Bimodules and Abelian Surfaces *

Kenneth A. Ribet†

To Professor K. Iwasawa

Introduction

In a manuscript on mod ℓ representations attached to modular forms [26], the author introduced an exact sequence relating the mod p reduction of certain Shimura curves and the mod q reduction of corresponding classical modular curves. Here p and q are distinct primes. More precisely, fix a maximal order $\mathcal{O}$ in a quaternion algebra of discriminant pq over $\mathbf{Q}$. Let M be a positive integer prime to pq. Let $\mathcal{C}$ be the Shimura curve which classifies abelian surfaces with an action of $\mathcal{O}$, together with a "$\Gamma_o(M)$-structure." Let $\mathcal{X}$ be the standard modular curve $X_o(Mpq)$. These two curves are, by definition, coarse moduli schemes and are most familiar as curves over $\mathbf{Q}$ (see, for example, [28], Th. 9.6). However, they exist as schemes over $\mathbf{Z}$: see [4, 6] for $\mathcal{C}$ and [5, 13] for $\mathcal{X}$.

In particular, the reductions $\mathcal{C}_{\mathbf{F}_p}$ and $\mathcal{X}_{\mathbf{F}_q}$ of $\mathcal{C}$ and $\mathcal{X}$, in characteristics p and q respectively, are known to be complete curves whose only singular points are ordinary double points. In both cases, the sets of singular points may be calculated in terms of the arithmetic of "the" rational quaternion algebra which is ramified precisely at q and ∞. (There is one such quaternion algebra *up to isomorphism*.) In [26], the author observed that these calculations lead to the "same answer" and concluded that there is a 1-1 correspondence between the two sets of singular points. He went on to relate the arithmetic of the Jacobians of the two curves $\mathcal{X}$ and $\mathcal{C}$ (cf. [14] and [10, 11]).

The correspondence of [26] depends on several arbitrary choices. More precisely, [26] used Drinfeld's theorem [6] to view the Shimura curve $\mathcal{C}$ over $\mathbf{Z}_p$ as the quotient of the appropriate "p-adic upper half-plane" by a discrete

*This version printed January 6, 2004

†Partially supported by the NSF

subgroup Γ of $\mathbf{PGL}_2(\mathbf{Q}_p)$. This group is obtained by choosing: (1) a rational quaternion algebra $\mathcal{H}$ of discriminant q, (2) an Eichler order in $\mathcal{H}$ of level M, and (3) an isomorphism $\mathcal{H} \otimes \mathbf{Q}_p \approx \mathrm{M}(2, \mathbf{Q}_p)$. The conjugacy class of Γ in $\mathbf{PGL}_2(\mathbf{Q}_p)$ is independent of these choices, but there is no *canonical* way to move between two different Γ's. This flabbiness makes awkward the verification that the correspondence of [26] is compatible with the natural actions of Hecke operators T_n on $\mathcal{X}$ and on $\mathcal{C}$.

The main conclusion of this article (Theorem 5.5, Theorem 5.3) is that the singular points in $\mathcal{X}(\overline{\mathbf{F}}_q)$ and $\mathcal{C}(\overline{\mathbf{F}}_p)$ are *canonically* in bijection, once one chooses the algebraically closed fields $\overline{\mathbf{F}}_p$ and $\overline{\mathbf{F}}_q$ to be algebraic closures of the two residue fields $\mathbf{F}_{p^2}$ and $\mathbf{F}_{q^2}$ of $\mathcal{O}$. A choice of this type appears quite natural if one considers the related, but simpler, problem of comparing the singular points of $\mathcal{X}(\mathbf{F})$ and $\mathcal{X}(\mathbf{F}')$ when $\mathbf{F}$ and $\mathbf{F}'$ are two algebraic closures of $\mathbf{F}_q$. These are the isomorphism classes of supersingular elliptic curves with $\Gamma_o(M)$-structures, over $\mathbf{F}$ and $\mathbf{F}'$, respectively. For a general prime number q, the isomorphism classes are defined only over the quadratic extensions of $\mathbf{F}_q$ in $\mathbf{F}$ and $\mathbf{F}'$, and the isomorphism classes cannot be identified until we choose an isomorphism between the two different fields $\mathbf{F}_{q^2}$.

We also discuss the analogous problem of expressing the set of components of $\mathcal{C}_{\overline{\mathbf{F}}_q}$ in terms of the singular points of $X_o(Mq)$ in characteristic q. Further, we treat the generalization of the two problems, first indicated by Jordan and Livné, to the case where the discriminant of $\mathcal{O}$ is of the form pqD, D being a product of an even number of distinct primes which are prime to pqM. For the generalization, we use a result indicated by Deligne-Rapoport in §7 of the Introduction to [5]. Although this result is not proved in [5], it was obtained by Morita in his unpublished thesis [18]. It may also be established by the techniques of [3].

As already indicated, we compare objects in characteristics p and q by relating them both to quaternion arithmetic. We take a point of view which is borrowed from Mestre-Oesterlé [17], involving what we call "oriented orders." As an illustration, consider the problem of classifying, up to isomorphism, supersingular elliptic curves over an algebraic closure $\mathbf{F}$ of $\mathbf{F}_q$.

This problem was solved by Deuring, and the solution is usually phrased in terms of a base point, i.e., a fixed supersingular elliptic curve E_o. The ring $R_o = \mathrm{End}(E_o)$ is a maximal order in the rational quaternion algebra $R_o \otimes \mathbf{Q}$, which is ramified precisely at q and ∞. To each supersingular elliptic curve, one associates the locally free rank-1 left R_o-module $\mathrm{Hom}(E, E_o)$. This association sets up a bijection between isomorphism classes of supersingular elliptic curves and left R_o-modules of the indicated type.

In the variant due to Mestre and Oesterlé, one dispenses with E_o and associates to each E its endomorphism ring R, plus the map $\phi\colon R \to \mathbf{F}$ which gives the action of R on the 1-dimensional $\mathbf{F}$-vector space $\mathrm{Lie}(E/\mathbf{F})$. The map ϕ takes values, necessarily, in the quadratic subfield $\mathbf{F}_{q^2}$ of $\mathbf{F}$. The pair (R, ϕ) is an "oriented maximal order" in a rational quaternion algebra of discriminant q. Deuring's theorem may be rephrased as the assertion that the construction $E \mapsto (R, \phi)$ induces a bijection between isomorphism classes of supersingular elliptic curves over $\mathbf{F}$ and oriented maximal orders of discriminant q.

In a mild generalization, one can classify supersingular elliptic curves with $\Gamma_o(Mp)$-structures; the result involves "oriented Eichler orders of level Mp" in a quaternion algebra of discriminant q. Here, by the result of Deligne and Rapoport [5], the objects being classified are naturally the singular points of $\mathcal{X}_{\mathbf{F}}$.

To complete the picture, we must relate the singular points of $\mathcal{C}_{\overline{\mathbf{F}}_p}$ to oriented orders. As shown by the method of Drinfeld [6] (cf. [31], Satz 3.10), these points are represented by those $\mathcal{O}$-abelian surfaces A (furnished with $\Gamma_o(M)$-structures) which satisfy the following property: Let σ be one of the two homomorphisms $\mathcal{O} \rightrightarrows \overline{\mathbf{F}}_p$. Then there is an $\mathcal{O}$-stable subgroup H of A, isomorphic to α_p, such that the homomorphism

$$\mathcal{O} \to \mathrm{End}(H) = k$$

giving the action of $\mathcal{O}$ on H coincides with σ.

In §4, we treat the problem of classifying such "mixed exceptional" objects, and show especially that they are classified by their endomorphism rings (viewed as oriented orders). The endomorphism rings are Eichler orders of level Mp in a rational quaternion algebra of discriminant q, just as above. We recover a result which is implicit in the existing literature in a base-point dependent form (cf. [31], §4).

The proof we have given for this classification theorem is direct, and perhaps unnecessarily long. In essence, we remark that A is isomorphic to the product $E \times E$, where E is a supersingular elliptic curve over $\overline{\mathbf{F}}_p$, which we can take to be fixed. If R is the endomorphism ring of E, to give an action of $\mathcal{O}$ on A is then to give an $(\mathcal{O}, R)$-bimodule which is $\mathbf{Z}$-free of rank 8. Such bimodules are presumably difficult to classify in general, since the tensor product $\mathcal{O} \otimes R$ is not a hereditary ring. (Recall that a ring is said to be left-hereditary if all left ideals of the ring are projective modules.) Fortunately, the condition satisfied by A implies that the corresponding bimodule

is "admissible" (in the sense of §2). We show in §2 that admissible rank-8 bimodules are classified by the endomorphism rings, viewed as oriented orders.

The author wishes to thank Professors C.J. Bushnell, N.M. Katz, R. Livné, B. Mazur, J. Oesterlé, and F. Oort for helpful conversations and correspondence. He also thanks the Max Planck Institute in Bonn, the IHES, and the Université de Paris XI for invitations during the preparation of this article.

Contents

1 Local Study of Certain Bimodules

Let p be a prime. Let $\mathcal{O}$ be a maximal order in a quaternion division algebra B over $\mathbf{Q}_p$. Let $\wp$ be the maximal ideal of $\mathcal{O}$ and let $\mathbf{F}_{p^2}$ be the residue field of $\wp$. Let π be a uniformizer of $\wp$. We can, and do, assume that $\pi^2 = p$. (For background on the arithmetic of quaternion algebras over local fields, see for example [30], Ch. II.)

A classification theorem

Recall that $B \otimes_{\mathbf{Q}_p} B$ is a matrix algebra (of degree 4) over $\mathbf{Q}_p$. Indeed, let $'$ denote the involution of B for which

$$x \mapsto xx'$$

is the reduced norm in B. The map $'$ thus induces an isomorphism between B and its opposite algebra. Define

$$\mu\colon B \otimes_{\mathbf{Q}_p} B \to \mathrm{End}_{\mathbf{Q}_p}(B)$$

by sending $x \otimes y$ to the composition of left multiplication by x and right multiplication by y'. The map μ is easily seen to be an isomorphism.

Let

$$\mathcal{C} = \mathcal{O} \otimes_{\mathbf{Z}_p} \mathcal{O}$$

and identify $\mathcal{C}$ with its image under μ. The ring $\mathcal{C}$ is visibly contained in the hereditary order

$$\mathcal{A} = \left\{\varphi \in \mathrm{End}_{\mathbf{Z}_p}(\mathcal{O}) \mid \varphi(\wp) \subseteq \wp\right\},$$

since $\wp$ is a 2-sided ideal of $\mathcal{O}$. (For background on hereditary orders, see [25] and [2], §1.2.)

It is to be noted, in fact, that $\mathcal{C}$ is strictly contained in $\mathcal{A}$. Indeed, $\mathcal{C}$ lies in the sub-order of $\mathcal{A}$ consisting of those $\varphi \in \mathcal{A}$ which induce $\mathbf{F}_{p^2}$-linear endomorphisms (i.e., homotheties) on the quotients $\mathcal{O}/\wp = \mathbf{F}_{p^2}$ and $\wp/\wp^2$.

Let θ be the element $\pi^{-1} \otimes \pi$ of $B \otimes_{\mathbf{Q}_p} B$. Viewed as an element of $\mathrm{End}_{\mathbf{Q}_p}(B)$, θ lies in $\mathcal{A}$, since it preserves both $\mathcal{O}$ and $\wp$. Note that θ is an involution, since $\pi^2 = p$ lies in the center of B.

PROPOSITION **1.1** *The ring $\mathcal{A}$ is generated by $\mathcal{C}$, together with the involution θ.*

Proof. Let W be the ring of Witt vectors over $\mathbf{F}_{p^2}$, i.e., the ring of integers of the unramified quadratic extension K of $\mathbf{Q}_p$. Let σ be the Frobenius automorphism of W: the non-trivial automorphism of K over $\mathbf{Q}_p$. We may view $\mathcal{O}$ explicitly as $W \oplus W\pi$, where the multiplication in $\mathcal{O}$ is such that we have

$$a\pi = \pi(\sigma a)$$

for $a \in W$. Once $\mathcal{O}$ is written this way, we have in particular an embedding $W \hookrightarrow \mathcal{O}$. We use this embedding to view $\mathcal{O}$ as a left W-module; it is a free W-module of rank 2. Define $\mathcal{A}^+$ to be the ring of W-linear endomorphisms of $\mathcal{O}$ which preserve $\wp$. Thus we have

$$\mathcal{A}^+ = \mathcal{A} \cap \mathrm{End}_W(\mathcal{O}) = \mathrm{End}_W(\wp) \cap \mathrm{End}_W(\mathcal{O}),$$

where the second intersection takes place in $K \otimes_{\mathbf{Q}_p} B$. The ring $\mathcal{A}^+$ is thus an Eichler order in $K \otimes_{\mathbf{Q}_p} B$ of level p. Now the map μ clearly induces an embedding

$$\lambda\colon W \otimes_{\mathbf{Z}_p} \mathcal{O} \hookrightarrow \mathcal{A}^+.$$

This embedding is, in fact, an isomorphism, as we verify by noting that both $W \otimes_{\mathbf{Z}_p} \mathcal{O}$ and $\mathcal{A}^+$ are orders in $K \otimes_{\mathbf{Q}_p} B$ with reduced discriminant p.

Let $\mathcal{B}$ be the ring generated by θ and by $\mathcal{C}$. We have $\mathcal{B} \subseteq \mathcal{A}$, and the Proposition asserts the equality of the two rings. As we have just seen, we have

$$\mathcal{A}^+ \subset \mathcal{B}.$$

We then have also

$$\mathcal{A}^- \subset \mathcal{B},$$

where $\mathcal{A}^- = \theta\mathcal{A}^+$. It is clear that $\mathcal{A}^-$ may be described alternately as the ring of σ-linear endomorphisms of $\mathcal{O}$ which preserve $\wp$. Indeed, the elements of $\mathcal{A}^-$ are certainly σ-linear, since θ is σ-linear and the elements of $\mathcal{A}^+$ are linear. On the other hand, if a is a σ-linear endomorphism of $\mathcal{O}$ which preserves $\wp$, then

$$a = \theta^2(a) = \theta\left(\theta(a)\right),$$

and $\theta(a) \in \mathcal{A}^+$.

To prove the equality $\mathcal{B} = \mathcal{A}$, it suffices now to show that $\mathcal{A} = \mathcal{A}^+ + \mathcal{A}^-$, i.e., to verify that an arbitrary element of $\mathcal{A}$ is the sum of (W-) linear and σ-linear elements of $\mathcal{A}$. For this, we consider the action of $W \otimes_{\mathbf{Z}_p} W$ on $\mathcal{A}$ for which $x \otimes y$ sends a to the endomorphism

$$(\text{left multiplication by } x) \circ a \circ (\text{left multiplication by } y).$$

of $\mathcal{O}$. We have available the isomorphism

$$W \otimes_{\mathbf{Z}_p} W \approx W \oplus W$$

mapping $x \otimes y$ to $(xy, x\sigma(y))$. Via this isomorphism, we consider $\mathcal{A}$ as a left $W \oplus W$-module. The action of $W \oplus W$ on $\mathcal{A}$ then breaks up $\mathcal{A}$ into the direct sum of two W-submodules. On the first submodule, $x \otimes y$ acts as xy for all $x, y \in W$. In particular, the actions of $x \otimes 1$ and $1 \otimes x$ coincide; therefore, the elements of the first submodule are W-linear. Similarly, the elements of the second factor are σ-linear. Since every element of $\mathcal{A}$ is the sum of elements in the two submodules, we have completed the necessary verification. ∎

An alternate proof. The author is grateful to C.J. Bushnell for communicating a second proof of Proposition 1.1. Here is a summary of his method:

Let $\mathcal{B}$ again be the order generated by θ and by $\mathcal{C}$. We have $\mathcal{B} \subseteq \mathcal{A}$. It is easy to check the equality

$$(\mathcal{B} : \mathcal{C}) = p^4. \tag{1}$$

Indeed, we may choose a $\mathbf{Z}_p$-basis $\{x, y, z, t\}$ of $\mathcal{O}$ for which $\{x, y, pz, pt\}$ is a basis of $\wp$. The ring $\mathcal{C}$ is then realized as the free $\mathbf{Z}_p$-module with the 16 basis vectors $\alpha \otimes \beta$, where α and β run through our chosen basis. Recognizing that $\mathcal{B}$ is the $\mathbf{Z}_p$-module $\mathcal{O} \otimes \mathcal{O} + \wp \otimes \wp^{-1}$, we see that $\mathcal{B}$ may be obtained as the $\mathbf{Z}_p$-module $\mathcal{C} + p^{-1}L$, where L is the free $\mathbf{Z}_p$-module of rank 4 generated by $x \otimes x$, $x \otimes y$, $y \otimes x$, and $y \otimes y$. This leads to (1).

We now use the standard trace form $\tau : u \otimes v \mapsto \mathrm{tr}(u) \cdot \mathrm{tr}(v)$ on $B \otimes B$, where "tr" denotes the reduced trace on B. For Λ a lattice in $B \otimes B$, we let $\hat{\Lambda}$ be its $\mathbf{Z}_p$-dual:

$$\hat{\Lambda} = \{\, \beta \in B \otimes B \mid \tau(\beta\Lambda) \subseteq \mathbf{Z}_p \,\}.$$

It is well known that

$$(\hat{\mathcal{C}} : \mathcal{C}) = p^{16}. \tag{2}$$

Comparing this with (1), we see that we have $(\hat{\mathcal{B}} : \mathcal{B}) = p^8$. On the other hand, it is known that $(\hat{\mathcal{A}} : \mathcal{A}) = p^8$, cf. [1], Prop. 1.11. Since $\mathcal{B} \subseteq \mathcal{A}$, the two orders $\mathcal{A}$ and $\mathcal{B}$ must be equal. ∎

We deduce from Proposition 1.1 a structure theorem involving free finite-rank $\mathbf{Z}_p$-modules L which are furnished with left and right $\mathcal{O}$-actions, i.e., which are given as $(\mathcal{O}, \mathcal{O})$-bimodules.

THEOREM **1.2** *Let L be an $(\mathcal{O},\mathcal{O})$-bimodule which is free of finite rank over $\mathbf{Z}_p$. Assume that L satisfies the equality*

$$\wp L = L\wp. \tag{3}$$

Then L is isomorphic to a finite direct sum of copies of $\mathcal{O}$ and $\wp$, regarded as bimodules via the natural left- and right-multiplications of $\mathcal{O}$ on itself and on $\wp$.

Remark. The equality (3) is not satisfied automatically. It is an amusing exercise to construct examples of $(\mathcal{O},\mathcal{O})$-bimodules which are $\mathbf{Z}_p$-free of rank 8 for which (3) fails.

Proof. To give a bimodule structure on L is to give a left action of the ring $\mathcal{O}\otimes_{\mathbf{Z}_p}\mathcal{O}$, since $\mathcal{O}$ is its own opposite ring. Equivalently, an $(\mathcal{O},\mathcal{O})$-bimodule is a left $\mathcal{C}$-module. Assume that L is such a module, free of finite rank over $\mathbf{Z}_p$. Then L satisfies (3) if and only if the operator θ (which acts *a priori* on $L\otimes_{\mathbf{Z}_p}\mathbf{Q}_p$) preserves L. Hence the bimodules L under considerations are $\mathcal{A}$-modules, in view of Proposition 1.1.

In view of the standard theory of representations of hereditary orders [2, 25], all $\mathcal{A}$-modules which are free of finite rank over $\mathbf{Z}_p$ are direct sums of copies of the $\mathcal{A}$-modules $\mathcal{O}$ and $\wp$. This proves Theorem 1.2. ∎

Variants

We consider two variants of Theorem 1.2.

THEOREM **1.3** *Let L and L' be bimodules as in Theorem 1.2. Then L and L' are isomorphic if and only if the $(\mathbf{F}_{p^2},\mathbf{F}_{p^2})$-bimodules $L/\wp L$ and $L'/\wp L'$ are isomorphic.*

(In the statement of this "Nakayama Lemma," both actions of $\mathcal{O}$ on $L/\wp L$ factor through $\mathbf{F}_{p^2}$ because of equation (3). Hence $L/\wp L$ is naturally an ($\mathbf{F}_{p^2}$,$\mathbf{F}_{p^2}$)-bimodule. Similarly for $L'/\wp L'$.)

To deduce Theorem 1.3 from Theorem 1.2, we first remark that an ($\mathbf{F}_{p^2}$,$\mathbf{F}_{p^2}$)-bimodule is nothing but a left module for the ring $\mathbf{F}_{p^2}\otimes_{\mathbf{F}_p}\mathbf{F}_{p^2}$. This latter ring is isomorphic to the direct sum $\mathbf{F}_{p^2}\oplus\mathbf{F}_{p^2}$ under the map

$$x\otimes y\mapsto (xy, x\bar{y}),$$

where $\bar{y}$ is the image of y under the non-trivial automorphism of $\mathbf{F}_{p^2}$ over $\mathbf{F}_p$. Further, to give an $\mathbf{F}_{p^2} \oplus \mathbf{F}_{p^2}$-module is to give a direct sum $M_1 \oplus M_2$ of $\mathbf{F}_{p^2}$-vector spaces. Hence a finite ($\mathbf{F}_{p^2}$,$\mathbf{F}_{p^2}$)-bimodule M is determined up to isomorphism by a pair of positive integers r and s: the dimensions of M_1 and M_2. (We can say that M is *of type* (r, s).)

One checks immediately that $L/\wp L$ is of type (r, s) when

$$L = \overbrace{\mathcal{O} \times \cdots \times \mathcal{O}}^{r \text{ factors}} \times \overbrace{\wp \times \cdots \times \wp}^{s \text{ factors}}.$$

Now if L and L' are given as in Theorem 1.3, then by Theorem 1.2 we have

$$L \approx \mathcal{O}^r \times \wp^s, \quad L' \approx \mathcal{O}^{r'} \times \wp^{s'}$$

for suitable integers r, s, r', s'. If $L/\wp L$ and $L'/\wp L'$ are isomorphic, then

$$(r, s) = (r', s'),$$

so that L and L' are isomorphic.

To deduce Theorem 1.2 from Theorem 1.3, we start with L, define (r, s) to be the type of $L/\wp L$, and observe that L and $\mathcal{O}^r \times \wp^s$ have isomorphic reductions. By Theorem 1.3, we deduce that L and $\mathcal{O}^r \times \wp^s$ are isomorphic.

THEOREM **1.4** *Let n be a positive integer. Let $f\colon \mathcal{O} \to \mathrm{M}(n, \mathcal{O})$ be a homomorphism of rings satisfying*

$$f(\wp) \subset \mathrm{M}(n, \wp), \tag{4}$$

where $\mathrm{M}(n, \wp)$ is the set of matrices in $\mathrm{M}(n, \mathcal{O})$ whose entries lie in $\wp$. Then f is $\mathbf{GL}(n, \mathcal{O})$-conjugate to a homomorphism of the form

$$x \mapsto \mathrm{diag}\left(a_1(x), \ldots, a_n(x)\right), \tag{5}$$

where each a_i is either the identity map or else the map

$$x \mapsto \pi^{-1} x \pi. \tag{6}$$

Proof. Let $L = \mathcal{O}^n$. Define a right $\mathcal{O}$-action on L by componentwise right-multiplication, and define a left $\mathcal{O}$-action on L via the homomorphism f: $x \in \mathcal{O}$ acts on the column vector $(u_1 \ldots u_n) \in L$ by multiplication by the matrix $f(x)$. It is easy to see that the bimodule so defined satisfies

the condition (3). Indeed, condition (4) implies that we have an inclusion $\wp L \subseteq L\wp$, and this leads to the equality (3) because $\wp L$ and $L\wp$ have the same index in L, namely p^{2n}.

By Theorem 1.2, we have an isomorphism of bimodules

$$\varphi\colon L \xrightarrow{\sim} \overbrace{\mathcal{O} \times \cdots \times \mathcal{O}}^{r \text{ factors}} \times \overbrace{\wp \times \cdots \times \wp}^{s \text{ factors}}.$$

for suitable r and s. In this isomorphism, we may replace each factor $\wp$ by a factor $\mathcal{O}$, provided that we twist the left action of $\mathcal{O}$ on $\mathcal{O}$. Namely, the map $t \mapsto \pi^{-1}t$ induces an isomorphism of right $\mathcal{O}$-modules $\wp \xrightarrow{\sim} \mathcal{O}$. This map becomes an isomorphism of bimodules if we re-define the left action of $\mathcal{O}$ on $\mathcal{O}$ so that x sends $t \in \mathcal{O}$ to $(\pi^{-1}x\pi)t$. Combining the two isomorphisms, we get an isomorphism

$$\mathcal{O}^n \approx \mathcal{O}^n,$$

where $\mathcal{O}$ acts on the right in the usual way on both copies of $\mathcal{O}^n$ and $x \in \mathcal{O}$ acts on the left as follows: By matrix multiplication by $f(x)$ on the first factor, and by matrix multiplication by the diagonal matrix

$$\operatorname{diag}(\overbrace{x, \ldots, x}^{r \text{ factors}}; \overbrace{\pi^{-1}x\pi, \ldots, \pi^{-1}x\pi}^{s \text{ factors}})$$

on the second factor. This isomorphism being $\mathcal{O}$-linear, it is given by left multiplication by a matrix in $\mathbf{GL}(n, \mathcal{O})$. ∎

Remark. Since every bimodule L as in Theorem 1.2 is isomorphic as a right-module to $\mathcal{O}^n$ for some n, every such bimodule is given by a map f as in the statement of the theorem. Hence Theorem 1.4 is in fact *equivalent* to Theorem 1.2.

COROLLARY **1.5** *Let f be a homomorphism $\mathcal{O} \to \mathrm{M}(n, \mathcal{O})$ as in Theorem 1.4. Suppose that there are r occurrences of the identity map and s occurrences of the map*

$$x \mapsto \pi^{-1}x\pi$$

in the diagonal representation of f which is given by Theorem 1.4. Then the commutant of $f(\mathcal{O})$ in $\mathrm{M}(n, \mathcal{O})$ is a hereditary ring isomorphic to the intersection

$$\operatorname{End}(\mathbf{Z}_p^n) \cap \operatorname{End}(\mathbf{Z}_p^r \oplus p\mathbf{Z}_p^s) \tag{7}$$

in $\mathrm{M}(n, \mathbf{Z}_p)$.

Proof. We may assume that f is given as in (5), with the first r a_i equal to the identity map and the next s a_i equal to the map (6). For $Z = (z_{ij})$ a matrix in $\mathrm{M}(n, \mathcal{O})$, it is easy to determine the condition on the z_{ij} imposed by the equation $f(x)Z = Zf(x)$ for all $x \in \mathcal{O}$. Namely, the z_{ij} must lie in $\pi\mathbf{Z}_p$ for all i and j such that $a_i \neq a_j$ and in $\mathbf{Z}_p$ for all i and j such that $a_i = a_j$. The commutant of $\mathcal{O}$ in $\mathrm{M}(n, \mathcal{O})$ is thus the subring $\mathcal{R}$ of $\mathrm{M}(n, \mathcal{O})$ consisting of matrices of this form.

Let δ now be the diagonal matrix $\mathrm{diag}(\pi, \ldots, \pi; 1, \ldots, 1)$ where there are r entries π and s entries 1. The ring $\mathcal{R}$ is isomorphic to $\delta\mathcal{R}\delta^{-1}$, which one recognizes as the subring (7) of $\mathrm{M}(n, \mathbf{Z}_p)$. This intersection is explicitly the subring of $\mathrm{M}(n, \mathbf{Z}_p)$ consisting of matrices (c_{ij}) for which c_{ij} is divisible by p whenever $j \leq r$ and $i > r$. (For example, suppose $n = 2$. Then (7) is all of $\mathrm{M}(2, \mathbf{Z}_p)$ whenever $r = 2, s = 0$ or $s = 2, r = 0$. It is the standard Eichler order of level p in $\mathrm{M}(2, \mathbf{Z}_p)$ when $r = 1 = s$.) ∎

To restate Theorem 1.3 in the context of matrices, we define for each f as in Theorem 1.4 the map

$$\bar{f}\colon \mathbf{F}_{p^2} \to \mathrm{M}(n, \mathbf{F}_{p^2}) \tag{8}$$

which is induced by f (thanks to (4)).

THEOREM **1.6** *Let f and f' be homomorphism $f\colon \mathcal{O} \to \mathrm{M}(n, \mathcal{O})$ satisfying (4). Assume that $\bar{f}$ and $\bar{f}'$ are $\mathbf{GL}(n, \mathbf{F}_{p^2})$-conjugate. Then f and f' are $\mathbf{GL}(n, \mathcal{O})$-conjugate.*

Proof. We may assume that f and f' are given by diagonal maps

$$x \mapsto \mathrm{diag}\,(a_1, \ldots, a_n)\,, \quad x \mapsto \mathrm{diag}\,(a'_1, \ldots, a'_n)$$

of the type described. Then $\bar{f}$ and $\bar{f}'$ are given *a fortiori* by diagonal maps $\mathbf{F}_{p^2} \to \mathrm{M}(n, \mathbf{F}_{p^2})$ whose components are either the identity map or the Frobenius automorphism $\mathbf{F}_{p^2} \to \mathbf{F}_{p^2}$. (The latter is induced by the map $x \mapsto \pi^{-1}x\pi \pmod{\wp}$.) It is clear that $\bar{f}$ and $\bar{f}'$ are conjugate if and only if the number of occurrences of the identity map $\mathbf{F}_{p^2} \to \mathbf{F}_{p^2}$ is the same for $\bar{f}$ and $\bar{f}'$. This is the case if and only if the number of i for which a_i is the identity map is the same as the number of i for which a'_i is the identity map. When this condition is satisfied, f and f' are conjugate, in fact, by a permutation matrix in $\mathbf{GL}(n, \mathbf{Z})$. ∎

2 Global Study of Certain Bimodules

Oriented Orders

Let D be a square free positive integer. For each prime p dividing D, we suppose given a field $\mathbf{F}_{p^2}$ of cardinality p^2. Let N be a positive integer which is prime to D. Suppose that $\mathcal{R}$ is an Eichler order of level N in a quaternion algebra over $\mathbf{Q}$ of discriminant D. Recall that, for each prime ℓ dividing N, the tensor product $\mathcal{R} \otimes \mathbf{Z}_\ell$ is the intersection of two maximal orders $\mathcal{S}_1$ and $\mathcal{S}_2$ in $\mathcal{R} \otimes \mathbf{Q}_\ell$. These orders are distinct, and they are unique up to permutation. (See, for example, [30], Lemme 2.4, page 39.) We shall refer to them as the *characteristic orders* of $\mathcal{R}$ at ℓ.

An orientation of $\mathcal{R}$ at $\ell|N$ is a choice of one of the two characteristic orders of $\mathcal{R}$ at ℓ. This choice may be given, simultaneously for all $\ell|N$, by an inclusion $\mathcal{R} \hookrightarrow \mathcal{R}'$, where $\mathcal{R}'$ is a maximal order of $\mathcal{R} \otimes \mathbf{Q}$ which is a characteristic order for $\mathcal{R}$ locally at each $\ell|N$. (We say that $\mathcal{R}'$ is a characteristic order of $\mathcal{R}$. There are 2^t such orders, where t is the number of prime divisors of N.) An orientation of $\mathcal{R}$ at $p|D$, relative to the field $\mathbf{F}_{p^2}$, is a homormorphism $\mathcal{R} \to \mathbf{F}_{p^2}$. To give such a homomorphism is to give one of the two isomorphisms between $\mathbf{F}_{p^2}$ and the residue field of $\mathcal{R}$ at p.

An *orientation of* $\mathcal{R}$ is an orientation of $\mathcal{R}$ locally at each prime dividing ND. We refer to $\mathcal{R}$ as an *oriented Eichler order*. It is clear what is meant by an isomorphism of oriented Eichler orders.

Local Isomorphism Classes

In this §, we suppose given maximal orders $\mathcal{O}$ and $\mathcal{S}$ in two quaternion algebras over $\mathbf{Q}$. The discriminants of the rings $\mathcal{O}$ and $\mathcal{S}$ are thus the discriminants of the quaternion algebras $\mathcal{O} \otimes \mathbf{Q}$ and $\mathcal{S} \otimes \mathbf{Q}$, respectively. We assume given a field $\mathbf{F}_{p^2}$ for each prime p which divides the discriminant of either $\mathcal{O}$ or $\mathcal{S}$. Further, we suppose that the two orders $\mathcal{O}$ and $\mathcal{S}$ have been oriented with respect to these fields $\mathbf{F}_{p^2}$.

For use below, we define:

- Σ to be the (possibly empty) set of prime numbers which ramify in each of $\mathcal{O}$ and $\mathcal{S}$;
- Δ to be the set of primes numbers which ramify in one of $\mathcal{O}$, $\mathcal{S}$, but not the other;
- D to be the product of the prime numbers in Δ.

We shall assume for convenience that D is different from 1, i.e., that Δ is non-empty.

We consider $(\mathcal{O}, \mathcal{S})$-bimodules which satisfy a condition which globalizes (3). Namely, we introduce for each $p \in \Sigma$ the maximal ideals $\wp_{\mathcal{O}}$ and $\wp_{\mathcal{S}}$ of $\mathcal{O}$ and $\mathcal{S}$ whose residue fields have cardinality p^2. We call an $(\mathcal{O}, \mathcal{S})$-bimodule M *admissible* if it is free of finite rank over $\mathbf{Z}$ and satisfies the condition

$$\wp_{\mathcal{O}} M = M \wp_{\mathcal{S}} \quad \text{for all } p \in \Sigma. \tag{9}$$

Our aim is to classify admissible modules of fixed rank.

Our assumption $D > 1$ easily implies that the $\mathbf{Z}$-rank of M is always divisible by 8. Indeed, let $\mathcal{A}$ be a quaternion algebra which represents the sum of $\mathcal{O} \otimes \mathbf{Q}$ and $\mathcal{S} \otimes \mathbf{Q}$ in the Brauer group $\mathrm{Br}(\mathbf{Q})$ of $\mathbf{Q}$. Because $D > 1$, $\mathcal{A}$ is a division algebra. If M is an $(\mathcal{O}, \mathcal{S})$-bimodule, there is an induced action on $M \otimes \mathbf{Q}$ of the tensor product

$$(\mathcal{O} \otimes \mathbf{Q}) \otimes (\mathcal{S} \otimes \mathbf{Q}) \approx \mathrm{M}(2, \mathcal{A}).$$

The action of $\mathrm{M}(2, \mathcal{A})$ on $M \otimes \mathbf{Q}$ breaks up $M \otimes \mathbf{Q}$ into the direct sum of two isomorphic $\mathcal{A}$-vector spaces, each of which has $\mathbf{Q}$-dimension divisible by 4.

In our application, $\mathcal{O}$ will be a maximal order in an indefinite quaternion algebra over $\mathbf{Q}$, while $\mathcal{S}$ will be a maximal order in a definite quaternion algebra over $\mathbf{Q}$. Thus the two quaternion algebras will not be isomorphic, and our assumption $D \neq 1$ is automatically satisfied. In any case, our main applications concern the situation where the $\mathbf{Z}$-rank of M is *equal* to 8.

If M is admissible and ℓ is a prime, we let M_ℓ be the tensor product $M \otimes \mathbf{Z}_\ell$ and similarly define $\mathcal{O}_\ell$ and $\mathcal{S}_\ell$. Then M_ℓ is a $(\mathcal{O}_\ell, \mathcal{S}_\ell)$-bimodule. In particular, when $\ell = p$ is an element of Σ, we may consider M_p as an $(\mathcal{O}_p, \mathcal{O}_p)$-bimodule after choosing an isomorphism $\mathcal{O}_p \approx \mathcal{S}_p$. This bimodule of course satisfies the condition (3). Consequently, the isomorphism class of M_p may be read off from that of

$$\overline{M}_p = M/(M\wp_{\mathcal{S}}) = M/(\wp_{\mathcal{O}} M)$$

in view of Theorem 1.3. The endomorphism ring of M_p is similarly calculated by Corollary 1 to Theorem 1.4. In particular, this endomorphism ring is isomorphic to a hereditary order in $\mathrm{M}(2n, \mathbf{Z}_p)$, where $n = \mathrm{rank}_{\mathbf{Z}}(M)/8$.

On the other hand, when $\ell \notin \Sigma$, it is easy to see that the isomorphism class of M_ℓ depends only on the rank of M over $\mathbf{Z}$. Indeed, suppose to fix

ideas that ℓ is unramified in $\mathcal{S}$, so that $\mathcal{S}_\ell$ is isomorphic to the matrix algebra $\mathrm{M}(2, \mathbf{Z}_\ell)$. The bimodule M_ℓ may be viewed as a left module over

$$\mathcal{O}_\ell \otimes \mathcal{S}_\ell \approx \mathrm{M}(2, \mathcal{O}_\ell).$$

Thus, to give M_ℓ is to give a module over $\mathcal{O}_\ell$ whose rank is half that of M_ℓ, i.e., 4n. On the other hand, it is standard that all $\mathcal{O}_\ell$-modules which are free of finite rank over $\mathbf{Z}_\ell$ are free over $\mathcal{O}_\ell$. (See, for example Theorem 18.7 of [25].) We find that $\mathrm{End}(M_\ell)$ is isomorphic to $\mathrm{M}(n, \mathcal{O}_\ell)$. In the typical case where ℓ is unramified in $\mathcal{O}$ (as well as in $\mathcal{S}$), $\mathrm{End}(M_\ell)$ is thus isomorphic to $\mathrm{M}(2n, \mathbf{Z}_\ell)$.

The following results now follow directly.

PROPOSITION **2.1** *Suppose that M is an admissible $(\mathcal{O}, \mathcal{S})$-bimodule of rank $8n$. Then the $\mathbf{Q}$-algebra $\mathrm{End}(M) \otimes \mathbf{Q}$ is isomorphic to the matrix algebra $\mathrm{M}(n, \mathcal{A})$, where $\mathcal{A}$ is a quaternion algebra over $\mathbf{Q}$ whose class in the Brauer group $\mathrm{Br}(\mathbf{Q})$ is the sum of the classes of the quaternion algebras $\mathcal{O} \otimes \mathbf{Q}$ and $\mathcal{S} \otimes \mathbf{Q}$. In particular, $\mathcal{A}$ is a matrix algebra locally at each prime p in Σ. The ring $\mathrm{End}(M)$ is a hereditary order in $\mathrm{End}(M) \otimes \mathbf{Q}$ which is maximal locally at all primes $\ell \notin \Sigma$.*

PROPOSITION **2.2** *Let M and N be admissible bimodules of equal rank $8n$. Then M_ℓ and N_ℓ are isomorphic $(\mathcal{O}_\ell, \mathcal{S}_\ell)$-bimodules for all $\ell \notin \Sigma$. For $p \in \Sigma$, M_p and N_p are isomorphic if and only if $\overline{M}_p$ and $\overline{N}_p$ are isomorphic $(\mathcal{O}/\wp_\mathcal{O}, \mathcal{S}/\wp_\mathcal{S})$-bimodules.*

In connection with the latter proposition, it should be stressed that the isomorphism classes of $\overline{M}_p$ and $\overline{N}_p$ are each determined by a pair of integers (r, s) summing to $2n$. Indeed, as in the discussion of Theorem 1.3, to give an $(\mathcal{O}/\wp_\mathcal{O}, \mathcal{S}/\wp_\mathcal{S})$-bimodule is to give a vector space over each of two fields isomorphic to $\mathbf{F}_{p^2}$.

Isomorphism classes and right modules

Let M be an admissible bimodule, and pose $\Lambda = \mathrm{End}(M)$. For each admissible bimodule N which is locally isomorphic to M (in the sense that it becomes isomorphic to M after tensoring with $\mathbf{Z}_\ell$ for all primes ℓ), let

$$J(N) = \mathrm{Hom}(M, N)$$

be the set of bimodule homomorphisms $M \to N$. This abelian group is a right Λ-module under composition. It is visibly locally free of rank 1 in the sense that we have an isomorphism

$$J(N) \otimes_{\mathbf{Z}} \mathbf{Z}_\ell \approx \Lambda \otimes_{\mathbf{Z}} \mathbf{Z}_\ell$$

for each prime ℓ. Indeed, if $\phi_\ell \in \mathrm{Hom}(M_\ell, N_\ell)$ is an isomorphism $M_\ell \approx N_\ell$, then ϕ_ℓ is a basis for $J(N) \otimes_{\mathbf{Z}} \mathbf{Z}_\ell$ over $\Lambda \otimes_{\mathbf{Z}} \mathbf{Z}_\ell$.

THEOREM **2.3** *The association $N \mapsto J(N)$ establishes a bijection between the sets of isomorphism classes of the following objects:*

- *$(\mathcal{O}, \mathcal{S})$-bimodules which are locally isomorphic to M;*
- *Locally free rank-1 right Λ-modules.*

Proof. For J locally free of rank 1 over Λ, consider

$$N(J) = J \otimes_\Lambda M.$$

This tensor product has a natural bimodule structure coming from the actions of $\mathcal{O}$ and $\mathcal{S}$ on the second factor. Locally at each prime ℓ, we have by hypothesis an isomorphism $J \sim \Lambda$; this establishes an isomorphism (locally) $N(J) \sim M$, which tells us that $N(J)$ is locally isomorphic to M.

To check that $N(J(N))$ is isomorphic to N, we note that the contraction map

$$\mathrm{Hom}(M, N) \otimes_\Lambda M \to N; \qquad \phi \otimes m \mapsto \phi(m)$$

is an isomorphism — this is clear locally. Similarly, we have

$$J \xrightarrow{\sim} \mathrm{Hom}(M, J \otimes_\Lambda M); \qquad j \colon m \mapsto j \otimes m.$$

Hence the two constructions are inverses of each other. ∎

Eliminating base points

We now complement Theorem 2.3 with a statement which describes the set of isomorphism classes of admissible bimodules of $\mathbf{Z}$-rank 8 in an intrinsic fashion, i.e., without demanding that a base point M be fixed as in Theorem 2.3. We first consider local equivalence: two bimodules M and N are *locally isomorphic* or *locally equivalent* if $M_\ell \approx N_\ell$ for all primes ℓ. Assuming that M and N both have rank 8, their localizations M_ℓ and N_ℓ are *a*

priori isomorphic for all $\ell \notin \Sigma$. Hence the local equivalence is the statement that we have $M_p \approx N_p$ for each $p \in \Sigma$.

As discussed above, the isomorphism class of M_p is determined by that of the $(\mathcal{O}/\wp\mathcal{O}, \mathcal{S}/\wp\mathcal{S})$-bimodule

$$\overline{M}_p = M/(M\wp_{\mathcal{S}}) = M/(\wp_{\mathcal{O}}M),$$

which has rank 4 over $\mathbf{F}_p$. Every finite $(\mathcal{O}/\wp\mathcal{O}, \mathcal{S}/\wp\mathcal{S})$-bimodule is a direct sum of a certain number of copies of $\mathbf{F}_{p^2}$, on which $\mathcal{O}/\wp\mathcal{O}$ and $\mathcal{S}/\wp\mathcal{S}$ act in the obvious way by multiplication, and a "twisted" $\mathbf{F}_{p^2}$, on which $\mathcal{O}/\wp\mathcal{O}$ acts in the obvious way by multiplication and $\mathcal{S}/\wp\mathcal{S}$ acts by conjugate multiplication. In particular, $\overline{M}_p$ is a sum of, say, r_p copies of $\mathbf{F}_{p^2}$ and $(2 - r_p)$ copies of the twisted $\mathbf{F}_{p^2}$. We may restrict consideration to bimodules in a fixed local equivalence class by requiring, for each $p \in \Sigma$, that r_p take a fixed value between 0 and 2.

We suppose, then, in the following discussion that numbers r_p have been fixed and that M is an admissible bimodule of $\mathbf{Z}$-rank 8 for which the modules $\overline{M}_p$ have "invariants" r_p. Let Λ be the ring of endomorphisms of the bimodule M. We shall show that the isomorphism class of M is characterized by the isomorphism class of Λ as an oriented Eichler order.

As a special case of Proposition 2.1, the endomorphism algebra $\Lambda \otimes \mathbf{Q}$ is (up to isomorphism) that quaternion algebra $\mathcal{A}$ over $\mathbf{Q}$ which is ramified precisely at the primes in Δ. The ring $\Lambda = \mathrm{End}(M)$ is an order in $\Lambda \otimes \mathbf{Q}$ which is maximal locally at all primes $\ell \notin \Sigma$. At a prime $p \in \Sigma$, Λ is a maximal order if $r_p = 0$ or 2 and is an Eichler order of level p if $r_p = 1$. (See Corollary 1 to Theorem 1.4 and the example given at the end of its proof.) We may summarize this information by saying that Λ is isomorphic to an Eichler order of level N in $\mathcal{A}$, where N is the product of those primes $p \in \Sigma$ for which $r_p = 1$.

Let p now be a prime in Δ. Then, in particular, Λ is maximal at p. There is a canonical isomorphism between the residue field of Λ at p and the field $\mathbf{F}_{p^2}$. To see this, consider the case where p is ramified in $\mathcal{O}$, but not in $\mathcal{S}$. Let $\wp$ be the prime of $\mathcal{O}$ whose residue field is $\mathbf{F}_{p^2}$. The quotient $M/\wp M$ is then an $(\mathbf{F}_{p^2}, \mathcal{S})$-bimodule, i.e., a left module over $\mathbf{F}_{p^2} \otimes \mathcal{S} \approx \mathrm{M}(2, \mathbf{F}_{p^2})$. Moreover, this quotient has rank 2 as an $\mathbf{F}_{p^2}$-vector space, since M has rank 8 over $\mathbf{Z}$. Therefore, the action of $\mathrm{M}(2, \mathbf{F}_{p^2})$ on M identifies $\mathrm{M}(2, \mathbf{F}_{p^2})$ with a subalgebra of the algebra of $\mathbf{F}_p$-endomorphisms of $M/\wp M$. The commutant of this subalgebra is $\mathbf{F}_{p^2}$; i.e., the algebra of bimodule endomorphisms of

$M/\wp M$ is precisely $\mathbf{F}_{p^2}$. Since Λ is the ring of bimodule endomorphisms of M, there is a natural map

$$\rho_p \colon \Lambda \to \mathbf{F}_{p^2}.$$

This map establishes the desired isomorphism. The set of maps

$$\{\, \rho_p \,;\, p \in \Delta \,\}$$

is the first part of our orientation of Λ.

The second part concerns the set Σ_o consisting of those primes $p \in \Sigma$ for which $r_p = 1$. If p is such a prime, M contains a canonical submodule of index p^2 for each of the two possible isomorphisms $\mathcal{O}/\wp\mathcal{O} \approx \mathcal{S}/\wp\mathcal{S}$. To see this, we remark again that the quotient $\overline{M}_p$ of M is intrinsically the direct sum of two 1-dimensional $\mathbf{F}_{p^2}$-vector spaces corresponding to the two isomorphisms. The kernels of the maps from M to each of these two submodules are the submodules of M in question. It is easy to see from the description in Corollary 1 to Theorem 1.4 that the endomorphism ring Λ of M is the intersection in $\mathrm{End}(M \otimes \mathbf{Q})$ of the endomorphism rings of these two submodules. These endomorphism rings are each Eichler orders of level N/p in $\mathrm{End}(M \otimes \mathbf{Q})$; they are, locally at p, the two maximal orders whose intersection is Λ. To choose one of these maximal orders is to orient Λ at p. Our order Λ is indeed oriented at each $p \in \Sigma_o$ because the chosen orientations furnish, in particular, isomorphisms $\mathcal{O}/\wp\mathcal{O} \approx \mathcal{S}/\wp\mathcal{S}$ for each such p. Since orders in a quaternion algebra may be specified locally, the local orientations of Λ determine a maximal order $\Lambda^\sim$ of $\Lambda \otimes \mathbf{Q}$ which contains Λ.

To summarize, we fixed a collection of integers

$$\{\, r_p \,;\, p \in \Sigma \,\}$$

where the r_p satisfy $0 \le r_p \le 2$. We considered admissible bimodules M, free of rank 8, for which the various reductions M_p of M have "invariants" r_p. Each M gives rise to its endomorphism ring Λ, which is an Eichler order of level N in a quaternion algebra of discriminant D. Here N is the product of the primes in Σ_o: those primes in Σ for which $r_p = 1$. The Eichler order Λ is oriented at each prime $p \in \Delta$ by the map ρ_p. It is oriented at each prime $p \in \Sigma_o$ by the maximal order $\Lambda^\sim \supset \Lambda$. It is thus an oriented Eichler order of level N in a quaternion algebra over $\mathbf{Q}$ of discriminant D.

THEOREM **2.4** *The map $M \mapsto \Lambda$ (with its orientation) induces a bijection between the set of isomorphism classes of admissible the rank-8 bimodules M with invariants r_p and the set of isomorphism classes of oriented Eichler orders of level N in quaternion algebras of discriminant D.*

Proof. First, let M and M' be bimodules of the type under consideration, and assume that they have isomorphic oriented Eichler orders Λ and Λ'. We must show that M and M' are isomorphic. Let J again be $\mathrm{Hom}(M, M')$, first considered as a right Λ-module. It will enough to show that J is trivial, i.e., free of rank 1 over Λ (Theorem 2.3).

For this, we choose and fix an isomorphism of oriented Eichler orders $\Lambda \approx \Lambda'$. Via this isomorphism, J (which is *a priori* a (Λ', Λ)-bimodule) becomes a (Λ, Λ)-bimodule. It is clear that this bimodule is invertible ([25], page 319) with inverse $\mathrm{Hom}(M', M)$. (Recall that M and M' are isomorphic locally.) It is *a fortiori* sufficient to show that this bimodule is isomorphic to the trivial invertible bimodule Λ. Equivalently, we must show that its class in the Picard group of Λ ([25], page 320) is trivial. Since the center of Λ is trivial, the Picard group of Λ coincides with the group Picent Λ (*loc. cit.*). The exact sequence (37.29) in Theorem (37.28) of [25] therefore shows that it is sufficient to check that J_p is trivial in Picent Λ_p for every prime number p.

It is known that the group $\mathrm{Picent}(\Lambda_p)$ is trivial for all p prime to $N \cdot D$ and cyclic of order 2 for all p dividing $N \cdot D$ (see [25], Theorem (37.27) and Exercise (39.6)). We need consider, then, only the situation for $p|D$ and for $p|N$.

First suppose that p divides D. Then J_p is, first, a free right Λ_p-module of rank 1, and we have naturally

$$\Lambda'_p = \mathrm{End}_{\Lambda_p}(J_p).$$

Each basis element for the right Λ_p-module J_p thus defines an isomorphism $\Lambda'_p \approx \Lambda_p$; changing the basis changes the isomorphism by an inner automorphism of Λ_p. In particular, there is a canonically defined isomorphism between the residue fields of Λ_p and Λ'_p, since these residue fields are commutative. This canonical isomorphism is, in another optic, the isomorphism resulting from the orientations of Λ and Λ' at p. Since our chosen isomorphism $\Lambda' \approx \Lambda$ is compatible with orientations, it induces the canonical isomorphism on the level of residue fields. It is easy to see from this that there is a basis element v of J_p for which the associated isomorphism $\Lambda'_p \approx \Lambda_p$ is the base extension to $\mathbf{Z}_p$ of the chosen isomorphism. This basis element defines the isomorphism $\lambda \mapsto v\lambda$ of Λ_p onto J_p. A tautological computation now shows that this is an isomorphism of Λ_p-bimodules. Hence J_p is trivial in Picent Λ_p.

A similar computation treats the primes p dividing N. Here, again, each basis element of the right Λ_p module J_p defines an isomorphism $\Lambda'_p \approx \Lambda_p$.

The point is that an isomorphism ${\Lambda'}_p \approx \Lambda_p$ is obtained from *some* basis element if and only if it is compatible with the orientations of Λ_p and ${\Lambda'}_p$. Explicitly, Λ_p comes equipped with a maximal order ${\Lambda_p}^\sim$ containing Λ_p, and similarly for ${\Lambda'}_p$. An isomorphism ${\Lambda'}_p \approx \Lambda_p$ is compatible with the orientations if it carries ${{\Lambda'}_p}^\sim$ to its analogue ${\Lambda_p}^\sim$. In particular, our chosen isomorphism $\Lambda' \approx \Lambda$ leads by base extension to an isomorphism ${\Lambda'}_p \approx \Lambda_p$ which comes from a basis vector. Making explicit what this means, we again find that J_p is trivial in Picent Λ_p.

We thus have shown that our association (bimodule) $\mapsto$ (oriented order) is injective, and we want to show that it is surjective. For this, we begin by verifying that there is at least one bimodule M of the type under consideration. (This does not seem to be obvious!) It is enough to carry out this step in the special case where all $r_p = 1$: the module M constructed in that case will have canonical submodules which exhibit all possible collections (r_p). (These canonical submodules are defined as in the discussion showing that Λ is oriented at p when p is in Σ_o.)

Furthermore, it is enough to construct M after a possible replacement of $\mathcal{O}$ and/or $\mathcal{S}$ by another maximal order having the same discriminant. Indeed, suppose for instance that we have constructed an $(\mathcal{O}, \mathcal{S}')$-module M' with the desired properties, where $\mathcal{S}'$ has the same discriminant as $\mathcal{S}$. Then we can find an $(\mathcal{S}', \mathcal{S})$-bimodule I which is locally free of rank 1 over each of $\mathcal{S}$ and $\mathcal{S}'$. (We can first reduce to the case where $\mathcal{S}$ and $\mathcal{S}'$ are orders in the same quaternion algebra. Then the I to be found is a left $\mathcal{S}'$-ideal whose right order is $\mathcal{S}$. It is classical that such ideals exist.) Once I is found, we can set

$$M = M' \otimes_{\mathcal{S}'} I.$$

Then M has a right $\mathcal{S}$-action as well as the left $\mathcal{O}$-action inherited from M; it is not hard to show that M is admissible and has invariants $r_p = 1$ if M' has these properties.

To carry out the construction, we choose a quadratic number field K which is ramified at all primes $p \in \Sigma$ and which can be embedded in both quaternion algebras $\mathcal{O} \otimes \mathbf{Q}$ and $\mathcal{S} \otimes \mathbf{Q}$. (It is enough that all primes $p \in \Delta$ ramify or stay prime in K and that K be imaginary if one of the two quaternion algebras is definite.) Let O_K be the integer ring of K. It is known that O_K can be embedded in some maximal orders in each of the quaternion algebras $\mathcal{O} \otimes \mathbf{Q}$ and $\mathcal{S} \otimes \mathbf{Q}$. (Although this fact is presumably very elementary, one may be deduce it from the more precise Th. 5.11 of [30].)

For the reasons explained above, we may (and do) assume that these orders are in fact $\mathcal{O}$ and $\mathcal{S}$. Let us fix, then embeddings $O_K \hookrightarrow \mathcal{O}$ and $O_K \hookrightarrow \mathcal{S}$. Consider the tensor product

$$M = \mathcal{O} \otimes_{O_K} \mathcal{S},$$

which has an evident $(\mathcal{O}, \mathcal{S})$-bimodule structure. It is (locally) free of rank 8 over $\mathbf{Z}$, since $\mathcal{O}$ and $\mathcal{S}$ are each locally free of rank 2 over O_K.

Let us check that M is admissible at each $p \in \Sigma$ and that its invariants r_p are all 1. Choose a basis for the right $O_K \otimes \mathbf{Z}_p$-module $\mathcal{O} \otimes \mathbf{Z}_p$. In terms of this basis, the left action of $\mathcal{O} \otimes \mathbf{Z}_p$ on $\mathcal{O} \otimes \mathbf{Z}_p$ is described by a homomorphism

$$f\colon \mathcal{O} \otimes \mathbf{Z}_p \hookrightarrow \mathrm{M}(2, O_K \otimes \mathbf{Z}_p).$$

Since p is ramified in K, the maximal ideal of $\mathcal{O} \otimes \mathbf{Z}_p$ is generated by a uniformizer π of $O_K \otimes \mathbf{Z}_p$. This shows that $f(\wp\mathcal{O} \otimes \mathbf{Z}_p)$ consists of matrices whose coefficients are divisible by π. Therefore M is admissible at p. Indeed, in matrix terms the local bimodule M_p is given by the composite of f and the map on matrix rings deduced from the inclusion of O_K in $\mathcal{S}$. Matrices divisible by π map to matrices divisible by $\wp_{\mathcal{S}}$ under this map.

To check that the value of r_p is 1, we reduce the matrix maps "mod $\wp$." The map f becomes an embedding

$$\mathcal{O}/\wp\mathcal{O} \hookrightarrow \mathrm{M}(2, \mathbf{F}_p), \tag{10}$$

since the residue field of K at p is the prime field $\mathbf{F}_p$. After extension to a quadratic extension of $\mathbf{F}_p$, this representation of $\mathcal{O}/\wp\mathcal{O} \approx \mathbf{F}_{p^2}$ necessarily becomes a direct sum of the two possible embeddings of $\mathbf{F}_{p^2}$ into the quadratic extension. In particular, the map

$$\mathcal{O}/\wp\mathcal{O} \hookrightarrow \mathrm{M}(2, \mathcal{S}/\wp_{\mathcal{S}}) \tag{11}$$

which describes the bimodule $\overline{M}_p$ is the direct sum of each of the two possible isomorphisms $\mathcal{O}/\wp\mathcal{O} \approx \mathcal{S}/\wp_{\mathcal{S}}$. This is another way of saying that $r_p = 1$.

Knowing that bimodules M of the desired type exist, we fix one of them, say M_o. Let Λ be the endomorphism ring of M_o. Thus Λ is an oriented Eichler order of level N in the quaternion algebra $\mathcal{H} = \Lambda \otimes \mathbf{Q}$ of discriminant D.

For the moment, regard Λ as an Eichler order and forget that it is endowed with an orientation. It will be enough (in view of Theorem 2.3) to show that the number of isomorphism classes of locally free rank-1 right Λ

modules is finite and equal to the number of types of oriented Eichler orders of level N in a quaternion algebra of discriminant D.

Let $\hat{\mathcal{H}}$ be the ring of finite adeles of $\mathcal{H}$. Similarly, let $\hat{\Lambda} = \Lambda \otimes \hat{\mathbf{Z}}$ be the product of the local completions of Λ. Then for each $x = (x_p) \in \hat{\mathcal{H}}^*$, a locally free rank-1 right Λ module is given by the intersection

$$\Lambda \cap \prod_p (x_p \Lambda_p)$$

in $\hat{\mathcal{H}}$. This construction sets up a 1-1 correspondence between the set of locally free rank-1 right Λ-modules and the double coset space $\mathcal{H}^* \backslash \hat{\mathcal{H}}^* / \hat{\Lambda}^*$, cf. [30], page 87. This double coset space is finite (*loc. cit.*, Th. 5.4).

On the other hand, the (unoriented) Eichler orders of level N inside $\mathcal{H}$ are in 1-1 correspondence with $\hat{\mathcal{H}}^* / \mathcal{N}(\hat{\Lambda})$, where $\mathcal{N}(\hat{\Lambda})$ is the normalizer of $\hat{\Lambda}$ in $\hat{\mathcal{H}}^*$. (To (x_p) we associate the order whose completions are the orders $x_p \Lambda_p {x_p}^{-1}$.) Therefore, the isomorphism classes of Eichler orders of level N in a quaternion algebra of discriminant D are represented by the double coset space $\mathcal{H}^* \backslash \hat{\mathcal{H}}^* / \mathcal{N}(\hat{\Lambda})$ (Skolem-Noether theorem). The evident surjection

$$\pi \colon \mathcal{H}^* \backslash \hat{\mathcal{H}}^* / \hat{\Lambda}^* \to \mathcal{H}^* \backslash \hat{\mathcal{H}}^* / \mathcal{N}(\hat{\Lambda})$$

corresponds to the association which attaches to each right Λ-module J its left order.

Remembering that Λ has an orientation, we can mimic the above construction and view adelically the set of isomorphism classes of oriented Eichler orders. The principal difference is that the "normalizer" of the oriented Eichler order Λ_p in $\mathcal{H} \otimes \mathbf{Q}_p$ is the product $\mathbf{Q}_p^* \Lambda_p^*$ for each prime p (whereas for unoriented orders the normalizer is "twice as big" when p divides ND). We thus find that the set of types of oriented Eichler orders of level N and discriminant D is in 1-1 correspondence with the double coset space

$$\mathcal{H}^* \backslash \hat{\mathcal{H}}^* / \hat{\Lambda}^* \hat{\mathbf{Q}}^*.$$

(Here $\hat{\mathbf{Q}}$ is of course the ring of finite adeles of $\mathbf{Q}$.) Since $\hat{\mathbf{Q}}^*$ is the product of $\mathbf{Q}^*$ and the group $\hat{\mathbf{Z}}^*$, and since the first of these factors is in $\mathcal{H}^*$ and the second in $\hat{\Lambda}^*$, the latter double coset space is equal to $\mathcal{H}^* \backslash \hat{\mathcal{H}}^* / \hat{\Lambda}^*$. ∎

3 Abelian Surfaces in Characteristic q

The aim of this § is to give a quaternionic classification of certain supersingular objects in finite characteristic. In order to avoid conflict with later

notation, we call the characteristic q, rather than p. We classify supersingular elliptic curves with $\Gamma_o(M)$-structures, obtaining a variant of the usual result (due to Deuring) in which no base point is fixed *a priori*. More generally, we classify supersingular abelian surfaces with an action of a maximal order R in a rational indefinite quaternion algebra which is split at q. The case of elliptic curves corresponds to the particular choice $R = \mathrm{M}(2, \mathbf{Z})$.

Supersingular Points

Let q be a prime number. Let R be a maximal order in an indefinite quaternion algebra over $\mathbf{Q}$ whose discriminant is prime to q. (We do not exclude the case where R is isomorphic to $\mathrm{M}(2, \mathbf{Z})$.) Let D be the product of q and the discriminant of R; thus, D is the discriminant of some definite quaternion algebra over $\mathbf{Q}$.

Suppose given finite fields $\mathbf{F}_{p^2}$ for each prime p dividing D. We assume that R is furnished with an orientation at each prime p dividing D/q, and we let $\mathbf{F}$ be an algebraic closure of $\mathbf{F}_{q^2}$. We consider pairs (A, ι), where A is an abelian surface over $\mathbf{F}$ and ι is an embedding

$$R \hookrightarrow \mathrm{End}_{\mathbf{F}}(A).$$

In our application, we shall study only those pairs which are *supersingular* in the sense that they are isogenous to a product of two supersingular elliptic curves over $\mathbf{F}$. Note that a well known theorem in [29], §3 states that all products of n supersingular elliptic curves over $\mathbf{F}$ are isomorphic, provided that $n > 1$. In [29], the result is attributed to P. Deligne. The proof depends on Eichler's theorem to the effect that the class number of $\mathrm{M}(n, \mathcal{B})$ is 1 whenever $\mathcal{B}$ is a quaternion algebra over $\mathbf{Q}$ and $n > 1$.

Let $a(A)$ be Oort's invariant

$$\dim_{\mathbf{F}} \left(\mathrm{Hom}(\alpha_q, A) \right),$$

where α_q is the usual group scheme α_p with $p = q$. We have *a priori*:

1. $1 \leq a(A) \leq 2$.
2. The abelian variety A is isomorphic to a product of two supersingular elliptic curves if and only if $a(A) = 2$.

For the first statement, see [21], §2. The second statement follows from [23], Theorem 2 and Remark 3.

In fact, it is clear that A is necessarily isomorphic to a product of two supersingular elliptic curves over $\mathbf{F}$. Indeed, the $\mathbf{F}$-vector space $\mathrm{Hom}_{\mathbf{F}}(\alpha_q, A)$ is naturally a module over $R \otimes \mathbf{F} \approx \mathrm{M}(2, \mathbf{F})$. Its dimension $a(A)$ is therefore even. Since $a(A)$ is *a priori* either 1 or 2, it follows that we have $a(A) = 2$, which implies the claim.

We wish to study the set of isomorphism classes of pairs (A, ι) with A supersingular. Before doing so, we observe that this set is independent of the choice of R *as an oriented order*. Indeed, if R' is another oriented maximal order of discriminant D/q, we can find an isomorphism $\phi\colon R \to R'$ of oriented orders because of Eichler's approximation theorem ([30], Th. 4.3, p. 81). (The Eichler condition is satisfied because $R \otimes \mathbf{Q}$ is an indefinite quaternion algebra.) This isomorphism is unique up to inner automorphisms of R or R'. Given a pair (A, ι'), where

$$\iota' : R' \hookrightarrow \mathrm{End}_{\mathbf{F}}(A),$$

we define

$$\iota : R \hookrightarrow \mathrm{End}_{\mathbf{F}}(A)$$

by the formula $\iota' \circ \phi$. The isomorphism class of the pair (A, ι) thus defined does not change if we change ϕ by an inner automorphism of R.

To study the pairs (A, ι), we fix a supersingular elliptic curve E over $\mathbf{F}$ and let $S = \mathrm{End}(E)$. To give (A, ι) is to give a homomorphism $R \to \mathrm{M}(2, S)$, or equivalently to give an (R, S)-bimodule M which is free of rank 8 over $\mathbf{Z}$. According to a well known theorem of M. Deuring, S is a maximal order in a quaternion algebra of discriminant q over $\mathbf{Q}$. The bimodule M is automatically admissible, as the discriminants D/q and q of R and S are relatively prime. By Theorem 2.4, the pairs (A, ι) are thus classified by isomorphism classes of oriented maximal orders in quaternion algebras over $\mathbf{Q}$ of discriminant D.

To be more precise, we note that for each (A, ι), the ring $\mathrm{End}(A, \iota) = \mathrm{End}_R(A)$ is a maximal order in the quaternion algebra $\mathrm{End}(A, \iota) \otimes \mathbf{Q}$, which has discriminant D. This order is naturally oriented:

- Let r be a prime divisor of D/q. Let $\mathbf{m}$ be the maximal ideal of R of residue characteristic r. Then $R/\mathbf{m}$ may be identified with $\mathbf{F}_{r^2}$, because of the given orientation of R. The kernel $A[\mathbf{m}]$ is an $\mathbf{F}_{r^2}$-vector space of dimension 1. The action of $\mathrm{End}(A, \iota)$ on this vector space thus defines a homomorphism

$$\mathrm{End}(A, \iota) \to \mathbf{F}_{r^2}.$$

This homomorphism is an orientation of $\mathrm{End}(A,\iota)$ at r.

- Let T be the Lie algebra of A, so that T is an $\mathbf{F}$-vector space of dimension 2. The action of R on A induces an action of $R\otimes\mathbf{F}$ on T. The ring $\mathrm{End}_R(T)$ is easily seen to coincide with the ring $\mathbf{F}$ of homotheties of the $\mathbf{F}$-vector space T. The action of $\mathrm{End}(A,\iota)$ on T thus defines a homomorphism

$$\mathrm{End}(A,\iota)\to\mathbf{F}.$$

  In view of the structure of the ring $\mathrm{End}(A,\iota)$, this homomorphism must in fact take values in the subfield $\mathbf{F}_{q^2}$ of $\mathbf{F}$. Hence it defines an orientation of $\mathrm{End}(A,\iota)$ at the prime q.

Theorem 2.4 then gives the following result:

THEOREM **3.1** *Let R be an oriented maximal order in a quaternion algebra of discriminant D/q over $\mathbf{Q}$. The construction*

$$(A,\iota)\mapsto \mathrm{End}(A,\iota)\ \text{ (with its natural orientation)}$$

induces a bijection between the set of isomorphism classes of supersingular abelian surfaces with R-action over $\mathbf{F}$ and the set of isomorphism classes of oriented maximal orders in quaternion algebras of discriminant D over $\mathbf{Q}$.

In the special case $D=q$, R may be taken to be the matrix ring $\mathrm{M}(2,\mathbf{Z})$. To give a pair (A,ι) is then to give a supersingular elliptic curve over $\mathbf{F}$. Our theorem then becomes a famous result of M. Deuring, as reformulated by Mestre and Oesterlé [17].

$\Gamma_o(M)$-structures

First, fix a pair (A,ι) over $\mathbf{F}$ for which A is supersingular. Suppose that $M\geq 1$ is an integer which is prime to D. A $\Gamma_o(M)$-structure on (A,ι) is an R-stable subgroup C of $A(\mathbf{F})$ which is isomorphic to $(\mathbf{Z}/M\mathbf{Z})^2$ as an abelian group. For each $\Gamma_o(M)$-structure C on (A,ι), let $\mathrm{End}(A,\iota,C)$ be the subring of $\mathrm{End}(A,\iota)$ consisting of R-endomorphisms λ of A for which $\lambda(C)\subseteq C$. Visibly, this ring is an order of $\mathrm{End}(A,\iota)\otimes\mathbf{Q}$ which lies between $M\cdot\mathrm{End}(A,\iota)$ and $\mathrm{End}(A,\iota)$. Hence it agrees with $\mathrm{End}(A,\iota)$ locally at each prime ℓ not dividing M.

Let us examine the situation at ℓ when ℓ divides M. To fix ideas, we will first assume that $M=\ell^\nu$ is a power of ℓ. Let T_ℓ be the $\mathbf{Z}_\ell$-adic Tate module

of A; this Tate module is a free left rank-1 module over the ring $R_\ell = R \otimes \mathbf{Z}_\ell$. Choose an isomorphism $R_\ell \approx \mathrm{M}(2, \mathbf{Z}_\ell)$, and let $L = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} T_\ell$. Then the map

$$t \in T_\ell \mapsto \left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} t, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} t \right)$$

induces an isomorphism $T_\ell \approx L \oplus L$. To give a $\Gamma_o(M)$-structure C on (A, ι) is to give an R-stable lattice $T' \supseteq T_\ell$ such that T'/T_ℓ is isomorphic to $(\mathbf{Z}/M\mathbf{Z})^2$. Such a lattice is necessarily of the form $L' \oplus L'$, where $L' \supseteq L$ is a lattice in $L \otimes \mathbf{Q}_\ell$ for which L'/L is cyclic of order M. Conversely, given any L' with this property, the lattice $L' \oplus L'$ is a suitable T'.

As is well known (cf. [30], pp. 40–41), the map $L' \mapsto \mathrm{End}(L')$ establishes a 1-1 correspondence between the following sets of objects:

(i) Lattices L' in the $\mathbf{Q}_\ell$-vector space $L \otimes \mathbf{Q}_\ell$ which contain L and such that L'/L is cyclic;

(ii) Maximal orders $\mathcal{S}$ in the ring $\mathrm{End}(L) \otimes \mathbf{Q}_\ell$.

Further, the map $\mathcal{S} \mapsto \mathcal{S} \cap \mathrm{End}(L)$ is injective. Indeed, as observed by Hijikata, if $\mathcal{S}_1$ and $\mathcal{S}_2$ are maximal orders in $\mathrm{End}(L) \otimes \mathbf{Q}_\ell$, they form the unique unordered pair of maximal orders with intersection $\mathcal{S}_1 \cap \mathcal{S}_2$ ([30], Lemme 2.4, p. 39). Hence we have a 1-1 correspondence between lattices L' as in (i) and certain orders contained in $\mathrm{End}(L)$. This correspondence is given explicitly as

$$L' \mapsto \mathrm{End}(L') \cap \mathrm{End}(L).$$

Now the intersections $\mathrm{End}(L') \cap \mathrm{End}(L)$ are Eichler orders of $\mathrm{End}(L) \otimes \mathbf{Q}_\ell$; they are more precisely those Eichler orders for which $\mathrm{End}(L)$ is one of the two *characteristic* orders. (Recall that, in the terminology we have introduced, the two characteristic orders of $R_1 \cap R_2$ are R_1 and R_2.) In the correspondence between lattices L' and Eichler orders with this property, it is clear that the index $(L' : L)$ coincides with the level of the Eichler order $\mathrm{End}(L') \cap \mathrm{End}(L)$. Therefore, we have

Lemma **3.2** *The $\Gamma_o(M)$-structures on (A, ι) are in 1-1 correspondence with the Eichler orders of level $M = \ell^\nu$ in $\mathrm{End}(L)$ for which $\mathrm{End}(L)$ is a characteristic order.*

In order to make the correspondence more canonical, we note that the natural operation of

$$\mathrm{End}(A, \iota) \otimes \mathbf{Z}_\ell = \mathrm{End}_{R \otimes \mathbf{Z}_\ell} T_\ell$$

on $L = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} T_\ell$ serves to identify $\mathrm{End}(A,\iota) \otimes \mathbf{Z}_\ell$ with $\mathrm{End}(L)$. A more intrinsic statement of Lemma 3.2 is that the map

$$C \mapsto \mathrm{End}(A,\iota,C) \otimes \mathbf{Z}_\ell$$

induces a 1-1 correspondence between the set of $\Gamma_o(M)$-structures on (A,ι) and the set of Eichler orders of level M in $\mathrm{End}(A,\iota) \otimes \mathbf{Z}_\ell$ for which

$$\mathrm{End}(A,\iota) \otimes \mathbf{Z}_\ell$$

is a characteristic order.

In the more general situation where M is no longer necessarily a power of ℓ, we invert only the primes dividing D. For each C, the ring

$$\mathrm{End}(A,\iota,C)[\frac{1}{D}]$$

is a $\mathbf{Z}[\frac{1}{D}]$-order in the quaternion algebra $\mathrm{End}(A,\iota) \otimes \mathbf{Q}$, whose discriminant is D. We have

PROPOSITION **3.3** *The map*

$$C \mapsto \mathrm{End}(A,\iota,C)[\frac{1}{D}]$$

induces a 1-1 correspondence between $\Gamma_o(M)$*-structures on* (A,ι) *and* $\mathbf{Z}[\frac{1}{D}]$*-Eichler orders in* $\mathrm{End}(A,\iota) \otimes \mathbf{Q}$*, of level* M*, for which* $\mathrm{End}(A,\iota)[\frac{1}{D}]$ *is a characteristic order.*

We now complement Theorem 3.1 with a classification of triples (A,ι,C), where A is supersingular and where C is a $\Gamma_o(M)$-structure on (A,ι). (We no longer consider the pair (A,ι) to be fixed.) The ring of endomorphisms of (A,ι,C) is then an Eichler order of level M in the quaternion algebra $\mathrm{End}(A,\iota) \otimes \mathbf{Q}$ over $\mathbf{Q}$ of discriminant D. To see this, we can work locally: the statement is true at primes not dividing M because $\mathrm{End}(A,\iota,C)$ and $\mathrm{End}(A,\iota)$ coincide locally there, and it is true at primes not dividing D by Proposition 3.3. By a similar reasoning, we observe that this order has a natural orientation at each prime dividing its discriminant MD. Indeed, locally at the primes dividing D, this ring coincides with $\mathrm{End}(A,\iota)$, which already has a natural orientation. On the other hand, at primes dividing M the inclusion

$$\mathrm{End}(A,\iota,C) \hookrightarrow \mathrm{End}(A,\iota)$$

becomes an orientation of $\mathrm{End}(A,\iota,C)$, since $\mathrm{End}(A,\iota)$ becomes a characteristic order of $\mathrm{End}(A,\iota,C)$ at those primes.

THEOREM **3.4** *Let M be a positive integer prime to D. Let R be a maximal order as in the statement of Theorem 3.1. The construction*

$$(A, \iota, C) \mapsto \mathrm{End}(A, \iota, C) \quad \text{(with its natural orientation)}$$

induces a bijection between the set of isomorphism classes of supersingular abelian surfaces over $\mathbf{F}$ with an R-action and a $\Gamma_o(M)$-structure, and the set of isomorphism classes of oriented Eichler orders of level M in a quaternion algebra of discriminant D over $\mathbf{Q}$.

Proof. We first consider the injectivity. Assume that there is an isomorphism of oriented orders

$$\mathrm{End}(A, \iota, C) \approx \mathrm{End}(A', \iota', C')$$

for two triples (A, ι, C) and (A', ι', C'). Since the isomorphism respects the orientations, it carries $\mathrm{End}(A, \iota)$ to $\mathrm{End}(A', \iota')$. By Theorem 3.1, the pairs (A, ι) and (A', ι') are isomorphic. Therefore, we may, and shall, assume that they are *equal*.

This means that our initial isomorphism of oriented orders is induced by an automorphism of the oriented order $\mathrm{End}(A, \iota)$. However, all such automorphisms are inner, i.e., induced by automorphisms of (A, ι). Replacing C' by $\alpha C'$, for α a suitable automorphism of (A, ι), we reduce to the case where the two orders $\mathrm{End}(A, \iota, C)$ and $\mathrm{End}(A, \iota, C')$ are equal inside $\mathrm{End}(A, \iota)$. By Proposition 3.3, we see that the groups C and C' are then equal.

The surjectivity is similar. Given an oriented Eichler order $\mathcal{A}$ as in the statement of the theorem, we let $\mathcal{B} \supseteq \mathcal{A}$ be the oriented maximal order which is deduced from $\mathcal{A}$ and its orientations at the primes dividing M. Using Theorem 3.1, we write $\mathcal{B}$ in the form $\mathrm{End}(A, \iota)$, for some pair (A, ι). By Proposition 3.3, we see that $\mathcal{A}$ is necessarily equal to $\mathrm{End}(A, \iota, C)$ for some C, as required. ∎

4 Abelian Surfaces in Characteristic p

The material in this § is a variation of Oort's theme that arbitrary supersingular abelian surfaces in characteristic p are obtained from a product of two elliptic curves by dividing the product by subgroups isomorphic to α_p. This theme is developed in [9, 12, 21, 23] and in [22]. (See also the articles

of Langlands [15] and [31] for generalizations to higher-dimensional Shimura varieties.)

In this §, we again consider abelian surfaces which are furnished with an action of a maximal order in an indefinite quaternion algebra over $\mathbf{Q}$. We suppose that we are in characteristic p and that the prime p ramifies in the maximal order we are considering. This latter assumption creates a situation which is quite different from that of the previous §, where it was explicitly assumed that the characteristic (which we called q) was prime to the discriminant of the maximal order R.

Exceptional pairs

Let p be a prime number. Let $\mathcal{O}$ be a maximal order in an indefinite quaternion division algebra over $\mathbf{Q}$. We assume that p divides the discriminant of $\mathcal{O}$, which we write as the product Dp. We suppose given finite fields $\mathbf{F}_{\ell^2}$ for each prime number ℓ dividing pD, and we suppose that $\mathcal{O}$ has been oriented relative to these fields. Further, we choose an algebraic closure k of $\mathbf{F}_{p^2}$.

We consider pairs (A, ι) over k, where ι is an embedding

$$\iota\colon \mathcal{O} \to \mathrm{End}(A).$$

In our initial discussion, we suppose that such a pair is given and fixed.

LEMMA **4.1** *The abelian variety A is supersingular.*

Proof. The proof is elementary ([6], §4): we consider the $\mathbf{Q}_p$-adic Tate module $V_p(A)$ of A constructed with p-power division points of $A(k)$. Then $V_p(A)$ has rank at most 2 over $\mathbf{Q}_p$. However, it is a vector space over the quaternion division algebra $\mathcal{O} \otimes \mathbf{Q}_p$. Its rank is therefore a multiple of 4 and must accordingly be 0. ∎

In contrast to the situation which we encountered in characteristic q, the abelian variety A in a pair (A, ι) need not be isomorphic to a *product* of two supersingular elliptic curves. To explore this phenomenon, we are led to study the Dieudonné module of A, cf. [23].

More precisely, let $\mathcal{M}$ be the contravariant Dieudonné module associated to the p-divisible group of A by Oda [20], cf. [21], §1. Thus $\mathcal{M}$ is a free rank-4 module over the ring $W = W(k)$ of Witt vectors over k. This module is furnished with its usual operators F and V, plus an induced right-action of the ring $\mathcal{O}$. It follows that the tensor product

$$\mathcal{O}_p = \mathcal{O} \otimes \mathbf{Z}_p$$

acts naturally on $\mathcal{M}$ on the right. In the following discussion, we recall some standard facts about $\mathcal{O}_p$. A convenient reference for them is the second chapter of [30].

The ring $\mathcal{O}_p$ is the maximal order in a quaternion division algebra over $\mathbf{Q}_p$. Let $\wp$ be the maximal ideal of $\mathcal{O}_p$. Then $\mathcal{O}_p/\wp$ is a finite field with p^2 elements, which we may identify with $\mathbf{F}_{p^2}$, using the given orientation of $\mathcal{O}$.

Consider the submodules $F\mathcal{M}$ and $V\mathcal{M}$ of $\mathcal{M}$, and let $(F,V)\mathcal{M}$ denote their sum. These modules contain $p\mathcal{M} = FV\mathcal{M}$, so that the quotients $\mathcal{M}/F\mathcal{M}$, $\mathcal{M}/V\mathcal{M}$, $\mathcal{M}/(F,V)\mathcal{M}$ are naturally k-vector spaces. Let $a(A)$ be Oort's invariant

$$\dim_k \left(\mathrm{Hom}(\alpha_p, A)\right) = \dim_k(\mathcal{M}/(F,V)\mathcal{M}).$$

We have:

1. $\dim_k(\mathcal{M}/F\mathcal{M}) = \dim_k(\mathcal{M}/V\mathcal{M}) = 2$,
2. $1 \leq a(A) \leq 2$.
3. *The abelian variety A is isomorphic to a product of two supersingular elliptic curves if and only if $a(A) = 2$.*

Indeed, the first statement is true for the Dieudonné module attached to every abelian surface over k, cf. [21], §1. The second and third statements are true because of the above lemma, cf. our discussion of supersingular abelian surfaces over $\mathbf{F}$.

The following definition is motivated by Drinfeld's article [6].

Definition. A pair (A,ι) is *exceptional* if the action of $\mathcal{O}/p\mathcal{O}$ on $\mathcal{M}/F\mathcal{M}$ factors through the quotient $\mathbf{F}_{p^2}$ of $\mathcal{O}/p\mathcal{O}$.

Proposition **4.2** *Suppose that (A,ι) is exceptional. Then A is isomorphic to a product of two supersingular elliptic curves.*

Proof. The hypothesis may be restated as the inclusion $\mathcal{M}\wp \subseteq F\mathcal{M}$. Using it twice, we obtain the chain

$$FV\mathcal{M} = p\mathcal{M} = \mathcal{M}\wp^2 \subseteq F\mathcal{M}\wp \subseteq F^2\mathcal{M},$$

from which we infer $V\mathcal{M} \subseteq F\mathcal{M}$. (The map F acts injectively on $\mathcal{M}$, since $FV = VF = p$ on $\mathcal{M}$ and since $\mathcal{M}$ is a free $W(k)$-module.) This

latter inclusion implies the equality $(F,V)\mathcal{M} = F\mathcal{M}$. Since $F\mathcal{M}$ has k-codimension 2 in $\mathcal{M}$, we get $a(A) = 2$. As mentioned above, this numerical condition is equivalent to the desired conclusion that A is a product of supersingular elliptic curves. ∎

Remarks.

- In the situation of Proposition 4.2, we have in fact $F\mathcal{M} = V\mathcal{M} = \mathcal{M}\wp$: all the inclusions above are equalities.
- It is possible to construct examples of non-exceptional pairs (A,ι) where $a(A) = 2$.

Pure and mixed pairs

Let π be a generator of $\wp$, i.e., a uniformizing element of $\mathcal{O}_p$. Fixing a splitting of the quotient map

$$\mathcal{O}/p\mathcal{O} = \mathcal{O}_p/p\mathcal{O}_p \to F_{p^2},$$

we view $\mathbf{F}_{p^2}$ as a subring of $\mathcal{O}/p\mathcal{O}$. We have

$$\mathcal{O}/p\mathcal{O} = \mathbf{F}_{p^2} \oplus \mathbf{F}_{p^2}\pi,$$

and

$$\pi a = a^p \pi \tag{12}$$

for $a \in \mathbf{F}_{p^2}$, cf. [30], pp. 34-35.

Consider the action of the *submodule* $\mathbf{F}_{p^2}$ of $\mathcal{O}/p\mathcal{O}$ on the 2-dimensional k-vector space

$$\mathcal{L} = \mathcal{M}/F\mathcal{M}.$$

Letting σ and τ be the two embeddings $\mathbf{F}_{p^2} \hookrightarrow k$, we find a canonical decomposition of k-vector spaces $\mathcal{L} = \mathcal{L}_\sigma \oplus \mathcal{L}_\tau$, where

$$\mathcal{L}_\sigma = \{\, t \in \mathcal{L} \mid at = \sigma(a)t \text{ for all } a \in \mathbf{F}_{p^2} \,\},$$

and where a similar definition is made for $\mathcal{L}_\tau$. (The action of $\mathbf{F}_{p^2}$ on $\mathcal{L}$ should, strictly speaking, be written on the right, but we write it on the left since $\mathbf{F}_{p^2}$ is commutative.)

Because of our choice of k as an algebraic closure of $\mathbf{F}_{p^2}$, we are able to "label" σ and τ so that one embedding is the inclusion $\mathbf{F}_{p^2} \hookrightarrow k$ and the

other embedding is the conjugate of this one. We will in fact do this below, but it is preferable for the moment to allow σ and τ to play symmetrical roles.

In (the English translation of) [6], the word "special" is used to denote situations where the two spaces $\mathcal{L}_\sigma$ and $\mathcal{L}_\tau$ are each non-zero (i.e., each of dimension 1). Let us instead use the term *mixed* to refer to such situations and the term *pure* in the case where one of $\mathcal{L}_\sigma$ and $\mathcal{L}_\tau$ is 2-dimensional and the other is 0. For precision, we say that (A, ι) is *pure of type* σ if L_σ is 2-dimensional and $\mathcal{L}_\tau = 0$. We say that (A, ι) is *pure of type* τ if the situation is reversed.

Thus the space of (isomorphism class of) pairs (A, ι) is divided into three "packages":

- The mixed pairs;
- The pure pairs of type σ;
- The pure pairs of type τ.

PROPOSITION **4.3** *All pure pairs are exceptional.*

Proof. Indeed, suppose that (A, ι) is pure. Then (12) shows that π maps $\mathcal{L}_\sigma$ to $\mathcal{L}_\tau$ and *vice versa*. Since one of these is 0 and the other all of $\mathcal{M}/F\mathcal{M}$, π must be 0 on $\mathcal{L}$. ∎

Classifying subgroups of A isomorphic to α_p

As will be explained below, there is a simple relation between the mixed and pure pairs, connected with $\mathcal{O}$-stable subgroups of A which are isomorphic to the group scheme α_p. Namely, suppose we consider triples (A, ι, H), where H is an $\mathcal{O}$-stable subgroup of A which is isomorphic to α_p. Then there is a simple 1-1 correspondence, reminiscent of the Atkin-Lehner involution, which maps such triples with (A, ι) pure to such triples with (A, ι) mixed, and *vice versa*. The fact that there are "many more" mixed pairs than pure pairs is counterbalanced by the following phenomenon: If (A, ι) is pure, then the possible subgroups H are parameterized by a projective line over k. On the other hand, for (A, ι) pure, there are at most two possible subgroups H (and always at least one).

For a given pair (A, ι), the subgroups H of A which are isomorphic to α_p correspond to submodules $\mathcal{N}$ of $\mathcal{M}$ satisfying

1. $(F,V)\mathcal{M} \subseteq \mathcal{N} \subseteq \mathcal{M}$,

2. $\dim_k(\mathcal{M}/\mathcal{N}) = 1$.

The correspondence attaches to H the Dieudonné module of the abelian variety A/H, viewed as a submodule of $\mathcal{M}$ via the map on Dieudonné modules induced by the canonical quotient map $A \to A/H$. The key point is simply that the Dieudonné module of α_p is the 1-dimensional k-vector space furnished with the maps $F = V = 0$.

The $\mathcal{O}$-stable subgroups H of A which are isomorphic to α_p thus correspond to modules $\mathcal{N}$ which satisfy 1. and 2. and which are furthermore $\mathcal{O}$-stable. Note that we may view $\mathcal{N}$ as a codimension-1 subspace of the k-vector space

$$\mathcal{M}/(F,V)\mathcal{M} = \mathcal{L}/V\mathcal{L}.$$

The dimension of this latter space is $a(A)$ and thus is *a priori* 1 or 2. It follows, for instance, that there is precisely one subgroup H in case $a(A) = 1$. This case, which should be thought of as the generic case, corresponds to the situation where A is *not* the product of two supersingular elliptic curves.

The action of $\mathcal{O}$ on the line $\mathcal{M}/\mathcal{N}$ is in any case given by a homomorphism

$$\omega\colon \mathcal{O} \to \mathrm{End}_k(\mathcal{M}/\mathcal{N}) = k.$$

The homomorphism ω is necessarily the composite of the quotient map $\mathcal{O} \to \mathbf{F}_{p^2}$ with one of the two embeddings

$$\sigma, \tau : \mathbf{F}_{p^2} \to k.$$

We say that H is of *type* σ or *type* τ according as the embedding giving ω is σ or τ.

PROPOSITION **4.4** *Suppose that (A,ι) is mixed. If (A,ι) is exceptional, then A has precisely two $\mathcal{O}$-stable subgroups which are isomorphic to α_p. If (A,ι) is not exceptional, then A has precisely one such subgroup.*

Proof. As already remarked above, there is precisely one subgroup whenever $a(A) = 1$. In this case, the statement of the Proposition is correct, in view of Proposition 4.2.

Suppose now that $a(A) = 2$, so that the α_p's in A correspond to lines in $\mathcal{L} = \mathcal{M}/(F,V)\mathcal{M}$. There are precisely two such lines which are $\mathbf{F}_{p^2}$-stable, namely $\mathcal{L}_\sigma$ and $\mathcal{L}_\tau$. On the other hand, it is easy to see that π maps $\mathcal{L}_\sigma$

to $\mathcal{L}_\tau$ and *vice versa*, because of the commutation relation between π and elements of $\mathbf{F}_{p^2}$. Thus a given line $\mathcal{L}_\sigma$ or $\mathcal{L}_\tau$ is $\mathcal{O}$-stable if and only if it is killed by π. In particular, both lines are $\mathcal{O}$-stable if and only if $\pi = 0$ on $\mathcal{L}$.

Suppose, finally, that $a(A) = 2$ and that $\mathcal{L}_\sigma$ is not $\mathcal{O}$-stable. Then π induces an isomorphism $\mathcal{L}_\sigma \xrightarrow{\sim} \mathcal{L}_\tau$. On the other hand,

$$\mathcal{L}_\sigma \pi^2 = p\mathcal{L}_\sigma = 0,$$

so π must then kill $\mathcal{L}_\tau$, which is consequently $\mathcal{O}$-stable. In other words, $\mathcal{L}_\tau$ is $\mathcal{O}$-stable if $\mathcal{L}_\sigma$ is not $\mathcal{O}$-stable. Hence there is always at least one subgroup of A which is $\mathcal{O}$-stable and isomorphic to α_p. ∎

PROPOSITION **4.5** *Suppose that (A, ι) is pure. Then all subgroups of A which are isomorphic to α_p are $\mathcal{O}$-stable. Such subgroups are in 1-1 correspondence with points of the 1-dimensional projective space $\mathbf{P}(\mathcal{L})$.*

Proof. As remarked above, (A, ι) is exceptional. By Proposition 4.2, we have $a(A) = 2$, which means that the subgroups H of A which are isomorphic to α_p correspond to lines in the two-dimensional k-vector space $\mathcal{L} = \mathcal{M}/F\mathcal{M}$. Furthermore, all such lines are $\mathcal{O}$-stable. Indeed, by hypothesis $\mathcal{O}$ acts on $\mathcal{L}$ by homotheties, through the quotient $\mathbf{F}_{p^2}$ of $\mathcal{O}/p\mathcal{O}$. An element t of this latter quotient acts by the homothety $\sigma(t)$ or $\tau(t)$, according as (A, ι) is pure of type σ or τ. ∎

PROPOSITION **4.6** *In the situation of the preceding proposition, the projective space $\mathbf{P}(\mathcal{L})$ has a canonical structure over $\mathbf{F}_p$. In other words, there is an isomorphism $\mathbf{P}(\mathcal{L}) \approx \mathbf{P}^1(k)$ which is defined modulo the action of $\mathbf{PGL}(2, \mathbf{F}_p)$ on $\mathbf{P}^1(k)$.*

Proof. We have $F\mathcal{M} = \mathcal{M}\pi$. Indeed, both subspaces of $\mathcal{M}$ contain $p\mathcal{M}$ and have codimension 2 in $\mathcal{M}$; on the other hand, Proposition 4.2 shows that we have $\mathcal{M}\pi \subseteq F\mathcal{M}$. This circumstance enables us to define a p-linear automorphism of $\mathcal{M}$ as the composite

$$\phi = F \circ \pi^{-1}.$$

It is easy to check that $\phi(F\mathcal{M}) = F\mathcal{M}$, using the coincidence of $F\mathcal{M}$, $V\mathcal{M}$, and $\mathcal{M}\pi$. Hence ϕ induces a p-linear automorphism ψ of $\mathcal{L}$.

As is well known, the automorphism ψ defines an $\mathbf{F}_p$-structure on the k-vector space $\mathcal{L}$: the $\mathbf{F}_p$-vector space

$$\mathcal{L}_o = \{\, x \in \mathcal{L} \mid \psi x = x \,\}$$

is a "model" for $\mathcal{L}$ over $\mathbf{F}_p$ in the sense that the inclusion $\mathcal{L}_o \subseteq \mathcal{L}$ induces an isomorphism

$$\mathcal{L}_o \otimes_{\mathbf{F}_p} k \xrightarrow{\sim} \mathcal{L}.$$

The space $\mathcal{L}_o$ defines a model for $\mathbf{P}(\mathcal{L})$ over $\mathbf{F}_p$; the set $\mathbf{P}(\mathcal{L})$ may be viewed as the space of k-rational points of the $\mathbf{F}_p$-scheme $\mathbf{P}(\mathcal{L}_o)$.

This model depends on the choice of the uniformizer π of $\wp$. If we make another choice, we replace ψ by $\lambda\psi$ for some $\lambda \in \mathbf{F}_{p^2}^* \subseteq k^*$, where the inclusion of $\mathbf{F}_{p^2}^*$ in k^* is via σ or τ according as (A, ι) is pure of type σ or τ. A calculation shows that the space $\mathcal{L}_o$ is replaced by $\mathcal{L}'_o = \mu\mathcal{L}_o$, where μ satisfies $\mu^{1-p} = \lambda$. Multiplication by μ induces an isomorphism

$$\mathbf{P}(\mathcal{L}_o) \approx \mathbf{P}(\mathcal{L}'_o)$$

which is independent of the choice of μ. Thus $\mathbf{P}(\mathcal{L}_o)$ is an $\mathbf{F}_p$-model of $\mathbf{P}(\mathcal{L})$ which is unique up to unique isomorphism. ∎

Division by subgroups of A isomorphic to α_p

Suppose now that H is an $\mathcal{O}$-stable subgroup of (A, ι) which is isomorphic to α_p. Let B be the abelian variety A/H, and let

$$j\colon \mathcal{O} \to \mathrm{End}(B)$$

be the homomorphism giving the induced action of $\mathcal{O}$ on the quotient A/H. Then we have

PROPOSITION **4.7** *1. If (A, ι) is pure, then (B, j) is mixed.*

2. If (A, ι) is mixed and H is of type σ, then (B, j) is pure of type τ.

3. If (A, ι) is mixed and H is of type τ, then (B, j) is pure of type σ.

Proof. Consider the descending sequence of Dieudonné modules

$$\mathcal{M} \supset \mathcal{N} \supset F\mathcal{M} \supset F\mathcal{N} \supset p\mathcal{M},$$

where $\mathcal{N}$ is the submodule of $\mathcal{M}$ attached to H. The quotient $\mathcal{M}/p\mathcal{M}$ is a 4-dimensional k-vector space, and the successive quotients in the above sequence are each of dimension 1. The various quotients involved all carry an induced k-linear action of $\mathcal{O}/p\mathcal{O}$ and therefore in particular an action of the subalgebra $\mathbf{F}_{p^2}$ of $\mathcal{O}/p\mathcal{O}$. Hence they are naturally finitely generated $k \otimes_{\mathbf{F}_p} \mathbf{F}_{p^2}$-modules.

Write again $\mathcal{L}$ for $\mathcal{M}/F\mathcal{M}$, and set $\mathcal{L}' = \mathcal{N}/F\mathcal{N}$. Then we have the equality

$$[\mathcal{M}/\mathcal{N}] + [\mathcal{L}'] = [F\mathcal{M}/F\mathcal{N}] + [\mathcal{L}]$$

in the Grothendieck group of finitely generated $k \otimes_{\mathbf{F}_p} \mathbf{F}_{p^2}$-modules. The key point is that F induces an isomorphism $\mathcal{M}/\mathcal{N} \xrightarrow{\sim} F\mathcal{M}/F\mathcal{N}$ which is linear relative to $\mathbf{F}_{p^2}$ and p-linear relative to k. In particular, we have

$$\begin{aligned} \dim_k(\mathcal{L}'_\sigma) &= \dim_k(\mathcal{L}_\sigma) + \dim_k(\mathcal{M}/\mathcal{N})_\tau - \dim_k(\mathcal{M}/\mathcal{N})_\sigma \\ &= \dim_k(\mathcal{L}_\sigma) \pm 1, \end{aligned}$$

where the sign is $+1$ if H is of type τ and -1 if H is of type σ. The three statements of the proposition now follow by general reasoning. ∎

Beginning again with the triple (A, ι, H), we now endow the pair (B, j) with the group $I = A[\mathrm{Frob}]/H$, where $A[\mathrm{Frob}]$ is the kernel of the Frobenius map $A \to A^{(p)}$. The subgroup I of B is visibly $\mathcal{O}$-stable.

LEMMA **4.8** *The group I is isomorphic to α_p.*

Proof. From the point of view of Dieudonné modules, we must establish the inclusion

$$F\mathcal{M} \supseteq (F, V)\mathcal{N},$$

where $\mathcal{N}$ is as usual the submodule of $\mathcal{M}$ associated with H. The inclusion $F\mathcal{M} \supseteq F\mathcal{N}$ is clear, as $\mathcal{N}$ is a submodule of $\mathcal{M}$. Hence it is enough to show that we have $F\mathcal{M} \supseteq V\mathcal{N}$ in the case where $V\mathcal{N}$ is different from $F\mathcal{N}$.

The condition $V\mathcal{N} \neq F\mathcal{N}$ means that $a(B) = 1$ and implies, in particular, that (B, j) is mixed. Hence (A, ι) is pure, so that we have $F\mathcal{M} = V\mathcal{M}$. As the inclusion $V\mathcal{M} \supseteq V\mathcal{N}$ is clear, the lemma is proved. ∎

Let Θ now be the operator on triples (A, ι, H) which maps a given triple (A, ι, H) to (B, j, I). Then we have the formula

$$\Theta(\Theta(A, \iota, H)) = (A, \iota, H)^{(p)}. \tag{13}$$

Indeed, on the level of Dieudonné modules, Θ replaces a pair $(\mathcal{M}, \mathcal{N})$ by the pair $(\mathcal{N}, F\mathcal{M})$. A second application of Θ then leads to the pair $(F\mathcal{M}, F\mathcal{N})$.

The map $(A, \iota, H) \mapsto (A, \iota, H)^{(p)}$ induces a bijection on isomorphism classes of triples (A, ι, H). Moreover, $(A, \iota) \mapsto (A, \iota)^{(p)}$ is easily seen to map pure pairs to pure pairs and mixed pairs to mixed pairs. (More precisely, it maps pure pairs of type σ to pure pairs of type τ and *vice versa*.) We deduce the following result.

THEOREM **4.9** *The restriction of Θ to the set of triples (A, ι, H) with (A, ι) pure* (resp. mixed) *induces a 1-1 correspondence between the set of isomorphism classes of such triples and the set of isomorphism classes of triples (A, ι, H) with (A, ι) mixed* (resp. pure).

Describing all pairs in terms of exceptional pairs

We now describe the mixed (or special) pairs (A, ι) in terms of the systems $((A, \iota), H)$ where (A, ι) is a pure pair and H is a subgroup of A which is isomorphic to α_p. (By Proposition 4.5, H is automatically $\mathcal{O}$-stable.) We regard such systems as triples (A, ι, H) and define $\Theta((A, \iota, H))$ as above. We let $\theta((A, \iota, H))$ be the pair consisting of the first two elements of the triple $\Theta((A, \iota, H))$. Thus $\theta((A, \iota, H))$ consists of the abelian variety A/H with its induced $\mathcal{O}$-action.

THEOREM **4.10** *The map θ induces a surjection from the set of isomorphism classes of triples (A, ι, H) with (A, ι) pure to the set of isomorphism classes of pairs (A, ι) with (A, ι) mixed. The fiber $\theta^{-1}(A, \iota)$, for (A, ι) mixed consists of either one or two elements. The fiber consists of two elements if and only if (A, ι) is exceptional (cf. Proposition 4.4).*

Proof. By Theorem 4.9, the fiber $\theta^{-1}(A, \iota)$ is in 1-1 correspondence with the set of isomorphism classes of triples (A, ι, H) obtained as H runs over the set of $\mathcal{O}$-stable α_p's in A. As we saw in Proposition 4.4, for (A, ι) given (and mixed), there are either one or two possible subgroups H. To prove our theorem, it thus suffices to check that the situation where there are two subgroups H leads to two distinct triples (A, ι, H) (up to isomorphism).

This is indeed the case, because it is clear from the proof of Proposition 4.4 that one of the two subgroups is of type σ and the other of type τ (in the sense explained before the statement of Proposition 4.4). ∎

Classifying exceptional pairs

We now give a classification of the exceptional pairs over k, i.e., those pairs which are either pure, or else mixed exceptional. Our treatment is based on the results of §2 concerning admissible bimodules of $\mathbf{Z}$-rank 8.

Fix a supersingular elliptic curve E over k, and let $\mathcal{S} = \mathrm{End}_k(E)$. According to a well known theorem of Deuring, $\mathcal{S}$ is a maximal order (i.e., an Eichler order of level 1) in the quaternion algebra $\mathcal{S} \otimes \mathbf{Q}$, which is of discriminant p. Let $\mathcal{M}(E)$ be the Dieudonné module of E, so that $\mathcal{M}(E)$ is a free $W(k)$-module of rank 2. The space $\mathcal{M}(E)/F\mathcal{M}(E)$ is a k-vector space of dimension 1. The functorial action of $\mathcal{S}$ on this vector space is thus described by a character

$$\kappa\colon \mathcal{S} \to k.$$

Its image is necessarily the subfield $\mathbf{F}_{p^2}$ of k of cardinality p^2. Thus $\mathcal{S}$ is canonically oriented.

It will be convenient in what follows to insist on our choice of k as an algebraic closure of the residue field $\mathbf{F}_{p^2}$ of $\mathcal{O}$ at p. The two embeddings σ and τ of $\mathbf{F}_{p^2}$ into k may consequently be "labeled": we take

$$\sigma = \text{the identity embedding } \mathbf{F}_{p^2} \hookrightarrow k$$

and

$$\tau = \text{the conjugate embedding } \mathbf{F}_{p^2} \hookrightarrow k.$$

Further, the map κ becomes a map $\mathcal{S} \to \mathbf{F}_{p^2}$ and serves to identify the residue fields at p of the two orders $\mathcal{O}$ and $\mathcal{S}$. (The residue field of $\mathcal{O}$ at p is identified with $\mathbf{F}_{p^2}$ via the given orientation of $\mathcal{O}$.)

Let $\wp_{\mathcal{O}}$ and $\wp_{\mathcal{S}}$ be the maximal ideals of $\mathcal{O}$ and $\mathcal{S}$ (respectively) whose residue fields are isomorphic to $\mathbf{F}_{p^2}$. Then we have an isomorphism

$$\mathcal{O}/\wp_{\mathcal{O}} \approx \mathcal{S}/\wp_{\mathcal{S}}. \tag{14}$$

Note that (14) picks out a distinguished class of isomorphisms $\mathcal{O} \otimes \mathbf{Z}_p \approx \mathcal{S} \otimes \mathbf{Z}_p$: those which induce (14) on the level of residue fields.

Let $f\colon \mathcal{O} \to \mathrm{M}(2, \mathcal{S})$ be a homomorphism of rings. Then f defines

- An action ι of $\mathcal{O}$ on the abelian variety $A = E \times E$ (whose endomorphism ring is $\mathrm{M}(2, \mathcal{S})$);
- An $(\mathcal{O}, \mathcal{S})$-bimodule M, free of rank 8 over $\mathbf{Z}$: $M = \mathcal{S} \oplus \mathcal{S}$, with the obvious componentwise right action of $\mathcal{S}$ and the action of $\mathcal{O}$ given by left matrix multiplication

$$x \in \mathcal{O} : (s, t) \mapsto f(x) \cdot (s, t),$$

  in which (s, t) is regarded as a column matrix.

This construction defines bijections among the following three sets:

- Homomorphisms $f \colon \mathcal{O} \to \mathrm{M}(2, \mathcal{S})$ modulo the action of $\mathbf{GL}(2, \mathcal{S})$;
- Pairs (A, ι) with $a(A) = 2$, up to isomorphism;
- Bimodules ${}_{\mathcal{O}}M_{\mathcal{S}}$, free of rank 8 over $\mathbf{Z}$, up to isomorphism.

Indeed, when $a(A) = 2$, the abelian variety A in the pair (A, ι) can be taken to be $E \times E$. The embedding ι then becomes a map f as above. Further, ι and ι' give isomorphic pairs if and only if ι and ι' differ by conjugation by an automorphism of A. Hence the first two sets may be identified.

For the third set, the key point is that if M is a right $\mathcal{S}$-module, free of rank $n > 4$ over $\mathbf{Z}$, then M is *free* over $\mathcal{S}$. (This well known result of Eichler [7] is discussed in [25], §34 and in [9], §2.) If M is of rank 4 over $\mathbf{Z}$, then M is isomorphic to $\mathcal{S} \oplus \mathcal{S}$. After we fix an isomorphism between these modules, we may write $\mathrm{End}_{\mathcal{S}} M = \mathrm{M}(2, \mathcal{S})$. Thus a left $\mathcal{O}$-structure on M is given by a map f as above.

In the dictionary $A \leftrightarrow f$, the Dieudonné module $\mathcal{M} = \mathcal{M}(A)$ is given as the direct sum of two copies of the Dieudonné module $\mathcal{M}(E)$ of E. The right-action of $\mathcal{O}$ on $\mathcal{M}$ is given by (transpose) matrix multiplication. Since

$$F\mathcal{M}(E) = \mathcal{M}(E)\wp_{\mathcal{S}},$$

the pair (A, ι) is exceptional if and only if we have

$$f(\wp_{\mathcal{O}}) \subseteq \mathrm{M}(2, \wp_{\mathcal{S}}),$$

where $\mathrm{M}(2, \wp_{\mathcal{S}})$ is the set of those matrices in $\mathrm{M}(2, \mathcal{S})$ whose coefficients lie in $\wp_{\mathcal{S}}$. In the language of bimodules M, this inclusion translates to the inclusion

$$\wp_{\mathcal{O}} M \subseteq M \wp_{\mathcal{S}}. \tag{15}$$

Since M is locally free over $\mathcal{O}$ and over $\mathcal{S}$, (15) is equivalent to the equality $\wp_{\mathcal{O}} M = M \wp_{\mathcal{S}}$. Hence (A, ι) is exceptional if and only if M is admissible in the sense of §2.

In the notation of §2, the set Σ is the singleton set containing the prime p. The set Δ contains those primes different from p which are ramified in $\mathcal{O}$. The integer D which was defined in §2 to be the product of those primes in Δ thus coincides with the integer D defined above. We have

$$D = \frac{\mathrm{disc}(\mathcal{O})}{p}.$$

Since Σ is a singleton set, admissible modules are described up to local isomorphism by a single parameter r_p, which can take the three possible values 0, 1, 2. In the dictionary $(A, \iota) \leftrightarrow M$, the value $r_p = 1$ clearly corresponds to mixed exceptional pairs. The values $r_p = 2$ and $r_p = 0$ correspond to the pure pairs of type σ and the pure pairs of type τ, respectively. Finally, in the notation of §2, the integer N (which describes the level of the Eichler order) takes the value p for mixed exceptional pairs and the value 1 for pure pairs.

From this discussion and from Theorem 2.4, we get information about the ring $\mathrm{End}((A, \iota))$, i.e., about the commutant of $\mathcal{O}$ in $\mathrm{End}(A)$, when (A, ι) is exceptional:

THEOREM **4.11** *For (A, ι) pure, the ring $\mathrm{End}((A, \iota))$ is a maximal order in a quaternion algebra of discriminant D. For (A, ι) mixed and exceptional, the ring $\mathrm{End}((A, \iota))$ is an Eichler order of level p in a quaternion algebra of discriminant D.*

As a translation of Theorem 2.3, we get the following statement.

THEOREM **4.12** *Let (A_o, ι_o) be an exceptional pair. The map*

$$(A, \iota) \mapsto \mathrm{Hom}((A_o, \iota_o), (A, \iota))$$

establishes a bijection between the set of isomorphism classes of exceptional pairs (A, ι) of the same "type" as (A_o, ι_o) (i.e., mixed, pure of type σ, pure of type τ) *and isomorphism classes of locally free rank-1 right $\mathrm{End}((A_o, \iota_o))$-modules.*

To have a theorem in the style of Theorem 2.4, we must translate into our context the canonical orientation of the order $\Lambda = \mathrm{End}(A, \iota)$. Thus, in

all cases we must exhibit a canonical map $\Lambda \to \mathbf{F}_{q^2}$ for each prime q dividing D, where $\mathbf{F}_{q^2}$ is the residue field of $\mathcal{O}$ at q. Further, in the case where (A, ι) is mixed (and exceptional), we must describe a canonical maximal order $\Lambda^\sim$ containing Λ.

For the latter point, we recall that for (A, ι) mixed exceptional, the abelian variety A contains precisely two subgroups which are $\mathcal{O}$-stable and isomorphic to α_p (Proposition 4.4). As shown by the proof of Proposition 4.4, one of these subgroups is of type σ and the other of type τ. Let H be the $\mathcal{O}$-stable α_p of type σ. The operator Θ considered above sends (A, ι, H) to a triple (B, j, I) where (B, j) is pure of type τ (Proposition 4.7). Because H is the unique α_p in A of type σ, H is stable under $\mathrm{End}((A, \iota))$. Hence there is an induced map

$$\Lambda = \mathrm{End}((A, \iota)) \to \mathrm{End}(B, j).$$

Since $\mathrm{End}(B, j)$ is a maximal order by Theorem 4.11, this inclusion is an orientation of $\mathrm{End}((A, \iota))$ at p.

Now let q be a prime divisor of D and let (A, ι) be an exceptional pair. Let $\mathcal{Q}$ be the maximal ideal of $\mathcal{O}$ whose residue field is $\mathbf{F}_{q^2}$. To orient $\mathrm{End}((A, \iota))$ at q, we remark that the Tate module $T_q(A)$ of A at q is naturally an $\mathcal{O} \otimes \mathbf{Z}_q$-module. It is necessarily free of rank 1 over $\mathcal{O} \otimes \mathbf{Z}_q$. In particular, the finite group $T_q(A)/\mathcal{Q}T_q(A)$ is a 1-dimensional $\mathbf{F}_{q^2}$-vector space. The natural operation of the ring $\mathrm{End}((A, \iota))$ on $T_q(A)/\mathcal{Q}T_q(A)$ is thus described by a canonical character

$$\rho_q \colon \mathrm{End}((A, \iota)) \to \mathbf{F}_{q^2}.$$

(One can check that this definition of ρ_q is consistent with the definition given in §2 and the dictionary $M \leftrightarrow A$.)

From Theorem 2.4, we now get the following result.

THEOREM **4.13** *The constructions* $(A, \iota) \mapsto \mathrm{End}((A, \iota))$ *give bijections between:*

- *The set of isomorphism classes of pure pairs* (A, ι) *of type* σ *and the set of isomorphism classes of oriented maximal orders in a quaternion algebra of discriminant* D*;*

- *The set of isomorphism classes of pure pairs* (A, ι) *of type* τ *and the set of isomorphism classes of oriented maximal orders in a quaternion algebra of discriminant* D*;*

- *The set of isomorphism classes of mixed exceptional pairs (A, ι) and the set of isomorphism classes of oriented Eichler orders of level p in a quaternion algebra of discriminant D.*

Remark. Theorem 4.13 constructs in particular a canonical bijection between the sets of isomorphism classes of pure pairs of type σ and pure pairs of type τ. This correspondence is the Frobenius map $(A, \iota) \mapsto (A, \iota)^{(p)}$.

$\Gamma_o(M)$-structures

Let (A, ι) be given over k. Suppose that $M \geq 1$ is an integer which is prime to the discriminant pD of $\mathcal{O}$. A $\Gamma_o(M)$-structure on (A, ι) is an $\mathcal{O}$-stable subgroup C of $A(k)$ which is isomorphic to $(\mathbf{Z}/M\mathbf{Z})^2$ as an abelian group. As in the situation we discussed above (in the context of characteristic q), let $\mathrm{End}(A, \iota, C)$ be the subring of $\mathrm{End}(A, \iota)$ consisting of $\mathcal{O}$-endomorphisms λ of A for which $\lambda(C) \subseteq C$. We have results which parallel those in the situation already discussed.

In particular, for each C, the ring

$$\mathrm{End}(A, \iota, C)[\frac{1}{pD}]$$

is a $\mathbf{Z}[\frac{1}{pD}]$-order in the quaternion algebra $\mathrm{End}(A, \iota) \otimes \mathbf{Q}$. (Incidentally, it is clear that this algebra is a quaternion algebra of discriminant D over $\mathbf{Q}$. This follows easily from Theorem 4.9 and Theorem 4.12.) We have

PROPOSITION **4.14** *The map*

$$C \mapsto \mathrm{End}(A, \iota, C)[\frac{1}{pD}]$$

induces a 1-1 correspondence between $\Gamma_o(M)$-structures on (A, ι) and $\mathbf{Z}[\frac{1}{pD}]$-Eichler orders in $\mathrm{End}(A, \iota) \otimes \mathbf{Q}$, of level M, for which $\mathrm{End}(A, \iota)[\frac{1}{pD}]$ is a characteristic order.

We now classify triples (A, ι, C), where (A, ι) is an exceptional pair and where C is a $\Gamma_o(M)$-structure on (A, ι). There are three cases to consider, according to the type of (A, ι) (mixed, pure of type σ, pure of type τ). To fix ideas, we treat in detail only the case where (A, ι) is mixed exceptional. The ring $\mathrm{End}(A, \iota, C)$ is then an Eichler order of level Mp in the quaternion algebra $\mathrm{End}(A, \iota) \otimes \mathbf{Q}$ over $\mathbf{Q}$ of discriminant D. To see this, we can work

locally: the statement is true at primes not dividing M by Theorem 4.11, and it is true at primes not dividing pD by Proposition 4.14. By a similar reasoning, we observe that this order has a natural orientation at each prime dividing its discriminant pMD. Indeed, locally at the primes dividing pD, this ring coincides with $\mathrm{End}(A,\iota)$, which already has a natural orientation. On the other hand, at primes dividing M the inclusion

$$\mathrm{End}(A,\iota,C) \hookrightarrow \mathrm{End}(A,\iota)$$

becomes an orientation of $\mathrm{End}(A,\iota,C)$, since $\mathrm{End}(A,\iota)$ becomes a characteristic order of $\mathrm{End}(A,\iota,C)$ at those primes.

THEOREM **4.15** *The map*

$$(A,\iota,C) \mapsto \mathrm{End}(A,\iota,C) \quad \text{(with its natural orientation)}$$

induces a bijection between the set of isomorphism classes of exceptional mixed pairs with $\Gamma_o(M)$-structure and the set of isomorphism classes of oriented Eichler orders of level pM in a quaternion algebra over $\mathbf{Q}$ of discriminant D.

Proof. We first consider the injectivity. Assume that there is an isomorphism of oriented orders

$$\mathrm{End}(A,\iota,C) \approx \mathrm{End}(A',\iota',C')$$

for two triples (A,ι,C) and (A',ι',C'). Since the isomorphism respects the orientations, it carries $\mathrm{End}(A,\iota)$ to $\mathrm{End}(A',\iota')$. By Theorem 4.13, the pairs (A,ι) and (A',ι') are isomorphic. Therefore, we may, and shall, assume that they are *equal*.

This means that our initial isomorphism of oriented orders is induced by an automorphism of the oriented order $\mathrm{End}(A,\iota)$. However, all such automorphisms are inner, i.e., induced by automorphisms of (A,ι). Replacing C' by $\alpha C'$, for α a suitable automorphism of (A,ι), we reduce to the case where the two orders $\mathrm{End}(A,\iota,C)$ and $\mathrm{End}(A,\iota,C')$ are equal inside $\mathrm{End}(A,\iota)$. By Proposition 4.14, we see that the groups C and C' are then equal.

The surjectivity is similar. Given an oriented Eichler order R as in the statement of the theorem, we let $S \supseteq R$ be the oriented order of level p which is deduced from R and its orientations at the primes dividing M. Using Theorem 4.13, we write S in the form $\mathrm{End}(A,\iota)$, for some mixed

exceptional (A, ι). By Proposition 4.14, we see that R is necessarily equal to $\mathrm{End}(A, \iota, C)$ for some C, as required. ∎

We have a similar result for pure pairs:

THEOREM **4.16** *The construction*

$$(A, \iota, C) \mapsto \mathrm{End}(A, \iota, C) \quad \text{(with its natural orientation)}$$

induces bijections between:

- *The set of isomorphism classes of pure pairs of type σ, with $\Gamma_o(M)$-structure, and the set of isomorphism classes of oriented Eichler orders of level M in a quaternion algebra over $\mathbf{Q}$ of discriminant D.*
- *The set of isomorphism classes of pure pairs of type τ, with $\Gamma_o(M)$-structure, and the set of isomorphism classes of oriented Eichler orders of level M in a quaternion algebra over $\mathbf{Q}$ of discriminant D.*

We remark that Theorem 4.10 extends in a straightforward manner to the case of pairs (A, ι) which are furnished with $\Gamma_o(M)$-structures. Namely, let (A, ι, C) be an abelian surface with an $\mathcal{O}$- action and a $\Gamma_o(M)$-structure. Let H be an $\mathcal{O}$-stable subgroup of A which is isomorphic to α_p. Then the $\mathcal{O}$-abelian variety $\theta(A, \iota, H)$ has a natural $\Gamma_o(M)$-structure, namely the image of C in A/H. We write $\theta(A, \iota, C, H)$ for the resulting triple.

THEOREM **4.17** *The map θ induces a surjection from the set of isomorphism classes of systems (A, ι, C, H) with (A, ι) pure to the set of isomorphism classes of pairs triples (A, ι, C) with (A, ι) mixed. The fiber $\theta^{-1}(A, \iota, C)$, for (A, ι) mixed consists of either one or two elements. The fiber consists of two elements if and only if (A, ι) is exceptional.*

5 Characteristic p and characteristic q

In this §, we suppose that p and q are distinct prime numbers. We consider as above a maximal order $\mathcal{O}$ in an indefinite quaternion algebra over $\mathbf{Q}$ whose discriminant is a product Dp. We assume further that this discriminant is divisible by q, so that $q|D$. As in §3, we consider a maximal order R in a quaternion algebra of discriminant D/q. This quaternion algebra may, for example, be isomorphic to $\mathrm{M}(2, \mathbf{Q})$; in that case, we have $D = q$.

As in the previous two §§, we wish to endow $\mathcal{O}$ and R with orientations. For this, we can take $\mathbf{F}_{\ell^2}$ to be the residue field of $\mathcal{O}$ at ℓ for each ℓ dividing Dp and give $\mathcal{O}$ its *canonical orientation*, consisting of the residue maps $\mathcal{O} \to \mathbf{F}_{\ell^2}$ for each ℓ. We assume that orientations of R have been chosen; these are maps $R \to \mathbf{F}_{\ell^2}$ for each prime ℓ dividing D/q. (In the case $D = q$, there are no choices to be made.)

We again choose k and $\mathbf{F}$ to be algebraic closures of $\mathbf{F}_{p^2}$ and $\mathbf{F}_{q^2}$, respectively.

Comparison of isomorphism classes

The results of the previous two §§ can be summarized compactly by the following result.

THEOREM **5.1** *Let M be a positive integer prime to pD. Then the following are in natural 1-1 correspondence:*

- *Isomorphism classes of supersingular abelian surfaces over $\mathbf{F}$ with R-multiplication and a $\Gamma_o(M)$-structure;*
- *Isomorphism classes of (supersingular) abelian surfaces over k with an $\mathcal{O}$-action which is pure of type σ, and a $\Gamma_o(M)$-structure;*
- *Isomorphism classes of (supersingular) abelian surfaces over k with an $\mathcal{O}$-action which is pure of type τ, and a $\Gamma_o(M)$-structure.*

Further, the following two sets are naturally in 1-1 correspondence:

- *The set of isomorphism classes of supersingular abelian surfaces over $\mathbf{F}$ with R-multiplication and a $\Gamma_o(pM)$-structure;*
- *The set of isomorphism classes of (supersingular) abelian surfaces over k with an $\mathcal{O}$-action which is mixed exceptional, and a $\Gamma_o(M)$-structure.*

Proof. Both assertions follow immediately on comparing the statements of Theorems 3.4, 4.15, and 4.16. ∎

Notice that, in the statement of Theorem 5.1, no explicit reference is made to the orientations of $\mathcal{O}$ and R. These orientations intervene, however, in the "natural" 1-1 correspondences of the Theorem. It is easy to trace how these correspondences change if we change one of the orientations. For example, suppose that we change the orientation of R at a prime ℓ dividing

D/q. Then our correspondences between characteristic p and characteristic q objects are composed with the Atkin-Lehner style involution $A \mapsto A/A[\lambda]$ on objects in characteristic p. (Here λ is the maximal ideal of R of residue characteristic ℓ.)

To make a concrete example of the statements of the Theorem, let us consider the case where $D = q$ and R is the matrix ring $\mathrm{M}(2, \mathbf{Z})$. To give a supersingular abelian surface with R-multiplication and a $\Gamma_o(M)$-structure is to give a supersingular elliptic curve with a $\Gamma_o(M)$-structure. Hence the Theorem provides a 1-1 correspondence between the set of isomorphism classes of supersingular elliptic curves, with $\Gamma_o(M)$-structures, over $\mathbf{F}$ and pure pairs (A, ι) of type σ over k. This correspondence in fact depends only on the orientation of $\mathcal{O}$ at the prime q, and it changes by the Frobenius automorphism of $\mathbf{F}$ if the orientation changes. It is entirely canonical, once one agrees to endow $\mathcal{O}$ with its canonical orientation and to choose $\mathbf{F}$ to be an algebraic closure of $\mathbf{F}_{q^2}$.

Similarly, we get a 1-1 correspondence between the set of isomorphism classes of supersingular elliptic curves with $\Gamma_o(Mp)$-structures over $\mathbf{F}$ and the set of mixed exceptional pairs (A, ι) over k, with $\Gamma_o(M)$-structures. This correspondence depends both on the orientation at p and the orientation at q of $\mathcal{O}$; since these orientations are natural, the correspondence is again completely canonical. If we change the orientation at p, we change the correspondence by the Atkin-Lehner involution, relative to the prime p, on the set of isomorphism classes of elliptic curves with $\Gamma_o(Mp)$-structures. It is perhaps worth stressing that we could hope for no such distinguished correspondence if we replaced, say, $\mathbf{F}$ by another algebraic closure $\mathbf{F}'$ of $\mathbf{F}_q$. Indeed, we would then deduce (for instance) a bijection between the sets of isomorphism classes of supersingular elliptic curves over $\mathbf{F}$ and $\mathbf{F}'$. Such a bijection amounts (in general) to an identification of the subfields of order q^2 of $\mathbf{F}$ and $\mathbf{F}'$.

We turn now to a compatibility question concerning the correspondences of Theorem 5.1. Suppose that (A, ι, C) is given over k, where (A, ι) is mixed exceptional and C is a $\Gamma_o(M)$-structure on (A, ι). Then we may make pure triples from the mixed triple (A, ι, C) in four ways. Indeed, as we have noted repeatedly, there are unique subgroups H_σ and H_τ of A on which $\mathcal{O}$ acts via σ and τ, respectively. The resulting quotients A/H_σ and A/H_τ carry natural $\mathcal{O}$-actions and $\Gamma_o(M)$-structures. Abusing notation somewhat, we will call the resulting two triples $(A/H_\sigma, \bar{\iota}, \overline{C})$ and $(A/H_\tau, \bar{\iota}, \overline{C})$. They are respectively pure of type τ and pure of type σ by Proposition 4.7. Applying the Frobenius automorphism ${}^{(p)}$ of k to these triples, we obtain two further

triples $(A/H_\sigma, \bar\iota, \overline{C})^{(p)}$ and $(A/H_\tau, \bar\iota, \overline{C})^{(p)}$, which are pure of type σ and τ, respectively. They are in fact the two triples in the fiber $\theta^{-1}(A, \iota, C)$, where θ is as in Theorem 4.17.

Suppose that (B, j, C_M, C_p) is the R-abelian surface which is associated to (A, ι, C) by Theorem 5.1. (We understand that C_M and C_p are $\Gamma_o(M)$- and $\Gamma_o(p)$-structures, respectively.) We deduce from (B, j, C_M, C_p) two abelian surfaces with $\Gamma_o(M)$-structures by the standard degeneracy constructions:

$$(B, j, C_M), \qquad (B/C_p, \bar\jmath, \overline{C}_M).$$

Here, $\bar\jmath$ and $\overline{C}_M$ represent the R-action and $\Gamma_o(M)$-structure on B/C_p which come from those on B.

PROPOSITION **5.2** *The correspondences of Theorem 5.1 take* $(A/H_\sigma, \bar\iota, \overline{C})$ *and* $(A/H_\sigma, \bar\iota, \overline{C})^{(p)}$ *to* (B, j, C_M). *They map the two triples* $(A/H_\tau, \bar\iota, \overline{C})$ *and* $(A/H_\tau, \bar\iota, \overline{C})^{(p)}$ *to* $(B/C_p, \bar\jmath, \overline{C}_M)$.

Proof. The proof consists of a simple tracing through of the definitions. In particular, we make use necessarily of the definition we have given for the orientation at p of the order $\mathrm{End}(A, \iota, C)$. This definition is given in the discussion which precedes Theorem 4.13. ∎

Bad Reduction of Shimura Curves

We return to the theme of singular points on Shimura curves, which has not been mentioned since the Introduction. Suppose that L is a maximal order in an indefinite quaternion division algebra over $\mathbf{Q}$. An L-abelian surface (over a base T) is a pair (A, ι), where ι is an injection $L \hookrightarrow \mathrm{End}_T(A)$. The pair (A, ι) is said to be *special* if the map ι satisfies the condition

$$\mathrm{Trace}_{\mathcal{O}_T}\Big(\iota(x) \;\Big|\; \mathrm{Lie}(A)\Big) = \mathrm{Tr}(x) \in \mathbf{Q}$$

for all $x \in L$, where "Tr" is the reduced trace $L \to \mathbf{Z}$. This condition, automatic when the discriminant of L is invertible on T, was introduced in [6]. In characteristic p, for p a divisor of the discriminant of L, it corresponds to the condition that (A, ι) be "mixed." For n a positive integer which is invertible on T, a level-n structure on (A, ι) is an L-isomorphism $\gamma\colon A[n] \approx L/nL$, where $A[n]$ is the kernel of multiplication of n on A.

Consider the functor on $\mathbf{Z}[\frac{1}{n}]$-schemes which maps T to the set of isomorphism classes of special (A, ι) with level-n structures. According to Drinfeld ([6], Proposition 4.4), this functor is representable by a projective 1-dimensional $\mathbf{Z}[\frac{1}{n}]$-scheme $\mathcal{S}_n$, provided that $n \geq 3$. (For generalizations to higher-dimensional Shimura varieties, see [31] and the summary in [24].) In the following discussion, we fix n and write simply $\mathcal{S}$ for $\mathcal{S}_n$. This gives us the freedom to append a subscript to $\mathcal{S}$ to denote a *base change*.

Assume that n is prime to the discriminant of L, and take a prime p dividing this discriminant. The formal completion of $\mathcal{S}$ along (p) was determined by Cerednik [4] and Drinfeld [6], §4. Their result implies that the curve $\mathcal{S}_n$ becomes a disjoint union of "degenerating curves" of the type considered by Mumford [19] over the completion of the ring of integers of the maximal unramified extension of $\mathbf{Z}_p$. In particular, the scheme $\mathcal{S}_{\overline{\mathbf{F}}_p}$ can be expressed as a projective curve whose normalization is a disjoint union of rational curves, and whose only singular points are ordinary double points. A modular interpretation of the singular points and irreducible components of $\mathcal{S}_{\overline{\mathbf{F}}_p}$ is implicit in Drinfeld's method and is provided (essentially in the form we need) by Zink in [31].

Namely, let k be an algebraic closure of $\mathbf{F}_p$. The singular points of $\mathcal{S}(k)$ are represented by those triples (A, ι, γ) for which (A, ι) is a mixed exceptional pair ([31], Satz 3.10, cf. [24], 1.6). For the components, one has a construction which associates a rational curve in $\mathcal{S}_k$ to each object (A, ι, γ) and each L-stable subgroup $H \approx \alpha_p$ of A ([31], 5.13 and 5.15). The set of k-rational points of this rational curve may be described as follows (in the language of §4): The quotient A/H (with the induced action of L) is a *pure* L-abelian surface. This quotient has a projective line of L-stable subgroups isomorphic to α_p (Proposition 4.5). Dividing by these subgroups, we obtain a series of mixed L-abelian surfaces which includes in particular the pair $(A, \iota)^{(p)}$. These mixed surfaces inherit level-n structures from (A, ι).

In classifying the components of $\mathcal{S}_k$, we may note that all pure L-abelian surfaces arise by dividing mixed surfaces by an α_p (Th. 4.9) and that all components of $\mathcal{S}_k$ arise from the construction we have just sketched ([31], 5.15). It follows that *the set of components of $\mathcal{S}_k$ is in bijection with the set of isomorphism classes of pure L-abelian surfaces over k with level-n structures.*

Thus the singular points are represented by mixed exceptional (A, ι)'s (with level structures), while the components correspond to pure (A, ι)'s (with level structures). Furthermore, the recipe we have given for associat-

ing components to pure surfaces provides the following additional piece of information. Let (A, ι) be a mixed exceptional pair, and let H_1 and H_2 be the two L-stable subgroups of A which are isomorphic to α_p (cf. Proposition 4.4). Then the components corresponding to A/H_1 and A/H_2 (with their induced L-actions and level structures) are the two components intersecting at the singular point $(A, \iota)^{(p)}$. Since all isomorphism classes of triples (A, ι, γ) with (A, ι) exceptional are defined over the subfield $\mathbf{F}_{p^2}$ of k, we may write instead that the components corresponding to the varieties $(A/H_i)^{(p)}$ are those which intersect at A.

We apply these results to the coarse moduli scheme $\mathcal{C}$ which was described in the Introduction to this article. For this, we take $L = \mathcal{O}$, where $\mathcal{O}$ is as in §4. We again write the discriminant of $\mathcal{O}$ as the product pD and let k be an algebraic closure of the residue field $\mathbf{F}_{p^2}$ of $\mathcal{O}$ at p.

Let M be a positive integer prime to the discriminant of $\mathcal{O}$, and consider the problem of classifying $\mathcal{O}$-abelian surfaces with a $\Gamma_o(M)$ structure. This problem is "solved" by considering a multiple $n \geq 3$ of M which is again prime to the discriminant of $\mathcal{O}$: we divide the scheme $\mathcal{S}_n$ by the appropriate subgroup Γ of $(\mathcal{O}/n\mathcal{O})^*$. Let $\mathcal{C}$ then denote the indicated quotient, so that $\mathcal{C}$ is a curve over $\mathbf{Z}[\frac{1}{n}]$.

It follows from general principles ([14], Proposition 3.2) that the curve $\mathcal{C}_{\overline{\mathbf{F}}_p}$ is again a projective curve whose normalization is a disjoint union of rational curves, and whose only singular points are ordinary double points. Moreover, the components and singular points of $\mathcal{C}_k$ are obtained by from the components and singular points of $\mathcal{S}_{nk}$ by division by Γ. This gives

THEOREM **5.3** *The singular points of the Shimura curve $\mathcal{C}_k$ represent the isomorphism classes of triples (A, ι, C_M), where (A, ι) is a mixed exceptional $\mathcal{O}$-abelian surface and C_M is a $\Gamma_o(M)$-structure on (A, ι). The components of $\mathcal{C}_k$ are in bijection with the isomorphism classes of triples (A, ι, C_M), where (A, ι) is a pure $\mathcal{O}$-abelian surface. Further, let P be the singular point of $\mathcal{C}_k$ parameterized by (A, ι, C_M). Then the two components meeting at P correspond to the triples $(A/H_\ell, \bar{\iota}, \overline{C}_M)^{(p)}$. Here H_ℓ denotes one of the two possible $\mathcal{O}$-stable subgroups of A which are isomorphic to α_p, while $\bar{\iota}$ and $\overline{C}_M$ denote the $\mathcal{O}$-action and $\Gamma_o(M)$-structure which are inherited by the quotient A/H_ℓ.*

In view of Theorems 4.16 and 4.15, Theorem 5.3 may be described in terms of quaternion arithmetic. For this, let $\mathcal{E}$ be the set of isomorphism

classes of oriented Echler orders of level pM in rational quaternion algebras of discriminant D. (The orientations are taken relative to the residue fields of $\mathcal{O}$ at the various primes r dividing D.) Similarly, let $\mathcal{V}$ be the set of isomorphism classes of oriented orders of level M in quaternion algebras of discriminant D. There are two natural "degeneracy" maps $\mathcal{E} \rightrightarrows \mathcal{V}$. The first map, $t\colon \mathcal{E} \to \mathcal{V}$, takes the class of an oriented order $\mathcal{A}$ of level Mp to the class of the oriented order $\mathcal{B} \supset \mathcal{A}$ in $\mathcal{A} \otimes \mathbf{Q}$ which is deduced from $\mathcal{A}$ together with the orientation of $\mathcal{A}$ at p. The second map, $h\colon \mathcal{E} \to \mathcal{V}$, first changes the orientation of $\mathcal{A}$ at p and then applies the first map.

Theorem 5.3 states that the set of singular points of $\mathcal{C}_k$ is canonically the set $\mathcal{E}$. Secondly, the set of components is the union of two subsets $\mathcal{V}_\sigma$ and $\mathcal{V}_\tau$ (the sets of pure triples of type σ and type τ, respectively), each of which is canonically $\mathcal{V}$. Finally (because of the orientation at p we have chosen for the endomorphism ring of an exceptional mixed triple) the two components meeting at $e \in \mathcal{E}$ are $t(e)$, viewed in $\mathcal{V}_\sigma$ and $h(e)$, viewed in $\mathcal{V}_\tau$.

Consider the "quaternionic" graph $\mathcal{G}$ with the following description:

- The set of edges of $\mathcal{G}$ is the set $\mathcal{E}$.
- The set of vertices of $\mathcal{G}$ is the set $\mathcal{V} \times \{1, 2\}$.
- An edge $e \in \mathcal{E}$ connects the vertices $(t(e), 1)$ and $(h(e), 2)$.

The author visualizes $\mathcal{G}$ with its vertices $(v, 1)$ to the left and its vertices $(v, 2)$ to the right. Each edge connects a vertex from the left-hand group to a vertex from the right-hand group. (Thus $\mathcal{G}$ is a "bipartite" graph.) Our edges, if oriented, would presumably have their tails in the left-hand group and their heads in the right-hand group. This motivated the choice of "h" and "t" as symbols for the maps $\mathcal{E} \rightrightarrows \mathcal{V}$.

Consider the *dual graph* attached to the curve $\mathcal{C}_k$, whose vertices are the components of $\mathcal{C}_k$ and whose edges are the singular points of $\mathcal{C}_k$. The edge which corresponds to a singular point P connects the two vertices corresponding to the components meeting at P.

THEOREM **5.4** *The dual graph attached to $\mathcal{C}_k$ is the quaternionic graph $\mathcal{G}$.*

Proof. The Theorem is a restatement of Theorem 5.3 along the lines of the discussion just above. The change introduced by the statement of the theorem is that we number two copies of $\mathcal{V}$, rather than index them by the maps $\mathcal{O} \rightrightarrows k$. This is possible because of our choice of k as an algebraic

closure of the residue field $\mathbf{F}_{p^2}$ of $\mathcal{O}$ at p. The residue map $\mathcal{O} \to \mathbf{F}_{p^2}$ defines $\sigma: \mathcal{O} \to k$, and its conjugate by the non-trivial automorphism of $\mathbf{F}_{p^2}$ gives τ. ∎

We turn now to the Shimura curve $\mathcal{X}$ which was described in the Introduction. We again let q be a prime dividing D and let R be a maximal order in a quaternion algebra of discriminant D/q. Note that D/q is a product of an even number of primes, so that R is a maximal order in an indefinite rational quaternion algebra. For definiteness, we assume that $R = \mathrm{M}(2, \mathbf{Z})$ if $D = q$. We also assume that orientations of R at the prime divisors D/q have been fixed; these are isomorphisms between the residue fields of R and of $\mathcal{O}$ at each prime dividing D/q. For each integer $N \geq 1$ which is prime to D/q, we have a modular curve $\mathcal{X}_o(N)$ over $\mathbf{Q}$:

- If $R = \mathrm{M}(2, \mathbf{Z})$, we let $\mathcal{X}_o(N)$ be the classical modular curve $X_o(N)$.
- If R is a maximal order in an indefinite quaterion *division* algebra, we let $\mathcal{X}_o(N)$ be the coarse moduli scheme over $\mathbf{Q}$ attached to the problem of classifying R-abelian surfaces with a $\Gamma_o(N)$-structure.

We are interested in the reduction of $\mathcal{X}_o(N)$ at the prime number q. If q is prime to N, there is no problem: the curve $\mathcal{X}_o(N)$ extends naturally to a curve over $\mathbf{Z}_{(q)}$, whose special fiber we will call $\mathcal{X}_o(N)_{\mathbf{F}_q}$. The *supersingular points* on $\mathcal{X}_o(N)_{\mathbf{F}_q}$ are those represented by elliptic curves or R-abelian surfaces which are supersingular in the sense that they have no points of q-power order over an algebraic closure of $\mathbf{F}_q$. As noted in §3, the supersingular R-abelian surfaces are automatically products of supersingular elliptic curves. Moreover, in the case $R = \mathrm{M}(2, \mathbf{Z})$ it is equivalent to classify supersingular elliptic curves or supersingular R-abelian surfaces.

Take $\mathbf{F}$ to be an algebraic closure of the residue field $\mathbf{F}_{q^2}$ of $\mathcal{O}$ at q, as in §3. Then by Theorem 3.4, we have a canonical bijection between the set of supersingular points on $\mathcal{X}_o(N)(\mathbf{F})$ and the set of isomorphism classes of oriented Eichler orders of level N in a quaternion algebra of discriminant D. Especially:

- The set of supersingular points on $\mathcal{X}_o(M)$ is canonically the set $\mathcal{V}$.
- The set of supersingular points on $\mathcal{X}_o(Mp)$ is canonically the set $\mathcal{E}$.

Now consider the curve $\mathcal{X}_o(Nq)$, where q is again prime to N. In the case where $R = \mathrm{M}(2, \mathbf{Z})$, the curve $\mathcal{X}_o(Nq)$ has a well known model over $\mathbf{Z}_{(q)}$

which was studied by Deligne-Rapoport [5] and by Katz-Mazur [13]. (See especially [5], Ch. VI, Th. 6.9.) As noted in the Introduction, an analogous model is available in the case where $R \otimes \mathbf{Q}$ is a division algebra [5, 18, 3]. The result is that the special fiber $\mathcal{X}_o(Nq)_{\mathbf{F}_q}$ has two irreducible components, each isomorphic to $\mathcal{X}_o(N)_{\mathbf{F}_q}$. The curve $\mathcal{X}_o(Nq)_{\mathbf{F}_q}$ is obtained from its normalization by the following construction: one attached a supersingular point P on the first copy of $\mathcal{X}_o(N)_{\mathbf{F}_q}$ to the point $P^{(q)}$ on the second copy. The set of singular points of $\mathcal{X}_o(Nq)_{\mathbf{F}}$ is thus in bijection with the set of isomorphism classes of oriented Eichler orders of level N in a quaternion algebra of discriminant D. In particular:

THEOREM **5.5** *Let M be a positive integer prime to pD. The set of singular points on $\mathcal{X}_o(Mpq)_{\mathbf{F}}$ is in bijection with the set $\mathcal{E}$. The set of singular points on $\mathcal{X}_o(Mq)_{\mathbf{F}}$ is in bijection with the set $\mathcal{V}$.*

By combining this result with Theorem 5.3 (or Theorem 5.4), we find a 1-1 correspondence between the sets of singular points of $\mathcal{X}_o(Mpq)_{\mathbf{F}_q}$ and of $\mathcal{C}_k$. Similarly, we find a 1-1 correspondence between the set of components of $\mathcal{C}_k$ and the disjoint union of two copies of the set of singular points of $\mathcal{X}_o(Mq)_{\mathbf{F}_q}$. Finally, the map taking each singular point of $\mathcal{C}_k$ to the pair of components which cross at that point may now be related to the two degeneracy maps $\mathcal{X}_o(Mp) \rightrightarrows \mathcal{X}_o(M)$ (Proposition 5.2).

References

[1] Bushnell, C.J. Hereditary orders, Gauss sums, and supercuspidal representations of $\mathbf{GL}_N$. *Journal für die reine und angewandte Mathematik* **375/376**, 184–210 (1987)

[2] Bushnell, C.J. and A. Fröhlich. Non-abelian congruence Gauss sums and p-adic simple algebras. *Proc. London Math. Soc.* (3) **50**, 207–264 (1985)

[3] Carayol, H. Sur la mauvaise réduction des courbes de Shimura. *Compositio Math.* **59**, 151–230 (1986)

[4] Cerednik, I.V. Uniformization of algebraic curves by discrete arithmetic subgroups of $\mathbf{PGL}_2(k_w)$ with compact quotients (in Russian). *Mat. Sb.* **100** , 59–88 (1976). Translation in *Math USSR Sb.* **29**, 55–78 (1976)

[5] Deligne, P. and Rapoport, M. Les schémas de modules de courbes elliptiques. *Lecture Notes in Math* **349**, 143–316 (1973)

[6] Drinfeld, V.G. Coverings of p-adic symmetric regions (in Russian). *Functional. Anal. i Prilozen.* **10**, 29–40 (1976). Translation in *Funct. Anal. Appl.* **10**, 107–115 (1976)

[7] Eichler, M. Über die Idealklassenzahl hyperkomplexer System. *Math. Z.* **43**, 481–494 (1938)

[8] Grothendieck, A. `SGA7 I`, Exposé IX. *Lecture Notes in Math.* **288**, 313–523 (1972)

[9] Ibukiyama, T., Katsura, T., and F. Oort. Supersingular curves of genus two and class numbers. *Compositio Math.* **57**, 127–152 (1986)

[10] Jordan, B. and R. Livné. Local diophantine properties of Shimura curves. *Math. Ann.* **270**, 235–248 (1985)

[11] Jordan, B. and R. Livné. On the Néron model of Jacobians of Shimura curves. *Compositio Math.* **60**, 227–236 (1986)

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

[13] Katz, N. M. and Mazur, B. Arithmetic Moduli of Elliptic Curves. Annals of Math. Studies **108**. Princeton: Princeton University Press, 1985

[14] Kurihara, A. On some examples of equations defining Shimura curves and the Mumford uniformization. *J. Fac. Sci. Univ. Tokyo*, Sec. IA, **25**, 277–300 (1979)

[15] Langlands, R.P. Sur la mauvaise réduction d'une variété de Shimura. *Astérisque* **65**, 125–154 (1979)

[16] Mazur, B. Modular curves and the Eisenstein ideal. *Publ. Math. IHES* **47**, 33–186 (1977)

[17] Mestre, J-F. and J. Oesterlé. Courbes de Weil de conducteur premier et courbes elliptiques supersingulières. In preparation

[18] Morita, Y. Unpublished thesis

[19] Mumford, D. An analytic construction of degenerating curves over complete local rings. *Compositio Math.* **24**, 129–174 (1972)

[20] Oda, T. The first de Rham cohomology group and Dieudonné modules. *Ann. scient. Ec. Norm. Sup.* (4^{e} série) **2**, 63–135 (1969)

[21] Oda, T. and F. Oort. Supersingular abelian varieties. Intl. Symp. on Algebraic Geometry (Kyoto, 1977), pp. 595–621

[22] Ogus, A. Supersingular $K3$ crystals. *Astérisque* **64**, 3–86 (1979)

[23] Oort, F. Which abelian surfaces are products of elliptic curves? *Math. Ann.* **214**, 35–74 (1975)

[24] Rapoport, M. On the local zeta function of Quaternionic Shimura varieties with bad reduction. *Math. Ann.* **279**, 673–697 (1988)

[25] Reiner, I. Maximal Orders. London-New York-San Francisco: Academic Press, 1975

[26] Ribet, K. On modular representations of $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms. MSRI preprint #06420-87 (June, 1987)

[27] Serre, J-P. Arbres, Amalgames, $\mathbf{SL}_2$. *Astérisque* **46** (1977). English translation: Trees. Berlin-Heidelberg-New York: Springer-Verlag 1980

[28] Shimura, G. Introduction to the Arithmetic Theory of Automorphic Functions. Princeton: Princeton University Press, 1971

[29] Shioda, T. Supersingular K3 surfaces. *Lecture Notes in Math* **732**, 564–591 (1979)

[30] Vignéras, M.-F. Arithmétique des Algèbres de Quaternions. *Lecture Notes in Math.* **800** (1980)

[31] Zink, Th. Über die schlechte Reduktion einiger Shimuramannigfaltigkeiten. *Compositio Math.* **45**, 15–107 (1982)

Author's address:

Mathematics Department
UC Berkeley
Berkeley, CA 94720
USA