta_1\mathrm{Norm}(\delta),$$

$$-\alpha_1 b\mathrm{Norm}(\delta) + \beta_1(a + b\mathrm{Tr}\delta) = a\beta_1 - b\mathrm{Norm}(\delta)\lambda_1,$$

$$a\delta_1 + b\lambda_1 = b\alpha_1 + \delta_1(a + b\mathrm{Tr}\delta),$$

$$-b\delta_1\mathrm{Norm}(\delta) + \lambda(a + b\mathrm{Tr}\delta) = b\beta_1 + \lambda_1(a + b\mathrm{Tr}\delta),$$

and these reduce to

$$\beta_1 = -\delta_1\mathrm{Norm}(\delta),$$

$$\lambda_1 = \alpha_1 + \delta_1\mathrm{Tr}\delta,$$

hence

$$\begin{pmatrix} \alpha_1 & \beta_1 \\ \delta_1 & \lambda_1 \end{pmatrix} = \begin{pmatrix} \alpha_1 & -\delta_1\mathrm{Norm}(\delta) \\ \delta_1 & \alpha_1 + \delta_1\mathrm{Tr}\delta \end{pmatrix},$$

i.e.

$$\begin{pmatrix} \alpha_1 & \beta_1 \\ \delta_1 & \lambda_1 \end{pmatrix} = \alpha_1 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \delta_1 \begin{pmatrix} 0 & \mathrm{Norm}(\delta) \\ 1 & \mathrm{Tr}\delta \end{pmatrix} \in \mathcal{O}_L \otimes \mathrm{End}(E),$$

and the converse is clear. □

Thus, we need to describe $\mathcal{O}_L \otimes \mathrm{End}(E)$. It will depend on the ramification of p in $\mathcal{O}_L$. First, we describe the quaternion algebra in which they embedd.

LEMMA 1.4. *([76, Théorème 1.3]) Let K be a (non-archimedean) local field. Let H be the unique quaternion division algebra over k, up to isomorphism. A finite extension F/K splits H iff its degree $[F : K]$ is even.*

PROPOSITION 1.5. *The quaternion algebra $B_{p,L}$ is :*

- *the totally definite quaternion algebra B_{∞_1,∞_2} ramified at both places at infinity if p is inert or ramified. Its discriminant is 1.*
- *the totally definite quaternion algebra B_S, $S = \{\mathfrak{p}, \overline{\mathfrak{p}}, \infty_1, \infty_2\}$ ramified at both places at infinity and at both primes over p if $p = \mathfrak{p} \cdot \overline{\mathfrak{p}}$. Its discriminant is $\mathfrak{p} \cdot \overline{\mathfrak{p}} = p$.*

PROOF. Let $S = \{p, \infty\}$, and consider the ramification S' of this set S in $\mathcal{O}_L$. Clearly, $\mathbf{Ram}(B_{p,L}) \subset S'$. By Lemma 1.1, $B_{p,L}$ is totally definite.

1. If p is inert or ramified, there is only one prime in $\mathcal{O}_L$ over p. Hence, by parity, $B_{p,L}$ is split over p.

2. If p is split, $p = \mathfrak{p} \cdot \bar{\mathfrak{p}}$. But for $p \neq 2$, $(d, p) = 1$

$$\left(\frac{d}{p}\right) = 1 \iff p \text{ is split in } \mathbb{Q}(\sqrt{d}) \iff [\mathbb{Q}_{\mathfrak{q}}(\sqrt{d}) : \mathbb{Q}_p] \text{ is odd , } \mathfrak{q} \text{ over } p$$

([**52**, Proposition 8.5]) hence $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ are in $\mathbf{Ram}(B_{p,L}$. Similarly, if $p = 2$,

$$[\mathbb{Q}_{\mathfrak{q}}(\sqrt{d} : \mathbb{Q}_2] \text{ is odd} \iff 2 \text{ is split in } \mathbb{Q}(\sqrt{d}), \mathfrak{q} \text{ over } 2.$$

□

PROPOSITION 1.6. 1. *The discriminant of* $\mathfrak{O} = \mathcal{O}_L \otimes \mathrm{End}(E)$ *is* p.

2. • $\mathfrak{O}$ *is an Eichler order if* p *is inert.*
   • $\mathfrak{O}$ *is maximal if* p *is split.*
   • $\mathfrak{O}$ *is none of the above if* p *is ramified..*

PROOF. 1. The discriminant of $\mathfrak{O} = \mathcal{O}_L \otimes \mathrm{End}(E)$ is p :

$$\begin{aligned} disc(\mathcal{O}_L \otimes_{\mathbb{Z}} \mathrm{End}(E)) &= disc(\mathrm{End}(E))(\mathcal{O}_L) \\ &= p\mathcal{O}_L \end{aligned}$$

since $\mathrm{Tr}_{B_{p,\infty}}(x) = \mathrm{Tr}_{B_{p,L}}(x), x \in \mathcal{O}_L \otimes \mathrm{End}(E)$.

2. • p inert.

   Using Proposition 2.18, Chapter I, Proposition 2.14, Chapter I and the fact that the maximal orders form a tree, it follows that any order in B_{∞_1,∞_2} of discriminant p is an Eichler order.

   • p split. The discriminant of $\mathfrak{O}$ is equal to the discriminant of the quaternion algebra, hence $\mathfrak{O}$ is maximal (Proposition 2.9, Chapter I).

   • p ramified.

   Lacking a more precise description, we may only say that local considerations indicates this order is not Eichler (and *fortiori*, not maximal, and this is clear from the discriminant).

□

1.2. Class number formula for Eichler orders.

PROPOSITION 1.7. [77, Théorème 3.1]

Let $\mathcal{O}$ be an Eichler order of level p.

Then the class number of $\mathcal{O}$ over $\mathbb{Q}(\sqrt{d})$ is given by the formula :

$$H(d) = h(d)\frac{\zeta_L(-1)}{2}(p^2+1) + a(d)\frac{h(-d)}{8} + b(d)\frac{h(-3d)}{12} + c(d)\frac{h(n)h(n')}{4},$$

where $a(d), b(d), c(d)$ are integers. If $c(d) \neq 0$, the norm of the fundamental unit ϵ of $\mathbb{Q}(\sqrt{d})$ is one and $n = 2 - \mathrm{Tr}(\epsilon)$ (modulo squares) and $nn' = disc(\mathbb{Q}(\sqrt{d}))$.

PROPOSITION 1.8. *([78, p.209]) Mass formula Let H/L be the totally definite quaternion division algebra, and $\mathcal{O}$ an Eichler order of L of level p. Let $\{I_i\}$ be representatives of left ideal classes of $\mathcal{O}$. If $\mathcal{O}_i$ is the right order of I_i, put $w_i = [\mathcal{O}_i^\times : R^\times]$. We have the formula :*

$$\sum \frac{1}{w_i} = h_L\frac{p^2+1}{2}\zeta_L(-1).$$

REMARK 1.9. The situation is similar to the elliptic case : the leading term of the class number formula is the mass formula, and the remainder should account for the ramification.

Compare the leading term of the class number formula with Corollary 3.26, Chapter II :

$$\frac{p^2+1}{2}[\mathcal{M}_n : \mathcal{M}_1]\zeta_L(-1) \text{ versus } \frac{p^2+1}{2}h\zeta_L(-1),$$

This suggests that the class number formula for Eichler orders over real quadratic fields actually counts (with multiplicities) superspecial points on a Hilbert modular surface. Furthermore, the weighted sum over the superspecial points would also coincide with the leading term of the class number formula, that is :

$$\sum \frac{1}{|\mathrm{Aut}(A,\iota)|} = \zeta_L(-1)h_L\frac{p^2+1}{2},$$

where the sum is over superspecial points.

REMARK 1.10. One would also expect that for p ramified, the same situation holds with the corresponding formulae :

$$\frac{1}{2}[\mathcal{M}_n : \mathcal{M}_1]\zeta_L(-1) \text{ versus } \frac{1}{2}h\zeta_L(-1),$$

and

$$\sum \frac{1}{|\mathrm{Aut}(A,\iota)|} = \frac{1}{2}\zeta_L(-1)h_L,$$

where the sum is over superspecial points.

2. $\zeta_L(-1)$ as a volume of moduli space

We denote the Hilbert modular group $\mathrm{SL}_2(\mathcal{O}_L)$ by Γ_L.

THEOREM 2.1. *(Siegel) The volume of $\Gamma_L\backslash\mathcal{H}^g$ is given by the formula :*

$$\int_{\Gamma_L\backslash\mathcal{H}^g} \omega = 2\zeta_L(-1).$$

If $\Gamma \subset \mathrm{PGL}_2^+(\mathbb{R})^g$ is commensurable with the Hilbert modular group Γ_L, one has the following formula for the volume of $\Gamma\backslash\mathcal{H}^n$:

$$vol(\Gamma\backslash\mathcal{H}^n) = [\Gamma_L : \Gamma]2\zeta_L(-1),$$

where the index $[\Gamma_L : \Gamma] \in \mathbb{Q}$ is defined as

$$\frac{[\Gamma_L : \Gamma \cap \Gamma_L]}{[\Gamma : \Gamma_L \cap \Gamma]}.$$

The Hilbert moduli space is naturally decomposed in h^+ components, parametrized by the groups $\mathrm{SL}_2(\mathcal{O}_L \oplus \mathfrak{a}_i)$, for $\mathcal{O}_L, \ldots, \mathfrak{a}_{h^+}$ representatives of the narrow class groups $Cl(L)^+$. Siegel's theorem states that the volume of the component associated to $\mathrm{SL}_2(\mathcal{O}_L \oplus \mathcal{O}_L)$ is $2\zeta_L(-1)$. The next proposition shows that all components have the same volume. Note that this requires justification, because the groups $\mathrm{SL}_2(\mathcal{O}_L \oplus \mathfrak{a}_i)$ and $\mathrm{SL}_2(\mathcal{O}_L \oplus \mathfrak{a}_j)$ will be conjugate iff $[\mathfrak{a}_i] = [\mathfrak{a}_j]$ in the genus group ($(Cl(L)^+/Cl(L)^{+2})$ (see [75, p.12]), and the volume is of course the same for conjugate groups; the point is that the volume doesn't depend on this data.

PROPOSITION 2.2. Volume computation

$$vol(\Gamma(\mathfrak{A})) = vol(\Gamma_L \backslash \mathcal{H}^g) = 2\zeta_L(-1).$$

PROOF. The idea is to combine [**75**, Chapter V, Theorem 5.1] and [**75**, Appendix to chapter V] in a straightforward way. Given $\Gamma = \Gamma(\mathfrak{A})$, the Theorem 5.1 stipulated that a certain generating series:

$$\frac{1}{4} vol(\Gamma \backslash \mathcal{H}^2) + \sum_{n=1}^{\infty} a_n q^n,$$

with constant coefficient $\frac{1}{4} vol(\Gamma \backslash \mathcal{H}^2)$ is in fact equal to the Eisenstein series of weight two in $M_2^{\gamma}(\Gamma_0(D), \chi_D)$ with γ the genus of $\mathfrak{A}$, $\mathcal{O}_L = \mathbb{Q}(\sqrt{D})$. The calculation of the Appendix in question yields that the associated Eisenstein series has q-expansion :

$$\frac{1}{2}\zeta_L(-1) + \sum_{n=1}^{\infty} a_n q^n.$$

Equalling the constant terms yields the result. □

REMARK 2.3. The volume associated to the Hilbert modular group Γ_L satisfies the properties of a "generalized" Euler characteristic, i.e. it is real-valued, and for any subgroup $\Gamma < \Gamma_L$ of finite index, $vol(\Gamma) = [\Gamma_L : \Gamma] \cdot vol(\Gamma_L)$. As we noticed earlier, since $vol(\Gamma_L) > 0$, two conjugate subgroups of finite index have actually the same index.

REMARK 2.4. **Other proofs of Proposition 2.2** The most elementary is to calculate directly the number $[\Gamma_L : \Gamma]$, and check that it is indeed equal to one. One can also use the fact that the Tamagawa number of $\mathrm{SL}_2(\mathcal{O}_L \oplus \mathfrak{A})$ is equal to 1. A third proof uses the fact that for any Γ a discrete subgroup commensurable with the Hilbert modular group, the Euler number of $\Gamma \backslash \mathcal{H}^2$ is constant and equal to the volume (see [**75**, Chapter IV, Theorem 1.2, p.60-61]).

REMARK 2.5. *Pure group theory.* One can see $[\Gamma_L : \Gamma] \cdot 2\zeta_L(-1)$ is the Euler number of Γ also in the sense of (rational) cohomology theory of groups.

3. Intersection theory

Let $\mathcal{M}_p$ be the Hilbert modular surface of principally polarized abelian surfaces with RM by $\mathcal{O}_L$, L quadratic over $\mathbb{Q}$, in characteristic p. We assume p inert as usual.

We present a different method to count the components of the supersingular locus. We follow the exposition of [**28**] . Let c_1, c_2 be the Chern classes of $\Omega^1_{\mathcal{M}}{}^{\bullet} = \mathfrak{t}_{\mathcal{M}}$, the tangent sheaf of $\mathcal{M}$. Note that c_1 is a canonical divisor. By the theorem of Siegel (Proposition 2.2), using the smoothness of the moduli scheme over $\mathbf{Z}_p$ whose special fibre is $\mathcal{M}_p$, we have ([**75**]) :

$$c_1^2 = 2c_2, \quad c_2 = 2\zeta_L(-1).$$

By the Kodaira-Spencer isomorphism, we have :

$$\Omega^1_{\mathcal{M}} \cong \underline{\omega}^{\otimes 2},$$

as $\mathcal{O}_L \otimes \mathcal{O}_{\mathcal{M}_p}$-modules, where $\underline{\omega}$ is the relative cotangent bundle of the universal abelian scheme

$$\pi : \mathcal{A}_p \longrightarrow \mathcal{M}_p,$$

so $\underline{\omega} = \pi_* \Omega^1_{\mathcal{A}_p/\mathcal{M}_p}$.

Let h denote the (total) Hasse invariant. Thus h is a section of $(\det \underline{\omega}^{\otimes p-1})$. Hence,

$$(h) = -\frac{p-1}{2} c_1, c_1 = c_1(\det \Omega^1_{\mathcal{M}}{}^{\bullet}).$$

3.0.1. *Number of components.* If we put aside for a moment problems arising from non-rigid level structure, we have on the one hand :

$$(p-1)c_1^2 = 4(p-1)\zeta_L(-1).$$

On the other hand,

$$(p-1)c_1^2 = (-2c_1) \cdot (-\frac{p-1}{2} c_1) = -2c_1 \cdot (h).$$

By [**47**, p. 137], using the Kodaira-Spencer isomorphism, one gets :

$$c_1 \text{| component of } (h) = 2 \cdot (p-1).$$

So

$$(p-1){c_1}^2 = 4 \cdot (\frac{1}{2}c_{1|\text{ component of }(h)}) \cdot \#(\text{ components }),$$

hence the number of components is given by $\zeta_L(-1)$.

3.0.2. *Number of superspecial points.* Under the hypotheses that there exists p^2+1 superspecial points on every component and that all have a fixed number b of branches, we use the adjunction formula to calculate b. We will clear those hypotheses in the next section.

We have :

$$(h)^2 = (\frac{p-1}{2})^2 c_1^2 = (p-1)^2 \zeta_L(-1).$$

On the other hand, if we write $(h) = \cup_{i=1}^{\zeta_L(-1)} D_i$ (the divisor is reduced by [**27**, Section 1.2]), then

$$(h)^2 = \sum_{i \neq j} D_i \cdot D_j + \sum_i D_i \cdot D_i.$$

By the adjunction formula,

$$D_i^2 = 2g(D_i) - 2 - c_1 \cdot D_i = -2 - 2(p-1) = -2p.$$

Also,

$$\sum_{i \neq j} D_i \cdot D_j = \#\text{ components } \cdot \#\text{ singular points on a components } \cdot (b-1)$$

$$= (p^2+1)\zeta_L(-1) \cdot (b-1).$$

Thus,

$$(p-1)^2 \zeta_L(-1) = ((p^2+1)(b-1) - 2p)\zeta_L(-1),$$

hence $b = 2$.

Summing up, we can count the number of superspecial points on the whole moduli space this way : we have $\zeta_L(-1)$ components, with p^2+1 points on every component, and there are two branches crossing at each superspecial points. Furthermore, there are h_L^+ components, hence in the SL_2-case, the total number of superspecial points is :

$$\frac{\zeta_L(-1)}{2}(p^2+1)h_L^+.$$

4. Moret-Bailly families with RM

We try doing the study of the supersingular locus for arbitrary polarized abelian varieties with RM and for arbitrary characteristic (i.e. for $p = 2$ as well). In fact the latter is merely a remark. The argument uses the following implication . For X a polarized superspecial abelian surface, $\mathcal{L}$ such that $K(\mathcal{L}) = \mathrm{Ker}(\phi_{\mathcal{L}} : X \longrightarrow X^t) = X[p]$, if $H \subset K(\mathcal{L})$ is of order p, then H is isotropic for $e^{\mathcal{L}} : K(\mathcal{L}) \times K(\mathcal{L}) \longrightarrow \mathbb{G}_m$ (i.e. $e^{\mathcal{L}}(H, H) = 1$), hence the polarization $\phi_{\mathcal{L}}$ descends to X/H. The argument for $p > 2$ is there are no nontrivial skew-symmetric bihomomorphisms:

$$e : K(\mathcal{L}) \times K(\mathcal{L}) \longrightarrow \mathbb{G}_m,$$

so $e^{\mathcal{L}} : H \times H \longrightarrow \mathbb{G}_m$ is necessarily trivial. But this argument is *false* when $H = \alpha_2$! There exists non-trivial maps :

$$\alpha_2 \times \alpha_2 \longrightarrow \mathbb{G}_m.$$

See [3] for the interesting consequences of this fact .

To explain our point with precision, we need to introduce the following definition :

DEFINITION 4.1. [50, Section 23] A Heisenberg group is a system of group schemes and homomorphisms :

$$0 \longrightarrow \mathbb{G}_m \xrightarrow{i} G \xrightarrow{\pi} K \longrightarrow 0,$$

such that

- K is commutative (but G need not be);
- there exists an open covering $\{U_i\}$ of K and sections σ_i of π ;
- i is a closed immersion, making $\mathbb{G}_m$ into the kernel of π ;
- $\mathbb{G}_m \subset$ the center of G.

We cite another theorem in [50] to explain how theta-groups arise :

THEOREM 4.2. *([50, Theorem 1, p.225]) Let $\mathcal{L}$ be a line bundle on an abelian variety X/k. For any scheme S, let* $\mathrm{Aut}(\mathcal{L}/X)(S)$ *be the group of automorphisms of $S \times_k \mathcal{L}$ covering a translation map of $S \times_k X$.* $\mathrm{Aut}(\mathcal{L}/X)$ *is a contravariant group-valued functor*

on the category of schemes. There exists a group scheme $\mathcal{G}(\mathcal{L})$ and an isomorphism of group functors:

$$\mathrm{Aut}(\mathcal{L}/X) \cong \mathcal{G}(\mathcal{L}).$$

Furthermore, for any scheme S, the natural homomorphisms of groups :

$$0 \longrightarrow H^0(S, \mathcal{O}_S^\times) \longrightarrow \mathrm{Aut}(\mathcal{L}/X)(S) \longrightarrow \mathcal{K}(\mathcal{L}) \longrightarrow 0,$$

where

$$\mathcal{K}(\mathcal{L}) = \left\{ S - \text{valued points } f : S \longrightarrow X \text{ such that } T_f^*(S \times \mathcal{L}) \cong S \times \mathcal{L} \right\},$$

induces homomorphisms of group schemes:

$$0 \longrightarrow \mathbb{G}_m \xrightarrow{i} \mathcal{G}(\mathcal{L}) \xrightarrow{j} K(\mathcal{L}) \longrightarrow 0,$$

making $\mathcal{G}(\mathcal{L})$ into a Heisenberg group.

REMARK 4.3. We may view $\mathcal{G}(\mathcal{L})$ alternatively either as the group $\{\phi | \phi : \mathcal{L} \longrightarrow \mathcal{L}\}$, such that ϕ is an isomorphism of $\mathcal{L}$ that covers a translation map on the base and induces a linear map on fibers, or equivalently as the set of pairs (ψ, a) where $a \in A$ and $\psi : \mathcal{L} \longrightarrow T_a^*\mathcal{L}$ is an isomorphism. With respect to this definition, the group $K(\mathcal{L})$ is defined as $\{a : T_a^*\mathcal{L} \cong \mathcal{L}\}$.

FACT 4.4. $\deg(\mathcal{L}) = \dim_k \Gamma(A, \mathcal{L})$, and $|K(\mathcal{L})| = (\deg(\mathcal{L}))^2$.

Now, since $\mathbb{G}_m$ is in the center of $\mathcal{G}(\mathcal{L})$, we may define an alternating bilinear pairing, the *Mumford pairing* :

$$e^{\mathcal{L}} : K(\mathcal{L}) \times K(\mathcal{L}) \longrightarrow \mathbb{G}_m$$

as the bihomomorphism associated to the commutator in the Heisenberg group $\mathcal{G}(\mathcal{L})$, that is :

$$e^{\mathcal{L}}(x, y) = [\tilde{x}, \tilde{y}],$$

where $\tilde{x}, \tilde{y}$ are lifts of x and y (resp.) to $\mathcal{G}(\mathcal{L})$, and $[a, b] = aba^{-1}b^{-1}$.

Another argument, including the case $p = 2$, goes as follows : according to [**50**, Lemma 1], if $K(\mathcal{L})$ is finite of prime order, then G is commutative, hence its commutator, being $e^{\mathcal{L}}$ is necessarily trivial.

Consider the natural projection $X \xrightarrow{\pi} X/H$. Since $H \subset K(\mathcal{L})$ and $e^{\mathcal{L}}|_{H\times H} = 1$, it follows from [**50**, Theorem 2], say, that there exists a line bundle $\mathcal{M}$ on Y such that $\pi^*\mathcal{M} \cong \mathcal{L}$, hence the polarization $\phi_{\mathcal{L}}$ descends to a polarization $\phi_{\mathcal{L}_H}$ on X/H, and we are finished proving the proposition :

PROPOSITION 4.5. *Let (X, μ) be a polarized abelian variety over an algebraically closed field of characteristic p, such that* $\mathrm{Ker}(\mu)$ *contains a subgroup scheme H of order p. Then the polarization descends to a polarization on X/H.*

We described earlier the $\Gamma_0(p)$-level structure for abelian schemes with real multiplication. We want to expose the details of the construction of Moret-Bailly in more general contexts. We consider certains abelian varieties with RM by $\mathcal{O}_L$, and a subgroup scheme H of A which is $\mathcal{O}_L$-invariant, of order p^2, killed by p and totally isotropic (i.e. isotropic with respect to any $\mathcal{O}_L$-linear pairing). Moduli theoretically, this is a point on the fibre of the morphism :

$$\mathcal{M}_0^n(p) \longrightarrow \mathcal{M}_L^n$$

over the moduli point of A. For a suitable choice of A and H, one obtains an abelian scheme with RM by $\mathcal{O}_L$:

$$\mathcal{X} \longrightarrow \mathbb{P}^1.$$

We now give the details of this construction. Let p be inert. This restriction implies that the non-ordinary locus coincides with the supersingular locus $\mathcal{S}$, which is given by the vanishing of the determinant of the Hasse-Witt matrix (one equation), hence it is a divisor (see [**30**]). As we have seen earlier, there are only finitely many superspecial points in $\mathcal{S}$. Thus, generically, the a-number is 1 in the non-ordinary locus. Let $A = (A_x, \iota_x, \lambda : (\mathfrak{M}_A, \mathfrak{M}_A^+) \cong (\mathfrak{A}, \mathfrak{A}^+))$ with a-number equal 1. We want to prove that A lies in a suitable Moret-Bailly family.

REMARK 4.6. It is sufficient to prove that the Frobenius transform $A^{(p)}$ of A lies on a projective line.

DEFINITION 4.7. The group :

$$\alpha(A) = \mathrm{Ker}(\mathrm{Ver} : A \longrightarrow A^{(\frac{1}{p})}) \cap \mathrm{Ker}(\mathrm{Fr} : A \longrightarrow A^{(p)}),$$

is called the alpha group of A.

Let $\alpha(A_x)$ be the alpha group of A_x. Since the a-number of A is 1, the alpha group is isomorphic to α_p. It is a characteristic subgroup, and therefore the action of $\mathcal{O}_L$ descends to an abelian variety with RM $A' = A_x/\alpha$: since the alpha group is contained in the kernel of Ver and Fr. Thus, we can consider the polarized abelian variety $A' = (A_x/\alpha(A_x), \lambda_\alpha)$.

We note the following points

1. The abelian variety A' has RM, but the cotangent space $\mathfrak{t}^*_A$ is *not* a free $\mathcal{O}_L$-module (Rapoport's condition fails), which implies that every subspace of $H^0(A, \Omega^1_A)$ is $\mathcal{O}_L$-invariant. Consider the exact sequence :

$$0 \longrightarrow H^0(A, \Omega^1_A) \longrightarrow H^1_{dR}(A) \longrightarrow H^1(A, \mathcal{O}_A) \longrightarrow 0.$$

These modules are always Dieudonné modules of group schemes, and we can write :

$$0 \longrightarrow \mathbb{D}(\mathrm{Ker}(\mathrm{Fr})) \longrightarrow \mathbb{D}(A[p]) \longrightarrow \mathbb{D}(\mathrm{Ker}(\mathrm{Ver})) \longrightarrow 0,$$

where $\mathbb{D}$ denotes the (covariant) Dieudonné functor. The cotangent space $\mathfrak{t}^*_A$ is the zeroth cohomology group $H^0(A, \Omega^1_A)$, and p acts as 0 on it. The finite $\mathcal{O}_L$-module $\mathcal{O}_L/p = \mathbb{F}_{p^2}$ acts in two ways $(\chi_1, \chi_2) = (\chi_1, \sigma \circ \chi_1)$ (σ is the Frobenius) on the cotangent space. To show that Rapoport's condition fails, we describe $(A/\alpha(A))[\mathrm{Fr}]$. Let $B = A/\alpha(A)$, and let

$$\mathbf{V} = \mathbb{D}(\alpha(B)) := \mathbb{D}\Big((\mathrm{Fr}^{-1}(\alpha(A)) \cap \mathrm{Ver}^{-1}(\alpha(A)))/\alpha(A)\Big).$$

It follows from [**13**, p.68] that $H^1_{dR}(A) \cong \mathbb{D}(A[p])$ is a free $\mathcal{O}_L \otimes k$-module of rank 2. We therefore get a decomposition:

$$\mathbb{D}(A[p]) = W_1 \oplus W_2,$$

where W_i is a 2-dimensional k-vector space, with the $\mathcal{O}_L$-action given by the character χ_i (see [**25**, Section 2.6, p.291] for more details). The behaviour of Fr and Ver with respect to this decomposition is :

$$F(W_i) \subseteq W_{i+1}, \quad \mathrm{Ver}(W_i) \subseteq W_{i+1}.$$

This follows from the σ-linearity of Frobenius and σ^{-1}-linearity of Verschiebung. For example, for $r \in \mathcal{O}_L, v_1 \in W_1$, we have:

$$r\mathrm{Fr}(v_1) = \mathrm{Fr}r(v_1) = \mathrm{Fr}(\chi_1(r)v_1) = \chi_1(r)^p\mathrm{Fr}(v_1) = \chi_2(r)\mathrm{Fr}(v_1) \in W_2.$$

It is true in general that for any abelian variety A,

$$\mathrm{Im}\mathrm{Ver} = \mathrm{Ker}\mathrm{Fr}, \quad \mathrm{Im}\mathrm{Fr} = \mathrm{Ker}\mathrm{Ver} \quad \text{on } \mathbb{D}(A[p]).$$

Without loss of generality, we can assume that $\mathrm{Ker}\mathrm{Fr} \cap \mathrm{Ker}\mathrm{Ver} = \mathbb{D}(\alpha(A)) \subseteq W_2$.

We claim that

$$\mathrm{Fr}(W_1) = \mathrm{Ver}(W_1) = \mathbb{D}(\alpha(A)). \tag{4.1}$$

Since $\mathrm{Im}(\mathrm{Fr}) = \mathrm{Ker}(\mathrm{Ver})$, $\mathrm{Fr}(W_1) \subseteq \mathrm{Ker}\mathrm{Ver} \cap W_2 = \mathbb{D}(\alpha(A))$. The kernel of Frobenius is a 1-dimensional vector space, hence non zero, and by dimension considerations, $\mathrm{Fr}(W_1) = \mathbb{D}(\alpha(A))$, similarly $\mathrm{Ver}(W_1) = \mathbb{D}(\alpha(A))$.

Recall that the dimension of $\mathbb{D}(A[p])$ is 4, and the dimension of the kernel of Frobenius is 2, hence Equation 4.1 implies that the rank of $\mathrm{Fr}^{-1}(\mathbb{D}(\alpha(A))$ is at most 3, because $\mathbb{D}(\alpha(A)$ is one-dimensional. But since it visibly contains $W_1 \oplus \mathbb{D}(\alpha(A))$ and this is already of dimension 3, we have :

$$\mathrm{Fr}^{-1}(\mathbb{D}(\alpha(A)) = W_1 \oplus \mathbb{D}(\alpha(A)).$$

Similarly,

$$\mathrm{Ver}^{-1}(\mathbb{D}(\alpha)) = W_1 \oplus \mathbb{D}(\alpha(A)).$$

We then conclude that

$$\begin{aligned}
\mathbf{V} &= \mathbb{D}(\alpha(B)) \\
&= \mathbb{D}\Big(\mathrm{Fr}^{-1}(\mathbb{D}(\alpha(A))) \cap \mathrm{Ver}^{-1}(\mathbb{D}(\alpha(A)))/\alpha(A)\Big) \\
&\cong \mathbb{D}(\mathrm{Fr}^{-1}(\mathbb{D}(\alpha(A)))) \cap \mathbb{D}(\mathrm{Ver}^{-1}(\mathbb{D}(\alpha(A))))/\mathbb{D}(\alpha(A)) \\
&\cong W_1 \oplus \mathbb{D}(\alpha(A))/\mathbb{D}(\alpha(A)) \\
&\cong W_1
\end{aligned}$$

Note that Frobenius and Verschiebung both act as 0 on W_1, and the $\mathcal{O}_L$-action is given by χ_1. Moreover, $\mathbf{V} = \mathbb{D}(B[\mathrm{Fr}])$. This argument also shows that the a-number of A' is equal to the dimension of W_1, that is, two.

2. We just proved that the a-number of A' is equal to 2, that is, the abelian variety is superspecial. The morphism Ver is identically zero on $H^0(A, \Omega^1_A)$, and every subspace of $H^0(A, \Omega^1_A)$ is Ver, Fr, and $\mathcal{O}_L$-stable, hence every embedded α_p in A' is $\mathcal{O}_L$-invariant. The various subgroup schemes isomorphic to α_p in a superspecial abelian variety are parametrized by $\mathbb{P}^1$, so we consider the family (see page 48) :

$$(A' \times \mathbb{P}^1)/\{\alpha_t\}_{t\in\mathbb{P}^1}.$$

Note that since any α_p is $\mathcal{O}_L$-stable, the action of $\mathcal{O}_L$ descends to the quotient. We get an abelian scheme $\mathcal{X} \xrightarrow{\pi} \mathbb{P}^1$ which satisfy Rapoport's condition, and we claim that one fibre of π is $A^{(p)}$. We first check locally that Rapoport's condition holds. The argument uses the same idea as in point 1.

Let $H \cong \alpha_p$. We want to show that Rapoport's condition holds for B/H. Let us write $\mathbb{D}(B[p]) = W_1 \oplus W_2$. We saw above that $\mathbb{D}(\alpha(B)) = W_1$, and $\mathrm{Fr}(W_1) = \mathrm{Ver}(W_1) = 0$. Since the rank of the homomorphisms Fr and Ver is p^2, on the level of Dieudonné module their kernel is of dimension two. Hence

$$W_1 = \mathrm{KerFr} = \mathrm{KerVer},$$

and

$$\mathrm{Fr} : W_2 \cong W_1, \quad \mathrm{Ver} : W_2 \cong W_1.$$

Put $Z_1 = H \cong \alpha_p$ and Z_2 the image of Z_1 (under Frobenius or Verschiebung) in W_2. Then by dimension count,

$$\begin{aligned}\mathbb{D}((B/H)[\mathrm{Fr}]) &= \mathrm{Fr}^{-1}(\mathbb{D}(H))/\mathbb{D}(H)\\ &= (W_1 \oplus Z_2)/Z_1\\ &\cong W_1/Z_1 \oplus Z_2,\end{aligned}$$

with $\mathcal{O}_L$ acting on W_1/Z_1 via χ_1 and $\mathcal{O}_L$ acting on Z_2 via χ_2, and we are done. Now, there is a unique way to embed $\alpha(A) \subseteq \mathrm{Ker}(\mathrm{Fr}_A) \subset A$, and we claim that $\beta \subset \mathrm{KerFr}_A/\alpha(A) \cong \alpha_p \subseteq A'$. This isomorphism follows since for any base field, any local-local group scheme of rank p is isomorphic to α_p (recall that local-local means that Fr and Ver acts nilpotently, and for any supersingular abelian variety, Ker(Fr) is annihilated by some power of Ver).

We get that

$$A'/\beta \cong A/\mathrm{Ker}(\mathrm{Fr}) = A^{(p)}.$$

In fact, A'/β with its $\mathcal{O}_L$-structure is $(A^{(p)}, \iota^{(p)})$. It follows that we may take $\lambda^{(p)}$ and get $(A^{(p)}, \iota^{(p)}, \lambda^{(p)})$ on the Moret-Bailly family $\mathcal{X} \longrightarrow \mathbb{P}^1$.

Summarizing, we have the following theorem :

THEOREM 4.8. *Let p be inert. Every component of the supersingular locus of the moduli space of (non-necessarily principally) polarized abelian surfaces with level $n \geq 3$ structure is a Moret-Bailly family, that is a family of supersingular varieties parametrized by the projective line $\mathbb{P}^1$.*

4.1. Local picture. It follows from the Serre-Tate theorem (2.7, Chapter II) that there is an equivalence of categories between the isomorphism classes of deformations of points(A, λ, α) on the Siegel moduli scheme to R and the corresponding isomorphism classes of deformations of the principally polarized p-divisible groups to R. Similarly, there is an equivalence of categories between the isomorphism classes of deformations of points (A, ι, α) on the Hilbert moduli scheme and the corresponding isomorphism classes of deformations of the p-divisible groups with real multiplication to R.

Since the equivalence of categories (following Serre-Tate) is insensitive to the polarization module, it follows that the local picture is the same as in the principally polarized case.

4.2. Counting points and components. Let us recapitulate the situation when the polarization is not necessarily principal :

1. the local picture is the same as in the principally polarized case. Namely, there are $[\mathcal{M}_{d_L,n} : \mathcal{M}_{d_L}]\zeta_L(-1)$ components, the intersection points are equal the superspecial points and there are $p^2 + 1$ of them. Each intersection is transversal with two branches. See Section 3, Chapter III.
2. Every component of S is parametrized by a projective line.

Indeed, the local picture is the same as in the principally polarized case, and this validates the appearance of the class number h_L in the formula counting the number of

superspecial points, since the map

$$(A, \iota, \lambda) \longrightarrow (A, \iota, (\mathcal{M}_A, \mathcal{M}_A^+))$$

has degree

$$[(\mathcal{O}_L^\times)^+ : (\mathcal{O}_L^\times)^2] = [\mathbf{PGL}(\mathfrak{A} \oplus \mathfrak{B})^+ : \mathbf{PSL}(\mathfrak{A} \oplus \mathfrak{B})] = \frac{h_L^+}{h_L}.$$

So the formulae for non-necessarily principally polarized case ($\mathbf{GL}_2$) are the same as in the principally polarized ($\mathbf{SL}_2$) case, replacing h_L^+ by h_L.

CHAPTER 4

Tensor constructions

1. Axiomatics of tensor construction

The matching between the number of superspecial points on the Hilbert modular surface in characteristic p (p inert) given in Section I, Chapter IV, and the class number formula for ideal of the non-maximal order of $B_{p,L}$ appearing as $\mathbf{Cent}_{E\otimes\mathcal{O}_L}(\mathcal{O}_L)$ given in Section II, Chapter IV, suggest that a direct equivalence of category between ideals and superspecial points should exist, as in the case of elliptic curves. We study in the section constructions involving tensoring an abelian variety by a finitely generated projective (left) module (under a ring action), in order to try systematizing (algebraically) the link between class numbers and isomorphism classes of superspecial abelian varieties.

DEFINITION 1.1. A ring is *left hereditary* if every left ideal is projective.

Let $\mathcal{O}$ be a left noetherian, left hereditary ring acting on A (i.e. we are provided with an injection in the endomorphism ring). In pratice, we are more precisely interested in Eichler orders of totally definite quaternion algebras.

DEFINITION 1.2. Let M be a finitely generated left ideal of $\mathcal{O}$. The tensor construction in question is a group functor $A\otimes_{\mathcal{O}} M$, with A an abelian variety with RM by $\mathcal{O}_L$. We define it with the formula :

$$(A\otimes_{\mathcal{O}} M)(S) = A(S)\otimes_{\mathcal{O}} M, \tag{1.1}$$

where S is a scheme over $\mathcal{O}$.

We construct $A\otimes_{\mathcal{O}}\mathfrak{A}$ as follows (see [74]) :

Let $\mathfrak{A}$ be of finite index in a free $\mathcal{O}$-module. For free $\mathcal{O}$-module $\mathfrak{A}\cong\mathcal{O}^n$, we pick a basis $e_1,\ldots,e_n$ and we define

$$A\otimes_{\mathcal{O}}\mathfrak{A}\cong A^n.$$

If $\mathfrak{b} \subset \mathcal{O}$ is a fractional ideal, there is a canonical isomorphism :

$$(A \otimes_{\mathcal{O}} \mathfrak{A})[\mathfrak{b}] \cong A[\mathfrak{b}] \otimes_{\mathcal{O}} \mathfrak{A}.$$

In general, if $\mathfrak{b}\mathfrak{A}' \subset \mathfrak{A} \subset \mathfrak{A}'$, $\mathfrak{A}'$ free and $\mathfrak{b}$ a non-zero ideal of $\mathcal{O}$, then:

$$A \otimes_{\mathcal{O}} \mathfrak{A} := (A \otimes_{\mathcal{O}} \mathfrak{b}\mathfrak{A}')/(A[\mathfrak{b}] \otimes_{\mathcal{O}} \mathfrak{A}/\mathfrak{b}\mathfrak{A}'),$$

independently of the choice of the superideal $\mathfrak{A} \subset \mathfrak{A}'$. We get the same canonical isomorphism :

$$A \otimes_{\mathcal{O}} \mathfrak{A}[\mathfrak{b}] \cong A[\mathfrak{b}] \otimes_{\mathcal{O}} \mathfrak{A}.$$

If $\mathfrak{A}$ has an action of $\mathcal{O} \longrightarrow K$, then $A \otimes_{\mathcal{O}} K$ canonically inherits this action.

If $\lambda : A \longrightarrow A^t$ is a polarization, and $f : \mathfrak{A} \longrightarrow \mathfrak{A}^\vee$ is a $\mathcal{O}$-linear map then $\lambda \otimes f$: $A \otimes_{\mathcal{O}} \mathfrak{A} \longrightarrow A^t \otimes_{\mathcal{O}} \mathfrak{A}^\vee$ is a polarization.

REMARK 1.3. We also have a canonical isomorphism of λ-adic Tate modules :

$$T_\lambda(A \otimes_{\mathcal{O}} \mathfrak{A}) \longrightarrow (T_\lambda A) \otimes_{\mathcal{O}} \mathfrak{A}.$$

When M is a projective rank 1 $\mathcal{O}$-module and A has RM, the functor $A \otimes_{\mathcal{O}} M$ is represented by an abelian variety with RM of the same dimension as A.

For the convenience of the reader, we reproduce the exposition found in [**22**, Proposition 1.2.7].

1. :

This is similar to the previous construction :

We write down a free resolution of $\mathfrak{A}$:

$$\cdots \longrightarrow \oplus^m \mathcal{O} \longrightarrow \oplus^n \mathcal{O} \longrightarrow \mathfrak{A} \longrightarrow 0.$$

Since $\mathfrak{A}$ is projective, $\oplus^n\mathcal{O}$ splits into $\mathfrak{A} \oplus \mathfrak{p}$, where $\mathfrak{p}$ is a projective $\mathcal{O}$-module. The map :

$$\oplus^m\mathcal{O} \longrightarrow \mathfrak{p},$$

gives a splitting $\oplus^m\mathcal{O}$ as $\mathfrak{p} \oplus \mathfrak{q}$. Thus, we have an exact sequence :

$$\cdots \leftarrow \oplus^m\mathcal{O} \xleftarrow{\phi} \oplus^n\mathcal{O} \xleftarrow{i} \mathfrak{A} \longrightarrow 0,$$

where i and ϕ are the maps obtained from the above splittings.

The maps :

$$\begin{array}{ccc} A(T)\otimes_{\mathcal{O}}\oplus^n\mathcal{O} & \xrightarrow{id\otimes_{\mathcal{O}}\phi} & A(T)\otimes_{\mathcal{O}}\oplus^m\mathcal{O} \\ \sim\downarrow & & \downarrow\sim \\ A^n(T) & \longrightarrow & A^m(T) \end{array}$$

(where T is an R-scheme, and A^i denotes $A\otimes_R\cdots\otimes_R A$) make $A\otimes_{\mathcal{O}}\phi$ into a natural transformation of functors, whence a morphism from A^n to A^m, which we call also ϕ. Define the scheme B as the fiber product :

$$\begin{array}{ccc} B & \longrightarrow & R \\ \downarrow & & \downarrow{\scriptstyle e_m} \\ A^n & \xrightarrow[\phi]{} & A^m \end{array}$$

where e_m is the identity section of X^m. Then, if T is an R-scheme,

$$B(T) = \ker(id\otimes_{\mathcal{O}}\phi),$$

which , by the splitting of $\oplus^n\mathcal{O}$, is just $A(T)\otimes_{\mathcal{O}}\mathfrak{A}$. So the functor $A\otimes_{\mathcal{O}}\mathfrak{A}$ is represented by B. It remains to show that B satisfy the definition of an abelian scheme with real multiplication.

2. : *B is a group scheme which is proper and locally of finite presentation over S*

Clearly, B is a group scheme. Since A^n and A^m are proper over R, A^n is proper over A^m, and, after base change, B is proper over R. Likewise, A^n is locally of finite presentation over R (because it is smooth) and A^m is locally of finite type over R (because it is proper). So A^n is locally of finite presentation over A^m, and, after base change, B is locally of finite presentation over R.

3. :

B is smooth. If X/R is an affine scheme endowed with a map $A\longrightarrow S$, $\mathcal{I}$ is a quasi-coherent sheaf of ideals on X with $\mathcal{I}^2=0$, and X_0 is the closed subscheme of X determined by $\mathcal{I}$, the map :

$$A(X)\longrightarrow A(X_0)$$

is surjective, because A is smooth. Thus

$$A(X) \otimes_{\mathcal{O}} \mathfrak{A} \longrightarrow A(X_0) \otimes_{\mathcal{O}} \mathfrak{A}$$

is also surjective, and because B is locally of finite presentation over S, it is smooth over S. (See [2] for a discussion of smoothness).

4. : *B has connected geometric fibers of dimension g.* Let $\tilde{k}$ be a geometric point of S. Then we have maps on fibers :

$$X_{\tilde{k}}^n \leftrightarrow Y_{\tilde{k}}$$

whose composition is the identity on $Y_{\tilde{k}}$. Since $X_{\tilde{k}}^n$ is connected, so is $Y_{\tilde{k}}$. Since $X_{\tilde{k}}^n$ has RM by $\mathcal{O}_L$, there is an exact sequence of $\mathcal{O}_L$-modules :

$$0 \longrightarrow \tilde{k} \otimes_{\mathbf{Z}} \mathcal{O}_L \longrightarrow A(\tilde{k}[\epsilon]/(\epsilon^2)) \longrightarrow A(\tilde{k}) \longrightarrow 0,$$

by the condition on $Lie(A)$ (see also [38]). Since $\mathfrak{A}$ is a flat $\mathcal{O}$-module, the sequence :

$$0 \longrightarrow (\tilde{k} \otimes_{\mathbf{Z}} \mathcal{O}_L) \otimes_{\mathcal{O}} \mathfrak{A} \longrightarrow B(\tilde{k}[\epsilon]/(\epsilon^2)) \longrightarrow B(\tilde{k}) \longrightarrow 0$$

is exact as well; $(\tilde{k} \otimes_{\mathbf{Z}} \mathcal{O}_L) \otimes_{\mathcal{O}} \mathfrak{A}$ has dimension g over $\tilde{k}$, so $B_{\tilde{k}}$ has dimension g.

5. : Lie(B/R) *is a locally free (on R) rank-1 $\mathcal{O}_L \otimes_{\mathbf{Z}} R$-module*

We have an exact sequence of sheaves on A^n :

$$\phi^* \Omega_{A^m/R} \longrightarrow \Omega_{X^n/R} \longrightarrow \Omega_{A^n/A^m} \longrightarrow 0.$$

Let e_n, e_Y denote identity sections; pulling back by e_n yields :

$$e_m^* \Omega_{A^m/R} \longrightarrow e_n^* \Omega_{A^n/R} \longrightarrow e_n^* \Omega_{A^n/A^m} \longrightarrow 0.$$

Now $i : B \longrightarrow A^n$ is just the base change of e_m by ϕ, so

$$e_B^* \Omega_{B/R} = e_Y^* i^* \Omega_{A^n/A^m} = e_n^* \Omega_{A^n/A^m}.$$

Replcaing $e_n^* \Omega_{A^n/A^m}$ by $e_Y^* \Omega_{Y/R}$ and dualizing, we get an exact sequence of sheaves on R :

$$0 \longrightarrow \text{Lie}(B/R) \longrightarrow \text{Lie}(A^n/R) \xrightarrow{\phi} \text{Lie}(A^m/R)$$

from which Lie(B/R) = Lie$(A/R) \otimes_{\mathcal{O}} \mathfrak{A}$, which is, locally on R, a free rank-1 $\mathcal{O}_L \otimes R$-module (since Lie(A/R) is so.)

PROPOSITION 1.4. *For any $a \in \mathfrak{A}$, the map :*

$$\epsilon(a) : A \longrightarrow A \otimes_{\mathcal{O}} \mathfrak{A},$$

given by

$$A(S) \longrightarrow A(S) \otimes_{\mathcal{O}} \mathfrak{A}$$

$$s \mapsto s \otimes a,$$

is an isogeny.

PROOF. First, $\epsilon(a)$ is a morphism of proper S-schemes, so it is proper. Now choose $d \in \mathfrak{A}^{-1}$ such that $ad = n \in \mathbb{Z}$. Then, by composing $\epsilon(d)\epsilon(a)$ with the natural isomorphism $(A \otimes_{\mathcal{O}_l(\mathfrak{A})} \mathfrak{A}) \otimes_{\mathcal{O}_l(\mathfrak{A}^{-1})} \mathfrak{A}^{-1} \longrightarrow A$, we see that $\epsilon(a)$ factors through $[n]$. So $\ker(\epsilon(a)) \subset \ker[n]$ is finite over S. Now by [**50**, Proposition 8.1c], $\epsilon(a)$ has finite fibers, so $\epsilon(a)$ is finite. □

REMARK 1.5.

$$\ker \epsilon(a) = \cap_{\{\alpha \in Q\ell(\mathcal{O}) | \mathfrak{A}\alpha\mathfrak{A} \subset \mathfrak{A}\}} \ker[\alpha].$$

One inclusion is clear, and $\ker \epsilon(a) \subset \ker[\alpha]$ follows as in the proof of Proposition 1.4.

This proposition enables us to show that the tensor construction satisfies Rapoport's condition more easily : just pick an element in $\mathfrak{A}$ such that the degree of the kernel of the isogeny is prime to p. Then the familiar argument shows that the tangent spaces are isomorphic :

$$\mathfrak{t}_A^* \cong \mathfrak{t}_{A \otimes_{\mathcal{O}} \mathfrak{A}}^*.$$

This tensor construction is therefore the direct generalization of the kernel ideal approach. It is easy to prove that the a-number and the f-number are stable under the tensor construction.

REMARK 1.6. A projective ideal is flat ([**64**, Corollary 3.46]). Since $\mathcal{O}$ is assumed to be left noetherian, any flat ideal is finitely presented, hence projective ([**64**, Theorem 3.61]). So flat is equivalent to projective in this context, and we can consider either the tensor construction $- \otimes_{\mathcal{O}} \mathfrak{A}$ or $\mathrm{Hom}(\mathfrak{A}, -)$ equivalently.

2. Application to superspecial points

In this section, we try describing a higher dimensional analogue of the equivalence between supersingular elliptic curves and left ideal classes of a maximal order in $B_{p,\infty}$.

CONJECTURE 2.1. (Bare conjecture)

Let S be the category of superspecial abelian varieties with real multiplication by $\mathcal{O}_L$ and isogenies, and let A_0 be an object in S. Then the functor $\mathrm{Hom}_S(A, -)$ *to the category of left ideals of $\mathcal{O} = \mathrm{End}A_0$ is an equivalence of categories, with inverse provided by $A \otimes_{\mathcal{O}} -$.*

A list of consequences of this conjecture :

COROLLARY 2.2. *(Mass formula for superspecial abelian varieties with RM)*

$$\sum \frac{1}{|\mathrm{Aut}(A, \iota)|} = \frac{\zeta_L(-1)}{2} h_L(p^2 + 1),$$

where the sum is over superspecial points.

COROLLARY 2.3. *For finite extensions of $\mathbb{F}_p$, the functor:*

$$B \mapsto (\mathrm{Hom}(A, B), \pi_*),$$

where π is the Frobenius morphism, gives an equivalence of superspecial abelian surfaces with RM with the suitable category of pairs.

COROLLARY 2.4. *For $\mathfrak{A}$ a projective rank one $\mathcal{O}$-module, we have*

$$A \otimes_{\mathcal{O}} \mathfrak{A} \text{ superspecial} \iff A \text{ superspecial},$$

where $\mathcal{O} \subset B_{\infty_1,\infty_2}$.

PROOF. This can be proven independently using Proposition 1.4. □

COROLLARY 2.5. 1. *Under the equivalence, isogenies of superspecial abelian surfaces correspond to nonzero $\mathcal{O}$-module homomorphisms.*

2. *The finite set of isomorphism classes in each category are in bijective correspondence. The cardinality of the set of superspecial point on the bare moduli space is given by the class number formula for Eichler order of level p.*

COROLLARY 2.6. *Every locally free rank one right module over $\mathcal{O}$ is isomorphic to one of the form* $\mathrm{Hom}(A, B)$ *for $A, B \in S$, and all of its embeddings in $\mathcal{O}$ are determined this way.*

REMARK 2.7. We can define the degree of a morphism $\phi : I \longrightarrow J$ of right $\mathcal{O}$-modules and various properties in the quaternion category in parallel with the geometric category.

DEFINITION 2.8. Let $\mathfrak{A}$ be a set of isogenies of A. We define $A[\mathfrak{A}]$ to be the scheme theoretic intersection of the kernel of all $\alpha \in \mathfrak{A}$, i.e.

$$A[\mathfrak{A}] = \ker(\epsilon(1) : A \longrightarrow A \otimes \mathfrak{A}).$$

A left $\mathcal{O}$-ideal $\mathfrak{A}$ is called a *kernel ideal* if $\mathfrak{A} = \{\alpha \in \mathcal{O} | \alpha(A[\mathfrak{A}]) = 0\}$.

PROOF. **Strategy of the proof of the bare conjecture** Since the tensor construction is essentially the same idea as the construction using kernel ideas, we could try using the same proof. Recall the

LEMMA 2.9. *([79, Theorem 3.11]) Let $\mathfrak{A}$ and $\mathfrak{B}$ be kernel ideals. Then*

$$A \otimes_{\mathcal{O}} \mathfrak{A} \cong A \otimes_{\mathcal{O}} \mathfrak{B} \iff [\mathfrak{A}] = [\mathfrak{B}],$$

i.e. $\mathfrak{A} = \nu\mathfrak{B}$ for some invertible $\nu \in \mathcal{O}$.

Thus, the result would follow if the equivalent of Theorem 2.21 is true, that is every left $\mathcal{O}$-ideal is a kernel ideal, for $\mathcal{O}$ an Eichler order of discriminant p in B_{∞_1,∞_2}. I believe that this follows from a modification of the proof of [79, Theorem 3.15] (since B_{∞_1,∞_2} is a simple algebra) and the rest of the proof would follow on the same lines as in the elliptic case. □

CHAPTER 5

Conclusion

We will digress briefly on a number of possibles avenues of research following the lines of this thesis.

Serre [**67**] developped an approach to the theory of modular forms mod p based on quaternion algebras; at the heart of the application of quaternion algebra is the connection between supersingular elliptic curves and class number of $B_{p,\infty}$. Can the connection between superspecial abelian surfaces and certain ideal class numbers improve our understanding of Hilbert modular forms mod p ? A similar theory valid for Hilbert modular varieties would already be extremely satisfying (keeping in mind the conjectural importance of such objects as cohomological motivic "building blocks"), but various ingredients used to develop mod p modular forms (such as the Ekedahl-Oort stratification) are being developped for general Shimura varieties. Of course, one wouldn't stop at studying the modular forms mod p, but also the p-adic theory : p-adic modular forms for Shimura varieties, including p-adic Hilbert modular forms. Back to the classical theory, since the trace formula for Hilbert modular forms has already been developped, one could try solving the basis problem by establishing a trace formula for the geometric Brandt matrices associated to totally definite quaternion algebras over totally real fields, and comparing the results, following the original strategy (pending a clarification of the connection between geometric Brandt matrices and Hilbert modular forms which, as we have noted earlier, does not follow the same lines as the elliptic case). In comparison with the classical case (with the motivation of understanding representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, it seems that little has been done with regard to arithmetical applications of quaternion algebras defined over number fields different than $\mathbb{Q}$; likewise for vector-valued theta series and modular forms : this clearly indicates the pertinence

of considering the "fibred product", considering vector-valued theta series and modular forms for more general congruence subgroups.

A perpendicular direction is to replace, following Gekeler, abelian varieties of dimension g by Drinfel'd modules of rank r.

Even though we take a geometric point of view to the arithmetic of quaternion algebra, one could pursue similar themes in the study of the arithmetic of octonion algebra [**21**] : compute the number of optimal embeddings of orders with application to modular forms, for example (the cardinalities being viewed as q-expansion coeffients).

Always in the theme of arithmetical applications, one might investigate the relation with the p-adic uniformization of related Shimura curves and applications to p-adic L-functions, Heegner points, etc.

Most concretely, classical Brandt matrices have been used by Pizer to construct Ramanujan graphs. Can we exploit the fact that certain of our geometric Brandt matrices are adjacency matrices and give application in extremal graph theory, say. In order to make computations easier and faster, can we build the Hecke theory wholly on quaternion algebras (considering Hecke modules as free abelian groups on left ideal classes of an order in a quaternion algebra, and Hecke operators as

$$T_n([I]) = \sum_{\phi}[J] = \sum_{J \in S} a_n(I,J)[J],$$

where the sum runs over cyclic R-modules homomorphisms $\phi : I \longrightarrow J$ of degree n, $(n,p) = 1.)$, etc.), so to be able to choose the less time consuming side of the picture? Note also that Hilbert modular forms arising from geometric Brandt matrices would be a good source of computable examples, and establishing this link satisfactorily shall constitue the evident next step for further research, provided a proof of the bare conjecture (at the time of writing, the author is optimistically working on a proof of a suitably formulated bare conjecture for Hilbert modular *varieties*).

On modular curves, the supersingular divisor group can be seen as the monodromy group at p (see [**41**]); can we pursue the monodromy point of view in the higher-dimensional case ?

One could study theta series coming from exotic lattices : E_8, Leech, Elkies-Borcherds, Thompson-Smith, Barnes-Wall, etc. and develop further sphere-packing properties of modular forms, or explore various theta series congruences (see [18]).

Bibliography

[1] Bachmat, E.; Goren, E. Z., On the non-ordinary locus in Hilbert-Blumenthal surfaces. *Math. Ann.* **313** (1999), no. 3, 475–506.

[2] Bosch, S.; Lütkebohmert, W.; Raynaud, M., *Néron models*. Ergebnisse der Mathematik und ihrer Grenzgebiete (3), 21. Springer-Verlag, Berlin, 1990. x+325 pp.

[3] Breen, L. S., On a nontrivial higher extension of representable abelian sheaves. *Bull. Amer. Math. Soc.* **75** 1969 1249–1253.

[4] Brzezinski, J., A generalization of Eichler's trace formula. Journées Arithmétiques (Barcelona, 1995). *Collect. Math.* **48** (1997), no. 1-2, 53–61.

[5] Brzezinski, J., A combinatorial class number formula. *J. Reine Angew. Math.* **402** (1989), 199–210.

[6] Chai, C.-L., Every ordinary symplectic isogeny class in positive characteristic is dense in the moduli. *Invent. Math.* **121** (1995), no. 3, 439–479.

[7] Chai, C.-L. Arithmetic minimal compactification of the Hilbert-Blumenthal moduli spaces. *Ann. of Math. (2)* **131** (1990), no. 3, 541–554.

[8] Chai, C.-L.; Norman, P., Bad reduction of the Siegel moduli scheme of genus two with $\Gamma_0(p)$-level structure. *Amer. J. Math.* **112** (1990), no. 6, 1003–1071.

[9] Chai, C.-L.; Norman, P., Singularities of the $\Gamma_0(p)$-level structure. *J. Algebraic Geom.* **1** (1992), no. 2, 251–278.

[10] de Jong, A. J., The moduli spaces of polarized abelian varieties. *Math. Ann.* **295** (1993), no. 3, 485–503.

[11] de Jong, A. J., The moduli spaces of principally polarized abelian varieties with $\Gamma_0(p)$-level structure. *J. Algebraic Geom.* **2** (1993), no. 4, 667–688.

[12] Deligne, P., La conjecture de Weil. I., *Inst. Hautes Études Sci. Publ. Math.* **No. 43**, (1974), 273–307.

[13] Deligne, P.; Pappas, G., Singularités des espaces de modules de Hilbert, en les caractéristiques divisant le discriminant. *Compositio Math.* **90** (1994), no. 1, 59–79.

[14] Deligne, P., Rapoport, M. , Les schémas de modules de courbes elliptiques. *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pp. 143-316. Lectures Notes in Math., **Vol. 349**, Springer, Berlin, 1973.

[15] Deligne, P.; Ribet, K. A., Values of abelian L-functions at negative integers over totally real fields. *Invent. Math.* **59** (1980), no. 3, 227–286.

[16] Deninger, C., Isogenies of abelian varieties with multiplications and Fitting ideals. *Abh. Math. Sem. Univ. Hamburg* **65** (1995), 249–257.

[17] Deuring, M. , Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hansischen Univ.* **14**, (1941). 197–272.

[18] Dummigan, N., Theta series congruences. *Integral quadratic forms and lattices (Seoul, 1998)*, 249–252, Contemp. Math., **249**, Amer. Math. Soc., Providence, RI, 1999.

[19] Eichler, M. , Zur Zahlentheorie der Quaternionen-Algebren. *J. Reine Angew. Math.* **195** (1955), 127–151

[20] Eichler, M., Über die Idealklassenzahl hypercomplexer Systeme, *Math. Z.* **43** (1938), 481-494.

[21] Elkies, N.; Gross, B. H., Embeddings into the integral octonions. Olga Taussky-Todd: in memoriam. *Pacific J. Math.* **1997**, Special Issue, 147–158.

[22] Ellenberg, J., *Hilbert modular forms and the Galois representations associated to Hilbert-Blumenthal abelian varieties* , Ph.D. thesis, Harvard, 1998.

[23] Faltings, G.; Chai, C.-L., *Degeneration of abelian varieties.* With an appendix by David Mumford. Ergebnisse der Mathematik und ihrer Grenzgebiete (3), **22**. Springer-Verlag, Berlin, 1990. xii+316 pp.

Class groups and Picard groups of orders. *Proc. London Math. Soc.* **(3)** 29 (1974), 405–434.

The Picard group of noncommutative rings, in particular of orders. *Trans. Amer. Math. Soc.* **180** (1973), 1–45.

[24] Gekeler, E.-U., Sur la géométrie de certaines algèbres de quaternions. *Sém. Théor. Nombres Bordeaux (2)* **2** (1990), no. 1, 143–153.

[25] Goren, E. Z. Hilbert modular varieties in positive characteristic. *The arithmetic and geometry of algebraic cycles (Banff, AB, 1998)*, 283–303, CRM Proc. Lecture Notes, **24**, Amer. Math. Soc., Providence, RI, 2000.

[26] Goren, E. Z.; Oort, F. Stratifications of Hilbert modular varieties. *J. Algebraic Geom.* **9** (2000), no. 1, 111–154.

[27] Goren, E.Z., Hilbert modular forms modulo p^m – the unramified case, CICMA pre-print **1998-10**, submitted, 22 pp.

[28] Goren, E.Z., Letter to Eitan Bachmat.

[29] Gross, B. H., Heights and the special values of L-series. *Number theory (Montréal, Qué., 1985)*, 115–187, CMS Conf. Proc., **7**, Amer. Math. Soc., Providence, RI, 1987.

[30] Ibukiyama, T.; Katsura, T.; Oort, F., Supersingular curves of genus two and class numbers. *Compositio Math.* **57** (1986), no. 2, 127–152.

[31] Ibukiyama, T.; Katsura, T., On the field of definition of superspecial polarized abelian varieties and type numbers. *Compositio Math.* **91** (1994), no. 1, 37–46.

[32] Igusa, J., Class number of a definite quaternion with prime discriminant. *Proc. Nat. Acad. Sci. U.S.A.* **44**, 1958, 312–314

[33] Jacobson, N., *Finite-dimensional division algebras over fields*. Springer-Verlag, Berlin, 1996. viii+278 pp.

[34] Jordan, B. W.; Livné, R., Integral Hodge theory and congruences between modular forms. *Duke Math. J.* **80** (1995), no. 2, 419–484.

[35] Kassei, P. L., *p-adic Modular Forms over Shimura Curves over* $\mathbb{Q}$, Ph.D. Thesis (MIT), 1999.

[36] Katsura, T.; Oort, F., Families of supersingular abelian surfaces. *Compositio Math.* **62** (1987), no. 2, 107–167.

[37] Katz, N. M., p-adic properties of modular schemes and modular forms. *Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pp. 69–190. Lecture Notes in Mathematics, Vol. **350**, Springer, Berlin, 1973.

[38] Katz, N. M. p-adic L-functions for CM fields. *Invent. Math.* **49** (1978), no. 3, 199–297.

[39] Katz, N. M.; Mazur, B., Arithmetic moduli of elliptic curves. *Annals of Mathematics Studies*, **108**. Princeton University Press, Princeton, N.J., 1985. xiv+514 pp.

[40] Kohel, D., Computing modular curves via quaternions, Based on a talk given at the Fourth CANT Conference Number Theory and Cryptography, University of Sydney, 3-5 December 1997.

[41] Kohel, D., Hecke module structure of quaternions, preprint, 1998.

[42] Kohel, D., *Endomorphism rings over finite fields*, Thesis, University of California, Berkeley, 1996.

[43] Li, K.-Z.; Oort, F., *Moduli of supersingular abelian varieties*. Lecture Notes in Mathematics, **1680**. Springer-Verlag, Berlin, 1998. iv+116 pp.

[44] Mestre, J.-F., La méthode des graphes. Exemples et applications. Proceedings of the international conference on class numbers and fundamental units of algebraic number fields (Katata, 1986), 217–242, Nagoya Univ., Nagoya, 1986.

[45] Mizumoto, S., On the second L-functions attached to Hilbert modular forms. *Math. Ann.* **269** (1984), no. 2, 191–216.

[46] Mizumoto, S., On integrality of certain algebraic numbers associated with modular forms. *Math. Ann.* **265** (1983), no. 1, 119–135.

[47] Moret-Bailly, L., Familles de courbes et de variétés abéliennes sur $\mathbb{P}^1$, Exposés 7 & 8, *Astérisque* **86** (1981), 109-140.

[48] Moret-Bailly, L., Polarisations de degré 4 sur les surfaces abéliennes. *C. R. Acad. Sci. Paris Sér. A-B* **289** (1979), no. 16, A787–A790.

[49] Mumford, D.; Fogarty, J.; Kirwan, F. *Geometric invariant theory*. Third edition. Ergebnisse der Mathematik und ihrer Grenzgebiete (2), **34**. Springer-Verlag, Berlin, 1994. xiv+292 pp.

[50] Mumford, D., *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics, **No. 5**, Published for the Tata Institute of Fundamental Research, Bombay; Oxford University Press, London 1970 viii+242 pp.

[51] Narasimhan, M. S.; Nori, M. V., Polarisations on an abelian variety. *Proc. Indian Acad. Sci. Math. Sci.* **90** (1981), no. 2, 125–128.

[52] Neukirch, J., *Algebraic number theory*. Translated from the 1992 German original and with a note by Norbert Schappacher. With a foreword by G. Harder. Grundlehren der Mathematischen Wissenschaften, **322**. Springer-Verlag, Berlin, 1999. xviii+571 pp.

[53] Ogg, A., *Modular forms and Dirichlet series*. W. A. Benjamin, Inc., New York-Amsterdam 1969 xvi+173 pp.

[54] Oort, F., Subvarieties of moduli spaces. *Invent. Math.* **24** (1974), 95–119.

[55] Oort, F., Which abelian surfaces are products of elliptic curves? Math. Ann. 214 (1975), 35–47

[56] Pappas, G., Arithmetic models for Hilbert modular varieties. *Compositio Math.* **98** (1995), no. 1, 43–76.

[57] Pizer, A., An algorithm for computing modular forms on $\Gamma_0(N)$. *J. Algebra* **64** (1980), no. 2, 340–390.

[58] Pizer, A., Ramanujan graphs. *Computational perspectives on number theory (Chicago, IL, 1995)*, 159–178, AMS/IP Stud. Adv. Math., **7**, Amer. Math. Soc., Providence, RI, 1998.

[59] Pizer, A., Theta series and modular forms of level p^2M. *Compositio Math.* **40** (1980), no. 2, 177–241.

[60] Pizer, A., Type numbers of Eichler orders. *J. Reine Angew. Math.* **264** (1973), 76–102.

[61] Rapoport, M., Compactifications de l'espace de modules de Hilbert-Blumenthal. *Compositio Math.* **36** (1978), no. 3, 255–335.

[62] Reiner, I. *Maximal orders*. London Mathematical Society Monographs, **No. 5**. Academic Press, London-New York, 1975. xii+395 pp.

[63] Ribet, K. A., On modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms. Invent. Math. 100 (1990), no. 2, 431–476.

[64] Rotman, J. J. *An introduction to homological algebra*. Pure and Applied Mathematics, **85**. Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], New York-London, 1979. xi+376 pp.

[65] Serre, J.-P., Groupes, p-divisibles (d'après J. Tate). *Séminaire Bourbaki*, **Vol. 10**, Exp. No. 318, 73–86, Soc. Math. France, Paris, 1995.

[66] Serre, J.-P. Complex multiplication. 1967, *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)* pp. 292–296, Thompson, Washington, D.C.

[67] Serre, J.-P. Two letters on quaternions and modular forms (mod p). With introduction, appendix and references by R. Livné. *Israel J. Math.* **95** (1996), 281–299.

[68] Shimura, G., Arithmetic of alternating forms and quaternion hermitian forms. *J. Math. Soc. Japan* **15** 1963 33–65.

[69] Shimura, G., Arithmetic of unitary groups, *Ann. of Math.* **81** (1965), pp. 166–193.

[70] Shioda, T., Supersingular $K3$ surfaces. *Algebraic geometry (Proc. Summer Meeting, Univ. Copenhagen, Copenhagen, 1978)*, pp. 564–591, Lecture Notes in Math., **732** Springer, Berlin, 1979.

[71] Silverman, J. H., *The arithmetic of elliptic curves*. Corrected reprint of the 1986 original. Graduate Texts in Mathematics, **106**. Springer-Verlag, New York, 1999. xii+400 pp.

[72] Stamm, H., On the reduction of the Hilbert-Blumenthal-moduli scheme with $\Gamma_0(p)$-level structure. *Forum Math.* **9** (1997), no. 4, 405–455.

[73] Takase, K., On the trace formula of the Hecke operators and the special values of the second L-functions attached to the Hilbert modular forms. *Manuscripta Math.* **55** (1986), no. 2, 137–170.

[74] Taylor, R., Remarks on a conjecture of Fontaine and Mazur, preprint

[75] van der Geer, G., *Hilbert modular surfaces*. Ergebnisse der Mathematik und ihrer Grenzgebiete (3), **16**. Springer-Verlag, Berlin-New York, 1988. x+291 pp.

[76] Vignéras, M.-F., *Arithmétique des algèbres de quaternions*. L.N.M. **800**. Springer, Berlin, 1980. vii+169 pp.

[77] Vignéras, M.-F. Nombre de classes d'un ordre d'Eichler et valeur au point -1 de la fonction zêta d'un corps quadratique réel. *Enseignement Math. (2)* **21** (1975), no. 1, 69–105

[78] Vignéras, M.-F., Invariants numériques des groupes de Hilbert. *Math. Ann.* **224** (1976), no. 3, 189–215

[79] Waterhouse, W. C., Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup. (4)* **2** 1969 521–560.

[80] Wilf, H. S., *generatingfunctionology*. Second edition. Academic Press, Inc., Boston, MA, 1994. x+228 pp.