Proceedings of Symposia in Pure Mathematics
Vol. 33 (1979), part 2, pp. 165–184

POINTS ON SHIMURA VARIETIES mod p

J. S. MILNE

There is associated to a reductive group G over $\boldsymbol{Q}$ with some additional structure a Shimura variety S_C defined over $\boldsymbol{C}$. In most cases it is known that S_C has a canonical model S_E defined over a specific number field E. For almost all finite primes v of E it is possible to reduce S_E modulo the prime and obtain a nonsingular variety S_v over a finite field $\boldsymbol{F}_{q_v}$. As is explained in [3], in order to identify the Hasse-Weil zeta-function of S_E or, more generally, of a locally constant sheaf on S_E it is necessary to have a description of $(S_v(\bar{\boldsymbol{F}}_{q_v}), \text{Frob})$ where $S_v(\bar{\boldsymbol{F}}_{q_v})$ is the set of points of S_v with coordinates in the algebraic closure $\bar{\boldsymbol{F}}_{q_v}$ of $\boldsymbol{F}_{q_v}$ and Frob is the Frobenius map $S_v(\bar{\boldsymbol{F}}_{q_v}) \to S_v(\bar{\boldsymbol{F}}_{q_v})$ which takes a point with coordinates $(a_1, \cdots, a_m)$ to $(a_1^{q_v}, \cdots, a_m^{q_v})$. To be useful, the description should be directly in terms of the group G.

Recently [13] Langlands has conjectured such a description of $(S_v(\bar{\boldsymbol{F}}_{q_v}), \text{Frob})$ for any Shimura variety S and any sufficiently good prime v. In [12] he has given a fairly detailed outline of a proof of the conjecture for those Shimura varieties which can be realized as coarse moduli schemes for problems involving only abelian varieties, (weak) polarizations, endomorphisms, and points of finite order. (So $G(\boldsymbol{Q})$ is of the form $\text{Aut}_B(H_1(A, \boldsymbol{Q}), \psi)$ where B is a semisimple $\boldsymbol{Q}$-algebra containing an order which acts on the abelian variety A, ψ is a Riemann form for A whose Rosati involution on $\text{End}(A) \otimes \boldsymbol{Q}$ stabilizes B, and Aut_B refers to B-linear automorphisms g of $H_1(A, \boldsymbol{Q})$ such that $\psi(gu, gv) = \psi(u, \mu(g)v)$ with $\mu(g)$ lying in some fixed algebra F contained in the centre of B and fixed by the Rosati involution; there is also a Hasse principle assumption.)

Earlier [8, Conjecture 1] Ihara had made a similar conjecture when S is a Shimura curve and had proved it when $G = \text{GL}_2$ [9, Chapter 5]. When $G = B^\times$, B a quaternion division algebra over $\boldsymbol{Q}$, Morita [15] proved Ihara's conjecture for all primes p of E ($= \boldsymbol{Q}$) not dividing the discriminant of B. Both he and Shimura have obtained partial results for more general quaternion algebras (unpublished). More recently Ihara has proved his conjecture for all Shimura curves and sufficiently good primes (announcement in [11]). While Ihara bases his proof on the Eichler-Shimura congruence relations, Morita's method, as described in [10], appears to be quite similar to that of Langlands.

In order to give some idea of the techniques Langlands uses in his proof I shall describe it in the case that G is the multiplicative group of a totally indefinite qua-

AMS (MOS) subject classifications (1970). Primary 14K10; Secondary 14G10, 14L05.

ternion algebra over a totally real number field. In §1 it is shown that S_C parametrizes, in a natural way, a family of abelian varieties with additional structure. The following section describes how Artin's representability criteria may be used to prove the existence of a variety $S_{\mathbf{Q}}$ over $\mathbf{Q}$ which is a canonical model for S_C and which, when reduced mod p, parametrizes a family of abelian varieties (with additional structure) in characteristic p. Thus the problem of describing $(S_p(\bar{F}_p)$, Frob) becomes one of describing this family. In §5 the Tate-Honda classification of isogeny classes of abelian varieties over finite fields is used to determine the isogeny classes in the family, and in §6 the individual isogeny classes are described. Since this requires the use of p-divisible groups and their Dieudonné modules, these are reviewed in §3.

Notation. F is a totally real number field of degree d over $\mathbf{Q}$, B is a quaternion division algebra over F which is split everywhere at infinity, $b \mapsto b^*$ is a positive F-involution on B, and O_B is a maximal order in B.

G is the group scheme over $\mathbf{Z}$ such that $G(R) = (O_B^{opp} \otimes R)^\times$ for all rings R, where O_B^{opp} is the opposite algebra to O_B.

$\mathbf{A}$ is the ring of adèles for $\mathbf{Q}$; $\mathbf{A} = \mathbf{R} \times \mathbf{A}_f = \mathbf{R} \times \mathbf{A}_f^p \times \mathbf{Q}_p^\times$; $\mathbf{A}_f = \mathbf{Z}_f \otimes \mathbf{Q}$, $\mathbf{Z}_f = \text{proj lim } \mathbf{Z}/m\mathbf{Z}$; $\mathbf{Z}_f = \mathbf{Z}_f^p \times \mathbf{Z}_p$.

K is a (sufficiently small) open subgroup of $G(\mathbf{Z}_f)$. Δ is a product of rational prime numbers such that if $p \nmid \Delta$ then p is unramified in F, B is split at all primes of F dividing p, and $K = K^p G(\mathbf{Z}_p)$ where $K^p = K \cap G(\mathbf{A}_f^p)$.

$S_C = {}_K S_C$ is the Shimura variety over $\mathbf{C}$ defined by G, K, and the map $h: \mathbf{C}^\times \to G(\mathbf{R})$ defined in §1; thus its points in $\mathbf{C}$ are $S_C(\mathbf{C}) = G(\mathbf{Q})\backslash G(\mathbf{A})/K_\infty K$ where K_∞ is the centralizer of h in $G(\mathbf{R})$.

If $V = V(\mathbf{Z})$ is a $\mathbf{Z}$-module then $V(R) = V \otimes_{\mathbf{Z}} R$ for any ring R.

1. S_C as a moduli scheme. Recall that an *abelian variety* over a field k is an algebraic group over k whose underlying variety is complete (and connected); its group structure is then commutative and the variety is projective. For example, an abelian variety of dimension one is an elliptic curve, and may be described by its equation, which is of the form

$$Y^2Z = X^3 + aXZ^2 + bZ^3, \qquad a, b \in k,\ 4a^3 + 27b^2 \neq 0.$$

It is impractical to describe abelian varieties of dimension greater than one by equations, but fortunately over $\mathbf{C}$ there is a classical description in terms of lattices in complex vector spaces. Let V be a lattice in $\mathbf{C}^g$, i.e., V is the subgroup generated by an $\mathbf{R}$-basis and so $V \otimes_{\mathbf{Z}} \mathbf{R} \approx \mathbf{C}^g$. Then $\mathbf{C}^g/V$ is a compact complex-analytic manifold which becomes a commutative Lie group under addition. When $g = 1$ the Weierstrass $\wp$-function corresponding to V, and its derivative, define an embedding

$$z \mapsto (\wp(z),\ \wp'(z),\ 1): \mathbf{C}/V \hookrightarrow \mathbf{P}_{\mathbf{C}}^2$$

of $\mathbf{C}/V$ as an algebraic subset of the projective plane. Thus $\mathbf{C}/V$ automatically has the structure of an algebraic variety and so is an abelian variety. This is no longer true if $g > 1$ for there may be too few functions on $\mathbf{C}^g/V$ to define an embedding of it into projective space. Since any meromorphic function on $\mathbf{C}^g/V$ is a quotient

of theta functions on $\boldsymbol{C}^g$, $\boldsymbol{C}^g/V$ will be algebraic if and only if there exist enough theta functions. By definition, a theta function for V is a holomorphic function θ on $\boldsymbol{C}^g$ such that, for $v \in V$, $\theta(z + v) = \theta(z) \exp(2\pi i(L(z, v) + J(v)))$ where $L(z, v)$ is a $\boldsymbol{C}$-linear function of z and $J(v)$ depends only on v. One shows that $L(z, v)$ is additive in v, and so extends to a function L: $\boldsymbol{C}^g \times \boldsymbol{C}^g \to \boldsymbol{C}$ which is $\boldsymbol{C}$-linear in the first variable and $\boldsymbol{R}$-linear in the second. Set $E(z, w) = L(z, w) - L(w, z)$.

Then

(a) E is $\boldsymbol{R}$-valued, $\boldsymbol{R}$-bilinear, and alternating;

(b) E takes integer values on $V \times V$;

(c) the form $(z, w) \mapsto E(iz, w)$ is symmetric and positive.

(The symmetry is equivalent to having $E(iz, iw) = E(z, w)$ for all z, w; the positivity means $E(iz, z) \geqq 0$ for all z.)

A form satisfying these conditions is called a *Riemann form* for V and it is known that there exist enough functions to define a projective embedding of $\boldsymbol{C}^g/V$ if and only if there exists a Riemann form for V which is nondegenerate (and hence such that $E(iz, z)$ is positive definite). If $g = 1$ we may always define $E(z, w)$ to be the ratio of the oriented area of the parallelogram with sides Ow, Oz to that of a fundamental parallelogram for the lattice. Since this form always exists, and is unique up to multiplication by an integer, one rarely bothers to mention it. By contrast, if $g > 1$, a nondegenerate Riemann form will not usually exist and when it does, it will not be unique up to multiplication by an integer. However since $\boldsymbol{C}^g/V$ is compact the algebraic structure on $\boldsymbol{C}^g/V$ (but not the projective embedding) defined by a Riemann form is independent of the form.

Thus, given a lattice in $\boldsymbol{C}^g$ for which there exists a nondegenerate Riemann form, we obtain an abelian variety. Conversely, from an abelian variety A of dimension g we can recover a complex vector space W of dimension g and a lattice V in W for which there exists a nondegenerate Riemann form. W can be described (according to taste) as the Lie algebra $\mathrm{Lie}(A)$ of A, the tangent space $\boldsymbol{t}_A$ to A at its zero element, or as the universal covering space of the topological manifold $A(\boldsymbol{C})$. The lattice V can be described as the kernel of the exponential $\exp$: $\mathrm{Lie}(A) \to A(\boldsymbol{C})$, or as the fundamental group of $A(\boldsymbol{C})$ which, being commutative, is equal to $H_1(A, \boldsymbol{Z})$. We shall always regard the isomorphism $W/V \xrightarrow{\approx} A(\boldsymbol{C})$ as arising from the exact sequence,

$$0 \to H_1(A, \boldsymbol{Z}) \to \boldsymbol{t}_A \xrightarrow{\exp} A(\boldsymbol{C}) \to 0.$$

Since $H_1(A, \boldsymbol{Z})$ is a lattice in $\boldsymbol{t}_A$; we have $H_1(A, \boldsymbol{R}) = H_1(A, \boldsymbol{Z}) \otimes \boldsymbol{R} \xrightarrow{\approx} \boldsymbol{t}_A$. Thus A is determined by $H_1(A, \boldsymbol{Z})$ and the complex vector space structure on $H_1(A, \boldsymbol{R})$.

A complex structure on a real vector space $V(\boldsymbol{R})$ defines a homomorphism h: $\boldsymbol{C}^\times \to \mathrm{Aut}_{\boldsymbol{R}}(V(\boldsymbol{R}))$, $h(z) = (v \mapsto zv)$, and the complex structure is determined by h. Thus an abelian variety A is uniquely determined by the pair $(H_1(A, \boldsymbol{Z}), h)$ where h: $\boldsymbol{C}^\times \to \mathrm{Aut}(H_1(A, \boldsymbol{R}))$ is defined by the complex structure on $H_1(A, \boldsymbol{R}) = \boldsymbol{t}_A$. Moreover every pair $(V(\boldsymbol{Z}), h)$ for which there exists a Riemann form arises from an abelian variety.

Let $V(\boldsymbol{Z}) = H_1(A, \boldsymbol{Z})$. A point of finite order on A corresponds to an element of $V(\boldsymbol{R})$ some multiple of which is in $V(\boldsymbol{Z})$. More precisely, the group of points of

finite order on A may be identified with $V(\boldsymbol{Q})/V(\boldsymbol{Z}) \subset V(\boldsymbol{R})/V(\boldsymbol{Z})$. For any integer $m > 0$, the group $A_m(\boldsymbol{C})$ of points of order m is equal to $m^{-1}V(\boldsymbol{Z})/V(\boldsymbol{Z}) \xrightarrow{\approx} V(\boldsymbol{Z}/m\boldsymbol{Z}) \approx (\boldsymbol{Z}/m\boldsymbol{Z})^{2\dim(A)}$. We define T_fA to be proj $\lim_m A_m(\boldsymbol{C}) = V(\boldsymbol{Z}_f)$ and, for any prime l, T_lA to be proj $\lim_m A_{l^m}(\boldsymbol{C}) = V(\boldsymbol{Z}_l)$; thus $T_fA = \prod_l T_lA$ and $T_lA \approx \boldsymbol{Z}_l^{2\dim(A)}$.

A homomorphism $A \to A'$ of abelian varieties induces a $\boldsymbol{C}$-linear map $\boldsymbol{t}_A \to \boldsymbol{t}_{A'}$ such that $H_1(A, \boldsymbol{Z})$ is mapped into $H_1(A', \boldsymbol{Z})$. Conversely, if A and A' correspond respectively to (V, h) and (V', h') then a map of $\boldsymbol{Z}$-modules $\alpha: V(\boldsymbol{Z}) \to V'(\boldsymbol{Z})$ extending to a $\boldsymbol{C}$-linear map $\alpha \otimes 1$: $V(\boldsymbol{R}) \to V'(\boldsymbol{R})$ (i.e., such that $\alpha \otimes 1 \circ h(z) = h'(z) \circ \alpha \otimes 1$ for all z) arises from a map of complex manifolds $A(\boldsymbol{C}) \to A'(\boldsymbol{C})$ and the compactness of $A(\boldsymbol{C})$ and $A'(\boldsymbol{C})$ implies that the map is algebraic. We write $\mathrm{End}(A)$ for the ring of endomorphisms of A and $\mathrm{End}^\circ(A)$ for $\mathrm{End}(A) \otimes_{\boldsymbol{Z}} \boldsymbol{Q}$. Since $\mathrm{End}^\circ(A)$ has a faithful representation on $H_1(A, \boldsymbol{Q})$, it is a finite-dimensional $\boldsymbol{Q}$-algebra; it is also semisimple, and its possible dimensions and structures are well understood.

To define a homomorphism i: $O_B \to \mathrm{End}(A)$ when A corresponds to (V, h) is the same as to define an action of O_B on V such that h maps $\boldsymbol{C}^\times$ into $\mathrm{Aut}_{O_B \otimes \boldsymbol{R}}(V(\boldsymbol{R}))$. When such an i is given we say that O_B *acts* on A provided $i(1) = 1$. Such an i induces an injection i: $B \hookrightarrow \mathrm{End}^\circ(A)$.

A nondegenerate Riemann form E for A defines an involution $\alpha \mapsto \alpha'$ of $\mathrm{End}^\circ(A)$ by the rule $E(\alpha z, w) = E(z, \alpha' w)$; this is the *Rosati involution*, which is known to be positive, i.e., $\mathrm{Tr}(\alpha\alpha') > 0$ for all $\alpha \neq 0$ where Tr denotes the reduced trace from $\mathrm{End}^\circ(A)$ to $\boldsymbol{Q}$. Suppose O_B acts on A. We say that two Riemann forms E and E' on A are *F-equivalent* if there exist nonzero c, $c' \in O_F$ such that $E(u, cv) = E(u, c'v)$ for all u, $v \in V(\boldsymbol{Z})$, and we define a *weak polarization* of A to be an F-equivalence class Λ of nondegenerate Riemann forms. Since F is the centre of B, the Rosati involutions defined by any two elements of such a Λ induce the same map on $i(B)$. We shall be interested in triples (A, i, Λ) such that $E(i(b)u, v) = E(u, i(b^*)v)$ for u, $v \in V(\boldsymbol{R})$, $b \in B$, $E \in \Lambda$, i.e., we require that the Rosati involutions defined by Λ stabilize $i(B)$ and induce the given involution $b \mapsto b^*$ on B.

We next review some notations concerning B. The *main involution* $b \mapsto b^\iota$ of B is so defined that under any $\boldsymbol{R}$-isomorphism $B \otimes_F \boldsymbol{R} \xrightarrow{\approx} M_2(\boldsymbol{R})$, if b corresponds to $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ then b^ι corresponds to $M^\iota = \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$; thus $b + b^\iota = \mathrm{Tr}_{B/F}(b)$ and $bb^\iota = Nm_{B/F}(b)$. The Skolem-Noether theorem shows that there exists a $t \in B$ such that $b^* = t^{-1}b^\iota t = tb^\iota t^{-1}$ for all $b \in B$; automatically $t^2 \in F$ and the positivity of $b \mapsto b^*$ implies that $t^2 < 0$, i.e., t^2 has negative image under all embeddings $F \hookrightarrow \boldsymbol{R}$. We fix an isomorphism $B \otimes_{\boldsymbol{Q}} \boldsymbol{R} \xrightarrow{\approx} M_2(\boldsymbol{R}) \times \cdots \times M_2(\boldsymbol{R})$ such that if $b \leftrightarrow (M_1, \cdots, M_n)$ then $b^* \leftrightarrow (M_1^{\mathrm{tr}}, \cdots, M_n^{\mathrm{tr}})$ where M_i^{tr} is the transpose of M_i. Since

$$M^{\mathrm{tr}} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1} M^\iota \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

t maps to an element $(c_1\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right), \cdots, c_n\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right))$ with each $c_i \in \boldsymbol{R}$, and t may be chosen so that $c_i > 0$.

The next lemma implies that if O_B acts on a complex manifold $\boldsymbol{C}^{2d}/V$ then there is a Riemann form E for V whose corresponding Rosati involution induces $b \mapsto b^*$ on B and any two such forms are F-equivalent, i.e., that there is a unique weak

polarization which is compatible with the O_B-action and the given involution.

LEMMA 1.1. *Let $V = V(\boldsymbol{Z})$ be a free $\boldsymbol{Z}$-module of rank $4d$ on which O_B acts. There is a nondegenerate alternating form ψ on $V(\boldsymbol{Q})$ such that:*

(a) *$\psi(u, v) \in \boldsymbol{Z}$ if $u, v \in V(\boldsymbol{Z})$;*

(b) *$\psi(ut, u) < 0$ for all $u \neq 0$, $u \in V(\boldsymbol{R})$;*

(c) *$\psi(bu, v) = \psi(u, b^*v)$ for all $b \in B$ and $u, v \in V(\boldsymbol{Q})$;*

(d) *for any B-automorphism α of $V(\boldsymbol{Q})$ there exists a $\mu(\alpha) \in F^\times$ such that $\psi(\alpha u, \alpha v) = \psi(u, \mu(\alpha)v)$ for all $u, v \in V(\boldsymbol{Q})$. Moreover' if ψ' is a second nondegenerate alternating form on $V(\boldsymbol{Q})$ satisfying* (c) *then there exists a $c \in F^\times$ such that $\psi(u, cv) = \psi'(u, v)$ for all $u, v \in V$.*

PROOF. $V(\boldsymbol{Q})$ has dimension one over B and so, after choosing an appropriate basis vector, we may identify $V(\boldsymbol{Q})$ with B and $V(\boldsymbol{Z})$ with a left ideal in O_B.

Define $\psi(u, v) = \mathrm{Tr}_{B/\boldsymbol{Q}}(uv^ct) = \mathrm{Tr}_{B/\boldsymbol{Q}}(utv^*)$. Then $\psi(u, v) = \mathrm{Tr}(utv^*) = \mathrm{Tr}(vt^*u^*) = \mathrm{Tr}(v(-t)u^*) = -\psi(v, u)$, and so ψ is alternating. (a) is obvious, and $\psi(ut, u) = \mathrm{Tr}_{B/\boldsymbol{Q}}(ut^2u^*) = \mathrm{Tr}_{F/\boldsymbol{Q}}(t^2\mathrm{Tr}_{B/F}(uu^*)) < 0$ for $u \neq 0$, which proves (b) and that ψ is nondegenerate. For (c) we note that $\psi(bu, v) = \mathrm{Tr}(utv^*b) = \mathrm{Tr}(ut(b^*v)^*) = \psi(u, b^*v)$. Finally, any B-automorphism α of $V(\boldsymbol{Q}) = B$ is multiplication on the right by an element $b \in B^\times$. Thus $\psi(\alpha u, \alpha v) = \mathrm{Tr}(ubb^cv^ct) = \psi(u, \mu(\alpha)v)$ with $\mu(\alpha) = Nm_{B/F}(b)$.

For the last part, consider the $\boldsymbol{Q}$-linear map $v \mapsto \psi'(1, v)\colon B \to \boldsymbol{Q}$. Since $\mathrm{Tr}_{B/\boldsymbol{Q}}\colon B \times B \to \boldsymbol{Q}$ is nondegenerate, there is a unique $b \in B$ such that $\psi'(1, v) = \mathrm{Tr}(btv^*)$ for all $v \in B$. Then $\psi'(u, v) = \psi'(1, u^*v) = \mathrm{Tr}(btv^*u) = \mathrm{Tr}(ubtv^*) = \mathrm{Tr}(ubv^ct)$. We also have $\psi'(1, v) = -\psi'(v, 1) = -\mathrm{Tr}(vbt) = -\mathrm{Tr}(t^cb^cv^c) = \mathrm{Tr}(b^cv^ct) = \mathrm{Tr}(b^ctv^*)$. Thus $b = b^c$, which implies that it is in F, and we may take $c = b$.

For the remainder of this section $V(\boldsymbol{Z})$ will be O_B regarded as an O_B-module and ψ will be as in the lemma. For any ring R we may identify $G(R)$ with $\mathrm{Aut}_{O_B\otimes R}(V(R))$ since any $O_B \otimes R$-endomorphism of $V(R) = O_B \otimes R$ is right multiplication by an element of $O_B \otimes R$. Define h to be the homomorphism $\boldsymbol{C}^\times \to G(\boldsymbol{R}) = \mathrm{Aut}_{B\otimes\boldsymbol{R}}(V(\boldsymbol{R}))$ such that $h(i)$ is right multiplication on $V(\boldsymbol{R}) = B \otimes \boldsymbol{R} \xrightarrow{\approx} M_2(\boldsymbol{R}) \times \ldots \times M_2(\boldsymbol{R})$ by $(\left(\begin{smallmatrix}0 & 1\\ -1 & 0\end{smallmatrix}\right), \cdots, \left(\begin{smallmatrix}0 & 1\\ -1 & 0\end{smallmatrix}\right))$. Thus $K_\infty = \{(M_1, \cdots, M_d)\}$ with M_i of the form $\left(\begin{smallmatrix}a & b\\ -b & a\end{smallmatrix}\right)$, $a, b \in \boldsymbol{R}$. The form $E = \psi$ is a Riemann form for $(V(\boldsymbol{Z}), h)$, e.g., $\psi(iu, iv) = \psi(uh(i), vh(i)) = \psi(u, Nm_{B/F}(h(i))v) = \psi(u, v)$ and $\psi(iu, u) = \psi(ut/-(-t^2)^{1/2}, u) > 0$ for $u \neq 0$. Thus $(V(\boldsymbol{Z}), h)$ defines an abelian variety A. The action of O_B on $V(\boldsymbol{Z})$ induces a map $i\colon O_B \to \mathrm{End}(A)$ and the Rosati involution defined by the weak polarization Λ containing ψ induces $b \mapsto b^*$ on B.

Recall that K is an open subgroup of $G(\boldsymbol{Z}_f)$. Two isomorphisms $\phi_1, \phi_2\colon T_fA \xrightarrow{\approx} V(\boldsymbol{Z}_f)$ are *K-equivalent* if there is a $k \in K$ such that $\phi_1 = k\phi_2$. For example, if $K = K_m = \mathrm{Ker}(G(\boldsymbol{Z}_f) \to G(\boldsymbol{Z}/m\boldsymbol{Z}))$ then to give a K-equivalence class of isomorphisms $T_fA \to V(\boldsymbol{Z}_f)$ is the same as to give an isomorphism $A_m(\boldsymbol{C}) \xrightarrow{\approx} V(\boldsymbol{Z}/m\boldsymbol{Z})$, i.e., a level m structure.

THEOREM 1.2. *There is a one-one correspondence between the set of points $S_{\boldsymbol{C}}(\boldsymbol{C}) = G(\boldsymbol{Q})\backslash G(\boldsymbol{A})/K_\infty K$ and the set of isomorphism classes of triples $(A, i, \bar{\phi})$ where A is an abelian variety of dimension $2d$, i defines an action of O_B on A, and $\bar{\phi}$ is a K-equivalence class of O_B-isomorphisms $T_fA \xrightarrow{\approx} V(\boldsymbol{Z}_f)$.*

REMARK 1.3. (a) We say that two triples $(A, i, \bar{\phi})$ and $(A', i', \bar{\phi}')$ are isomorphic if there exists an isomorphism $\alpha: A \to A'$ such that $\alpha \circ i(b) = i'(b) \circ \alpha$ for all $b \in O_B$ and $\phi' \circ (T_f\alpha) \in \bar{\phi}$ for all $\phi' \in \bar{\phi}'$.

(b) Normally when considering families of abelian varieties parametrized by Shimura varieties it is necessary to work with quadruples $(A, i, \Lambda, \bar{\phi})$ with Λ a (weak) polarization. This is not necessary in our case because, as we observed above, Λ always exists uniquely.

PROOF OF 1.2. We first show how to associate to any $g \in G(\boldsymbol{A})$ a triple $(A_g, i_g, \bar{\phi}_g)$. If $g = 1$ we take $(A, i, \bar{\phi})$ with (A, i) as defined before and $\bar{\phi}$ the class of the identity map $T_fA = V(\boldsymbol{Z}_f) \xrightarrow{\text{id}} V(\boldsymbol{Z}_f)$. We write a general g as $g = g_\infty g_f$, $g_\infty \in G(\boldsymbol{R})$, $g_f \in G(\boldsymbol{A}_f)$, and use g_∞ and g_f to modify respectively the complex structure on $V(\boldsymbol{R})$ and the lattice. Define $h_g: \boldsymbol{C}^\times \to G(\boldsymbol{R})$ by the formula $h_g(z) = g_\infty h(z) g_\infty^{-1}$ and define $gV(\boldsymbol{Z})$ to be the lattice $g_fV(\boldsymbol{Z}_f) \cap V(\boldsymbol{Q})$, the intersection taking place inside $V(\boldsymbol{A}_f)$. Then A_g is to be the abelian variety defined by the pair (gV, h_g). Since O_B still acts on $gV(\boldsymbol{Z})$ we have an obvious map $i_g: O_B \hookrightarrow \text{End}(A)$. We define $\phi_g: T_fA_g = g_fV(\boldsymbol{Z}_f) \xrightarrow{\approx} V(\boldsymbol{Z}_f)$ to be multiplication by g_f^{-1}.

If g is replaced by gk_∞ with $k_\infty \in K_\infty$ then h_g is unchanged since K_∞ is the centralizer of h in $G(\boldsymbol{R})$. If g is replaced by gk_f with $k_f \in K$ then h_g and $gV(\boldsymbol{Z})$ are unchanged while ϕ_g is replaced by $k_f^{-1}\phi_g$, which is K-equivalent to ϕ_g. If g is replaced by qg with $q \in G(\boldsymbol{Q})$ then $q^{-1}: V(\boldsymbol{R}) \to V(\boldsymbol{R})$ defines an isomorphism $(A_{qg}, \cdots) \xrightarrow{\approx} (A_g, \cdots)$. Thus $(A_g, \cdots)$ depends only on the double coset of g.

Conversely, an isomorphism $\alpha: (A_g, \cdots) \to (A_{g'}, \cdots)$ is induced by an isomorphism $V(\boldsymbol{R}) \to V(\boldsymbol{R})$ which sends $gV(\boldsymbol{Z})$ isomorphically onto $g'V(\boldsymbol{Z})$. In particular α defines a B-isomorphism $q: V(\boldsymbol{Q}) \to V(\boldsymbol{Q})$. Thus $q \in G(\boldsymbol{Q})$ and so, after replacing g' by $q^{-1}g'$ and α by $q^{-1}\alpha$, we may assume that the map $V(\boldsymbol{Q}) \to V(\boldsymbol{Q})$ corresponding to α is the identity. Thus $g_\infty h(z) g_\infty^{-1} = g'_\infty h(z) g_\infty'^{-1}$ for all z, and so $g_\infty^{-1} g'_\infty \in K_\infty$. Moreover, $gV(\boldsymbol{Z}) = g'V(\boldsymbol{Z})$ implies $g_f^{-1} g'_f \in G(\boldsymbol{Z}_f)$, and $g_f^{-1}: gV(\boldsymbol{Z}_f) \to V(\boldsymbol{Z}_f)$ being K-equivalent to $g_f'^{-1}: g'V(\boldsymbol{Z}_f) \to V(\boldsymbol{Z}_f)$ implies that $g_f^{-1} g'_f \in K$.

Finally we have to show that every $(A, i, \bar{\phi})$ arises from some g. Since B is a division algebra there is a B-isomorphism $H_1(A, \boldsymbol{Q}) \xrightarrow{\approx} V(\boldsymbol{Q})$ which we may use to identify $H_1(A, \boldsymbol{Q})$ with $V(\boldsymbol{Q})$. Then $H_1(A, \boldsymbol{Z})$ is a lattice in $V(\boldsymbol{Q})$ and so is of the form $g_fV(\boldsymbol{Z})$ for some $g_f \in G(\boldsymbol{A}_f)$. The isomorphism $V(\boldsymbol{R}) \approx \boldsymbol{t}_A$ induces a complex structure on $V(\boldsymbol{R})$, and we let $h': \boldsymbol{C}^\times \to \text{Aut}_{\boldsymbol{R}}(V(\boldsymbol{R}))$ be the corresponding map. Since B acts $\boldsymbol{C}$-linearly on $\boldsymbol{t}_A$, h maps into $\text{Aut}_{B\otimes\boldsymbol{R}}(V(\boldsymbol{R})) = G(\boldsymbol{R})$. Obviously there exists a $g_\infty \in G(\boldsymbol{R})$ such that $h'(z) = g_\infty h(z) g_\infty^{-1}$. Any $\phi \in \bar{\phi}$ is of the form $v \mapsto g_1^{-1}g_f^{-1}\, v: g_fV(\boldsymbol{Z}_f) \to V(\boldsymbol{Z}_f)$ for some $g_1 \in G(\boldsymbol{Z}_f)$. It is now clear that $(A, \cdots) \approx (A_g, \cdots)$ with $g = g_\infty g_f g_1$.

REMARK 1.4. (a) A map $\alpha: A \to A'$ of abelian varieties is an isogeny if it is surjective and has finite kernel; when O_B acts on A and A', α is called an O_B-isogeny if it commutes with the two actions. Clearly any isogeny (over $\boldsymbol{C}$) induces an isomorphism on the tangent spaces and so A_g is isogenous to $A_{g'}$ only if g_∞ and g'_∞ define the same double coset in $G(\boldsymbol{Q})\backslash G(\boldsymbol{R})/K_\infty$. On the other hand, the set $\text{End}_B^\circ(A)^\times \backslash G(\boldsymbol{A}_f)/K$ classifies the triples $(A, i, \bar{\phi})$ for which there is an O_B-isogeny $A \to A_1$. For example, if $g = g_f$ then, after replacing g_f by an integral multiple, we may assume that $gV(\boldsymbol{Z}) \subset V(\boldsymbol{Z})$. The identity map $V(\boldsymbol{R}) \to V(\boldsymbol{R})$ now defines an isogeny $A_g \to A_1$ with kernel $V(\boldsymbol{Z})/gV(\boldsymbol{Z})$ (cf. §6 below).

(b) In the case that $F = \boldsymbol{Q}$, the theorem may be strengthened. Consider the

projection $V(\boldsymbol{R}) \times (G(\boldsymbol{A})/K_\infty K) \to G(\boldsymbol{A})/K_\infty K$. We give $G(\boldsymbol{A})/K_\infty K$ its usual complex structure and the copy of $V(\boldsymbol{R})$ over $gK_\infty K$ the complex structure defined by h_g. Inside each V_g we have a lattice $gV(\boldsymbol{Z})$, and these vary continuously with g. Thus we may divide out and obtain a map of complex manifolds $\mathscr{T} \to G(\boldsymbol{A})/K_\infty K$ such that the fibre over $gK_\infty K$ is the abelian variety A_g. We may now let $G(\boldsymbol{Q})$ act on both manifolds and divide out again to obtain an analytic family $\mathscr{A} \to S_{\boldsymbol{C}}$ of abelian varieties. Each fibre A_g has the structure defined by $(i_g, \bar{\phi}_g)$, and these vary continuously. In fact $\mathscr{A} \to S_{\boldsymbol{C}}$ is an algebraic family, i.e., $\mathscr{A}$ is an algebraic variety and the map is algebraic.

If $F \neq \boldsymbol{Q}$ the above construction fails because units of F may act on (A_g, i_g, ϕ_g) and so the action of $G(\boldsymbol{Q})$ on $\mathscr{T}$ is not free. However we may "rigidify" the situation as follows: consider quadruples $(A, i, \bar{\phi}, \varepsilon)$ where A, i, and $\bar{\phi}$ are as before and ε is an injection from the unique weak polarization Λ to $F^\times$ such that $\varepsilon(\psi') = c\varepsilon(\psi)$ if $\psi'(u, v) = \psi(u, cv)$. The isomorphism classes of quadruples are classified by $F^\times \times S_{\boldsymbol{C}}(\boldsymbol{C})$ which is a disjoint union of copies of $S_{\boldsymbol{C}}(\boldsymbol{C})$, one for each element of $F^\times$, on which $F^\times$ acts by permuting the copies. $F^\times \times S_{\boldsymbol{C}}$ may be regarded as a scheme over $\boldsymbol{C}$ which is an infinite disjoint union of varieties and the previous process gives an algebraic family of $\mathscr{A} \to F^\times \times S_{\boldsymbol{C}}$ of abelian varieties with structure.

References. The most elegant elementary and nonelementary treatments of abelian varieties over $\boldsymbol{C}$ are to be found respectively in [**20**] and [**17**, Chapter I]. Families of abelian varieties parametrized by Shimura varieties were extensively studied by Shimura in the 1960's (see his Annals papers of that period). They are also discussed briefly in [**4**].

2. S as a scheme over $\boldsymbol{Z}[\Delta^{-1}]$. We shall see shortly that $S_{\boldsymbol{C}}$ has a model $S_{\boldsymbol{Q}}$ over $\boldsymbol{Q}$, i.e., that there is a scheme $S_{\boldsymbol{Q}}$ over $\boldsymbol{Q}$ whose defining equations, when considered over $\boldsymbol{C}$, give $S_{\boldsymbol{C}}$. There is no reason to believe that $S_{\boldsymbol{Q}}$ will be unique but Shimura has given conditions which will be satisfied by at most one model; such a model (when it exists) is said to be *canonical.* For example, let F' be a quadratic totally imaginary extension of F which splits B and let A_0 be the abelian variety of dimension d defined by the lattice $O_{F'} \subset F' \otimes \boldsymbol{R}$. Then $O_{F'}$ acts on A_0 and A_0 is said to have complex multiplication by F'. Let $A = A_0 \times A_0$. If we embed F' in B and choose a basis $\{e_1, e_2\}$ for B over F' with $e_1, e_2 \in O_B$, then we get a map $B \hookrightarrow M_2(F') \subset M_2(\mathrm{End}^\circ(A_0)) = \mathrm{End}^\circ(A)$ sending O_B into $\mathrm{End}(A)$. Also we get a map $T_f A = (O_{F'} \oplus O_{F'}) \otimes \boldsymbol{Z}_f \xrightarrow{\phi} O_B \otimes \boldsymbol{Z}_f = V(\boldsymbol{Z}_f)$ (in the notation of §1). The triple $(A, i, \bar{\phi})$ defines a point of $S_{\boldsymbol{C}}$, and hence a point of $S_{\boldsymbol{Q}}$ with complex coordinates. For $S_{\boldsymbol{Q}}$ to be canonical these coördinates must be algebraic over $\boldsymbol{Q}$ and generate a certain explicitly described class field.

For the reasons explained in the introduction we would like to have a scheme S defined by equations in $\boldsymbol{Z}[\Delta^{-1}]$ which, when regarded over $\boldsymbol{Q}$, is the canonical model $S_{\boldsymbol{Q}}$ of $S_{\boldsymbol{C}}$, and which is such that it is possible to describe explicitly $(S(\bar{\boldsymbol{F}}_p), \mathrm{Frob})$ for any $p \nmid \Delta$. Such an S will define a functor $R \mapsto S(R)$ which associates to any ring R in which Δ is invertible the set of points of S with coordinates in R. (More generally, it associates to any scheme T over spec $\boldsymbol{Z}[\Delta^{-1}]$ the set $S(T)$ of maps $T \to S$.) Since the functor determines the scheme uniquely this suggests that in constructing S we should write down a functor $\mathscr{S}$ such that, in particular, $\mathscr{S}(\boldsymbol{C}) = S_{\boldsymbol{C}}(\boldsymbol{C}) = G(\boldsymbol{Q})\backslash G(\boldsymbol{A})/K_\infty K$ and try to prove that it is the points functor of a

scheme. After §1 it is natural to define $\mathscr{S}(R)$ to consist of isomorphism classes of triples $(A, i, \bar{\phi})$ where each of the three objects is the analogue over R of the corresponding object over C. Thus A is a projective abelian scheme of dimension $2d$ over R. Intuitively, A can be thought of as an algebraic family of abelian varieties, each of which is defined over a residue field of R. More precisely it is a projective smooth group scheme over spec R with geometrically connected fibres. As before i is to be a homomorphism $O_B \hookrightarrow \mathrm{End}(A)$ such that $i(1)$ is the identity map. We assume that A has a polarization whose Rosati involution induces $b \mapsto b^*$ on B. Two problems arise in defining $\bar{\phi}$ which may be best understood if we write $\phi: T_f A \to V(\boldsymbol{Z}_f)$ as a product $\prod \phi_l: \prod T_l A \to \prod V(\boldsymbol{Z}_l)$ of maps. Firstly, if p is not invertible in R there will never exist an isomorphism $\phi_p: T_p A \xrightarrow{\simeq} V(\boldsymbol{Z}_p)$; thus we take ϕ_p to be a map defined only over $R[p^{-1}]$. Secondly, unless R is an algebraically closed field it is unrealistic to expect there to be an isomorphism $\phi_l: T_l A \to V(\boldsymbol{Z}_l)$ for any l, for this would imply that all coordinates of all l-power torsion points of A are in R. Instead we assume that $K \supset K_m = \mathrm{Ker}(G(\boldsymbol{Z}_f) \to G(\boldsymbol{Z}/m\boldsymbol{Z}))$ some m, and consider isomorphisms $\phi: A_m \xrightarrow{\simeq} V(\boldsymbol{Z}/m\boldsymbol{Z})$ defined on some étale covering of R, two such isomorphisms ϕ_1 and ϕ_2 being K-equivalent if $\phi_1 = k\phi_2$, $k \in K$, locally on spec(R), and we take $\bar{\phi}$ to be a K-equivalence class in this new sense. It is necessary to put one extra condition on the triple $(A, i, \bar{\phi})$: if the R-algebra R' is such that $O_B \otimes R' \approx M_2(O_F \otimes R')$ then the two submodules of $\boldsymbol{t}_{A/R}$ corresponding to the idempotents $\left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}0&0\\0&1\end{smallmatrix}\right)$ should be free $O_F \otimes R'$-modules of rank 1 locally on spec(R'). (This condition holds automatically if $R = \boldsymbol{C}$; for examples where it fails in an analogous situation in characteristic p, see [**18**, 1.29].)

Having defined our functor $\mathscr{S}$ we now have to see whether it is the points functor of a scheme. Generally speaking this is a very delicate question but M. Artin has given an often-manageable set of criteria for a functor to be the points functor of an algebraic space. An algebraic space is a slightly more general object than a scheme, but for our purposes it is just as good; it makes good sense to speak of its points with coordinates in a ring, and the proper and smooth base change theorems in étale cohomology, which are the theorems which allow us to compute Hasse-Weil zeta-functions by reducing modulo a prime, hold for algebraic spaces. (In fact, the algebraic spaces we get are almost certainly schemes, and this surely could be proved by using Mumford's methods [**16**] instead of Artin's.)

Consider first the case that $F = \boldsymbol{Q}$. Then Artin's criteria may be checked and show that there is an algebraic space S, proper and smooth over $\boldsymbol{Z}[\Delta^{-1}]$, such that $S(R) = \mathscr{S}(R)$ for any ring R in which Δ is invertible. In particular $S(\boldsymbol{C}) = \mathscr{S}(\boldsymbol{C}) = S_{\mathscr{C}}(\boldsymbol{C})$ and $S(\bar{\boldsymbol{F}}_p) = \mathscr{S}(\bar{\boldsymbol{F}}_p)$ for any p not dividing Δ. The algebraic family $\mathscr{A} \to S_{\mathscr{C}}$ constructed in 1.4(b) is an element of $\mathscr{S}(S_{\mathscr{C}}) = S(S_{\mathscr{C}})$, and so gives a map $S_{\mathscr{C}} \to S$. This induces a map $S_{\mathscr{C}} \to S \times \mathrm{spec}\ \boldsymbol{C}$ which is an isomorphism. Moreover it is known that $S_{\boldsymbol{Q}}$ is the canonical model.

When $F \neq \boldsymbol{Q}$, then a slightly weaker result holds, but one which is just as useful to us. Since there are nontrival automorphisms of $(A, i, \bar{\phi})$ there can be no algebraic space S with $S(R) = \mathscr{S}(R)$ for all R. However, there does exist an algebraic space S, proper and smooth over $Z[\Delta^{-1}]$, and a functorial map $\mathscr{S}(R) \to S(R)$ which is an isomorphism whenever R is an algebraically closed field. Thus $S(\boldsymbol{C}) = \mathscr{S}(\boldsymbol{C}) = S_{\mathscr{C}}(\boldsymbol{C})$ as before, and $S_{\boldsymbol{Q}}$ is the canonical model of $S_{\mathscr{C}}$. To prove these facts one may "rigidify" the moduli problem as in the second paragraph of 1.4(b), make the

constructions as in the case $F = \boldsymbol{Q}$, and then form quotients under the left action by $F^\times$, or else work directly with stacks.

Note that in either case, $S(\bar{F}_p) = \mathscr{S}(\bar{F}_p)$ has a description in terms of abelian varieties with additional structure.

References. [1] contains a short introduction to Artin's techniques for representing functors by algebraic spaces and [2] a more complete one. In [5] and [18] these techniques are applied to a situation which is very similar to ours. (In fact, it is almost identical; see §7 of the Introduction to [5].) The basic definitions concerning abelian schemes can be found in [16].

3. Finite group schemes, p-divisible groups, and Dieudonné modules. In the remaining sections we shall need to consider the finite subgroup *schemes* of an abelian variety and so, in this section, we review some of their properties. We fix a perfect field k of characteristic $p \neq 0$.

Let R be a finite k-algebra (so R is finite-dimensional as a vector space over k) and let $N = \operatorname{spec} R$. For any k-algebra R', a point of N in R' is simply a map of k-algebras $R \to R'$; thus $N(R') = \operatorname{Hom}_{k\text{-alg}}(R, R')$. If every $N(R')$ is given the structure of a commutative group in such a way that the maps $N(R') \to N(R'')$ induced by maps $R' \to R''$ are homomorphisms, then we call N, together with the family of group structures, a *finite group scheme* over k. As for affine algebraic groups, giving the family of group structures corresponds to giving a comultiplication map $R \xrightarrow{m} R \otimes_k R$.

EXAMPLE 3.1. (a) Any (commutative) finite group M can be regarded in an obvious way as an algebraic group over k and hence as a finite group scheme. Indeed, let R be a product of copies of k, one for each element of M, and let $N = \operatorname{spec} R$. Then N, as a set, is equal to M. The group law on M induces a comultiplication on R which, in turn, induces compatible group structures on $N(R')$ for all R'. If R' has no idempotents other than 0 and 1, then $N(R') = M$.

(b) $\boldsymbol{\mu}_{p^n} = \operatorname{spec} k[T]/(T^{p^n} - 1)$. Then $\boldsymbol{\mu}_{p^n}(R') = \{\zeta \in R' | \zeta^{p^n} = 1\}$ is a group under multiplication for any R', and these group structures make $\boldsymbol{\mu}_{p^n}$ into a finite group scheme. Note that $\boldsymbol{\mu}_{p^n}(R) = \{1\}$ if R has no nilpotents and, in particular, if R is an integral domain.

(c) $\boldsymbol{\alpha}_p = \operatorname{spec} k[T]/(T^p)$. Then $\boldsymbol{\alpha}_p(R') = \{a \in R' | a^p = 0\}$. As $(a + b)^p = a^p + b^p$ in any k-algebra, $\boldsymbol{\alpha}_p(R')$ is a group under addition, and these group laws make $\boldsymbol{\alpha}_p$ into a finite group scheme. Again $\boldsymbol{\alpha}_p(R')$ has only one element if R' has no nilpotents.

(d) $\boldsymbol{Z}/p\boldsymbol{Z} = \operatorname{spec} k[T]/(T^p - T)$. If R' has no idempotents other than 0 and 1 (e.g., R' an integral domain) then $(\boldsymbol{Z}/p\boldsymbol{Z})(R') = \boldsymbol{F}_p$, the prime subfield of R', which is a group under addition. This example is a special case of (a), because $k[T]/(T^p - T) = k[T]/T(T - 1) \cdots (T - (p - 1)) \approx k \times \cdots \times k$ (p copies).

The *rank* or *order* of a finite group scheme $N = \operatorname{spec} R$ is the dimension of R as a vector space over k. For example the order of the group scheme defined by M in 3.1(a) is the order of M, while the orders of $\boldsymbol{\mu}_{p^n}$, $\boldsymbol{\alpha}_p$, and $\boldsymbol{Z}/p\boldsymbol{Z}$ are p^n, p and p respectively.

A homomorphism from one finite group scheme $N_1 = \operatorname{spec} R_1$ to a second $N_2 = \operatorname{spec} R_2$ is a k-algebra homomorphism $R_2 \to R_1$ such that the induced maps $N_1(R') \to N_2(R')$ are all homomorphisms of commutative groups.

From now on we consider only finite group schemes of p-power order. The essential facts are the following.

Facts. 3.2.(a) They form an abelian category. Thus we may form kernels, quotients, etc. exactly as if we were working with a category of modules.

(b) When k is algebraically closed the only simple objects are $\boldsymbol{\mu}_p$, $\boldsymbol{\alpha}_p$, $\boldsymbol{Z}/p\boldsymbol{Z}$.

This means that any finite group scheme of p-power order has a composition series whose quotients are $\boldsymbol{\mu}_p$, $\boldsymbol{\alpha}_p$, or $\boldsymbol{Z}/p\boldsymbol{Z}$. There can be no homomorphism from one simple object to another of a different type.

(c) The category is self-dual, i.e., there is a contravariant functor $N \mapsto \hat{N}$ (= Cartier dual of N) which is an equivalence of the category with itself.

More precisely, for each N there is a pairing $N \times \hat{N} \to \boldsymbol{G}_m$ (= GL_1) such that, for any k-algebra R, the pairing induces isomorphisms $N(R) \xrightarrow{\approx} \mathrm{Hom}_R(\hat{N}, \boldsymbol{G}_m)$, $\hat{N}(R) \xrightarrow{\approx} \mathrm{Hom}_R(N, \boldsymbol{G}_m)$. For example, $(\boldsymbol{Z}/p\boldsymbol{Z})^\wedge = \boldsymbol{\mu}_p$ and the pairing $(\boldsymbol{Z}/p\boldsymbol{Z})(R) \times \boldsymbol{\mu}_p(R) \to \boldsymbol{G}_m(R)$ is $(n, \zeta) \mapsto \zeta^n$; $\hat{\boldsymbol{\alpha}}_p = \boldsymbol{\alpha}_p$ and the pairing $\boldsymbol{\alpha}_p(R) \times \boldsymbol{\alpha}_p(R) \to \boldsymbol{G}_m(R)$ is $(a, b) \to \exp(ab) = 1 + ab + \cdots + (ab)^{p-1}/(p-1)!$.

(d) $\mathrm{Hom}(\boldsymbol{Z}/p\boldsymbol{Z}, \boldsymbol{Z}/p\boldsymbol{Z}) = \boldsymbol{Z}/p\boldsymbol{Z}$, $\mathrm{Hom}(\boldsymbol{\mu}_p, \boldsymbol{\mu}_p) = \boldsymbol{Z}/p\boldsymbol{Z}$, $\mathrm{Hom}(\boldsymbol{\alpha}_p, \boldsymbol{\alpha}_p) = k$.

The statement for $\boldsymbol{Z}/p\boldsymbol{Z}$ is obvious, and that for $\boldsymbol{\mu}_p$ follows by Cartier duality. The map $\boldsymbol{\alpha}_p \to \boldsymbol{\alpha}_p$ corresponding to $c \in k$ is $(T \mapsto cT)$: $k[T]/(T^p) \to k[T]/(T^p)$ on the algebra of $\boldsymbol{\alpha}_p$ and $(a \mapsto ca)$: $\boldsymbol{\alpha}_p(R') \to \boldsymbol{\alpha}_p(R')$ on its points.

(e) If $0 \to N' \to N \to N'' \to 0$ is exact then $\mathrm{order}(N) = \mathrm{order}(N')\mathrm{order}(N'')$.

Let A be an abelian variety over k. For each n, $A_{p^n} \overset{\mathrm{df}}{=} \mathrm{Ker}(p^n\colon A \to A)$ is a finite group scheme of order $(p^n)^{2\dim(A)}$, i.e., the order is the same as when $p \neq$ characteristic(k). The system $A_p \hookrightarrow A_{p^2} \hookrightarrow \cdots$ is called the *p-divisible* (or *Barsotti-Tate*) *group* $A(p)$ of A. More generally, a p-divisible group of *height* h is a system of finite group schemes and maps $N = (N_1 \xrightarrow{i_1} N_2 \xrightarrow{i_2} N_3 \xrightarrow{i_3} \cdots)$ such that N_n has order p^{nh} and i_{n-1} identifies N_{n-1} with the kernel of $(N_n \xrightarrow{p^{n-1}} N_n)$. For example $\boldsymbol{Q}_p/\boldsymbol{Z}_p = (\boldsymbol{Z}/p\boldsymbol{Z} \to \boldsymbol{Z}/p^2\boldsymbol{Z} \to \cdots)$ and $\boldsymbol{\mu}_{p^\infty} = (\boldsymbol{\mu}_p \to \boldsymbol{\mu}_{p^2} \to \boldsymbol{\mu}_{p^3} \to \cdots)$ are p-divisible groups of height one. $A(p)$ is of height $2\dim(A)$. A homomorphism $\phi\colon N \to N'$ of p-divisible groups is a family of maps $\phi_n\colon N_n \to N_n'$ commuting with the maps i_n and i_n'.

Exercise 3.3. (k algebraically closed.) For any abelian variety A there are maps $\phi_n\colon A_{p^n} \to \hat{A}_{p^n}$ such that $\mathrm{Ker}(\phi_n) = \mathrm{Ker}(\phi_{n+1})$ for all sufficiently large n. Deduce that A has $\leqq p^{\dim A}$ points of order p, and that when equality holds $A(p) = (\boldsymbol{Q}_p/\boldsymbol{Z}_p)^{\dim(A)} \times (\boldsymbol{\mu}_{p^\infty})^{\dim(A)}$. (Such abelian variety is said to be *ordinary*.)

Let $W = W_k$ be the ring of Witt vectors over k; it is a complete discrete valuation ring of characteristic zero whose maximal ideal is generated by p and which has residue field k. There is a unique automorphism $a \mapsto a^{(p)}$ of W which induces the pth power map on k. If $k = \bar{\boldsymbol{F}}_p$ then W is the completion of the ring of integers in the maximal unramified extension $\boldsymbol{Q}_p^{un}$ of $\boldsymbol{Q}_p$ and $a \mapsto a^{(p)}$ is induced by the usual Frobenius automorphism of $\boldsymbol{Q}_p^{un}$ over $\boldsymbol{Q}_p$. Let $W[F, V]$ be the ring of noncommutative polynomials over W in which the relations $FV = p = VF$ and $Fa = a^{(p)}F$, $aV = Va^{(p)}$, hold for all $a \in W$. There is a contravariant functor, $N \mapsto DN =$ Dieudonné module of N, associating to each p-power order finite group scheme a $W[F, V]$-module which is of finite length as a W-module; D defines an antiequivalence of categories. The length of DN as a W-module is equal to the order of N. Thus manipulations with finite group schemes correspond exactly to manipulations with modules over the noncommutative ring $W[F, V]$. Examples:

$D(\boldsymbol{\mu}_p) = W/pW = k$; F acts as 0, V acts as 1;

$D(\boldsymbol{\alpha}_p) = k$; $F = 0$, $V = 0$;
$D(\boldsymbol{Z}/p\boldsymbol{Z}) = k$; $F = 1$, $V = 0$.

If N is unipotent and $pN = 0$, then $DN = \mathrm{Lie}(\hat{N})$; the bracket operation on $\mathrm{Lie}(\hat{N})$ is zero but it has the structure of a p-Lie-algebra and F acts as the "p-power" operation and V acts as zero. More generally, if N is unipotent and killed by p^n, then $DN = \mathrm{Hom}(N, W_n)$ where $W_1 = \boldsymbol{G}_a$ = the additive group and W_n = the Witt vectors of length n regarded as an algebraic group. There are canonical, nondegenerate, W-bilinear pairings $\langle\ ,\ \rangle: DN \times D\hat{N} \to W \otimes \boldsymbol{Q}_p/\boldsymbol{Z}_p$ such that $\langle Fm, n\rangle = \langle m, Vn\rangle^{(p)}$, $\langle Vm, n\rangle^{(p)} = \langle m, Fn\rangle$.

The notion of Dieudonné module can be extended to p-divisible groups. On applying D to $N = (N_1 \to N_2 \to \cdots)$ we obtain a sequence of modules and maps $(DN_1 \leftarrow DN_2 \leftarrow \cdots)$, and we define $DN = \text{proj lim } DN_n$. This is a $W[F, V]$-module which is free of finite rank equal to height(N) as a W-module.

In classifying p-divisible groups one begins by considering them up to isogeny: N and N' are *isogenous* if there is a surjective homomorphism $N \to N'$ with finite kernel or, equivalently, if there exists an injective homomorphism $DN' \to DN$ whose cokernel has finite length over W. If we write $W' = W[1/p] = W \otimes_{\boldsymbol{Z}_p} \boldsymbol{Q}_p$, $W'[F, F^{-1}] = W'[F, V] = W[F, V] \otimes_{\boldsymbol{Z}_p} \boldsymbol{Q}_p$, and $D'N$ for $DN \otimes_{\boldsymbol{Z}_p} \boldsymbol{Q}_p$ regarded as a $W'[F]$-module, then we see that N and N' are isogenous if and only if $D'N \approx D'N'$.

Let $\mathcal{M}$ be the category of $W'[F]$-modules whose objects occur as $D'N$ for some p-divisible group N. When k is algebraically closed one knows that $\mathcal{M}$ has exactly one simple object $D^\lambda = W'[F]/(F^r - p^s)$ for each rational number λ, $0 \leqq \lambda \leqq 1$, $\lambda = s/r$, $(r, s) = 1$. D^λ has dimension r over W', $\mathrm{End}(D^\lambda)$ is the unique division algebra over $\boldsymbol{Q}_p$ of degree r^2, and any $D \in \mathcal{M}$ can be written uniquely as a finite direct sum $D = (D^{\lambda_1})^{m_1} \oplus \cdots \oplus (D^{\lambda_t})^{m_t}$ with distinct λ_i. Then $\lambda_1, \cdots, \lambda_t$ are the *slopes* of D and $m_i r_i$, where $\lambda_i = s_i/r_i$, is the multiplicity of λ_i. We sometimes write $(D^{s/r})^m$ as $D^{sm/rm}$. Thus $D^{s/r}$ may now be a multiple of a simple module; it has slope s/r with multiplicity r and has dimension r over W'.

When k is algebraically closed and N is a p-divisible group over k, the slopes of $D'N$ are called the slopes of N. Clearly N is uniquely determined up to isogeny by its slopes and their multiplicities. For example, all p-divisible groups of height one are isogenous (in fact, isomorphic) to $\boldsymbol{\mu}_{p^\infty}$ or $\boldsymbol{Q}_p/\boldsymbol{Z}_p$ because $D'(\boldsymbol{\mu}_{p^\infty}) = D^1$ and $D'(\boldsymbol{Q}_p/\boldsymbol{Z}_p) = D^0$ are the only D^λ of dimension one over W'. There is only one simple D^λ of dimension two over W'; it is $D^{1/2} = D'(A(p))$ where A is a supersingular elliptic curve (cf. §5).

Let k have algebraic closure $\bar{k} \neq k$. Any p-divisible group N over k defines a p-divisible group $N_{\bar{k}}$ over $\bar{k}$ and it is known that $DN_{\bar{k}} \approx DN \otimes_{W_k} W_{\bar{k}}$. If $k = \boldsymbol{F}_q$ with $q = p^a$ then $F^a: DN \to DN$ is W-linear and so its characteristic polynomial $\det(T - F^a|DN) = \prod_1^{\mathrm{ht}(N)}(T - \alpha_i)$ is defined. The set of slopes of $D'N_{\bar{k}}$ is $\{\mathrm{ord}_q(\alpha_1), \mathrm{ord}_q(\alpha_2), \cdots\}$ where ord_q is the valuation of the algebraic closure of W'_k such that $\mathrm{ord}_q(q) = 1$.

If A is an abelian variety, we write DA for $DA(p)$. When A is defined over $\boldsymbol{F}_q$ the Frobenius endomorphism $\pi: (a_1, a_2, \cdots) \mapsto (a_1^q, a_2^q, \cdots)$ of A induces F^a on DA. The characteristic polynomial $P_A(T)$ of $\pi: A \to A$ in the sense of [**17**, §19] is $\det(T - F^a|DA)$. Thus the slopes of $D'A_{\bar{k}}$ can be read off from $P_A(T)$.

We can also define profinite group schemes $T_f A = \text{proj lim} A_n$ and $T_l A = \text{proj lim} A_{l^n}$. If $l \neq \mathrm{char}(k)$ and k is algebraically closed then $T_l A$ can be regarded

(as before) as a free $\boldsymbol{Z}_l$-module of rank 2 dim(A). We write $T_f A = T_f^p A \times T_p A$.

Finally we note that to classify p-divisible groups up to isomorphism, it is necessary to classify the (F, V)-stable lattices in the objects of $\mathscr{M}$.

References. The best introduction to the subject matter of this section is [**6**].

4. $S(\bar{\boldsymbol{F}}_p)$ as a family of abelian varieties. Fix a prime p not dividing Δ. From §2 we know that points of $S(\bar{\boldsymbol{F}}_p)$ correspond to isomorphism classes of triples $(A, i, \bar{\phi})$ where A is an abelian variety of dimension $2d$ over $\bar{\boldsymbol{F}}_p$, i is an action of O_B on A, and $\bar{\phi}$ is a K^p-equivalence class of isomorphisms $\phi\colon T_f^p A \to V(\boldsymbol{Z}_f^p)$ where $T_f^p A = \operatorname{proj\,lim}_{p\nmid n} A_n(\bar{\boldsymbol{F}}_p)$. (Recall that $\phi_p\colon T_p A \to V(\boldsymbol{Z}_p)$ is defined only over the ground ring with p inverted, and $\boldsymbol{F}_p[p^{-1}]$ is the zero ring.) The $O_B \otimes \bar{\boldsymbol{F}}_p$-module $\boldsymbol{t}_A$ satisfies the following condition:

(4.1) the subspaces corresponding to the idempotents $\left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}0&0\\0&1\end{smallmatrix}\right)$ in $O_B \otimes \bar{\boldsymbol{F}}_p \approx M_2(\bar{\boldsymbol{F}}_p)$ are free $O_F \otimes \bar{\boldsymbol{F}}_p$-modules of rank 1.

If A is defined by equations $\Sigma a_{(i)} T^{(i)}$, let $A^{(p)}$ be the abelian variety over $\bar{\boldsymbol{F}}_p$ defined by the equations $\Sigma a_{(i)}^p T^i$. There is a Frobenius map $F = F_A\colon A \to A^{(p)}$ which takes a point with coordinates $(t_1, \cdots, t_{\cdot,\cdot})$ to $(t_1^p, \cdots, t_n^p)$. The map F_A is a purely inseparable isogeny of degree p^{2d}, which means that A_F, the kernel of F, is a finite group scheme of order p^{2d} with only one point in any field (so that only $\boldsymbol{\alpha}_p$ and $\boldsymbol{\mu}_p$ occur in any composition series for it). As groups, $D(A) = D(A^{(p)})$, but the identity map $DA \to DA^{(p)}$ is (p)-linear, i.e., $am \mapsto a^{(p)}m$ for $a \in W$, $m \in DA$. The composite $DA \xrightarrow{\mathrm{id}} DA^{(p)} \xrightarrow{DF_A} DA$ is a multiplication on the left by $F \in W[F, V]$ (see [**6**, p. 63]). Since F_A is zero on $\boldsymbol{t}_A$, $\boldsymbol{t}_A \approx \boldsymbol{t}_{A_F} \approx D\hat{A}_F \approx (DA_F)^* = \operatorname{dual}(\operatorname{Coker}(DA \xrightarrow{F} DA))$. Thus (4.1) may be checked on $DA/F(DA)$ instead of $\boldsymbol{t}_A$.

If $P \in S(\bar{\boldsymbol{F}}_p)$ corresponds to $(A, i, \bar{\phi})$ then, intuitively, we may think of the coordinates $(a_1, \cdots, a_r)$ of P as being the coefficients of the equations defining A. Thus Frob(P) corresponds to $(A^{(p)}, i^{(p)}, \phi^{(p)})$ where $i^{(p)}$ and $\bar{\phi}^{(p)}$ are such that F_A defines a map of triples $(A, i, \bar{\phi}) \to (A^{(p)}, i^{(p)}, \bar{\phi}^{(p)})$.

Finally we observe that there are "Hecke operators" acting. Let $g \in G(\boldsymbol{A}_f)$ and suppose that K' is an open subgroup of $G(\boldsymbol{Z}_f)$ such that $g^{-1}K'g \subset K$; then $x \mapsto xg\colon G(\boldsymbol{A}) \to G(\boldsymbol{A})$ induces a map $G(\boldsymbol{Q})\backslash G(\boldsymbol{A})/K_\infty K' \to G(\boldsymbol{Q})\backslash G(\boldsymbol{A})/K_\infty K$ which arises from a map of varieties $\mathscr{T}(g)\colon {}_{K'}S_C \to {}_K S_C$. If P corresponds to $(A', i', \bar{\phi}')$ then $\mathscr{T}(g)P$ corresponds to $(A, i, \bar{\phi})$ if there is an O_B-isogeny $\alpha\colon A \to A'$ such that

$$\begin{array}{ccc} T_f A & \xrightarrow{T_f\alpha} & T_f A' \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi'} \\ V(\boldsymbol{Z}_f) & \xrightarrow{mg} & V(\boldsymbol{Z}_f) \end{array}$$

commutes with m some positive integer. When we pass to S_p, only $G(\boldsymbol{A}_f^p)$ continues to act: if $g \in G(\boldsymbol{A}_f^p)$ and $P \in {}_{K'}S(\bar{\boldsymbol{F}}_p)$ and $\mathscr{T}(g)P \in {}_K S(\bar{\boldsymbol{F}}_p)$ correspond respectively to $(A', i', \bar{\phi}')$ and $(A, i, \bar{\phi})$ then there is an isogeny $\alpha\colon A \to A'$ whose kernel has order prime to p and a commutative diagram

$$\begin{array}{ccc} T_f^p A & \xrightarrow{T_f^p\alpha} & T_f A' \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi'} \\ V(\boldsymbol{Z}_f^p) & \xrightarrow{mg} & V(\boldsymbol{Z}_f^p) \end{array}$$

with m a positive integer prime to p. This definition is compatible with that over $\boldsymbol{C}$ in the sense that both mappings $\mathscr{T}(g)$ come by base change from a mapping $\mathscr{T}(g)\colon {}_{K'}S \times \operatorname{spec} \boldsymbol{Z}_{(p)} \to {}_{K}S \times \operatorname{spec} \boldsymbol{Z}_{(p)}$ where $\boldsymbol{Z}_{(p)} = \{m/n \in \boldsymbol{Q} | (n, p) = 1\}$. (More concretely, this means that if $(A, i, \bar{\phi})$ in characteristic zero specializes to $(\bar{A}, \bar{\imath}, \bar{\bar{\phi}})$ in characteristic p then $\mathscr{T}(g)(A, i, \bar{\phi})$ specializes to $\mathscr{T}(g)(\bar{A}, \bar{\imath}, \bar{\bar{\phi}})$.)

5. The isogeny classes. Fix a prime p not dividing Δ and consider pairs (A, i) where A is an abelian variety of dimension $2d$ over $\bar{\boldsymbol{F}}_p$ and i is a homomorphism $B \hookrightarrow \operatorname{End}^\circ(A)$ such that $i(1) = 1$. We write $A \sim A'$ if A and A' are isogenous, and $(A, i) \sim (A', i')$ if the pairs are B-isogenous in an obvious sense. $\mathscr{I}_p$ denotes the set of all B-isogeny classes and $(A, i) \otimes \boldsymbol{Q}$ the class containing (A, i). It will turn out (last paragraph below) that the map $(A, i, \bar{\phi}) \mapsto (A, i) \otimes \boldsymbol{Q}\colon S(\bar{\boldsymbol{F}}_p) \to \mathscr{I}_p$ is surjective and so, to describe $S(\bar{\boldsymbol{F}}_p)$, it suffices to describe $\mathscr{I}_p$ and the fibres of the map. The first is done in this section and the second in the next. Note that Frob (and $\mathscr{T}(g)$) preserves the fibres.

We first remark that, as in characteristic zero, there is a unique weak polarization on A inducing the given involution on B, and that it gives an F-equivalence class of pairings $A_n \times A_n \to \boldsymbol{G}_m$ for all n (cf. [17, §23]). In turn these pairings give an equivalence class of skew-symmetric pairings $\psi_l\colon T_lA \times T_lA \to T_l\boldsymbol{G}_m \approx \boldsymbol{Z}_l$ with nonzero discriminant for each $l \neq p$, and a similar pairing $\psi_p\colon DA \times DA \to W$; this last pairing satisfies the conditions $\psi_p(Fm, n) = \psi_p(m, Vn)^{(p)}$, $\psi_p(Vm, n)^{(p)} = \psi_p(m, Fn)$. All pairings satisfy $\psi(bm, n) = \psi(m, b^*n)$, $b \in B$.

The description of $\mathscr{I}_p$ will be based on the following classification of isogeny classes over a finite field. (Recall that an abelian variety over a field k is *simple* if it contains no nonzero, proper abelian subvariety defined over k and that any abelian variety is isogenous to a product of simple abelian varieties. If A is defined over $\boldsymbol{F}_q$ then $\pi = \pi_A$ is the Frobenius endomorphism $(a_1, a_2, \cdots) \mapsto (a_1^q, a_2^q \cdots)$.)

THEOREM 5.1. (a) *Let A be a simple abelian variety over $\boldsymbol{F}_q$ and let $E = \operatorname{End}^\circ(A)$. Then E is a division algebra with centre $\boldsymbol{Q}[\pi]$, π is an algebraic integer with absolute value $q^{1/2}$ under any embedding $\boldsymbol{Q}[\pi] \hookrightarrow \boldsymbol{C}$, and for any prime v of $\boldsymbol{Q}[\pi]$ the invariant of E at v is given by*

$$\begin{aligned} \operatorname{inv}_v(E) &= \tfrac{1}{2} && \text{if } v \text{ is real,} \\ &= 0 && \text{if } v|l,\ l \neq p, \\ &= \frac{\operatorname{ord}_v(\pi)}{\operatorname{ord}_v(q)}[\boldsymbol{Q}[\pi]_v\colon \boldsymbol{Q}_p] && \text{if } v|p. \end{aligned}$$

Moreover $2 \dim(A) = [\boldsymbol{Q}[\pi]\colon \boldsymbol{Q}][E\colon \boldsymbol{Q}[\pi]]^{1/2}$ *and* $e = [E\colon \boldsymbol{Q}[\pi]]^{1/2}$ *is the least common denominator of the* $\operatorname{inv}_v(E)$. *The characteristic polynomial $P_A(T)$ of $\pi\colon A \to A$ is $m(T)^e$ where $m(T)$ is the minimal polynomial of π over $\boldsymbol{Q}$.*

(b) *The simple abelian varieties A and A' over $\boldsymbol{F}_q$ are isogenous if and only if there is an isomorphism $\boldsymbol{Q}[\pi_A] \xrightarrow{\sim} \boldsymbol{Q}[\pi_{A'}]$ such that $\pi_A \mapsto \pi_{A'}$.*

(c) *Every algebraic integer π which has absolute value $q^{1/2}$ under any embedding $\boldsymbol{Q}[\pi] \hookrightarrow \boldsymbol{C}$ arises as the Frobenius endomorphism of a simple abelian variety A_π over $\boldsymbol{F}_q$.*

(d) *For any abelian varieties A and B over $\boldsymbol{F}_q$ and any prime l (including $l = p$) the canonical map*

$$\mathrm{Hom}(A, B) \otimes \boldsymbol{Z}_l \to \mathrm{Hom}(A(l), B(l)) = \mathrm{Hom}(T_l A, T_l B)$$

is an isomorphism. (If $l \neq p$ then $A(l)$ and $B(l)$ can be regarded as $\mathrm{Gal}(\bar{\boldsymbol{F}}_q/\boldsymbol{F}_q)$*-modules.)*

PROOF. The first part of (a) (the Riemann hypothesis) is due to Weil, part (c) to Honda, and the remainder to Tate; see [17], [21], [7], [22], [23].

For example, if in (c) we take $\pi = p^a$, $q = p^{2a}$ then we obtain an elliptic curve A_{p^a} such that $\mathrm{End}^\circ(A_{p^a})$ is a quaternion algebra over $\boldsymbol{Q}$ which is split everywhere except at p and the real prime. Any such elliptic curve is said to be *supersingular*.

It follows easily from (a) that if $\boldsymbol{Q}[\pi]$ has a real prime then either A is a supersingular elliptic curve or becomes isogenous to a product of two such curves over $\boldsymbol{F}_{q^2}$.

From now on we let p factor as $(p) = \mathfrak{p}_1 \cdots \mathfrak{p}_m$ in O_F, where the $\mathfrak{p}_i$ are distinct prime ideals, and we let d_i be the residue class degree of $\mathfrak{p}_i$ over p; thus $d = \sum d_i$.

PROPOSITION 5.2. *Let (A, i) be as above. The centralizer of B in* $\mathrm{End}^\circ(A)$ *is either*:

(a) *a quaternion algebra B' over F which splits except at the infinite primes, the primes where B is not split, and the $\mathfrak{p}_i$ for which d_i is odd, and there does not split*; *or*

(b) *a totally imaginary quadratic field extension F' of F which splits B.*

In the first case $A \sim A_0^{2d}$ where A_0 is a supersingular elliptic curve and in the second $A \sim A_0^2$ where A_0 is an abelian variety such that $F' \subset \mathrm{End}^\circ(A_0)$.

PROOF. Suppose $A \sim A_0^r \times A_1$, $r \geqq 1$, where A_0 is a supersingular elliptic curve and $\mathrm{Hom}(A_0, A_1) = 0$. Then $\mathrm{End}^\circ(A) \approx M_r(E) \times \mathrm{End}^\circ(A_1)$, where $E = \mathrm{End}^\circ(A_0)$, and B embeds into $M_r(E)$. Consider $F \hookrightarrow M_r(E)$; we must have $d|2r$, but $d = 2r$ is impossible because F does not split E [19, Theorem 10], and so $r = d$ or $2d$. The Skolem-Noether theorem shows that, when composed with an inner automorphism, the map $F \to M_r(E)$ factors through $M_r(\boldsymbol{Q})$. Thus the centralizer $C(F)$ of F in $M_r(E)$ is isomorphic to $M_{r/d}(F) \otimes E = M_{r/d}(E \otimes F)$. Let C be the centralizer of B in $M_r(E)$. Then $B \otimes_F C \approx C(F)$ because $C(F)$ and B are central simple algebras over F [19, §8]. It follows that either $r/d = 1$, $C = F$, and $B = E \otimes F$, or $r/d = 2$ and C is a quaternion algebra over F such that, in the Brauer group of F, $[B] + [C] = [E \otimes F]$. The first is impossible because B splits at infinite primes while E does not; thus the second holds, and this proves that case (a) of the proposition holds.

Next assume that $\mathrm{Hom}(A_0, A) = 0$ when A_0 is a supersingular elliptic curve, and fix a large subfield $\boldsymbol{F}_q$ of $\bar{\boldsymbol{F}}_p$ such that A and all its endomorphisms are defined over $\boldsymbol{F}_q$. From considering $A/\boldsymbol{F}_q$ we get a Frobenius endomorphism $\pi \in \mathrm{End}^\circ(A)$, and the assumption implies that there is no homomorphism $\boldsymbol{Q}[\pi] \to \boldsymbol{R}$. Consider

$$\begin{array}{ccccccc} B & - & B[\pi] & - & B \otimes_F C & - & E \\ | & & | & & | & & \\ F & - & F[\pi] & - & C & & \\ | & & | & & & & \\ \boldsymbol{Q} & - & \boldsymbol{Q}[\pi] & & & & \end{array}$$

where E is $\mathrm{End}^\circ(A)$ and C is the centralizer of B in E. Clearly, $F[\pi] = F$ would contradict our assumption. On the other hand we must have $[F[\pi]: F] \leqq 2$ and $F[\pi] = C$ for otherwise E would contain a commutative subring of dimension

$> 4d = 2\dim(A)$ over $\boldsymbol{Q}$, which is impossible by 5.1(a). Let $F' = C = F[\pi]$; it is a quadratic extension of F and can have no real prime because that would contradict our assumption. It splits B because, for any finite prime $l \neq p$, $(T_l A) \otimes_{\boldsymbol{Z}_l} \boldsymbol{Q}_l$ is free of rank 2 over $F_l' = F' \otimes \boldsymbol{Q}_l$, from which it follows that $B \otimes F_l' \approx M_2(F_l')$, and we are assuming that B splits at any infinite prime or prime dividing p. Let e be an idempotent $\neq 0, 1$, in $(B \otimes F') \cap \mathrm{End}(A)$. Then $A_0 = eA$ is an abelian variety such that $A \sim A_0 \times A_0$. Since elements of F' commute with e, $F' \subset \mathrm{End}^\circ(A_0)$.

REMARK 5.3. In case (b) of 5.2, A_0 is isogenous to a power of a simple abelian variety, $A_0 \sim A_1^r$, because the centre of $E = \mathrm{End}^\circ(A)$ is a subfield of the field F'.

It follows that, for any pair (A, i) as above, A is isogenous to a power of a simple abelian variety and hence $\mathrm{End}^\circ(A)$ is a central simple algebra over the field $\boldsymbol{Q}[\pi]$. Let (A, i) and (A', i') be such that there exists an isogeny $\alpha: A \to A'$. The Skolem-Noether theorem shows that the map $B \xrightarrow{i} \mathrm{End}^\circ(A) \xrightarrow{\alpha_*} \mathrm{End}^\circ(A')$, where $\alpha_*(\gamma) = \alpha\gamma\alpha^{-1}$, differs from $i': B \to \mathrm{End}^\circ(A')$ by an inner automorphism ($\gamma \mapsto \beta\gamma\beta^{-1}$) of $\mathrm{End}^\circ(A')$. Thus $\beta\alpha$ is a B-isogeny $A \to A'$, and we have shown that $A \sim A'$ implies $(A, i) \sim (A', i')$.

We now consider in more detail the situation in 5.2(b). Let $\mathfrak{p}_1, \cdots, \mathfrak{p}_t$, $0 \leqq t \leqq m$, be the primes of F dividing p which split in F' and write $\mathfrak{p}_i = \mathfrak{q}_i\mathfrak{q}_i'$ for $i \leqq t$. Since $O_F \cap \mathrm{End}(A_0)$ and $\boldsymbol{Z}_p$ both act on $A_0(p)$, their tensor product does, and the splitting $F \otimes \boldsymbol{Q}_p \approx F_{\mathfrak{p}_1} \times \cdots \times F_{\mathfrak{p}_m}$ induces an isogeny $A_0(p) \sim A_0(\mathfrak{p}_1) \times \cdots \times A_0(\mathfrak{p}_m)$ and an isomorphism $D'A_0 \approx D'A_0(\mathfrak{p}_1) \times \cdots \times D'A_0(\mathfrak{p}_m)$. Clearly $A_0(\mathfrak{p}_i)$ has height $2d_i$ and so $D'(A_0(\mathfrak{p}_i))$ has dimension $2d_i$ over W'. Since $\phi_p(am, n) = \phi_p(m, an)$ for $a \in F$ the decomposition of $D'A_0$ is orthogonal for ϕ_p, and ϕ_p restricts to a non-degenerate form on each $D'(A_0(\mathfrak{p}_i))$. This implies that the set of slopes $\{\lambda_1, \lambda_2, \cdots\}$ of $D'(A_0(\mathfrak{p}_i))$ is invariant under $\lambda \mapsto 1 - \lambda$.

Fix an $i \leqq t$. As $F_{\mathfrak{p}_i}' \approx F_{\mathfrak{q}_i}' \times F_{\mathfrak{q}_i'}'$ acts on $D'A_0(\mathfrak{p}_i)$, $A_0(\mathfrak{p}_i)$ splits further: $A_0(\mathfrak{p}_i) \sim A_0(\mathfrak{q}_i) \times A_0(\mathfrak{q}_i')$, $D'A_0(\mathfrak{p}_i) \approx D'(A_0(\mathfrak{q}_i)) \times D'(A_0(\mathfrak{q}_i'))$. Since $F_{\mathfrak{q}_i}' \subset \mathrm{End}^\circ(A(\mathfrak{q}_i))$ has degree $d_i = \mathrm{height}(A_0(\mathfrak{q}_i))$ over $\boldsymbol{Q}_p$, $A(\mathfrak{q}_i)$ is isogenous to a power of a simple p-divisible group: we may write $D'A(\mathfrak{q}_i) = D^{k_i/d_i}$, $0 \leqq k_i \leqq d_i$. Correspondingly, $D'A(\mathfrak{q}_i') = D^{k_i'/d_i}$ with $k_i + k_i' = d_i$.

Fix an $i > t$. The $[F_{\mathfrak{q}_i}'\colon \boldsymbol{Q}_p] = 2d_i = \text{height } A_0(\mathfrak{p}_i)$ and so, as above, $A_0(\mathfrak{p}_i)$ is isogenous to a power of a simple p-divisible group and we may write $DA_0(\mathfrak{p}_i) = D^{s/r}$. Since $s/r = 1 - s/r$ we must have $s/r = d_i/2d_i$. We write $k_i = d_i/2$.

Note that for some i, $1 \leqq i \leqq m$, we must have $k_i \neq d_i/2$ for otherwise all slopes of $A(p)$ would equal $\frac{1}{2}$. Then (see §3 and 5.1(a)) $|\pi/q^{1/2}| = 1$ for all primes v of $\boldsymbol{Q}[\pi]$ and so some power of it would equal one. On replacing $\boldsymbol{F}_q$ by a larger finite field we would have $\pi = q^{1/2}$, and this would imply that A is isogenous to a power of a supersingular elliptic curve, i.e., we would be in case (a). This means that $t \geqq 1$—at least one prime $\mathfrak{p}_i$ splits in F'.

THEOREM 5.4. *$\mathscr{I}_p$ contains one element for each pair $(F', (k_i)_{1 \leqq i \leqq m})$ where F' is a totally imaginary quadratic extension of F which splits B and is such that at least one $\mathfrak{p}_i$ splits in it; if $\mathfrak{p}_i$ splits in F' then k_i is an integer with $0 \leqq k_i \leqq d_i$ and otherwise $k_i = d_i/2$; for at least one i, $k_i \neq d_i - k_i$. When $\mathfrak{p}_i$ splits in F' we regard k_i and k_i' as being associated to $\mathfrak{q}_i$ and $\mathfrak{q}_i'$, and we do not distinguish between two pairs $(F', (k_i))$ and $(\bar{F}', (\bar{k}_i))$ which are conjugate over F. There is one additional "supersingular" element.*

For example, if $F = \mathbf{Q}$ then there is the supersingular isogeny class and one class for each quadratic imaginary number field F' which splits B and in which p splits. If p splits completely in F then there is the supersingular class and one class for each totally imaginary quadratic extension F' of F of the right type and choice of one out of each pair of primes dividing a $\mathfrak{p}_i$ which splits in F'; one family of choices is not distinguished from the opposite family.

PROOF OF 5.4. We first construct an isogeny class $(A, i) \otimes \mathbf{Q}$ corresponding to $(F', (k_1, \cdots, k_m))$. As before we let $\mathfrak{p}_i$, $1 \leqq i \leqq t$, be the primes dividing p which split in F'. Consider the ideal in $O_{F'}$,

$$\mathfrak{a} = \mathfrak{q}_1^{(f/d_1)k_1}\,\mathfrak{q}_1'^{(f/d_1)k_1'} \cdots \mathfrak{q}_{t+1}^{(f/d_{t+1})k_{t+1}} \cdots \mathfrak{q}_m^{(f/d_m)k_m}$$

where $f = 2d_1 \cdots d_m$. For some h, $\mathfrak{a}^h$ is principal, say $\mathfrak{a}^h = (\pi)$. If we write $a \mapsto \bar{a}$ for the nontrivial F-automorphism of F' then $\pi\bar{\pi} \in F$ and

$$(\pi\bar{\pi}) = (\mathfrak{q}_1^f\,\mathfrak{q}_1'^f \cdots \mathfrak{q}_m^f)^h \cap O_F = \mathfrak{p}_1^{fh} \cdots \mathfrak{p}_m^{fh} = (p^{fh}).$$

Thus $\pi\bar{\pi} = up^{fh}$ with u a unit in O_F. If u is a square in F then we may replace π by $\pi/u^{1/2}$ and obtain an equation $\pi\bar{\pi} = q$ with $q = p^{fh}$. If u is not a square then we replace π by π^2/u and obtain a similar equation with $q = p^{2fh}$. Note that the condition $k_i \neq k_i'$ for some i implies that $\pi \notin F$ and hence that $F' = F[\pi]$. Under any embedding $F' \hookrightarrow \mathbf{C}$, F maps into $\mathbf{R}$. Thus complex conjugation on $\mathbf{C}$ induces $a \mapsto \bar{a}$ on F'. In particular $\bar{\pi}$ is the complex conjugate of the complex number π and so $\pi\bar{\pi} = q$ implies that $|\pi| = q^{1/2}$.

Let A_π be the abelian variety corresponding, as in 5.1(c) to π, and let $E = \mathrm{End}^\circ(A_\pi)$. For any prime v of $\mathbf{Q}[\pi]$

$$\begin{aligned} \mathrm{inv}_v(E) &= 0 && \text{if } v \nmid p, \\ &= (k_i/d_i)[\mathbf{Q}[\pi]_v\colon \mathbf{Q}_p] && \text{if } v \mid p \text{ and } \mathfrak{q}_i \mid v, \\ &= (k_i'/d_i)[\mathbf{Q}[\pi]_v\colon \mathbf{Q}_p] && \text{if } v \mid p \text{ and } \mathfrak{q}_i' \mid v. \end{aligned}$$

Let e_v be the denominator of $\mathrm{inv}_v(E)$ (when it is expressed in its lowest terms) and let e be the least common multiple of the e_v. Then $2\dim(A_\pi) = re$ where $r = [\mathbf{Q}[\pi]\colon \mathbf{Q}]$. Clearly $e_v \mid [F_{\mathfrak{q}}'\colon \mathbf{Q}[\pi]_v]$ for any $\mathfrak{q} \mid v$, $v \mid p$, which implies (by class field theory) that F' splits E and (trivially) that e divides $[F'\colon \mathbf{Q}[\pi]] = 2d/r$. As $[M_{2d/re}(E)\colon \mathbf{Q}[\pi]] = (2d/re)^2e^2 = [F'\colon \mathbf{Q}[\pi]]^2$, F' embeds into $M_{2d/re}(E)$ [**19**, Theorem 10]. Let $A_0 = A_\pi^{2d/re}$. The characteristic polynomial $P_{A_\pi}(T)$ of π on A_π is $c_\pi(T)^e$ where $c_\pi(T)$ is the minimal polynomial of $\pi \in \mathbf{Q}[\pi]$ over $\mathbf{Q}$ (5.1(a)). Thus $P_{A_0}(T)$ is $c_\pi(T)^{2d/r}$ which equals the characteristic polynomial of $\pi \in F'$ over $\mathbf{Q}$. Corresponding to the splitting $F_p' = F_{\mathfrak{q}_1}' \times F_{\mathfrak{q}_1'}' \times \cdots$, we have $A_0(p) \sim A_0(\mathfrak{q}_1) \times A_0(\mathfrak{q}_1') \times \cdots$ and $P_{A_0}(T) = P_1(T)P_1'(T) \cdots$ where $P_i(T)$ (resp. $P_i'(T)$) is the characteristic polynomial of the image π_i of π in $F_{\mathfrak{q}_i}'$ (resp. π_i' of π in $F_{\mathfrak{q}_i'}'$) over $\mathbf{Q}_p$. Thus (see §3) $A(\mathfrak{q}_i)$ has slopes equal to $\mathrm{ord}_q(\pi_i) = (fh/d_i)k_i/fh = k_i/d_i$ and $A(\mathfrak{q}_i')$ has slopes equal to k_i'/d_i. Thus $A = A_0 \times A_0$, regarded as an abelian variety over $\bar{\mathbf{F}}_p$, and the map i induced by $B \hookrightarrow M_2(F')$ represent an isogeny class corresponding to $(F', (k_1, \cdots, k_m))$.

(A_0^{2d}, i), where A_0 is a supersingular elliptic curve, represents the supersingular class.

Obviously if $(A, i) \sim (A', i')$ then both represent the supersingular class or correspond to the same pair $(F', (k_1, \cdots, k_m))$.

It remains to show that if (A, i) and (A', i') both correspond to $(F', (k_1, \ldots, k_m))$ then $(A, i) \sim (A', i')$. By considering A and A' to be defined over some finite subfield of $\bar{F}_p$ we get elements $\pi = \pi_A \in F'$ and $\pi' = \pi_{A'} \in F'$. The assumption implies that $\mathrm{ord}_{\mathfrak{q}}(\pi) = \mathrm{ord}_{\mathfrak{q}}(\pi')$ for all $\mathfrak{q}|p$, $\mathfrak{q}$ a prime of F', and 5.1(a) then shows that $|\pi/\pi'|_v = 1$ for all primes of F'. Thus π and π' differ by a root of 1 and so, after extending the finite field, we may take them to be equal. It follows that A and A', being isogenous to powers of the same abelian variety A_π, are themselves isogenous, and 5.3 completes the proof.

The proof that any class in $\mathscr{S}_p$ is represented by an element of $S(\bar{F}_p)$ requires the following lemma.

LEMMA 5.5. *Let $T \subset T_f A$ be such that $T_f A/T$ is finite; then there exists an isogeny $\alpha: A' \to A$ such that $T_f\alpha$ maps $T_f A'$ isomorphically onto T.*

PROOF. The finiteness of $T_f A/T$ means that, for all $n \gg 0$, the cokernel N of $T/nT \to T_f A/nT_f A$ is independent of n. Thus there is a map $A_n = T_f A/nT_f A \xrightarrow{\phi} N$. Define A' to be the cokernel of $a \mapsto (\phi(a), a): A_n \to N \times A$, and $\alpha: A' \to A$ to be $(b, a) \mapsto na$; then $(T_f\alpha)(T_f A') = T$.

Let (A, i) represent a class in $\mathscr{S}_p$ and let $O' = B \cap \mathrm{End}(A)$; it is an order in B. Regard (A, i) as being defined over a large finite field F_q; then $\mathrm{End}(A) \otimes \boldsymbol{Z}_l \approx \mathrm{End}_{F_q}(T_l A)$ and $O' \otimes \boldsymbol{Z}_l = (B \otimes \boldsymbol{Z}_l) \cap \mathrm{End}_{F_q}(T_l A)$. For almost all l, $O' \otimes \boldsymbol{Z}_l$ will equal $O_B \otimes \boldsymbol{Z}_l$ and we take $T_l = T_l A$; for the remaining l we may choose a T_l of finite index in $T_l A$ which is stable under O_B, i.e., such that $\mathrm{End}_{F_q}(T_l) \cap (B \otimes \boldsymbol{Z}_l) = O_B \otimes \boldsymbol{Z}_l$. Note that $D(T_p/pT_p) = M$ is a $W[F, V]$-module of finite length over W. We may choose T_p such that M/FM satisfies (4.1). Let A' correspond to $T = \prod_l T_l$ as in the lemma. Then A' together with the obvious i and some $\bar{\phi}$ lies in $S(\bar{F}_p)$ and represents $(A, i) \otimes \boldsymbol{Q}$.

6. An isogeny class. It remains to describe the set $Z = Z(A, i, \phi_A)$ of elements $(A', i', \bar{\phi}')$ of $S(\bar{F}_p)$ such that (A', i') is isogenous to a given pair (A, i). An O_B-isogeny $A' \xrightarrow{\alpha} A$ determines an injective map $T_f\alpha: T_f A' \to T_f A$ whose image Λ satisfies the following conditions:

(a) Λ is O_B-stable.

(b) $T_f A/\Lambda$ is a finite group scheme. (More precisely, $\mathrm{Coker}(\Lambda/n\Lambda \to T_f A/nT_f A) = \mathrm{Coker}(A'_n \to A_n) = \mathrm{Ker}(A' \xrightarrow{\alpha} A)$ for $n \gg 0$.)

(c) $D(\Lambda/p\Lambda)/FD(\Lambda/p\Lambda)$ satisfies (4.1). (For $\Lambda/p\Lambda = A'_p$ and so $D(\Lambda/p\Lambda)/FD(\Lambda/p\Lambda) = DA/F(DA)$.)

Consider all subobjects Λ of $T_f A$ satisfying (a), (b), (c). Any such Λ may be written $\Lambda = \Lambda^p \times \Lambda_p$ with Λ^p a $\boldsymbol{Z}_f^p$-lattice in $T_f^p A$ (in the usual sense of modules over $\boldsymbol{Z}_f^p$) and $\Lambda_p \subset T_p A$. We let Y be the set of pairs $(\Lambda, \bar{\phi})$ with Λ as above and $\bar{\phi}$ a K-equivalence class of isomorphisms $\Lambda^p \xrightarrow{\approx} V(\boldsymbol{Z}_f^p)$. Since $(\Lambda, \bar{\phi})$ is determined by a pair $((\Lambda^p, \bar{\phi}), \Lambda_p)$, we may write $Y = Y^p \times Y_p$.

By 5.5, every $(\Lambda, \bar{\phi}) \in Y$ arises from a triple $(A', i', \bar{\phi}') \in S(\bar{F}_p)$ equipped with an isogeny α; $A' \to A$. Thus we have a surjective map $Y \twoheadrightarrow Z \subset S(\bar{F}_p)$.

For n a positive integer we set $n(\Lambda, \bar{\phi}) = (n\Lambda, n\bar{\phi})$, and we define $Y \otimes \boldsymbol{Q}$ to be the set of pairs (y, n) with $y \in Y$ and $n \in \boldsymbol{Z}_{>0}$, where (y, n) and (y', n') are identi-

fied if $n'y = ny'$. Then we write $Y \otimes \mathbf{Q} = (Y^p \otimes \mathbf{Q}) \times (Y_p \otimes \mathbf{Q})$ where $Y^p \otimes \mathbf{Q}$ may be identified with the set of O_B-stable lattices Λ in $(T_f A) \otimes \mathbf{Q}$ equipped with a K-equivalence class of isomorphisms $\Lambda \xrightarrow{\sim} T_f A$.

There is an action of $H(\mathbf{Q}) = \mathrm{End}^\circ_{O_B}(A)^\times$ on $Y \otimes \mathbf{Q}$: for $\alpha \in H(\mathbf{Q})$ we choose a positive integer m such that $m\alpha$ is an isogeny of A and define $\alpha(\Lambda, \bar{\phi}, n) = (T_f(m\alpha), \overline{\phi T_f(m\alpha)^{-1}}, mn)$.

LEMMA 6.1. *The map $Y \to Z$ described above induces a bijection $H(\mathbf{Q})\backslash Y \otimes \mathbf{Q} \xrightarrow{\sim} Z$.*

PROOF. $(\Lambda, \bar{\phi}, n)$ and $(\Lambda', \bar{\phi}', n')$ map to the same element of $S(\bar{\mathbf{F}}_p)$ if and only if there exist O_B-isogenies

$$A' \underset{\alpha'}{\overset{\alpha}{\rightrightarrows}} A$$

and an O_B-isomorphism $\phi_0 \colon T_f A' \to V(\mathbf{Z}_f)$ such that

$$n((T_f\alpha)T_f A', \overline{\phi_0(T_f\alpha)}) = (\Lambda, \bar{\phi}) \quad \text{and} \quad n'((T_f\alpha')T_f A', \overline{\phi_0(T_f\alpha')}) = (\Lambda', \bar{\phi}').$$

Then $\alpha'\alpha^{-1}$ makes sense as an element of $\mathrm{End}^\circ(A)$ and $\alpha'\alpha^{-1}(\Lambda, \bar{\phi}, n) = (\Lambda', \bar{\phi}', n')$.

LEMMA 6.2. *The map $G(\mathbf{A}_f^p) \to Y^p \otimes \mathbf{Q}$, $g \mapsto (g(T_f A), \phi_A g^{-1})$, induces a bijection $G(\mathbf{A}_f^p)/K \to Y^p \otimes \mathbf{Q}$.*

PROOF. Obvious.

LEMMA 6.3. *There is a one-one correspondence between $Y_p \otimes \mathbf{Q}$ and the set X of $W[F, V]$-submodules M of $D'A$ which are free of rank $4d$ over W, O_B-stable, and such that M/FM satisfies* (4.1).

PROOF. $p \colon \Lambda \to \Lambda$ induces maps $i_n \colon \Lambda/p^n\Lambda \hookrightarrow \Lambda/p^{n+1}\Lambda$ which define a p-divisible group $\Lambda(p) = (\Lambda/p^n\Lambda, i_n)$. The exact sequence $0 \to \Lambda \to T_p A \to N \to 0$ (N finite) gives rise to $0 \to N \to \Lambda(p) \to A(p) \to 0$. On applying D we get

$$0 \to DA \to D\Lambda(p) \to DN \to 0.$$

Since DN is torsion, we may identify $D'\Lambda(p)$ with $D'A$. To $(\Lambda, n) \in Y^p$ we associate $n^{-1}(D\Lambda(p)) \in X$.

THEOREM 6.4. *With the above notations,*

$$Z(A, i, \bar{\phi}) \approx H(\mathbf{Q})\backslash G(\mathbf{A}_f^p) \times X/K^p.$$

Frob *acts by sending $M \in X$ to FM; the Hecke operator $\mathscr{T}(g)$, $g \in G(\mathbf{A}_f^p)$, "acts" by multiplication on the right on $G(\mathbf{A}_f^p)$.*

PROOF. This simply summarizes the above.

It remains to give a more explicit description of X. Note that, corresponding to the splitting $D'A \approx D'A(\mathfrak{p}_1) \times \cdots \times D'A(\mathfrak{p}_m)$, we have $X \approx X_1 \times \cdots \times X_m$. It is convenient to write $\bar{G}_i(\mathbf{Z}_p) = \mathrm{Aut}_{O_B}(A(\mathfrak{p}_i))$ and $\bar{G}_i(\mathbf{Q}_p) = \mathrm{End}^\circ_{O_B}(A(\mathfrak{p}_i))^\times = \mathrm{End}_{O_B}(D'A(\mathfrak{p}_i))^\times$. In the simplest cases $\bar{G}_i(\mathbf{Q}_p)$ acts transitively on the lattices $M \subset D'A(\mathfrak{p}_i)$ which belong to X_i, and in this case $X_i \approx \bar{G}_i(\mathbf{Q}_p)/\bar{G}_i(\mathbf{Z}_p)$. (To say that $\bar{G}_i(\mathbf{Q}_p)$ acts transitively means that each $A'(\mathfrak{p}_i)$ is isomorphic to $A(\mathfrak{p}_i)$ and not merely isogenous; cf. [6, p. 93].)

EXAMPLES 6.5. (a) $F = \mathbf{Q}$, F' is a quadratic extension of $\mathbf{Q}$, $(p) = \mathfrak{q}\mathfrak{q}'$ in F', and $(A, i, \bar{\phi})$ is in the isogeny class corresponding to $(F', (0))$.

Then $A(p) \approx (\mathbf{Q}_p/\mathbf{Z}_p)^2 \times (\mu_{p^\infty})^2$ with $O_B \otimes \mathbf{Z}_p = M_2(\mathbf{Z}_p)$ acting in the obvious way on each factor. Thus $\bar{G}(\mathbf{Z}_p) = \{\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right) \mid a,\ b \in \mathbf{Z}_p^\times\}$ and $\bar{G}(\mathbf{Q}_p) = \{\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right) \mid a,\ b \in \mathbf{Q}_p^\times\}$. In this case $X = \bar{G}(\mathbf{Q}_p)/\bar{G}(\mathbf{Z}_p)$. Frob acts as $\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$.

(b) As above, except $(A, i, \bar{\phi})$ corresponds to $(F', (1))$.

Then $A(p) \approx (\mu_{p^\infty})^2 \times (\mathbf{Q}_p/\mathbf{Z}_p)^2$ (i.e., in the splitting $F'_p = F'_{\mathfrak{q}} \times F'_{\mathfrak{q}'}$, $F'_{\mathfrak{q}}$ now corresponds to the μ_{p^∞} factor). $\bar{G}(\mathbf{Z}_p)$, $\bar{G}(\mathbf{Q}_p)$ and X are as before but Frob acts as $\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

(c) $F = \mathbf{Q}$, $(A, i, \bar{\phi})$ is in the supersingular class.

Then $D'A(p) \approx D^{1/2} \times D^{1/2}$ and $\mathrm{End}(D^{1/2}) = B'_p$, the unique division quaternion algebra over $\mathbf{Q}_p$. B acts through the embedding

$$B \otimes \mathbf{Q}_p \approx M_2(\mathbf{Q}_p) \xrightarrow{\text{canon}} M_2(B'_p).$$

Thus $\bar{G}(\mathbf{Q}_p)$, the centralizer of $B \otimes \mathbf{Q}_p$ in $M_2(B'_p)$, is $(B'_p)^\times$. Moreover $\bar{G}(\mathbf{Z}_p)$ may be taken to be $O^\times$ where O is the maximal order in B'_p. In this case $X \approx \bar{G}(\mathbf{Q}_p)/\bar{G}(\mathbf{Z}_p)$. Frob acts as multiplication by $\bar{\omega}$, a generator of the maximal ideal of O.

(d) F arbitrary, p splits completely in F, $(p) = \mathfrak{p}_1 \cdots \mathfrak{p}_d$, $(A, i, \bar{\phi})$ corresponds to $(F', (k_1, \cdots, k_d))$.

Then $X \approx X_1 \times \cdots \times X_d$ where X_i is as in case (a) if $\mathfrak{p}_i$ splits in F' and $k_i = 0$, as in case (b) if $\mathfrak{p}_i$ splits and $k_i = 1$, and as in case (c) otherwise.

(e) The general case. For a statement of the result, see [**14**]. (This case is treated in detail in: J. Milne, *Etude d'une classe d'isogenie*, Séminaire sur les groupes réductifs et les formes automorphes, Université Paris VII (1977–1978).)

Added in proof (*November* 1978). The outline of a proof in [12] of the conjecture for those Shimura varieties which are moduli varieties is less complete than appeared at the time of the conference. The above proof (completed in the report referred to in 6.5(e)) for the case of the multiplicative group of a quaternion algebra differs a little from the outline in that it depends more heavily on the Honda-Tate classification of isogeny classes of abelian varieties over finite fields. The complete seminar referred to in 6.5(e), which redoes in greater detail much of the material in this article and [3], will be published in the series ***Publications Mathématiques de l'Université Paris 7***.

BIBLIOGRAPHY

1. M. Artin, *The implicit function theorem in algebraic geometry*, Colloq. in Algebraic Geometry, Bombay, 1969, pp. 13–34.

2. ———, *Théorèmes de représentabilité pour les espaces algébriques*, Presses de l'Université de Montréal, Montréal, 1973.

3. W. Casselman, *The Hasse-Weil ζ-function of some moduli varieties of dimension greater than one*, these PROCEEDINGS, part 2, pp. 141–163.

4. P. Deligne, *Travaux de Shimura*, Séminaire Bourbaki, 1970/71, no. 389.

5. P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, Antwerp II, Lecture Notes in Math., vol. 349, Springer, New York, pp. 143–316.

6. M. Demazure, *Lectures on p-divisible groups*, Lecture Notes in Math., vol. 302, Springer, New York, 1972.

7. T. Honda, *Isogeny classes of abelian varieties over finite fields*, J. Math. Soc. Japan **20** (1968), 83–95.

8. Y. Ihara, *The congruence monodromy problems*, J. Math. Soc. Japan **20** (1968), 107–121.

9. ———, *On congruence monodromy problems*, Lecture Notes, vols. 1, 2, Univ. Tokyo, 1968, 1969.

10. ———, *Non-abelian class fields over function fields in special cases*, Actes Congr. Internat. Math., vol. 1, Nice, 1970, pp. 381–389.

11. ———, *Some fundamental groups in the arithmetic of algebraic curves over finite fields*, Proc. Nat. Acad. Sci. U.S.A. **72** (1975), 3281–3284.

12. R. Langlands, *Letter to Rapoport* (Dated June 12, 1974—Sept. 2, 1974).

13. ———, *Some contemporary problems with origins in the Jugendtraum*, Proc. Sympos. Pure Math., vol. 28, Amer. Math. Soc., Providence, R. I., 1976, pp. 401–418.

14. ———, *Shimura varieties and the Selberg trace formula*, Canad. J. Math. **29** (1977), 1292–1299.

15. Y. Morita, *Ihara's conjectures and moduli space of abelian varieties*, Thesis, Univ. Tokyo (1970).

16. D. Mumford, *Geometric invariant theory*, Springer, 1965.

17. ———, *Abelian varieties*, Oxford, 1970.

18. M. Rapoport, *Compactifications de l'espace de modules de Hilbert-Blumenthal*, Compositio Math. (to appear).

19. J. P. Serre, Exposé 7, Séminaire Cartan 1950/51.

20. H. Swinnerton-Dyer, *Analytic theory of abelian varieties*, L.M.S. lecture notes **14** (1974).

21. J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144.

22. ———, *Classes d'isogénie des variétés abéliennes sur un corps fini*, Séminaire Bourbaki, 1968–1969, no. 352.

23. W. Waterhouse and J. Milne, *Abelian varieties over finite fields*, Proc. Sympos. Pure Math., vol. 20, Amer. Math. Soc., Providence, R.I., 1971, pp. 53–64.

UNIVERSITY OF MICHIGAN