Math. Ann. 313, 475–506 (1999)

Mathematische Annalen

On the non ordinary locus in Hilbert-Blumenthal surfaces

E. Bachmat[1], **E.Z. Goren**[2]

[1] Department of Mathematics, M.I.T., Cambridge, MA 02139, USA (e-mail: ebachmat@math.mit.edu)

[2] Department of Mathematics and Statistics, 805 Sherbrooke St. W., McGill University, Montreal, QC, Canada, H3A 2K6 (e-mail: goren@math.mcgill.ca)

Received: 3 February 1998 / in revised form: 7 September 1998

Mathematics Subject Classification (1991): 14K10, 14G35, 14D15

1. Introduction

Let $L = \mathbb{Q}(\sqrt{D})$ (D a square free integer) be a totally real quadratic field, and let $\mathcal{M}_{d_L,n}$ be the moduli space, in characteristic $p \geq 3$, parameterizing principally polarized abelian surfaces (A, λ), in characteristic p, together with a symplectic level $n \geq 3$ structure and an embedding of rings $\iota : \mathcal{O}_L \to \mathrm{End}(A)^\lambda$ (here $\mathrm{End}(A)^\lambda$ are the endomorphisms fixed by the Rosati involution associated to λ). We refer the reader to [DP], [Ra] and [vG] for further details.

Let $\mathcal{V} = \mathcal{V}_{d_L,n}$ be the complement of the ordinary locus in $\mathcal{M}$ and let $\mathcal{S} = \mathcal{S}_{d_L,n}$ be the supersingular locus. This paper is about $\mathcal{V}$. The analysis and the results are divided according to the decomposition of p in L. We establish the following results:

1. If p is inert or ramified in L then $\mathcal{V} = \mathcal{S}$. Every component of $\mathcal{S}$ is a smooth rational curve and the number of components is

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

where $C_p = 1$ if p is inert and $C_p = 1/2$ if p is ramified. For generalizations to the case of moduli spaces obtained by considering the action of an order of $\mathcal{O}_L$, see the appendix.

2. If p is inert or split in L then the singularities of $\mathcal{V}$ are ordinary with two branches and correspond to intersection points of the irreducible components; the singular points being exactly the superspecial points (if p is

split every supersingular point is superspecial). Furthermore, the intersection graph of $\mathcal{V}$ is bipartite.

3. If p is ramified in L then on each rational component there are $p+1$ singular points (counted with multiplicity) which are all superspecial. The singularity being ordinary with $p+1$ branches. These points are exactly the points where the cotangent space of the corresponding abelian variety is not free over $\mathcal{O}_L/p$ and they are exactly the singular points of $\mathcal{M}$ (the tangent cone being $z^2 = xy$).

4. When p is split in L, we prove that the orbit of any $x \in \mathcal{V} \setminus \mathcal{S}$ under a certain Hecke algebra is dense in $\mathcal{V}$.

When p is inert the equality $\mathcal{V} = \mathcal{S}$ and the structure of $\mathcal{S}$ as appears in 2. above were first determined by H.Stamm ([St]) . We present a different proof of his results in Sect. 6.1. When p is ramified, 3. complements a result of Deligne-Pappas ([DP]) in the case of surfaces.

Our approach to counting the number of components of $\mathcal{S}$ is based on the work of T. Katsura and F. Oort ([KO1]).

Acknowledgements. Both authors would like to thank G. van der Geer and F. Oort for stimulating conversations. This work was prepared while the first author was at Brown university . The second author was partially supported by a Rothschild fellowship and by Harvard university. Special thanks are due to B.Gross.

2. Background

2.1.

We fix the following notation: $p \geq 3$ is a rational prime and k is an algebraically closed field of characteristic p. Let E_1, E_2 denote supersingular elliptic curves (abbreviated: *ssg*) over k and $X = E_1 \times E_2$. We let Y, Z denote general abelian varieties over k and A will usually denote a supersingular abelian surface over k.

The a-number and f-number of $Y/\mathbb{F}$ ($\mathbb{F}$ a characteristic p field) are defined as follows:

$$a(Y) = \dim \ \mathrm{Hom}(\alpha_p, Y) \ ; \quad p^{f(Y)} = |Y[p](\overline{\mathbb{F}})|.$$

We denote by $Fr : Y \to Y^{(p)}$ the Frobenius morphism and by $V : Y^{(p)} \to Y$ the Verschiebung morphism. For $f : Z \to Y$ we let $f^t : Y^t \to Z^t$ denote the dual morphism and $f^* : \mathrm{End}^0(Y) \to \mathrm{End}^0(Z)$ the induced homomorphism, where as usual $\mathrm{End}^0(Y) = \mathrm{End}(Y) \otimes \mathbb{Q}$. Similar conventions hold for groups G.

Given such G, we denote its contravariant Dieudonné module over $W(k)[F,V]$ by $\mathcal{D}(G)$ (see [Dm]). For example, it is known that $\mathcal{D}(E_i[p])$

(respectively $H^1_{Cr}(E_i)$) has a basis over k (resp. $W(k)$) of the form (e_i, Fe_i) where $F^2 e_i = -pe_i, Ve_i = -Fe_i$ and such a basis is unique up to substitutions $e_i \mapsto \alpha e_i + \beta F e_i$ where $\alpha \in \mathbb{F}_{p^2}^{\times}, \beta \in \mathbb{F}_{p^2}$ (resp. $\alpha \in W(\mathbb{F}_{p^2})^{\times}, \beta \in W(\mathbb{F}_{p^2})$) . Such a basis will be called a *distinguished basis*.

2.2.

Let $G = X[p]$ and let (e_1, Fe_1, e_2, Fe_2) be a distinguished basis for $\mathcal{D}(G)$. Let $\mu = \mu(E_1, E_2)$ be the product polarization on X. Then μ induces a perfect alternating pairing $B_\mu : \mathcal{D}(G) \times \mathcal{D}(G) \to k$, which is determined by $\theta_i = B_\mu(e_i, Fe_i)$.

Let $H \subset \mathrm{Ker}(p\mu) = X[p]$ be a subgroup of order p, and let $\pi_H : X \to X/H$ be the natural projection. Such an H is automatically isotropic w.r.t the Mumford pairing induced by $p\mu$ on $X[p]$. Thus, there exists a polarization λ_H on X/H such that $\pi_H^* \lambda_H = p\mu$. We would like to determine when is $\mathrm{Ker}(\lambda_H) \cong \alpha_p \oplus \alpha_p$.

Such an H is determined by a surjective homomorphism of Dieudonné modules $\Pi_H : \mathcal{D}(X[p]) \to k = \mathcal{D}(\alpha_p)$. The following lemma is straightforward (see also [KO2], [MB]).

Lemma 2.1. *In the notation above:*

1. For every choice of distinguished bases $\theta_i \in \mathbb{F}_p$.

2. $\mathrm{Ker}(\lambda_H) \cong \alpha_p \oplus \alpha_p$ *iff* $\mathrm{Ker}(\Pi_H) = \mathrm{Span}_k \{Fe_1, Fe_2, e_2 - te_1\}$, *where* $t^{p+1} = -\theta_2/\theta_1$. *In particular* $t \in \mathbb{F}_{p^2}$.

One calls such t *very good directions*.

2.3.

In [KO1] one finds a description of the supersingular locus in $\mathcal{A} = \mathcal{A}_{2,1}$ – the moduli space of principally polarized abelian surfaces in characteristic p. We briefly recall the main idea.

Choose a principal polariztion ν on X and let $H \subset X[p]$ be a subgroup of order p such that $\mathrm{Ker}(\lambda_H) \cong \alpha_p \oplus \alpha_p$. Then, every $H_1 \subset X/H$ of order p is a maximal isotropic subgroup of $\mathrm{Ker}(\lambda_H)$ and thus $(X/H)/H_1$ is naturally principally polarized. Fixing an embedding $\alpha_p \oplus \alpha_p \to X/H$, the subgroups H_1 are parameterized by $\mathbb{P}^1$. This gives a finite map $\mathbb{P}^1 \to \mathcal{A}$. Furthermore, it follows from [KO1] that every component of the supersingular locus in $\mathcal{A}$ can be obtained in this way when one may just take ν's of the form $\mu(E_1, E_2)$.

2.4. Translation to submodules

To give a subgroup H_1 of $\mathrm{Ker}(\lambda_H)$ is equivalent to giving a sub-Dieudonné module U of $\mathcal{D}(X[p])$ such that $\mathrm{Ker}(\Pi_H)^{\perp} \subsetneqq U \subsetneqq \mathrm{Ker}(\Pi_H)$. Equiva-

lently, using the canonical isomorphism $H^1_{Cr}(X)/pH^1_{Cr}(X) \cong \mathcal{D}(X[p])$, this amounts to giving a sub-Dieudonné module W of $H^1_{Cr}(X)$ such that $W \supset pH^1_{Cr}(X)$ and $W/pH^1_{Cr}(X)$ is a module U of this type. Note that

$$W = \mathrm{Span}_{W(k)}\{pH^1_{Cr}(X), v, w\}, \tag{1}$$

$$v = Fe_2 - T^{\sigma}Fe_1, \;\; w = -Ta_2e_1 + a_1Fe_1 + a_2e_2,$$

where $T \equiv t \pmod p$ and $(a_1 : a_2) \pmod p \in \mathbb{P}^1(k)$. Note also that W depends only on $T \pmod p, (a_1 : a_2) \pmod p$. We will use the notation X_W (*resp.* $(X, \mu)_W$) to denote the abelian variety (*resp.* with the principal polarization) associated to W. We will use the notation $\overline{z}$ to denote $z \pmod p$.

Lemma 2.2. *$X_W \cong X$ if and only if $(\overline{a_1} : \overline{a_2}) \in \mathbb{P}^1(\mathbb{F}_{p^2})$.*

Proof. Note that Ver is the zero map on the finite group scheme of order p^2 $G = \mathrm{Ker}(Fr : X_W \longrightarrow X_W^{(p)})$, if and only if $G \cong \alpha_p \oplus \alpha_p$. This holds if and only if $X_W \cong X$. Since $\mathcal{D}(G) \cong W/FW$, we are reduced to checking the inclusion $VW \subseteq FW$.

Since $Vpe_i = pVe_i = -pFe_i = F(-pe_i)$, and $VpFe_i = FpVe_i$, we have

$$VpH^1_{Cr}(X) \subseteq FpH^1_{Cr}(X) \subseteq FW.$$

Also,

$$Vv = pe_2 - Tpe_1 = F(-Fe_2 + T^{\sigma^{-1}}Fe_1).$$

Hence, using Lemma 2.1, we get

$$Vv + Fv = F((T^{\sigma^{-1}} - T^{\sigma})Fe_1) \in FpH^1_{Cr}(X) \subseteq FW.$$

Therefore, $VW \subseteq FW$, if and only if $Vw \in FW$. Now,

$$\begin{aligned} Vw &= -T^{\sigma^{-1}}a_2^{\sigma^{-1}}Ve_1 + a_1^{\sigma^{-1}}pe_1 + a_2^{\sigma^{-1}}Ve_2 \\ &= F(T^{\sigma^{-2}}a_2^{\sigma^{-2}}e_1 - a_1^{\sigma^{-2}}Fe_1 - a_2^{\sigma^{-2}}e_2). \end{aligned}$$

Thus, $Vw \in FW \Longleftrightarrow T^{\sigma^{-2}}a_2^{\sigma^{-2}}e_1 - a_1^{\sigma^{-2}}Fe_1 - a_2^{\sigma^{-2}}e_2 \in W$. If $a_2 = 0$ we can assume $a_1 = 1$ and hence $Vw \in FW$. Else, we may take $a_2 = 1$ and since $W \supset pH^1_{Cr}(X)$ and $\overline{T} \in \mathbb{F}_{p^2}$, we find that $Vw \in FW$, if and only if

$$\begin{aligned} &T^{\sigma^{-2}}a_2^{\sigma^{-2}}e_1 - a_1^{\sigma^{-2}}Fe_1 - a_2^{\sigma^{-2}}e_2 + w \\ &\quad = (a_1 - a_1^{1/p^2})Fe_1 \in W \pmod p. \end{aligned}$$

The claim now follows easily from (1). *q.e.d.*

3. Existence of embeddings

3.1.

Let $\mu = \mu(E_1, E_2)$ be the product polarization on $X = E_1 \times E_2$, and let

$$\Lambda = \begin{cases} \sqrt{D} & D \equiv 2,3 \pmod 4 \\ \frac{-1+\sqrt{D}}{2} & D \equiv 1 \pmod 4 \end{cases}, \quad \epsilon = \begin{cases} 0 & D \equiv 2,3 \pmod 4 \\ 1 & D \equiv 1 \pmod 4 \end{cases},$$

$$\Delta = \begin{cases} D & D \equiv 2,3 \pmod 4 \\ \frac{D-1}{4} & D \equiv 1 \pmod 4 \end{cases}.$$

An embedding $L \hookrightarrow \mathrm{End}^0(X)^\mu$ is determined by the image of Λ, which is a matrix of the form

$$\begin{pmatrix} a & \beta \\ \hat{\beta} & -(\epsilon + a) \end{pmatrix},$$

where $a \in \mathbb{Q},\ \beta \in \mathrm{Hom}(E_2, E_1) \otimes \mathbb{Q},\ a^2 + a\epsilon + \beta\hat{\beta} = \Delta$.

Proposition 3.1. *Let (A, λ) be a ssg principally polarized abelian surface. Let E_1, E_2 be appropriate ssg elliptic curves and W a suitable submodule of $H^1_{Cr}(X)$ such that $(A, \lambda) \cong (X, \mu)_W$ and let $\pi_W : X \longrightarrow A$ be the corresponding homomorphism (see Sect. 2.4). Then, for a given embedding $L \hookrightarrow \mathrm{End}^0(A)$,*

$$\Lambda \in \mathrm{End}(A)^\lambda \Longleftrightarrow \pi_W^*(\Lambda) \in \mathrm{End}^0(X)^\mu \ \ and \ \ \pi_W^*(\Lambda)(W) \subseteq W.$$

In this case,

$$h = \pi_W^*(\Lambda) = \frac{1}{p} \begin{pmatrix} a & \beta \\ \hat{\beta} & -(p\epsilon + a) \end{pmatrix}, \tag{2}$$

where $a \in \mathbb{Z},\ \beta \in \mathrm{Hom}(E_2, E_1)$ and

$$a^2 + ap\epsilon + \beta\hat{\beta} = \Delta p^2. \tag{3}$$

Conversely, given an endomorphism h as above, we have

$$h \in \pi_W^*(\mathrm{End}(A)^\lambda) \Longleftrightarrow h(W) \subset W, \tag{4}$$

and in this case $h = \pi_W^*(\Lambda)$ for a suitable embedding $\mathcal{O}_L \hookrightarrow \mathrm{End}(A)^\lambda$.

Proof. This follows from general facts on abelian varieties. The main point is to note first that $W = \pi_W^*(H^1_{Cr}(X_W))$, and for abelian variety Y and $f \in \mathrm{End}^0(Y)$ such that $p^n f \in \mathrm{End}(Y)$, one has $f \in \mathrm{End}(Y)$ if and only if $f^*(H^1_{Cr}(Y)) \subseteq H^1_{Cr}(Y)$. *q.e.d.*

3.2. Embeddings

We will determine when $\mathrm{End}(A)^\lambda$ contains an element of the form Λ. By Subsection 2.3 and Proposition 3.1, such elements correspond in a non unique way to the following data:
A) $X = E_1 \times E_2$ with the standard polarization $\mu = \mu(E_1, E_2)$.
B) An element h of $\mathrm{End}^0(X)^\mu$ as in Proposition 3.1. Note that h preserves

$$W = \mathrm{Span}_{W(k)}(pH^1_{Cr}(X), v, w)$$

where v and w are as in Subsection 2.4 . Namely:

$$v = Fe_2 - T^\sigma Fe_1, \quad , w = -Ta_2e_1 + a_1Fe_1 + a_2e_2$$

C) A very good direction t (see Subsection 2.2)
D) A point $r = a_2/a_1 \in \mathbb{P}^1$.

The following theorem establishes which sets of data (X, μ, h, t, r) correspond to points on the Hilbert-Blumenthal surface. We keep the notation above and put $b = \beta\hat{\beta}$ in the notation of equation (2).

Theorem 3.2. *The following sets of data (X, μ, h, t, r) correspond to points on the Hilbert-Blumenthal surface $\mathcal{M}_{d_L,1}$:*

Case 1: $p|b$.

(1.1) All sets with $p^4|b$, arbitrary t and $r = 0$.

(1.2.1) All sets with $p^3||b$, $-2a/p \equiv \epsilon \pmod p$, t and r arbitrary. The conditions imply that $p|D$.

(1.2.2) All sets with $p^3||b$, t arbitrary and r=0.

(1.3.1) All sets with $p^2||b$, $t = -c - \epsilon/2$ and r arbitrary. The conditions imply that $p|D$.

(1.3.2) All sets with $p^2||b$, $t \notin \mathbb{F}_p$, $-(t^p + t + \epsilon)/2 = c$ and r arbitrary. The conditions define two t's given the rest of the data and imply that p is inert in L.

(1.3.3) All sets with $p^2||b$, t arbitrary and r=0. The conditions imply that p is either inert or ramified in L.

Case 2:

All sets with $(p, b) = 1$, $t = -a$ and $r = \infty$.

Definition 1. *In any of the above cases, given E_1, E_2, a matrix $h \in \mathrm{End}^0(E_1 \times E_2)$ and a very good direction t, if r can be taken to be arbitrary then we say that t is* adjusted *to h.*

Proof. We shall present a case by case analysis of such h, which will prove the theorem. The case indexing in the proof corresponds to that in the statement

of the theorem. Subcases are given by additional indices. The computation being lenghty we leave Case 2 and some other details to the reader.

Using the structure of the p^ℓ torsion of a supersingular elliptic curve and equation (3), one verifies that either $p|\beta$ or $(p,b) = 1$ (and similarly in subcases below).

Case 1: $p|\beta$.
By equation (3), $p|a$, so we may write

$$h = \begin{pmatrix} c & \delta \\ \hat{\delta} & -(\epsilon + c) \end{pmatrix},$$

with $c = a/p$ and $\beta = p\delta$. We also have

$$c^2 + \epsilon c + d = \Delta, \tag{5}$$

where $d = \delta\hat{\delta}$.

Case (1.1) $p|\delta$.
Since h is integral it preserves $pH^1_{Cr}(E_1 \times E_2)$ and hence preserves W if and only if it preserves $U = W \pmod p$ (This applies to Cases 1.2 , 1.3 as well). In this case $h \pmod p$ becomes

$$h = \begin{pmatrix} c & 0 \\ 0 & -(\epsilon + c) \end{pmatrix},$$

and its action on $H^1_{Cr}(E_1 \times E_2)$ is given with respect to a pair of distinguished bases e_1, Fe_1, e_2, Fe_2 by

$$\begin{pmatrix} c & 0 & 0 & 0 \\ 0 & c & 0 & 0 \\ 0 & 0 & -(\epsilon + c) & 0 \\ 0 & 0 & 0 & -(\epsilon + c) \end{pmatrix}.$$

The corresponding equations are

$$(0, -ct^p, 0, -(\epsilon + c))^t = x_1(0, -t^p, 0, 1)^t + y_1(-ta_2, a_1, a_2, 0)^t,$$

and

$$(-cta_2, ca_1, -(\epsilon + c)a_2, 0)^t = x_2(0, -t^p, 0, 1)^t + y_2(-ta_2, a_1, a_2, 0)^t.$$

Assume $a_2 \neq 0$ then the first equation implies $y_1 = 0$ and $x_1 = -(\epsilon + c)$. These in turn give the condition $-ct^p = (\epsilon + c)t^p$. Since $t^p \neq 0$ we obtain $2c + \epsilon \equiv 0 \pmod p$. If $\epsilon = 0$, then we obtain from equation (5) that

$p^2|D$, which is a contradiction since D is square free. If $\epsilon = 1$, we obtain $4c^2 + 4c + 1 = (2c+1)^2 \equiv D \pmod{p^2}$, which again gives $p^2|D$ and hence a contradiction.

Assuming therefore that $a_2 = 0$ and fixing $a_1 = 1$, we may verify that

$$x_1 = -(\epsilon + c), \;\; y_1 = (-2c - \epsilon)t^p, \;\; x_2 = 0, \;\; y_2 = c,$$

provides a solution for any good direction t.

Case (1.2) $d = pm$ and $(m, p) = 1$.
We claim that we can find a basis for $H^1_{Cr}(E_1 \times E_2)$ in which $h \pmod{p}$ is written as

$$h = \begin{pmatrix} c & 0 & 0 & 0 \\ 0 & c & -m & 0 \\ 0 & 0 & -(\epsilon + c) & 0 \\ 1 & 0 & 0 & -(\epsilon + c) \end{pmatrix}. \tag{6}$$

To do this, first choose a distinguished basis (e_1, Fe_1) for $H^1_{Cr}(E_1)$. We claim that there exists an $e_2 \in H^1_{Cr}(E_2)$ such that $Fe_2 = \delta^*(e_1)$. Indeed:

We first note that we can factor δ as

$$E_2[p] \twoheadrightarrow \alpha_p \hookrightarrow E_1[p],$$

and hence factor δ^* as

$$\mathcal{D}(E_2[p]) \hookleftarrow \mathcal{D}(\alpha_p) \twoheadleftarrow \mathcal{D}(E_1[p]),$$

and since F kills $\mathcal{D}(\alpha_p)$ we conclude that F kills $\delta^*(\mathcal{D}(E_1[p]))$. In particular $F(\delta^*(e_1)) \in pH^1_{Cr}(E_2)$. Next we choose a distinguished basis (e_2', Fe_2') for $H^1_{Cr}(E_2)$. We have

$$\begin{aligned} pH^1_{Cr}(E_2) &= p\,\mathrm{Span}(e_2', Fe_2') \\ &= \mathrm{Span}(FVe_2', Fpe_2') = F^2\mathrm{Span}(-e_2', Ve_2'). \end{aligned}$$

Therefore, by the injectivity of F, there exists an e_2 such that

$$\delta^*(e_1) = Fe_2.$$

We shall choose (e_2, Fe_2) as our basis for $H^1_{Cr}(E_2)$.

Next one checks that (e_2, Fe_2) is distinguished and that h has the form above with respect to (e_1, Fe_1, e_2, Fe_2). Since h is integral, the inclusion $h(W) \subseteq W$ can be verified again mod p.
We obtain the following equations

$$(0, -ct^p, 0, -(\epsilon + c))^t = x_1(0, -t^p, 0, 1)^t + y_1(-ta_2, a_1, a_2, 0)^t,$$

and

$$(-cta_2, ca_1 - ma_2, -(\epsilon + c)a_2, -ta_2)^t \\ = x_2(0, -t^p, 0, 1)^t + y_2(-ta_2, a_1, a_2, 0)^t.$$

Case (1.2.1) Assuming $a_2 \neq 0$, the first equation gives $x_1 = -(\epsilon + c)$ and $y_1 = 0$ and the condition

$$-ct^p = (\epsilon + c)t^p,$$

which implies

$$2c + \epsilon \equiv 0 \pmod{p}. \tag{7}$$

Using equation (5) and separating cases ($\epsilon = 0, 1$) this implies that $p|D$. The second equation yields $x_2 = -ta_2$ and $y_2 = -(\epsilon + c)$ and the conditions

$$-ct = (\epsilon + c)t \ , \ ca_1 - ma_2 = t^{p+1}a_2 - (\epsilon + c)a_1. \tag{8}$$

The condition (7) implies the first condition of (8) and transforms the second into

$$-m = t^{p+1}.$$

We shall now show that this condition holds precisely for those t's which are very good directions. Indeed, $p\theta_2 = B(pe_2, Fe_2) = B(VFe_2, Fe_2) = B(Fe_2, F^2e_2)^{1/p} = B(\delta^* e_1, \delta^* Fe_1)^{1/p} = B((\hat{\delta}\delta)^* e_1, Fe_1)^{1/p} = (pm\theta_1)^{1/p} = pm\theta_1$, by Lemma 2.1 . Hence $m = \frac{\theta_2}{\theta_1} = -t^{p+1}$ by the same lemma.

Case (1.2.2) If $a_2 = 0$, taking $a_1 = 1$, one easily verifies that the equations are solved for any t by

$$x_1 = -(\epsilon + c), \ \ y_1 = -(\epsilon + 2c)t^p; \quad x_2 = 0, \ \ y_2 = c.$$

Note that this also complements Case 1.2.1 .

Case (1.3) $(p, d) = 1$. Let (e_1, Fe_1) be a distinguished basis for $H^1_{Cr}(E_1)$. Let $e_2 = \delta^*(e_1)$, then (e_2, Fe_2) is a distinguished basis for $H^1_{Cr}(E_2)$. With respect to (e_1, Fe_1, e_2, Fe_2) h is given by

$$\begin{pmatrix} c & 0 & d & 0 \\ 0 & c & 0 & d \\ 1 & 0 & -(\epsilon + c) & 0 \\ 0 & 1 & 0 & -(\epsilon + c) \end{pmatrix}. \tag{9}$$

Again by the integrality of h , we get that $h(W) \subseteq W$, if and only if the following equations can be solved mod p:

$$(0, -ct^p + d, 0, -t^p - (\epsilon + c))^t \\ = x_1(0, -t^p, 0, 1)^t + y_1(-ta_2, a_1, a_2, 0)^t,$$

and

$$(-cta_2 + da_2, ca_1, -ta_2 - (\epsilon + c)a_2, a_1)^t \\ = x_2(0, -t^p, 0, 1)^t + y_2(-ta_2, a_1, a_2, 0)^t.$$

Assuming $a_2 \neq 0$ the first equation yields $x_1 = -(t^p + \epsilon + c)$ and $y_1 = 0$ and the condition

$$t^{2p} + (\epsilon + 2c)t^p - d = 0. \tag{10}$$

The second equation yields $x_2 = a_1$ and $y_2 = -(t+\epsilon+c)$ and the conditions

$$t^2 + (\epsilon + 2c)t - d = 0, \tag{11}$$

and

$$a_1(-2c - \epsilon) = a_1(t^p + t). \tag{12}$$

By our choice of bases we have

$$\theta_2 = B(e_2, Fe_2) = B(\delta^*(e_1), \delta^*(Fe_1)) = B((\delta\hat{\delta})^*(e_1), Fe_1) = d\theta_1.$$

Hence the criterion for very good direction becomes:

$$t^{p+1} = -d. \tag{13}$$

Equation (11) obviously implies equation (10). We also note that equation (11) and equation (13) imply equation (12) . Indeed equation (13) implies that $-d$ which is the product of the roots of equation (11) – say t and t' – is also equal to tt^p. Hence $t' = t^p$ and therefore $-(\epsilon+2c) = t+t' = t+t^p$. Hence the above conditions on the very good direction t (which automatically satisfies $t^{p+1} = -d$) amount to equation (11).

Substituting equation (12) and equation (13) into equation (5) we obtain

$$(t^p + t + \epsilon)^2 - 2(t^p + t + \epsilon)\epsilon - 4t^{p+1} = 4\Delta,$$

which implies

$$(t^p - t)^2 - \epsilon^2 = 4\Delta,$$

which finally gives

$$(t^p - t)^2 = (2 - \epsilon)^2 D. \tag{14}$$

This shows that either $p|D$ (if and only if $t \in \mathbb{F}_p$) or p is inert in L (Since $t \notin \mathbb{F}_p$ implies $t^p - t \notin \mathbb{F}_p$). Conversely we have the following two cases:

Case (1.3.1) Assume $p|D$. Then choosing $t = -c - \frac{\epsilon}{2}$ one may easily verify by working backwards through the above argument that all the equations are satisfied and that t is a very good direction. Moreover this is the only solution.

Case (1.3.2) Assume p is inert in D. Let $s \in \mathbb{F}_{p^2}$ satisfy $s^2 = (2-\epsilon)^2 D$. Since solutions to the Artin-Schreier equation

$$t^p - t - s = 0$$

lie in $\mathbb{F}_{p^2}$ and form a coset $t + \mathbb{F}_p$ we may find one t_0 which further satisfies $\mathrm{Tr}(t_0) = -(2c + \epsilon)$. Again one may easily verify that t_0 satisfies all the conditions. There are two choices for t_0 corresponding to the two choices for s.

Case (1.3.3) $a_2 = 0$. Let $a_1 = 1$. we then have the solution

$$x_1 = -(t^p + c + \epsilon), y_1 = -t^{2p} - t^p(2c + \epsilon) + d, \quad x_2 = 1, y_2 = c + t^p$$

complementing our discussion of Cases 1.3.1 and 1.3.2 .

If $b = pm$ and $(m, p) = 1$ then equation (3) yields $p|a$ which in turn implies $p|m$. A contradiction. Therefore we are left with the case:

Case 2: $(p, b) = 1$. This case, proved similarly, is left to the reader. *q.e.d.*

4. On the V locus

Definition 2. *Assume that p is split in L then $\mathcal{O}_L/p \cong \mathbb{F}_p \oplus \mathbb{F}_p$. We let e_1, e_2 be the corresponding orthogonal idempotents. We abuse notation and write e_1, e_2 also for the idempotents coming from the decomposition $\mathcal{O}_L \otimes W(\overline{\mathbb{F}_p}) \cong W(\overline{\mathbb{F}_p}) \oplus W(\overline{\mathbb{F}_p})$.*

Proposition 4.1. *The complement of the ordinary locus, $\mathcal{V}$, is an effective divisor whose support is a complete curve. Moreover:*

1. If p is inert in L, then $\mathcal{V}$ is equal to the supersingular locus $\mathcal{S}$.

2. If p splits in L then $\mathcal{S}$ is zero dimensional and consists of superspecial points only.

3. If p is ramified in L, then $\mathcal{V} = \mathcal{S}$.

Proof. It is easy to see that we always have supersingular points therefore $\mathcal{V}$ is not empty. Since it is given locally by the vanishing of the determinant of the Hasse-Witt matrix it is an effective divisor.

One can define the f number also as

$$f(A) = \dim(\mathrm{Hom}(\mu_p, A)).$$

Since the cusps stand for totally degenerating abelian surfaces (i.e., tori) the fact that $\mathcal{V}$ is complete follows.

We remark that given (A, λ, ι) we can view $A[p]_{\text{ét}}$ as a module over $\mathcal{O}_L/p$. Therefore the case of p inert follows immediately.

Assume that p splits in L and $f(A) = 0$. Then $A[p]$ is a local-local group scheme and furthermore $A[p]$ is a direct sum $G_1 \oplus G_2$ induced from the idempotents e_1, e_2. Hence $a(A) = 2$ and A is superspecial. Finally, since the natural map $\mathcal{M} \to \mathcal{A}$ (see 2.3) is quasi-finite and the superspecial locus in $\mathcal{A}$ is zero dimensional the supersingular locus in $\mathcal{V}$ is zero-dimensional.

Consider now the case where p is ramified in L. Again $\mathcal{O}_L/p$ acts on $A[p]_{\text{ét}}$. Since $\sqrt{D}$ generates the maximal ideal of $\mathcal{O}_L/p$ ($p > 2$) the kernel of $\sqrt{D}$ in its action on $A[p]$, say K, is of order p^2. It is thus enough to show that $A[p]/K \cong K$ and indeed $\sqrt{D}$ gives the isomorphism *q.e.d.*

The study of the structure of the supersingular locus when p is inert or ramified in L will be carried out in Sect. 6 below. We now treat the case when p splits in L.

Definition 3. *Let p be split in L. We denote by $\mathcal{H}$ the following algebra of Hecke correspondences on $\mathcal{M}$. By definition it is generated by the following correspondences: Let ℓ be a prime. Define $\mathcal{M}_{d_L}(\ell)$ to be the moduli space of quadruples (A, λ, ι, H) where (A, λ, ι) is a principally polarized abelian scheme with real multiplication by $\mathcal{O}_L$ and $H \subseteq A[\ell]$ is a maximal isotropic and $\mathcal{O}_L$-invariant subgroup. We have two projections*

$$p_i : \mathcal{M}_{d_L}(\ell) \longrightarrow \mathcal{M}_{d_L},$$

given by

$$p_1((A, \lambda, \iota, H)) = (A, \lambda, \iota),$$

and

$$p_2((A, \lambda, \iota, H)) = (A/H, \pi_* \lambda, \pi_* \iota),$$

where $\pi : A \to A/H$ is the projection. The ℓ-th Hecke correspondence is by definition $p_{2*} \circ p_1^*$.

We define the Galois-Hecke algebra, $\mathcal{GH}$, to be the algebra of correspondences generated by $\mathcal{H}$ and the involution

$$(A, \lambda, \iota) \mapsto (A, \lambda, \iota \circ \sigma),$$

where $\sigma : L \to L$ is the non-trivial involution.

Remark. Note that also for $\ell = p$ the maps

$$p_i : \mathcal{M}_{d_L}(\ell) \longrightarrow \mathcal{M}_{d_L},$$

are quasi-finite. In particular the action of the Hecke correspondences is well defined on points. This fails when p is not split in L (see [St]).

Theorem 4.2. *Assume that p splits in L. Every singular point of $\mathcal{V}$ is an ordinary singularity with two branches. The singular points are exactly the superspecial points.*

The components of $\mathcal{V}$ can be divided into two sets such that the intersection graph of $\mathcal{V}$ is bipartite. In particular, every component is smooth and $\mathcal{V}$ is reducible.

Proof. Let $x/k \in \mathcal{V}$ be a geometric point such that $f(A_x) = 1$. Consider the action of the Hecke operators of order ℓ^n, $(\ell, p) = 1$, on x. The orbit is infinite (see [Ch]). Moreover, if x is a singular point so is every point in the orbit. This is impossible. Hence x is a smooth point.

Now let x be a point with $f(A_x) = 0$ hence x is superspecial. The ring

$$\mathcal{O}_L \otimes W(k) \cong R_1 \oplus R_2,$$

where $R_i \cong W(k)$, acts on the p-divisible group of A_x, say $\mathcal{G}$, which decomposes accordingly as

$$\mathcal{G} \cong \mathcal{G}_1 \oplus \mathcal{G}_2.$$

It is crucial to note that this decomposition is $\mathcal{O}_L$-invariant and the principal quasi-polarization decomposes as well. By Serre-Tate, the local deformations of A_x as a principally polarized abelian variety with real multiplication are the same as those of $\mathcal{G}$ (with the induced principal quasi-polarization and the $\mathcal{O}_L \otimes W(k)$ structure). The deformations of $\mathcal{G}$ together with the extra structure are just the products of the deformations of $\mathcal{G}_1$ and $\mathcal{G}_2$ – the endomorphisms and poalrizations now being automatic. The deformations of the $\mathcal{G}_i$ are just the deformations of a supersingular elliptic curve.

We see then that the local structure of $\mathcal{V}$ at a superspecial geometric point is an ordinary singularity with two branches given by taking the constant deformation of $\mathcal{G}_1$ and the universal deformation of $\mathcal{G}_2$ and the othe r component is obtained by exchanging the roles of $\mathcal{G}_1$ and $\mathcal{G}_2$.

We assign an invariant to the components of $\mathcal{V}$ as follows: The p-torsion of the generic point of a component has an étale quotient isomorphic to $\mathbb{Z}/p\mathbb{Z}$ (after base change). Therefore, either e_1 or e_2 acts as zero on it. We say that the component is of type i if e_i acts as zero on the étale quotient of the p-torsion of the generic (hence any) point. Note that the argument above shows that at a superspecial point one of the branches is of type 1 and the

other is of type 2. Therefore, components of the same type do not intersect, every component is smooth and the intersection graph is bipart ite. *q.e.d.*

The techniques of the proof of the next theorem can be applied to similar situation in higher dimensional Hilbert modular varieties. It is of interest also because of the methods of [Ch].

Theorem 4.3. *Assume that p is split in L.*

1. The action of $\mathcal{GH}$ is transitive on the superspecial points and on the components of $\mathcal{V}$.

2. The $\mathcal{GH}$ orbit of every non-superspecial point of $\mathcal{V}$ is dense in $\mathcal{V}$.

Proof. We first prove that the action of $\mathcal{H}$ on the superpsecial points is transitive (this holds in much more general situations):

Let $(A,\lambda,i),(B,\mu,j)$ be two superspecial points. It is known that $A \cong B$. Thus by the Skolem-Noether theorem, after conjugation we may assume $A = B, i = j$ and we are reduced to proving that for every principal polarization λ a nd L-linear polarization λ', (A,λ,i) and (A,λ',i) are in the same $\mathcal{H}$ orbit.

Let $\Psi_\lambda : \mathrm{NS}^0(A) \to \mathrm{End}^0(A),\ \Psi_\lambda(\gamma) = \lambda^{-1}\gamma$. It is known that Ψ_λ identifies $\mathrm{NS}^0(A)$ with the symmetric totally positive elements of $\mathrm{End}^0(A)$ w.r.t. the Rosati involution given by λ (denoted $x \mapsto \bar{x}$). An element of $\mathrm{NS}^0(A)$ is L-linear precisely when its image lands in $B = \mathrm{Cent}_{\mathrm{End}^0(A)}(L)$. It is known that B is a quaternion algebra over L which is everywhere ramified at infinity (see [Ch]). In particular, the Rosati involution induced by λ is the unique positive involution on B and is equal to the standard involution. Hence the symmetric elements of B are just L. It follows that the L-linear rational polarizations are identified with the totally positive elements of L. It is easy to check that the pull-back action of an endomorphism $b \in B$ on an L-linear polarization is given via Ψ_λ as multiplication by $b\bar{b}$. Strong approximation tells us that we can find such b satisfying $b\bar{b}\Psi_\lambda(\lambda') = \Psi_\lambda(\lambda)$. Multiplying b by a suitable natural number n we may assume that $b^*\lambda' = m\lambda, m \in \mathbb{N}, b \in \mathrm{End}(A)$.

We next show that the action of $\mathcal{H}$ preserves the types:

This is clear for operators of degree prime to p. It is easy to check that if $f(A) = 1$ then geometrically $A[p] \cong E[p] \oplus \mu_p \oplus \mathbb{Z}/p\mathbb{Z}$, where E is a supersingular elliptic curve, and $\alpha_p \oplus \mu_p,\quad \alpha_p \oplus \mathbb{Z}/p\mathbb{Z}$, are the only maximal isotropic $\mathcal{O}_L$-invariant subgroups. Note that e_1 kills μ_p iff it kills $\mathbb{Z}/p\mathbb{Z}$. Since division by such a maximal isotropic subgroup induces an $\mathcal{O}_L$-linear isomorphism either on the étale-local or local-étale part of the p-torsion we are done.

Now take x with $f(A_x) = 1$. From [Ch] we know that the $\mathcal{GH}$ orbit of x is infinite and hence its closure, Z, contains a component C_1 of type 1 and C_2 of type 2 (Galois involution exchanges the types). Let C be any component of $\mathcal{V}$, then C contains a superspecial point (" Raynaud's trick"). Similarly C_i contains a superspecial point c_i. Assume w.l.o.g. that C is of type 1. Using the previous observations we may find an operator $T \in \mathcal{H}$ such that $c \in T(c_1)$. It follows that the type 1 component through c, i.e., C, is in $T(C_1)$. Since Z is closed under $\mathcal{H}$ we have $C \in Z$. Note also that we have shown that $\mathcal{GH}$ acts transitively on the components of $\mathcal{V}$. *q.e.d.*

5. Components of the supersingular locus

Following the method of [KO1] and their notation (as much as possible), we construct and count the components of the supersingular locus $\mathcal{S} = \mathcal{S}_{d_L,n}$ in the Hilbert modular surface $\mathcal{M} = \mathcal{M}_{d_L,n}$ for $L = \mathbb{Q}(\sqrt{D}), D > 0$ square free, $p > 2$, and p inert or ramified in L. The reader should consult [KO1] for more details.
For an abelian variety Y we let $\mathrm{Aut}_v(Y)$ denote the automorphisms of Y as a variety (i.e. not necessarily preserving the zero point). We denote by

$$\gamma : \mathrm{Aut}_v(Y) \longrightarrow \mathrm{Aut}(Y),$$

the canonical projection. We denote by $\hbar$ the number of isomorphism classes of supersingular elliptic curves over $\bar{\mathbb{F}}_p$.

5.1. Construction of families

Let $E_1, \cdots, E_\hbar$ be representatives for the isomorphism classes of supersingular elliptic curves over k – an algebraically closed field of characteristic p. Let $n \geq 3$ be an integer. Let $\mathcal{A} = \mathcal{A}_{2,n}$ be the moduli space of principally polarized abelian surfaces in characteristic p.

Let t be adjusted to h be as in Theorem 3.2 in any of the cases where r is arbitrary. Let $A = E_m \times E_n / H_t$ where H_t is the subgroup corresponding to t. Let

$$\tilde{\pi} : E_m \times E_n \longrightarrow A,$$

be the canonical projection, then $\tilde{\pi}(E_m + E_n) = N$ is a reducible divisor of degree p with $\ker(\phi_N) \cong \alpha_p \oplus \alpha_p$ and $\tilde{\pi}^*(\phi_N) = p\mu(E_m, E_n)$ (see Subsection 2.2). Then, as in Subsection 2.3, we get from (A, N) a family $q : \mathfrak{X} \longrightarrow \mathbb{P}^1$ of principally polarized supersingular abelian surfaces and a natural map $\pi : A \times \mathbb{P}^1 \longrightarrow \mathfrak{X}$. Since for every $z \in \mathbb{P}^1$ the module $W_z = \tilde{\pi}^*\pi^* H^1_{Cr}(\mathfrak{X}_z)$ is stable under h, we see that h descends to an endomorphism

$h_{\mathfrak{X}}$ of the abelian scheme $\mathfrak{X}$. Moreover, following [KO1] p.114 one endows $\mathfrak{X}$ with a level n structure. The family $\mathfrak{X}$ is obviously non-isotrivial and therefore we get a component Ξ of the supersingular locus $\mathcal{S}$ in $\mathcal{M}$.

Conversely, let Ξ be a component of $\mathcal{S}$. Let ξ be a generic point of Ξ and let $(Y, \lambda, \iota : \mathcal{O}_L \longrightarrow \mathrm{End}(Y), \alpha)$ be a quadruple parameterized by ξ. The image of Ξ under $\Psi : \mathcal{M} \to \mathcal{A}$ is a component of the supersingular locus. Therefore, there exists ([KO1], Theorem 2.1) a family $\mathfrak{X} \longrightarrow \mathbb{P}^1$ giving rise to $\Psi(\Xi)$ and m, n, t such that as before we have

$$E_m \times E_n \times \mathbb{P}^1 \stackrel{\tilde{\pi} \times id.}{\longrightarrow} A \times \mathbb{P}^1 \stackrel{\pi}{\longrightarrow} \mathfrak{X}.$$

Let $x \in \mathfrak{X}$ such that x projects to $\Psi(\xi)$. Then $(Y, \lambda, \iota : \mathcal{O}_L \longrightarrow \mathrm{End}(Y), \alpha)$ gives us a module $W_x = \tilde{\pi}^* \pi^* H^1_{Cr}(\mathfrak{X}_{\Psi(\xi)})$ and an endomorphism h preserving W_x and a t adjusted to h. By the generality of ξ, we can get in this way infinitely many such distinct W_ξ with the same h and t (the number of h's and t's is finite) and hence, using Theorem 3.2, we deduce that p is not split in L. Obviously the component Ξ' of $\mathcal{M}$ constructed from E_m, E_n, h and t adjusted to h intersects Ξ at the point ξ. This implies that Ξ' is equal to Ξ. We proved the following

Theorem 5.1. *If p is inert or ramified in L then every component of $\mathcal{S}_{d_L,n}$ is a rational curve and can be parameterized as in Theorem 3.2.* q.e.d.

One says that two families, $\pi_1 : \mathfrak{X}_1 \longrightarrow \mathbb{P}^1 \quad , \pi_2 : \mathfrak{X}_2 \longrightarrow \mathbb{P}^1$, as constructed above, are isomorphic, if there exists an isomorphism, $f : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$, such that the two abelian schemes over $\mathbb{P}_1$, $\mathfrak{X}_1$ and $\mathfrak{X}_2 \times_{\mathbb{P}^1, f} \mathbb{P}^1$, are isomorphic with the polarization, endomorphism structure and level structure. Following [KO1] we get

Theorem 1. *([KO1], Theorem 2.7) Assume that p is inert or ramified in L. The number Ω_n of irreducible components of $\mathcal{S}_{d_L,n}$ is equal to the number of isomorphism classes of families $\mathfrak{X} \longrightarrow \mathbb{P}^1$ with relative polarization, endomorphism and level structure as constructed above.*

5.2. Standard data

Let E be a fixed supersingular elliptic curve over k and put $X = E \times E$. For every m, n we choose and fix an isomorphism

$$\kappa_{m,n} : E_m \times E_n \longrightarrow X.$$

Fix, once and for all, a very good direction a of X. Then for every very good direction b of $(E_m \times E_n, E_m + E_n)$ we fix an automorphism $\Theta_{\kappa_{m,n}(b)}$

such that $\Theta_{\kappa_{m,n}(b)}(\kappa_{m,n}(b)) = a$. Put $\Theta_{m,n,b} = \Theta_{\kappa_{m,n}(b)} \circ \kappa_{m,n}$ – an isomorphism $E_m \times E_n \to X$ taking the very good direction b to a. Let

$$M(m,n) = \left\{ h = \begin{pmatrix} c & \delta \\ \hat{\delta} & -(\epsilon + c) \end{pmatrix} : \right.$$
$$\left. h \in \mathrm{End}(E_m \times E_n), c \in \mathbb{Z}, c^2 + \epsilon c + \delta\hat{\delta} = \Delta \right\}.$$

For every $h \in M(m,n)$ and every t a very good direction adjusted to h, we consider quadruples $(E_m \times E_n, E_m + E_n, h, t)$. We say that $(E_m \times E_n, E_m + E_n, h, t)$ is isomorphic to $(E_m \times E_n, E_m + E_n, h', t')$ if there exists a $\theta \in \mathrm{Aut}(E_m \times E_n)$ such that $\theta_* h \stackrel{\mathrm{def}}{=} \theta h \theta^{-1} = h'$ and $\theta_* t = t'$ where $\theta_* t$ is the direction corresponding to the composition $\theta \circ t$.

One easily checks that

$$(E_m \times E_n, E_m + E_n, h, t) \cong (E_m \times E_n, E_m + E_n, h', t'),$$

if and only if there exists $\tau \in \mathrm{Aut}(X)$, such that under τ

$$(X, \Theta_{m,n,t}(E_m + E_n), \Theta_{m,n,t*}(h), a)$$
$$\cong (X, \Theta_{m,n,t'}(E_m + E_n), \Theta_{m,n,t'*}(h'), a).$$

We consider now the resulting equivalence classes of $(\Theta_{m,n,t}(E_m + E_n), \Theta_{m,n,t*}(h))$. Two such couples are equivalent if and only if there exists a $\tau \in \mathrm{Aut}(X)$ such that $\tau(a) = a$ taking one into the other.

Definition 4. *For every such equivalence class choose a* representative. *Let $\tilde{\pi} : X \longrightarrow A = X/H_a$ be the canonical map. Then*

$$(\tilde{\pi}(\Theta_{m,n,t}(E_m + E_n)), \pi_*(\Theta_{m,n,t*}(h)))$$

will be called a standard data. *Let $\tilde{\mathcal{D}}(m,n)$ be the set of all representatives obtained from the possible $h \in M(m,n)$ and t's adjusted to h. Let*

$$\mathcal{D}(m,n) = \big\{ (\tilde{\pi}\Theta_{m,n,t}(E_m + E_n), \pi_*\Theta_{m,n,t*}(h)) :$$
$$(\Theta_{m,n,t}(E_m + E_n), \Theta_{m,n,t*}(h)) \in \tilde{\mathcal{D}}(m,n) \big\},$$

$$\tilde{\mathcal{D}} = \coprod_{1 \le m \le n \le \hbar} \tilde{D}(m,n), \qquad \mathcal{D} = \bigcup_{1 \le m \le n \le \hbar} D(m,n).$$

Lemma 5.2. *1. The map $\tilde{\mathcal{D}} \longrightarrow \mathcal{D}$ is a bijection.*

2. Let $\tau \in \mathrm{Aut}_v(A)$ and $C, C'' \in \mathcal{D}$. If $\tau(C) = C'$ then $C = C'$ (by definition the action of τ on an endomorphism is given by the action of $\gamma(\tau)$ on that endomorphism).

Proof. We first note that the map $\tilde{\pi} : X \longrightarrow A$ has the following properties:

a. It induces an injective map $Div(X) \longrightarrow Div(A)$.

b. It induces on any $\Theta_{m,n,b}(E_i), i = m, n$ the Frobenius morphism.

Property a and the injectivity of the map $\pi_* : \mathrm{End}(X) \longrightarrow \mathrm{End}(A)$ give part 1 of the lemma.

Let $C = \tilde{\pi}\Theta_{m,n,b}(E_m + E_n, h)$, $C' = \tilde{\pi}\Theta_{m',n',b'}(E_{m'} + E_{n'}, h')$ and let $\tau \in \mathrm{Aut}_v(A)$. Assume that $\tau(C) = C'$. Then property b implies that $m = m'$ and $n = n'$. Now since $\tau(\tilde{\pi}\Theta_{m,n,b}(E_m) \cap \tilde{\pi}\Theta_{m,n,b}(E_n)) = \tilde{\pi}\Theta_{m,n,b}(E_m) \cap \tilde{\pi}\Theta_{m,n,b}(E_n) = \tilde{\pi}(\mathrm{Ker}(Fr : X \longrightarrow X))$ we get that $\tau = \tilde{\pi}_*\tau'$ for some $\tau' \in \mathrm{Aut}_v(X)$ and by property a $\tau'(\Theta_{m,n,b}(E_m + E_n)) = \Theta_{m,n,b'}(E_m + E_n)$. Since $\tau'(0) = \tau'(\Theta_{m,n,b}(E_m) \cap \Theta_{m,n,b}(E_n)) = \Theta_{m,n,b'}(E_m) \cap \Theta_{m,n,b'}(E_n) = 0$, we must have $\tau' \in \mathrm{Aut}(X)$. It then follows that $C = C'$ by the definition of standard data ***q.e.d.***

Following [KO1] one establishes the following

Lemma 2. *([KO1] Lemma 3.7) Let $C' = (E' + E'', g)$ where $E', E'' \in Div(A)$ are two elliptic curves whose sum $E' + E''$ is a symmetric divisor such that $\mathrm{Ker}(\phi_{E'+E''}) \cong \alpha_p \oplus \alpha_p$ and where $g \in \mathrm{End}^0(A)$ descends to an endomorphism of every quotient A/α_p. Assume further that g satisfies the equation $x^2 + \epsilon x - \Delta = 0$ (and hence defines an embedding $L \hookrightarrow \mathrm{End}^0(A)$) and that the polarization defined by $E' + E''$ is $L - linear$. Then there exists a unique standard data $C \in \mathcal{D}$ and an element $\theta \in \mathrm{Aut}_v(A)$ such that $\theta(C) = C'$.*

Using the abelian surface A and a standard data $C \in \mathcal{D}$, we obtain, as above, a family $q : \mathfrak{X} \longrightarrow \mathbb{P}^1$ of principally polarized supersingular abelian surfaces with level n structure and an embedding $\mathcal{O}_L \hookrightarrow \mathrm{End}(\mathfrak{X}/\mathbb{P}^1)$ with a relative principal effective divisor $H \subseteq \mathfrak{X}$. We use the same notation for the "defining map" $\pi : A \times \mathbb{P}^1 \longrightarrow \mathfrak{X}$.

By [MB] the relative divisor $\pi^{-1}(H)$ has exactly $5p-5$ degenerate fibers, each consists of two supersingular elliptic curves whose scheme-theoretic intersection is isomorphic to α_p and all are linearly equivalent to each other. Lets fix the following notation:

$$\mathcal{B}(\mathfrak{X}, H) = \left\{\pi^{-1}(H)_x : \pi^{-1}(H)_x \text{ is reducible}, x \in \mathbb{P}^1\right\},$$

$$\mathcal{D}(\mathcal{B}(\mathfrak{X}, H)) = \left\{C \in \mathcal{D} : \exists C' \in \mathcal{B}(\mathfrak{X}, H), \theta \in \mathrm{Aut}_v(A)\ s.t.\ \theta(C) = C'\right\}$$

(i.e., if $C = (E' + E'', g)$ where $g \in \mathrm{End}^0(A)$ then

$$C' = (\theta(E') + \theta(E''), \gamma(\theta) g \gamma(\theta)^{-1})),$$

$$\Gamma(\mathcal{B}(\mathfrak{X}, H)) = \{\theta \in \mathrm{Aut}_v(A) : \theta \text{ permutes the elements of } \mathcal{B}(\mathfrak{X}, H)\}.$$

To every $C \in \mathcal{D}(\mathcal{B}(\mathfrak{X}, H))$ we can associate an orbit of $\Gamma(\mathcal{B}(\mathfrak{X}, H))$ in its action on $\mathcal{B}(\mathfrak{X}, H)$. Namely, all those $C' \in \mathcal{B}(\mathfrak{X}, H)$ for which there exists a $\theta \in \mathrm{Aut}_v(A)$ such that $\theta(C) = C'$. The fact that these form a single orbit under $\Gamma(\mathcal{B}(\mathfrak{X}, H))$ follows from Lemma 2 and the following theorem (the proof follows [KO1]):

Theorem 3. *([KO1], Theorem 4.1) The group of automorphisms of the family $q : \mathfrak{X} \longrightarrow \mathbb{P}^1$ which preserves the relative polarization on it, is isomorphic to the group $\Gamma(\mathcal{B}(\mathfrak{X}, H))$.*

Convention. We will encounter many automorphism groups G containing ± 1. We will use the notation RG to denote the quotient $G/\pm 1$.
Let $C \in \mathcal{D}(\mathcal{B}(\mathfrak{X}, H))$ then we put $R\Gamma(\mathcal{B}(\mathfrak{X}, H))_C$ to be the stabilizer in $R\Gamma(\mathcal{B}(\mathfrak{X}, H))$ of any element in the orbit associated to C. This is well defined only up to conjugacy but if $C = \tilde{\pi}(\Theta_{m,n,t}(E_m + E_n), \Theta_{m,n,t*}(h))$ then (using the same arguments as in Lemma 5.2) one verifies that this subgroup is isomorphic to $RA(m, n, h, t)$ (defined below).

We have the following mass formula

$$5p - 5 = \sum_{C \in \mathcal{D}(\mathcal{B}(\mathfrak{X}, H))} \frac{|R\Gamma(\mathcal{B}(\mathfrak{X}, H))|}{|R\Gamma(\mathcal{B}(\mathfrak{X}, H))_C|}. \tag{15}$$

5.3. The number of components

Let $\mathfrak{X}_1, ..., \mathfrak{X}_{\Omega_1}$ be the isomorphism classes of families over $\mathbb{P}^1$ giving rise to the components $\Xi_1, ..., \Xi_{\Omega_1}$ of the supersingular locus in $\mathcal{M}_{d_L,1}$. We have a map

$$\Lambda : \mathcal{D} \longrightarrow \{1, ..., \Omega_1\}$$

Let $G(n)$ be the galois group of the covering $\mathcal{M}_{d_L,n} \longrightarrow \mathcal{M}_{d_L,1}$. We denote its order by J_n. Let $\sigma_1(x)$ be the sum of divisors of x for x positive, and zero otherwise. Let $\sigma_{p,1}(x)$ be the sum of divisors which are prime to p for x positive, and zero otherwise.

Let $A(m, n, h, t)$ (*resp.* $A(m, n)$, *resp.* $A(m)$) be the group of automorphisms of $E_m \times E_n$ (*resp.* $E_m \times E_n$, *resp.* E_m) preserving the natural product polarization h and t (*resp.* the natural product polarization, *resp.* no condition).

Theorem 5.3. *Let C_p equal 1 for p inert and $1/2$ for p ramified. Let $n \geq 3$. Let Ω_n be the number of components of $\mathcal{S}_{d_L,n}$. Then*

$$\Omega_n = C_p J_n \, \zeta_L(-1).$$

Proof. As in [KO1], Theorem 4.2, one can prove, using Theorem 3, that

$$R\Gamma(\mathcal{B}(\mathfrak{X}_i)) = G(n)_{\Xi_i}.$$

For convenience we write $Q = Q(n,p) = \frac{J_n}{5p-5}$.

We have

$$\begin{aligned}
\Omega_n &= \sum_{i=1}^{\Omega_1} J_n/|R\Gamma(\mathcal{B}(\mathfrak{X}_i)| \\
&= Q\sum_{i=1}^{\Omega_1} \sum_{x\in\mathcal{D}(\mathcal{B}(\mathfrak{X}_i))} \frac{1}{|R\Gamma(\mathcal{B}(\mathfrak{X}_i))_x|} \\
&= Q\sum_{x\in\mathcal{D}} \frac{1}{|R\Gamma(\mathcal{B}(\mathfrak{X}_{\Lambda(x)}))_x|} \\
&= Q\sum_{1\le m\le n\le\hbar} \sum_{x\in\mathcal{D}(m,n)} \frac{1}{|R\Gamma(\mathcal{B}(\mathfrak{X}_{\Lambda(x)}))_x|} \\
&= Q\sum_{1\le m\le n\le\hbar} \sum_{x\in\mathcal{D}(m,n)} \frac{1}{|RA(m,n,h_x,t_x)|} \quad ,
\end{aligned}$$

where x is constructed from the data $(E_m \times E_n, E_m + E_n, h_x, t_x)$.

We first consider the case of p inert in D.

Define $M(m,n)^+ = \{(h,t)|h \in M(m,n)\ , t \text{ adjusted to } h\}$ (see Subsection 5.2 for the definition of $M(m,n)$). Using the transpose we have $|M(n,m)| = |M(m,n)|$ and $|M(n,m)|^+ = |M(m,n)|^+$. Furthermore, by Theorem 3.2, Case 1.3.2, the map $M(m,n)^+ \longrightarrow M(m,n)$ is 2:1 .
Let

$$w(m,n) = \begin{cases} 2 & m = n \\ 1 & m \neq n \end{cases} .$$

Let $B(k)_{mn}$ denote the mn entry of the k'th Brandt matrix. For basic properties of the Brandt matrices we refer the reader to [Gr].

The group $RA(m,n)$ acts on $M(m,n)^+$ and the class equation for that action reads

$$|M(n,m)^+| = \sum_{x\in\mathcal{D}(m,n)} \frac{|RA(m,n)|}{|RA(m,n,h_x,t_x)|} \quad .$$

Hence, we obtain

$$\Omega_n = Q \sum_{1\le m\le n\le \hbar} \frac{2|M(m,n)|}{|RA(m,n)|} = Q \sum_{m,n=1}^{\hbar} \frac{|M(m,n)|w(m,n)}{|RA(m,n)|} \quad .$$

Let $\Delta(c,\epsilon) = \mathrm{Max}(\Delta - c^2 - \epsilon c, 0)$. We calculate the last expression in the following manner

$$\begin{aligned}
&\frac{|M(n,m)|w(m,n)}{|RA(m,n)|} \\
&= 2\sum_{c\in\mathbb{Z}} \frac{\sharp\{\delta \in \mathrm{Hom}(E_m, E_n) : \deg(\delta) = \Delta(c,\epsilon)\}}{|A(m)|\ |A(n)|} \\
&= 2\sum_{c\in\mathbb{Z}} \frac{\sharp\{H \subseteq E_m :\ |H| = \Delta(c,\epsilon),\ \ E_m/H \cong E_n\}}{|A(m)|} \\
&= 2\sum_{c\in\mathbb{Z}} \frac{B(\Delta(c,\epsilon))_{m,n}}{|A(m)|}
\end{aligned}$$

(the last equality by properties of the Brandt matrices). We now have

$$\begin{aligned}
\Omega_n &= 2Q\sum_{c\in\mathbb{Z}}\sum_{m}\sum_{n} \frac{B(\Delta(c,\epsilon))}{|A(m)|} \\
&= 2\frac{J_n}{5p-5}\sum_{c\in\mathbb{Z}}\ \sum_{m=1}^{\hbar} \frac{1}{|A(m)|}\sigma_{p,1}(\Delta(c,\epsilon)) \\
&= \frac{J_n}{60}\sum_{c\in\mathbb{Z}}\sigma_{p,1}(\Delta(c,\epsilon)) \\
&= \frac{J_n}{60}\sum_{c\in\mathbb{Z}}\sigma_{1}(\Delta(c,\epsilon)) \quad .
\end{aligned}$$

The second equality follows again from properties of the Brandt matrices and the third equality from Eichler's mass formula. The last equality follows from our assumption that p is inert in L. Indeed if $p|\Delta(c,\epsilon)$ then a case by case study shows that D is a square $mod\ p$.

Now use the Siegel-Zagier formula ([Za] p. 69) for $\zeta_L(-1)$ and the observation that writing $d_L = n^2 + 4ac$ is the same as writing $\frac{d_L-1}{4} = m^2 + m + ac$ if $D \equiv 1 \pmod 4, n = 2m+1$ and as $\frac{d_L}{4} = m^2 + ac$ if $D \equiv 2,3 \pmod 4, n = 2m$. We get

$$\Omega_n = J_n\, \zeta_L(-1).$$

We now consider the case $p|D$.
Define

$$M(m,n)_d = \left\{ h \in M(m,n) \mid \deg(\hat{\delta}\delta) = d \right\},$$

and $M(m,n)_d^+$ as the inverse image of $M(m,n)_d$ in $M(n,m)^+$. By Theorem 3.2, Cases 1.2.1 and 1.3.1, we have

$$|M(m,n)_d^+| = \begin{cases} (p+1)\,|M(m,n)_d| & p||d \\ |M(m,n)_d| & (p,d)=1 \end{cases} .$$

From the definition we have

$$|M(m,n)| = \sum_{c\in\mathbb{Z}} |M(m,n)_{\Delta(c,\epsilon)}|.$$

We also define

$$\mathcal{D}(m,n)_d = \left\{ x \in \mathcal{D}(m,n) \mid \deg(\delta_x\hat{\delta}_x) = d \right\},$$

where x is constructed from (m,n,h_x,t_x) and $h_x = \begin{pmatrix} c_x & \delta_x \\ \hat{\delta}_x & -(\epsilon+c_x) \end{pmatrix}$. One easily verifies that $RA(m,n)$ acts on $M(m,n)_d^+$ and the corresponding class equation is

$$|M(m,n)_d^+| = \sum_{x\in\mathcal{D}(m,n)_d} \frac{|RA(m,n)|}{|RA(m,n,h_x,t_x)|} .$$

Using this equation we obtain as before

$$\begin{aligned}
\Omega_n &= \sum_{1\le m\le n\le\hbar} \frac{|M(m,n)^+|}{|RA(m,n)|} \\
&= Q \sum_{m,n=1}^{\hbar} \frac{|M(n,m)^+|w(m,n)}{2|RA(m,n)|} \\
&= Q \sum_{m,n} \sum_{c\in\mathbb{Z}} \frac{|M(m,n)^+_{\Delta(c,\epsilon)}|w(m,n)}{2|RA(m,n)|} \\
&= Q \sum_{m,n} \left(\sum_{\{c:p\nmid\Delta(c,\epsilon)\}} \frac{B(\Delta(c,\epsilon))_{m,n}}{|A(m)|} \right. \\
&\qquad \left. + \sum_{\{c:p|\Delta(c,\epsilon)\}} \frac{(p+1)B(\Delta(c,\epsilon))_{m,n}}{|A(m)|} \right)
\end{aligned}$$

$$= \frac{J_n}{5p-5}\sum_m \left(\sum_{\{c:p\nmid \Delta(c,\epsilon)\}} \frac{\sigma_{p,1}(\Delta(c,\epsilon))}{|A(m)|} + \sum_{\{c:p|\Delta(c,\epsilon)\}} \frac{(p+1)\sigma_{p,1}(\Delta(c,\epsilon))}{|A(m)|} \right)$$

$$= \frac{J_n}{120}\left(\sum_{\{c:p\nmid \Delta(c,\epsilon)\}} \sigma_{p,1}(\Delta(c,\epsilon)) + \sum_{\{c:p|\Delta(c,\epsilon)\}} (p+1)\sigma_{p,1}(\Delta(c,\epsilon)) \right).$$

We note that since D is square free it is easy to verify from equation (5) that if $p|\Delta(c,\epsilon)$ then $p||\Delta(c,\epsilon)$. Therefore , for such $\Delta(c,\epsilon)$

$$\sigma_1(\Delta(c,\epsilon)) = \sigma_1(p)\sigma_1(\Delta(c,\epsilon)/p) = (p+1)\sigma_1(\Delta(c,\epsilon)/p),$$

and

$$\sigma_{p,1}(\Delta(c,\epsilon)) = \sigma_1(\Delta(c,\epsilon)/p).$$

Hence , for such $\Delta(c,\epsilon)$

$$(p+1)\sigma_{p,1}(\Delta(c,\epsilon)) = \sigma_1(\Delta(c,\epsilon)).$$

The result now follows from the Siegel-Zagier formula as before. *q.e.d.*

6. Local structure of the supersingular locus

In this section we study the supersingular locus for p inert or ramified. We begin by giving a short proof of the structure theorem of Stamm (see [St]) for the inert case.

6.1. The inert case

Assume p is inert in L.

Theorem 6.1. *The set of singular points of $\mathcal{S}$ is exactly the set of supersingular points. Every singularity is ordinary with two branches and corresponds to the intersection of different components.*

To every component one can assign an invariant in $\{1,2\}$ – called the type – such that the intersection graph of $\mathcal{S}$ is bipartite. Each component has exactly p^2+1 intersection points with other components.

Proof. Write $\mathrm{Emb}(\mathcal{O}_L, W(\overline{\mathbb{F}_p})) = \{\sigma_1, \sigma_2\}$. We say that a supersingular point x with $a(A_x) = 1$ is of type i if $\mathcal{O}_L$ acts on $\mathcal{D}(\alpha(A_x))$ via σ_i. The type is locally constant on the set of such points, hence we may speak of the type of a component.

Now let X/k be a supersingular geometric point and $\mathbb{D}$ the *covariant* Dieudonné module of the p-divisible group of A_x. We use the theory of displays as in [N],[NO](see also [GO]) to study equi-characteristic deformations.

We have the decomposition

$$\mathcal{O}_L \otimes W(k) \cong W(k) \oplus W(k),$$

which induces a decomposition

$$\mathbb{D} = \mathbb{D}_1 \oplus \mathbb{D}_2.$$

Note that $\mathbb{D}_i$ is a free module of degree 2 over $W(k)$. The following properties hold: $F(\mathbb{D}_i) \subset \mathbb{D}_{i+1}$, $\dim_k(\mathbb{D}_{i+1}/F(\mathbb{D}_i)) = 1$, $V(\mathbb{D}_{i+1}) \subset \mathbb{D}_i$, $\dim_k(\mathbb{D}_i/V(\mathbb{D}_{i+1})) = 1$. Furthermore, the pairing $\mathbb{D} \times \mathbb{D} \to W(k)$ defined by the given principal polarization on A_x induces a perfect symplectic pairing on each $\mathbb{D}_i$.

Choose a symplectic $W(k)$ basis x_i, y_i for $\mathbb{D}_i$ such that $y_i \in V(\mathbb{D}_{i+1})$. Note that the Dieudonné module is then displayed by

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} 0 & f_{12} & 0 & f_{14} \\ f_{21} & 0 & f_{23} & 0 \\ 0 & f_{32} & 0 & f_{34} \\ f_{41} & 0 & f_{43} & 0 \end{pmatrix}.$$

Using the deformation theory in loc.cit., one checks that the universal equi characteristic local deformation ring of $(A_x, \lambda_x, \iota_x)/k$ is $\mathrm{Spec}(k[[t_1, t_2]])$ and the Dieudonné module of the p-divisible group of the universal deformation is displayed by

$$\begin{pmatrix} A + TC & B + TD \\ C & D \end{pmatrix},$$

where $T = diag(T_1, T_2)$, T_i the Teichmuller lift of t_i. In particular the determinant of the Hasse-Witt matrix, $A + TC$, is

$$-(f_{12} + t_1 f_{32})(f_{21} + t_2 f_{41}) \pmod{p}.$$

Assume that $a(A_x) = 1$ and w.l.o.g that x is of type 1, hence $p | f_{12}, p \not| f_{21}$. Note that $p \not| f_{41}$ becuase the rank of Frobenius mod p is 2. Thus, the determinant of the Hasse-Witt matrix is

$$-t_1 f_{32}(f_{21} + t_2 f_{41}) \pmod{p}.$$

Since $(f_{21} + t_2 f_{41})$ is invertible in $k[[t_1, t_2]]$, the closed subscheme where the determinant vanishes is given by (t_1) and in particular is smooth. If $a(A_x) = 2$, then the determinant is

$$-t_1 t_2 f_{32} f_{41} \pmod{p},$$

and the supersingular locus is given locally by $(t_1 t_2)$. It is thus an ordinary singularity with two branches of different type, hence the graph is bipartite and everything follows. *q.e.d.*

6.2. The ramified case

Assume that p is ramified in L. We study the local deformation theory using [Gk] and [Ko].

Theorem 6.2. *For a geometric point x of $\mathcal{M}$ the following are equivalent:*

(i) It is a singular point of the surface;

(ii) The action of $\mathcal{O}_L/p$ on $H^0(\Omega^1_{A_x})$ is not free;

(iii) It is a singular point of the supersingular locus.

When this holds x is in fact superspecial, the tangent cone of the surface at x is isomorphic to $z^2 = xy$ and the singularity of $\mathcal{S}$ at x is ordinary with $p + 1$ branches. On each component there are $p + 1$ values of its parameterization such that the corresponding point satisfies the above.

Proof. Let x be an ordinary point. We first show that x is smooth and $H^0(\Omega^1_{A_x})$ is free over $\mathcal{O}_L/p$ hence we may assume x is supersingular. Indeed, by the density of the Hecke orbit of x, x must be smooth (see proof of Theorem 4.2). If $H^0(\Omega^1_{A_x})$ is not free then it is killed by $\sqrt{D}$. But $H^0(\Omega^1_{A_x}) = \mathcal{D}(A_x[p]_{\text{lé}})$ therefore $\sqrt{D}$ kills $A_x[p]_{\text{él}}$ as well. Hence $p|\sqrt{D}$. A contradiction.

Assume $x \in \mathcal{S}$. We assume that $\epsilon = 0$, the case $\epsilon = 1$ is similar. As in Subsection 2.4, let $W = \text{Span}_{W(k)} \left\{ pH^1_{Cr}(X), v, w \right\}$ be the first crystalline cohomology of an abelian variety A, which is obtained from the data $(X = E_1 \times E_2, \mu(E_1, E_2), h, t, r)$, embedded in $H^1_{Cr}(X)$.

We first treat components arising from Case (1.3.1) of Theorem 3.2.

We assume that we have chosen a basis (e_1, Fe_1, e_2, Fe_2) for $H^1_{Cr}(X)$ which is distinguished and with respect to which h is given as in Case (1.3.1) of Theorem 3.2, Formula 9.

We also have $B_{E_i}(e_i, Fe_i) = \theta_i$. One may further assume that $\theta_1 = 1$ and hence $\theta_2 = d \pmod{p}$.

Assume $r \neq 0$ (equivalently $a_2 = 1$).

In this case one may verify that the vectors

$$\{pe_1, pFe_1, -T^\sigma Fe_1 + Fe_2, -Te_1 + a_1 Fe_1 + e_2\}$$

form a basis for W/pW. Let us denote these vectors by $\gamma_1, ..., \gamma_4$ respectively.

Reducing mod pW, one finds the following matrix for the action of Frobenius on W/pW with respect to the γ_i

$$F|_{\gamma_i} = \begin{pmatrix} 0 & 0 & 0 & -a_1^{\sigma} \\ 1 & 0 & a_1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \tag{16}$$

We note that $\mathrm{Ker}F|_{W/pW} = \mathrm{Span}_k(\beta_1, \beta_2)$, where $\beta_1 = \gamma_2$, $\beta_2 = a_1^{\sigma^{-1}}\gamma_1 - \gamma_3$. We want to complete β_1, β_2 to a symplectic basis for W/pW. First we compute the matrix of the alternating form with respect to the γ_i to be

$$\begin{pmatrix} 0 & 0 & -T^{\sigma} & a_1 \\ 0 & 0 & 0 & T \\ T^{\sigma} & 0 & 0 & -(T^{\sigma+1}+d)/p \\ -a_1 & -T & (T^{\sigma+1}+d)/p & 0 \end{pmatrix}. \tag{17}$$

We note that in our case setting $T = -c$ – which lifts equation (12) of Case (1.3) of Theorem 3.2 – we obtain $(T^{\sigma+1}+d)/p = D/p$ and we let

$$s = D/p, \;\; \ell = -(a_1^{1+1/p} + s), \;\; k = a_1/t.$$

We then compute that

$$\beta_3 = \frac{-\ell}{t^{p+1}}\gamma_1 + \frac{1}{t}\gamma_4 \;,\; \beta_4 = \frac{-1}{t^p}\gamma_1 + \frac{a_1}{t^{p+1}}\gamma_2,$$

complete β_1, β_2 to a symplectic basis .

The matrix of h with respect to the β_i is given by

$$h_{\{\beta_i\}} = \begin{pmatrix} 0 & \ell & 0 & k \\ 0 & 0 & -k & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & \ell & 0 \end{pmatrix},$$

and Frobenius is given by

$$F_{\{\beta_i\}} = \begin{pmatrix} 0 & B \\ 0 & H \end{pmatrix} = \begin{pmatrix} 0 & 0 & \ell/d & -1/t \\ 0 & 0 & -1/t & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & a_1^p - a_1^{1/p} & 0 \end{pmatrix}.$$

We now look at deformations. Since $W = H^1_{Cr}(A)$, we have $W/pW = H^1_{dR}(A)$. By our choice of basis $H^0(\Omega^1_A) = \mathrm{Ker}F|_{W/pW} = \mathrm{Span}_k(\beta_1, \beta_2)$.

A deformation $A(U)$ of the abelian variety A over the ring $k[\delta]/(\delta^2)$ is given by a sub - $k[\delta]/(\delta^2)$- module of $H^1_{dR}(A) \otimes k[\delta]/(\delta^2)$ extending $H^0(\Omega^1_A)$, viz., by a basis of the form

$$\begin{pmatrix} 1 \\ 0 \\ u_{11} \\ u_{21} \end{pmatrix}, \quad \begin{pmatrix} 0 \\ 1 \\ u_{12} \\ u_{22} \end{pmatrix},$$

which will be denoted $\beta_1(U), \beta_2(U)$. Here $u_{ij} \in (\delta)$ and we put $u_{ij} = \delta b_{ij}, b_{ij} \in k$. By [DP], the deformations as a principally polarized abelian varieties are given by the condition $u_{12} = u_{21}$ and among them, the deformations lying on our Hilbert-Blumenthal surface, are given by the submodules invariant under h (or $h \otimes 1$ to be exact).

Writing the equations

$$h\beta_i(U) = x_i\beta_1(U) + y_i\beta_2(U),$$

we obtain

$$x_1 = ku_{12},\ y_1 = -ku_{11}\ ,\ \ x_2 = \ell + ku_{22},\ y_2 = -ku_{22}, \tag{18}$$

and the condition

$$ku_{12}^2 - ku_{11}u_{22} - \ell u_{11} = 0.$$

Hence, the points which satisfy

$$\ell = 0,$$

or, equivalently,

$$a_1^{p+1} = -s,$$

are precisely the supersingular points at which the surface is singular. Note that since $s \in \mathbb{F}_p$, all the solutions a_1 to the equation lie in $\mathbb{F}_{p^2}$, hence the points are superspecial. At nonsingular points we obtain

$$u_{11} = 0. \tag{19}$$

Consider the matrix Y such that

$$\delta Y = UB.$$

Using the computation of Frobenius and equation (19) we obtain

$$Y = \begin{pmatrix} -b_{12}/t & 0 \\ \ell b_{12}/d - b_{22}/t & -b_{12}/t \end{pmatrix}$$

(here the b_{ij} are not the entries of B but, defined by $u_{ij} = \delta b_{ij}$). By a simple calculation,

$$YY^{(p)} = 0 \Leftrightarrow b_{12} = 0.$$

Hence, at these nonsingular points (of the surface), the supersingular locus is nonsingular as well.

Returning to the case of the singular points, by [DP], Theorem 3.3, the deformations (of all orders) of the Hilbert-Blumenthal surface at A are given by the isotropic h invariant deformations of $H^0(\Omega^1_A)$. Computing to the second order, using the x_i and y_i computed in equation (18) above, we obtain

$$u_{12}^2 = u_{11}u_{22}. \tag{20}$$

Note that by the symmetry of the matrix U, equation (20) is equivalent to the statement that U has rank at most 1. Since the matrix B is nonsingular (we are at a superspecial point) all solutions to $YY^{(p)} = 0$ must come from matrices U which have rank at most 1. Hence we obtain $p + 1$ branches as in [Ko] Pg. 193.

Note that in the ramified case $\mathcal{O}_L \otimes \bar{\mathbb{F}}_p$ is isomorphic to $\bar{\mathbb{F}}_p[\delta]/(\delta^2)$, and under the isomorphism $h = \sqrt{D}$ is sent to δ (note that we are assuming that $\epsilon = 0$). Therefore, the action of $\mathcal{O}_L$ on the cotangent space is free if the action of h is nonzero. The action of h is given by

$$\begin{pmatrix} 0 & \ell \\ 0 & 0 \end{pmatrix},$$

and hence the action is not free precisely when

$$\ell = 0.$$

That is, precisely at the singular points of the surface (as expected from the discussion in [DP]).

The case $a_2 = 0$ is treated similarily and the computations (which are easier) show that both the surface and the supersingular locus are smooth.

We now consider Case (1.2.1) of Theorem 3.2.
Assume first that $a_2 \neq 0$.

We assume that the distinguished bases where chosen so that h has the same form as in Case (1.2.1) of Theorem 3.2, Formula 6, and that

$$\theta_1 = 1 \ , \ \theta_2 = m \ , \ T^{\sigma+1} = -d/p.$$

We choose the same γ_i as before and hence the computation of Frobenius, the alternating form and the symplectic basis remain intact if we replace d by d/p.
We then compute h to be

$$\begin{pmatrix} 0 & t^p(a_1 + a_1^{1/p} + 2c/p) & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & t^p(a_1 + a_1^{1/p} + 2c/p) & 0 \end{pmatrix}.$$

Setting $\ell = t^p(a_1 + a^{1/p} + 2c/p)$ and $k = 1$ we notice that we obtain precisely the situation of Case (1.3.1), which we have analyzed above. Hence, the surface is singular at the points where $\ell = 0$. Note that all the solutions a_1 to the equation are in $\mathbb{F}_{p^2}$ and hence the points are superspecial. The singularity is of the form

$$b_{12}^2 = b_{11}b_{22},$$

as before. Following the argument presented in Case (1.3.1) we obtain $p+1$ branches of the supersingular locus at these points.

Finally let $a_2 = 0$. We choose our basis as follows:

$$pe_1,\ pe_2,\ Fe_1,\ \frac{1}{d}Fe_2,$$

where $\{e_1, Fe_1, e_2, Fe_2\}$ is a distinguished basis. One may calculate that h is given by

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Hence, the surface and locus singularities are as before. We also note that the point corresponding to $a_2 = 0$ under the parameterization arising from (X, μ, h, t) is independent of t (it is the image under Frobenius of (X, μ)). One may then easily verify by calculating the branches directly in terms of t that different t's give rise to different branches. *q.e.d.*
G. Pappas has informed us that the structure of the tangent cone was sketched in a letter of his to Deligne.

Using Theorems 5.3, 6.1 and 6.2, we get

Corollary 6.3. *Let $n \geq 3$ and p be inert or ramified in L. The number of singular points of $\mathcal{S}_{d_L,n}$ is*

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

where $D_p = (p^2+1)/2$ if p is inert and $D_p = 1/2$ if p is ramified.

7. Appendix

Consider a slightly different moduli problem:

Let R_m be the order of conductor m in $\mathcal{O}_L$, and consider triples (A, λ, ι) and a level n structure, where (A, λ) is a principally polarized abelian surface and $\iota : R_m \hookrightarrow \mathrm{End}(A)^\lambda$. Such an embedding is determined by the image of $m\Lambda$, which after pullback to X, as in Sect. 3.2, has the form

$$\frac{1}{p}\begin{pmatrix} a & \beta \\ \hat{\beta} & -(mp\epsilon + a) \end{pmatrix},$$

where $a \in \mathbb{Z}$, $\beta \in \mathrm{Hom}(E_2, E_1)$, $a^2 + mp\epsilon + b = m^2p^2\Delta$ and $\deg(\beta) = b$.

The resulting moduli space is an algebraic stack (non-reduced if $p|m$), which we denote by $\mathcal{M}_{md_L,n}$. We leave details about the construction and structure of these stacks for a future paper.

The following theorem is proved using the methods of Theorem 3.2.

Theorem 7.1. *The following sets of data (X, μ, h, t, r) correspond to points on the Hilbert-Blumenthal surface of conductor m:*
1) If $(m, p) = 1$, then we obtain the same results as in Theorem 3.2, where we replace ϵ by $m\epsilon$.
2) If $(m, p) = p$, then:
2.A) If $(p, b) = 1$, we get the same sets as in Case 2 of Theorem 3.2. In particular, we obtain no new components.
2.B) If $ord_p(b) = 2$, we get a single very good direction, which leads to a component. It is given by $t = -c - m\epsilon/2$.
2.C) If $ord_p(b) \geq 4$, all sets of data lead to components.

Using this theorem and the methods of Sect. 5.3, one can count the number of components of the supersingular locus (with reduced structure) of $\mathcal{M}_{md_L,n}$. We now state the results for p inert in L.

Following [Co], let

$$c_1(n) = \sum_{0 \leq n-k^2 \equiv 0 \pmod 4} \sigma_1\left(\frac{n-k^2}{4}\right).$$

Let $a_n = \frac{1}{60}c_1(n)$ and $\zeta_{L,m}$ be the zeta function of the order R_m (see [Co], Sect. 3). Then, for $(m, p) = 1$, we have:

Theorem 7.2. *The number of components of the supersingular locus in* $\mathcal{M}_{md_L,n}$ *is*

$$[\mathcal{M}_{md_L,n} : \mathcal{M}_{md_L,1}]a(m^2 d_L),$$

and the number of components for which R_m *is optimally embedded in the endomorphism ring of the generic point is*

$$[\mathcal{M}_{md_L,n} : \mathcal{M}_{md_L,1}]m^3\zeta_{L,m}(-1).$$

We also remark that for $m = p$ we obtain that the number of components is

$$1/2[\mathcal{M}_{md_L,n} : \mathcal{M}_{md_L,1}]\left(a(p^2 d_L) - p^2 a(d_L)\right)$$

($a(d_L) = \zeta_L(-1)$). Finally, we note that the $c_1(n)$'s form the Fourier coefficients of a weight 5/2 modular form on $\Gamma_0(4)$ (see [Co], Sect. 4).

References

[Ch] Chai, C.-L.: Every ordinary symplectic isogeny class in positive characteristic is dense in the moduli, Invent. Math. **121** (1995), 439–479

[Co] Cohen H.: Variations sur un thème de Siegel et Hecke, Acta Arithmetica, **30** (1976), 63–93

[Dm] Demazure, M.: Lectures on p-divisible groups, Lecture Notes in Math. **302**, Springer Verlag, 2nd printing 1986

[DP] Deligne, P., Pappas, G.: Singularités des espaces de modules de Hilbert, en les caractéristiques divisant le discriminant, Compositio Math. **90** (1994), 59–74

[Gk] Grothendieck, A.: Groupes de Barsotti-Tate et cristaux de Dieudonné, Les Presses de l'Univ. de Montréal, 1974

[GO] Goren, E.-Z., Oort, F.: Stratifications of Hilbert modular varieties in positive characteristic I, In preparation

[Gr] Gross, B.-H.: Heights and the special values of L-series, Canadian Mathmatical Society, Conference Proceedings volume **7** (1987), 115–187

[KO1] Katsura, T., Oort, F.: Families of supersingular abelian surfaces, Compositio Math. **62** (1987), 107–167

[KO2] Katsura, T., Oort, F.: Supersingular abelian varieties of dimension two or three and class numbers, Advanced Studies in Pure Math. **10** (1987), Algebraic Geometry, Sendai (1985), 253–281

[Ko] Koblitz, N.: P-adic variation of the zeta-function over families of varieties defined over finite fields, Compositio Math. **31** (1975), 119–218

[MB] Moret-Bailly, L.: Familles de courbes et de variétés abéliennes sur $\mathbb{P}^1$, Asterisque **86** (1981), exposés n^{o} 7 & 8, 109–140

[N] Norman, P.: An algorithm for computing local moduli of abelian varieties, Ann. of Math. **101** (1975), 499–509

[NO] Norman, P., Oort F.: Moduli of abelian varieties, Annals of Math. **112** (1980), 413–439

[Ra] Rapoport, M.: Compactifications de l'espace de modules de Hilbert-Blumenthal, Compositio Math. **36** (1978), 255–335

[St] Stamm, H.: On the reduction of the Hilbert-Blumenthal moduli scheme with $\Gamma_0(p)$ level structure, Forum Math. **9** (1997), 405–455

[vG] van der Geer, G.: Hilbert modular surfaces, Ergebnisse der Mathematik und ihrer Grenzgebiete, 3.Folge, Band 16, Springer Verlag, 1988

[Za] Zagier, D.: On the values at negative integers of the zeta-function of a real quadratic field, L'ens. Math **22** (1976) 55–95