Superspecial abelian varieties, theta series and the Jacquet-Langlands correspondence

Marc-Hubert Nicole

Department of Mathematics and Statistics,
McGill University, Montréal
Québec, Canada

June, 2005

A thesis submitted to McGill University in partial fulfillment of the requirements of the degree of Doctor of Philosophy

Abstract

Let E_i, $i = 1, ..., n$, be all the supersingular elliptic curves over $\overline{\mathbb{F}}_p$ up to isomorphism. The modules of isogenies $\mathrm{Hom}(E_i, E_j)$, equipped with the degree map, are quadratic modules that give rise to theta series of level p. The space of modular forms of weight two for $\Gamma_0(p)$ is thus spanned by the theta series coming from supersingular elliptic curves in this fashion. We generalize this classical result to Hilbert modular forms by showing that for totally real fields L of narrow class number one, the space of Hilbert modular newforms of parallel weight 2 for $\Gamma_0(p)$, p unramified, is spanned by theta series coming from quadratic modules $\mathrm{Hom}_{\mathcal{O}_L}(A_i, A_j)$, where A_i, A_j range across all superspecial abelian varieties with real multiplication by $\mathcal{O}_L$. We also provide a version of this theorem in the more delicate case where p is totally ramified in $\mathcal{O}_L$, building on the classification of superspecial crystals following from the generalization of Manin's Habilitationschrift that we present in the first Chapter.

Résumé

Soient E_i, $i = 1, ..., n$, toutes les courbes elliptiques supersingulières définies sur $\overline{\mathbb{F}}_p$, à isomorphisme près. Les modules d'isogénies $\mathrm{Hom}(E_i, E_j)$, munis de l'application degré, sont des modules quadratiques qui donnent lieu à des séries thêta de niveau p. L'espace des formes modulaires de poids 2 pour $\Gamma_0(p)$ est donc engendré par des combinaisons de séries thêta provenant des courbes elliptiques supersingulières. Nous généralisons ce résultat classique aux formes modulaires de Hilbert en montrant que pour un corps totalement réel L de nombre de classes restreintes un, l'espace des nouvelles formes modulaires de Hilbert de poids parallèle 2 pour $\Gamma_0(p)$, p non ramifié, est engendré par les séries thêta provenant de modules quadratiques $\mathrm{Hom}_{\mathcal{O}_L}(A_i, A_j)$, où les A_i, A_j parcourent l'ensemble des variétés abéliennes superspéciales à multiplication réelle par $\mathcal{O}_L$. Nous fournissons aussi une version de ce théorème dans le cas plus délicat où p est totalement ramifié dans $\mathcal{O}_L$, en nous appuyant sur la classification des cristaux superspéciaux qui découle de la généralisation de l'Habilitationschrift de Manin que nous exposons dans le chapitre premier.

Remerciements

J'aimerais respectueusement remercier mon superviseur Prof. Eyal Z. Goren pour sa patience et pour son professionnalisme; en particulier pour les commentaires à la fois instructifs et fouillés découlant de sa lecture de différentes versions de cette thèse.

J'aimerais aussi remercier les membres de ma famille et mes amis pour leur constante affection et support, même à distance parfois considérable.

Une catégorie importante de gens qui ont enrichi grandement mon séjour sur l'île de Montréal sont les hyperactivistes impliqués dans la défense des opprimés partout dans le monde, du territoire mohawk de Kanehsatake jusqu'à l'État du Guerrero. Chapeau surtout aux membres d'IPSM, qui est pour moi un modèle exemplaire en terme d'activisme social, par le mélange de lucidité, d'efficacité et d'humanité qui le caractérise.

J'ai apprécié quelques commentaires d'une version préliminaire de cette thèse que m'a fait parvenir en mai 2005 Dr. A. Ghitza. Je dois aussi remercier mon collègue du bureau, A. Stanculescu, pour des excellents conditions de travail.

J'ai été financé successivement par des bourses du CRSNG, du FCAR et de l'ISM pendant la majeure partie de mes études doctorales.

Table of Contents

Introduction

Let p be a prime number. Let E be a supersingular elliptic curve over $\overline{\mathbb{F}}_p$. Deuring showed that the endomorphism ring $\mathrm{End}(E)$ is a maximal order in the rational quaternion algebra $B_{p,\infty}$ ramified at p and ∞. The number h of supersingular j-invariants, and thus the number of supersingular elliptic curves $E_i/\overline{\mathbb{F}}_p$, is finite. The left ideal classes of $\mathrm{End}(E)$ are in bijection with supersingular elliptic curves defined over $\overline{\mathbb{F}}_p$, and any maximal order in $B_{p,\infty}$ arises as the endomorphism ring of a suitable supersingular elliptic curve E_i for some i. All maximal orders of $B_{p,\infty}$ are locally conjugate. The number of maximal orders, up to isomorphism, is thus bounded by h. It is called the type number, and it can be strictly less than h: $\mathrm{End}(E_i)$ is isomorphic to $\mathrm{End}(E_k)$ if and only if $j_i^p = j_k$. The $\mathbb{Z}$-module $\mathrm{Hom}(E_1, E_2)$ of homomorphisms between two supersingular elliptic curves E_1 and E_2 is naturally equipped with the degree map, a quadratic form in four variables with values in $\mathbb{Z}$. Indeed, as the above bijection suggests, this data can be formulated in terms of quaternion algebras only. Let $I_1, \ldots, I_h$ be ideals of $B_{p,\infty}$ representing the left ideal classes of $\mathcal{O} = \mathrm{End}(E)$, viewed as a maximal order in $B_{p,\infty}$. Then $E \otimes_{\mathcal{O}} I_j$ for $j = 1, \ldots, h$, are equal to $E_1, \ldots, E_h$, up to isomorphism (and up to re-indexing), and we have the formula $\mathrm{Hom}(E \otimes_{\mathcal{O}} I_k, E \otimes_{\mathcal{O}} I_j) = I_j^{-1} I_k$. Moreover, the quadratic forms on $\mathrm{Hom}(E \otimes_{\mathcal{O}} I_k, E) = I_k$, given by the degree map and by $\mathrm{Norm}(-)/\mathrm{Norm}(I_k)$, are

equal. The theta series

$$\Theta_{jk} = \sum_{n=0}^{\infty} |\{f \in I_j^{-1} I_k : \deg(f) = n\}| \cdot q^n, \quad q = e^{2\pi i z},$$

are modular forms of level $\Gamma_0(p)$ and weight 2 (with trivial character). Eichler's Theorem states that these theta series span the vector space of weight 2 modular forms for $\Gamma_0(p)$. The geometry enters the picture when one considers the reduction $\overline{X_0(p)}$ of the modular curve $X_0(p)$ modulo p. It has a canonical projection $\overline{X_0(p)} \longrightarrow \overline{X_0(1)}$ and $\overline{X_0(p)}$ consists of two copies of $\overline{X_0(1)}$, one projecting isomorphically and one via the Frobenius map on $\overline{X_0(1)}$. The two components intersect transversally at the supersingular points. Cusp forms of weight 2 on $X_0(p)$ with integral Fourier coefficients can be viewed as holomorphic differentials; they can also be reduced modulo p. There, we view them as meromorphic differentials on $\overline{X_0(1)}$ with simple poles along the supersingular locus. Since $\overline{X_0(1)}$ is $\mathbb{P}^1$, we get functions on the supersingular locus (with the value at a point being defined as the residue) such that the sum of its values is zero.

We generalize some of these results to the Hilbert modular setting in the second Chapter. From the perspective of this thesis, a key point is the uniqueness of the superspecial crystal, for p unramified.

The first Chapter of this thesis generalizes mutatis mutandis Manin's Habilitationschrift to obtain a classification up to isomorphism of F-crystals over *totally ramified* extensions of the Witt vectors over a perfect field of characteristic p. The key point of the classification is the concept of a special module. The supersingular special, or *superspecial* crystals, arise in geometry from superspecial points on Hilbert moduli spaces. We derive from the general classification some geometrical results relative to Hilbert-Siegel moduli spaces e.g., determining the number of superspecial crystals in the totally ramified case and studying the stratification of the supersingular locus suggested by the decomposition of the module spaces à la Manin, examples of which

are calculated explicitly. This stratification of moduli spaces of abelian varieties with additional structure that we are suggesting, which essentially consists of associating its special Dieudonné module to an abelian variety with additional structure, is shown to be the same as the slope stratification of Andreatta and Goren for the supersingular Newton polygon stratum. We show in particular that the isomorphism type of the Dieudonné module depends only on the singularity index (which measures the failure of the tangent space to be a free $\mathcal{O}_L \otimes \overline{\mathbb{F}}_p$-module). We also establish a truncation conjecture of Traverso in a particular case, showing that a (classical) supersingular Dieudonné module of rank $2g$ is determined up to non-canonical isomorphism by its truncation modulo p^g.

The second Chapter of this thesis generalizes for Hilbert moduli spaces the above mentioned results of Deuring and Eichler. The Main Theorem is a geometric interpretation of Eichler's Basis Problem for Hilbert modular forms: in short, under the hypothesis that the narrow class number of the totally real field L is 1 and p unramified, we show that the theta series stemming from superspecial points on the Hilbert moduli space span the vector space of Hilbert newforms of level p and weight two. We also investigate the case where p is totally ramified. The proof follow the general strategy of the elliptic case. The Hilbert moduli space parametrizes principally polarized abelian varieties with an action of $\mathcal{O}_L$, where the polarization is $\mathcal{O}_L$-linear. The superspecial points on the Hilbert moduli space in characteristic p form a finite set $A_1, \ldots, A_H$. In fact, if $E_1, \ldots, E_g$ are any supersingular elliptic curves over $\overline{\mathbb{F}}_p$, then any A_j is isomorphic to $E_1 \times \cdots \times E_g$ as abelian varieties and so the A_i's are distinguished precisely by the action of $\mathcal{O}_L$ (once the $\mathcal{O}_L$-action is given, all choices of $\mathcal{O}_L$-linear principal polarizations are isomorphic).

Let A be a superspecial abelian variety with RM. We first show that the centralizer of $\mathcal{O}_L$ in $\mathrm{End}(A)$ i.e., $\mathrm{End}_{\mathcal{O}_L}(A)$ is an order of discriminant dividing p in $B_{p,L}$ that is, the quaternion algebra $B_{p,\infty} \otimes L$. In particular, if p is unramified, it is an Eichler

order of level p. Let E be a supersingular elliptic curve over $\overline{\mathbb{F}}_p$. The key example is the abelian variety $E \otimes_{\mathbb{Z}} \mathcal{O}_L$, which is principally polarized. One has

$$\mathrm{End}_{\mathcal{O}_L}(E \otimes \mathcal{O}_L) = \mathrm{End}(E) \otimes \mathcal{O}_L = \mathcal{O} \otimes \mathcal{O}_L,$$

where $\mathcal{O}$ is a maximal order in $B_{p,\infty}$. The order $\mathcal{O} \otimes \mathcal{O}_L$ clearly has discriminant p. The local nature of $\mathrm{End}_{\mathcal{O}_L}(A_i)$ can be studied by a version of Tate's theorem that we provide, which states that $\mathrm{End}_{\mathcal{O}_L}(A_i) \otimes \mathbb{Z}_\ell \cong \mathrm{End}_{\mathcal{O}_L \otimes \mathbb{Z}_\ell}(T_\ell(A_i))$ and $\mathrm{End}_{\mathcal{O}_L}(A_i) \otimes \mathbb{Z}_p \cong \mathrm{End}_{\mathcal{O}_L \otimes W(\overline{\mathbb{F}}_p)[F,V]}(\mathbb{D}(A_i))$, where $\mathbb{D}(A_i)$ is the Dieudonné module of A_i. Since all $T_\ell(A_i)$ and $\mathbb{D}(A_i)$ are independent of i when p is unramified, one concludes that all the orders $\mathrm{End}_{\mathcal{O}_L}(A_i)$ are locally conjugate. When p is ramified, there is more than one isomorphism class of Dieudonné module, and we get orders of different levels. For the rest of this introduction, we suppose that p is unramified. Using our version of Tate's theorem, we show that $\mathrm{Hom}_{\mathcal{O}_L}(A_i, A_j)$ is a projective rank 1 module over $\mathrm{End}_{\mathcal{O}_L}(A_i)$. Conversely, left ideals classes of $\mathrm{End}_{\mathcal{O}_L}(A)$ are in bijection with superspecial abelian varieties with RM. Also, any superspecial order of level $p\mathcal{O}_L$ i.e., an order admitting the same local description as $\mathrm{End}_{\mathcal{O}_L}(E \otimes \mathcal{O}_L)$ (see Definition 2.3.11), arises as the endomorphism ring of a suitable superspecial abelian variety with RM. One can also define the type number in this context (and it is bounded by the class number H) but we do not study its geometric interpretation in this thesis. We then consider the $\mathcal{O}_L$-module $\mathrm{Hom}_{\mathcal{O}_L}(A_1, A_2)$ of $\mathcal{O}_L$-isogenies between two superspecial abelian varieties A_1, A_2, equipped with a totally definite quadratic form called the $\mathcal{O}_L$-degree $||-||$. This $\mathcal{O}_L$-degree is defined as $||f|| = \lambda_1^{-1} f^t \lambda_2 f$, for $f \in \mathrm{Hom}_{\mathcal{O}_L}(A_1, A_2)$, and λ_1 (respectively, λ_2) the principal polarization on the abelian variety A_1 (respectively A_2). Thus, the $\mathcal{O}_L$-degree is defined up to the choices of polarizations, which are unique up to totally positive units in $\mathcal{O}_L$. Since the norm $\mathrm{Norm}(I_j)$ of an ideal I_j of $\mathrm{End}(A_1)$ is an ideal in $\mathcal{O}_L$, we can make sense of it by choosing a totally positive generator r of $\mathrm{Norm}(I_j)$ and looking at $\mathrm{Norm}(-)/r$, which is well-defined up to a totally positive unit of $\mathcal{O}_L$. Therefore, $\mathrm{Norm}(-)/r$ is equal

to the $\mathcal{O}_L$-degree up to a totally positive unit. This quadratic form allows us to construct a theta series of level p from the quadratic module $(\mathrm{Hom}_{\mathcal{O}_L}(A_1, A_2), ||-||)$ in the usual way. The Jacquet-Langlands correspondence, translated in classical terms, implies that the space of Hilbert modular newforms of weight 2 for $\Gamma_0(p)$ is thence spanned by the theta series coming from superspecial abelian varieties with RM, and we get the desired result this way.

An isolated result we include in this thesis concerns the Siegel moduli space, which parametrizes principally polarized abelian varieties. The a-number allows to slice the Siegel moduli space in characteristic p in finitely many strata T_a. Using deformation theory, we show that the singular locus of T_a is T_{a+1}, completing a result of van der Geer.

More detailed introductions are given at the beginning of each Chapter.

Chapter 1

Dieudonné modules

1.1 Introduction

This mainly utilitarian chapter covers the basics about Dieudonné modules over perfect fields, and treats some questions in line with Manin's Habilitation [66], especially its chapter III on the classification, up to isomorphism, of Dieudonné modules. In particular, we show that Manin's results extend mutadis mutandis to Dieudonné modules with real multiplication (RM) in the totally ramified case. Revisiting the spaces of Dieudonné modules à la Manin in the combined light of old conjectures and modern theorems enables us to reap many interesting results about supersingular Dieudonné modules:

1. In Subsection 1.3.6: The classification of superspecial crystals with RM; this, in turn, is used in the ramified case of the geometric interpretation of Eichler's Basis Problem in Chapter II of the present thesis.

2. In Sections 1.4 and 1.5: Some optimal results in line with Traverso's boundedness conjecture (for classical Dieudonné modules). In particular, we optimize two propositions of Vasiu ([99]): by proving Traverso's conjecture in the su-

persingular case, and by giving the optimal bound for the isocrystal of slopes $\{\frac{1}{n}, \frac{n-1}{n}\}$, $n \geq 3$. A combination of Oort's result that the first truncation $\mathbb{D}/p\mathbb{D}$ of a *minimal* Dieudonné module $\mathbb{D}$ determines uniquely the isomorphism class of $\mathbb{D}$ and the computation of the classical supersingular Dieudonné module space à la Manin proves that case of Traverso's conjecture.

3. In Section 1.6: A description of the slope stratification of [1] of the supersingular Newton polygon stratum of Hilbert modular varieties purely in terms of the geometry of the Dieudonné module spaces à la Manin. Note that the geometric properties of the slope stratification of Hilbert moduli spaces have been investigated in depth in [1] and [2].

1.2 Basics

We introduce, in this section, all relevant definitions about Dieudonné modules, and we state the classical Dieudonné-Manin classification. The connection with p-divisible groups is explained in detail in [18] and also [41], which is nicely complemented by the lecture notes [78].

Let k be a perfect field of characteristic $p > 0$, and let K be the fraction field of the Witt ring $W(k)$; k perfect implies that $W(k)$ is a complete discrete valuation ring with residue field k. The Frobenius automorphism σ of k induces an automorphism (also noted σ) of K.

Definition 1.2.1. An **F-isocrystal** (V, Φ) is a finite dimensional vector space V over the field K, equipped with a σ-linear bijection $\Phi : V \longrightarrow V$.

More generally, we can replace K by the compositum $K_{\mathfrak{F}} := K \cdot \mathfrak{F}$ of K and a finite extension $\mathfrak{F}$ of $\mathbb{Q}_p$ in $\overline{K}$. We give a few necessary words of explanation, following Kottwitz ([60, §1]). Suppose that k is algebraically closed. Let $k_{\mathfrak{F}}$ denote the residue

field of $\mathfrak{F}$ and let M denote the fraction field of $W(k_{\mathfrak{F}})$. The extension $\mathfrak{F}/M$ is totally ramified of degree g, the absolute ramification index of $\mathfrak{F}$. The canonical homomorphism $K \otimes_M \mathfrak{F} \longrightarrow K_{\mathfrak{F}}$ is an isomorphism, since an Eisenstein polynomial over M remains Eisenstein over K. In particular, the extension $K_{\mathfrak{F}}/K$ is totally ramified of degree g, which means that g is also the absolute ramification index of $K_{\mathfrak{F}}$. The Frobenius automorphism σ of k relative to $k_{\mathfrak{F}}$ induces an automorphism of K over M, which in turn induces an automorphism (also noted σ) of $K_{\mathfrak{F}}$ over the field $\mathfrak{F}$. The fixed field of σ on $K_{\mathfrak{F}}$ is $\mathfrak{F}$ (see [60, Lem. 1.2]).

Definition 1.2.2. An F**-isocrystal** (V, Φ) **with RM** by $\mathfrak{F}$ is a finite dimensional vector space V over $K_{\mathfrak{F}}$ equipped with a σ-linear bijection $\Phi : V \longrightarrow V$.

Remark 1.2.3. The terminology "with RM" stems from the fact that Hilbert moduli spaces classify g-dimensional polarized abelian varieties A over k with real multiplication e.g., equipped with an action

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

where $\mathcal{O}_L$ is the ring of integers of a totally real field L. By functoriality, the action of $\mathcal{O}_L$ carries over to the first crystalline cohomology group $H^1_{crys}(A/W(k))$. If $p\mathcal{O}_L = \mathfrak{p}^g$ is totally ramified, $H^1_{crys}(A/W(k)) \otimes \mathbb{Q}$ can be viewed as an F-isocrystal with RM by $\mathcal{O}_{L_{\mathfrak{p}}}$, the ring of integers of the totally ramified extension of $\mathbb{Q}_p$ obtained by completing L at $\mathfrak{p}$.

Theorem 1.2.4. (Dieudonné-Manin) Let k be an algebraically closed field. The category of F-isocrystals with RM over $K_{\mathfrak{F}}$ is semisimple with simple objects parametrized by $\mathbb{Q}$. To $\lambda \in \mathbb{Q}$ corresponds the simple object E_λ defined as follows. If $\lambda = \frac{r}{s}$, with $r, s \in \mathbb{Z}, s > 0, (r, s) = 1$, then

$$E_\lambda = K_{\mathfrak{F}}[F]/(F^s - T^r),$$

where T is a uniformizer of $K_{\mathfrak{F}}$, and F is σ-linear i.e., $Fx = x^\sigma F$.

Proof. [60, §3] □

Definition 1.2.5. We call the collection of rational numbers $\{\frac{r_i}{gs_i}\}$ associated to a semisimple object $\oplus_i E_{\lambda_i}, \lambda_i = \frac{r_i}{s_i}$ its **slopes**.

Denote by $W_{\mathfrak{F}}(k)$ the ring of integers of $K_{\mathfrak{F}}$. The ring $W_{\mathfrak{F}}(k)$ is a totally ramified extension of $W(k)$ of degree g, and since $W_{\mathfrak{F}}(k)$ arises from an Eisenstein polynomial, the relation $T^g = \mu p$ holds for some $\mu \in W_{\mathfrak{F}}(k)^\times$ i.e., some μ of T-valuation zero. If the field k is algebraically closed, then the equation $X^\sigma = (T^\sigma/T)X$ in X has a nonzero solution modulo T, and so by the σ-variant of Hensel's lemma (e.g., used in [66, Lem. 2.2, p.29]), has a non-zero solution in $W_{\mathfrak{F}}(k)$. Then T/X is a uniformizer of $W_{\mathfrak{F}}(k)$. Unless otherwise mentioned, k is algebraically closed in the sequel, and we thus suppose that T is a uniformizer such that $T^\sigma = T$.

Definition 1.2.6. An **F-crystal** (M, Φ) with RM by $\mathfrak{F}$ is a free module M of finite rank over $W_{\mathfrak{F}}(k)$ equipped with a σ-linear injective map $\Phi : M \longrightarrow M$ such that $M/\Phi M$ has finite length as a $W_{\mathfrak{F}}$-module.

Since we are interested in p-divisible groups, it is useful to introduce *Dieudonné modules*, which give a full subcategory of the category of F-crystals, anti-equivalent to the category of p-divisible groups ([18]). This anti-equivalence holds with additional structure e.g., RM, by functoriality of the construction.

Definition 1.2.7.

- The ring $E = W_{\mathfrak{F}}(k)[F, V]$ is the ring of non-commutative polynomials of the form

$$w + \sum_{r=1}^{n} a_r F^r + \sum_{s=1}^{m} b_s V^s, \qquad w, a_r, b_s \in W_{\mathfrak{F}}(k),$$

satisfying the multiplication rules :

$$VF = FV = p,\ Fw = w^\sigma F,\ wV = Vw^\sigma.$$

- The ring $\widehat{E_k}$ is:

$$W_{\mathfrak{F}}(k)((F)) = \left\{ \sum_{i>-\infty} a_i F^i, a_i \in W_{\mathfrak{F}}(k), Fa = a^\sigma F, a \in W_{\mathfrak{F}}(k) \right\}.$$

- The ring E_k is defined to be the subring $W_{\mathfrak{F}}(k)[[F]] \subset \widehat{E_k}$. Note that $\widehat{E_k}$ is the localization of E_k at (F).

Remark 1.2.8. The letter F (resp. V) stands for Frobenius (resp. Verschiebung).

Definition 1.2.9. A **Dieudonné module** $\mathbb{D}$ is a left $W_{\mathfrak{F}}(k)[F,V]$-module free of finite rank over $W_{\mathfrak{F}}(k)$ with the condition that $\mathbb{D}/F\mathbb{D}$ has finite length.

Remark 1.2.10. A Dieudonné module M is closed under Frobenius and Verschiebung i.e., $FM \subseteq M$, and $VM \subseteq M$. These conditions imply that the slopes of M (i.e., of the associated F-isocrystal) are ≥ 0 (respectively, ≤ 1) (cf. [66, §4, p. 34]).

An F-crystal M with RM can be viewed as a $W_{\mathfrak{F}}(k)[F]$-module, where F acts Frobenius-linearly. If F is *topologically nilpotent* e.g., $\cap_{i\geq 0} F^i M = 0$, M can be viewed as an E_k-module, and reciprocally, any E_k-module M free of finite rank over $W_{\mathfrak{F}}(k)$ with M/FM of finite length can be viewed as an F-crystal with RM on which F is topologically nilpotent.
A Dieudonné module M is free of finite rank over $W_{\mathfrak{F}}(k)$, hence (M,F) is always an F-crystal, but an F-crystal (M,F) is a Dieudonné module if and only if $pM \subset FM$ (so that Verschiebung is defined as the map $V := F^{-1}p : M \longrightarrow M$).

Proposition 1.2.11. (Fitting's Lemma, [64, §VI 5.7-5.8, p. 180]) A crystal (M,F) with RM is decomposable uniquely in a direct sum:

$$M = M_{etale} \oplus M_{local},$$

where M_{etale} is a crystal with RM on which F is an isomorphism, and M_{local} is a crystal with RM on which F is topologically nilpotent.

Proof. Let $n \in \mathbb{N}$. We will prove things mod T^n. Let $(M/T^nM, \overline{F})$ be the reduced crystal. Since k is perfect, for all $m \in \mathbb{N}$, $\mathrm{Im}(\overline{F^m})$ is a $W_{\mathfrak{F}}(k)/T^nW_{\mathfrak{F}}(k)$-submodule of M/T^nM. Since the latter is of finite length, for m big enough, the following equalities hold :

$$(M/T^nM)_{local} := \bigcup_{i\geq 0} \ker \overline{F^i} = \ker \overline{F^m} \text{ and } (M/T^nM)_{etale} := \bigcap_{i\geq 0} \mathrm{Im}\overline{F^i} = \mathrm{Im}\overline{F^m},$$

and $M/T^nM = (M/T^nM)_{local} \oplus (M/T^nM)_{etale}$ since M/T^nM is a finite length $W_{\mathfrak{F}}(k)$-module (cf. [41, Lem., p. 39]). We then define $M_{local} = \varprojlim (M/T^nM)_{local}$ and $M_{etale} = \varprojlim (M/T^nM)_{etale}$.

□

Similarly, we can replace F by V in the statement of Fitting's Lemma for F-crystals, and we obtain the following decomposition for any Dieudonné module $\mathbb{D}$:

$$\mathbb{D} = \mathbb{D}_{etale,etale} \oplus \mathbb{D}_{etale,local} \oplus \mathbb{D}_{local,etale} \oplus \mathbb{D}_{local,local}.$$

However, $\mathbb{D}_{etale,etale} = 0$, for if F and V are both isomorphisms on a Dieudonné module $\mathbb{D}'$, then $FV\mathbb{D}' = p\mathbb{D}' = \mathbb{D}'$, and thus $\mathbb{D}'/p\mathbb{D}' = 0$, and since $rk_k(\mathbb{D}'/p\mathbb{D}') = g \cdot rk_{W_{\mathfrak{F}}(k)}\mathbb{D}'$, if follows that $\mathbb{D}' = 0$). Also, there is a duality functor called *Cartier duality* which in particular switches Frobenius and Verschiebung ([41]); Cartier duality establishes an equivalence of categories between the category of local-étale Dieudonné modules and the category of étale-local Dieudonné modules. Thus, to classify Dieudonné modules, it suffices to classify all local Dieudonné modules. Since the category of *local* F-crystals with RM is equivalent to the category of E_k-modules, it suffices to classify E_k-modules. This is the content of the next section.

1.3 Classification up to isomorphism

We go over Manin's arguments and establish the classification of Dieudonné modules up to isomorphism. Only trivial technical modifications are applied to Manin's original ideas. Our goal in Subsections 3.1 to 3.5 is to convince the reader that this is indeed the case. To this end, we highly recommend that the reader keep a copy of [66, §III] at hand, since we do not reproduce Manin's proofs in their entirety. As noted earlier, even though the statements of Theorems, Lemmas, Corollaries involve general Dieudonné modules, the proofs (especially those quoted from [66]) are written for local Dieudonné modules, i.e. E_k-modules.
In the classification up to isomorphism of Dieudonné modules, we suppose that:

- the field k is algebraically closed;
- the field $\mathfrak{F}$ is a totally ramified extension of $\mathbb{Q}_p$.

1.3.1 Overview of Manin's classification in the totally ramified case

Let k be algebraically closed, and let $\mathfrak{F}$ be a totally ramified extension of $\mathbb{Q}_p$. The main tools that appear in Manin's classification are two finiteness theorems and some algebro-geometric classifying spaces. The key idea behind the Finiteness Theorems is the concept of a *special* module, a concept we define below; a crucial fact is that every module has a unique maximal special submodule, of finite colength. Here are the results we establish below.

Definition 1.3.1. Two Dieudonné modules M_1, M_2 are **isogenous** if there is an injective homomorphism $\phi : M_1 \hookrightarrow M_2$ such that $M_2/\phi(M_1)$ has finite length over $W_{\mathfrak{F}}(k)$. If M_1 is isogenous to M_2, we write: $M_1 \sim M_2$.

Remark 1.3.2. Since k is algebraically closed, the isogeny class of a Dieudonné module is uniquely determined by the associated isocrystal. Isogeny is an equivalence relation.

Theorem 1.3.3. (First Finiteness Theorem) Let M be a Dieudonné module. There exists only a finite number of non-isomorphic special modules isogenous to M.

Theorem 1.3.4. (Second Finiteness Theorem) Let M be a Dieudonné module. The module M has a maximal special submodule M_0. The length $[M : M_0]$ is bounded uniformly in the isogeny class of M.

Theorem 1.3.5. (Classification Theorem) Let k be an algebraically closed field. A Dieudonné module M is determined by the following collection of invariants:

- the system of non-negative integers (m_i, n_i, q_i) which defines the isogeny class of M :

  $$M \sim \oplus_i E/E(F^{m_i} - T^{q_i}V^{n_i}).$$

  The numbers $\frac{gn_i+q}{g(m_i+n_i)}$ are the slopes of M, thus the restriction

  $$(m_i + n_i, gn_i + q_i) = 1.$$

  The triples (m_i, n_i, q_i) are uniquely defined from the slopes by the condition $0 \leq q_i < g$, and the condition on slopes $0 \leq \frac{gn_i+q}{g(m_i+n_i)} \leq 1$ (arising from the fact that M is a Dieudonné module) implies that q_i, n_i are nonnegative and $m_i > 0$;

- the maximal special submodule $M_0 \subset M$ (parametrized by discrete invariants);

- a $\Gamma(M_0, H)$-orbit of a point corresponding to M in a constructible algebraic set $A(M_0, H)$, where H is a nonnegative integer that depends only on (m_i, n_i, q_i), $A(M_0, H)$ and $\Gamma(M_0, H)$ depend only on M_0 and H, and $\Gamma(M_0, H)$ is a *finite* group.

Two E-modules are isomorphic if and only if all these invariants coincide.

We explain how the decomposition $M \sim \oplus_i E/E(F^{m_i} - T^{q_i}V^{n_i})$ is equivalent to the Dieudonné-Manin decomposition.
Note that $V := pF^{-1}$, so $E/E(F^m - T^qV^n) \sim E/E(F^m - T^q(pF^{-1})^n)$. Moreover, by [66, Lem. 2.5],

$$E/E(F^m - T^q(pF^{-1})^n) \sim E/E(F^m - F^{-n}T^{gn+q}) \sim E/E(F^{m+n} - T^{gn+q}),$$

hence the condition $(m+n, gn+q) = 1$. Note that the rank of M over $W_{\mathfrak{F}}(k)$ is $\sum_i (m_i + n_i)$. We show how to find the system of triples of integers starting from the Dieudonné-Manin classification. Without loss of generality, suppose

$$M \sim E/E(F^r - T^s), (r,s) = 1,$$

and $r, s > 0$. Define q such that $q = s \mod g$, $0 \leq q < g$ and define $n := \frac{s-q}{g}$. The integer m is defined as $r - n$.

Remark 1.3.6. The spaces arising in the classification up to isomorphism are quite amenable to study. In particular, the dimensions of their components are often easy to determine.

1.3.2 Special modules

Definition 1.3.7. ([66, §2, p. 37]) Let M be a local Dieudonné module.
An E_k-submodule M' of $M_F := \widehat{E_k} \otimes_{E_k} M$ is **dense** if its localization M'_F is M_F.

Lemma 1.3.8. An E_k-module M' is isogenous to an E_k-module M if and only if it is isomorphic to a dense E_k-submodule of M_F.

Proof. [66, Lem. 3.1]. □

We henceforth classify dense submodules of M_F.

Lemma 1.3.9. ([66, Lem. 3.2]) Let $M = \oplus_i E/E(F^{m_i} - T^{q_i}V^{n_i})$. An E_k-submodule M' of M_F is dense if and only if its rank, as $W_{\mathfrak{F}}(k)$-module, is $\sum_i (m_i + n_i)$.

Proof. Clear, because the rank of M is $\sum_i (m_i + n_i)$. □

Corollary 1.3.10. Dieudonné modules that are isogenous have the same rank.

Definition 1.3.11.

- An **isoclinic** module M of type (m, n, q) is a Dieudonné module M isogenous to $r \cdot E/E(F^m - T^q V^n), (gn + q, m + n) = 1$, $r \in \mathbb{N}$.
- An isoclinic module M of type (m, n, q) is said to be **special** if $F^m M = T^q V^n M$. An arbitrary Dieudonné module M is said to be **special** if $M \cong M_1 \oplus \cdots \oplus M_\ell$, where M_i, $1 \leq i \leq \ell$, are maximal isoclinic special submodules of M.

N.B. Manin calls isoclinic modules *homogenous*.

Example 1.3.12. The module $\oplus_i E/E(F^{m_i} - T^{q_i} V^{n_i})$ is special. It suffices to check the claim on isoclinic components. Consider $M = E/E(F^m - T^q V^n)$. A basis of the module M is given by $1, F, F^2, \ldots, F^{m+n-1}$. Let $x = \sum_{i=0}^{m+n-1} a_i F^i$, for $a_i \in W_{\mathfrak{F}}(k)$. Then

$$F^m x = \sum_{i=0}^{m+n-1} a_i^{\sigma^m} F^m F^i = \sum_{i=0}^{m+n-1} a_i^{\sigma^m} T^q V^n F^i = T^q V^n \sum_{i=0}^{m+n-1} a_i^{\sigma^{m+n}} F^i,$$

i.e., for any $x \in M$, there exists $y \in M$ such that $F^m x = T^q V^n y$, and reciprocally. Thus, $F^m M = T^q V^n M$.

Definition 1.3.13. Let M be an isoclinic module of type (m, n, q). An element $x \in M$ is said to be **special** if $F^m x = T^q V^n x$.

Example 1.3.14. The module $\oplus_i E/E(F^{m_i} - T^{q_i} V^{n_i})$ is special, but not all its elements are special. E.g., if x is special in $E/E(F^m - T^q V^n)$, then λx is special if $F^m(\lambda x) = T^q V^n(\lambda x)$, that is, if and only if $\lambda^{\sigma^m} F^m x = \lambda^{\sigma^{-n}} T^q V^n x$, or $\lambda^{\sigma^m} = \lambda^{\sigma^{-n}}$ since $F^m x = T^q V^n x$. Succinctly, $\lambda^{\sigma^{m+n}} = \lambda$ i.e., $\lambda \in W_{\mathfrak{F}}(\mathbb{F}_{p^{m+n}})$.

Lemma 1.3.15. ([66, Lem. 3.3]) A isoclinic module M of type (m, n, q) is special if and only if as a $W_{\mathfrak{F}}(k)$-module, it has a basis consisting of special elements (called a special basis) i.e., elements $x_1, \ldots, x_{m+n}$ such that $F^m x_i = T^q V^n x_i$ for all i.

Proof. (Sketch) The proof in Manin is terse; we make explicit his reference to a result of Fitting. Incidentally, the proof shows that a non-trivial Dieudonné module M such that $F^m M = T^q V^n M$ is necessarily isoclinic of type (m, n, q). Manin's proof first proceeds to show in a one-line computation that if the module M has a special basis, then it is special. Conversely, from an isoclinic special module with an arbitrary free $W_{\mathfrak{F}}$-basis, it is possible to construct a special basis by using Fitting's result applied to the operator $T^{-q}V^{-n}F^m$, which induces a σ^{m+n}-semilinear automorphism on the k-vector space M/pM. Fitting's Lemma thus shows that there is a basis $x_i^{(1)}$ such that $T^{-q}V^{-n}F^m x_i^{(1)} = x_i^{(1)} \mod p$. The rest of the proof shows that we can find compatible elements $x_i^{(r)}$ such that $T^{-q}V^{-n}F^m x_i^{(r)} = x_i^{(r)} \mod p^r$ for all r.

Lemma 1.3.16. (Fitting) Let k be an algebraically closed field of characteristic p, and let $\mathcal{V}$ a k-vector space of dimension n. Let $q = p^a$, for some $a \in \mathbb{Z}\backslash 0$ and $\phi : \mathcal{V} \longrightarrow \mathcal{V}$ an additive bijection such that for all $\lambda \in k$, for all $v \in \mathcal{V}$, we have $\phi(\lambda v) = \lambda^q \phi(v)$. Then there exists a base $(e_1, \ldots, e_n)$ of $\mathcal{V}$ such that $\phi(e_i) = e_i \ \forall i$.

Proof. Without loss of generality, we may suppose that $a > 0$. We first claim there is a $w \in \mathcal{V}\backslash\{0\}$ such that $\phi(w) = w$. Let $0 \neq v \in \mathcal{V}$, and $r \in \mathbb{N}^*$ be the biggest integer such that $(v, \phi(v), \ldots, \phi^{r-1}(v))$ is free. There exist $\alpha_i \in k$ such that

$$\phi^r(v) = \sum_{i=0}^{r-1} \alpha_i \phi^i(v).$$

For $x = (x_1, \ldots, x_n) \in k^n$, let $w = w(x) = \sum_{i=0}^{r-1} x_i \phi^i(v)$. We solve for $\phi(w) = w$. We reduce this to solving a single equation:

$$\phi(w) = \sum_{i=0}^{r-2} x_i^q \phi^{i+1}(v) + x_{r-1}^q \sum_{i=0}^{r-1} \alpha_i \phi^i(v) = \sum_{i=0}^{r-1} x_i \phi^i(v) = w.$$

We obtain a linear system by equating terms:

$$\alpha_0 x_{r-1}^q = x_0$$

$$x_0^q + \alpha_1 x_{r-1}^q = x_1$$

$$\cdots$$

$$x_{r-2}^q + \alpha_{r-1} x_{r-1}^q = x_{r-1}$$

If we combine all equations into one, we obtain :

$$x_{r-1} = \alpha_0^{q^{r-1}} x_{r-1}^{q^r} + \cdots + \alpha_{r-1}.$$

Since this equation is non-trivial (there is an i such that $\alpha_i \neq 0$ and $q > 0$) and the field k is algebraically closed, there is a non-trivial solution, and thus $\phi(w) = w$. Let $(e_1, \ldots, e_r)$ be a system of linearly independant vectors such that for all i, $\phi(e_i) = e_i$. Consider the subspace $\mathcal{W} \subset \mathcal{V}$ generated by all these vectors. If $\mathcal{W} \neq \mathcal{V}$, it follows from our previous claim that there exists $f \in \mathcal{V} \backslash \mathcal{W}$ such that $\pi(f) \in \mathcal{V}/\mathcal{W}$, (where $\pi : \mathcal{V} \twoheadrightarrow \mathcal{V}/\mathcal{W}$ is the projection), and $\pi(f)$ is fixed under $\pi(\phi)$. This means that there are β_i such that

$$\phi(f) = f + \sum_{i=1}^{r} \beta_i e_i.$$

Just put $e_{r+1} = f + \sum_{i=1}^{r} y_i e_i$ for some variables $y_i \in k$. Again, we solve the equation $\phi(e_{r+1}) = e_{r+1}$ in the variables y_i, e.g. we solve

$$e_{r+1} + \sum_{i=1}^{r} (\beta_i + y_i^q) e_i = e_{r+1} + \sum_{i=1}^{r} y_i e_i,$$

which is possible, since for all i, $y_i^q - y_i = -\beta_i$ has a solution (k being algebraically closed). □

□

Theorem 1.3.17. ([66, Thm. 3.1, p. 39]) Let M be a Dieudonné module. Then among the special submodules of M there exists a unique maximal one, $M_0 \subset M$. The factor module M/M_0 is of finite length.

Proof. The maximal special submodule is obtained as a direct sum of isoclinic special submodules, and the proof is the same as in [66, Thm. 3.1]. □

1.3.3 The First Finiteness Theorem

We define the cyclic local algebra $E_{m,n,q}$ we use in the proof of the First Finiteness Theorem. We denote by $K_{\mathfrak{F}}(\mathbb{F}_{p^{m+n}})$ the subfield of $K_{\mathfrak{F}}$ fixed under σ^{m+n}. With this notation, $K_{\mathfrak{F}}(\mathbb{F}_p) = \mathfrak{F}$.

Definition 1.3.18. Let m, n, q be non-negative integers such that $0 \leq q < g$ and $\frac{gn+q}{g(m+n)}$, is the slope of an isosimple Dieudonné module (i.e., $(m+n, gn+q) = 1$, and $0 \leq \frac{gn+q}{g(m+n)} \leq 1$). Let $E_{m,n,q}$ be the associative $W_{\mathfrak{F}}(\mathbb{F}_{p^{m+n}})$-algebra (with unit) generated by θ such that

$$\theta^{m+n} = T, \theta\alpha = \alpha^{\sigma^{-b}}\theta, \ \alpha \in W_{\mathfrak{F}}(\mathbb{F}_{p^{m+n}}),$$

where b is such that $-b(gn+q) = 1 \mod m+n$.

Note that the center of $E_{m,n,q}$ is $\mathcal{O}_{\mathfrak{F}}$, the ring of integers of $\mathfrak{F}$: since $-b$ is a unit modulo $m+n$, $\alpha^{\sigma^{-b}} = \alpha$ implies that $\alpha^{\sigma^{-b(gn+q)}} = \alpha^{\sigma^{1+a(m+n)}} = \alpha^{\sigma} = \alpha$, and thus $\alpha \in \mathcal{O}_{\mathfrak{F}}$.

Let $K_{m,n,q} := E_{m,n,q} \otimes \mathbb{Q}$. It is a division algebra: let $x = \sum_{i=0}^{m+n-1} a_i \otimes \theta^i$ be a right zero divisor. By multiplying by suitable powers of T and θ, we can suppose that $a_i \in W_{\mathfrak{F}}(\mathbb{F}_{p^{m+n}})$, and $a_0 \notin TW_{\mathfrak{F}}(\mathbb{F}_{p^{m+n}})$, up to relabeling. The matrix of right multiplication by X in the basis $1, \ldots, \theta^{m+n-1}$ is (write τ for σ^{-b}) :

$$\begin{pmatrix} a_0 & a_1 & \cdots & a_{m+n-1} \\ Ta_{m+n-1}^{\tau} & a_0^{\tau} & \cdots & a_{m+n-2}^{\tau} \\ \cdots & \cdots & \cdots & \cdots \\ Ta_1^{\tau^{m+n-1}} & a_{m+n-1}^{\tau^{m+n-1}} & \cdots & a_0^{\tau^{m+n-1}} \end{pmatrix}$$

Its determinant is congruent to $a_0 a_0^{\tau} \cdot \cdots \cdot a_0^{\tau^{m+n-1}} = \mathrm{Norm}(a_0) \mod T$, which cannot be zero, contradiction.

We introduce an isosimple module $M_{m,n,q}$ which will be useful in the explicit computation of modules spaces. Define:

$$M_{m,n,q} := W_{\mathfrak{F}}(k) \otimes_{W_{\mathfrak{F}}(\mathbb{F}_{p^{m+n}})} K_{m,n,q}.$$

Recall that $T^g = p \cdot \mu$ for some $\mu \in W_{\mathfrak{F}}(k)^{\times}$ from the discussion following the Dieudonné-Manin classification (Theorem 1.2.4). The module $M_{m,n,q}$ is a vector space over $K_{\mathfrak{F}}$, a right $K_{m,n,q}$-module and has a E-module structure given by:

$$\begin{aligned} F\theta^i &= \theta^{i+gn+q}; \\ V\theta^i &= \mu\theta^{i+gm-q}; \\ T\theta^i &= \theta^{i+m+n}, \end{aligned}$$

bearing in mind that F is σ-linear on $W_{\mathfrak{F}}(\mathbb{F}_{p^{m+n}})$ and V is σ^{-1}-linear on $W_{\mathfrak{F}}(\mathbb{F}_{p^{m+n}})$. The relation $V\theta^i = \mu\theta^{i+gm-q}$ actually follows from the actions of F and T by using the relations $T^g = \mu \cdot p$ and $FV = p$. Note that $gm - q \geq 0$ since $\frac{gn+q}{g(m+n)} \leq 1$ implies that $gn + q \leq gm + gn$. Note that $FV = VF = p$, with the above relations, is equivalent to the equality $\mu = \mu^{\sigma}$ because we picked our uniformizer T such that $T^{\sigma} = T$, and $T^g = \mu \cdot p$ implies that $\mu = \mu^{\sigma}$.

Lemma 1.3.19. ([66, Lem. 3.5])

- The module $M_{m,n,q}$ is isogenous to $E/E(F^{m+n} - T^{gn+q})$.
- Any non-zero finitely generated E-submodule of $M_{m,n,q}$ is dense.

Proof.

- Since $F^{m+n}\theta^i = \theta^{i+(gn+q)(m+n)}$, and $T^{gn+q}\theta^i = \theta^{i+(m+n)(gn+q)}$, the result follows from the relation: $F^{m+n}\theta^i = T^{gn+q}\theta^i$ and the fact that both modules have the same rank $m + n$.

- The second statement follows from the fact that $M_{m,n,q}$ is isosimple.

□

Lemma 1.3.20. Let $\mathfrak{T} \subset W_{\mathfrak{F}}(k)$ be a multiplicative system of representatives for the field k such that $0 \in \mathfrak{T}$. Any $x \in M_{m,n,q}$ can be uniquely expressed as:

$$x = \sum_{i > -\infty} \epsilon_i \theta^i, \quad \epsilon_i \in \mathfrak{T}.$$

In this notation, the element x is special if and only if $\epsilon_i^{\sigma^{m+n}} = \epsilon_i$.

Proof. [66, Lem. 3.6]. In particular, the condition of x to be special is that

$$F^{-m} T^q V^n x = x,$$

i.e., $\sum \epsilon_i \theta^i = \sum \epsilon_i^{\sigma^{-m-n}} \theta^i$, since $m(gn+q) - n(gm-q) = q(m+n)$, hence the equality $\epsilon_i^{\sigma^{m+n}} = \epsilon_i$. □

Lemma 1.3.21. One has

$$\mathrm{Aut}_{\widehat{E_k}}(M_{m,n,q}) = K^{\times}_{m,n,q},$$

where the action of $K^{\times}_{m,n,q}$ is given by multiplication on the right. In particular, an automorphism of $M_{m,n,q}$ leaving all special elements fixed is the identity.

Proof. As in the proof of [66, Lem. 3.7], it is enough to check this on $\alpha = \epsilon\theta^j \neq 0$, $\epsilon \in \mathfrak{T} \cap W_{\mathfrak{F}}(\mathbb{F}_{p^{m+n}})$. Then we have:

$$F\Big((\sum_i a_i \theta^i)\epsilon\theta^j\Big) = F\Big(\sum_i a_i \epsilon^{\sigma^{-bi}} \theta^{i+j}\Big) = \sum_i a_i^{\sigma} \epsilon^{\sigma^{-bi+1}} \theta^{i+j+gn+q}.$$

On the other hand,

$$\Big(F(\sum_i a_i \theta^i)\Big)\epsilon\theta^j = (\sum_i a_i^{\sigma} \theta^{i+gn+q})\epsilon\theta^j = \sum_i a_i^{\sigma} \epsilon^{\sigma^{-b(i+gn+q)}} \theta^{i+j+gn+q}.$$

Since $-b(gn+q) = 1$ modulo $m+n$, the assertion follows. □

The following discussion follows closely [66, §§2, p. 47]. Let M be a module isogenous to a simple module of slope $(m+n, gn+q)$. We embed M in $W_{\mathfrak{F}}(k) \otimes K_{n,m,q}$. Every element x of M can be written in the form $x = \sum_{i>-\infty} \epsilon_i \theta^i$. Let us put $\nu(x)$ to be the minimal i such that $\epsilon_i \neq 0$. We choose an element $x = \sum_{i \geq i_0} \epsilon_i \theta^i$ for which $i_0 = \nu(x)$ has the least possible value (for the given embedding), and consider a new embedding $M \longrightarrow M_F$ for which $1 + \sum_{i>0} \eta_i \theta^i \in M$ (this is the composition $M \xrightarrow{\psi} M_F \xrightarrow{\phi} M_F$, where ϕ is right multiplication by $\theta^{-i_0} \in K_{m,n,q}$ and ψ is the original embedding). We identify M with its image under this embedding. Then M is included in the submodule $W_{\mathfrak{F}}(k) \otimes E_{m,n,q}$ and contains an element congruent to 1 mod $W_{\mathfrak{F}}(k) \otimes E_{m,n,q}\theta$.

We define:

$$J = J(M) = \{\nu(x) | x \in M\}.$$

It is a set of non-negative integers containing 0. It is easy to see that $\nu(Fx) = \nu(x) + gn + q$, $\nu(Vx) = \nu(x) + gm - q$, $\nu(Tx) = \nu(x) + m + n$. Thus, the set J is invariant under translations of the form

$$a(gn+q) + b(gm-q) + c(m+n), \quad a, b, c \geq 0.$$

Since $(gn+q, m+n) = 1$, $\mathbb{N} \backslash J$ is finite: clearly, from [66, Lem. 3.8], every integer $N \geq (gn+q-1)(m+n-1)$ is in J.

Example 1.3.22. We list the possible sets $\overline{J}$ that can arise for $g = 4$ and rank 2 modules under the condition that $(gn+q, m+n) = 1$.

	$m=2, n=0$	$m=1, n=1$
$q=1$	$\varnothing$	$\varnothing, \{1\}$
$q=3$	$\varnothing, \{1\}$	$\varnothing$

We now give a nice description of isosimple modules.

Lemma 1.3.23. ([66, Lem. 3.9]) Let M be an isosimple module of type (m, n, q), with $(gn + q, m + n) = 1$. Consider the finite set of integers $\overline{J}(M) = \mathbb{N}\backslash J(M)$.

1. The set $\overline{J}$ does not depend on the choice of the embedding and is an invariant of the module M (N.B. we restrict ourselves to embeddings that satisfy $\min\{\nu(x)|x \in M\} = 0$).

2. For the given embedding $M \hookrightarrow W_{\mathfrak{F}}(k)\otimes E_{m,n,q}$, the module M contains a system of elements of the form:

$$z_{j_i} = \theta^{j_i} + \sum_{k\in\overline{J},k>j_i} \epsilon_{ik}\theta^k, \quad \epsilon_{ik} \in \mathfrak{T},$$

where $\mathfrak{T}$ is a multiplicative system of representatives for k. Here j_i runs over all numbers of J such that

$$j_i - (gn + q), j_i - (gm - q), j_i - (m + n) \in \overline{J}.$$

The system $\{z_{j_i}\}$ is uniquely determined and coincides with a minimal generating set of the E-module M. It will be called a standard system.

3. The module M is special if and only if all elements z_{j_i} are special.

Proof. We follow the proof of [66, Lem. 3.9] very closely.

1. By Proposition 1.3.21, any embedding $M \hookrightarrow W_{\mathfrak{F}}(k) \otimes E_{m,n,q}$ containing x such that $\nu(x) = \min_{y\in M} \nu(y) = 0$, differs from another such embedding by right multiplication by a *unit* in $E_{m,n,q}$ i.e., an element of valuation zero, for which $\{\nu(y), y \in M\}$ is invariant.

2. As in Manin, one constructs such a system by choosing at the j-th step, $j \in J$, any element $z' \in M$ of the form $z' = \theta^j + \sum_{i>j} \epsilon_{ij}\theta^i$ and then putting:

$$z_j = 0 \text{ if } j \in \cup_{j_k<j}\{j_k + a(gn + q) + b(gm - q) + c(m + n)\},$$

$$z_j = z'_j - \sum_{i\in J} \eta_{ij} z'_i, \quad \text{if } j \notin \cup_{j_k<j}\{j_k + a(gn+q) + b(gm-q) + c(m+n)\},$$

where the elements $\eta_{ij} \in W_{\mathfrak{F}}(k)$ are chosen so that the decomposition of the element z_j has the form given in the lemma i.e., $\epsilon_{ik} \in \mathfrak{T}$, the multiplicative system of representative fixed earlier, which is always possible by multiplying η_{ij} by a suitable unit. Let us show now that the elements z_j form a minimal generating system of the E_k-module M. In fact, from the equality

$$J = \cup_i\{j_i + a(gn+q) + b(gm-q) + c(m+n)\},$$

it follows that $M = \sum_i Ez_{j_i}$. The minimal number of generators of M agrees with the dimension of the k-linear space $M/(FM+VM+TM)$, by Nakayama's Lemma. But the images of z_{j_i} in this linear space are linearly independant, because the leading coefficients θ^{j_i} are all different by construction. Since the z_{j_i} generate M, it follows that they form a minimal system.

The same argument as in Manin gives the uniqueness of the system $\{z_{j_i}\}$ as well as statement (3).

□

Corollary 1.3.24. (First Finiteness Theorem for isosimple modules, [66, Cor. 1, p. 48]) There exists only a finite number of non-isomorphic special modules isogenous to a fixed simple module.

Proof. As in Manin, one notes that by Lemma 1.3.23, every such M is determined by its standard system $\{z_{j_i}\}$, where the condition that M is special implies that coefficients $\epsilon_{ik} \in \mathfrak{T} \cap W_{\mathfrak{F}}(\mathbb{F}_{p^{m+n}})$ that occur in the standard system, satisfy the conditions $\epsilon_{ik}^{\sigma^{m+n}} = \epsilon_{ik}$. The number of coefficients in such a collection is finite, and this implies that the number of non-isomorphic special modules isogenous to $E/E(F^m - T^qV^n)$ is finite.

□

Manin gives a reformulation of the description of special isosimple modules in more classical terms. The (non-principal) order $E^0_{m,n,q}$ is defined as

$$W_{\mathfrak{F}}(\mathbb{F}_{p^{m+n}})[\theta^{gn+q}, \theta^{gm-q}] \subset E_{m,n,q}.$$

Theorem 1.3.25. ([66, Thm. 3.6, p. 50]) The isomorphism classes of special modules of type (m, n, q) can be put into one-to-one correspondence with the classes of (fractional left) ideals of the order $E^0_{m,n,q}$.

Proof. Put $W_{m,n} := W_{\mathfrak{F}}(\mathbb{F}_{p^{m+n}})$. There is a correspondence between the special modules $M \subset W_{\mathfrak{F}}(k) \otimes K_{m,n,q}$ and the sets M_s of special elements in M via picking a special basis of M. By Lemma 1.3.20, the set M_s is actually a $W_{m,n}[F, V]$-submodule of M and, moreover, $F^m - T^q V^n$ belongs to the annihilator of M_s. Hence there is a natural left $W_{m,n}[F, V]/W_{m,n}[F, V](F^m - T^q V^n)$-module structure on M_s. The ring

$$W_{m,n}[F, V]/W_{m,n}[F, V](F^m - T^q V^n)$$

is isomorphic to the order $E^0_{m,n,q}$, by the map:

$$F \mapsto \theta^{gn+q}, \quad V \mapsto \theta^{gm-q},$$

hence M corresponds to the $E^0_{m,n,q}$-ideal M_s. We have supposed that M embeds into $W_{\mathfrak{F}}(k) \otimes K_{m,n,q}$ under a given embedding. Any other embedding of M in $W_{\mathfrak{F}}(k) \otimes K_{m,n,q}$ differs from the one chosen only by right multiplication by an element $\alpha \in K_{m,n,q}$, which maps special elements to special elements since $\alpha \in \mathrm{Aut}(M_{m,n,q}) = K^{\times}_{m,n,q}$ commutes with F and V. Finally, we can reconstruct an E-module M uniquely (up to isomorphism) from the $E^0_{m,n,q}$-module M_s, again by picking a special basis of M_s and letting M be the $W(k)$-module generated by this special basis. □

Lemma 1.3.26. (First Finiteness Theorem for isoclinic modules) Let

$$M \sim r \cdot E/E(F^m - T^q V^n)$$

be a special E-module and M_s the left $E^0_{m,n}$-module of its special elements.

- The module M_s is isomorphic to a certain $E^0_{m,n,q}$-submodule of a free $E_{m,n,q}$-module M'_s of rank r, containing a generating system $(x_1, \cdots, x_r)$ of M'_s as a $E_{m,n,q}$-module.

- Any $E^0_{m,n,q}$-submodule M_s of M'_s containing the system $(x_1, \cdots, x_r)$ possesses over $E^0_{m,n,q}$ a system of generators of the form

$$\sum_{i=1}^{r} x_i \sum_{j=0}^{c_{m,n,q}} \epsilon_{ij}\theta^j, \quad \epsilon_{ij} \in \mathfrak{T} \cap W_{\mathfrak{F}}(\mathbb{F}_{p^{m+n}}),$$

  where $c_{m,n,q}$ is the biggest number not representable as a sum

$$a(gn+q) + b(gm-q) + c(m+n),$$

  with $a, b, c \geq 0$, or 0.

Proof. Same proof as in [66, Lem. 3.10, p. 51].

- We take $M'_s := E_{m,n,q} \otimes M_s$. M'_s is clearly free of rank r. The map

$$M_s \longrightarrow E_{n,m} \otimes M_s, \quad m \mapsto 1 \otimes m,$$

  yields the required isomorphism.

- For any $N > c_{m,n,q}$, we have $x_i\theta^N \in M_s$ for all $i = 1, \ldots, r$, by definition of $c_{m,n,q}$. Pick any generating system, and write its elements in the form :

$$\sum_{i=1}^{r} x_i \sum_{j=0}^{\infty} \epsilon_{ij}\theta^j, \quad \epsilon_{ij} \in \mathfrak{T} \cap W_{\mathfrak{F}}(\mathbb{F}_{p^{m+n}}),$$

  removing terms in θ^j, $j > c_{m,n,q}$ since they already are in M_s.

□

Corollary 1.3.27. (First Finiteness Theorem) Let M be a Dieudonné module. There exist only a finite number of non-isomorphic special modules isogenous to M.

Proof. This follows from the definition of a special module: a special module is the sum of its maximal isoclinic special modules. Up to replacing M by an isogenous Dieudonné module, we can decompose it in a finite sum of isoclinic components $M = \oplus_t M_t$ of pairwise different slopes. Then by the First Finiteness Theorem for isoclinic modules, every isoclinic component M_t admits only finitely many non-isomorphic special modules isogenous to it. It is thus clear that the number of non-isomorphic special modules isogenous to M is also finite. □

1.3.4 Second finiteness theorem

Theorem 1.3.28. Let M be a Dieudonné module. Let M_0 be its maximal special module. Then $F^t M \subset M_0$ holds, for some $t \in \mathbb{N}$ depending only on the isogeny class of M.

Proof. See the proof of [66, §6, Thm. 3.8]. □

1.3.5 The algebraic structure on the module space

We follow [66, Chapter III, §3] very closely. For a reference on the general theory of ramified Witt vectors, see [45].

Definition 1.3.29. Let M be a Dieudonné module. Let M **belong** to M_0 if the maximal special submodule of M is isomorphic to M_0.

Remark 1.3.30. The module M belonging to M_0 can be realized as a dense submodule of $(M_0)_F$ containing M_0. There exists $h, g \in \mathbb{N}$ such that

$$M_0 \subset M \subset T^{-h} M_0 \quad \text{and } M_0 \subset M \subset F^{-g} M_0.$$

Definition 1.3.31. The T-height of $x \in M_F$ over the dense submodule M' of M_F is the least integer h such that $T^h x \in M'$. The T-height of a module $M'' \supset M'$ is the maximum of the T-heights of the elements of M'' over M'.

Theorem 1.3.32. ([66, Thm. 3.2]) There is a bijection between on one hand: the E-modules M such that M belongs to M_0 and M satisfies

$$M_0 \subset M \subset T^{-h}M_0 \tag{1.3.1}$$

and on the other hand : a certain constructible algebraic set $A(M_0, h)$ defined over k, i.e. a finite union of subsets of projective space that are locally closed in the Zariski topology.

Remark 1.3.33. In view of the Second Finiteness Theorem, we can take h big enough to get *all* modules M belonging to M_0.

Proof. The strategy of Manin's proof is outlined as follows :

- Parametrize all $W_{\mathfrak{F}}(k)$-modules satisfying Equation 1.3.1.
- Cut out algebraically the E_k-modules.
- Cut out algebraically the points not belonging precisely to M_0 (i.e. having too many special elements) to get the final constructible algebraic set.

We begin the proof per se:

- **Parametrize all $W_{\mathfrak{F}}(k)$-modules satisfying Equation 1.3.1**

  Definition 1.3.34. Let $M_0 \subset M \subset T^{-h}M_0$ be a $W_{\mathfrak{F}}(k)$-module. There exists a $W_{\mathfrak{F}}(k)$-basis $(x_1, \ldots, x_N)$ of M_0 such that

  $$(T^{-e_1}x_1, \ldots, T^{-e_N}x_n), \quad 0 \leq e_1 \leq e_2 \leq \cdots \leq e_N \leq h,$$

  is a $W_{\mathfrak{F}}(k)$-basis for M. We call the string of integers

  $$i(M_0, M) = e = (e_1, \ldots, e_N),$$

  the **e-index** of M.

The index defines the module M uniquely; note that we only used the $W_{\mathfrak{F}}(k)$-module structure.

Any module satisfying Equation 1.3.1 is completely determined by its image in $T^{-h}M_0/M_0$ under the homomorphism

$$M \longrightarrow M/M_0 \longrightarrow T^{-h}M_0/M_0.$$

We check that the group of automorphisms of $T^{-h}M_0/M_0$ is defined over k. The trick is to replace h by gh (we bring back the whole set-up to truncated Witt vectors $W_h(k) = W(k)/p^hW(k)$), and note that :

$$W_{\mathfrak{F}}(k) \cong \oplus_{i=1}^{g} W(k) \text{ as } W(k)\text{-modules ;}$$

$$W_{\mathfrak{F}}(k)/p^kW_{\mathfrak{F}}(k) \cong \oplus_{i=1}^{g} W_h(k) \text{ as } W(k)\text{-modules,}$$

where $W_h(k)$ are the Witt vectors of length h. Note that $T^{-h}M_0/M_0$ is a free module (of rank N, say) over $W_{\mathfrak{F}}(k)/p^hW_{\mathfrak{F}}(k)$.

Lemma 1.3.35. The group of automorphisms of $T^{-h}M_0/M_0$ is:

$$\begin{aligned} G_k := (M_N(W_{\mathfrak{F}}(k)/p^hW_{\mathfrak{F}}(k))^\times &\cong (M_N(\oplus_{i=1}^{g} W_h(k))^\times \\ &\cong \mathrm{GL}_N(W_h(k)) \oplus_{i=2}^{g} M_N(W_h(k)), \end{aligned}$$

where M_N represents the N-by-N matrices.

Proof. This follows from the formulae defining the multiplication of Witt vectors: The units in the Witt vectors $W(k)$ are the elements $w = (w_1, w_2, \dots,)$ whose *first* coefficient w_1 is non-zero, and the similar statement holds for the truncated Witt vectors. Since the multiplication of $\mathfrak{f}$ and $\mathfrak{h}$ for $\mathfrak{f} = (\mathfrak{f}_1, \mathfrak{f}_2, \dots, \mathfrak{f}_g)$ and $\mathfrak{h} = (\mathfrak{h}_1, \mathfrak{h}_2, \dots, \mathfrak{h}_g)$ in $W_{\mathfrak{F}}(k)$ is $\mathfrak{f} \cdot \mathfrak{h} = (P_1(\mathfrak{f}, \mathfrak{h}) = \mathfrak{f}_1\mathfrak{h}_1, P_2(\mathfrak{f}, \mathfrak{h}), \dots, P_g(\mathfrak{f}, \mathfrak{h}))$, for some polynomials $P_i(x, y)$ ([45, Eq. 6.14, §6.7, p. 60]), we can pick the

isomorphism $W_{\mathfrak{F}}(k) \cong \oplus_{i=1}^{g} W(k)$ so that an element $\mathfrak{f} \in W_{\mathfrak{F}}(k) \cong \oplus_{i=1}^{g} W(k)$ is invertible if and only if the first coefficient $\mathfrak{f}_1$ of $\mathfrak{f} = (\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_g)$ is invertible. Thus, a matrix $D \in (M_N(W_{\mathfrak{F}}(k)/p^h W_{\mathfrak{F}}(k))^{\times}$ with coefficients d^{ij}, $1 \leq i, j \leq N$ will be invertible if and only if the matrix D_1 whose entries are the coefficients $d_1^{ij}, 1 \leq i, j \leq N$, is invertible i.e., $D_1 \in \mathrm{GL}_N(W_h(k))$. □

This group G_k is defined over k (since the composition law of Witt vectors is defined over k), and its action on the space A_e of modules of index e is transitive. The action of the group can be transferred to M as follows : let $M_0 \subset M$, $g \in G_k$. Fix a right action of G_k on the factor module $T^{-h}M_0/M_0$; then

$$M_g = \{x | x \mod M_0 \in (M/M_0)g\}.$$

The same proof as in Manin's paper show that the stabilizer G_0 of the module M of index e is closed in G. Consequence : A_e is the set of geometric points of the homogeneous space of right cosets G/G_0.

- **Cut out algebraically the E-modules.**

  The module Mg is an E-module if $F(Mg) \subset Mg; V(Mg) \subset Mg$. Manin translates these conditions into two morphisms ϕ_1, ϕ_2 from G to a closed variety such that the set we are looking for is $H = \phi_1^{-1}(\overline{G_0}) \cap \phi_2^{-1}(\overline{G_0}), \overline{G_0}$ closed. The image of H under the projection $G \longrightarrow G/G_0$ is a constructible algebraic set whose geometric points are in one-to-one correspondence with the set of E-modules $M_0 \subset M$ of index e.

- **Cut out, among the E-modules, those that belong to M_0 only.** A special element $x \in T^{-h}M_0$ lies in M if and only if $(x \mod M_0)g^{-1} \in M/M_0$. But if we see $T^{-h}M_0/M_0$ as an affine variety over k,

$$\phi_x : G \longrightarrow T^{-h}M_0/M_0,$$

$$g \mapsto (x \mod M_0)g^{-1},$$

is a morphism. Thence $x \in Mg$ if and only if $g \in \phi_x^{-1}(M/M_0) = F_x$, a closed set. So we discard $\cup_x F_x$, for x special, $x \in T^{-h}M_0, x \notin M_0$.

Lemma 1.3.36. ([66, Lem. 3.4]) The set $\cup_x F_x$ is closed, since the special elements $x \in T^{-h}M_0$ belong to a finite number of cosets $\mod M_0$.

Proof. The cosets $x \mod (M_0)$ of special elements are in bijection with N-tuples $(a_1, \ldots, a_N), a_i \in W_{\mathfrak{F}}(k)/T^h W_{\mathfrak{F}}(k)$ such that $a_i^{\sigma^{m+n}} = T^q a_i$, and those N-tuples are finite in number. □

Summing up, we get a constructible algebraic set $A(M_0, h)$, but there are different points on it that correspond to isomorphic E-modules. The next theorem takes care of this.

Theorem 1.3.37. ([66, Thm. 3.3]) There exists a finite group of automorphisms $\Gamma(M_0, h)$ such that two points correspond to isomorphic Dieudonné modules if and only if they are contained in the same the orbit relative to $\Gamma(M_0, h)$.

Proof. We follow Manin's proof. The group $\Gamma = \mathrm{Aut}(\mathrm{M}_0)$ acts on $A(M_0, h)$ (it acts on A_e, and it maps $A(M_0, h)$ to $A(M_0, h)$, since the condition on the module M_0 is invariant under isomorphisms of M_0). Let $M', M'' \in A(M_0, h)$ be isomorphic modules. Any isomorphism $M' \longrightarrow M''$ induces an isomorphism of the corresponding special modules. Now M', M''' have the same maximal special submodule, namely M_0, therefore any isomorphism induces a certain automorphism of M_0. Since any element of Γ that does not move the coset of $x \mod M_0$ for all special elements $x \in T^{-h}M_0$, leaves all points of $A(M_0, h)$ fixed. But the special elements $x \in T^{-h}M_0$ belong to a finite number of cosets

mod M_0. We can thus take $\Gamma(M_0, h)$ to be the permutation group (of cosets) induced by the action of Γ, and it is clearly finite. □

This finishes the proof of Theorem 1.3.32.

□

1.3.6 Superspecial Dieudonné modules with real multiplication

Let L be a totally real field of degree g. In this section, we show that the general theory yields effective computations by counting the number of supersingular special Dieudonné modules with RM. We call a supersingular special module a **superspecial** module with RM by $\mathcal{O}_L$ if it is a $W(k) \otimes \mathcal{O}_L$-module. If $p\mathcal{O}_L = \mathfrak{p}^g$, then $W(k) \otimes \mathcal{O}_L$ is a totally ramified extension of $W(k)$ of degree g i.e., $\mathfrak{F} = L_{\mathfrak{p}}$.

Corollary 1.3.38. The number of isomorphism classes of superspecial Dieudonné modules with RM by $\mathcal{O}_L$ of rank 2 over a totally ramified prime $p = \mathfrak{p}^g$ is

$$\left[\frac{g}{2}\right] + 1.$$

Proof. This follows in a straightforward way from Lemmas 1.3.23 and 1.3.26: The supersingular isocrystal has slope $\frac{gn+q}{g(m+n)} = \frac{1}{2}$. We are looking at rank 2 modules (over $W_{\mathfrak{F}}(k)$), hence if g is odd, $m + n = 2$, and it follows that $gn + q = g$, hence

$$n = 1, q = 0 \text{ and } m = 1,$$

and the supersingular isocrystal is given by the isosimple module $E/E(F - V)$. We count the number of special crystals isogenous to $E/E(F - V)$ by looking at the discrete invariants. The triplet $\{gm-q, gn+q, m+n\}$ boils down to $\{g, 2\}$, hence for $g = 2k + 1$, the sets $\overline{J}$ have the shape $(1, 3, \ldots, 2c - 1)$, where $0 \leq c \leq k$ ($\overline{J}$ is empty

if $c = 0$): $|\overline{J}| \leq g$ since $g \in \{g, 2\}$, and even integers are ruled out since $2 \in \{g, 2\}$. The complement of such a set is

$$J_c = \{2a + (2k+1)b\} \cup \{2c + 1 + 2a + (2k+1)b\}, a, b \geq 0.$$

Recall that $E^0_{1,1,0} = W_{\mathfrak{F}}(\mathbb{F}_{p^2})[\theta^g]$, $\theta^2 = T$. By Lemma 1.3.23, the special submodule $M \subset W_{\mathfrak{F}}(k) \otimes E_{1,1,0}$ containing 1 is generated by the elements $1, \theta^{2c+1}$ if the set $J(M) = \{v(x) | x \in M\}$ coincides with J_c, and all the corresponding modules are non-isomorphic. Note that the number of modules is precisely $k + 1 = [g/2] + 1$, so this proves the classification theorem for g odd. If g is even, the isogeny class is given by the *non-simple* module $2{\cdot}E/E(F{-}T^{\frac{g}{2}})$, so $m = 1, n = 0, q = \frac{g}{2}$. What we need to conclude is a computation-free application of Lemma 1.3.26: since $E^0_{1,0,g/2} = W_{\mathfrak{F}}(\mathbb{F}_p)[\theta^{g/2}]$, $\theta = T$, the generating system of the special module M as an $E_{1,0,g/2}$-module can be chosen to be $\{1, \theta^c\}$, for $0 \leq c \leq g/2$, since it depends only on the valuations of the generators. According to Lemma 1.3.26, any $E^0_{1,0,g/2}$-submodule of M'_s, the left $E^0_{1,0,g/2}$-module of special elements of M, is generated by a system of the form:

$$z_1 = \epsilon_{11} \cdot 1 + \epsilon_{12} \cdot \theta^c,$$

$$z_2 = \epsilon_{21} \cdot 1 + \epsilon_{22} \cdot \theta^c,$$

$\epsilon_{cj} \in \mathfrak{T} \cap W_{\mathfrak{F}}(\mathbb{F}_p)$. By changing variables, we can suppose that $z_1 = 1, z_2 = \theta^c$, thence there is a unique superspecial crystal for every c, $0 \leq c \leq g/2$. The number of superspecial Dieudonné modules is uniformly $[g/2] + 1$ as claimed. □

Definition 1.3.39. We define the superspecial Dieudonné module M_c as follows, for $c \in \{0, \ldots, [g/2]\}$:

$$M_c \text{ is generated by } \begin{cases} \{1, \theta^{2c+1}\} & \text{if } g \text{ is odd} \\ \{1, \theta^c\} & \text{if } g \text{ is even} \end{cases}$$

Proposition 1.3.40. Supersingular special modules M are supersingular modules M with maximal a-number $a(M) = g$ (hence the name **superspecial**).

Proof. Recall that the a-number of a Dieudonné module M over $W(k)$ is defined as $a(M) := \dim_k M/FM + VM$. A supersingular special module M is supersingular i.e., of slope $\frac{1}{2}$ and special, therefore $F \cdot M = V \cdot M$ and since the $W(k)$-rank of M is $2g$, the a-number $a(M) = \dim_k M/FM + VM = \dim_k M/FM = \dim_k M/VM = g$, since $\dim_k M/FM + \dim_k M/VM = 2g$. In other words, any supersingular special module M is isomorphic to $\oplus_{i=1}^{g} W(k)[F,V]/(F-V)$ as $W(k)[F,V]$-module. □

We postpone a proof and a discussion of the endomorphism orders of superspecial crystals to Section 7 in Chapter II of this thesis, where we compute the orders of superspecial points on Hilbert moduli spaces in the totally ramified case.

1.4 Traverso's boundedness conjecture

In this section, we treat classical Dieudonné modules (without RM!). Traverso in his 1967 Pisa thesis [97] proved the following result:

Theorem 1.4.1. ([97]) Let k be an algebraically closed field of characteristic p. Let M, N be two Dieudonné modules over $W(k)$ of rank $2g$. If $M \cong N \mod p^{g^2+1}$, then $M \cong N$.

His work on a conjecture of Grothendieck led Traverso to speculate that much more is true:

Conjecture 1.4.2. ([98]) Let k be an algebraically closed field of characteristic p. Let M, N be two Dieudonné modules over $W(k)$ of rank $2g$. If $M \cong N \mod p^{g}$, then $M \cong N$.

Traverso also showed that for any g, there are Dieudonné modules M, N of rank $2g$ which are isomorphic modulo p^{g-1} but such that $M \ncong N$ ([98]).

Remark 1.4.3. ([13, p.8]) Zink proved in a letter to Chai ([115]) the following truncation result: A *crystal* M over k is determined, up to non-unique isomorphisms, by its quotient modulo p^N, for some suitable $N > 0$, depending only on the height of the module M and the maximum among the slopes of M.

An interesting test for Traverso's conjecture is the supersingular isocrystal.

Lemma 1.4.4. ([74, Proof of Prop. 1.6]) Let $\mathbb{D}_1$ be determined by its truncation modulo p^{n_1}, up to isomorphism. Let $\mathbb{D}_2 \longrightarrow \mathbb{D}_1$ be a degree p^{n_2} isogeny. Then $\mathbb{D}_2$ is determined by its truncation modulo $p^{n_1+n_2}$, up to isomorphism.

Minimal Dieudonné modules were first introduced by Manin ([66, p.45]): they are isomorphic to direct sums of modules $M_{m,n}, (m,n) = 1$, that we defined in Section 1.3.3. There is thus a unique minimal module for each Newton polygon. A minimal module is *special*, since $M_{m,n}$ is special.

Example 1.4.5. The superspecial crystal is minimal.

Minimal modules were also used in [54, Section 5.3] and their key truncation property was proved in [75].

Theorem 1.4.6. ([75, Thm. 1.2]) Let M, N be Dieudonné modules. Suppose that the module M is minimal. If $M/pM \cong N/pN$, then $M \cong N$.

Corollary 1.4.7. Let $\mathbb{D}_1$ be a *minimal* Dieudonné module. Suppose that the minimal degree of the isogeny between $\mathbb{D}_2$ and $\mathbb{D}_1$ is p^n. Then $\mathbb{D}_2$ is determined by its truncation modulo p^{n+1}.

We proceed with the computation in the supersingular isocrystal case. The superspecial module, denoted M_0, is the minimal supersingular module. We therefore only want to bound the degree of the isogeny between an arbitrary supersingular crystal and the superspecial crystal. To this end, we generalize [66, Theorem 3.15].

Theorem 1.4.8. The Dieudonné modules isogenous to $g \cdot E/E(F^m - V), m \geq 1$ split into $m(g-1)+1$ components. The indices are the $m(g-1)+1$ possibilities ranging from $(0, \ldots, 0)$ to $(0, \ldots, 0, 1, \ldots, 1)$ (with $m(g-1)$ repetitions of 1's).

Proof. The analogue of [66, Lem. 3.14] holds: any module is isomorphic to a *primitive* submodule whose F-height does not exceed m, and any primitive submodule whose F-height h is small or equal than m admits a cyclic factor module M/M_0, a generator of which is given by the image of an element of the form:

$$z = \theta_1^{-h} + \sum_{j=2}^{g} \sum_{i=1}^{h} \epsilon_{ij} \theta_j^{-i}, \epsilon_{ij} \in \mathfrak{T}, e_{hj} \neq 0 \text{ for all } j,$$

where θ_j is the element $\theta \in E_{m,1}$ in the jth copy of $E_{m,1}$. The rest of the proof follows exactly as in [66, Thm. 3.15]. □

Corollary 1.4.9. Let $m = 1$. The crystal $g \cdot E/E(F - V)$ is superspecial, and the maximal index corresponds to isogenies of degree p^{g-1}.

Corollary 1.4.10. Any supersingular crystal is determined up to isomorphism by its truncation modulo p^g.

Remark 1.4.11. This strengthens Traverso's and Vasiu's results ([97], [99, Prop. 3.4.1.1]) which gave the bound $g^2 + 1$ (resp. g^2).

1.5 Explicit computations of module spaces à la Manin

We present in this subsection explicit computations of modules spaces: an infinite family of non-supersingular Dieudonné modules (without RM), and the supersingular isocrystal with RM.

1.5.1 A family of non-supersingular Dieudonné modules

This example concerns classical Dieudonné modules i.e., $\mathfrak{F} = \mathbb{Q}_p$. Note that there is only one special module in the isogeny class of $M_0 = E/E(F - V^n) \oplus E/E(F^n - V)$, $n \geq 2$ (the case $n = 1$ is covered in [66, Thm. 3.15]). Write it as:

$$M_0 = W(k) \otimes E_{1,n} \oplus W(k) \otimes E_{n,1} = M_{01} \oplus M_{02}.$$

We will consider modules M containing M_0 and contained in:

$$M_{0F} = W(k) \otimes K_{1,n} \oplus W(k) \otimes K_{n,1}.$$

Any module isogenous to M_0 is isomorphic to a module contained in M_{0F}. We denote the element $\theta \in E_{1,n}$ (resp. $\theta \in E_{n,1}$) by θ_1 (resp. θ_2). By height, we mean in this example the F-height.

Lemma 1.5.1. Let M be isogenous to $E/E(F - V^n) \oplus E/E(F^n - V)$, $n \geq 2$.
Let M be an E-module such that $M_0 \subset M \subset M_{0F}$. Then the height of M over M_0 is smaller or equal to one. Moreover, M/M_0 is cyclic, and a generator is given by the image of an element of the form:

$$z = \theta_1^{-1} + \epsilon\theta_2^{-1}, \epsilon \neq 0.$$

The module $Ez + M_0$ belongs to the special submodule M_0 and its index over M_0 is $(0, \cdots, 0, 1)$.

Proof. • The calculations are similar to the proof of [66, Lem. 3.13a]. Let $x = F^{-h_1}x_1 + F^{-h_2}x_2 \in M$, $x_1 \in M_{01} \backslash FM_{01} \cup 0$, $x_2 \in M_{02} \backslash FM_{02} \cup 0$. We may suppose that x_i belong to a special basis of M_{0i}. We also assume that $M \neq M_0$, $x \neq 0$ and $h_1 h_2 > 0$. Then $x_2 \neq 0$, for otherwise $EF^{-h_1}x_1$ would be a special submodule of M not contained in M_0, which is impossible, because M_0 is maximal. Similarly, $x_1 \neq 0$. Further, $h_1 = h_2 = h$; for if $h_1 > h_2$, the element

$F^{h_2}x - x_2 = F^{-h_1+h_2}x \in M$ generates a special submodule not contained in M_0. Similarly, we obtain a contradiction in the case where $h_1 < h_2$. Finally, $h \leq 1$. For if $h > 1$, then

$$Vx = x' + x'', x' \in (M_{01})_F, x'' \in (M_{02})_F,$$

is such that $x'' \in M_{02}$, but $x' \in M_{01}$. Therefore x' generates a special submodule not contained in M_0, which is impossible. One sees that $h = 1$ if and only if $x_2 = V^{n-1}y$ for some $y \notin VM_{02}$.

- Same proof as in [66, Lem. 3.13b]
- The same argument as in [66, Lem. 3.13c] applies word for word, since $val_V(z) = n - 1$ for z of height 1.

□

Theorem 1.5.2. The modules isogenous to $E/E(F - V^n) \oplus E/E(F^n - V)$ are parametrized by $\mathbb{A}^1$.

Proof. The Dieudonné modules isogenous to $E/E(F - V^n) \oplus E/E(F^n - V)$ split into 2 components A_h, $0 \leq h \leq 1$. The component A_h consists of modules having a maximal special submodule of index $(0, \cdots, 0)$ if $h = 0$ (resp. $(0, \cdots, 0, 1)$ if $h = 1$). The space A_0 consists of one point, the special module itself, while A_1 is isomorphic to $\mathbb{A}^1\backslash\{0\}$, since $\epsilon = 0$ is excluded. The quotient of $\mathbb{A}^1\backslash\{0\}$ by the associated finite group Γ_h is necessarily isomorphic to $\mathbb{A}^1\backslash\{0\}$, since Γ_h is finite, and quotients of affine varieties by finite groups are affine varieties. We then glue A_0 and A_1 in the obvious way and we get $\mathbb{A}^1$, the affine line. □

Theorem 1.5.3. Let M_1, M_2 be two modules isogenous to

$$E/E(F - V^n) \oplus E/E(F^n - V).$$

Then $M_1/p^2M_1 \cong M_2/p^2M_2$ implies that $M_1 \cong M_2$.

Proof. Note that the special module $E/E(F-V^n) \oplus E/E(F^n-V)$ is *minimal* in the sense of [75]. Oort has shown that a minimal Dieudonné module M can be identified from its M/pM only. The index of any non-trivial module N over $E/E(F-V^n) \oplus E/E(F^n-V)$ is p, thence there is an isogeny $\phi : N \longrightarrow E/E(F-V^n) \oplus E/E(F^n-V)$ of degree p, and so N is determined by $N/p^{1+1}N = N/p^2N$ by Corollary 1.4.7. □

Remark 1.5.4. This theorem recovers a result of Vasiu ([99, Prop. 3.4.4.1, p. 32]).

1.5.2 The supersingular isocrystal in the totally ramified case

Case I: g odd.

We follow [66, Thm. 3.12] to study the case g odd. Any supersingular module is isogenous to the isosimple module $E/E(F-V)$. In Definition 1.3.39, we enumerated all special modules M_c isogenous to $E/E(F-V)$ by giving the set of discrete invariants J_c. By Lemma 1.3.23, any module over a special module corresponding to the set J_c has two standard generators:

$$z_1 = 1 + \sum_{k=1}^{h} \epsilon_{2k-1}\theta^{2k-1}, z_2 = \theta^{2h+1},$$

where $\epsilon_{2k-1} \in \mathfrak{T}$ are determined by M. We define a number d, $0 \leq d \leq h$, by the conditions:

$$\epsilon_{2k-1} \in W_{\mathfrak{F}}(\mathbb{F}_{p^2}), k \leq h-d,$$

$$\epsilon_{2(h-d)+1} \notin W_{\mathfrak{F}}(\mathbb{F}_{p^2}).$$

Theorem 1.5.5. Let M be a module belonging to M_c. The following holds:

1. The T-height of M is at most $[g/2]+1$.

2. The factor module M/M_c is generated by the coset of one element z, where

$$z = 1 + \sum_{k=1}^{d} \epsilon_{2k-1}\theta^{-(2k-1)}.$$

3. The **e**-index of M (see Definition 1.3.34) is $(0, d)$, for some $d \leq c \leq [g/2]$.

4. The space $\mathfrak{M}_c^d$ of modules M of **e**-index $(0, d)$ belonging to a fixed special module M_c has dimension d and is isomorphic to the complement of the disjoint union of p^2 hyperplanes

$$\overline{\epsilon_d} = a, a \in \mathbb{F}_{p^2}.$$

Proof. This follows very closely the calculations of [66, Thm. 3.12, Thm.3.15]. □

Case II: g even.

For g even, any supersingular module is isogenous to $2E/E(F - T^{\frac{g}{2}})$. The space of modules M belonging to a superspecial module M_c are always finite union of quasi-affine varieties. We use the same notation as in Example 1.5.1 i.e., we label θ_i the generator of the cyclic local algebra coming from the i-th copy of $E/E(F - T^{\frac{g}{2}})$. A submodule M, where $M_c \subset M \subset M_{c,F}$ is called *primitive* if it does not contain θ_1^{-1} and θ_2^{-1}. Any module isogenous to M_c is isomorphic to a primitive submodule of $M_{c,F}$ ([66, Lem. 3.14]).

Define the invariant d in the same fashion as in the g odd case.

Theorem 1.5.6. Let M be a module belonging to M_c. The following holds:

1. There is a primitive module M' isomorphic to M with T-height $d \leq \frac{g}{2}$.

2. The factor module M'/M_c is generated by the coset of z, where

$$z = \theta_1^{-d} + \sum_{k=1}^{d} \epsilon_k \theta_2^{-k}, \epsilon \in \mathfrak{T}, \epsilon_c \neq 0.$$

3. The index of M is $(0, d)$, for some $d \leq c \leq [g/2]$.

4. The space $\mathfrak{M}_c^d$ of modules M of index $(0, d)$ belonging to a fixed special module M_c has dimension d, and is isomorphic to the complement of the disjoint union of p^2 hyperplanes

$$\overline{\epsilon_d} = a, a \in \mathbb{F}_{p^2}.$$

Proof. Same as in [66, Lem. 3.14, Thm. 3.15]. □

Corollary 1.5.7. There are infinitely many non-isomorphic supersingular Dieudonné modules.

Remark 1.5.8. Cf. [1, Appendix].

1.6 Stratification(s) of the supersingular Newton polygon stratum

In this section, we show that the stratification introduced by Andreatta-Goren in [1] coincides with the stratification suggested by the decomposition of the moduli spaces à la Manin at least on the supersingular Newton polygon stratum.

We recall briefly the definition of the stratification of [1]. Let p be a totally ramified prime. Let A/k be a polarized abelian variety with RM, defined over a field k of characteristic p. Fix an isomorphism $\mathcal{O}_L \otimes_{\mathbb{Z}} k \cong k[T]/(T^g)$. One knows that $H^1_{dR}(A)$ is a free $k[T]/(T^g)$-module of rank 2, and there are two generators α and β such that:

$$H^1(A, O_A) = (T^i)\alpha + (T^j)\beta, i \geq j, i + j = g.$$

The index $j = j(A)$ is called the **singularity index**. For perspective, recall the short 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 Dieudonné modules of group schemes, and we rewrite this exact sequence as:

$$0 \longrightarrow (k, \mathrm{Fr}^{-1}) \otimes_k \mathbb{D}(\mathrm{Ker}(\mathrm{Fr})) \longrightarrow \mathbb{D}(A[p]) \longrightarrow \mathbb{D}(\mathrm{Ker}(\mathrm{Ver})) \longrightarrow 0.$$

The **slope** $n = n(A)$ is defined by $j(A) + n(A) = a(A)$, where $a(A)$ is the a-number of the abelian variety.

The subsets $\mathfrak{W}_{(j,n)}$ parameterizing abelian varieties with singularity index j and slope n are quasi-affine, locally closed and form a stratification ([1, Thm. 10.1], [2, §6.1]).

Note that for any Dieudonné module M with RM of rank 2, we can define abstractly $j(M)$ and $n(M)$ without any reference to abelian varieties i.e., $j(M) = j$ is the integer such that

$$T^i\alpha + T^j\beta = \mathrm{Ker}(V : M/pM \longrightarrow M/pM), i \geq j,$$

for α, β some generators of M. The slope is $n(M) := a(M) - j(M)$.

Remark 1.6.1. Here is our first main observation: Outside the supersingular locus, the slope n defines the Newton polygon uniquely as $\{\frac{n}{g}, \frac{g-n}{g}\}$. For each non-supersingular Newton polygon, there is a *unique* special module, given by

$$E/E(F - T^n) \oplus E/E(F - T^{g-n}).$$

In the visual representation of the stratification of [1, p.1829], this means that the maximal special module is constant along *diagonals* i.e., it depends only on the slope n. In the supersingular locus, the diagonal constancy of the maximal special modules is also *de rigueur*, but we need more computations to establish it.

Remark 1.6.2. We present our second main observation: Consider the supersingular Newton stratum. It decomposes in $([g/2]+1)\cdot([g/2]+2)/2$ strata indexed by the type (j, n), $n/g \geq 1/2$. Recall that for a fixed superspecial module M_c, the component classifying modules of index $(0, d)$ over the special module M_c is denoted by $\mathfrak{M}_c^d$. The explicit computations of the supersingular module spaces à la Manin carried out in Section 1.5 indicate that the dimension of $\mathfrak{M}_c^d$ is the same as the dimension of the stratum $\mathfrak{W}_{(c-d,g-c)}$ of type $(i - d, g - i)$ i.e.,

$$\dim \mathfrak{M}_c^d = \dim \mathfrak{W}_{(c-d,g-c)}.$$

Moreover, the components $\mathfrak{M}_c^d$, like the corresponding strata $\mathfrak{W}_{(c-d,g-c)}$, are quasi-affine by our explicit computations.

Conjecture 1.6.3. Define $\mathfrak{N}_c^d$ as the strata on the Hilbert moduli space such that for $\underline{A} \in \mathfrak{N}_c^d$, the Dieudonné module $\mathbb{D}(\underline{A})$ of $\underline{A}$ belongs to $\mathfrak{M}_c^d$. Then the stratification induced by the components $\mathfrak{M}_c^d$ coincide with the slope stratification $\{\mathfrak{W}_{(j,n)}\}_{j,n}$ i.e.,

$$\mathfrak{N}_i^d = \mathfrak{W}_{(c-d,g-c)}.$$

Given the conjecture, we may draw the following conclusions:

Let M belong to M_c, M_c a superspecial Dieudonné module.

- The slope n of M depends only on the maximal special submodule M_c.
- The a-number of M depends only on the **e**-index $i(M_c, M)$:

$$a(M) = a(M_c) - i(M_c, M).$$

We prove these conclusions independently, thus providing evidence for Conjecture 1.6.3 by settling it for the supersingular strata. The proofs consist in translating the precise, explicit knowledge of the supersingular moduli spaces à la Manin in terms of the invariants of [1]. We first prove that the a-number of a supersingular slope stratum only depends on $i(M_c, M)$. Recall that in the *contravariant* Dieudonné theory we are using, an embedding $\alpha_p \hookrightarrow A[p^\infty]$ at the level of p-divisible groups corresponds to a surjection $\mathbb{D}(A[p^\infty]) \twoheadrightarrow \mathbb{D}(\alpha_p) \cong k$.

Proposition 1.6.4. The a-number of the Dieudonné module M belonging to a fixed superspecial module M_c depends only on the index $i(M_c, M) = (0, d)$ over this module:

$$a(M) = g - d.$$

Proof. Let M be a module belonging to M_c such that $i(M_c, M) = (0, d)$. We use the specific computations of Section 1.5. The a-number of M is, by definition, $\dim_k M/FM + VM$. Since M_c is superspecial, $\dim_k M_c/FM_c + VM_c = g$. Thence, showing that $a(M) = g - d$ is equivalent to showing that the **e**-index of $FM + VM$

over $FM_c + VM_c$ is $(0, d)$ i.e., $i(FM_c + VM_c, FM + VM) = (0, d)$. This is possible if and only if $d \leq c \leq [g/2]$.

Let g be odd.

$$F(1 + \sum_{k=1}^{d} \epsilon_{2k-1}\theta^{-(2k-1)}) = \theta^g + \sum_{k=1}^{d} \epsilon_{2k-1}^{\sigma}\theta^{-2k+1+g}, \quad F\theta^{2c+1} = \theta^{2c+1+g},$$

and

$$V(1 + \sum_{k=1}^{d} \epsilon_{2k-1}\theta^{-2k+1}) = \mu \left\{ \theta^g + \sum_{k=1}^{d} \epsilon_{2k-1}^{\sigma^{-1}}\theta^{-2k+1+g} \right\}, \quad V\theta^{2c+1} = \mu\theta^{2c+1+g}.$$

This implies that

$$FM+VM =< \theta^g + \sum_{k=1}^{d} \epsilon_{2k-1}^{\sigma}\theta^{-2k+1+g}, \theta^{2c+1+g} > + < \theta^g + \sum_{k=1}^{d} \epsilon_{2k-1}^{\sigma^{-1}}\theta^{-2k+1+g}, \theta^{2c+1+g} >,$$

as we can ignore the unit μ by changing the generator (note the crucial difference in the action of σ (resp. σ^{-1}) for F (resp. V). Of course,

$$FM_c + VM_c =< \theta^g, \theta^{2c+1+g} > .$$

Since the second generator θ^{2c+1+g} of FM and VM is the same as the second generator of FM_c+VM_c, to compute the **e**-index of $FM+VM$ over FM_c+VM_c, we only need to inspect the coefficients of the first generators. Since $\epsilon_{2d-1}^{\sigma} \neq \epsilon_{2d-1}^{\sigma^{-1}}$, the corresponding coefficient in the generator of $FM + VM$ is non-trivial, and this implies that the **e**-index of $FM + VM$ over $FM_c + VM_c$ is $(0, d)$, since for g odd, $\theta^2 = T$.

Let g be even. We exploit Theorem 1.5.6. Similarly to the g odd case, F acts by σ on the coefficients $\epsilon_k \in \mathfrak{T}$ and by multiplication by $\theta^{g/2}$ in the cyclic local algebra $M_{m,n,q}$, and V acts by σ^{-1} on the coefficients $\epsilon_k \in \mathfrak{T}$ and by multiplication by $\mu\theta^{g/2}$ in the cyclic local algebra $M_{m,n,q}$, where $\theta = T$. We can ignore μ as before by making the obvious change of generator of VM. Since $M_c = \{1, \theta^c\}$, $FM_c+VM_c = \{\theta^{g/2}, \theta^{g/2+c}\}$. In the same way as in the g odd case, the **e**-index of $FM + VM$ over $FM_c + VM_c$ is also clearly $(0, d)$, and we are done.

□

We provide the conversation to Proposition 1.3.40.

Corollary 1.6.5. A supersingular module M with a-number $a(M) = g$ is special.

Proposition 1.6.6. Let M be a module belonging to M_c with **e**-index $(0, d)$. Then M has type $(c - d, g - c)$.

Proof. The invariants $j(M)$ and $i(M)$ are computable modulo p. In particular,

$$g - j = \min\{m | T^m H^1(A, \mathcal{O}_A) = 0 \mod p\}.$$

Recall that $H^1(A, \mathcal{O}_A) \cong H^1_{dR}(A)/H^0(A, \Omega^1_A)$, and, in terms of the contravariant version of Dieudonné theory, $H^1(A, \mathcal{O}_A) = \mathbb{D}(A[p])/V\mathbb{D}(A[p]) = \mathbb{D}(A[p])/\mathbb{D}(A[p])[F]$. We can compute the singularity index $j(M)$ by computing $\min\{m | T^m(M/M[F]) = 0 \mod p\}$ for any Dieudonné module M. We reduce the claim to the case of **e**-index $(0, d) = (0, 0)$. Fix an isomorphism $M \cong W_{\mathfrak{F}}(k) \oplus W_{\mathfrak{F}}(k)$, such that $\overline{M_c} = M_c \mod p \cong k[T]/(T^g) \oplus T^d k[T]/(T^g)$. In this representation, it is obvious that $j(M_c) - d = j(M)$. We now show that

$$j(M_c) = c.$$

Suppose first that g is odd. Recall that in this case,

$$E^0_{1,1,0} = W_{\mathfrak{F}}(\mathbb{F}_{p^2})[\theta^g], \theta^2 = T.$$

Recall that the superspecial module M_c is generated by $< 1, \theta^{2c+1} >$. Therefore

$$\theta^{2g-2c-1}(\overline{M}/V\overline{M}) = 0, \theta^{2g-2c-2}(\overline{M}/V\overline{M}) \neq 0,$$

and so

$$T^{g-c}(\overline{M}/V\overline{M}) = 0, T^{g-c-1}(\overline{M}/V\overline{M}) \neq 0,$$

i.e., $j(M_c) = c$. Suppose now that g is even. Recall that in this case,

$$E^0_{1,0,g/2} = W_{\mathfrak{F}}(\mathbb{F}_p)[\theta^{g/2}], \theta = T,$$

and M_c is generated by $\{1, \theta^c\}$. Therefore,

$$\theta^{g-c}(\overline{M}/V\overline{M}) = 0, \theta^{g-c-1}(\overline{M}/V\overline{M}) \neq 0,$$

and since $\theta = T$, $j(M_c) = c$. □

Corollary 1.6.7. A supersingular module M of type (j, n) belongs to a maximal special module of type $(g - n, n)$.

Chapter 2

Superspecial Abelian Varieties and Theta Series

2.1 Introduction

Supersingular points on modular curves are highly significant in arithmetic geometry: 1) for the connection with modular forms via quaternion algebras, 2) for the geometric realization of the monodromy pairing (Picard-Lefschetz formula à la Grothendieck ([42, Exposé IX, Thm. 12.5])), 3) for the geometric analogue of the Jacquet-Langlands correspondence ([86, Thm. 4.1]), etc. Polarized abelian varieties with *real multiplication* i.e., equipped with an action of the ring of integers $\mathcal{O}_L$ of a totally real field L, constitute a generalization of elliptic curves that carries a strong arithmetic flavour. The algebraic stacks classifying these objects are called *Hilbert moduli spaces* and are the main object of study of this chapter. Albeit our treatment does not do justice to the depth of its topic, we lay the groundwork to some extent for all three aspects mentioned above for *superspecial* points on Hilbert moduli spaces. Grosso modo, our results can be viewed as geometric variations on the theme of trace formulae.

We describe the main features of this chapter in more details.

Let $h^+(L) = 1$. This implies that the abelian varieties under consideration are principally polarized. Our starting point is the investigation of the abelian variety $E \otimes_{\mathbb{Z}} \mathcal{O}_L$, where E is a supersingular elliptic curve. We show that its ring of endomorphisms $\mathrm{End}_{\mathcal{O}_L}(E \otimes_{\mathbb{Z}} \mathcal{O}_L)$ is isomorphic to $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathcal{O}_L$, a primitive order (in the sense of Eichler) of level $p\mathcal{O}_L$. It turns out that, in general, the endomorphism ring of a superspecial abelian variety A is of a particular type of Bass order that we call a superspecial order.

Theorem:(cf. Theorem 2.5.27) Let p be unramified. Let A be a superspecial abelian variety with RM. Then the order $\mathrm{End}_{\mathcal{O}_L}(A)$ is an *Eichler* order of level p.

The knowledge of the order $\mathrm{End}_{\mathcal{O}_L}(A)$ allows us to parameterize the set of superspecial points using the double cosets of the adelic points of a quaternionic group.

Theorem:(cf. Theorem 2.5.35) Let p be unramified. The left (resp. right) ideals classes of $\mathrm{End}_{\mathcal{O}_L}(A)$ are in bijection with superspecial abelian varieties with RM.

Corollary:(cf. Corollary 2.5.36) Any superspecial order of level p arises as the endomorphism ring of a suitable superspecial abelian variety with RM.

Our next step is to consider the $\mathcal{O}_L$-module $\mathrm{Hom}_{\mathcal{O}_L}(A_1, A_2)$ of $\mathcal{O}_L$-homomorphisms between two superspecial abelian varieties A_1, A_2. We equip $\mathrm{Hom}_{\mathcal{O}_L}(A_1, A_2)$ with the structure of a quadratic module by defining a notion of $\mathcal{O}_L$-degree $||-||$, which is essentially the norm form of the quaternion algebra $B_{p,L} := B_{p,\infty} \otimes L$, hence a totally definite positive quadratic form in four variables. This allows us to construct a theta series of level p from the quadratic module $M = (\mathrm{Hom}_{\mathcal{O}_L}(A_1, A_2), ||-||)$, that is, $\Theta_M := \sum_{\nu \in \mathcal{O}_L} \sharp \{m \in M |\ ||m|| = \nu\}\, q^\nu$. From the bijection between left ideal classes of a superspecial order of level p and the superspecial abelian varieties, it follows that all theta series of level p coming from $B_{p,L}$ arise from geometry. The Jacquet-Langlands correspondence, translated in classical terms, implies that the space of Hilbert modular newforms of weight 2 for $\Gamma_0(p)$ is thence spanned by the theta series coming from superspecial abelian varieties with RM.

Denote by $X_0(1)/\overline{\mathbb{F}}_p$ the Hilbert moduli space (à la Deligne-Pappas) with no level structure in characteristic p. It has dimension $[L:\mathbb{Q}]$.

Main Theorem: Let $h^+(L) = 1$, p unramified. The theta series attached to the superspecial points of the Hilbert moduli space $X_0(1)/\overline{\mathbb{F}}_p$ span the vector space of weight 2 Hilbert modular newforms of level $\Gamma_0(p)$.

We can view this theorem as a geometric version of Eichler's Basis Problem for Hilbert modular forms. We also study the case where the prime $p = \mathfrak{p}^g$ is totally ramified in $\mathcal{O}_L$. We show that results analogous to the unramified case hold, with the added subtlety that the Hilbert modular forms arising from $\mathrm{Hom}_{\mathcal{O}_L}(A_1, A_2)$ can have level $\mathfrak{p}^i$, $g - [g/2] \leq i \leq g$, depending on the superspecial crystal of A_1 and A_2. We illustrate numerically to a limited extent some of the results concerning theta series in Subsection 2.7.1 and Section 2.9.

We also prove a theorem about the singularities of the a-number stratification of the Siegel moduli space $\mathcal{A}_g$ classifying principally polarized abelian varieties of dimension g. Let T_a be the locus of points $A \in \mathcal{A}_g \otimes \overline{\mathbb{F}}_p$ such that $a(A) \geq a$.

Theorem:(cf. Theorem 2.4.14) Let $a > 0$. The set $\mathrm{Sing}(T_a)$ of singular points of the locus T_a is precisely T_{a+1}.

2.2 Orders in quaternion algebras

2.2.1 Basic definitions

The main reference for this section is Vignéras' book [102], and we follow its notation for this subsection, in which we recall succinctly the basic definitions pertaining to quaternion algebras.

We need the notion of a Bass order to describe accurately in the general case the orders arising as endomorphism orders of a superspecial abelian variety with RM. On the other hand, a hurried reader might want to restrict to the case p unramified, in

which case she only needs the well-known concept of an Eichler order. On the other hand, in the totally ramified case, the orders arising from geometry are never Eichler orders, so the algebraic terminology is necessary.

Let K be a field.

Definition 2.2.1. ([102, p.1]) A **quaternion algebra** H over K is a central, simple algebra of rank 4 over K.

If the characteristic of K is different from two, a quaternion algebra H is given by a couple (a, b), where $a, b \in K\backslash\{0\}$, as the K-algebra of basis $1, i, j, k$, where $i, j \in H, k = ij$, and

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

A quaternion algebra is equipped with a canonical involutive K-endomorphism $h \mapsto \overline{h}$ called **conjugation**. The (reduced) **norm** of H is defined as $n(h) := h\overline{h}$, and the (reduced) **trace** is defined as $t(h) := h + \overline{h}$.

Any field K admits over itself the quaternion algebra $M_2(K)$. For local fields (different than $\mathbb{C}$), there is only one more:

Theorem 2.2.2. ([102, p.31]) Let $K \neq \mathbb{C}$ be a local field. Then there exists a unique quaternion division algebra over K, up to isomorphism.

Definition 2.2.3. ([102, p.58]) Let H be a quaternion algebra over a number field K. Let v be a place of K. We denote $H_v := H \otimes_K K_v$. A place v is **ramified** if H_v is a division algebra. If $H_v \cong M_2(K_v)$, we say the place v is **split** (or **unramified**).

Global fields admit infinitely many quaternion algebras, but we can classify them according to the ramification of places:

Theorem 2.2.4. ([102, Thm. 3.1]) Let K be a number field. The number $|\mathbf{Ram}(H)|$ of ramified places is even. For any even set S of places, there exists a unique quaternion algebra H/K up to isomorphism such that $\mathbf{Ram}(H) = S$.

We will later need the notion of a **splitting field**:

Definition 2.2.5. ([102, p.4]) Let F be a field containing K, and let H be a quaternion algebra over K. The tensor product $H_F := H \otimes_K F$ is a quaternion algebra. If $H_F \cong M_2(F)$, we call F/K a **splitting field** of H.

There are useful criteria to determine whether a quadratic field extension of K is a splitting field, when K is a local or global field.

Theorem 2.2.6. ([102, p.9]) Let K be a local or a global field. Let L be a quadratic extension of K. Then L is a splitting field of a quaternion algebra H/K if and only if L is isomorphic to a (maximal) subfield of H.

Theorem 2.2.7. ([102, Thm. 1.3, p.33]) Let K be a non-archimedean local field. A finite extension F/K splits H if and only if its degree $[F : K]$ is even.

Remark 2.2.8. The archimedean cases i.e., $\mathbb{R}$ and $\mathbb{C}$, are simpler: $M_2(\mathbb{C})$ is the only quaternion algebra over $\mathbb{C}$, and $\mathbb{C}$ is the only finite extension of $\mathbb{R}$. Over $\mathbb{R}$ there are, up to isomorphism, two quaternion algebras: $M_2(\mathbb{R})$ and the Hamilton quaternions $\mathbb{H}_{\mathbb{R}}$ given by the couple $(-1, -1)$.

Theorem 2.2.9. ([102, Cor. 3.5]) An extension L/K of degree $[L : K] < \infty$ splits a quaternion algebra H over a number field K if and only if L_w splits H_v for any place $w|v$ of L.

Theorem 2.2.10. ([102, Thm. 3.8]) A quadratic extension L/K can be embedded in a quaternion algebra H over a global field K if and only if $L_v = L \otimes K_v$ is a field, for all $v \in \mathbf{Ram}(H)$.

2.2.2 Orders

We are motivated by the study of orders like $\mathcal{O} \otimes_{\mathbb{Z}} \mathcal{O}_L$, where $\mathcal{O}$ is a maximal order in the quaternion algebra $B_{p,\infty}$ over $\mathbb{Q}$ ramified at p and ∞, and $\mathcal{O}_L$ is the ring

of integers of a totally real field L. They arise as endomorphism orders of some superspecial points on Hilbert modular varieties. Our main reference for orders is [6]; we also found [15, p.970-977] useful.

Let R be an integral domain. Let V be a finite dimensional vector space over the quotient field of R. A finitely generated left R-module M contained in V is called a left R**-lattice** of V. Let K be a number field. Let $\mathcal{O}_K$ be its ring of integers and H/K a quaternion algebra. All $\mathcal{O}_K$-lattices M we consider in H are **ideals** i.e., lattices such that $M \otimes_{\mathcal{O}_K} K \cong H$.

Definition 2.2.11. Let (M, q) be an $\mathcal{O}_K$-lattice M equipped with a quadratic form $q : M \longrightarrow \mathcal{O}_K$. We denote $N(M)$ the **norm** of M, defined as the $\mathcal{O}_K$-ideal generated by the values $q(x)$ for $x \in M$ (the name originates from the particular instance where $M \subset H$, and the quadratic form is the reduced norm of the quaternion algebra).

Definition 2.2.12. Let $x_1, \ldots, x_4 \in H$. Let $d(x_1, \ldots, x_4)$ be the determinant of the matrix $[t(x_i\overline{x_j})]$. If M is an $\mathcal{O}_K$-lattice in H, then the $\mathcal{O}_K$-ideal in K generated by all $d(x_1, \ldots, x_4)$, where $x_i \in M, 1 \leq i \leq 4$, is basis of H, is a square of an $\mathcal{O}_K$-ideal in K, which we call the **discriminant** $d(M)$ of M.

Definition 2.2.13. The **dual** of an $\mathcal{O}_K$-lattice $M \subset H$ is defined as

$$M^\sharp := \{x \in H : t(xM) \subset \mathcal{O}_K\}.$$

The $\mathcal{O}_K$-ideal $N(M^\sharp)^{-1}$ is called the **level** of M.

This definition of the level of a quaternionic lattice using the trace coincides with the definition of the level of an arbitrary quadratic lattice equipped with a bilinear form for lattices of norm 1. Denote by $N(x)$ the K-valued quadratic form associated to a quadratic lattice M. We denote by V the vector space $M \otimes \mathbb{Q}$. We denote by $B(x, y)$ the symmetric, bilinear form defined by:

$$B(x, y) := \frac{1}{2}\left(N(x + y) - N(x) - N(y)\right).$$

The dual of M is thus defined as $M^\flat := \{x \in V | B(x, M) \subseteq \mathcal{O}_K\}$. Moreover, the $\flat$-level is defined as $(N(M)N(M^\flat))^{-1}$, where $N(M)$ is the ideal generated by $N(x)$, for $x \in M$. Observe that in the quaternionic case, $B(x, y) = t(x\overline{y}) = x\overline{y} + y\overline{x}$ for all x, y implies immediately that $M^\flat = M^\sharp$ and that for all lattices M such that $N(M) = (1)$, the two notions of level coincide.

Definition 2.2.14. An **order** of H is an ideal of H which is a ring (containing 1, by definition).

Let $\mathcal{O}$ be an order of H.

Definition 2.2.15. An ideal I of H is a left **$\mathcal{O}$-ideal** if it is an ideal and its left order $\mathcal{O}_g(I) := \{h \in H | hI \subset I\}$ is $\mathcal{O}$.

Definition 2.2.16. Two ideals I and J are (right) equivalent if $I = Jh, h \in H^\times$. This is an equivalence relation, and the equivalence classes of ideals whose left order is $\mathcal{O}$ are called the left **ideal classes** of $\mathcal{O}$.

A **maximal order** is an order which is not properly contained in any order. Maximal orders always exist, and any order is contained in a maximal order. An order is maximal if and only if its discriminant is equal to the product of the ramified, finite places of H.

Definition 2.2.17. An order $\mathcal{O}$ in H is **Gorenstein** if $\mathcal{O}^\sharp$ is $\mathcal{O}$-projective as a left (or right) $\mathcal{O}$-lattice.

Proposition 2.2.18. ([6, Prop. 1.3]) The discriminant of an order $\mathcal{O}$ is equal to its level i.e., $d(\mathcal{O}) = N(\mathcal{O}^\sharp)^{-1}$, if and only if the order is Gorenstein.

Remark 2.2.19. The level $N(\mathcal{O}^\sharp)^{-1}$ of an order $\mathcal{O}$ always divides the discriminant $d(\mathcal{O})$ ([6, Prop. 1.3]).

Definition 2.2.20. An order $\mathcal{O}$ in a quaternion algebra H over K is **primitive** if it contains the maximal order of a quadratic field extension of K or the maximal order of the split extension $K \oplus K$.

Primitive orders were first studied by Eichler in his Ph.D. thesis [22].

Definition 2.2.21. An order $\mathcal{O}$ is a **Bass order** if each order in H containing it is a Gorenstein order. In particular, a Bass order is Gorenstein.

Proposition 2.2.22. ([6, Cor. 1.6]) An order $\mathcal{O}$ in H whose discriminant is cube-free is a Bass order.

Let $\mathcal{O}$ be an order in the quaternion algebra H/K. Let $\mathcal{O}_\mathfrak{p} := \mathcal{O} \otimes \mathcal{O}_{K_\mathfrak{p}}$. Denote by k the residue field of $\mathcal{O}_{K_\mathfrak{p}}$. The Jacobson radical $\mathcal{N}_\mathfrak{p}$ of $\mathcal{O}_\mathfrak{p}$ is the intersection of all maximal left (or equivalently right) ideals of $\mathcal{O}_\mathfrak{p}$. An order $\mathcal{O}_\mathfrak{p}$ is said to be an **Azumaya order** if $\mathcal{O}_\mathfrak{p}/\mathcal{N}_\mathfrak{p}$ is a non-trivial central simple algebra over k. Since $\mathfrak{p}\mathcal{O}_\mathfrak{p} \subseteq \mathcal{N}_\mathfrak{p}$, $\mathcal{O}_\mathfrak{p}/\mathcal{N}_\mathfrak{p}$ is a k-vector space with $\dim_k(\mathcal{O}_\mathfrak{p}/\mathcal{N}_\mathfrak{p}) \leq 4$. If $\mathcal{O}_\mathfrak{p}$ is Azumaya, then we must have $\mathcal{O}_\mathfrak{p}/\mathcal{N}_\mathfrak{p} \cong M_2(k)$, since there are no skew fields over a finite field.

Definition 2.2.23. (cf. [6]) The **Eichler symbol** $(\frac{\mathcal{O}}{\mathfrak{p}})$ at $\mathfrak{p}$ of a Gorenstein order $\mathcal{O}$ of H, which is not Azumaya at $\mathfrak{p}$, is defined by

$$\left(\frac{\mathcal{O}}{\mathfrak{p}}\right) = \begin{cases} 1 & \text{if } \mathcal{O}_\mathfrak{p}/\mathcal{N}_\mathfrak{p} \cong k \times k, \\ 0 & \text{if } \mathcal{O}_\mathfrak{p}/\mathcal{N}_\mathfrak{p} \cong k, \\ -1 & \text{if } \mathcal{O}_\mathfrak{p}/\mathcal{N}_\mathfrak{p} \text{ is a quadratic field extension of } k. \end{cases}$$

Remark 2.2.24. The previous definition exhausts all possibilities: If $\mathcal{O}_\mathfrak{p}/\mathcal{N}_\mathfrak{p}$ is not $k \times k, k$ nor a quadratic field extension of k, then $\mathcal{O}$ is necessarily Azumaya at $\mathfrak{p}$ ([6]).

Definition 2.2.25. Let $\mathcal{O}$ be an $\mathcal{O}_K$-order in H. The order $\mathcal{O}$ is **Eichler** if $\mathcal{O}$ is an intersection of two maximal orders, not necessarily distinct.

Remark 2.2.26. One source of confusion arises from the terminology of the level e.g., in the literature, an Eichler order will often be said to be of level N, for $(N, p) = 1$, in the quaternion algebra ramified at p and infinity $B_{p,\infty}$ (see [102, p.84]), while according to our terminology, it is of level Np, that is, the reduced discriminant of the quaternion algebra is always included in the level.

Proposition 2.2.27. An Eichler order $\mathcal{O}$ in a quaternion algebra over $K_{\mathfrak{p}}$ is a Bass order, independently of its level.

Proof. Use [6, Cor. 2.2, 2.4] and the observation that Bass is a local property. □

Proposition 2.2.28. (cf. [6, Prop. 5.3])

- Let $e \in \{-1, 1\}$. Two orders $\mathcal{O}_1$ and $\mathcal{O}_2$ in $H_{\mathfrak{p}}$ with $(\frac{\mathcal{O}_1}{\mathfrak{p}}) = (\frac{\mathcal{O}_2}{\mathfrak{p}}) = e$ are conjugate in $H_{\mathfrak{p}}$ if and only if their discriminants are equal.
- Two Bass orders $\mathcal{O}_1$ and $\mathcal{O}_2$ in $H_{\mathfrak{p}}$ with $(\frac{\mathcal{O}_1}{\mathfrak{p}}) = (\frac{\mathcal{O}_2}{\mathfrak{p}}) = 0$ are conjugate in $H_{\mathfrak{p}}$ if their discriminants are equal.

Proposition 2.2.29. Let $\mathcal{O}$ be a Bass order [1] in H/K.
If $\mathrm{val}_{\mathfrak{p}}(d(\mathcal{O})) = 1$, then:

- if $\mathfrak{p} \notin \mathbf{Ram}(H)$, $(\frac{\mathcal{O}}{\mathfrak{p}}) = 1$, and $\mathcal{O}_{\mathfrak{p}}$ does not contain the ring of integers of an unramified quadratic field extension of $K_{\mathfrak{p}}$;
- if $\mathfrak{p} \in \mathbf{Ram}(H)$, $(\frac{\mathcal{O}}{\mathfrak{p}}) = -1$ and $\mathcal{O}_{\mathfrak{p}}$ does not contain a split extension $\mathcal{O}_{K_{\mathfrak{p}}} \oplus \mathcal{O}_{K_{\mathfrak{p}}}$;

If $\mathrm{val}_{\mathfrak{p}}(d(\mathcal{O})) \geq 2$, then:

- $(\frac{\mathcal{O}}{\mathfrak{p}}) = 1$ if and only if $\mathcal{O}_{\mathfrak{p}}$ contains a split quadratic extension $\mathcal{O}_{K_{\mathfrak{p}}} \oplus \mathcal{O}_{K_{\mathfrak{p}}}$;
- $(\frac{\mathcal{O}}{\mathfrak{p}}) = 0$ if and only if $\mathcal{O}_{\mathfrak{p}}$ contains the ring of integers of a ramified quadratic field extension of $K_{\mathfrak{p}}$;

[1] A Bass order is locally primitive by the proof of Proposition 2.3.5.

- $(\frac{\mathcal{O}}{\mathfrak{p}}) = -1$ if and only if $\mathcal{O}_\mathfrak{p}$ contains the ring of integers of an unramified quadratic field extension of $K_\mathfrak{p}$.

Proof. [8, Prop. 1.11, 1.12, 1.16]. □

Corollary 2.2.30. ([9, Prop. 3]) Let $\mathcal{O}$ be a primitive order [2] in H/K. Let S be a maximal order in a maximal commutative subfield of H/K and assume $S \subset \mathcal{O}$.
If $\mathrm{val}_\mathfrak{p}(d(\mathcal{O})) = 1$, then:

- the prime $\mathfrak{p}$ is split or ramified in S when $\mathfrak{p} \notin \mathbf{Ram}(H)$, and $(\frac{\mathcal{O}}{\mathfrak{p}}) = 1$;
- the prime $\mathfrak{p}$ is ramified or inert in S when $\mathfrak{p} \in \mathbf{Ram}(H)$, and $(\frac{\mathcal{O}}{\mathfrak{p}}) = -1$.

If $\mathrm{val}_\mathfrak{p}(d(\mathcal{O})) \geq 2$, then:

- $(\frac{\mathcal{O}}{\mathfrak{p}}) = 1$ if $\mathfrak{p}$ splits in S;
- $(\frac{\mathcal{O}}{\mathfrak{p}}) = 0$ if $\mathfrak{p}$ is ramified in S;
- $(\frac{\mathcal{O}}{\mathfrak{p}}) = -1$ if $\mathfrak{p}$ is inert in S.

According to [6, Prop. 2.1], an order $\mathcal{O}$ in a quaternion algebra over $K_\mathfrak{p}$ has Eichler symbol 1 if and only if is conjugate to the order consisting of matrices

$$\begin{pmatrix} \mathcal{O}_{K_\mathfrak{p}} & \mathcal{O}_{K_\mathfrak{p}} \\ \pi_\mathfrak{p}^d \mathcal{O}_{K_\mathfrak{p}} & \mathcal{O}_{K_\mathfrak{p}} \end{pmatrix},$$

where $\pi_\mathfrak{p}$ is a uniformizer of the maximal ideal of $\mathcal{O}_{K_\mathfrak{p}}$, and d is a non-negative integer. Since a division quaternion algebra over a local field has a unique maximal order, it follows ([6, Cor. 2.2]) than an Eichler order in H/K is characterized by its Eichler symbols being 1 for all non-zero prime ideals $\mathfrak{p}$ such that $\mathcal{O}_\mathfrak{p}$ is not maximal.

[2] A primitive order is Bass; cf. Proposition 2.3.5.

Definition 2.2.31. An order $\mathcal{O}$ is left (respectively right) **hereditary** if each left (respectively right) $\mathcal{O}$-lattice is projective.

Remark 2.2.32. Another source of confusion is the terminology used in the literature on quaternion algebras for the completions of modules. If M is an $\mathcal{O}$-module the completion $M \otimes \mathcal{O}_{K_\mathfrak{p}}$ for a prime $\mathfrak{p}$ of $\mathcal{O}_K$ is called the **localization** of M at $\mathfrak{p}$. Note that there *is* a different notion of non-commutative localization in line with the usual localization of commutative algebra, subject to some extra hypothesis called Ore's condition (which is automatically satisfied in the commutative case).

Definition 2.2.33. An $\mathcal{O}$-lattice M is **locally principal** if the localizations $M \otimes \mathcal{O}_{K_\mathfrak{p}}$ are principal for all $\mathfrak{p}$.

Proposition 2.2.34. ([6, Prop. 1.1]) Let $\mathcal{O}$ be an order in H/K. An $\mathcal{O}$-ideal M is projective if and only if M is locally principal.

A complementary result is that an order $\mathcal{O}$ is hereditary if and only if all the completions $\mathcal{O}_\mathfrak{p}$ are hereditary ([84, Thm. 40.5, p.368]).

Proposition 2.2.35. ([6, Prop. 1.2, p.504]) An order is hereditary if and only if its discriminant is square-free. In particular, a hereditary order is always Bass.

Proof. The second statement follows from Proposition 2.2.22. □

Theorem 2.2.36. ([21, Satz 27, p.106]) Every ideal class of a hereditary order $\mathcal{O}$ contains an ideal I whose norm is relatively prime to the norms of a given, finite number of ideals J_i of $\mathcal{O}$ i.e., for any J_i, $N(J_i) + N(I) = \mathcal{O}_K$ as $\mathcal{O}_K$-ideals.

Proof. The proof in [21] only uses the fact that the ideals are locally principal, which is automatic for hereditary orders. □

2.3 Ideal theory in quaternion algebras

We will encounter in the sequel some very specific quaternion algebras. They are closely related to the rational quaternion algebra $B_{p,\infty}$ ramified at p and ∞, and they arise from geometry as algebras of endomorphisms of supersingular abelian varieties with real multiplication. We study in this subsection which orders and which quadratic modules derived from these orders can be retrieved from the geometry of Hilbert modular varieties.

2.3.1 $B_{p,\infty}$ and related quaternion algebras

Definition 2.3.1. A quaternion algebra H over a totally real field L is **totally definite** if $H \otimes_{L,\sigma} \mathbb{R}$ is a division algebra for all embeddings $\sigma : L \hookrightarrow \mathbb{R}$.

The totally definite quaternion algebra $B_{p,L} := B_{p,\infty} \otimes L$ over L and its orders of level p will be our central concern.

Example 2.3.2. The ring of endomorphisms $\mathrm{End}(E)$ of a supersingular elliptic curve (over an algebraically closed field of characteristic p) is a maximal order in $B_{p,\infty}$ ([40, §2], [20]). We give explicit descriptions of some maximal orders, following [80, Prop. 5.1, 5.2]. First, the quaternion algebra $B_{p,\infty}$ over $\mathbb{Q}$ ramified precisely at p and ∞ can be given by:

$B_{p,\infty} = (-1,-1)$ if $p = 2$;

$B_{p,\infty} = (-1,-p)$ if $p = 3 \mod 4$;

$B_{p,\infty} = (-2,-p)$ if $p = 5 \mod 8$;

$B_{p,\infty} = (-p,-q)$ if $p = 1 \mod 8$, where $q = 3 \mod 4$ is a prime and $(p/q) = -1$.

Moreover, *one* maximal order of $B_{p,\infty}$ can be given by the $\mathbb{Z}$-basis:

$\frac{1}{2}(1+i+j+k), i, j, k$ if $p = 2$;

$\frac{1}{2}(1+j), \frac{1}{2}(i+k), j, k$ if $p = 3 \mod 4$;

$\frac{1}{2}(1+j+k), \frac{1}{4}(i+2j+k), j, k$ if $p = 5 \mod 8$;

$\frac{1}{2}(1+j), \frac{1}{2}(i+k), \frac{1}{q}(j+dk), k$ if $p = 1 \mod 8$, where d is such that $q|(d^2p+1)$.

Here $1, i, j, k$ is the canonical basis of $B_{p,\infty} = (a, b)$ with relations $i^2 = a, j^2 = b$, and $ij = k = -ji$.

Proposition 2.3.3. Let $\mathcal{O}$ be a maximal order in $B_{p,\infty}$.

1. A quadratic imaginary field $\mathbb{Q}(\sqrt{-D})$ embeds in $B_{p,\infty}$ if and only if p does not split in $\mathbb{Q}(\sqrt{-D})$. Moreover, for any integer n, we can choose a D prime to n such that the ring of integers of $\mathbb{Q}(\sqrt{-D})$ embeds in $\mathcal{O}$.

2. The order $\mathcal{O} \otimes_{\mathbb{Z}} \mathcal{O}_L$ in $B_{p,\infty} \otimes L$ is primitive of level $p = p\mathcal{O}_L$. Moreover, if p is unramified, the order $\mathcal{O} \otimes_{\mathbb{Z}} \mathcal{O}_L$ is hereditary.

Proof. The first statement in Part 1 is Theorem 2.2.10. The second statement follows from the surjectivity of Deuring's map of singular moduli onto supersingular j-invariants for $-D \ll_p 0$ ([27, Thm. 1.2]). To prove Part 2, we check that $\mathcal{O} \otimes \mathcal{O}_L$ contains the ring of integers of a quadratic field extension of L. Recall ([53, Cor. 9.4]) that for S an imaginary quadratic field, $\mathcal{O}_S \otimes \mathcal{O}_L$ is a maximal order if the discriminants of S and L are relatively prime. The proof of Part 1 gives us an appropriate ring of integers of discriminant coprime to the discriminant of L for any $\mathcal{O}$ maximal. We compute the level: The discriminant of $\mathcal{O}$ is p, and $d(\mathcal{O} \otimes_{\mathbb{Z}} \mathcal{O}_L) = d(\mathcal{O})\mathcal{O}_L = p\mathcal{O}_L$, since $\mathrm{Tr}_{B_{p,L}}(\sum_i a_i \otimes b_i) = \sum_i \mathrm{Tr}_{B_{p,\infty}}(a_i)b_i$, for $\sum_i a_i \otimes b_i \in \mathrm{End}(E) \otimes \mathcal{O}_L$. Since $\mathcal{O} \otimes_{\mathbb{Z}} \mathcal{O}_L$ is primitive, it is Gorenstein by Proposition 2.3.5 and Definition 2.2.21, and its level is equal to its discriminant by Proposition 2.2.18. Proposition 2.2.35 shows that $\mathcal{O} \otimes_{\mathbb{Z}} \mathcal{O}_L$ is hereditary when p is unramified. □

2.3.2 Algebraic aspects of ideals

Proposition 2.3.4. (Local-global principle, [102, Prop. 5.1]) Let K be a number field. Let X be a lattice of a quaternion algebra H/K. There exists a bijection between the lattices Y of H, and the set of lattices

$$\{Y_{\mathfrak{p}} | Y_{\mathfrak{p}} \text{ a lattice of } H_{\mathfrak{p}}, Y_{\mathfrak{p}} = X_{\mathfrak{p}} \text{ for all but finitely many } \mathfrak{p}\},$$

given by the applications:

$$Y \mapsto (Y_{\mathfrak{p}})_{\mathfrak{p}} \text{ and } (Y_{\mathfrak{p}})_{\mathfrak{p}} \mapsto Y = \{x \in H | x \in Y_{\mathfrak{p}}, \forall \mathfrak{p}\},$$

where on both sides the prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ are the index set.

Many properties can be read off locally e.g., the property of being an order, a maximal order, an Eichler order, a Bass order, a Gorenstein order, an ideal, etc. Note, though, that we cannot check locally that an order is globally primitive.

Proposition 2.3.5. A primitive order $\mathcal{O}$ in H/K is a Bass order.

Proof. Being a Bass order is a local property. According to [8, Prop. 1.11], being primitive and being Bass are the same thing locally. It is clear that a (global) primitive order is locally primitive at all primes. □

Proposition 2.3.6. An order $\mathcal{O}$ in a quaternion algebra H is Eichler of square-free level if and only if it is hereditary.

Proof. By Propositions 2.2.18 and 2.2.27, the level of an Eichler order is equal to the discriminant, which is thus square-free. This implies that an Eichler order of square-free level is hereditary by Proposition 2.2.35. By the same Proposition, a hereditary order $\mathcal{O}$ is Bass of square-free discriminant. Therefore, the level, being equal to the discriminant since a hereditary order is Gorenstein, is also square-free. It suffices to show that a hereditary order $\mathcal{O}$ is Eichler. Recall that an order is

Eichler if and only if for every prime ideal $\mathfrak{p}$: $\mathcal{O}_\mathfrak{p}$ is a maximal order or a Bass order with Eichler symbol equal to one. A hereditary order is maximal at all primes $\mathfrak{p} \in \mathbf{Ram}(H)$. By Proposition 2.2.29, a hereditary order, being Bass, has Eichler symbol $+1$ if $\mathfrak{p} \notin \mathbf{Ram}(H)$, and we are done. □

We gather in a succinct form the relationships between the various kinds of orders:

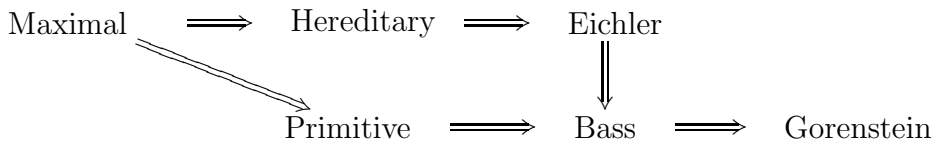

Diagram I: Properties of orders in quaternion algebras

- A hereditary order $\mathcal{O}$ is maximal if and only if its discriminant $d(\mathcal{O})$ is equal to the discriminant of the quaternion algebra.
- An Eichler order $\mathcal{O}$ is hereditary if and only if its discriminant $d(\mathcal{O})$ is square-free.
- A Bass order $\mathcal{O}$ in H/K is Eichler if $(\frac{\mathcal{O}}{\mathfrak{p}})$ is 1 when $\mathcal{O}_\mathfrak{p}$ is not maximal, for all primes $\mathfrak{p}$.
- A Gorenstein order $\mathcal{O}$ is Bass if its discriminant $d(\mathcal{O})$ is cube-free.
- An order in a quaternion algebra over a local field is primitive if and only if it is Bass.

2.3.3 Arithmetic aspects of ideals

Cf. [79, §2]. Define the idele group J_B of $B := B_{p,\infty} \otimes L$ as:

$$J_B := \left\{ \widetilde{a} = (a_\mathfrak{p}) \in \prod_\mathfrak{p} B_\mathfrak{p}^\times | a_\mathfrak{p} \in M_\mathfrak{p}^\times \text{ for almost all } \mathfrak{p} \right\},$$

where M is any order in B, and $\mathfrak{p}$ runs over all places of L. This is independent of M. The set J_B is a locally compact group with the topology induced by the product topology on the open sets $\prod_{\mathfrak{p}\in S} B_{\mathfrak{p}}^{\times} \prod_{\mathfrak{p}\notin S} M_{\mathfrak{p}}^{\times}$, where S ranges over all finite subsets of primes containing the infinite primes. If $\widetilde{a} = (a_{\mathfrak{p}}) \in J_B$, we define the volume of $\widetilde{a}$ as $\mathrm{vol}(\widetilde{a}) = \prod_{\mathfrak{p}} |N(a_{\mathfrak{p}})|$, where $|-|_{\mathfrak{p}}$ is normalized such that $|\mathfrak{p}|_{\mathfrak{p}} = \frac{1}{\mathrm{Norm}(\mathfrak{p})}$ for $\mathfrak{p} < \infty$ and with the usual absolute value at infinity. Let J_B^1 denote the ideles of volume 1 i.e.,

$$J_B^1 := \left\{ \widetilde{a} \in J_B^1 | \mathrm{vol}(\widetilde{a}) = 1 \right\},$$

and embed $B^{\times} \subset J_B^1$ with the diagonal embedding. If M is an order of B, define

$$B^1(M) := \left\{ \widetilde{a} = (a_{\mathfrak{p}}) \in J_B^1 | a_{\mathfrak{p}} \in M_{\mathfrak{p}}^{\times} \text{ for all } \mathfrak{p} < \infty \right\}.$$

Proposition 2.3.7. The following holds:

- $B^{\times}$ is a discrete subgroup in J_B^1;
- $J_B^1/B^{\times}$ is compact;
- For any order $\mathcal{O}$ of B, $B^1(\mathcal{O})$ is an open compact subgroup of J_B^1.

Proof. The references are scattered in Weil's book ([110]): the first statement is proved in [110, p. 71]; the second statement follows immediately from [110, Thm. 4, p.74], and the third statement follows from the definition. □

Corollary 2.3.8. ([79, Prop. 6]) Let $\mathcal{O}$ be hereditary. The double cosets

$$B^1(\mathcal{O}) \backslash J_B^1 / B^{\times}$$

correspond bijectively to the ideal classes of (right) $\mathcal{O}$-ideals.

Proof. If I is a left $\mathcal{O}$-ideal, then since $\mathcal{O}$ is hereditary,

$$I_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}} a_{\mathfrak{p}},$$

for some $a_{\mathfrak{p}} \in B_{p,L} \otimes L_{\mathfrak{p}}$, for all finite places $\mathfrak{p}$ and $a_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{p}}^{\times}$ for almost all $\mathfrak{p}$, since $I_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}$ for almost all $\mathfrak{p}$. Thus there exists an element $\widetilde{a} \in J_B^1$ with the $\mathfrak{p}$-th component of $\widetilde{a}$ equal to $a_{\mathfrak{p}}$ for all finite places $\mathfrak{p}$. Conversely, if $\widetilde{a} = (a_{\mathfrak{p}}) \in J_B^1$, then by the local-global correspondence, there is a unique lattice I such that $I_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}} a_{\mathfrak{p}}$ for all finite places $\mathfrak{p}$. Thus, via the local-global correspondence, we get a transitive action of J_B^1 on the left $\mathcal{O}$-ideals. Under this action, the isotopy subgroup of $\mathcal{O}$ is $B^1(\mathcal{O})$ and the corollary follows from the decomposition:

$$J_B^1 = \cup_{n=1}^{H} B^1(\mathcal{O}) \widetilde{a(n)} B^{\times}.$$

The $\mathcal{O}\widetilde{a(n)}$ represent the distinct $\mathcal{O}$-ideal classes. □

Proposition 2.3.9. ([79, Prop. 7]) J_B^1 acts transitively (by conjugation) on hereditary orders of level p in B.

Proof. Recall that a hereditary order is Bass (Proposition 2.2.35) and that hereditary orders of equal discriminant (equivalently, level) are locally conjugate by Propositions 2.2.28 and 2.2.29. The action is: for $\widetilde{a} = (a_{\mathfrak{p}}) \in J_B^1$, a hereditary order of level p:

$$M \mapsto \{M_{\mathfrak{p}}\} \mapsto \left\{a_{\mathfrak{p}}^{-1} M_{\mathfrak{p}} a_{\mathfrak{p}}\right\} \mapsto N,$$

and we write $N = \widetilde{a}^{-1} M \widetilde{a}$. □

Corollary 2.3.10. ([79, Prop. 8]) The class number $H(\mathcal{O})$ is finite and independent of the particular hereditary order of level p used in its definition. It is also the same for left or right ideals.

2.3.4 Superspecial orders

We flesh out the local properties of the primitive order $R = \mathcal{O} \otimes_{\mathbb{Z}} \mathcal{O}_L$ of level p, where $\mathcal{O}$ is a maximal order in $B_{p,\infty}$. To this end, we determine the possible Eichler symbols, and then model on this our general definition of a superspecial order.

Our choice of terminology is motivated by the fact that the endomorphism orders of superspecial points on the Hilbert modular variety associated to L modulo p are superspecial orders (see Theorem 2.5.27 and Corollary 2.8.10). Note first that R is maximal outside p by Proposition 2.2.28. Let

$$p = \prod_i \mathfrak{p}_i^{\alpha_i} \cdot \prod_j \mathfrak{q}_j^{\beta_j},$$

for $\mathfrak{p}_i \in \mathbf{Ram}(B_{p,L})$, $\mathfrak{q}_j \notin \mathbf{Ram}(B_{p,L})$. We remark that $\mathfrak{p}_i \in \mathbf{Ram}(B_{p,L})$ if and only if $[L_{\mathfrak{p}_i} : \mathbb{Q}_p]$ is odd (Lemma 2.5.23). Using Corollary 2.2.30 (cf. [6, §§2,3,4]), we get the following possibilities:

- $\left(\frac{R}{\mathfrak{p}_i}\right) = -1$ if $\alpha_i = 1$;
- $\left(\frac{R}{\mathfrak{q}_i}\right) = \ \ 1$ if $\beta_i = 1$.

By Proposition 2.2.30, if $\alpha_i = 1$, an embedded quadratic extension can be unramified or ramified; if $\beta_i = 1$, an embedded quadratic extension can be split or ramified. In general for primitive orders, the Eichler symbol is allowed to be zero for exponents bigger or equal than two. But in the proof that $\mathcal{O} \otimes_{\mathbb{Z}} \mathcal{O}_L$ is primitive, we could pick the order S to have discriminant prime to p, so no ideal dividing p can ramify in S, and this forces the Eichler symbol to be ± 1 for any $\mathfrak{p}_i, \mathfrak{q}_j$. Moreover, since $\mathfrak{p}_i \in \mathbf{Ram}(B_{p,L})$, $\mathfrak{p}_i$ is not split in S for otherwise $S \otimes \mathbb{Q}$ cannot be embedded in $B_{p,L}$. In short, we have the following possibilities:

- $\left(\frac{R}{\mathfrak{p}_i}\right) = -1$ if $\alpha_i > 1$;
- $\left(\frac{R}{\mathfrak{q}_i}\right) \neq 0$ if $\beta_i > 1$.

In fact, $\left(\frac{R}{\mathfrak{q}_i}\right) = (-1)^{f(\mathfrak{p}_i/p)}$, as we explain now. Since $\mathfrak{q}_i$ is not ramified in $B_{p,L}$, $[L_{\mathfrak{q}_i} : \mathbb{Q}_p]$ is even. Suppose we write $\mathcal{O}_K \cdot \mathcal{O}_L = \mathcal{O}_{K \cdot L} = \mathcal{O}_L[X]/(X^2 - d)$, with $(d_K, pd_L) = 1$, and $\sqrt{d} \notin \mathbb{Z}_p$, $(p, d) = 1$. Then $\mathfrak{q}_i$ is split if and only if $\sqrt{d} \in L_{\mathfrak{q}_i} \iff$

$\sqrt{d} \in k_L \iff 2|f(\mathfrak{q}_i/p)$, and otherwise is inert. Proposition 2.2.30 implies that $\left(\frac{R}{\mathfrak{q}_i}\right) = (-1)^{f(\mathfrak{p}_i/p)}$ encapsulates this data.
This observation suggests the following definition for superspecial orders:

Definition 2.3.11. Let $\mathcal{P} = \prod_i \mathfrak{p}_i^{\alpha_i} \cdot \prod_j \mathfrak{q}_j^{\beta_j}$ for $\mathfrak{p}_i \in Ram(B_{p,L})$, $\mathfrak{q}_j \notin Ram(B_{p,L})$, be an ideal of $\mathcal{O}_L$ dividing p. An order $\mathcal{O}$ in $B_{p,L}$ of level $\mathcal{P}$ is **superspecial** if the following conditions hold:

- if $\alpha_i \geq 1$, $\left(\frac{\mathcal{O}}{\mathfrak{p}_i}\right) = -1$;
- if $\beta_j > 1$, $\left(\frac{\mathcal{O}}{\mathfrak{q}_i}\right) = (-1)^{f(\mathfrak{q}_j/p)}$;
- if $\beta_j = 1$, $\left(\frac{\mathcal{O}}{\mathfrak{q}_i}\right) = +1$;
- for any other finite prime $\mathfrak{l}$ satisfying $(\mathfrak{l}, p) = 1$, $\mathcal{O}_\mathfrak{l}$ is maximal.

In particular, by Proposition 2.2.28, a superspecial order is Bass i.e., locally primitive.

We rephrase these findings by specifying at each prime which quadratic extension of $L_\mathfrak{p}$ arises, and describing the (local) primitive order containing it, using the terminology and ideas of [50].

Definition 2.3.12. ([49, Def. 2.3, p.64], [50]) Let B be the quaternion algebra over $L_\mathfrak{p}$. Let $K = K_\mathfrak{p}$ be a quadratic extension of $L_\mathfrak{p}$ contained in B. Set

$$R_v(K) = \mathcal{O}_K + P_B^{v-1},$$

for P_B the unique maximal ideal in $\mathcal{O}_B$ and $v = 1, 2, \ldots$.

Definition 2.3.13. An order $\mathcal{O}$ is superspecial of level $\mathcal{P}$ dividing p, $\mathcal{P} = \prod_i \mathfrak{p}_i^{\alpha_i} \cdot \prod_j \mathfrak{q}_j^{\beta_j}$, for $\mathfrak{p} \in Ram(B_{p,L})$, $\mathfrak{q}_j \notin Ram(B_{p,L})$, if the following conditions hold:

- if $\alpha_i \geq 1$, there is an unramified quadratic extension $\mathcal{O}_K$ of $\mathcal{O}_{L_\mathfrak{p}}$ such that $\mathcal{O}_{\mathfrak{p}_i} = R_{\alpha_i}(K)$;

- if $\beta_j > 1$, if $f(\mathfrak{q}_j/p)$ is even, $\mathcal{O}_{q_j}$ contains a split quadratic extension; if $f(\mathfrak{q}_j/p)$ is odd, there is an unramified quadratic extension $\mathcal{O}_K$ such that

$$\mathcal{O}_{\mathfrak{q}_j} \cong \left\{ \begin{pmatrix} \alpha & \beta^\sigma \\ \pi_{\mathfrak{q}_j}^{\beta_j}\beta & \alpha^\sigma \end{pmatrix}, \alpha, \beta \in \mathcal{O}_K \right\},$$

  for σ the involution on K, $\pi_{\mathfrak{q}_j}$ a uniformizer in $\mathcal{O}_{L_{\mathfrak{q}_j}}$;

- if $\beta_j = 1$, $\mathcal{O}_{\mathfrak{q}_j}$ contains a split extension, more precisely

$$\mathcal{O}_{\mathfrak{q}_j} \cong \begin{pmatrix} \mathcal{O}_{L_{\mathfrak{q}_j}} & \mathcal{O}_{L_{\mathfrak{q}_j}} \\ \mathfrak{q}_j\mathcal{O}_{L_{\mathfrak{q}_j}} & \mathcal{O}_{L_{\mathfrak{q}_j}} \end{pmatrix};$$

- for any other finite prime $\mathfrak{l}$, $\mathcal{O}_\mathfrak{l}$ contains a split extension.

Proposition 2.3.14. The two definitions of superspecial orders are equivalent.

Proof. It is clear a superspecial order in the second sense is superspecial in the first sense by Propositions 2.2.29 and 2.2.28. We show that a superspecial order in the first sense is also superspecial in the second sense.

- For $\alpha_i = 1$, this follows directly from Proposition 2.2.29;

- For $\beta_j = 1$, the order $\mathcal{O}_{\mathfrak{q}_j}$ is Eichler, and thus contains a split extension

$$\mathcal{O}_{L_{\mathfrak{q}_j}} \oplus \mathcal{O}_{L_{\mathfrak{q}_j}};$$

- For $\alpha_i > 1$, since $\left(\frac{\mathcal{O}}{\mathfrak{p}_i}\right) = -1$, the order $\mathcal{O}_{\mathfrak{p}_i}$ contains an unramified quadratic extension $\mathcal{O}_K$ of $\mathcal{O}_{L_{\mathfrak{p}_i}}$ by Proposition 2.2.29 and this forces $\mathcal{O}_{\mathfrak{p}_i} = R_{\alpha_i}(K)$ by [50, Cor. 2.4, p.64].

- For $\beta_j > 1$, if $\left(\frac{\mathcal{O}}{\mathfrak{q}_j}\right) = 1$, the order $\mathcal{O}_{L_{\mathfrak{q}_j}}$ is Eichler by Proposition 2.2.29, and thus contains a split extension, as before. If $\left(\frac{\mathcal{O}}{\mathfrak{q}_j}\right) = -1$, $\mathcal{O}_{\mathfrak{q}_j}$ contains an unramified quadratic extension by Proposition 2.2.29. Since a (local) primitive order is determined by its Eichler symbol and its discriminant by Proposition 2.2.28, the result follows.

□

We can now see that superspecial orders are quite similar to special orders:

Definition 2.3.15. ([50, Def. 6.1]) An order $\mathcal{O}$ in $B_{p,\infty} \otimes L$ is **special** if

- there exists an integral ideal I of $\mathcal{O}_L$, prime to the ramified primes $\mathfrak{p}_i$ of $B_{p,\infty} \otimes L$, such that for each finite split prime $\mathfrak{p}$ of $B_{p,\infty} \otimes L$, $\mathcal{O}_{\mathfrak{p}}$ is conjugate to $\left(\begin{smallmatrix} \mathcal{O}_{\mathfrak{p}} & \mathcal{O}_{\mathfrak{p}} \\ I\mathcal{O}_{\mathfrak{p}} & \mathcal{O}_{\mathfrak{p}} \end{smallmatrix}\right)$ by an element of $(B_{p,\infty} \otimes L)_{\mathfrak{p}}^{\times}$;

- for each finite ramified prime $\mathfrak{p}_i$ of $B_{p,\infty} \otimes L$, there exists a quadratic extension $K = K(\mathfrak{p}_i)$ of $L_{\mathfrak{p}_i}$ and a positive integer $\nu = \nu(\mathfrak{p}_i)$ such that $\mathcal{O}_{\mathfrak{p}_i} = R_\nu(K)$. If $\mathcal{O}$ is a special order of $B_{p,\infty} \otimes L$, the collection of local data:

$$(I; \dots, L(\mathfrak{p}_i), \nu(\mathfrak{p}_i), \dots),$$

  is called the (extended) **level** of $\mathcal{O}$.

Definition 2.3.16. Let $\mathcal{O}$ be a special order of $B_{p,L}$ with local data $(I; L(\mathfrak{p}_i), \nu(\mathfrak{p}_i))$. The classical level is $I \prod_i \mathfrak{p}_i^{\nu(\mathfrak{p}_i)}$.

Remark 2.3.17. We transpose the terminology of extended and classical level to Bass orders in the obvious way e.g., keeping in mind that the extended level uniquely determines the Eichler symbols.

2.3.5 Norm forms of orders

The main reference is [59, §6]. We recall that a **quadratic space** (V, q) over a field F of characteristic different than 2 is a finite dimensional F-vector space V with a symmetric bilinear form $\Phi : V \times V \longrightarrow F$. To the bilinear form Φ we can associate a quadratic map $q : V \longrightarrow F$ by $q(v) = \frac{1}{2}\Phi(v, v)$. A quadratic space is said to be **regular** if for every $v \in V$, the condition that $\Phi(u, v) = 0$ for all u in V implies $v = 0$. We only consider regular quadratic spaces of rank 4.

Let R be an integral domain with field of fractions F, and let Λ be an R-lattice in space V i.e., a finitely generated R-submodule of V containing a basis for V over F. If $q(\Lambda)$ is contained in R, we say that (Λ, q) is a **quadratic module** over R. If R is a principal ideal domain, then every quadratic module has a basis, and thus determines a quadratic form $f(x)$ over F. The ideal generated by the coefficients of a quadratic form $f(x)$ is defined to be the **content** of $f(x)$. If the content of a quadratic form $f(x)$ is equal to 1, then we say that f is **proper**.

In order to distinguish which quadratic modules arise from projective rank one left modules for an order in a quaternion algebra, we need to recall the notion of a Clifford algebra (a general reference for Clifford algebras is [62]).

Definition 2.3.18. An injective homomorphism of R-modules $\iota : \Lambda \longrightarrow A$ of Λ in an R-algebra A is said to be **compatible** with q if $\iota(v)^2 = q(v) \cdot 1$, for all $v \in V$. An R-algebra $C = C(\Lambda)$ with an injection $\iota_C : \Lambda \longrightarrow C$ compatible with q is said to be a **Clifford algebra** for (Λ, q) if for any R-algebra A and R-module monomorphism $\iota_A : \Lambda \longrightarrow A$, there exists a unique R-algebra homomorphism $\phi : C(\Lambda) \longrightarrow A$ such that $\phi \circ \iota_C = \iota_A$.

The Clifford algebra of (Λ, q) exists and is unique up to unique isomorphism. Let

$$T^i(\Lambda) = \begin{cases} R & i = 0 \\ \Lambda \otimes_R \cdots \otimes_R \Lambda \quad (i \text{ times }) & i > 0 \end{cases}$$

The Clifford algebra can be constructed as the quotient of the tensor algebra $T(\Lambda) = \oplus_i T^i(\Lambda)$ of Λ by the relations $v \otimes v - q(v)$, with ι defined to be the isomorphism of Λ with $T^1(\Lambda)$. The relations $v \otimes v - q(v)$ generating the kernel of the surjection $T(\Lambda) \longrightarrow C(\Lambda)$ lie in $\oplus_i T^{2i}(\Lambda)$. It follows that $C(\Lambda)$ has a $\mathbb{Z}/2\mathbb{Z}$-grading and we have a decomposition of R-modules $C(\Lambda) = C_0(\Lambda) \oplus C_1(\Lambda)$, where $C_0(\Lambda)$ is the even part of $C(\Lambda)$ and $C_1(\Lambda)$ is the odd part. The ring $C_0(\Lambda)$ is called the **even** Clifford algebra of (Λ, q). The Clifford algebra of the quadratic space (V, q) is defined to be the Clifford algebra $C(V)$ of (V, q) as a quadratic module over F. Let e be a nontrivial central idempotent of $C_0(V)$. The algebra $eC_0(\Lambda) \otimes \mathbb{Q}$ is a quaternion algebra ([62, Thm. 5.2.5]).

Let (Λ, q) be a quadratic module of rank 4 over R admitting a basis $\{v_1, \ldots, v_4\}$. Let Φ_q be the bilinear form associated to q. Then the **determinant** of Λ, denoted $\det(\Lambda)$, is defined to be $\det(\Phi_q(v_i, v_j))$. This is the square of the discriminant of (Λ, q) (see Definition 2.2.12) i.e., $\det(\Lambda) = d(\Lambda, q)^2$. The determinant is nonzero if and only if (Λ, q) is regular. The determinant is well-defined modulo $(R^\times)^2$.

Theorem 2.3.19. ([59, Thm. 61], [77]) (Kohel-Pays' criterion) Let (Λ, q) be a proper regular quadratic module of rank 4 over R of square determinant, contained in the quadratic space (V, q). Let e be a nontrivial central idempotent of $C_0(V)$. Then (Λ, q) is the quadratic module associated to a projective rank one left module for an order in the quaternion algebra $eC_0(\Lambda) \otimes \mathbb{Q}$ if and only if one of the following equivalent statements is true.

- $e\Lambda = eC_1(\Lambda)$;

- $e\Lambda$ is a left module for $eC_0(\Lambda)$;
- Λe is a right module for $eC_0(\Lambda)$;
- For every u in Λ, $e\Lambda u$ is a left ideal of $eC_0(\Lambda)$;
- For some u in Λ, $e\Lambda u$ is a left ideal of $eC_0(\Lambda)$;
- For some v in Λ, $v\Lambda e$ is a right ideal of $eC_0(\Lambda)$.

For any projective $\mathcal{O}$-module I of rank one, for $\mathcal{O}$ an order in the quaternion algebra H/L, we can define a reduced norm map from the reduced norm of $\mathcal{O}$. For every finite place $\mathfrak{l}$ of $\mathcal{O}_L$, fix a generator $x_\mathfrak{l}$ of $I_\mathfrak{l}$ as an $\mathcal{O}_\mathfrak{l}$-module. Since I is locally principal, every $x \in I$ is of the form $\alpha_\mathfrak{l} x_\mathfrak{l} \in I_\mathfrak{l}$ for some $\alpha_\mathfrak{l} \in \mathcal{O}_\mathfrak{l}$. Since $x_\mathfrak{l}$ is defined up to a unit in $\mathcal{O}_\mathfrak{l}^\times$, and $\mathrm{Norm}(\mathcal{O}_\mathfrak{l}^\times) = \mathcal{O}_{L_\mathfrak{l}}^\times$, we define $\mathrm{Norm}(x) = \mathrm{Norm}(\alpha_\mathfrak{l}) \mod \mathcal{O}_{L_\mathfrak{l}}^\times$. Since H is totally definite, the reduced norm on $H \otimes_{\sigma_i} \mathbb{R}$ is contained in $\mathbb{R}_{\geq 0}$ for all σ_i. Thus we define $\mathrm{Norm}(x)$ to be a totally positive generator of $\cap_\mathfrak{l}(\mathrm{Norm}(\alpha_\mathfrak{l})\mathcal{O}_{L_\mathfrak{l}} \cap \mathcal{O}_L)$, it is thus defined up to a totally positive unit (which is a square of an element of $(\mathcal{O}_L)^\times$, since $h^+(L) = 1$).

Proposition 2.3.20. (cf. [59, Prop. 51]) Let $\mathcal{O}$ be an order in a quaternion algebra H/L. Let I be a projective $\mathcal{O}$-module of rank one, with the quadratic map defined by the reduced norm on I. Then the determinant of I is $d(\mathcal{O})^2$. Any isomorphism of I with an ideal J of $\mathcal{O}$ determines a similitude $\sigma : I \longrightarrow \mathcal{O}$ with similitude factor $\mathrm{Norm}(J)$.

Proof. The reduced norm on I is defined using the local isomorphisms $I_\mathfrak{l} \cong \mathcal{O}_\mathfrak{l}$. Thus $\det(I_\mathfrak{l}) = \det(\mathcal{O}_\mathfrak{l}) \mod {\mathcal{O}_{L_\mathfrak{l}}^\times}^2$ for all $\mathfrak{l}$ and the two determinants are equal, since determinants (and levels likewise) are determined locally. The reduced norm on the order $\mathcal{O}$, restricted to elements of J is $\mathrm{Norm}(J)$ times the reduced norm on J defined via its left $\mathcal{O}$-module structure. Thus an isomorphism of I with J defines a similitude with factor $\mathrm{Norm}(J)$. □

Recall that L is a totally real field of narrow class number $h^+(L) = 1$.

Corollary 2.3.21. Suppose that p is unramified. Any totally positive definite, proper, quadratic module (Λ, q) over $\mathcal{O}_L$ of level p (and determinant p^2) contained in $B_{p,L}$ arises from a projective rank one left module for an order in $B_{p,L}$ if and only if the level of the associated order $eC_0(\Lambda)$ is p.

Remark 2.3.22. This corollary is not used in the sequel, but a priori, a totally definite, proper, quadratic module of level p could maybe come from a non-projective rank one left module for an order of level $\mathfrak{q}p$, for some $\mathfrak{q}|p$.

Proof. Since p is unramified, the level of $eC_0(\Lambda)$ will be p if and only if its discriminant is p (Propositions 2.2.22, 2.2.18) if and only if its determinant is p^2. We check Kohel-Pays' criterion. Note that $eC_0(\Lambda) \otimes \mathbb{Q} \cong B_{p,L}$ by assumption. Since the composite map $V \longrightarrow C_1(V) \longrightarrow eC_1(V) = eV$ is an isometry (cf. [59, Prop. 59, p. 76]); $\det(\Lambda) = \det(e\Lambda)$ and the quadratic module $e\Lambda$ is contained in the quadratic module $eC_1(\Lambda)$:

$$e\Lambda \subseteq eC_1(\Lambda).$$

Since $h(L) = 1$, any quadratic module is free over $\mathcal{O}_L$, and the two modules $e\Lambda$ and $eC_1(\Lambda)$ coincide if and only if the quadratic module $eC_1(\Lambda)$ has determinant equal to the determinant of $e\Lambda$ i.e., p^2 by [59, Prop. 50]. Since $eC_1(\Lambda)$ is a projective module over $eC_0(\Lambda)$ by [59, Prop. 60], $\det(eC_1(\Lambda)) = \det(eC_0(\Lambda))$ by the proof of Proposition 2.3.20 and we are done. □

Remark 2.3.23. More generally, the same proof applies when we know a priori that the associated order $eC_0(\Lambda)$ of (Λ, q) in $B_{p,L}$ is Gorenstein i.e., that its level is equal to its discriminant.

2.4 Abelian varieties

2.4.1 Polarizations and endomorphisms

Let L be a totally real number field of degree g over $\mathbb{Q}$ and let $\mathcal{O}_L$ be its ring of integers. Let S be a scheme. Let A be an abelian scheme over S of relative dimension $g = [L : \mathbb{Q}]$. Consider abelian schemes with $\mathcal{O}_L$-action

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

Definition 2.4.1. Let λ be a polarization on an abelian variety A, and put $\mathrm{End}^0(A) = \mathrm{End}(A) \otimes \mathbb{Q}$. The **Rosati involution** associated to λ is the map

$$\mathrm{End}^0(A) \longrightarrow \mathrm{End}^0(A), \qquad f \mapsto f^* := \lambda^{-1} f^t \lambda.$$

The Rosati involution is a positive involution on $\mathrm{End}^0(A)$. The semi-simple rational finite-dimensional algebras with positive involution were classifed by Albert. Every division algebra over $\mathbb{Q}$ with a positive involution belongs to one of the following four types of algebras ([92, §1]):

1. Type I: Totally real number field L;
2. Type II: Central simple algebra B over L such that the simple components of $B \otimes \mathbb{R}$ are all isomorphic to $M_2(\mathbb{R})$;
3. Type III: Central simple algebra B over L such that the simple components of $B \otimes \mathbb{R}$ are all isomorphic to the Hamilton quaternions over $\mathbb{R}$.
4. Type IV: Central simple algebra B over a totally imaginary quadratic extension of L.

The canonical involution σ is defined by $x \mapsto \sigma(x) = \mathrm{Tr}(x) - x$. For Type III algebras, the positive involution is necessarily the canonical involution.

Denote by $\mathcal{P}(A)$ the sheaf of $\mathcal{O}_L$-linear, symmetric morphisms from A to its dual abelian scheme A^t for the étale topology on (Sch/S). The sheaf $\mathcal{P}(A)^+$ is the subsheaf of $\mathcal{P}(A)$ obtained by imposing the extra condition that the morphisms be polarizations. We call $\mathcal{P}(A)$ the **polarization module** of A and $\mathcal{P}(A)^+$ the **positive cone** of polarizations. A **principal polarization** is a polarization $A \longrightarrow A^t$ which is also an isomorphism.

Definition 2.4.2. ([17, 2.1.3, p.64]) The abelian scheme A satisfies the **condition of Deligne-Pappas** if the canonical morphism $A \otimes_{\mathcal{O}_L} \mathcal{P}(A) \longrightarrow A^t$, $(a, \lambda) \mapsto \lambda(a)$ is an isomorphism.

This condition implies that $\mathcal{P}(A)$ is locally constant ([103, Lem. 1.8]).

Definition 2.4.3. An **abelian scheme with RM** is an abelian scheme with action by $\mathcal{O}_L$ satisfying the Deligne-Pappas condition.

Definition 2.4.4. ([82, §1, Def. 1.1, p. 257]) The abelian scheme A satisfies **the condition of Rapoport** if the Lie algebra of A is locally on S a free $\mathcal{O}_L \otimes_{\mathbb{Z}} \mathcal{O}_S$-module of rank 1.

Proposition 2.4.5. ([39, Lem. 5.5,p. 99]) The condition of Rapoport implies the condition of Deligne-Pappas.

Proposition 2.4.6. ([17, Cor. 2.9, p.66]) If p is unramified, the condition of Deligne-Pappas is equivalent to the condition of Rapoport.

Narrow class number one

Let $S = \mathrm{Spec}(k)$, k a field. Our theorems are proved under the hypothesis that the narrow class number $h^+(L)$ of the totally real number field L is one. This is equivalent to asking that $h(L) = 1$, and that all totally positive units are squares. If the class number $h(L) = 1$, $\mathcal{P}(A)$ is unique up to isomorphism as a projective $\mathcal{O}_L$-module of

rank one. If $h^+(L) = 1$, then $(\mathcal{P}(A), \mathcal{P}(A)^+) \cong (\mathcal{O}_L, \mathcal{O}_L^+)$ as invertible $\mathcal{O}_L$-modules with a notion of positivity. A principally polarized abelian variety with RM satisfies the Deligne-Pappas condition automatically. Conversely, an abelian variety A with RM always admits an $\mathcal{O}_L$-polarization ([82, Prop. 1.10]). Let $(\mathfrak{A}, \mathfrak{A}^+)$ be a projective $\mathcal{O}_L$-module with a notion of positivity.

The moduli space of pairs (A, ι) such that $(\mathcal{M}_A, \mathcal{M}_A^+) \cong (\mathfrak{A}, \mathfrak{A}^+)$, and the moduli space of triples (A, ι, ϕ), where $\phi : (\mathcal{M}_A, \mathcal{M}_A^+) \xrightarrow{\cong} (\mathfrak{A}, \mathfrak{A}^+)$ are the same when $h^+(L) = 1$. Since $Cl(L)^+$ classifies the isomorphism classes of projective $\mathcal{O}_L$-modules with a notion of positivity, we can assume that (A, ι) comes equipped with a given *principal* $\mathcal{O}_L$-linear polarization (see [17, §2.6]).

2.4.2 Dieudonné modules

Dieudonné modules were discussed extensively in the first part of this thesis (see Chapter I). The following is the bare minimum needed for the sequel. Let k be a perfect field. Denote by $W(k)$ the ring of Witt vectors over k. Let σ be the unique automorphism of $W(k)$ which reduces to the map $x \mapsto x^p$ on the residue field k. Let $W(k)[F, V]$ denote the non-commutative ring with indeterminates F, V subject to the relations $FV = VF = p$, and $Fa = a^\sigma F$ and $aV = Va^\sigma$ for $a \in W(k)$. The first crystalline cohomology group $\mathbb{D}(A) := H^1_{crys}(A/W(k))$ of an abelian variety A/k is a **Dieudonnné module**, i.e., a $W(k)[F, V]$-module that is free of finite rank over $W(k)$. This Dieudonné module (or equivalently, the corresponding p-divisible group) plays the role at p of the more familiar ℓ-adic Tate modules, which we review in the next subsection.

2.4.3 Tate modules

Our reference for this section is [109]. Let A, B be abelian varieties over a perfect field k, of dimension g, and let ℓ be a prime different from p. The scheme $A[\ell^n] := \ker(A \xrightarrow{\ell^n} A)$ is a finite étale group scheme of order $(\ell^n)^{2g}$, moreover $A[\ell^n] \cong (\mathbb{Z}/\ell^n\mathbb{Z})^{2g}$ when k is algebraically closed. The group schemes $A[\ell^n]$ form an inverse system under the maps $\ell^m : A[\ell^n] \longrightarrow A[\ell^{n-m}]$, $n \geq m$, and we fit them together to form the **Tate module** $T_\ell(A) = \varprojlim_n A[\ell^n]$. Over an algebraically closed field, $T_\ell(A) \cong \mathbb{Z}_\ell^{2g}$. We denote by $T_p(A)$ the p-divisible group of A, defined as the limit $\varinjlim A[p^n]$ of the inductive system of closed immersions

$$A[p] \hookrightarrow A[p^2] \hookrightarrow A[p^3] \hookrightarrow \cdots,$$

provided by the finite flat commutative group schemes $A[p^n]$ of rank $(p^n)^{2g}$.

Theorem 2.4.7. ([109, Thms. 3, 5]) The maps

$$\mathrm{Hom}_k(A, B) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \longrightarrow \mathrm{Hom}_{\mathrm{Gal}(\overline{k}/k)}(T_\ell(A), T_\ell(B)),$$

$$\mathrm{Hom}_k(A, B) \otimes \mathbb{Z}_p \longrightarrow \mathrm{Hom}_{\mathrm{Gal}(\overline{k}/k)}(T_p(A), T_p(B)),$$

are injective with torsion-free cokernels.

Theorem 2.4.8. ([109, Thm. 6]) Let k be a finite field. Then the maps of Theorem 2.4.7 are bijective.

Remark 2.4.9. Here is a confusing point: If A is a supersingular abelian variety over $\overline{\mathbb{F}}_p$, $\mathrm{End}(A) \otimes \mathbb{Z}_p \cong \mathrm{End}(A[p^\infty])$, but $\mathrm{End}(A) \otimes W(k) \cong \mathrm{End}_{W(k)}(\mathbb{D}(A))$ as $W(k)$-modules. The correct version of Tate's theorem using Dieudonné modules is

$$\mathrm{End}(A) \otimes \mathbb{Z}_p \cong \mathrm{End}_{W(k)[F,V]}(\mathbb{D}(A)).$$

2.4.4 The a-number

The main result of this section is not needed in the sequel. The reader can acquaint herself with the definition of the a-number and Theorems 2.4.10 and 2.4.11.
Let A be an abelian variety of dimension g over an algebraically closed field k of characteristic p. The a-number of A (cf. [70, §II 12-3]) is defined by

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

where α_p is the local-local group scheme of order p i.e., $\mathrm{Ker}(\mathrm{Fr} : \mathbb{G}_a/k \longrightarrow \mathbb{G}_a/k)$. Note that $0 \leq a(A) \leq g$.

Theorem 2.4.10. [95, Thm. 3.5, p.580] Let E_1, E_2, E_3, E_4 be supersingular elliptic curves over $k = \overline{k}$. Then $E_1 \times E_2 \cong E_3 \times E_4$.

Theorem 2.4.11. ([71, Thm. 2]) Let $k = \overline{k}$. A d-dimensional abelian variety A has a-number $a(A) = g$ if and only if $A \cong E^g$, E a supersingular elliptic curve.

An abelian variety A such that $A \cong E^g$, E a supersingular elliptic curve, is called **superspecial**.

Let $\mathcal{A}_g/\mathrm{Spec}(\mathbb{Z})$ be the moduli stack of principally polarized abelian varieties of dimension g. It is an irreducible algebraic stack of relative dimension $\frac{g(g+1)}{2}$. The fibres $\mathcal{A}_g \otimes \mathbb{F}_p$ and $\mathcal{A}_g \otimes \mathbb{Q}$ are irreducible. Let T_a be the locus of points $A \in \mathcal{A}_g \otimes \overline{\mathbb{F}}_p$ with $a(A) \geq a$.

Theorem 2.4.12. ([31, §6]) The dimension of T_a is equal to

$$\dim(T_a) = g(g+1)/2 - a(a+1)/2.$$

Theorem 2.4.13. ([32, Thm. 2.11]) The loci T_a are irreducible for $a < g$.

The T_a loci are analogous to *special Schubert cycles* ([57]). We give some support for this statement in the next theorem.

Theorem 2.4.14. Let $a > 0$. The set $\mathrm{Sing}(T_a)$ of singular points of the locus T_a is precisely T_{a+1}.

Remark 2.4.15. Note that $\mathcal{A}_g = T_0$ is smooth (as a stack).

Before proving the theorem, we need to state a well-known lemma.

Lemma 2.4.16. Let U_1, U_2 be two closed subsets of a variety $\mathcal{A}$, and let U_1 be irreducible. Suppose there exists $x \in U_1$ such that formally around x, U_1 is contained in U_2 i.e., $x \in U_2$ and $U_1 \subseteq U_2$ in $\widehat{\mathcal{O}_{x,\mathcal{A}}}$. Then $U_1 \subseteq U_2$.

Proof. Since U_1 is irreducible, the claim is reduced to verifying that the inclusion of sets infinitesimally implies the inclusion of sets locally i.e., we suppose without loss of generality that U_1, U_2 are affine. Since U_1, U_2 are closed, they correspond to ideals $\mathfrak{A}_1, \mathfrak{A}_2$ in $\mathcal{O}_{x,\mathcal{A}}$. Since U_1 is contained in U_2 formally around x i.e., $\widehat{\mathfrak{A}_2} \subseteq \widehat{\mathfrak{A}_1}$, where $\widehat{\mathfrak{A}_i} := \mathfrak{A}_i \cdot \widehat{\mathcal{O}_{x,\mathcal{A}}}$. Since $\widehat{\mathfrak{A}_i} \cap \mathcal{O}_{x,\mathcal{A}} = \mathfrak{A}_i$ ([113, Cor. 2, p. 257]), the inclusion $\mathfrak{A}_2 \subseteq \mathfrak{A}_1$ follows. □

Proof. (of Theorem 2.4.14) The inclusion $\mathrm{Sing}(T_a) \subset T_{a+1}$ is known ([31, Prop. 6.2]). We only need to prove the other inclusion : $T_{a+1} \subset \mathrm{Sing}(T_a)$. The locus T_a is irreducible, and contains T_g. If we can show locally around the superspecial points that $T_{a+1} \subseteq \mathrm{Sing}(T_a)$ holds, we are done by Lemma 2.4.16. The standard superspecial display has the form $\begin{pmatrix} 0 & -I_g \\ I_g & 0 \end{pmatrix}$ (where I_g is the g-by-g identity matrix), hence the Hasse-Witt matrix of the universal display (mod p) is given by a symmetric g-by-g matrix $\mathfrak{D} = (t_{ij})$, where $t_{ij} = t_{ji}$ are indeterminates. We can describe the locus of T_{a+1} and T_a as so-called symmetric determinantal varieties in terms of the Hasse-Witt matrix, given by the subdeterminants of rank $g - a$ (respectively $g - a + 1$). It is well-known (the "second fundamental theorem of invariant theory", see [3, Prop., p. 69]) that for so-called generic determinantal varieties the relation $T_{a+1} = \mathrm{Sing}(T_a)$ holds for $0 < a < g$. A similar result holds for symmetric matrices, as we show now.

Let I_a be the ideal generated by the $(g-a+1)\times(g-a+1)$-minors of $\mathfrak{D}$ for $0<a<g$. It is known ([61]) that I_a is a radical ideal in the symmetric case also. Thus, since I_a defines T_a, to show $T_{a+1}\subset \mathrm{Sing}(T_a)$, it is enough to show that the rank of the Jacobi matrix coming from T_a i.e., composed of the derivatives of the $(g-a+1)\times(g-a+1)$-minors at any points of T_{a+1} is smaller than $a(a+1)/2$. Observe that the derivative with respect to any variable t_{ij} of the subdeterminant of any m-by-m minor in the generic matrix is a subdeterminant of an $(m-1)$-by-$(m-1)$ minor. That is, if $(t_{i_rj_r})$, $1\leq r\leq m$, is an m-by-m minor, then

$$\frac{\delta}{\delta t_{i_{r_0}j_{r_0}}}\det(t_{i_rj_r})=\det(t_{i_sj_s}),\, s\neq r_0,$$

e.g., the line i_{r_0} and the column j_{r_0} being removed from the m-by-m minor to produce the $(m-1)$-by-$(m-1)$ minor. An analogous statement holds when we replace the generic matrix by the symmetric matrix e.g., the derivative of the subdeterminant of an m-by-m minor of the symmetrix matrix can be written as the sum of subdeterminants of $(m-1)$-by-$(m-1)$ minors of the symmetrix matrix. Let G be an arbitrary subdeterminant of the generic matrix and denote by ^{sym} the operation consisting in identifying t_{ij} and t_{ji}: as G runs through all subdeterminants of m-by-m minors of the generic matrix, G^{sym} runs through all subdeterminants of m-by-m minors of the symmetric matrix, trivially. If $G=G^{sym}$, or $G\neq G^{sym}$ and $i=j$, the result follows from the generic case, e.g., we actually get only one subdeterminant of a $(m-1)$-by-$(m-1)$ minor. In contrast, if $G\neq G^{sym}$ and $i\neq j$, the chain rule allows to write explicitly what the derivative is in the symmetric case:

$$\frac{\delta G^{sym}}{\delta t_{ij}}=\left(\frac{\delta G}{\delta t_{ij}}+\frac{\delta G}{\delta t_{ji}}\right)^{sym}=\left(\frac{\delta G}{\delta t_{ij}}\right)^{sym}+\left(\frac{\delta G}{\delta t_{ji}}\right)^{sym},$$

and this is clearly a sum of two subdeterminants. Summing up, the elements of the Jacobi matrix of T_a all vanish on T_{a+1}, and therefore $T_{a+1}\subset \mathrm{Sing}(T_a)$. □

2.5 The algebra of superspecial points on Hilbert modular varieties

2.5.1 Tate's theorem for supersingular abelian varieties with RM

Let $\overline{k}$ be the algebraic closure of a finite field k. All varieties will be defined over $\mathrm{Spec}(\overline{k})$. We show in this section a variant of Tate's Theorem for supersingular abelian varieties with RM.

Definition 2.5.1. An **α_p-isogeny** is an isogeny of abelian varieties that can be decomposed in a sequence of isogenies whose kernel is the local-local group scheme α_p. We say that two abelian varieties are α_p-isogenous if there exists an α_p-isogeny between them.

Remark 2.5.2. Note that α_p has a unique form over any perfect field.

The Siegel space $\mathcal{A}_{g,1}$ parametrizes g-dimensional principally polarized abelian varieties. Its supersingular locus $S_{g,1}$ has been much studied by Li and Oort in [65]. In particular, it is shown that any point in $S_{g,1}$ is linked to an arbitrary superspecial point by a sequence of α_p-isogenies ([65, p.23], cf. [65, §6.3]), called a rigid PFTQ. Li and Oort's work has been generalized in detail by S. Harashita to principally polarized supersingular abelian varieties with RM by $\mathcal{O}_L$ ([43, Prop. 4.10] and [43, §6 Coarse moduli spaces]; Harashita's thesis appeared in print in [44]), so the mere existence of rigid PFTQ with $\mathcal{O}_L$-structure i.e., in which in each step the α_p-isogeny respects the $\mathcal{O}_L$-structure, gives us the following result right away.

Proposition 2.5.3. (Harashita) Any two principally polarized supersingular abelian varieties with RM are α_p-isogenous.

Note that the $\mathcal{O}_L$-structure on an abelian variety A induces an $\mathcal{O}_L \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$-structure on its Tate module $T_\ell(A)$. Thus, the Tate module decomposes according to the primes $\mathfrak{l}|\ell\mathcal{O}_L$:

$$T_\ell(A) = \varprojlim A[\ell^n] = \prod_{\mathfrak{l}|\ell} \varprojlim A[\mathfrak{l}^n] =: \prod_{\mathfrak{l}|\ell} T_{\mathfrak{l}}(A).$$

Lemma 2.5.4. ([82, Lem. 1.3]) Let A be an abelian variety with RM over an algebraically closed field $\overline{k}$ of characteristic p. Then the Tate module $T_\ell(A)$ is a free $\mathcal{O}_L \otimes \mathbb{Z}_\ell$-module of rank 2 for any $\ell \neq p$.

Note that any two abelian varieties A defined over $\overline{k}$ are actually defined up to an isomorphism over a finite subfield of $\overline{k}$. We can fix k to be big enough i.e., so that A_1, A_2 and all $\mathcal{O}_L$-homomorphisms are defined over k.

Theorem 2.5.5. Let A_1, A_2 be two supersingular abelian varieties with RM by $\mathcal{O}_L$ defined over a finite field k. Then

$$\begin{aligned} \mathrm{Hom}_{\mathcal{O}_L,k}(A_1, A_2) \otimes \mathbb{Z}_\ell &\cong \mathrm{Hom}_{\mathcal{O}_L \otimes \mathbb{Z}_\ell}(T_\ell(A_1), T_\ell(A_2)) \\ &\cong M_2(\mathcal{O}_L \otimes \mathbb{Z}_\ell), \\ \mathrm{Hom}_{\mathcal{O}_L,k}(A_1, A_2) \otimes \mathbb{Z}_p &\cong \mathrm{Hom}_{\mathcal{O}_L \otimes W(k)[F,V]}(\mathbb{D}(A_2), \mathbb{D}(A_1)), \end{aligned}$$

where the homomorphisms respect the $\mathcal{O}_L$-structures.

Note that

$$\mathbb{Z}_\ell \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathcal{O}_L}(A_1, A_2) \cong \mathrm{Hom}_{\mathcal{O}_L \otimes \mathbb{Z}_\ell}(T_\ell(A_1), T_\ell(A_2))$$

if and only if

$$\mathcal{O}_{L_{\mathfrak{l}}} \otimes_{\mathcal{O}_L} \mathrm{Hom}_{\mathcal{O}_L}(A_1, A_2) \cong \mathrm{Hom}_{\mathcal{O}_{L_{\mathfrak{l}}}}(T_{\mathfrak{l}}(A_1), T_{\mathfrak{l}}(A_2)) \quad \forall \mathfrak{l}|\ell,$$

since

$$\prod_{\mathfrak{l}|\ell} \mathcal{O}_{L_{\mathfrak{l}}} \otimes_{\mathcal{O}_L} \mathrm{Hom}_{\mathcal{O}_L}(A_1, A_2) \cong \mathbb{Z}_\ell \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathcal{O}_L}(A_1, A_2)$$

and

$$\prod_{\mathfrak{l}|\ell} \mathrm{Hom}_{\mathcal{O}_{L_\mathfrak{l}}}(T_\mathfrak{l}(A_1), T_\mathfrak{l}(A_2)) \cong \mathrm{Hom}_{\mathcal{O}_L}(T_\ell(A_1), T_\ell(A_2)).$$

Proof. We explain the modifications to Tate's original argument ([96, §2]) that are necessary to adapt his proof to supersingular abelian varieties with RM by $\mathcal{O}_L$. Also, we skip the details of the proof for $\ell = p$, since the argument is similar.

We begin by explaining the disappearance of the Galois group $G = \mathrm{Gal}(\overline{k}/k)$ compared to the statement of the original Tate theorem (Theorem 2.4.7, cf. [14, Lemma 7.1]). This has everything to do with the fact that supersingular abelian varieties have lots of endomorphisms. We need to verify that the canonical map

$$\mathbb{Z}_\ell \otimes \mathrm{Hom}_{\mathcal{O}_L,k}(A_1, A_2) \longrightarrow \mathrm{Hom}_{\mathcal{O}_L \otimes \mathbb{Z}_\ell}(T_\ell(A_1), T_\ell(A_2)), \tag{2.5.1}$$

is injective. To see that, look at the following diagram:

$$\begin{array}{ccc} \mathbb{Z}_\ell \otimes \mathrm{Hom}_k(A_1, A_2) & \xrightarrow{f_1} & \mathrm{Hom}_G(T_\ell(A_1), T_\ell(A_2)) \\ {\scriptstyle f_2}\uparrow & & \uparrow{\scriptstyle f_3} \\ \mathbb{Z}_\ell \otimes \mathrm{Hom}_{\mathcal{O}_L,k}(A_1, A_2) & \xrightarrow[canonical]{} & \mathrm{Hom}_{G,\mathcal{O}_L \otimes \mathbb{Z}_\ell}(T_\ell(A_1), T_\ell(A_2)) \end{array}$$

The maps f_1, f_2 (and f_3) are all injective, hence the map "canonical" is also injective. Since the left side of the canonical map (2.5.1) has $\mathbb{Z}_\ell$-rank equal to $4g$ and the right side, once coordinates are chosen, is an order inside of $M_2(\mathcal{O}_L \otimes \mathbb{Z}_\ell)$, the cokernel is torsion. It follows that the Galois group G acts through scalars. Thus, after proving the analogue of Tate's theorem, we can eliminate the mention of G from the statement of the theorem in the end.

Recall the main ideas of Tate's proof: we reduce the desired bijection (in the statement of the theorem) to the bijection of the map:

$$\mathbb{Q}_\ell \otimes \mathrm{End}_{\mathcal{O}_L}(A) \longrightarrow \mathrm{End}_{\mathcal{O}_L}(V_\ell(A)), \tag{2.5.2}$$

for any abelian variety A defined over k, where $V_\ell(A) = T_\ell(A) \otimes \mathbb{Q}$. To show that the map in Equation (2.5.2) is bijective, we first use the fact that $h(L) = 1$ to show that

the canonical map is injective with *torsion-free* cokernel: if an $\mathcal{O}_L$-homomorphism $f : A_1 \longrightarrow A_2$ vanishes on $A_1[\mathfrak{l}]$, we pick a generator $\eta_\mathfrak{l}$ of the principal ideal $\mathfrak{l}$ to define the homomorphism $g := \eta_\mathfrak{l}^{-1} \circ f$ as in Tate's proof.

Tate then introduces two commuting subalgebras E_ℓ and F_ℓ of the $\mathbb{Q}_\ell$-algebra $\mathrm{End}(V_\ell(A))$ which are defined as follows: E_ℓ is the image of $\mathbb{Q}_\ell \otimes \mathrm{End}_k(A)$ under the map 2.5.2, while F_ℓ is the subalgebra of $\mathrm{End}(V_\ell(A))$ generated by the automorphisms of $V_\ell(A)$ defined by elements of G. Tate then proceeds to show that the desired bijection is again equivalent, by the theorem of bicommutation, to the fact that F_ℓ is the commutant of E_ℓ in $\mathrm{End}(V_\ell(A))$, if F_ℓ is semisimple.
The name of the game is now to consider the obvious $\mathcal{O}_L$-versions of these subalgebras and show that they are also commutant to one another.
In Tate's axiomatic proof comes next a hypothesis called $\mathrm{Hyp}(k, A, d, \ell)$ which is satisfied for finite fields: $\mathrm{Hyp}(k, A, d, \ell)$ stipulates that there exists (up to k-isomorphism) only a finite number of abelian varieties B defined over k such that:

- There exists a polarization ψ of B of degree d^2 defined over k
- There exists a k-isogeny $B \longrightarrow A$ of ℓ-power degree.

It is clear that the $\mathcal{O}_L$-version of this hypothesis holds for supersingular abelian varieties with RM by $\mathcal{O}_L$. Tate then proves two propositions under the hypothesis $\mathrm{Hyp}(k, A, d, \ell)$. The first proposition is to show that for any G-stable maximal isotropic subspace W of $V_\ell(A)$ with respect to the non-degenerate alternating bilinear form on $V_\ell(A)$ corresponding to an $\mathcal{O}_L$-linear polarization of A defined over k, there exists an element $u \in E_\ell$ such that W is the image of $V_\ell(A)$ under u. An additional ingredient necessary in the $\mathcal{O}_L$-setting is the existence of $\mathcal{O}_L$-polarizations of A: The existence of such a polarization was proved by Rapoport in his thesis ([82]).
Tate's second proposition shows that the Hypothesis $\mathrm{Hyp}(k, A, d, \ell)$ and the fact the the $\mathbb{Q}_\ell$-algebra F_ℓ is isomorphic to a product of copies of $\mathbb{Q}_\ell$ implies that the map

2.5.2 is bijective. The proof proceeds by descending induction of the dimension of an isotropic subspace of $V_\ell(A)$, and thus the first induction is guaranteed by Tate's first proposition, and the rest of the proof is completely general. Tate's proof finishes by using the particulars of assuming k to be finite to relate F, the subalgebra of $\mathbb{Q} \otimes \mathrm{End}_k(A)$ generated by the Frobenius endomorphism of A relative to k, with F_ℓ, thus showing that F_ℓ is indeed semisimple and moreover isomorphic to a product of copies of $\mathbb{Q}_\ell$. The $\mathcal{O}_L$-version of the proof's ending follows from the fact that the Frobenius endomorphism commutes with any $\mathcal{O}_L$-endomorphism. □

Corollary 2.5.6. Let A_1, A_2 be two principally polarized superspecial abelian varieties with RM with isomorphic Dieudonné modules $\mathbb{D}(A_1) \cong \mathbb{D}(A_2)$ defined over a finite field k. Then $\mathrm{Hom}_{\mathcal{O}_L}(A_1, A_2)$ is a projective $\mathrm{End}_{\mathcal{O}_L}(A_1)$-module of rank one.

Proof. Let $\mathcal{O} := \mathrm{End}_{\mathcal{O}_L}(A_1)$. By Proposition 2.2.34, an $\mathcal{O}$-ideal is projective if and only if it is locally principal. We thus check the latter condition. Tate's theorem for supersingular $\mathcal{O}_L$-abelian varieties shows that

$$\mathrm{Hom}_{\mathcal{O}_L}(A_1, A_2) \otimes \mathbb{Z}_\ell \cong \mathrm{Hom}_{\mathcal{O}_L \otimes \mathbb{Z}_\ell}(T_\ell(A_1), T_\ell(A_2));$$

respectively,

$$\mathrm{Hom}_{\mathcal{O}_L}(A_1, A_2) \otimes \mathbb{Z}_p \cong \mathrm{Hom}_{\mathcal{O}_L \otimes W(k)[F,V]}(\mathbb{D}(A_2), \mathbb{D}(A_1)).$$

It follows that

$$\begin{aligned} \mathrm{Hom}_{\mathcal{O}_L}(A_1, A_2) \otimes \mathbb{Z}_\ell &\cong \mathrm{Hom}_{\mathcal{O}_L \otimes \mathbb{Z}_\ell}(T_\ell(A_1), T_\ell(A_2)) \\ &\cong \mathrm{Hom}_{\mathcal{O}_L \otimes \mathbb{Z}_\ell}(T_\ell(A_1), T_\ell(A_1)) \\ &\cong \mathrm{End}_{\mathcal{O}_L}(A_1) \otimes \mathbb{Z}_\ell \end{aligned}$$

where we have used that $T_\ell(A_i) \cong (\mathcal{O}_L \otimes \mathbb{Z}_\ell)^2$, and thus $\mathrm{Hom}_{\mathcal{O}_L}(A_1, A_2)$ is locally principal at $\ell \neq p$. A similar argument shows that $\mathrm{Hom}_{\mathcal{O}_L}(A_1, A_2)$ is locally principal at p.

□

The projective $\mathrm{End}_{\mathcal{O}_L}(A_1)$-module $\mathrm{Hom}_{\mathcal{O}_L}(A_1, A_2)$ can be embedded as an integral ideal in $\mathrm{End}_{\mathcal{O}_L}(A_1)$ by the map $f \mapsto \phi \circ f$, where $\phi : A_2 \longrightarrow A_1$ is an arbitrarily chosen $\mathcal{O}_L$-isogeny.

Corollary 2.5.7. Let p be unramified in $\mathcal{O}_L$. Let A_1, A_2 be two principally polarized superspecial abelian varieties with RM. Then $\mathrm{Hom}_{\mathcal{O}_L}(A_1, A_2)$ is a projective $\mathrm{End}_{\mathcal{O}_L}(A_1)$-module.

Proof. If p is unramified, there is a *unique* superspecial Dieudonné module with RM. Indeed, since in general Dieudonné modules factorize according to the ramification of p (cf. [38, §2.3]), we can reduce the question to the inert case, which is found in [36, Thm. 5.4.4]; see also Chapter I of the present thesis for a discussion of the totally ramified case. □

We need a version of Tate theorem's for supersingular abelian varieties with RM that holds for principally polarized abelian varieties.
Denote by $\mathbb{Z}_\ell(1) = \varprojlim \mu_{\ell^r}$ the inverse limit of ℓ^r-th roots of unity for all positive integers r and let λ be an $\mathcal{O}_L$-polarization of (A, ι). The polarization λ and the Weil pairing

$$e_\ell : T_\ell(A) \times T_\ell(A^t) \longrightarrow \mu_{\ell^\infty},$$

induce an alternating form $e_\lambda := e_\ell(-, \lambda(-))$ on $T_\ell(A)$ such that the elements of $\mathcal{O}_L$ are self-adjoint. This is equivalent to an alternating $\mathcal{O}_L \otimes \mathbb{Z}_\ell$-bilinear form

$$\psi_\lambda : T_\ell(A) \times T_\ell(A) \longrightarrow \mathcal{D}_L^{-1} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell(1),$$

such that $\mathrm{Tr}_{L/\mathbb{Q}} \circ \psi_\lambda = e_\ell(-, \lambda(-))$. We shall call a pairing such as ψ_λ an **alternating pairing of a Tate module with RM**.

Definition 2.5.8. A quasi-polarization on $\mathbb{D}(A)$ is an $(\mathcal{O}_L \otimes W(k))$-bilinear form $e_\lambda = e_p(-, \lambda(-))$ from

$$\mathbb{D}(A) \otimes \mathbb{D}(A) \longrightarrow \mathcal{D}_L^{-1} \otimes W(k)$$

satisfying the conditions:

$$e_\lambda(Fx, y) = e_\lambda(x, Vy)^\sigma, \quad e_\lambda(Vx, y) = e_\lambda(x, Fy)^{\sigma^{-1}},$$

$$e_\lambda(x, y) = -e_\lambda(y, x),$$

where σ is the Frobenius.

Theorem 2.5.9. Let $(A_1, \iota_1, \lambda_1), (A_2, \iota_2, \lambda_2)$ be two principally polarized supersingular abelian varieties with RM by $\mathcal{O}_L$. Then

$$\mathrm{Hom}_{\mathcal{O}_L}((A_1, \lambda_1), (A_2, \lambda_2)) \otimes \mathbb{Z}_\ell \cong \mathrm{Hom}_{\mathcal{O}_L \otimes \mathbb{Z}_\ell}((T_\ell(A_1), e_{\lambda_1}), (T_\ell(A_2), e_{\lambda_2})),$$

and

$$\mathrm{Hom}_{\mathcal{O}_L}((A_1, \lambda_1), (A_2, \lambda_2)) \otimes \mathbb{Z}_p \cong \mathrm{Hom}_{\mathcal{O}_L \otimes W(k)}((\mathbb{D}(A_2), e_{\lambda_2}), (\mathbb{D}(A_1), e_{\lambda_1})),$$

where

$$\mathrm{Hom}_{\mathcal{O}_L}((A_1, \lambda_1), (A_2, \lambda_2)) \otimes R := \{\phi \in \mathrm{Hom}_{\mathcal{O}_L}(A_1, A_2) \otimes R \text{ such that } \phi^* \lambda_2 = \lambda_1\},$$

and where

$$\mathrm{Hom}_{\mathcal{O}_L \otimes \mathbb{Z}_\ell}((T_\ell(A_1), e_{\lambda_1}), (T_\ell(A_2), e_{\lambda_2}))$$

$$:= \{\phi \in \mathrm{Hom}_{\mathcal{O}_L \otimes \mathbb{Z}_\ell}((T_\ell(A_1), (T_\ell(A_2)) | \phi^* e_{\lambda_2} = e_{\lambda_1}\},$$

and similarly at $\ell = p$.

Proof. Let $\ell \neq p$. The map

$$\mathrm{Hom}_{\mathcal{O}_L}((A_1, \lambda_1), (A_2, \lambda_2)) \otimes \mathbb{Z}_\ell \hookrightarrow \mathrm{Hom}_{\mathcal{O}_L \otimes \mathbb{Z}_\ell}((T_\ell(A_1), e_{\lambda_1}), (T_\ell(A_2), e_{\lambda_2})),$$

is clearly injective. Pick a map $\phi \in \mathrm{Hom}_{\mathcal{O}_L\otimes\mathbb{Z}_\ell}((T_\ell(A_1), e_{\lambda_1}), (T_\ell(A_2), e_{\lambda_2}))$. Then, by Theorem 2.5.5, there exists a map $\psi \in \mathrm{Hom}_{\mathcal{O}_L}(A_1, A_2) \otimes \mathbb{Z}_\ell$ which induces ϕ and $\psi^*\lambda_2 = q \cdot \lambda_1$ for some $q \in \mathcal{O}_L \otimes \mathbb{Z}_\ell$. An alternating pairing on $T_\ell(A)$ can be viewed as an element of

$$\mathrm{Hom}_{\mathcal{O}_L\otimes\mathbb{Z}_\ell}(\wedge^2_{\mathcal{O}_L\otimes\mathbb{Z}_\ell} T_\ell(A), \mathcal{D}_L^{-1} \otimes \mathbb{Z}_\ell(1)),$$

so a map $\psi \in \mathrm{Hom}_{\mathcal{O}_L}(A_1, A_2)$ will induce a map $\wedge^2\psi : \wedge^2 T_\ell(A_1) \longrightarrow \wedge^2 T_\ell(A_2)$ that makes the obvious diagram commute i.e., $e_{\lambda_1} = e_{\lambda_2} \circ \wedge^2\psi$. Since A_1 and A_2 are principally polarized, they are α_p-isogenous, we can suppose that $e_{\lambda_1} = e_{\lambda_2}$ for $\ell \neq p$, and this amounts to $\wedge^2\psi = 1$ i.e., $q = \wedge^2\psi = 1$. The proof is similar for $\ell = p$. □

Corollary 2.5.10.

$$\mathrm{Aut}(\mathrm{End}^{e_\lambda}_{\mathcal{O}_L}(T_\ell(A)) = \{\phi \in \mathrm{End}_{\mathcal{O}_L}(A) \otimes \mathbb{Z}_\ell |\ \phi'\phi = 1\},$$

$$\mathrm{Aut}(\mathrm{End}^{e_\lambda}_{\mathcal{O}_L}(\mathbb{D}(A)) = \{\phi \in \mathrm{End}_{\mathcal{O}_L}(A) \otimes \mathbb{Z}_p |\ \phi'\phi = 1\},$$

where ϕ' is the Rosati involution induced by λ.

Proof. If $A_1 = A_2 = A$, the condition $\phi^*\lambda_1 = \lambda_1$ is the same as $\phi'\phi = 1$. □

2.5.2 Transitivity of the Hecke action of $\mathcal{H}_\ell$

We prove the existence of an ℓ-power degree $\mathcal{O}_L$-isogeny between any two superspecial abelian varieties with RM with isomorphic Dieudonné modules: this follows from the strong approximation theorem ([12, Proof of Prop. 4.6]) and using Corollary 2.5.10 to adapt the argument to the RM case. The idea of the proof is that the ℓ-power Hecke orbit of a supersingular point on the Hilbert moduli space can be described by double cosets for the ℓ-adic points of a suitable algebraic group. To obtain the desired result, we apply the strong approximation theorem to show that the double cosets parameterizing the ℓ-power Hecke orbit of a superspecial point x on the Hilbert

moduli space has the same cardinality as the double cosets (for the adelic points of the same algebraic group) parameterizing the set of superspecial points with the same Dieudonné module as x.

This argument in the elliptic case is to be found in great detail in Cornut's Ph.D. thesis (see [16, Cor. 5.5.6], but bear in mind that the prime characteristic in that reference is ℓ, not p).

Let A_x be a fixed (principally polarized) superspecial abelian variety with RM by $\mathcal{O}_L$. Let G_x denote the group scheme over $\mathrm{Spec}(\mathbb{Z})$ whose group of R-points, for any commutative ring R, is :

$$G_x(R) = \left\{\phi \in (\mathrm{End}_{\mathcal{O}_L}(A_x) \otimes R)^\times ; \phi'\phi = 1\right\},$$

where $\phi \mapsto \phi'$ is the Rosati involution induced by the polarization of A_x. We will sometimes drop the suffix in G_x if no confusion can arise.

Let Λ_x denotes the set of isomorphism classes of principally polarized superspecial abelian varieties with RM (A, λ, ι) of dimension g over k such that the Dieudonné module $\mathbb{D}(A)$ is isomorphic to $\mathbb{D}(A_x)$ as quasi-polarized Dieudonné modules with RM, and the Tate module $T_\ell(A)$ is isomorphic to $T_\ell(A_x)$ as nondegenerate alternating $\mathcal{O}_L \otimes \mathbb{Z}_\ell$-modules for all $\ell \neq p$. We know that these conditions are automatically satisfied i.e., that the prime-to-p Tate modules are isomorphic, since there exists an α_p-isogeny between any two principally polarized superspecial abelian varieties with RM by Proposition 2.5.3; the condition at p is satisfied by hypothesis.

Theorem 2.5.11. ([111, Thm. 10.5]) The set Λ_x is in natural bijection with the (adelic) double cosets $G_x(\mathbb{Q})\backslash G_x(\mathbb{A}_f)/G_x(\hat{\mathbb{Z}})$.

We now describe the ℓ-Hecke orbit of a superspecial point on the Hilbert moduli space can be describe by the ℓ-adic points of the same algebraic group G_x.

We adapt to our algebraic group G_x the argument of Ching-Li Chai ([12, Proof of Prop. 4.6]): The special unitary group G_x over $\mathbb{Q}$ attached to the semisimple algebra

$\mathrm{End}_{\mathcal{O}_L}(A_x) \otimes_{\mathbb{Z}} \mathbb{Q} \cong B_{p,L}$ with Rosati involution is an inner form of SU_2 such that $G_x(\mathbb{R}_\sigma) \cong SU_2(\mathbb{R})$ is compact for any embedding $\sigma : L \hookrightarrow \mathbb{R}$, while

$$G_x(\mathbb{Q}_\ell) = \{b \in (B_{p,L} \otimes \mathbb{Q}_\ell)^\times | \mathrm{Norm}(b) = 1\}$$

is non-compact for every prime number $\ell \neq p$. The $\mathbb{Z}_\ell$-lattice $\mathrm{End}_{\mathcal{O}_L}(A_x) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ in $\mathrm{End}_{\mathcal{O}_L}(A_x) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$ defines a maximal compact subgroup $G_x(\mathbb{Z}_\ell)$ of $G_x(\mathbb{Q}_\ell)$. Note that

$$\mathrm{End}_{\mathcal{O}_L}(A_x) \otimes_{\mathbb{Z}} \mathbb{Z}_p \xrightarrow{\cong} \mathrm{End}_{\mathcal{O}_L}(\mathbb{D}(A_x))$$

by our supersingular version of Tate's theorem. Moreover,

$$G_x(\mathbb{Z}_p) = \mathrm{Aut}(\mathrm{End}^{e_\lambda}_{\mathcal{O}_L}(\mathbb{D}(A_x)))$$

by Corollary 2.5.10.

We now describe the Hecke orbits in terms of G_x: by the argument of [11, End of §1] (cf. [12, p.9], [16, Prop. 5.5.2]), the prime-to-p Hecke orbit of x on the Hilbert moduli space of $\Gamma_0(N)$ level $(N, p) = 1$, is in natural bijection with the finite set

$$(G_x(\mathbb{Q}) \cap G_x(\mathbb{Z}_p)) \backslash \prod_{r \neq p}{}' G_x(\mathbb{Q}_r) / \Gamma_0(N),$$

where $\Gamma_0(N)$ is the usual congruence subgroup of restricted product $\prod'_{r \neq p} G_x(\mathbb{Q}_r)$ of level N. We are only interested in the $N = 1$ case, so the prime-to-p Hecke orbit of the point x on the Hilbert moduli space is in natural bijection with the double cosets

$$(G_x(\mathbb{Q}) \cap G_x(\mathbb{Z}_p)) \backslash \prod_{r \neq p}{}' G_x(\mathbb{Q}_r) / \prod_{r \neq p}{}' G_x(\mathbb{Z}_r).$$

A similar argument of course applies to the ℓ-power Hecke orbit. The ℓ-power Hecke orbit $\mathcal{H}_\ell \cdot x$ of a point x is thus parametrized by:

$$\Big(G_x(\mathbb{Q}) \cap \prod_{\ell' \neq \ell} G_x(\mathbb{Z}_{\ell'})\Big) \backslash G_x(\mathbb{Q}_\ell) / \Gamma_0(N)',$$

where $\Gamma_0(N)'$ is the congruence subgroup of $G_x(\mathbb{Q}_\ell)$ of level N e.g., $G_x(\mathbb{Z}_\ell)$ if $N = 1$.

Now that we have the description of the ℓ-Hecke orbit, we use the strong approximation theorem to related the ℓ-adic double cosets with the adelic double cosets.

For the group G_x, the statement of the strong approximation theorem ([102, p.81]) is: $G_x(\mathbb{Q})G_x(\mathbb{Q}_\ell)$ is dense in $G_x(\mathbb{A}_f)$. Since $G_x(\widehat{\mathbb{Z}})$ is open in $G_x(\mathbb{A}_f)$, we thus get the equality:

$$G_x(\mathbb{Q}_\ell)G_x(\widehat{\mathbb{Z}})G_x(\mathbb{Q}) = G_x(\mathbb{A}_f).$$

It follows that for any $\widehat{g}_{\mathbb{A}_f} \in G_x(\mathbb{A}_f)$, there exists some $g_{\mathbb{Q}} \in G_x(\mathbb{Q})$, $g_\ell \in G_x(\mathbb{Q}_\ell)$ and $\widehat{g}_{\widehat{\mathbb{Z}}} \in G_x(\widehat{\mathbb{Z}})$ such that $g_{\mathbb{Q}} g_\ell \widehat{g}_{\widehat{\mathbb{Z}}} = \widehat{g}_{\mathbb{A}_f}$. This implies that the map $\mathbb{Q}_\ell \hookrightarrow \mathbb{A}_f$ induces a surjection:

$$G_x(\mathbb{Q}_\ell) \twoheadrightarrow G_x(\mathbb{Q})\backslash G_x(\mathbb{A}_f)/G_x(\hat{\mathbb{Z}}).$$

which in turn yields a bijection at the level of double cosets

$$G_x(\mathbb{Z}[\frac{1}{\ell}])\backslash G_x(\mathbb{Q}_\ell)/G_x(\mathbb{Z}_\ell) \longrightarrow G_x(\mathbb{Q})\backslash G_x(\mathbb{A}_f)/G_x(\hat{\mathbb{Z}}).$$

Since $G_x(\mathbb{Z}[\frac{1}{\ell}]) = G_x(\mathbb{Q}) \cap \prod_{\ell' \neq \ell} G_x(\mathbb{Z}_{\ell'})$, this shows that the ℓ-power Hecke orbit of the point x is Λ_x. We therefore conclude:

Proposition 2.5.12. Let A_1, A_2 be principally polarized supersingular abelian varieties with RM with Tate modules $T_\ell(A_1), T_\ell(A_2)$ and Dieudonné modules $\mathbb{D}(A_1)$, $\mathbb{D}(A_2)$. Recall that $T_\ell(A_1) \cong T_\ell(A_2)$ as $\mathcal{O}_L \otimes \mathbb{Z}_\ell$-module with alternate pairings by Proposition 2.5.3. Assume further that $\mathbb{D}(A_1) \cong \mathbb{D}(A_2)$ as quasi-polarized $\mathcal{O}_L \otimes W(k)$-modules, a condition holding automatically if p is unramified (see Proposition 2.5.7). Then for any prime $\ell \neq p$, there exists an ℓ-power isogeny between A_1 and A_2. In particular, the module $\mathrm{Hom}_{\mathcal{O}_L}(A_1, A_2)$ contains two isogenies which are of coprime degrees.

2.5.3 Quadratic forms arising from superspecial points

Let A_1, A_2 be two abelian varieties with RM. Let $\lambda_i = A_i \longrightarrow A_i^t, i = 1, 2$, be principal $\mathcal{O}_L$-polarizations, and define, for $\phi \in \mathrm{Hom}_{\mathcal{O}_L}(A_1, A_2)$

$$||\phi|| = ||\phi||_{\lambda_1,\lambda_2} := \lambda_1^{-1} \circ \phi^t \circ \lambda_2 \circ \phi, \qquad \begin{array}{ccc} A_2^t & \xleftarrow{\lambda_2} & A_2 \\ {\scriptstyle \phi^t}\downarrow & & \uparrow{\scriptstyle \phi} \\ A_1^t & \xrightarrow[\lambda_1^{-1}]{} & A_1 \end{array} .$$

Then we obtain a function:

$$|| - || : \mathrm{Hom}_{\mathcal{O}_L}(A_1, A_2) \longrightarrow \mathrm{End}_{\mathcal{O}_L}(A_1).$$

Lemma 2.5.13. The function $|| - ||$ takes values in $\mathcal{O}_L \subset \mathrm{End}_{\mathcal{O}_L}(A_1)$ and is a totally positive $\mathcal{O}_L$-integral quadratic form,

1. $||\phi|| = 0$ if and only if $\phi = 0$ and $||\phi|| \gg 0$ for all $\phi \neq 0$;
2. $< \phi, \psi >_{\mathcal{O}_L} := ||\phi + \psi|| - ||\phi|| - ||\psi|| = \lambda_1^{-1}\psi^t\lambda_2\phi + \lambda_1^{-1}\phi^t\lambda_2\psi$ is a symmetric $\mathcal{O}_L$-bilinear form. In particular,
3. $||\ell \circ \phi|| = \ell^2||\phi||$, for $\ell \in \mathcal{O}_L$.

Proof. The element $||\phi||$ is fixed by the Rosati involution $f \mapsto f' = \lambda_1^{-1} f^t \lambda_1$:

$$\lambda_1^{-1} \cdot (\lambda_1^{-1} \circ \phi^t \circ \lambda_2 \circ \phi)^t \lambda_1 = \lambda_1^{-1} \circ \phi^t \circ \lambda_2 \circ \phi.$$

This implies that $||\phi|| \in \{\psi \in \mathrm{End}_{\mathcal{O}_L}(A_1) | \psi' = \psi\} = \mathcal{O}_L$, since in general, the Rosati involution fixes L in $\mathrm{End}^0_{\mathcal{O}_L}(A_1)$: If A_1 and A_2 are supersingular abelian varieties, it follows from Albert's classification that we are in the Type III situation: the quaternion algebra $\mathrm{End}_{\mathcal{O}_L}(A_1) \otimes \mathbb{Q}$ over the totally real field L is totally definite, hence the Rosati involution is the canonical involution i.e., the conjugation map i.e., $x^\sigma = \mathrm{Tr}(x) - x = \overline{x}$ on the quaternion algebra $B_{p,L}$. Since λ_1 is principal, all computations are integral, and the image of $|| - ||$ is $\mathcal{O}_L$.

Let us check Assertion (1). Clearly, $||\phi|| = 0$ if and only if ϕ is the zero map (any non-zero $\mathcal{O}_L$-homomorphism of abelian varieties is an isogeny). The total positivity follows from properties of the embedding of the Néron-Severi group $NS^0(A)$ in $\mathrm{End}^0_{\mathcal{O}_L}(A_1)^{sym}$ via the map $\mu \mapsto \lambda_1^{-1}\mu$ ([39, p.46]): the polarizations are sent to positive symmetric elements. We finally check the $\mathcal{O}_L$-linearity of the symmetric bilinear form. The argument is essentially the same for the first variable and the second variable:

$$\begin{aligned}
||\ell \circ \phi + \psi|| - ||\ell \circ \phi|| - ||\psi|| &= \lambda_1^{-1}\psi^t\lambda_2(\ell \circ \phi) + \lambda_1^{-1}(\ell \circ \phi)^t\lambda_2\psi \\
&= \lambda_1^{-1}\psi^t\ell^t\lambda_2\phi + \lambda_1^{-1}\phi^t\ell^t\lambda_2\psi \\
&= \lambda_1^{-1}\ell^t\psi^t\lambda_2\phi + \lambda_1^{-1}\ell^t\phi^t\lambda_2\psi \\
&= \ell\lambda_1^{-1}\psi^t\lambda_2\phi + \ell\lambda_1^{-1}\phi^t\lambda_2\psi \\
&= \ell(||\phi + \psi|| - ||\phi|| - ||\psi||)
\end{aligned}$$

□

How can we compare $||-||$ with the norm form on $\mathrm{End}^0_{\mathcal{O}_L}(A)$?

Proposition 2.5.14. The $\mathcal{O}_L$-degree $||-||$ is multiplicative: if $\psi \in \mathrm{Hom}_{\mathcal{O}_L}(A_2, A_3)$ and $\phi \in \mathrm{Hom}_{\mathcal{O}_L}(A_1, A_2)$, then

$$||\psi \circ \phi||_{\lambda_1,\lambda_3} = ||\psi||_{\lambda_2,\lambda_3} \cdot ||\phi||_{\lambda_1,\lambda_2}.$$

Proof.

$$\begin{aligned}
||\psi \circ \phi||_{\lambda_1,\lambda_3} &= \lambda_1^{-1}(\psi\phi)^t\lambda_3(\psi\phi) \\
&= \lambda_1^{-1}\phi^t\lambda_2\lambda_2^{-1}\psi^t\lambda_3\psi\phi \\
&= \lambda_1^{-1}\phi^t\lambda_2||\psi||_{\lambda_2,\lambda_3}\phi \\
&= ||\psi||_{\lambda_2,\lambda_3}\lambda_1^{-1}\phi^t\lambda_2\phi \\
&= ||\psi||_{\lambda_2,\lambda_3} \cdot ||\phi||_{\lambda_1,\lambda_2}.
\end{aligned}$$

□

Remark 2.5.15. This property defines the quadratic form up to a constant multiple.

Lemma 2.5.16. Let $\psi \in \mathrm{Hom}_{\mathcal{O}_L}(A_1, A_2)$. Let $\mathcal{O} = \mathrm{End}_{\mathcal{O}_L}(A_1)$. We can use ψ to embed $\mathrm{Hom}_{\mathcal{O}_L}(A_1, A_2)$ as an $\mathcal{O}$-ideal:

$$\mathrm{Hom}_{\mathcal{O}_L}(A_1, A_2) \overset{j_\psi}{\hookrightarrow} \mathrm{End}_{\mathcal{O}_L}(A_1),$$

$$\phi \mapsto \lambda_1^{-1} \circ \psi^t \circ \lambda_2 \circ \phi.$$

Then

$$\mathrm{Norm}(j_\psi(\phi)) = ||\psi^t|| \cdot ||\phi||.$$

Let I_ψ be the $\mathcal{O}$-ideal $j_\psi(\mathrm{Hom}_{\mathcal{O}_L}(A_1, A_2))$. Then the reduced norm $N(I_\psi)$ is equal to the ideal $(||\psi^t||)$.

Remark that for $A_1 = A_2$, $\lambda_1 = \lambda_2$,

$$||\phi|| = \phi' \cdot \phi = \mathrm{Norm}(\phi),$$

for $\phi \in \mathrm{End}_{\mathcal{O}_L}(A_1)$.

Proof. Compute the norm of $j_\psi(\phi)$:

$$\begin{aligned}
\mathrm{Norm}(j_\psi(\phi)) &= \overline{j_\psi(\phi)} j_\psi(\phi) \\
&= [\lambda_1^{-1} \circ (\lambda_1^{-1} \circ \psi^t \circ \lambda_2 \circ \phi)^t \circ \lambda_1] \circ [\lambda_1^{-1} \circ \psi^t \circ \lambda_2 \circ \phi] \\
&= [\lambda_1^{-1} \phi^t \lambda_2 \psi][\lambda_1^{-1} \psi^t \lambda_2 \phi] \\
&= [\lambda_2 \psi \lambda_1^{-1} \psi^t][\lambda_1^{-1} \phi^t \lambda_2 \phi] \\
&= ||\psi^t|| \cdot ||\phi||,
\end{aligned}$$

since $\lambda_2 \psi \lambda_1^{-1} \psi^t \in \mathcal{O}_L$. It follows that

$$||j_\psi(\phi)|| = \mathrm{Norm}(j_\psi(\phi)) = ||\psi^t|| \cdot ||\phi||,$$

hence the norm of I_ψ, being the greatest common denominator of the norms of the elements $||j_\psi(\phi)||$, is the greatest common denominator of all $||\psi^t|| \cdot ||\phi||$, for $\phi \in \mathrm{Hom}_{\mathcal{O}_L}(A_1, A_2)$. Since any superspecial abelian varieties with isomorphic superspecial crystal admit two isogenies ϕ_1, ϕ_2 of relatively coprime absolute degree by Proposition 2.5.12 i.e., such that

$$\Big(\mathrm{Norm}_{L/\mathbb{Q}}||\phi_1||, \mathrm{Norm}_{L/\mathbb{Q}}||\phi_2||\Big) = 1,$$

and thus $(||\phi_1||, ||\phi_2||) = (1)$, thence it follows that $N(I_\psi) = (||\psi^t||)$. □

Summarizing the previous discussion, we obtain the desired link between the norm map and the $\mathcal{O}_L$-degree.

Proposition 2.5.17. Let $\mathcal{O} := \mathrm{End}_{\mathcal{O}_L}(A_1)$. Let $\mathrm{Hom}_{\mathcal{O}_L}(A_1, A_2) \cong \mathfrak{A}$, $\mathfrak{A}$ an integral $\mathcal{O}$-ideal. Then the $\mathcal{O}_L$-degree of an $\mathcal{O}_L$-isogeny ϕ_x corresponding to a non-zero element $x \in \mathfrak{A}$ is related to the norm of the quaternion algebra by the formula, valid up to a unit:

$$||\phi_x|| = \frac{\mathrm{Norm}(x)}{\mathrm{Norm}(\mathfrak{A})}.$$

The indeterminacy between the $\mathcal{O}_L$-degree and the norm of an *element* is thus a constant multiple: it is a totally positive element well-defined up to a totally positive unit.

2.5.4 Tensor construction

We gather a few well-known properties of a tensor construction attributed to Serre (cf. [14, §7] and [16, §10]).

Definition 2.5.18. ([14, Thm. 7.2]) Let S be a scheme. Let R be an associative ring with identity, M be a finitely generated projective right R-module with dual left R-module $M^t := \mathrm{Hom}_R(M, R)$ of right R-linear homomorphisms and $\mathfrak{M}$ be a left

R-module scheme over S i.e., an R-module object in the category of S-schemes. The functor

$$T \longrightarrow M \otimes_R \mathfrak{M}(T) \cong \mathrm{Hom}_R(M^t, \mathfrak{M}(T)) \tag{2.5.3}$$

is represented by a commutative group scheme over S, denoted by $M \otimes_R \mathfrak{M}$.

In particular, if $\mathfrak{M}$ is an abelian scheme, then $M \otimes_R \mathfrak{M}$ is also an abelian scheme.

Definition 2.5.19. ([14, Def. 7.6]) A finitely generated projective (right) R-module M has **constant rank r** if the finitely generated right K-module $M \otimes_{R,\phi} K$ has length $d_K r$ for every map $\phi : R \longrightarrow K$ to a finite-dimensional central simple algebra over an algebraically closed field $k = Z(K)$, with $\dim_k K = d_K^2$. In other words, as a right K-module, $M \otimes_{R,\phi} K$ is isomorphic to an r-fold direct sum of copies of K.

Proposition 2.5.20. ([14, Proof of Thm. 7.8]) Let $\mathfrak{M} \longrightarrow S$ be a locally finite type left R-module scheme over S, and let M be a finitely generated projective (right) R-module. We use the notation $\mathfrak{T}_0$ to denote the tangent space at 0. There is a natural isomorphism:

$$M \otimes_R \mathfrak{T}_0(\mathfrak{M}) \cong \mathfrak{T}_0(M \otimes_R \mathfrak{M}).$$

Proposition 2.5.21. ([14, Thm. 7.5]) Let $\mathfrak{M}$ be a left R-module scheme which has relative dimension g over S. Then $M \otimes_R \mathfrak{M}$ has relative dimension gr over S if the module M has constant rank r over R.

Proposition 2.5.22. ([14, Lem. 8.2]) Let R be an associative ring and M a finitely generated projective left R-module. For any left R-module scheme $\mathfrak{M}$ over S and any commutative S-group scheme G, view the group $\mathrm{Hom}_S(\mathfrak{M}, G)$ as a right R-module via the R-action on $\mathfrak{M}$. Then the natural map:

$$\eta_M : \mathrm{Hom}_S(\mathfrak{M}, G) \otimes_R M \longrightarrow \mathrm{Hom}_S(\mathrm{Hom}_R(M, \mathfrak{M}), G),$$

defined functorially by $\eta_M(\phi \otimes m) : f \mapsto \phi(f(m))$ (on the level of points in S-schemes) is well-defined and an isomorphism.

2.5.5 Endomorphism orders of superspecial abelian varieties

In this section, we need to establish another property of the tensor construction. In general, if A is an abelian scheme equipped with an action by a commutative ring R, and T is an R-algebra, it is natural to expect that the following isomorphism holds:

$$\mathrm{End}_R(A) \otimes_R T \cong \mathrm{End}_T(A \otimes_R T).$$

In fact, as we will see shortly, a more general statement holds. We specifically need the case $R = \mathbb{Z}$, A a supersingular elliptic curve and $T = \mathcal{O}_L$.

Lemma 2.5.23. ([11, Lem. 6]) Let L be a totally real field. Let (A, ι) be an abelian variety of dimension $g = [L : \mathbb{Q}]$ 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/k. Let $D = \mathrm{End}_k(B) \otimes_{\mathbb{Z}} \mathbb{Q}$, so $\mathrm{End}_k(A) \otimes_{\mathbb{Z}} \mathbb{Q} \cong M_n(D)$. Consider the case when D is a totally definite quaternion division algebra over $\mathbb{Q}$, $dim(B) = 1$ and the field k has characteristic p. Then the algebra $D = B_{p,\infty}$ is the quaternion division algebra over the rationals ramified at p and ∞, and B is a supersingular elliptic curve over k. The centralizer of L in $\mathrm{End}_k(A) \otimes_{\mathbb{Z}} \mathbb{Q}$,

$$\mathbf{Cent}_{\mathrm{End}_k(A)\otimes\mathbb{Q}}(L),$$

is the quaternion division algebra $B_{p,\infty} \otimes L$ which is ramified at all infinite places of the totally real field L and all places v of L above p such that $[L_v : \mathbb{Q}_p]$ is odd, and is unramified at all other finite places.

Lemma 2.5.24. ([14, Lem. 7.14]) Let R be an associative ring, M_1 and M_2 two finite projective left R-modules. Let M_1^t denote the right module of left-linear maps from M_1 to A. For any two left R-module schemes $\mathfrak{M}_1$ and $\mathfrak{M}_2$ over a base S, view the group $\mathrm{Hom}_S(\mathfrak{M}_1, \mathfrak{M}_2)$ as a right R-module via the R-action on $\mathfrak{M}$ and as a left

R-module via the action on $\mathfrak{M}_2$. Then the natural map:

$$\eta_{M_2,M_1} : M_1^t \otimes_R \mathrm{Hom}_S(\mathfrak{M}_1, \mathfrak{M}_2) \otimes_R M_2 \longrightarrow \mathrm{Hom}_S(\mathrm{Hom}_R(M_2, \mathfrak{M}_1), \mathrm{Hom}_R(M_1, \mathfrak{M}_2)) \tag{2.5.4}$$

defined functorially by

$$\eta_{M_2,M_1}(\ell_1 \otimes \phi \otimes m_2))(f) : m_1 \mapsto \ell_1(m_1)\phi(f(m_2)),$$

(on the level of points in S-schemes) is well-defined and an isomorphism.
In particular, there is a natural isomorphism

$$M^t \otimes_R \mathrm{End}_S(\mathfrak{M}) \otimes_R M \cong \mathrm{End}_S(\mathrm{Hom}_R(M, \mathfrak{M})),$$

given by $\ell \otimes \phi \otimes m \mapsto (f \mapsto \ell(-) \cdot \phi(f(m)))$, and this is an isomorphism of associative rings.

Remark 2.5.25. An interesting feature of Lemma 2.5.24 is that the natural map 2.5.4 upgrades to an isomorphism of associative rings when both sides of 2.5.4 are rings e.g., $\mathfrak{M}_1 = \mathfrak{M}_2$ and $M_1 = M_2$; $\mathfrak{M}_1 = \mathfrak{M}_2$ and $M_2 = R$, M_1^t an R-algebra (or vice versa);

Proposition 2.5.26. Let E be a supersingular elliptic curve. Then $\mathrm{End}_{\mathcal{O}_L}(E \otimes \mathcal{O}_L) \cong \mathrm{End}(E) \otimes \mathcal{O}_L$. In particular, the order $\mathrm{End}_{\mathcal{O}_L}(E \otimes \mathcal{O}_L)$ is Bass.

Proof. We have seen earlier (2.3.3) that $\mathrm{End}(E) \otimes \mathcal{O}_L$ is primitive. Thence, it suffices to show that the centralizer of $\mathcal{O}_L$ in $\mathrm{End}(E \otimes \mathcal{O}_L)$, $\mathrm{End}_{\mathcal{O}_L}(E \otimes \mathcal{O}_L)$, is isomorphic to $\mathrm{End}(E) \otimes \mathcal{O}_L$.

First, the general algebraic properties of Hom and $\otimes$ gives the following isomorphism of rings:

$$\begin{aligned} \mathrm{End}_{\mathcal{O}_L}(E \otimes_{\mathbb{Z}} \mathcal{O}_L) &\cong \mathrm{Hom}(E, \mathrm{Hom}_{\mathcal{O}_L}(\mathcal{O}_L, E \otimes_{\mathbb{Z}} \mathcal{O}_L)) \\ &\quad \text{(by the Hom-}\otimes\text{ adjunction)} \\ &\cong \mathrm{Hom}(E, E \otimes_{\mathbb{Z}} \mathcal{O}_L) \text{ (by definition).} \end{aligned}$$

From Lemma 2.5.24, we get the second isomorphism of rings needed:

$$\begin{aligned}\mathcal{O}_L \otimes_{\mathbb{Z}} \mathrm{End}(E) &\cong \mathrm{Hom}(\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, E), \mathrm{Hom}_{\mathbb{Z}}(\mathcal{O}_L^t, E)) \\ &\cong \mathrm{Hom}(E, E \otimes_{\mathbb{Z}} \mathcal{O}_L) \text{ (cf. Equation 2.5.3)}\end{aligned}$$

We conclude immediately that

$$\mathrm{End}_{\mathcal{O}_L}(E \otimes_{\mathbb{Z}} \mathcal{O}_L) \cong \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathcal{O}_L.$$

□

Theorem 2.5.27. Let p be unramified. Let A be a principally polarized superspecial abelian variety with RM. Then $\mathrm{End}_{\mathcal{O}_L}(A)$ is a superspecial order of level p.

Proof. By Proposition 2.5.12, the order $\mathrm{End}_{\mathcal{O}_L}(A)$ is locally conjugate to the order $\mathrm{End}_{\mathcal{O}_L}(E \otimes \mathcal{O}_L) = \mathrm{End}(E) \otimes \mathcal{O}_L$, which is a superspecial order of level p. Since being superspecial is a local property, we are done.

Remark 2.5.28. This also follows straight from Theorem 2.5.5.

□

2.5.6 The bijection between ideal classes and superspecial points

Let p be unramified. The goal of this section is to give a direct connection between superspecial abelian varieties with real multiplication and the arithmetic of quaternion algebras over totally real fields, generalizing the classical bijection between supersingular elliptic curves and left ideals classes of a maximal order in the rational quaternion algebra ramified at p and ∞. We suppose that p is unramified throughout, so that the order $\mathcal{O}$ under consideration is an Eichler order of level p. The precise identification of the orders appearing as endomorphism orders of superspecial

abelian varieties with RM by $\mathcal{O}_L$ enabled us to derive, using standard tools, the class number formula or rather an expression in terms of double cosets of the number of ideal classes (see Corollary 2.3.8). It turns out that this finite set $B^1(\mathcal{O})\backslash J_B^1/B^\times$ has the same cardinality as the set of superspecial points on a Hilbert modular variety à la Deligne-Pappas. We use the Serre tensor construction to establish a functorial bijection. The argument using kernel ideals we generalize was already developed and applied to the case of elliptic curves in [108, §3], where the endomorphism order is maximal.

Definition 2.5.29. Let A be a superspecial abelian variety with RM by $\mathcal{O}_L$. Denote by I an integral left $\mathcal{O}$-ideal, where $\mathcal{O} = \mathrm{End}_{\mathcal{O}_L}(A)$. We define $A[I]$ to be the scheme-theoretic intersection of the kernels of all $\alpha \in I$. A left $\mathcal{O}$-ideal I is called a **kernel ideal** if $I = \{\alpha \in \mathcal{O} | \alpha(A[I]) = 0\}$.

The tensor construction is defined in Definition 2.5.18 and studied in depth in Section 2.5.4. It was also defined in detail in the context of Hilbert modular varieties in [28, Proposition 1.2.7].

Proposition 2.5.30. Let A be a superspecial abelian variety with RM. Let I be a projective rank one $\mathcal{O}$-module, where $\mathcal{O} = \mathrm{End}_{\mathcal{O}_L}(A)$. Then $A \otimes_{\mathcal{O}} I$ is also a superspecial abelian variety with RM.

Proof. Since A is principally polarized, the cotangent space will be killed by Verschiebung if and only if the tangent space is killed by Frobenius. Both conditions are equivalent to A being superspecial. It follows from Proposition 2.5.20 that Frobenius also kills the tangent space of $A \otimes_{\mathcal{O}} I$, and we are done. □

Theorem 2.5.31. ([108, Prop. 3.11]) Let $\mathfrak{A}$, $\mathfrak{B}$ be kernel ideals. Then

$$A \otimes_{\mathcal{O}} \mathfrak{A} \cong A \otimes_{\mathcal{O}} \mathfrak{B}$$

if and only if

$$[\mathfrak{A}] = [\mathfrak{B}]$$

i.e., $\mathfrak{A} = \mathfrak{B}\nu$ for some $v \in B_{p,L}^{\times}$.

We now make this theorem relevant by showing that any left ideal of the hereditary order $\mathcal{O} = \mathrm{End}_{\mathcal{O}_L}(A)$, as in the case of a maximal order in $B_{p,\infty}$, is a kernel ideal.

Definition 2.5.32. ([108, Def., p.533]) Let I_1 be a left $\mathcal{O}$-ideal. The ideal

$$I_2 := \{\rho \in \mathcal{O} | \rho(A[I_1]) = 0\}$$

is called the **associated kernel ideal** to I_1. Note that $A[I_1] = A[I_2]$, so I_2 is indeed a kernel ideal.

Lemma 2.5.33. Let I_1 be a left $\mathcal{O}$-ideal, and let $I_1 \subset I_2$ be the associated kernel ideal. Then $N_{L/\mathbb{Q}}(\mathrm{Norm}(I_1)) = N_{L/\mathbb{Q}}(\mathrm{Norm}(I_2))$, and therefore $I_1 = I_2$ i.e., all $\mathcal{O}$-ideals are kernel ideals.

Proof. The proof by Waterhouse ([108, Thm. 3.15]) in the maximal case essentially relies on a theorem of Nehrkorn (see below) which generalizes without modification to the hereditary case. □

Proposition 2.5.34. (Nehrkorn) Let I be an $\mathcal{O}$-ideal. Let $\mathcal{O}_r(I)$ be its right order. Then there is an $\mathcal{O}_r(I)$-ideal J such that $IJ = R\lambda$ for $\lambda \in B_{p,L}$, and

$$(\mathrm{Norm}_{L/\mathbb{Q}}(N(J)), |A[I]|) = 1.$$

Proof. The proof of Nehrkorn's theorem in Deuring's book ([21, Satz 27, p. 106]) only uses the fact that a (left) ideal is locally principal, which is always true in the hereditary case. □

Theorem 2.5.35. The map $\mathfrak{B} \mapsto A \otimes_{\mathcal{O}} \mathfrak{B}$ from ideal classes of $\mathcal{O}$ to superspecial abelian varieties with RM by $\mathcal{O}_L$ is a bijection at the level of sets and is functorial in A.

Proof. The functoriality is clear from the construction given in Section 2.5.4. We have seen that all $\mathcal{O}$-ideals are kernel ideals, hence the map $\mathfrak{B} \mapsto A \otimes_{\mathcal{O}} \mathfrak{B}$ is injective. We just need to prove it is surjective. Let A' be a superspecial variety with RM. We want to find a projective module $\mathfrak{B}$ such that $A \otimes_{\mathcal{O}} \mathfrak{B} \cong A'$. Consider $\mathfrak{B} := \mathrm{Hom}_{\mathcal{O}_L}(A, A')$. The natural map ψ:

$$A \otimes_{\mathcal{O}} \mathrm{Hom}_{\mathcal{O}_L}(A, A') \xrightarrow{\psi} A', \quad a \otimes \phi \mapsto \phi(a).$$

is a well-defined, and an isomorphism of abelian varieties with RM. □

Corollary 2.5.36. Let p be unramified. All superspecial orders $\mathcal{O}$ of $B_{p,L}$ of level $p\mathcal{O}_L$ arise from geometry.

Proof. Since superspecial orders $\mathcal{O}$ of level p are locally isomorphic (Proposition 2.2.28), the set of right orders of a complete set of representatives of left, projective ideal classes of any superspecial order of level p represent all isomorphism classes of superspecial orders by [102, Lem. 4.10, p. 26] and Proposition 2.2.34 (cf. [102, Cor. 5.5, p. 88]). □

2.5.7 Application of Kneser's Theorem to superspecial orders

The avowed purpose of this subsection is to coin Kneser's Theorem, and derive an easy corollary pertaining to superspecial abelian varieties.

Theorem 2.5.37. (Kneser) Let f be a totally positive definite quadratic form in $n \geq 4$ variables over the totally real field L. There is a constant C_f (depending

effectively on f) such that if $\nu \in \mathcal{O}_L$ is totally positive and $\mathrm{Norm}(\nu) \geq C_f$, then the number ν is primitively represented by f if and only if it is primitively represented locally at every completion v of L. By primitive representation, we mean an integral n-tuple $(x_1, \ldots, x_n)$ such that $gcd(x_1, \ldots, x_n) = (1)$.

Proof. The proof in ([10, §11, Section 9]) for $\mathbb{Q}$ works for any totally real number field L. □

Definition 2.5.38. An $\mathcal{O}_L$-isogeny $\phi : A_1 \longrightarrow A_2$ is **primitive** if for any factorization $\phi = [m] \circ \psi$, where ψ is an $\mathcal{O}_L$-isogeny and $[m]$ is multiplication-by-m for $m \in \mathcal{O}_L$, it is necessary that $m \in \mathcal{O}_L^{\times}$.

The strategy of the proof of the existence of an isogeny of arbitrary degree in the elliptic case (as in [59, Cor. 77]) works in the Hilbert case. Recall that we proved the existence of an ℓ-power isogeny in Proposition 2.5.12.

Theorem 2.5.39. Let A_1, A_2 be two principally polarized superspecial abelian varieties with RM. Then for every $n \in \mathcal{O}_L$ sufficiently large and relatively prime to p, there exists a primitive isogeny $\phi : A_1 \longrightarrow A_2$ over k of $\mathcal{O}_L$-degree n.

Proof. We equip the module M of k-isogenies with the structure of a quaternary quadratic module with the $||-||$ map. It is sufficient to look at solutions locally. Put $\mathcal{O} := \mathrm{End}_{\mathcal{O}_L}(A_1)$. For all primes $\mathfrak{l}$ in $\mathcal{O}_L$, the projective $\mathcal{O}_{\mathfrak{l}}$-module $M_{\mathfrak{l}}$ is free of rank one over $\mathcal{O}_{\mathfrak{l}}$ and generated by an isogeny of degree relatively prime to $\mathfrak{l}$. For all primes away from p, $\mathcal{O}_{\mathfrak{l}}$ splits and the local condition is trivially satisfied, because the matrix algebra $M_2(\mathcal{O}_L)$ represents all (totally positive) integers primitively. Thus we need only consider the primes $\mathfrak{p}$ over p in $B_{p,\infty} \otimes L$. Here also, every integer n relatively prime to p is represented, since $\mathcal{O}_{\mathfrak{p}}$ contains a split extension or an unramified quadratic extension $R_{\mathfrak{p}}$ of $\mathcal{O}_{L_{\mathfrak{p}}}$, $\mathcal{O}$ being superspecial (see Definition 2.3.13), and the reduced norm map on $\mathcal{O}_{\mathfrak{p}}$ induces the surjective norm map on units

Norm : $R_{\mathfrak{p}}^{\times} \longrightarrow \mathcal{O}_{L_{\mathfrak{p}}}^{\times}$. Since n lies in $\mathcal{O}_{L_{\mathfrak{p}}}$, any representation of n is trivially primitive in $M_{\mathfrak{p}}$. At places $\mathfrak{p}||p$ unramified in $B_{p,L}$, there is also a split or an unramified extension, and the same argument applies. Thus the conditions of Kneser's theorem are satisfied, and the result follows. □

2.6 Theta series arising from superspecial points

In this section, p is arbitrary. Let A_1, A_2 be two principally polarized superspecial abelian varieties. The $\mathcal{O}_L$-module $\mathrm{Hom}_{\mathcal{O}_L}(A_1, A_2)$ becomes a quadratic module when equipped with the $\mathcal{O}_L$-degree $||-||$ (see Lemma 2.5.13). We study in this section the theta series that arise from these quadratic modules. We prove that the q-expansion

$$\Theta := \sum_{\mathcal{O}_L \ni \nu \gg 0 \text{ or } \nu = 0} a_\nu q^\nu,$$

where

$$a_\nu = |\{\phi \in \mathrm{Hom}_{\mathcal{O}_L}(A_1, A_2) \text{ such that } ||\phi|| = \nu\}|,$$

is the q-expansion of a Hilbert modular form. This actually stems from the fact that Θ is a theta series i.e., a_ν is given by the totally positive quadratic form $||-||$. In particular, $a_0 = 1$ (the zero map!). Since $h^+(L) = 1$, all totally positive units are squares and thus the quadratic form $||-||$ is uniquely defined as the norm up to an integral change of basis, operation under which the representation numbers of the quadratic form are invariant. This shows that the theta series does not depend on the polarizationos λ_1, λ_2 used for the definition of the $\mathcal{O}_L$-degree $||-||$.

Theorem 2.6.1. A theta series constructed from a quadratic $\mathcal{O}_L$-lattice (M, q) of level $\mathcal{N}$ yields a Hilbert modular form of weight 2 and quadratic character χ_M (modulo the level) given by a Gauss sum, which transforms under the group

$$\mathrm{SL}_2(\mathcal{O}_L \oplus \mathcal{N} \cdot \mathrm{Norm}(M)\mathcal{D}_L) := \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \begin{pmatrix} \mathcal{O}_L & (\mathrm{Norm}(M)\mathcal{D}_L)^{-1} \\ \mathcal{N}\mathrm{Norm}(M)\mathcal{D}_L & \mathcal{O}_L \end{pmatrix} | ad - bc = 1\},$$

where $\mathcal{N} = (p)$ is the level of the lattice M, and $\mathcal{D}_L$ is the different of L.

Proof. This was first proved by Eichler ([24, Th. I]). □

We apply this general theorem to the $\mathcal{O}_L$-lattices $(\mathrm{Hom}_{\mathcal{O}_L}(A_1, A_2), ||-||)$ of level (p) (the level has been calculated in Proposition 2.3.20).
We need to explain why the quadratic character χ is identically 1 for the theta series coming from quaternion algebras. The expression of χ_M in terms of a Gauss sum in [24, Thm. I] for a lattice of $\mathcal{O}_L$-rank 4 is given by the formula:

$$\chi_M(\delta) = \frac{i^{2g}}{n(\gamma)^2\sqrt{\Phi}} \sum_{\mathcal{X} \in M/\delta M} e^{\pi i tr(\delta^{-1} q(\mathcal{X}))}, \quad \Phi = \det(tr(q(I_\mu, I_\nu))),$$

where $\gamma \in \mathcal{N}\mathrm{Norm}(M)\mathcal{D}_L$, and Φ is computed with respect to a basis I_μ, I_ν of M. This is a quadratic character modulo the level, and it is equal to 1 if the determinant of M is a square. Since the determinant of $(\mathrm{Hom}_{\mathcal{O}_L}(A_1, A_2), ||-||)$ is always a square (in this occurrence p^2), the quadratic character χ_M is thus identically 1.
For $(M, q) = (\mathrm{Hom}_{\mathcal{O}_L}(A_1, A_2), ||-||)$, the existence of two isogenies of coprime degrees imply that $\mathrm{Norm}(M)$ is 1. But since $h(L) = 1$, the group of transformation is actually isomorphic to $\Gamma_0(p)$ i.e., the matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \left(\begin{smallmatrix} \mathcal{O}_L & \mathcal{O}_L \\ p\mathcal{O}_L & \mathcal{O}_L \end{smallmatrix}\right)$ such that $ad - bc = 1$: the bottom-left entry and the top-right entry "cancel out" if the ideals are principal, since $\mathrm{SL}_2(\mathcal{O}_L)$ and $\mathrm{SL}_2(\mathcal{O}_L, \mathcal{D}_L)$ are conjugate. Thus, the value of the norm of the quadratic $\mathcal{O}_L$-lattice $\mathrm{Hom}_{\mathcal{O}_L}(A_1, A_2))$ disappears completely from the end result.

2.7 The Basis Problem for Hilbert modular forms

We explain the derivation of a special case of the Basis Problem for Hilbert modular forms from the Jacquet-Langlands correspondence i.e., we show that theta series coming from ideals of an Eichler order of level p in $B_{p,\infty} \otimes L$ span the space of Hilbert modular newforms of weight two for $\Gamma_0(p)$ (and trivial character).

The Jacquet-Langlands correspondence ([52, Thm. 16.1]) establishes, for any totally definite quaternion algebra B, a Hecke-equivariant injection $\pi \mapsto JL(\pi)$ from the set of classes of automorphic representations $\pi = \otimes_v \pi_v$ of $G_B(\mathbb{A}) = (B \otimes_F \mathbb{A})^\times$ with the set of classes of automorphic representations of $\mathrm{GL}_2(\mathbb{A})$. The image of the map is the set of cuspidal automorphic representations of $\mathrm{GL}_2(\mathbb{A})$ that are discrete series (i.e., special or supercuspidal at a finite place) at all ramified places of B. Imposing that the representation is of the discrete series at infinite places means that it is holomorphic of weight $k \geq 2$. A complete proof of the Jacquet-Langlands correspondence can be found in [34, §VI, Section 2]; for a more complete discussion, see [47, §5].

The key fact that we use is that the representation $\pi_{\mathfrak{p}}$ corresponding to a newform at a prime $\mathfrak{p}$ whose exponent is odd in the level is necessarily in the discrete series, since the conductor at $\mathfrak{p}$ is not a square (see [33, Proof of Prop. 5.21, p. 95; Table 4.20, p. 73]). Recall from Lemma 2.5.23 that a prime $\mathfrak{p}$ dividing p is ramified in $B_{p,\infty} \otimes L$ if and only if $[L_{\mathfrak{p}} : \mathbb{Q}_p]$ is odd. It is necessary for this to happen that the exponent α of $\mathfrak{p}^\alpha$ occuring in the prime decomposition of p is odd i.e., for level p, only odd exponents occur. But then the local representation $\pi_{\mathfrak{p}}$ of any cuspidal automorphic representation of $\mathrm{GL}_2(\mathbb{A})$ of level p occurs in the discrete series at $\mathfrak{p}$ for any ramified place p of $B_{p,L}$.

In brief, in the case of level exactly equal to p, the Jacquet-Langlands correspondence implies that all cuspidal automorphic representations of $\mathrm{GL}_2(\mathbb{A})$ arise as quaternionic representations on the adelic group associated to the quaternion algebra $B_{p,L}$.

Having explained the situation in the representation-theoretic setting, we derive the classical statement that the corresponding space of Hilbert newforms of weight 2 and level (p) is spanned by classical theta series. We follow [46, §5].

The space $S_2^{B_{p,L}}(\mathfrak{N}, \mathbb{C})$ of modular forms on $B_{p,L}$ is defined as the space of functions satisfying [48, Condition (SB1), p. 201]. The space $S_2(\mathfrak{N}, \mathbb{C})$ is the space of functions $f : GL_2(\mathbb{A}) \longrightarrow \mathbb{C}$ satisfying [48, Conditions (SA1), (SA2), (SA3), p. 193], that

is, the automorphy condition, the holomorphy condition and some rapid decreasing condition at all cusps of GL_2; this space corresponds to classical Hilbert cusp forms of weight 2 and $\Gamma_0(\mathfrak{N})$-level.

Theorem 2.7.1. ([48, Thm. 4.34, p.202]) Suppose $\mathfrak{N} = \mathfrak{N}_0 d(B_{p,L})$ for an integral ideal $\mathfrak{N}_0$ prime to $d(B_{p,L})$. Then we have an Hecke-equivariant embedding $S_2^{B_{p,L}}(\mathfrak{N}, \mathbb{C}) \hookrightarrow S_2(\mathfrak{N}, \mathbb{C})$. The image of this embedding only depends on $B_{p,L}$ and is made up of cusp forms in $S_2(\mathfrak{N}, \mathbb{C})$ new at all primes dividing $d(B_{p,L})$.

Remark 2.7.2. Since $B_{p,L}$ is totally definite, the elements of $S_2^{B_{p,L}}(\mathfrak{N}, \mathbb{C})$ can be viewed as functions on the double cosets parametrizing ideals classes of an Eichler order of level $d(B_{p,L})\mathfrak{N}_0$ (cf. [46, p.2112] and [47, p. 46]): Put $\mathfrak{N} = p$ and $\mathfrak{N}_0$ such that $\mathfrak{N}_0 d(B_{p,L}) = p$; $\mathfrak{N}_0$ is clearly prime to $d(B_{p,L})$. We now explain why a maximal order in $B_{p,L}$ equipped with $\mathfrak{N}_0$-level structure is the same thing as an Eichler order of level p in $B_{p,L}$. This is clear from the local description of Eichler orders: at primes dividing $d(B_{p,L})$, we locally have a maximal orders, so there is no difference with the global maximal order at those primes; at a prime $\mathfrak{q}$ dividing $\mathfrak{N}_0$, the local order $\mathcal{O}_q$ is isomorphic to $\begin{pmatrix} \mathcal{O}_{L_\mathfrak{q}} & \mathcal{O}_{L_\mathfrak{q}} \\ \mathfrak{q}\mathcal{O}_{L_\mathfrak{q}} & \mathcal{O}_{L_\mathfrak{q}} \end{pmatrix}$, which we recognize to be the local maximal order $M_2(\mathcal{O}_{L_\mathfrak{q}})$ with $\Gamma_0(\mathfrak{q})$-level.

Corollary 2.7.3. ([46, p. 2113]) Let $\mathcal{H}(\mathbb{C})$ be the Hecke algebra in $\mathrm{End}(S_2^{B_{p,L}}(\mathfrak{N}, \mathbb{C}))$. Then $S_2^{B_{p,L}}(\mathfrak{N}, \mathbb{C})$ is free of rank 1 over $\mathcal{H}(\mathbb{C})$.

Hida then defines a "theta map"

$$\Theta : S_2^{B_{p,L}}(\mathfrak{N}, \mathbb{C}) \otimes_{\mathcal{H}(\mathbb{C})} S_2^{B_{p,L}}(\mathfrak{N}, \mathbb{C}) \longrightarrow S_2^{new}(\Gamma_0(\mathfrak{N}); \mathbb{C}),$$

which is an isomorphism by [46, Cor. 5.2] since $S_2^{B_{p,L}}(\mathfrak{N}, \mathbb{C})$ is free of rank 1 over $\mathcal{H}(\mathbb{C})$ for $\mathfrak{N}$ squarefree. As pointed out by Hida ([46, Case $r = 0$, p. 2114] and [47, Equation 7.9], $\Theta(f, g)$, for $f, g \in S_2^{B_{p,L}}(\mathfrak{N}, \mathbb{C})$, is the classical theta series associated to an ideal of an Eichler order of level $\mathfrak{N}$ of $B_{p,L}$. We thus get that all Hilbert newforms

of weight 2 and level $\Gamma_0(\mathfrak{N})$ come from the space $S_2^{B_{p,L}}(\mathfrak{N},\mathbb{C})$ via the theta map i.e., theta series of left ideals of an Eichler order of level $\mathfrak{N}$ in $B_{p,L}$ span $S_2^{new}(\Gamma_0(\mathfrak{N});\mathbb{C})$. We state our conclusion.

Theorem 2.7.4. Let p unramified. Let $S_2(\Gamma_0(p),1)^{new}$ be the subspace of new-forms of the vector space of Hilbert modular forms of weight two, level p. Then $S_2(\Gamma_0(p),1)^{new}$ is spanned by theta series coming from left ideals of an Eichler order of level p in the quaternion algebra $B_{p,L}$.

Remark 2.7.5. A self-contained exposition of this result can be found [33, Thm. 10.13] in the elliptic case.

2.7.1 Examples

The more explicit examples of Hilbert modular forms and theta series that appear in the literature are typically computed for real quadratic fields of narrow class number one e.g., $\mathbb{Q}(\sqrt{5})$; nonetheless, fairly general explicit formulas are available for the arithmetic invariants (e.g., type number, class number, etc.) of orders in quaternion algebras and the dimensions of spaces of modular forms.

We begin with an example of theta series. Consider a maximal order $\mathcal{O}$ of $B_{p,\infty}$ given by the $\mathbb{Z}$-basis

$$e_1=\frac{1}{2}(1+j), e_2=\frac{1}{2}(i+k), e_3=j, e_4=k, \quad \text{if } p=3 \mod 4.$$

An element $\sum_{i=1}^4 x_ie_i=\frac{x_1}{2}+i(\frac{x_2}{2})+j(\frac{x_1}{2}+x_3)+k(\frac{x_2}{2}+x_4)$ has norm $(\frac{x_1}{2})^2+(\frac{x_2}{2})^2+p(\frac{x_1}{2}+x_3)^2+p(\frac{x_2}{2}+x_4)^2=(p+1)\Big((\frac{x_1}{2})^2+(\frac{x_2}{2})^2\Big)+p(x_3^2+x_4^2+x_1x_3+x_2x_4)$. Consider the order $\mathcal{O}\otimes\mathcal{O}_L$. Its norm form is the same norm form $N(x_1,x_2,x_3,x_4)$ but with values in $\mathcal{O}_L$. The associated theta series is defined as:

$$\theta(z)=a(0)+\sum_{\nu>>0}a(\nu)q^\nu, \quad a(\nu)=\sharp|\{N(x_1,x_2,x_3,x_4)=\nu, \text{ for } x_i\in\mathcal{O}_L\}|.$$

Of course, $a(0) = 1$. For $L = \mathbb{Q}(\sqrt{5})$ and $p >> 0$, we can easily compute the first coefficients a_1, say. We first use the fact that 1 is self-conjugate to eliminate the terms in $\sqrt{5}$ that arise form the norm form. Putting $x_i = \frac{a_i + b_i\sqrt{5}}{2}$, $i = 1, ..., 4$, and exploit the fact that the terms in p vanish for p big in the expression:

$$\sum_{j=1}^{2} \Big(\frac{a_j}{4}\Big)^2 + \Big(\frac{b_j\sqrt{5}}{4}\Big)^2 + p\sum_{j=1}^{2} \Big(\frac{a_j}{4} + \frac{a_{j+2}}{2}\Big)^2 + 5\Big(\frac{b_j}{4} + \frac{b_{j+2}}{2}\Big)^2.$$

We see that we need only solve $\frac{a_1^2}{16}+5\frac{b_1^2}{16}+\frac{a_2^2}{16}+5\frac{b_2^2}{16} = 1$. The solutions are $(a_1, b_1, a_2, b_2) = (\pm 4, 0, 0, 0)$ and $(a_1, b_1, a_2, b_2) = (0, 0, \pm 4, 0)$. Thus there are 4 solutions, and $a(1) = 4$.

In [102], one can find useful formulas concerning Eichler orders; we list a few. Let H/L be a totally ramified quaternion algebra over a totally real number field L of degree g, and let $\mathcal{O}$ be an Eichler order of squarefree level $\mathfrak{n}$. Let d be the discriminant of H.

Proposition 2.7.6. ([102, Cor. 2.3, p.142]) (Mass formula) Let d be the discriminant of the quaternion algebra H/L. Let $\mathcal{O}$ be an Eichler order of squarefree level $\mathfrak{n}$. Let $\{I_i\}$ be representatives of left ideal classes of $\mathcal{O}$. For $\mathcal{O}_i$ the right order of I_i, define $w_i := [\mathcal{O}_i^\times : \mathcal{O}_L^\times]$. The following holds:

$$\sum_{i=1}^{h} \frac{1}{w_i} = 2^{1-g} h |\zeta_L(-1)| \prod_{\mathfrak{p}|d} (\mathrm{Norm}(\mathfrak{p}) - 1) \prod_{\mathfrak{p}|\mathfrak{n}/d} (\mathrm{Norm}(\mathfrak{p}) + 1).$$

Remark 2.7.7. For a table of values of $\zeta_L(-1)$ for L of small discriminant, consult e.g., [37, p.373-374].

The number $M := \sum_{i=1}^{h} \frac{1}{w_i}$ is called the Mass of $\mathcal{O}$.

In general, the celebrated Siegel-Weil formula allows to show that a suitable weighted sum of theta series is an Eisenstein series (see [94, Introduction]). The sum of theta series is $\sum_{i=1}^{h} \frac{1}{w_i}\Theta_{\mathrm{Hom}_{\mathcal{O}_L}(A_1, A_i)}$, where $w_i = |[\mathrm{End}_{\mathcal{O}_L}(A_i)^\times : \mathcal{O}_L^\times]|$ and $\mathrm{Hom}_{\mathcal{O}_l}(A_1, A_i)$ runs through all projective $\mathrm{End}_{\mathcal{O}_L}(A_1)$-ideals. The first coefficient of the corresponding Eisenstein series is thus given by the Mass formula (cf. [29, Prop. 3.15]).

Definition 2.7.8. Let B be an order in a separable, quadratic algebra K/L contained in H. An **optimal embedding** of B in $\mathcal{O}$ is an isomorphism f of K into h such that $\mathcal{O} \cap f(K) = f(B)$.

Let m_i be the number of optimal embeddings of B in $\mathcal{O}_i$. The number $M(B) = \sum_{i=1}^{h} \frac{m_i}{w_i}$ is called the Mass of B. Define $w(B) := [B^\times : \mathcal{O}_L^\times]$.

Proposition 2.7.9. ([102, Cor. 2.5, p.144]) (Class number formula) Let $\mathcal{O}$ be an Eichler order. Recall that the number of left ideal classes of $\mathcal{O}$ is called the class number $h(\mathcal{O})$. It is given by the following formula:

$$h(\mathcal{O}) = M + \frac{1}{2} \sum_{B} M(B)(w(B) - 1),$$

where B runs through orders of quadratic extensions K/L.

Let (A) be a list of representatives of principal ideals of $\mathcal{O}_L$, representing all principal ideals that are reduced norms of two-sided ideals of $\mathcal{O}$, modulo squares of principal ideals.

Proposition 2.7.10. ([102, Cor. 2.6, p.145]) (Type number formula) Let $\mathcal{O}$ be an Eichler order of level $\mathfrak{n}$. Recall that the number of isomorphism classes of Eichler orders of level $\mathfrak{n}$ is called the type number $t(\mathcal{O})$. It is given by the following formula:

$$t(\mathcal{O}) = \frac{1}{h2^{r+1}} \sum_{B} M(B)w(B)x(B) + \frac{M}{h2^r},$$

where $x(B)$ is the number of principal ideals of B of reduced norm in (A). The orders in question run through orders of quadratic extensions K/L.

We give explicit formulas for the class number in some special cases.

Proposition 2.7.11. ([100, Thm. 3.1, 3.2]) Let p be unramified. Let $L = \mathbb{Q}(\sqrt{D})$. Let $\mathcal{O}$ be an Eichler of order p in $B_{p,L}$. The class number of $\mathcal{O}$ is given by the formula,

for $D > 5$:

$$\frac{Cl(\mathcal{O})}{h_L} = \frac{\zeta_L(-1)}{2} \prod_{\mathfrak{p}|d(B_{p,L})} (\mathrm{Norm}(\mathfrak{p}) - 1) \prod_{\mathfrak{p}|p/d(B_{p,L})} (\mathrm{Norm}(\mathfrak{p}) + 1)$$

$$+a(D)\frac{h(-D)}{8} + b(D)\frac{h(-3D)}{12} + c(D)\frac{h(n)h(n')}{4},$$

where $a(D), b(D), c(D)$ are integers that are defined as follows. Let

$$E_{d,p/d}(f) = \prod_{\mathfrak{p}|d(B_{p,L})} \left(1 - \left(\frac{O}{\mathfrak{p}}\right)\right) \cdot \prod_{\mathfrak{p}|p/d(B_{p,L})} \left(1 + \left(\frac{O}{\mathfrak{p}}\right)\right),$$

where O is an order in a quadratic extension of L, $f = f(O)$ is the conductor and $\left(\frac{O}{\mathfrak{p}}\right)$ is equal to 1 if $\mathfrak{p}$ divides $f(O)$ or $\mathfrak{p}$ is split in O; $\left(\frac{O}{\mathfrak{p}}\right)$ is equal to 0 is $\mathfrak{p}$ is ramified in O and -1 otherwise. The integers $a(D), b(D)$ and $c(D)$ are determined by the following relations:

$$S_2 = \frac{h(D)h(-D)}{8}a(m);$$

$$S_3 = \frac{h(D)h(-3D)}{12}b(m);$$

$$S_\epsilon = \frac{h(D)h(-n)h(-n')}{4}c(D),$$

where

$$S_2 = \frac{h(D)h(-D)}{8}[E_{d,p/d}(1) + 9E_{d,p/d}(2)];$$

$$S_3 = \frac{h(D)h(-3D)}{12}[5E_{d,p/d}(1) + 2bE_{d,p/d}(3) + cE_{d,p/d}(2)],$$

with $b = 4$ (resp. 2) if $m = 3 \mod 9$ (resp. if $m = 6 \mod 9$) and $c = 3$ if $m = 5 \mod 8$, 15 if $m = 1 \mod 8$ and 9 otherwise. We skip the definition of S_ϵ for brevity, but it is similar to the others. 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 $nn' = disc(\mathbb{Q}(\sqrt{D}))$.

We give a general formula for the dimension of the space of Hilbert modular forms for the sake of comparison.

Theorem 2.7.12. ([30, Thm. 4.8]) Let $\Gamma \subset \mathrm{SL}_2(\mathbb{R})^n$ be a discrete subgroup such that the extended quotient $\Gamma\backslash(\mathfrak{H}^n)^*$ is compact. We assume that the restriction of each of the n projections $p_j : \mathrm{SL}_2(\mathbb{R})^n \longrightarrow \mathrm{SL}_2(\mathbb{R}), 1 \leq j \leq n$ to Γ is injective. If $\Gamma\backslash\mathfrak{H}^n$ is compact, we assume that the image of Γ under each of the n projections: $\pi_j : \mathrm{SL}_2(\mathbb{R})^n \longrightarrow \mathrm{SL}_2(\mathbb{R})^{n-1}, 1 \leq i \leq n$, (cancelling off one component) is dense in $\mathrm{SL}_2(\mathbb{R})^{n-1}$. Then the following formula holds:

$$1 + (-1)^n \dim S_2(\Gamma) = (-1)^n \mathrm{vol}(\mathfrak{H}^n/\Gamma) + \sum_a E(\Gamma, a) + \sum_\kappa L(\Gamma, \kappa),$$

where a (resp. κ) runs over a complete set of representatives of Γ-equivalence classes of elliptic fixed points (resp. cusps). Here, $E(\Gamma, a)$ is some finite sum in terms of the stabilizer Γ_a that captures the contribution of elliptic fixed points, while $L(\Gamma, \kappa)$ is Shimizu L-series (for details, see [30, p. 121, p.109]).

Remark 2.7.13. We point out that the first term (although not necessarily the "main" term) of the formula giving the dimension of the space of Hilbert modular forms is precisely the volume $\mathrm{vol}(\mathfrak{H}^n/\Gamma)$. For $\Gamma = \mathrm{SL}_2(\mathcal{O}_L)$, the volume is $2^{1-g}(-1)^g\zeta_L(-1)$; thus the volume for $\Gamma_0(p)$ is precisely the index of $\Gamma_0(p)$ in $\mathrm{SL}_2(\mathcal{O}_L)$ times $2^{1-g}(-1)^g\zeta_L(-1)$.

Let $L = \mathbb{Q}(\sqrt{5})$. We find in [37, p. 373] that $\zeta_{\mathbb{Q}(\sqrt{5})}(-1) = \frac{1}{30}$. The numerical data we discuss in the rest of this section is taken from [19]. This is the real quadratic field of narrow class number one of smallest discriminant. According to [19], the smallest level p (p inert) such that the space of newforms is non-trivial is $p = 7$. The quaternion algebra $B_{p,\infty} \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{5}) = B_{\infty_1,\infty_2}$ is the totally definite quaternion algebra unramified at every finite prime. The class number of B_{∞_1,∞_2} is equal to one; therefore, the class number $h(\mathcal{O})$ of an Eichler order $\mathcal{O}$ of level p in B is roughly $p^2 + 1$. But there are $\frac{h(\mathcal{O})\cdot(h(\mathcal{O})+1)}{2}$ different quadratic modules $\mathrm{Hom}_{\mathcal{O}_L}(A_i, A_j)$, for A_i, A_j superspecial abelian varieties with RM by $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$. It will be clear to the reader that some computational effort would have to be exerted to illustrate our general theory satisfactorily beyond the simplest cases (cf. [40, §6] for examples over $\mathbb{Q}$).

2.8 The ramified case

The ramified case is more complex than the unramified case, since different superspecial points might have non-isomorphic superspecial crystals (see Appendix I), and in general the endomorphism orders are not hereditary. We explain in detail the simplest possible situation, and we give the essential results for the general totally ramified case. Let $g = 2$, and $p\mathcal{O}_L = \mathfrak{p}^2$. There are then two kinds of superspecial points (cf. [5]): those that satisfy the Rapoport condition (the non-singular superspecial points), and those that do not (the singular superspecial points). The abelian surface $E \otimes_{\mathbb{Z}} \mathcal{O}_L$ has non-singular type. In [1], it has been shown that $E \otimes_{\mathbb{Z}} \mathcal{O}_L$ admits a unique subgroup scheme $H \cong \alpha_p$ invariant under $\mathcal{O}_L$, and the quotient $(E \otimes_{\mathbb{Z}} \mathcal{O}_L)/H$ has singular type (the $\mathcal{O}_L$-structure and the principal polarization always descend). We compute the level of the endomorphism order of $(E \otimes_{\mathbb{Z}} \mathcal{O}_L)/H$. Recall that $\mathrm{End}_{\mathcal{O}_L}(E \otimes \mathcal{O}_L)$ has level $p = \mathfrak{p}^2$ and $B_{p,L} = B_{\infty_1,\infty_2}$.

Proposition 2.8.1. Let $A = E \otimes_{\mathbb{Z}} \mathcal{O}_L$, and let H be the unique $\mathcal{O}_L$-invariant copy of α_p in A. Then $\mathrm{End}_{\mathcal{O}_L}(A/H)$ has level $\mathfrak{p}$.

Before the proof *per se*, we need a few preliminaries. Since $p\mathcal{O}_L = \mathfrak{p}^2$, $\mathcal{O}_L \otimes \mathbb{F}_p \cong \mathbb{F}_p[\epsilon]/(\epsilon^2)$, and $H = \alpha_p \otimes (\epsilon)$ ([1, Prop. 6.5]). We denote A/H by B. The map $f : A \longrightarrow B$ is the projection map.

Lemma 2.8.2. Let $g \in \mathrm{End}_{\mathcal{O}_L}(A) \otimes \mathbb{Q}$. If g descends to an element in $\mathrm{End}_{\mathcal{O}_L}(B)$, then $pg \in \mathrm{End}_{\mathcal{O}_L}(A)$.

Proof. If g descends, then there exists $h \in \mathrm{End}(B)$ such that $g = \frac{1}{p}(pf^{-1}) \circ h \circ f$ i.e., $pg \in \mathrm{End}_{\mathcal{O}_L}(A)$.

□

In the sequel, we write H^1 for the first crystalline cohomology group H^1_{crys}.

Corollary 2.8.3. If $g \in \mathrm{End}_{\mathcal{O}_L}(A) \otimes \mathbb{Q}$, then $g \in \mathrm{End}_{\mathcal{O}_L}(B)$ if and only if either

- $g \in \mathrm{End}_{\mathcal{O}_L}(A)$ and g preserves $H^1(B)$;
- $g = g_0/p, g_0 \in \mathrm{End}_{\mathcal{O}_L}(A), p \not| g_0$, g preserves $H^1(B)$.

Proof. Clear, since $\mathrm{End}_{\mathcal{O}_L}(A)$ and $\mathrm{End}_{\mathcal{O}_L}(B)$ only differ at p, and there, it is controlled by $H^1(B)$ by Tate's theorem for supersingular abelian varieties with RM. □

We now prove Proposition 2.8.1.

Proof. Since $pH^1(A) \subseteq f^*(H^1(B)) \subseteq H^1(A)$, we can study the situation modulo p:

$$\frac{H^1(A)}{pH^1(A)} \cong \frac{H^1(E)}{pH^1(E)} \otimes \mathcal{O}_L,$$

as $\mathrm{End}(E) \otimes \mathcal{O}_L$-modules.
There exists a basis e_0, e_1 for $H^1(E)$ such that

$$\mathrm{End}(E) \otimes W(\mathbb{F}_p) = \left\{ \left(\begin{smallmatrix} a & b \\ pb^\sigma & a^\sigma \end{smallmatrix} \right) | a, b \in W(\mathbb{F}_{p^2}) \right\}, \ \sigma \text{ the non trivial involution.}$$

Recall that $H^1(E)/pH^1(E) = \mathbb{D}(E[p])$. For the following computations, it is easier to use *covariant* Dieudonné theory, so that an embedding $\alpha_p \hookrightarrow A$ becomes an inclusion $\mathbb{D}(\alpha_p) \subset \mathbb{D}(A)$. The condition that $H^1(B)$ is preserved means modulo p that the following filtration is preserved:

$$\langle \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix} \right) \rangle \otimes (\epsilon) \subseteq \mathbb{D}(\alpha_p) \otimes \mathcal{O}_L \subseteq \mathbb{D}(E[p]) \otimes \mathcal{O}_L.$$

We compute the divisibility conditions on the coefficients of g_0 so that g_0/p preserves $H^1(B)$. Since e_0, e_1 is a basis of $H^1(E)$, $e_0, \otimes 1, e_1 \otimes 1, e_0 \otimes \pi, e_1 \otimes \pi$ is a basis of $H^1(A)$, where π is a uniformizer of $W(\mathbb{F}_p) \otimes \mathcal{O}_L$. We thus write $g_0 = r_0 \otimes 1 + r_1 \otimes \pi$, where $r_i = \left(\begin{smallmatrix} a_i & b_i \\ pb^\sigma & a_i^\sigma \end{smallmatrix} \right)$, $i = 0, 1$. The element g_0/p preserves $H^1(B)$ if and only if

$$g_0 \left\{ \langle \left(\begin{smallmatrix} 1/p \\ 0 \end{smallmatrix} \right) \rangle \otimes (\pi) + H^1(A) \right\} \subseteq \ \langle \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix} \right) \rangle \otimes (\pi) + pH^1(A).$$

We decompose this in five subcases:

$$g_0(\langle \left(\begin{smallmatrix} 1/p \\ 0 \end{smallmatrix}\right) \rangle \otimes (\pi)) \subseteq \langle \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) \rangle \otimes (\pi) + pH^1(A);$$

$$g_0(e_0 \otimes 1) \in \langle \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) \rangle \otimes (\pi) + pH^1(A);$$

$$g_0(e_0 \otimes \pi) \in \langle \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) \rangle \otimes (\pi) + pH^1(A);$$

$$g_0(e_1 \otimes 1) \in \langle \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) \rangle \otimes (\pi) + pH^1(A);$$

$$g_0(e_1 \otimes \pi) \in \langle \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) \rangle \otimes (\pi) + pH^1(A).$$

Explicitly,

$$\left[\left(\begin{smallmatrix} a_0 & b_0 \\ pb_0^\sigma & a_0^\sigma \end{smallmatrix}\right) \otimes 1 + \left(\begin{smallmatrix} a_1 & b_1 \\ pb_1^\sigma & a_1^\sigma \end{smallmatrix}\right) \otimes (\pi)\right] \cdot (e_0 \otimes 1) = \left(\begin{smallmatrix} a_0 \\ pb_0^\sigma \end{smallmatrix}\right) \otimes 1 + \left(\begin{smallmatrix} a_1 \\ pb_1^\sigma \end{smallmatrix}\right) \otimes (\pi).$$

This forces p to divide a_0.

$$\left[\left(\begin{smallmatrix} a_0 & b_0 \\ pb_0^\sigma & a_0^\sigma \end{smallmatrix}\right) \otimes 1 + \left(\begin{smallmatrix} a_1 & b_1 \\ pb_1^\sigma & a_1^\sigma \end{smallmatrix}\right) \otimes (\pi)\right] \cdot (e_0 \otimes \pi) = \left(\begin{smallmatrix} a_0 \\ pb_0^\sigma \end{smallmatrix}\right) \otimes (\pi) + \left(\begin{smallmatrix} a_1 \\ pb_1^\sigma \end{smallmatrix}\right) \otimes (p)$$

This has no consequence.

$$\left[\left(\begin{smallmatrix} a_0 & b_0 \\ pb_0^\sigma & a_0^\sigma \end{smallmatrix}\right) \otimes 1 + \left(\begin{smallmatrix} a_1 & b_1 \\ pb_1^\sigma & a_1^\sigma \end{smallmatrix}\right) \otimes (\pi)\right] \cdot (e_1 \otimes 1) = \left(\begin{smallmatrix} b_0 \\ a_0^\sigma \end{smallmatrix}\right) \otimes 1 + \left(\begin{smallmatrix} b_1 \\ a_1^\sigma \end{smallmatrix}\right) \otimes (\pi)$$

This forces p to divide a_0, b_0, a_1.

$$\left[\left(\begin{smallmatrix} a_0 & b_0 \\ pb_0^\sigma & a_0^\sigma \end{smallmatrix}\right) \otimes 1 + \left(\begin{smallmatrix} a_1 & b_1 \\ pb_1^\sigma & a_1^\sigma \end{smallmatrix}\right) \otimes (\pi)\right] \cdot (e_1 \otimes \pi) = \left(\begin{smallmatrix} b_0 \\ a_0^\sigma \end{smallmatrix}\right) \otimes (\pi) + \left(\begin{smallmatrix} b_1 \\ a_1^\sigma \end{smallmatrix}\right) \otimes (p)$$

This forces p to divide a_0.

$$\left[\begin{pmatrix} a_0 & b_0 \\ pb_0^\sigma & a_0^\sigma \end{pmatrix} \otimes 1 + \begin{pmatrix} a_1 & b_1 \\ pb_1^\sigma & a_1^\sigma \end{pmatrix} \otimes (\pi)\right] \cdot \left[\langle \begin{pmatrix} 1/p \\ 0 \end{pmatrix} \rangle \otimes (\pi)\right] = \begin{pmatrix} a_0/p \\ b_0^\sigma \end{pmatrix} \otimes (\pi) + \begin{pmatrix} a_1/p \\ b_1^\sigma \end{pmatrix} \otimes (p)$$

We see from this implies that p divides a_0, a_1 and b_0. Note that this last line gives *redundant* information.

Summing up,

$$g_0/p = \frac{1}{p}\begin{pmatrix} a_0 & b_0 \\ pb_0^\sigma & a_0^\sigma \end{pmatrix} \otimes 1 + \frac{1}{p}\begin{pmatrix} a_1 & b_1 \\ pb_1^\sigma & a_1^\sigma \end{pmatrix} \otimes (\pi);$$

with $p|a_0, b_0, a_1$. We thus obtain a slightly bigger order than $\mathrm{End}(E) \otimes \mathcal{O}_L$ since p does not necessarily divide b_1. More precisely, $g_0/p = \begin{pmatrix} a_0' & b_0' \\ pa_0^\sigma & b_0^\sigma \end{pmatrix} \otimes 1 + \begin{pmatrix} a_1' & b_1/p \\ b_1^\sigma & a_1'^\sigma \end{pmatrix} \otimes \pi$, where all coefficients are in $W(\mathbb{F}_{p^2})$. To compute the level, we compute the index of this order over $\mathrm{End}(E) \otimes \mathcal{O}_L$. Recall that the level of $\mathrm{End}(E) \otimes \mathcal{O}_L$ is p. A priori, we know that the level of a strictly bigger order will divide p strictly, so in this case it will be either 1 or $\mathfrak{p}$. The quotient of $\mathrm{End}(E \otimes \mathcal{O}_L/H)$ over $\mathrm{End}(E) \otimes \mathcal{O}_L$ is $W(\mathbb{F}_{p^2})/pW(\mathbb{F}_{p^2}) \cong \mathbb{F}_{p^2}$, which is also the quotient of an order of level $\mathfrak{p}$ over an order of level $\mathfrak{p}^2$, since $\mathcal{O}_{L_\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{L_\mathfrak{p}} \cong \mathbb{F}_p$, and the residue degree of an unramified quadratic extension of $\mathcal{O}_{L_\mathfrak{p}}$ is 2. This shows that the discriminant of this bigger order is indeed $\mathfrak{p}$. □

Remark 2.8.4. Note that all the computations rely on the facts that if we normalize the valuation of p to be 1, the valuation of π is $\frac{1}{g}$.

We recalled the connection with de Rham cohomology and the descriptions of the slope stratification and the type (j, i) in Subsection 1.6 of Chapter I.

Theorem 2.8.5. Suppose that $p\mathcal{O}_L = \mathfrak{p}^g$. Let A be a superspecial abelian variety with RM by $\mathcal{O}_L$ of type (j, i), $i \geq j$. The order $\mathrm{End}_{\mathcal{O}_L}(A)$ is Bass of level $\mathfrak{p}^{g-j}$, where $j \leq [g/2]$. Moreover, we can give an explicit description at p of this order. Use the decomposition

$$(\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathcal{O}_L) \otimes W(\mathbb{F}_p) = \left\{ \oplus_{k=0}^{g-1} \begin{pmatrix} a_k & b_k \\ pb_k^\sigma & a_k^\sigma \end{pmatrix} \otimes (\pi^k), a_k, b_k \in W(\mathbb{F}_{p^2}) \right\},$$

and denote by M_k the set of matrices of the form $\begin{pmatrix} a_k & b_k/p \\ b_k^\sigma & a_k^\sigma \end{pmatrix}$, for $a_k, b_k \in W(\mathbb{F}_{p^2})$. then

$$\mathrm{End}_{\mathcal{O}_L}(A) \otimes W(\mathbb{F}_p) \cong \oplus_{k=0}^{i-1} \mathrm{End}(E) \otimes (\pi^k) \oplus \oplus_{k=i}^{g-1} M_k \otimes (\pi^k).$$

Remark 2.8.6. We explain later on that all such Bass orders of level $\mathfrak{p}^{g-j}, 0 \leq j \leq [g/2]$ (with the extra condition that $(\frac{\mathcal{O}}{\mathfrak{p}}) = (\frac{\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathcal{O}_L}{\mathfrak{p}})$ if $2 \leq g-j$), arise as endomorphism orders of superspecial abelian varieties on the Hilbert moduli space.

The ideas involved in the proof all arose in the $g = 2$ case. The structure of Moret-Bailly family of abelian varieties with RM ([1, Proposition 6.6, (2c) and (2d)]) indicates that there is a **canonical chain** of $\mathcal{O}_L$-invariant α_p-isogenies of superspecial abelian varieties starting from $E \otimes_{\mathbb{Z}} \mathcal{O}_L$:

- for g odd:

$$A = A_{0,g} \xrightarrow{\exists! \alpha_p} A_{1,g-1} \xrightarrow{\exists! \alpha_p} A_{2,g-2} \xrightarrow{\exists! \alpha_p} \ldots \xrightarrow{\exists! \alpha_p} A_{[g/2],[g/2]+1};$$

- for g even:

$$A = A_{0,g} \xrightarrow{\exists! \alpha_p} A_{1,g-1} \xrightarrow{\exists! \alpha_p} A_{2,g-2} \xrightarrow{\exists! \alpha_p} \ldots \xrightarrow{\exists! \alpha_p} A_{g/2,g/2},$$

  where the pair $(j,i), i+j=g$ is the type of the superspecial abelian variety.

All α_p-isogenies above are uniquely defined by being $\mathcal{O}_L$-invariant. The idea of the proof consists in bootstrapping the computation done for $g = 2$. Note that these supersingular abelian varieties are specific examples of superspecial points of type (j,i). It suffices to study this specific subset because (1) there is a unique superspecial crystal for every type (j,i), as shown in Chapter I (we also derived the result in the language of [1] in Appendix I) and (2) the Tate modules at $\ell \neq p$ are isomorphic (Proposition 2.5.3).

Lemma 2.8.7. Let $\mathcal{O}_L \otimes \mathbb{F}_p = \mathbb{F}_p[T]/(T^g)$. Let $A_{j,i}$ be a superspecial abelian variety of type (j,i) in a canonical chain. The $\mathcal{O}_L$-invariant α_p is isomorphic to $\alpha_p \otimes (T^{i-1})/(T^i)$ (cf. Section 4, Chapter *I*).

Proof. This is immediate from [1, Section 6.2, Table 6.1], where $r = i-1$ if $i \geq j+2$, which is verified for every abelian variety in a canonical chain (except the last one, which is not needed). □

We abuse the notation by writing $\alpha_p \otimes (T^{i-1})$ for the group scheme $\alpha_p \otimes (T^{i-1})/(T^i)$.

Lemma 2.8.8. If $g \in \mathrm{End}_{\mathcal{O}_L}(A_{j,i}) \otimes \mathbb{Q}$, then $g \in \mathrm{End}_{\mathcal{O}_L}(A_{j+1,i-1})$ if and only if either

- $g \in \mathrm{End}_{\mathcal{O}_L}(A_{j,i})$ and g preserves $H^1(A_{j+1,i-1})$;
- $g = g_0/p, g_0 \in \mathrm{End}_{\mathcal{O}_L}(A_{j,i})$, $p \nmid g_0$, g preserves $H^1(A_{j+1,i-1})$.

Proof. The proof of Lemma 2.8.3 applies without change. □

We now prove Theorem 2.8.5.

Proof. We proceed by induction on j. We have already shown in Proposition 2.5.26 that the level of the endomorphism order of $E \otimes \mathcal{O}_L$ is p. We explain the computation for the passage from type $(0, g)$ to type $(1, g-1)$. The divisibility conditions are given by:

$$g_0/p \left\{ \langle \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) \rangle \otimes (\pi^{g-1}) + pH^1(A) \right\} \subseteq \langle \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) \rangle \otimes (\pi^{g-1}) + pH^1(A),$$

for $g_0 = \oplus_{k=0}^{g-1} \left(\begin{smallmatrix} a_k & b_k \\ pb_k^\sigma & a_k^\sigma \end{smallmatrix}\right) \otimes (\pi^k) \in \mathrm{End}_{\mathcal{O}_L}(A_{0,g}) = \mathrm{End}_{\mathcal{O}_L}(A)$. As in the case $g = 2$, it is enough to check the divisibility conditions on the basis

$$e_0 \otimes 1, e_1 \otimes 1, \ldots, e_0 \otimes (\pi^{g-1}), e_1 \otimes (\pi^{g-1}).$$

First, necessarily

$$\frac{1}{p} \left(\begin{smallmatrix} a_0 & b_0 \\ pb_0^\sigma & a_0^\sigma \end{smallmatrix}\right) \otimes 1 \cdot \langle \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) \rangle \otimes (\pi^{g-1}) = \left(\begin{smallmatrix} a_0/p \\ b_0 \end{smallmatrix}\right) \otimes (\pi^{g-1}) \in \langle \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) \rangle \otimes (\pi^{g-1});$$

this implies that p divides a_0 and b_0. Second, necessarily

$$\left(\begin{smallmatrix} a_{g-1} & b_{g-1} \\ pb_{g-1}^\sigma & a_{g-1} \end{smallmatrix}\right) \otimes (\pi^{g-1}) \cdot e_0 \otimes 1 = \left(\begin{smallmatrix} a_{g-1} \\ pb_{g-1}^\sigma \end{smallmatrix}\right) \otimes (\pi^{g-1}) \in \langle \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) \rangle \otimes (\pi^{g-1}),$$

and

$$\begin{pmatrix} a_{g-1} & b_{g-1} \\ pb_{g-1}^{\sigma} & a_{g-1} \end{pmatrix} \otimes (\pi^{g-1}) \cdot e_1 \otimes 1 = \begin{pmatrix} b_{g-1} \\ a_{g-1}^{\sigma} \end{pmatrix} \otimes (\pi^{g-1}) \in \langle \begin{pmatrix} 1 \\ 0 \end{pmatrix} \rangle \otimes (\pi^{g-1});$$

therefore, we get that p divides a_{g-1} from the second vector. All other coefficients a_i, b_i, $0 < i < g-1$ are easily seen to be divisible by p, since the corresponding vectors all have to land in $pH^1(A)$. Now, suppose that we know $\mathrm{End}_{\mathcal{O}_L}(A_{g-i,i})$. The divisibility conditions are now given by:

$$g_0/p \left\{ \langle \begin{pmatrix} 1 \\ 0 \end{pmatrix} \rangle \otimes (\pi^{i-1}) + pH^1(A_{g-i,i}) \right\} \subseteq \langle \begin{pmatrix} 1 \\ 0 \end{pmatrix} \rangle \otimes (\pi^{i-1}) + pH^1(A_{g-i,i}),$$

or, in terms of $H^1(A)$,

$$g_0/p \left\{ \langle \begin{pmatrix} 1 \\ 0 \end{pmatrix} \rangle \otimes (\pi^{i-1}) + pH^1(A) \right\} \subseteq \sum_{t=i-1}^{g-1} \langle \begin{pmatrix} 1 \\ 0 \end{pmatrix} \rangle \otimes (\pi^{t}) + pH^1(A),$$

for $g_0 \in \mathrm{End}_{\mathcal{O}_L}(A_{g-i,i})$, that is,

$$g_0 = \oplus_{k=0}^{i-1} \begin{pmatrix} a_k & b_k \\ pb_k^{\sigma} & a_k^{\sigma} \end{pmatrix} \otimes (\pi^k) \oplus \oplus_{i}^{g-1} \begin{pmatrix} a_k & \frac{1}{p} b_k \\ b_k^{\sigma} & a_k^{\sigma} \end{pmatrix} \otimes (\pi^k).$$

Again, almost all coefficients will be divisible by p: p will divide all a_k's: since

$$\frac{1}{p} \begin{pmatrix} a_k & b_k \\ pb_k^{\sigma} & a_k^{\sigma} \end{pmatrix} \otimes (\pi^k) \cdot \langle \begin{pmatrix} 1 \\ 0 \end{pmatrix} \rangle \otimes (\pi^{i-1}) = \begin{pmatrix} a_k/p \\ b_k^{\sigma} \end{pmatrix} \otimes (\pi^{k+i-1}) \in \sum_{t=i-1}^{g-1} \langle \begin{pmatrix} 1 \\ 0 \end{pmatrix} \rangle \otimes (\pi^{t}),$$

then p divides a_k for $k = 0$ to $g - i$, and since

$$\frac{1}{p} \begin{pmatrix} a_k & b_k \\ pb_k^{\sigma} & a_k^{\sigma} \end{pmatrix} \otimes (\pi^k) \cdot \langle \begin{pmatrix} 1 \\ 0 \end{pmatrix} \rangle \otimes (\pi^{i-1}) = \begin{pmatrix} a_k \\ pb_k^{\sigma} \end{pmatrix} \otimes (\pi^{k+i-1-g}) \in pH^1(A),$$

then p divides a_k for $k = g - i + 1$ to $g - 1$. Let us show that b_{i-1} does not have to be divisible by p. Since $i \geq g - [g/2] + 1$, $2(i-1) \geq g$, and thus $\frac{1}{p} \begin{pmatrix} a_{i-1} & b_{i-1} \\ pb_{i-1}^{\sigma} & a_{i-1}^{\sigma} \end{pmatrix} \otimes (\pi^{i-1}) \cdot \langle \begin{pmatrix} 1 \\ 0 \end{pmatrix} \rangle \otimes (\pi^{i-1}) = \begin{pmatrix} a_{i-1} \\ pb_{i-1}^{\sigma} \end{pmatrix} \otimes (\pi^{2i-2-g}))$, and the term pb_{i-1}^{σ} will always be divisible by p. What about the other b_k's ? If $k < i - 1$, p divides b_k because necessarily

$$\begin{pmatrix} a_k & b_k \\ pb_k^{\sigma} & a_k^{\sigma} \end{pmatrix} \otimes (\pi^k) \cdot e_1 \otimes 1 = \begin{pmatrix} b_k \\ a_k^{\sigma} \end{pmatrix} \otimes (\pi^k) \in pH^1(A).$$

If $k > i-1$, the induction hypothesis shows that p has to divide b_k because

$$\begin{pmatrix} a_k & \frac{b_k}{p} \\ b_k^\sigma & a_k^\sigma \end{pmatrix} \otimes (\pi^k) \cdot e_0 \otimes 1 = \begin{pmatrix} a_k \\ b_k^\sigma \end{pmatrix} \otimes (\pi^k).$$

To finish the computation, recall that $g_0 \in \mathrm{End}_{\mathcal{O}_L}(A_{g-i,i})$, and therefore, as expected

$$g_0/p \in \oplus_{k=0}^{i-2} \mathrm{End}(E) \otimes (\pi^k) \oplus \oplus_{k=i-1}^{g-1} M_k \otimes (\pi^k).$$

To finish the proof, note the every type admits a unique isomorphism class of superspecial crystal: therefore all superspecial points of type (j,i) have Bass endomorphism orders of the same level. □

In the previous section, we relied heavily on the fact that for p unramified, the proof for supersingular elliptic curves generalizes without too much difficulty. On the other hand, the Jacquet-Langlands correspondence allows for more general levels (in particular, it applies to level p independently of the ramification). Recall that a superspecial order is hereditary if and only if p is unramified. In particular, since it is Bass, the discriminant $\mathfrak{p}^i$ of a given superspecial order is equal to its level, and thus the corresponding theta series also has level $\mathfrak{p}^i$.

Recall that the quadratic modules $\mathrm{Hom}_{\mathcal{O}_L}(A_1, A_2)$ are projective (Proposition 2.5.6) when the Dieudonné modules of A_1 and A_2 are isomorphic, which is the case if and only if A_1 and A_2 have the same Dieudonné module.

Proposition 2.8.9. The projective left ideals of a superspecial order $\mathcal{O}$ of $B_{p,L}$ of level $\mathfrak{p}^i$ are parametrized by the double cosets $B^1(\mathcal{O})\backslash J_B^1 / B^\times$.

Proof. This follows from the proof of the quaternionic parametrization of the locally principal left ideals which are therefore in bijection with the superspecial points of given type (j,i) by exactly the same argument as in the hereditary case. □

Corollary 2.8.10. All superspecial orders $\mathcal{O}$ of $B_{p,L}$ of level $\mathfrak{p}^i$ arise from geometry.

Proof. Since superspecial orders $\mathcal{O}$ of level $\mathfrak{p}^i$ are locally isomorphic (Proposition 2.2.28), the proof of Corollary 2.5.36 applies with no further modification. □

Recall that in the totally ramified case, $\mathfrak{p}$ is ramified in $B_{p,L}$ if and only if $[L:\mathbb{Q}]$ is odd.

Question 2.8.11. Let $h^+(L)=1$, $p\mathcal{O}_L=\mathfrak{p}^g$. Let $0\leq j\leq [g/2]$. If $[L:\mathbb{Q}]$ is odd, suppose that $g-j$ is odd. Do the theta series attached to superspecial points of type $(j,g-j)$ of the Hilbert moduli space $X_0(1)/\overline{\mathbb{F}}_p$ of dimension $[L:\mathbb{Q}]$ span the vector space of Hilbert modular newforms of level $\mathfrak{p}^{g-j}$?

Proposition 2.8.12. Let $h^+(L)=1$, $p\mathcal{O}_L=\mathfrak{p}^2$. The theta series attached to singular superspecial points of the Hilbert moduli space $X_0(1)/\overline{\mathbb{F}}_p$ of dimension $[L:\mathbb{Q}]$ span the vector space of Hilbert modular newforms of level $\mathfrak{p}$.

Proof. The order $\mathrm{End}_{\mathcal{O}_L}(A)$, for A a singular superspecial point, is Eichler. □

Recall that local deformation theory decomposes according to the primes, and that the *type* allows to label uniquely the isomorphism classes of superspecial crystals. We therefore conjecture that a similar pattern holds for general p and $g>2$ (i.e., all theta series "come from geometry", within the inescapable limits imposed by the Jacquet-Langlands correspondence and the levels arising on Hilbert moduli spaces).

2.9 Lifts of theta series and twists by $\mathrm{Aut}(\mathcal{O}_\mathrm{L})$

Tensoring supersingular elliptic curves with $\mathcal{O}_L$ enables us to lift elliptic modular forms of level p to Hilbert modular forms of level p: Let E_1,E_2 be supersingular elliptic curves, and let $(\mathrm{Hom}_{\mathbb{Z}}(E_1,E_2),q)$ be a quadratic module giving rise to an elliptic theta series θ_{E_1,E_2}. We associate to θ_{E_1,E_2} the theta series $\Theta_{E_1\otimes\mathcal{O}_L,E_2\otimes\mathcal{O}_L}$ coming from the quadratic module

$$(\mathrm{Hom}_{\mathcal{O}_L}(E_1\otimes\mathcal{O}_L,E_2\otimes\mathcal{O}_L),||-||_{\lambda_{E_1\otimes\mathcal{O}_L},\lambda_{E_2\otimes\mathcal{O}_L}}).$$

We also study the effect of changing the $\mathcal{O}_L$-action by an $\mathcal{O}_L$-automorphism. That is, let $\sigma : \mathcal{O}_L \longrightarrow \mathcal{O}_L$ be an automorphism. We then define the σ-twist of an $\mathcal{O}_L$-abelian variety (A, ι) by putting $\sigma \star (A, \iota) := (A, \iota \circ \sigma)$.

2.9.1 Comparing the lifts

The lift we are interested in takes an elliptic modular form for $\Gamma_0(p)$ with trivial character to Hilbert modular forms for $\Gamma_0((p))$ with trivial character. We call the lift obtained by tensoring supersingular elliptic curves by $\mathcal{O}_L$ the trivial lift. In fact, our first proposition justifies its name, by showing it has little to do with geometry. First, observe that Lemma 2.5.24 shows that

$$\mathrm{Hom}(E_1 \otimes_{\mathbb{Z}} \mathcal{O}_L, E_2 \otimes_{\mathbb{Z}} \mathcal{O}_L) \cong \mathcal{O}_L \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathbb{Z}}(E_1, E_2) \otimes_{\mathbb{Z}} \mathcal{O}_L^t.$$

This suggests the following $\mathcal{O}_L$-version:

Proposition 2.9.1.

$$\mathrm{Hom}_{\mathcal{O}_L}(E_1 \otimes \mathcal{O}_L, E_2 \otimes \mathcal{O}_L) \cong \mathrm{Hom}_{\mathbb{Z}}(E_1, E_2) \otimes_{\mathbb{Z}} \mathcal{O}_L.$$

Proof. Recall that Proposition 2.5.26 states that $\mathrm{End}_{\mathcal{O}_L}(E_i \otimes \mathcal{O}_L) \cong \mathrm{End}(E_i) \otimes \mathcal{O}_L$, for $i = 1, 2$. We know from the bijection between left ideal classes of

$$\mathcal{O} = \mathrm{End}_{\mathcal{O}_L}(E_1 \otimes_{\mathbb{Z}} \mathcal{O}_L)$$

and superspecial points that there exists an ideal $\mathfrak{A}$ such that

$$(E_1 \otimes \mathcal{O}_L) \otimes_{\mathcal{O}} \mathfrak{A} \cong E_2 \otimes \mathcal{O}_L.$$

Using these extra informations and Proposition 2.5.22, the isomorphism:

$$\mathrm{Hom}_{\mathcal{O}_L}(E_1 \otimes \mathcal{O}_L, E_2 \otimes \mathcal{O}_L) \cong \mathrm{Hom}_{\mathbb{Z}}(E_1, E_2) \otimes_{\mathbb{Z}} \mathcal{O}_L,$$

is recast via

$$\mathrm{Hom}_{\mathcal{O}_L}(E_1 \otimes_{\mathbb{Z}} \mathcal{O}_L, E_1 \otimes_{\mathbb{Z}} \mathcal{O}_L) \otimes_{\mathrm{End}(E_1)\otimes\mathcal{O}_L} \mathfrak{A} \cong \mathrm{Hom}_{\mathbb{Z}}(E_1, E_2) \otimes_{\mathbb{Z}} \mathcal{O}_L$$

as

$$\mathfrak{A} \cong \mathrm{Hom}_{\mathbb{Z}}(E_1, E_2) \otimes_{\mathbb{Z}} \mathcal{O}_L.$$

Thus, to prove the desired isomorphism, it is enough to show that:

$$(E_1 \otimes_{\mathbb{Z}} \mathcal{O}_L) \otimes_{\mathrm{End}(E_1)\otimes_{\mathbb{Z}}\mathcal{O}_L} (\mathrm{Hom}_{\mathbb{Z}}(E_1, E_2) \otimes \mathcal{O}_L) \cong E_2 \otimes \mathcal{O}_L.$$

This, in turn, is proved by general properties of the tensor product. The universal property of the tensor product shows that for M_1, N_1 two R_1-modules, M_2, N_2 two R_2-modules, and R_1, R_2 two R_0-algebras, R_0 a commutative ring, the following isomorphism holds:

$$(M_1 \otimes_{R_1} N_1) \otimes_{R_0} (M_2 \otimes_{R_2} N_2) \cong (M_1 \otimes_{R_0} M_2) \otimes_{R_1\otimes_{R_0}R_2} (N_1 \otimes_{R_0} N_2).$$

In our specific case, this becomes:

$$\begin{aligned}(E_1 \otimes \mathcal{O}_L) \otimes_{\mathrm{End}(E_1\otimes_{\mathbb{Z}}\mathcal{O}_L)} (\mathrm{Hom}(E_1, E_2) \otimes \mathcal{O}_L) &\cong (E_1 \otimes \mathrm{Hom}_{\mathbb{Z}}(E_1, E_2)) \otimes_{\mathbb{Z}} \mathcal{O}_L \\ &\cong E_2 \otimes \mathcal{O}_L,\end{aligned}$$

since $E_1 \otimes \mathrm{Hom}_{\mathbb{Z}}(E_1, E_2) \cong E_2$.

□

Thus, the trivial lift amounts to tensoring left ideals of $B_{p,\infty}$ with $\mathcal{O}_L$. This extends to the quadratic modules, since the natural quadratic map on $\mathrm{Hom}_{\mathcal{O}_L}(E_1\otimes\mathcal{O}_L, E_2\otimes\mathcal{O}_L)$ i.e., the degree map on $\mathrm{Hom}_{\mathbb{Z}}(E_1, E_2)$ tensored with $\mathcal{O}_L$ is always the same as the $\mathcal{O}_L$-degree (as it is clear from the $E_1 = E_2$ case).

Corollary 2.9.2. The number of isomorphism classes of quadratic modules of the form $\mathrm{Hom}_{\mathcal{O}_L}(E_1 \otimes \mathcal{O}_L, E_2 \otimes \mathcal{O}_L)$ is equal to the number of isomorphism classes of quadratic modules of the form $\mathrm{Hom}_{\mathbb{Z}}(E_1, E_2)$.

Proof. This follows from a general theorem of Kitaoka ([56, Theorem 7.5.1]) about tensoring with the maximal order of a totally real field, which says that

$$\mathfrak{A}_1 \otimes \mathcal{O}_L \cong \mathfrak{A}_2 \otimes \mathcal{O}_L \text{ implies } \mathfrak{A}_1 \cong \mathfrak{A}_2,$$

for $\mathfrak{A}_1, \mathfrak{A}_2$ two positive definite quadratic lattices over $\mathbb{Z}$. □

Question 2.9.3. Does the trivial lift coincide with the base change lift à la Langlands ([63]) when the latter is defined?

The answer to this question is surely well-known to base change experts, and we guess it is yes.
We investigate symmetric forms in the next section.

2.9.2 Automorphisms of $\mathcal{O}_L$ and theta series

In this section, we take a look at the twist of the $\mathcal{O}_L$-action by an automorphism $\sigma : \mathcal{O}_L \longrightarrow \mathcal{O}_L$. Recall that the σ-twist of an $\mathcal{O}_L$-abelian variety (A, ι) is $\sigma \star (A, \iota) := (A, \iota \circ \sigma)$.

Proposition 2.9.4. The $\mathcal{O}_L$-modules $\mathrm{Hom}_{\mathcal{O}_L}(A_1, A_2)$ and $\mathrm{Hom}_{\mathcal{O}_L}(\sigma \star A_1, \sigma \star A_2)$ are canonically isomorphic as quadratic modules.

Proof. Note that $\mathrm{Hom}_{\mathcal{O}_L}(\sigma \star A_1, \sigma \star A_2) = \mathrm{Hom}_{\sigma(\mathcal{O}_L)}(A_1, A_2)$. We consider the identity map sending $\phi \in \mathrm{Hom}_{\mathcal{O}_L}(A_1, A_2)$ to $\phi \in \mathrm{Hom}_{\sigma(\mathcal{O}_L)}(A_1, A_2)$. We check it is well-defined: Note that

$$\phi(\iota_1(\mathfrak{t})(x)) = \iota_2(\mathfrak{t})(\phi(x))$$

for all $\mathfrak{t} \in \mathcal{O}_L$ and $x \in A_1$ is equivalent to

$$\phi((\iota_1 \circ \sigma)(\mathfrak{t})(x)) = (\iota_2 \circ \sigma)(\mathfrak{t})(\phi(x))$$

for any $\sigma \in \mathrm{Aut}(\mathcal{O}_L)$. This shows that $\mathrm{Hom}_{\mathcal{O}_L}(A_1, A_2) = \mathrm{Hom}_{\sigma(\mathcal{O}_L)}(A_1, A_2)$. We check that the polarizations λ_1, λ_2 of A_1, A_2 are also polarizations of $\sigma \star A_1$, $\sigma \star A_2$: this is an immediate consequence of the identity

$$\iota^t \circ \sigma = (\iota \circ \sigma)^t,$$

which follows trivially from the definition of the dual action ι^t, that is $\iota^t(\mathfrak{t}) = (\iota(\mathfrak{t}))^t$. Since the polarizations are the same, the induced $\mathcal{O}_L$-degrees also coincide, and therefore the quadratic modules are canonically isomorphic. □

This suggests looking at the quadratic modules $\mathrm{Hom}_{\mathcal{O}_L}(\sigma_i \star A_1, \sigma_j \star A_2)$ for different $\mathcal{O}_L$-automorphisms σ_i, σ_j, and study the effect on the coefficients of the q-expansions of the corresponding theta series.

Definition 2.9.5. An order $\mathcal{O}$ in a quaternion algebra $B = B_{p,\infty} \otimes L$ is called **totally (weakly) symmetric** or simply **symmetric** if for any $\sigma \in \mathrm{Aut}(L/\mathbb{Q})$ there exist an extension $\overline{\sigma}$ such that

$$\mathcal{O}^{\overline{\sigma}} = C^{-1}\mathcal{O}C,$$

with some $C \in B^\times$ i.e., $\mathcal{O}^{\overline{\sigma}}$ and $\mathcal{O}$ are conjugate.

Remark 2.9.6. In general, there would be infinitely many extensions of an automorphism of L to an automorphism (of the same order) of a quaternion algebra $B \otimes L$, for B a quaternion algebra over $\mathbb{Q}$.

Proposition 2.9.7. Let E be a supersingular elliptic curve. The endomorphism order $\mathrm{End}_{\mathcal{O}_L}(E \otimes \mathcal{O}_L)$ is symmetric.

Proof. Let $\sigma = 1 \otimes \sigma_0$ be the extension of an $\mathcal{O}_L$-automorphism σ_0. Note that it fixes

$\mathrm{End}(E)$.

$$\begin{aligned}(\mathrm{End}_{\mathcal{O}_L}(E\otimes\mathcal{O}_L))^\sigma &\cong (\mathrm{End}_{\mathbb{Z}}(E)\otimes\mathcal{O}_L)^\sigma\\ &\cong \mathrm{End}_{\mathbb{Z}}(E)\otimes\sigma(\mathcal{O}_L)\\ &\cong \mathrm{End}_{\mathbb{Z}}(E)\otimes_{\mathbb{Z}}\mathcal{O}_L\\ &\cong \mathrm{End}_{\mathcal{O}_L}(E\otimes_{\mathbb{Z}}\mathcal{O}_L).\end{aligned}$$

□

Corollary 2.9.8. The theta series $\Theta_{\mathrm{Hom}_{\mathcal{O}_L}(E_1\otimes\mathcal{O}_L,E_2\otimes\mathcal{O}_L)}$ is symmetric.

Proof. This theta series is defined in terms of a projective ideal of the symmetric order $\mathrm{End}_{\mathcal{O}_L}(E_1\otimes\mathcal{O}_L)$, hence necessarily has symmetric coefficients. □

2.10 Appendix I: The number of superspecial crystals in the totally ramified case is $[g/2]+1$

We present a derivation of the classification theorem for superspecial crystal with RM in the totally ramified setting on the lines of [1] so that the reader interested in the ramified case of Eichler's Basis Problem can skip Chapter I of this thesis. The result that we need gives a certain normal form for the Frobenius, and a tiny computation involving σ-algebra yields the result. We prove this by exhibiting a canonical form for the Frobenius operator of the associated display. Recall that L is a totally real field of degree g over $\mathbb{Q}$, $p\in\mathbb{Z}$ such that $p=\mathfrak{p}^g$ is totally ramified in $\mathcal{O}_L$.

Lemma 2.10.1. A non-constant σ-linear equation in one variable with coefficients in $\mathcal{O}_L\otimes_{\mathbb{Z}}W(k)$ with $k=\overline{k}$ of characteristic p always has a solution.

Proof. This is a standard trick of reducing the problem to solving successive polynomials over k: reduction mod T gives a polynomial which has a solution, k being

algebraically closed. Now suppose we have a solution $x_n \mod T^n$ i.e., $p(x_n) = T^n \cdot c$, $c \in \mathcal{O}_L \otimes W(k)$. Put $x_{n+1} - x_n = T^n y$, and plug x_{n+1} in $p(X) \mod T^{n+1}$:

$$p(x_n + T^n y) = p(x_n) + T^n p(y) = T^n \cdot c + T^n p(y) \mod T^{n+1},$$

hence we have to find a solution to $p(y) + c = 0 \mod T$, which is always possible, thence we have a solution $x_{n+1} \mod T^{n+1}$ and we are done by induction.

□

Proposition 2.10.2. Let D be a principally polarized superspecial display

$$(P, Q, F, V^{-1}),$$

of type (i, j) over an algebraically closed field k of characteristic p. There exists a basis α', β' generating P such that Frobenius is given by :

$$F = \begin{pmatrix} 0 & T^i \\ T^j & 0 \end{pmatrix}.$$

Proof. According to [1, Proposition 4.3.1], the display can be given in a normal form as follows : there exists α, β such that $P \cong (\mathcal{O}_L \otimes W(k))\alpha \oplus (\mathcal{O}_L \otimes W(k))\beta$ such that Frobenius is given by :

$$F = \begin{pmatrix} T^m & c_3 T^i \\ T^j & 0 \end{pmatrix},$$

where $i + j = g, 0 \leq j \leq \frac{g}{2}, m \geq i$ and $c_3 \in (\mathcal{O}_L \otimes W(k))^\times$.

- Step 1. Suppose $i > j$.

  First observe that in this case the requirement on the determinant of the change of basis matrix is given by $AA^\sigma \neq 0 \mod T$, e.g. A is a unit in $\mathcal{O}_L \otimes W(k)$.

  Put $\alpha' = A\alpha + B\beta$, for $A, B \in \mathcal{O}_L \otimes W(k)$.

We compute $F(\alpha')$ in order to get the formula expressing β' in terms of α and β.

$$F(\alpha') = A^{\alpha}F(\alpha) + B^{\alpha}F(\beta) = A^{\sigma}(T^m\alpha + T^j\beta) + B^{\sigma}c_3T^i\alpha,$$

and on the other hand

$$F(\alpha') = T^j\beta';$$

thence, since $m \geq i > j$,

$$\beta' = (A^{\sigma}T^{m-j} + B^{\sigma}c_3T^{i-j})\alpha + A^{\sigma}\beta.$$

We now compute $F(\beta')$:

$$T^jF(\beta') = (A^{\sigma^2}T^m + B^{\sigma^2}c_3^{\sigma}T^i)(T^m\alpha + T^j\beta) + A^{\sigma^2}c_3T^g\alpha$$

$$= (A^{\sigma^2}T^{2m} + B^{\sigma^2}c_3^{\sigma}T^{i+m} + A^{\sigma^2}c_3T^g)\alpha + (A^{\sigma^2}T^{m+j} + B^{\sigma^2}c_3^{\sigma}T^g)\beta,$$

and on the other hand

$$T^jF(\beta') = T^g\alpha' = T^g(A\alpha + B\beta);$$

thence we get the following system of equations :

$$B = A^{\sigma^2}T^{m+j-g} + B^{\sigma^2}c_3^{\sigma}; \tag{2.10.1}$$

$$A = A^{\sigma^2}T^{2m-g} + B^{\sigma^2}c_3^{\sigma}T^{i+m-g} + A^{\sigma^2}c_3; \tag{2.10.2}$$

and the determinant condition insuring the change of basis is invertible :

$$\det\begin{pmatrix} A & B \\ A^{\sigma}T^{m-j} + B^{\sigma}c_3T^{i-j} & A^{\sigma} \end{pmatrix} \in (\mathcal{O}_L \otimes W(k))^{\times}.$$

We multiply Equation 2.10.1 by T^{m-j} and subtract Equation 2.10.2 to obtain

$$BT^{m-j} - A = -A^{\sigma^2}c_3.$$

We plug this expression for B in Equation 2.10.2; this yields one equation:

$$A^{\sigma^2}T^{2m-g} - A^{\sigma^4}c_3^{\sigma^2}c_3^{\sigma} + A^{\sigma^2}c_3^{\sigma} + A^{\sigma^2}c_3 - A = 0. \tag{2.10.3}$$

According to Lemma 2.10.1, this equation has a solution. Let us verify that it is possible to pick a unit among all such solutions. The reduction mod T of the Equation 2.10.3 is :

$$-a^{p^4}c^{p^2}c^p + a^{p^2}c^p + a^{p^2}c - a = 0,$$

where $c = \overline{c_3}$.

The degree of this polynomial is clearly greater than one and we can thus pick $a \neq 0$, hence we obtain a unit solution for A.

- Step 2. Suppose $i = j$.

  Recall that under p-isogenies, we can map any superspecial point to any other superspecial point. Our strategy is simple : we start from a point of type $(j-1, j+1)$ and map it to a point of type (j, j), and see how Frobenius vary.

  We use the Moret-Bailly families described in [1, Proposition 6.8,2.d], since $j+1-(j-1) = 2$, hence $[\mathcal{A}_{(0:1)}] \in \mathfrak{M}_{(j,j)}$. We describe the map at the level of crystals : let (P, Q, F, V^{-1}) be the superspecial of type $(j-1, j+1)$, given in a canonical form as in the first step of this proof, explicitly :

$$P = \mathcal{O}_L \otimes W(k)\alpha \oplus \mathcal{O}_L \otimes W(k)\beta,$$

$$Q = \mathcal{O}_L \otimes W(k)T^{j+1}\alpha \oplus \mathcal{O}_L \otimes W(k)T^{j-1}\beta,$$

$$F = \begin{pmatrix} 0 & T^{j+1} \\ T^{j-1} & 0 \end{pmatrix}.$$

The superspecial crystal of type (j, j) is constructed as follows ([1, Definition 6.1]) :

$$P_\gamma := \frac{1}{p}W(k)\gamma + P \text{ where } Q \ni \gamma := T^{g-1}\beta,$$

and

$$Q_\gamma := Q + F^{-1}(W(k)\gamma).$$

Explicitly, this yields :

$$P_\gamma = \mathcal{O}_L \otimes W(k)\alpha \oplus \mathcal{O}_L \otimes W(k)\frac{\beta}{T},$$

and

$$Q_\gamma = \mathcal{O}_L \otimes W(k)T^j \oplus \mathcal{O}_L \otimes W(k)T^{j-1}\beta,$$

and in the basis $\alpha' = \alpha, \beta' = \frac{\beta}{T}$, Frobenius is given by :

$$F = \begin{pmatrix} 0 & T^j \\ T^j & 0 \end{pmatrix}.$$

□

Proposition 2.10.3. The local deformation theory is the same at any superspecial point of given type on a Hilbert modular variety over a totally ramified prime.

Proof. Since for every type (i, j), there is a unique principally polarized superspecial crystal associated to it, the statement follows from Zink's theorem (cf [1, Theorem 4.1.7]). □

Conclusion

The exploration of the generalization of the superspecial locus for general Shimura varieties offers many opportunities for interesting work: generalizing the Picard-Lefschetz formula à la Grothendieck, the character group, and Ribet's Exact Sequence, using the powerful tool of p-adic uniformization of [83] which enables us to get our hands on the relevant strata for a wide class of Shimura varieties (thus including cases of bad reduction). Moreover, p-adically uniformized varieties and the simple Shimura varieties of Harris-Taylor satisfy the weight-monodromy conjecture of Deligne (see [51]). More concretely, we can put our hand on the superspecial locus of a certain quaternionic Shimura variety of dimension g coming from the totally indefinite quaternion algebra over L ramified at the finite ramified primes of $B_{p,L}$ and at the primes $\mathfrak{q}_i$ dividing a totally split prime q, and we can show that the superspecial locus of the Hilbert modular variety is in bijection with the superspecial locus of that quaternionic Shimura variety. By varying the splitness of q, we get quaternionic Shimura varieties of dimension between 1 and g; except for the example we have just discussed, these are not of P.E.L. type, but their geometry has been thoroughly investigated by H. Reimann. It would be interesting to investigate this circle of ideas for a Shimura variety with non-trivial endoscopy. Moreover, the stratification of moduli spaces of abelian varieties with additional structure that we are suggesting, which essentially consists of associating its special Dieudonné module to an abelian variety with additional structure, could be generalized beyond the Hilbert moduli spaces that

we studied (say, to Hilbert moduli spaces with $\Gamma_0(p)$-level structure). As mentioned in the introduction, we did not investigate the geometric interpretation of the type number. Any principally polarized superspecial abelian variety with RM is defined over $\mathbb{F}_{p^2}$. We expect that the number of superspecial points defined over $\mathbb{F}_p$ should be given by a very simple formula in terms of the class number and the type number.

Let p be unramified. We have shown that the space of Hilbert modular newforms of weight 2 of level p can be spanned by theta series coming from superspecial abelian varieties with RM by relying on the fact that the endomorphism order $\mathrm{End}_{\mathcal{O}_L}(A)$ of A, a superspecial abelian variety with RM, is an Eichler order of level p and the related description of the superspecial locus of the Hilbert moduli space by suitable double cosets. On the other hand, the exploration of the ramified case is not complete, since we could not describe yet the span of the theta series (note that we also left the realm of special orders à la Hijikata-Pizer-Shemanske). The issue is that the Jacquet-Langlands correspondence in its current form deals with greatest ease with Eichler orders. It is not clear what is the most general class of orders for which we get the usual solution to Eichler's Basis Problem, and how we could apply directly the Jacquet-Langlands correspondence in all known cases.

This thesis also offers the opportunity to revisit [40] for Hilbert modular forms (see [114]) or to investigate the integral version of Eichler's Basis Theorem via geometric methods (see [29], [46]).

Also, Eichler proved additional results about symmetric modular forms whose generalization has not been investigated e.g., we expect that the number of linearly independent symmetric Hilbert modular forms of level $p\mathcal{O}_L$ and weight 2 is equal to the number of symmetric Eichler orders of level $p\mathcal{O}_L$ (for un ramified p).

On the other hand, the Main Theorem of this thesis begs to be improved. It is indeed an easy matter to adapt the argument to deal with $\Gamma_0(Np)$, $(N,p)=1$. What is not clear to us is how to tackle weights higher than 2 geometrically i.e., to find a

interpretation of spherical polynomials in terms of Hilbert modular data. It is also not so clear to us how hard it would be to avoid the restriction on the narrow class number of L, which has quite a simplifying effect. It is possible that a geometric proof of the Main Theorem using vanishing cycles along the lines of Mestre-Oesterlé graph method could work for an arbitrary L.

Bibliography

[1] Andreatta, F., Goren, E.Z., Geometry of Hilbert Modular Varieties over Totally Ramified Primes, *Int. Math. Res. Not.* 2003, no. **33**, 1786–1835.

[2] Andreatta, F., Goren, E.Z., Hilbert modular varieties of low dimension. *Geometric aspects of Dwork theory.* Vol. **I**, 113–175, Walter de Gruyter, Berlin, 2004.

[3] Arbarello, E.; Cornalba, M.; Griffiths, P. A.; Harris, J., *Geometry of algebraic curves.* Vol. I. Grundlehren der Mathematischen Wissenschaften, **267**. Springer-Verlag, New York, 1985.

[4] Asai, T., On certain Dirichlet series associated with Hilbert modular forms and Rankin's method. *Math. Ann.* **226** (1977), no. 1, 81–94.

[5] Bachmat, E.; Goren, E.Z., On the non-ordinary locus in Hilbert-Blumenthal surfaces. *Math. Ann.* **313** (1999), no. 3, 475–506.

[6] Brzeziński, J., On orders in quaternion algebras. *Comm. Algebra*, **11**, (1983), no. 5, 501–522.

[7] Brzeziński, J., Spinor class groups of orders. *J. Algebra*, **84**, (1983), no. 2, 468–481.

[8] Brzeziński, J., On automorphisms of quaternion orders. *J. Reine Angew. Math.*, **403**, (1990), 166–186.

[9] Brzeziński, J., Eichler, M., On the imbeddings of imaginary quadratic orders in definite quaternion orders. *J. Reine Angew. Math.*, **426**, (1992), 91–105.

[10] Cassels, J.W.S., *Rational quadratic forms*, London Mathematical Society Monographs, **13**. Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], London-New York, 1978. xvi+413 pp.

[11] Chai, C.-L., Every ordinary symplectic isogeny class in positive characteristic is dense in the moduli. *Invent. Math.*, **121**, (1995), no. 3, 439–479.

[12] Chai, C.-L., Monodromy of Hecke-invariant subvarieties, preprint, version of 25/04/2003. *http* : *//www.math.upenn.edu/* $\sim$ *chai/*

[13] Chai, C.-L., Hecke Orbits on Siegel Modular Varieties, version 8/20/2004. *http* : *//www.math.upenn.edu/* $\sim$ *chai/*

[14] Conrad, B., Gross-Zagier revisited. With an appendix by W.R. Mann., Math. Sci. Res. Inst. Publ., **49**, *Heegner points and Rankin L-series*, 67–163, Cambridge Univ. Press, Cambridge, 2004.

[15] Consani, K., Scholten, J., Arithmetic on a quintic threefold. *Internat. J. Math.*, **12**, (2001), no. 8, 943–972.

[16] Cornut, C., *Réduction de familles de points CM*, thèse de doctorat, Université de Strasbourg, 2000.

[17] 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

[18] Demazure, M., *Lectures on p-divisible groups.* Lecture Notes in Mathematics, Vol. **302**. Springer-Verlag, Berlin-New York, 1972.

[19] Dembelé, L., Explicit computations of Hilbert modular forms on $\mathbb{Q}(\sqrt{5})$, Ph.D. thesis, McGill University, 2002.

[20] Deuring, M., Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, *Abh. Math. Sem. Hansischen Univ.*, **14**, (1941), 197–272.

[21] Deuring, M., *Algebren.* Zweite, korrigierte auflage. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band **41**, Springer-Verlag, Berlin-New York, 1968.

[22] Eichler, M., Untersuchungen in der Zahlentheorie der rationalen Quaternionenalgebren, *J. reine angew. Math.*, **174**, (1936), 129-159.

[23] Eichler, M., Allgemeine Kongruenzklasseneinteilungen der Ideale einfacher Algebren über algebraischen Zahlkörpern und ihre L-Reihen, *J. reine Angew. Math.*, **179**, (1938), 227-251.

[24] Eichler, M., On theta functions of real algebraic number fields. *Acta Arith.* **33** (1977), no. 3, 269–292.

[25] Eichler, M., Theta functions over $\mathbb{Q}$ and over $\mathbb{Q}(\sqrt{q})$, *Modular functions of one variable, VI* (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), pp. 197 − −225. Lecture Notes in Math., Vol. **627**, Springer, Berlin, 1977.

[26] Eichler, M., On symmetric and unsymmetric theta functions over a real quadratic field. *Acta Arith.*, **37**, (1980), 167–179.

[27] Elkies, N., Ono, K., Yang, T., Reduction of CM elliptic curves and modular function congruences, preprint 2005.

[28] Ellenberg, J., *Hilbert modular forms and the Galois representations associated to Hilbert-Blumenthal abelian varieties*, Ph.D. thesis, Harvard University, 1998.

[29] Emerton, M., Supersingular elliptic curves, theta series and weight two modular forms. *J. Amer. Math. Soc.*, **15**, (2002), no. 3, 671–714.

[30] Freitag, E., *Hilbert modular forms.* Springer-Verlag, Berlin, 1990.

[31] van der Geer, G., Katsura, T., An invariant for varieties in positive characteristic. *Algebraic number theory and algebraic geometry*, 131–141, Contemp. Math., **300**, Amer. Math. Soc., Providence, RI, 2002.

[32] van der Geer, G., Cycles on the moduli space of abelian varieties. *Moduli of curves and abelian varieties*, 65–89, Aspects Math., **E33**, Vieweg, Braunschweig, 1999.

[33] Gelbart, S., *Automorphic forms on adèle groups.* Annals of Mathematics Studies, No. **83**. Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1975.

[34] Gelbart, S. *Lectures on the Arthur-Selberg trace formula.* University Lecture Series, **9.** American Mathematical Society, Providence, RI, 1996.

[35] Ghate, E., Congruences between base-change and non-base-change Hilbert modular forms. *Cohomology of arithmetic groups, L-functions and automorphic forms (Mumbai, 1998/1999)*, 35–62, Tata Inst. Fund. Res. Stud. Math., **15**, Tata Inst. Fund. Res., Bombay, 2001.

[36] Goren, E.Z., Oort, F., Stratifications of Hilbert modular varieties. *J. Algebraic Geom.* **9** (2000), no. 1, 111–154.

[37] Goren, E.Z. Hilbert modular forms modulo p^m: the unramified case. *J. Number Theory* **90** (2001), no. 2, 341–375.

[38] 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.

[39] Goren, E.Z., *Lectures on Hilbert modular varieties and modular forms.* With the assistance of Marc-Hubert Nicole. CRM Monograph Series, **14**. American Mathematical Society, Providence, RI, 2002.

[40] 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.

[41] Grothendieck, A., *Groupes de Barsotti-Tate et cristaux de Dieudonné*, Séminaire de Mathématiques Supérieures, No. **45**, 1970. Les Presses de l'Université de Montréal, Montréal, Qué., 1974.

[42] *Groupes de monodromie en géométrie algébrique. I.* Séminaire de Géométrie Algébrique du Bois-Marie, 1967–1969 (SGA 7 I). Dirigé par A. Grothendieck. Avec la collaboration de M. Raynaud et D. S. Rim. Lecture Notes in Mathematics, Vol. **288**. Springer-Verlag, Berlin-New York, 1972.

[43] Harashita, S., *Moduli of supersingular abelian varieties with endomorphism structure*, University of Tokyo, M.Sc. thesis, 2002.

[44] Harashita, S., Geometrical structure and number theory on supersingular logic with endomorphism structure. Young philosophers in number theory (Kyoto, 2001). Sūrikaisekikenkyūsho Kōkyūroku No. 1256, (2002), 131–160.

[45] Hazewinkel, M. Twisted Lubin-Tate formal group laws, ramified Witt vectors and (ramified) Artin-Hasse exponentials. *Trans. Amer. Math. Soc.* **259** (1980), no. 1, 47–63.

[46] Hida, H., The integral basis problem of Eichler, *I.M.R.N.*,**34**, 2005, 2101-2122.

[47] Hida, H., Anticyclotomic main conjectures, preprint, 2004. *http* : *//www.math.ucla.edu/* $\sim$ *hida/*

[48] Hida, H., *p-adic automorphic forms on Shimura varieties.* Springer Monographs in Mathematics. Springer-Verlag, New York, 2004.

[49] Hijikata, H.; Pizer, A.; Shemanske, T., *The basis problem for modular forms on* $\Gamma_0(N)$. Mem. Amer. Math. Soc. **82**, (1989), no. 418.

[50] Hijikata, H.; Pizer, A.; Shemanske, T., Orders in quaternion algebras. *J. Reine Angew. Math.*, **394**, (1989), 59–106.

[51] Illusie, L., Réalisation ℓ-adique de l'accouplement de monodromie d'après A. Grothendieck. *Courbes modulaires et courbes de Shimura* (Orsay, 1987/1988). Astérisque No. **196-197**, (1991), 7, 27–44 (1992).

[52] Jacquet, H.; Langlands, R.P., *Automorphic forms on* GL(2). Lecture Notes in Mathematics, Vol. **114**. Springer-Verlag, Berlin-New York, 1970.

[53] Janusz, G., *Algebraic number fields.* Second edition. Graduate Studies in Mathematics, **7**. American Mathematical Society, Providence, RI, 1996.

[54] de Jong, A. J.; Oort, F., Purity of the stratification by Newton polygons. *J. Amer. Math. Soc.* **13**, (2000), no. 1, 209–241.

[55] Katz, N., Slope filtration of F-crystals. Journéees de Géométrie Algébrique de Rennes (Rennes, 1978), Vol. I, pp. 113–163, *Astérisque*, **63**, Soc. Math. France, Paris, 1979.

[56] Kitaoka, Y., *Arithmetic of quadratic forms.* Cambridge Tracts in Mathematics, **106**,Cambridge University Press, Cambridge, 1993.

[57] Kleiman, S.; Landolfi, J., Geometry and deformation of special Schubert varieties. *Compositio Math.*, **23**, (1971), 407–434.

[58] Kneser, M., Strong approximation. 1966, *Algebraic Groups and Discontinuous Subgroups* (Proc. Sympos. Pure Math. **IX**, Boulder, Colo., 1965) pp. 187–196, Amer. Math. Soc., Providence, R.I.

[59] Kohel, D., *Endomorphism rings of elliptic curves over finite fields*, Ph.D. thesis, U.C. Berkeley, 1996.

[60] Kottwitz, R., Isocrystals with additional structure. *Compositio Math.* **56**, (1985), no. 2, 201–220.

[61] Kutz, R., Cohen-Macaulay rings and ideal theory in rings of invariants of algebraic groups. *Trans. Amer. Math. Soc.*, **194**, (1974), 115–129.

[62] Lam, T.Y., *The algebraic theory of quadratic forms.* Revised second printing. Mathematics Lecture Note Series. Benjamin/Cummings Publishing Co., Inc., Advanced Book Program, Reading, Mass., 1980.

[63] Langlands, R.P., *Base change for* GL(2). Annals of Mathematics Studies, **96**. Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1980.

[64] Lazard, M., *Commutative formal groups.* Lecture Notes in Mathematics, Vol. **443**. Springer-Verlag, Berlin-New York, 1975.

[65] Li, K.-Z, Oort, F., *Moduli of Supersingular Abelian Varieties*, Lecture Notes in Mathematics, **1680**. Springer-Verlag, Berlin, 1998.

[66] Manin, Yu.I., Theory of commutative formal groups over fields of finite characteristic. *Uspehi Mat. Nauk*, **18**, 1963, no. 6, (114), 3–90.

[67] Milne, J.S., Points on Shimura varieties mod p. *Automorphic forms, representations and L-functions* (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2, pp. 165–184, Proc. Sympos. Pure Math., **XXXIII**, Amer. Math. Soc., Providence, R.I., 1979.

[68] Moonen, B.J.J., A dimension formula for Ekedahl-Oort strata. *Ann. Inst. Fourier (Grenoble)*, **54**, (2004), no. 3, 666–698.

[69] 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.

[70] Oort, F., *Commutative group schemes.* Lecture Notes in Mathematics, **15**, Springer-Verlag, Berlin-New York, 1966.

[71] Oort, F., Which abelian surfaces are products of elliptic curves? *Math. Ann.*, **214**, (1975), 35–47.

[72] Ogus, A., Supersingular $K3$ crystals. Journées de Géométrie Algébrique de Rennes (Rennes, 1978), Vol. II, pp. 3–86, Astérisque, **64**, Soc. Math. France, Paris, 1979.

[73] Oort, F., A stratification of a moduli space of abelian varieties. *Moduli of abelian varieties (Texel Island, 1999)*, 345–416, Progr. Math., **195**, Birkhäuser, Basel, 2001.

[74] Oort, F., Foliations in moduli spaces of abelian varieties. *J. Amer. Math. Soc.* **17** (2004), no. 2, 267–296.

[75] Oort, F., Minimal p-divisible groups, accepted for publication in the Annals of Mathematics. *http* : *//www.math.ruu.nl/people/oort/*

[76] Pappas, G., Arithmetic models for Hilbert modular varieties. *Compositio Math.* **98**, (1995), no. 1, 43–76.

[77] Pays, I., Formes normes d'ordres. *J. Algebra*, **155**, (1993), no. 2, 325–334.

[78] Pink, R., *Finite group schemes*, lecture notes, 2005. *http* : *//www.math.ethz.ch/ ∼ pink/*

[79] Pizer, A., On the arithmetic of quaternion algebras. *Acta Arith.* **31**, (1976), no. 1, 61–89.

[80] Pizer, A., An algorithm for computing modular forms on $\Gamma_0(N)$. *J. Algebra*, **64**, (1980), no. 2, 340–390.

[81] Platonov, V.; Rapinchuk, A., *Algebraic groups and number theory.* Translated from the 1991 Russian original by Rachel Rowen. Pure and Applied Mathematics, **139**. Academic Press, Inc., Boston, MA, 1994.

[82] Rapoport, M., Compactifications de l'espace de modules de Hilbert-Blumenthal. *Compositio Math.* **36**, (1978), no. 3, 255–335.

[83] Rapoport, M., Zink, Th., *Period spaces for p-divisible groups*, Annals of Mathematics Studies, **141**. Princeton University Press, Princeton, NJ, 1996.

[84] Reiner, I., *Maximal orders.* London Mathematical Society Monographs, No. **5**. Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], London-New York, 1975.

[85] Ribet, K. *Bimodules and abelian surfaces.*, Algebraic number theory, 359–407, Adv. Stud. Pure Math., **17**, Academic Press, Boston, MA, 1989.

[86] 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.

[87] Saito, H., Automorphic forms and algebraic extensions of number fields. II. *J. Math. Kyoto Univ.* **19**, (1979), no. 1, 105–123.

[88] Schulze-Pillot, R., Theta liftings and theta series, expanded version of talks at IAS, Princeton, Nov. 23rd, 1999, and at RIMS, Kyoto, Jan. 1998. *http* : $//www.math.uni - sb.de/ \sim ag - schulze/Preprints/rims.ps$

[89] Serre, J.-P., *Corps locaux.* Publications de l'Institut de Mathématique de l'Université de Nancago, VIII, Actualités Sci. Indust., No. **1296**. Hermann, Paris 1962.

[90] Serre, J.-P., Complex multiplication, in *Algebraic number theory*. Proceedings of the instructional conference held at the University of Sussex, Brighton, September 1–17, 1965. Edited by J. W. S. Cassels and A. Fröhlich. Reprint of the 1967 original. Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], London, 1986.

[91] Shimizu, H., Theta series and automorphic forms on GL_2. *J. Math. Soc. Japan*, **24**, (1972), 638–683.

[92] Shimura, G., On analytic families of polarized abelian varieties and automorphic functions. *Ann. of Math.* (2), **78**, 1963, 149–192.

[93] Shimura, G., *Introduction to the arithmetic theory of automorphic functions.* Kano Memorial Lectures, No.**1**. Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo; Princeton University Press, Princeton, N.J., 1971.

[94] Shimura, G., The number of representations of an integer by a quadratic form. *Duke Math. J.* **100** (1999), no. 1, 59–92.

[95] 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.

[96] Tate, J., Endomorphisms of abelian varieties over finite fields. *Invent. Math.* **2**, 1966, 134–144.

[97] Traverso, C., Sulla classificazione dei gruppi analitici commutativi di caratteristica positiva. *Ann. Scuola Norm. Sup. Pisa* (3), **23**, 1969, 481–507.

[98] Traverso, C., Specializations of Barsotti-Tate groups. *Symposia Mathematica*, Vol. **XXIV** (Sympos., INDAM, Rome, 1979), pp. 1–21, Academic Press, London-New York, 1981.

[99] Vasiu, A., Crystalline Boundedness Principle, preprint AG/0205199.

[100] 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.

[101] Vignéras, M.-F., Invariants numériques des groupes de Hilbert. *Math. Ann.* **224** (1976), no. 3, 189–215.

[102] Vignéras, M.-F., *Arithmétique des algèbres de quaternions.* Lecture Notes in Mathematics, **800.**, Springer, Berlin, 1980.

[103] Vollaard, I., On the Hilbert-Blumenthal moduli problem, To appear in: Journal of the Inst. of Math. Jussieu.

http : *//io.math.uni* − *bonn.de/people/vollaard/*

[104] Waldspurger, J.-L., Engendrement par des séries thêta de certains espaces de formes modulaires. *Invent. Math.* **50**, (1978/79), no. 2, 135–168.

[105] Waldspurger, J.-L., Formes quadratiques à 4 variables et relèvement. *Acta Arith.* **36**, (1980), no. 4, 377–405.

[106] Walling, L., Hecke operators on theta series attached to lattices of arbitrary rank. *Acta Arith.* **54**, (1990), no. 3, 213–240.

[107] Walling, L., The Eichler commutation relation for theta series with spherical harmonics. *Acta Arith.* **63**, (1993), no. 3, 233–254

[108] Waterhouse, W., Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup.* (4), **2**, 1969, 521–560.

[109] Waterhouse, W. C.; Milne, J. S., Abelian varieties over finite fields. 1969 Number Theory Institute, (Proc. Sympos. Pure Math., Vol. **XX**, State Univ. New York, Stony Brook, N.Y., 1969), pp. 53–64. Amer. Math. Soc., Providence, R.I., 1971.

[110] Weil, A., *Basic number theory.* Die Grundlehren der mathematischen Wissenschaften, Band **144**, Springer-Verlag New York, Inc., New York 1967.

[111] Yu, C.-F., On the supersingular locus in Hilbert-Blumenthal 4-folds. *J. Algebraic Geom.* **12** (2003), no. 4, 653–698.

[112] Yu, C.-F., On reduction of Hilbert-Blumenthal varieties. *Ann. Inst. Fourier (Grenoble)*, **53**, (2003), no. 7,

[113] Zariski, O., Samuel, P. *Commutative algebra.* Vol. II. The University Series in Higher Mathematics., D. Van Nostrand Co., Inc., Princeton, N. J.-Toronto-London-New York, 1960.

[114] Zhang, S.-W., Gross-Zagier formula for GL_2. *Asian J. Math.* **5** (2001), no. 2, 183–290.

[115] Zink, T., Letter dated May 1, 1999.

*www.math.upenn.edu/~chai/zinkletter*050199*.pdf*