ANNALES SCIENTIFIQUES DE L'É.N.S.

WILLIAM C. WATERHOUSE

Abelian varieties over finite fields

Annales scientifiques de l'É.N.S. 4e série, tome 2, nº 4 (1969), p. 521-560

<http://www.numdam.org/item?id=ASENS_1969_4_2_4_521_0>

Ann. scient. Éc. Norm. Sup.,
4e série, t. 2, 1969, p. 521 à 560.

ABELIAN VARIETIES OVER FINITE FIELDS

BY WILLIAM C. WATERHOUSE.

INTRODUCTION.

The classical treatment of complex abelian varieties represents the varieties as quotients of $\mathbf{C}^n$ by lattices, and the study of these lattices (sometimes in the abstract disguise of homology groups) is crucial for the theory. When we leave $\mathbf{C}$ for the wilds of positive characteristic, however, these lattices abandon us. Indeed, as Serre has pointed out, in characteristic p one cannot functorially attach any free abelian group of rank $2g$ to a g-dimensional abelian variety A. To see this it suffices to take A as a supersingular elliptic curve (*cf.* Chapter 4); here $g = 1$ and End $A \otimes_{\mathbf{Z}} \mathbf{Q}$ is a quaternion algebra over $\mathbf{Q}$, and such an algebra simply has no two-dimensional representations over $\mathbf{Q}$.

To replace the lattices, Weil showed that for a prime l, $l \neq p$, the points of A of l-power order look just as they would over $\mathbf{C}$. From them one can then form a free $\mathbf{Z}_l$-module of rank $2g$ on which End A acts. The corresponding results for $l = p$ took longer to find, since multiplication by p^m is not a separable morphism. Its kernel A_{p^m} is however still a group scheme (not étale) of rank $(p^m)^{2g}$, and the A_{p^m} fit together to form what Tate and Serre call a p-divisible group. Ideas beginning in the work of Dieudonné have recently been carried through to establish a correspondence between p-divisible groups over a perfect field and modules over a certain ring.

Over a finite field, Tate has proved that the homomorphisms from one abelian variety to another correspond precisely to the homomorphisms of these various modules. Using this, Tate, Serre and Honda have developed a complete classification of abelian varieties up to isogeny. My article rides the crest of this wave to results on the precise endomorphism rings and isomorphism types of abelian varieties over finite fields.

The theoretical basis of the work is Chapter 3, which discusses a technique for passing from ideals of End A to varieties isogenous to A. (An alternative technique is discussed in the Appendix.) The theory is then applied in Chapter 4 to rederive the classical results of Deuring on elliptic curves. Chapter 5 discusses varieties with End A maximal commutative, and turns up some curious phenomena concerning separability. Chapter 6 shows how over the prime field the theory yields a complete classification of the elementary abelian varieties; at this point it should be clear to the reader how the theory can be applied to other problems. Finally, Chapter 7 considers some pleasant properties of " ordinary " varieties, which seem to be the right generalization of singular elliptic curves that are not supersingular.

I assume some familiarity with basic theorems on abelian varieties. For example, the Poincaré-Weil theorem that any abelian variety is isogenous to a product of elementary abelian varieties (those with only finite subgroups) is used without comment. For this material the reader is referred (inevitably) to Weil [22] and Lang [10]. The other prerequisites are currently available only in fragmented form, and I have ventured to gather them into a coherent body in Chapters 1 and 2.

Indocti discant, et ament meminisse periti. Specific references for them are as follows. On l-adic representations : [10]. On finite group schemes : [13]. On p-divisible groups : [16], [20]. On generalized Dieudonné modules : [12]. On Tate's theorems for finite fields : [18], [19]. On Honda's theorem : [8], [24].

This paper is my Harvard doctoral thesis. At various stages during its preparation I was supported by an NSF Graduate Fellowship and a Putnam Fellowship. The typing was paid for from the contract NSF GP-6432. Finally, my work would not have been possible without Professor John Tate — obviously, since it rests on the lovely theorems for which all mathematicians can be grateful to him. But I have the additional privilege of thanking him here for his invaluable conversations and advice.

TABLE OF CONTENTS.

CHAPTER 1.

l-Adic Representations and p-Divisible Groups.

1.1. l-Adic Representations. — Let A be an abelian variety over a perfect field k, and l a prime $\neq p =$ char k. Multiplication by l^m is a group homomorphism whose kernel A_{l^m} is a finite group scheme of rank $(l^m)^{2g}$, where g is the dimension of A. Being of rank prime to p, A_{l^m} is étale, and hence is completely described by (1) the group $A_{l^m}(\bar{k})$ of its points in the algebraic closure $\bar{k}$ of k and (2) the action on that group of $\mathcal{G}$, the Galois group of $\bar{k}$ over k.

The A_{l^m} form an inverse limit system under $A_{l^{m+1}} \xrightarrow{l} A_{l^m}$, and we can define T_lA as $\varprojlim A_{l^m}(\bar{k})$. This is a free $\mathbf{Z}_l$-module of rank $2g$, and $\mathcal{G}$ operates on it by $\mathbf{Z}_l$-linear maps. The A_{l^m} can all be recovered from it, since T_lA/l^mT_lA is isomorphic as a $\mathcal{G}$-module to $A_{l^m}(\bar{k})$.

Since T_lA is free, we can embed it in a vector space $V_lA = T_lA \otimes_{\mathbf{Z}_l} \mathbf{Q}_l$, which has dimension $2g$ over $\mathbf{Q}_l$ and is a $\mathbf{Q}_l[\mathcal{G}]$-module. The maps

$$l^{-m}T_lA/T_lA \underset{l^m}{\simeq} T_lA/l^mT_lA \simeq A_{l^m}(\bar{k})$$

are $\mathcal{G}$-isomorphisms compatible with inclusion; thus V_lA/T_lA is canonically isomorphic to $A(l) = \varinjlim A_{l^m}(\bar{k})$, the set of all points in $A(\bar{k})$ of l-power order. In particular, the finite subgroups of A defined over k and of l-power order are given by those $\mathbf{Z}_l$-lattices in V_lA which contain T_lA and are taken into themselves by the action of $\mathcal{G}$.

If k is replaced by a finite extension field, the lattice T_lA remains the same; the only change is that the group $\mathcal{G}$ acting on it is replaced by a subgroup of finite index.

Let $\varphi : A \rightarrow B$ be a homomorphism of abelian varieties over k. It clearly takes A_{l^m} to B_{l^m}, and so defines a map $\varphi_l : T_lA \rightarrow T_lB$. Putting $T_l\varphi = \varphi_l$ makes T_l a functor from abelian varieties over k to $\mathbf{Z}_l[\mathcal{G}]$-modules. Extending φ_l to a map $\varphi_l : V_lA \rightarrow V_lB$ likewise makes V_l a functor.

If φ is an isogeny (i. e., surjective with finite kernel), φ_l on V_lA is an isomorphism. On T_lA, φ_l is injective with finite cokernel, and T_lB/φ_lT_lA is isomorphic to the l-primary part $(\ker\varphi)_l$ of $\ker\varphi$. Alternatively, pulling back by φ_l^{-1}, we have $(\ker\varphi)_l \simeq \varphi_l^{-1}T_lB/T_lA$ inside $V_lA/T_lA \simeq A(l)$.

Weil proved that Hom (A, B) is a free $\mathbf{Z}$-module of finite rank, showing in fact that the map

$$\mathrm{Hom}(A, B) \otimes_{\mathbf{Z}} \mathbf{Z}_l \to \mathrm{Hom}_{\mathbf{Z}_l[\mathcal{G}]}(T_l A, T_l B)$$

is injective. Over finite fields the result is much more precise :

Theorem (Tate). — *Assume k is finite. Then*

$$\mathrm{Hom}(A, B) \otimes \mathbf{Z}_l \xrightarrow{\sim} \mathrm{Hom}_{\mathbf{Z}_l[\mathcal{G}]}(T_l A, T_l B).$$

Furthermore, on $A(l)$ the action of the Frobenius automorphism (which generates $\mathcal{G}$) is the action of the Frobenius endomorphism $\mathfrak{f}_A$ of A over k. Thus the right-hand term of the isomorphism is simply all the $\mathbf{Z}_l$-linear $\psi : T_l A \to T_l B$ which satisfy $\psi(\mathfrak{f}_A)_l = (\mathfrak{f}_B)_l \psi$.

1.2. The Module $T_p A$. — Multiplication by p^m is again a homomorphism, and its kernel A_{p^m} is a finite group scheme over k of rank $(p^m)^{2g}$. It is not étale, and so cannot be described by points in $A(\bar{k})$. Now by definition a p-divisible group of height h is a system

$$G_0 \xrightarrow{i_0} G_1 \xrightarrow{i_1} G_2 \to \ldots \to G_m \xrightarrow{i_m} \ldots$$

in which G_m is a finite commutative group scheme of rank $(p^m)^h$, the i_m are group homomorphisms, and for all m

$$0 \to G_m \xrightarrow{i_m} G_{m+1} \xrightarrow{p^m} G_{m+1}$$

is exact. This definition is concocted precisely so that we can say the A_{p^m} form a p-divisible group $A(p)$ of height $2\,g$.

Modules corresponding to such objects are constructed as follows. Let $W = W(k)$ be the ring of infinite Witt vectors over k, i. e. the integers in the absolutely unramified complete extension field L of $\mathbf{Q}_p$ with residue field k. Let σ be the automorphism of W induced by the Frobenius automorphism $x \mapsto x^p$ of k. Let $\mathfrak{A} = W[F, V]$, where F and V are two indeterminates subject to the relations $FV = VF = p$, $F\lambda = \lambda^\sigma F$ and $\lambda V = V\lambda^\sigma$ for $\lambda \in W$.

Let $\mathbf{W}_n$ be the n-th Witt group scheme. If G is any commutative k-group scheme, its Dieudonné module M(G) is

$$\varinjlim \mathrm{Hom}_{k\text{-gp.}}(G, \mathbf{W}_n) \oplus \left[W(\bar{k}) \underset{\mathbf{Z}}{\otimes} \mathrm{Hom}_{\bar{k}\text{-gp.}}(G_{\bar{k}}, \mathbf{G}_{m,\bar{k}}) \right]^{\mathcal{G}}.$$

Theorem (Dieudonné-Cartier-Oda). — M *defines an anti-equivalence from the category of finite commutative group schemes over k of p-power rank to the category of left $\mathfrak{A}$-modules of finite* W*-length, taking a group of rank p^n to a module of length n. It is compatible with perfect base extension, i. e., if* K/k *is perfect,* $M^K(G_K) \simeq W(K) \otimes_{W(k)} M(G)$.

From this Oda easily deduced the

Theorem. — *If* $G = (G_n)$ *is a p-divisible group of height h,* $M(G) = \varprojlim M(G_n)$

is a left $\mathfrak{A}$-module which is W-free of rank h. This gives an anti-equivalence of these two categories, compatible with perfect base extension.

If now A is our abelian variety, we denote by T_pA the left $\mathfrak{A}$-module, W-free of rank $2g$, which is associated to $A(p)$ by this construction. From it A_{p^m} can be recovered as the finite group scheme whose Dieudonné module is T_pA/p^mT_pA. More generally, the finite p-power subgroups of A defined over k are given by those W-sublattices of T_pA which are $\mathfrak{A}$-modules, i. e. taken into themselves by F and V. We can embed T_pA in $V_pA = T_pA \otimes_W L$; this is a $\mathfrak{B}$-module, where

$$\mathfrak{B} = L \otimes_W \mathfrak{A} = L[F, V] = L[F, F^{-1}].$$

Let $\varphi : A \to B$ be a homomorphism; it induces $\varphi_p : T_pB \to T_pA$ and $\varphi_p : V_pB \to V_pA$, and $\varphi \mapsto \varphi_p$ gives a functor to $\mathfrak{A}$-modules or $\mathfrak{B}$-modules. If φ is an isogeny, φ_p on V_p is an isomorphism; on T_p it is an injection with finite cokernel, and T_pA/φ_pT_pB is the Dieudonné module of the p-primary part $(\ker\varphi)_p$.

THEOREM (Tate). — *If k is finite, then*

$$\operatorname{Hom}(A, B) \otimes \mathbf{Z}_p \xrightarrow{\sim} \operatorname{Hom}_{\mathfrak{A}}(T_pB, T_pA).$$

Thus the use of Dieudonné modules gives a theory at $l = p$ corresponding to that for $l \neq p$. The only change is in the variance of the functor, and anyone upset by that can use dual modules in one case or the other.

1.3. FACTS ABOUT p-DIVISIBLE GROUPS. — Any finite commutative group scheme G over k can be written uniquely as a product $G^{et} \times G^0$ with G^{et} étale (i. e. = Spec R with R separable over k) and G^0 local (i. e. = Spec R with R local). This decomposition is compatible with the maps in a p-divisible group, so we have $A(p) = A(p)^{et} \times A(p)^0$. There is of course a corresponding decomposition of T_pA into a direct sum of two $\mathfrak{A}$-modules.

Etale groups can be characterized as those for which the Frobenius $F : G \to G^{(p)}$ is bijective; this is equivalent to saying that F is bijective on the Dieudonné module M(G). The groups sometimes called " of multiplicative type " (the duals of p-power étale groups) are characterized by the fact that V is bijective on their Dieudonné modules. These statements extend immediately to p-divisible groups.

If G is a finite group scheme, its Cartier dual $DG = \mathcal{H}om(G, \mathbf{G}_m)$ is also a finite group scheme, and the double dual is canonically isomorphic to G. If now (G_m) is a p-divisible group, one defines its Serre dual as the p-divisible group (DG_m), where $DG_m \to DG_{m+1}$ is dual to the map $G_{m+1} \xrightarrow{p} G_m$. If A is an abelian variety and $\hat{A}$ the dual variety, then $\hat{A}(p)$ is the Serre dual of $A(p)$.

If $A(p)^{et}$ has height h, the same is true for the étale part of any p-divisible group isogenous to $A(p)$ (i. e., a quotient of it by a finite subgroup). Since A and $\hat{A}$ are isogenous, so are $A(p)$ and $\hat{A}(p)$. Thus the Serre dual of $A(p)$ has an étale part of height h. But groups of multiplicative type are not étale, and so we deduce $h \leqq g = \frac{1}{2}$ height $A(p)$. If $h = g$, so $A(p)$ is half-étale, we say A is *ordinary*. In simple terms, A is ordinary if and only if $A(\bar{k})$ has p^g points killed by p, this being the largest possible number.

CHAPTER 2.

Classification up to Isogeny.

From here on we fix a finite field k with $q = p^a$ elements. — Let A be an abelian variety over k. Any endomorphism φ of A has a characteristic polynomial $P \in \mathbf{Z}[T]$, a monic polynomial of degree $2g$ such that if

$$P = \prod (T - \alpha_i), \qquad \deg Q(\varphi) = \prod Q(\alpha_i) \qquad \text{for all } Q \in \mathbf{Z}[T].$$

Then P is the characteristic polynomial of φ_l on $V_l A$; it is also the characteristic polynomial of φ on $A(p)$, i. e. the characteristic polynomial of φ_p as an L-linear map of $V_p A$.

In particular, the Frobenius endomorphism π of A over k has a characteristic polynomial h_A. This is of special interest because of the

Theorem (Tate). — *The varieties* A *and* B *are isogenous over k if and only if $h_A = h_B$.*

Thus the polynomial determines the isogeny class; we now describe this correspondence in more detail.

On all the $T_l A$, π_l acts semisimply. The algebra $E = \mathbf{Q} \otimes \mathrm{End}_k A$ is semisimple with center $\Phi = \mathbf{Q}(\pi)$. The splitting of A up to isogeny into powers of elementary factors corresponds to the decomposition of E into simple factors, which in turn is given by the factorization of the center Φ into fields Φ_j. This is determined by the factorization of h_A into $\mathbf{Q}$-irreducible factors $\prod P_j^{m_j}$. If A is B^n, then E is an n by n matrix algebra over E(B), and $h_A = h_B^n$.

Thus we may as well assume A is elementary, whence $\Phi = \mathbf{Q}(\pi)$ is a field. As the notation suggests, we identify the Frobenius endomorphism $\mathfrak{f}_{A}$ with an algebraic integer π. By the Weil " Riemann hypothesis ", $|\pi| = q^{\frac{1}{2}}$ in all embeddings of Φ in $\mathbf{C}$; such algebraic integers we will call *Weil numbers*. We now describe how E can be determined from π.

Let then A be elementary, $h_{A} = P^{e}$, with P irreducible over $\mathbf{Q}$ and $P(\pi) = 0$. Let $f = \deg P$, so $ef = 2g$. Then E is a division algebra of dimension e^{2} over its center, which is $\mathbf{Q}(\pi)$. It therefore is determined up to isomorphism by its invariants, which are computed as follows. First, E does not split over the real primes of $\mathbf{Q}(\pi)$, if there are any.

At all primes lying over $l \neq p$, E splits; thus $E_{l} = E \otimes \mathbf{Q}_{l}$ is isomorphic to the sum $\bigoplus M_{e}(\Phi_{j})$ of e by e matrix algebras, where $\Phi \otimes \mathbf{Q}_{l}$ decomposes into the sum of fields $\bigoplus \Phi_{j}$. The space $V_{l}A$ is free of rank e over $\bigoplus \Phi_{j}$, and the action of E_{l} on it is the only possible one, namely the natural action of the matrix algebras on their respective vector spaces.

Suppose finally $\Phi \otimes \mathbf{Q}_{p} = \bigoplus \Phi_{v}$, corresponding to the factorization $P = \prod P_{v}$ in $\mathbf{Q}_{p}$. The space $V_{p}A$ is $2g$-dimensional over L, the unramified extension of $\mathbf{Q}_{p}$ with degree a. On it π_{p} acts by the endomorphism F^{a}, which is in the center of $\mathcal{B} = L[F, F^{-1}]$. As a $\mathcal{B}$-module it is a direct sum $\bigoplus V_{v}$, where on V_{v} π satisfies P_{v}. Then $\mathcal{B}$ operates on V_{v} through $\mathcal{B}_{v} = \mathcal{B}/P_{v}(F^{a})\mathcal{B}$, which is central simple of dimension a^{2} over the field Φ_{v}. Its invariant i_{v} is $\frac{f_{v} \operatorname{ord}_{v} \pi}{a}$, where f_{v} is the residue degree at v; this can also be written as $i_{v} = \frac{\operatorname{ord}_{p} P_{v}(0)}{a}$, or as the equality $q^{-i_{v}} = \| \pi \|_{v}$, where $\| \ \|_{v}$ is the normalized absolute value.

Now by Tate's theorem the commutant of $\mathcal{B}_{v}$ is the image of E_{v}. We check $\dim_{L} V_{v} = en_{v}$, where $n_{v} = |\Phi_{v} : \mathbf{Q}_{p}| = \deg P_{v}$, so $\dim_{\Phi_{v}} v_{v} = ae$; hence E_{v} has degree e^{2} over Φ_{v}, as it should. Its invariant is the same i_{v} as for $\mathcal{B}_{v}$, since $\varphi \mapsto \varphi_{p}$ is contravariant. Since it is simple, its representation on V_{v} is necessarily just a sum of copies of its unique irreducible representation.

Thus given π we can compute the invariants of E. Furthermore, e is the period of E in the Brauer group of Φ, and so is the least common denominator of all the i_{v} (where we include $1/2$ if Φ has a real prime). Hence π determines e, and so gives us $h_{A} = p^{e}$ and determines A up to isogeny. Conversely, of course, π is determined up to conjugacy by A. To top this off, we have the

THEOREM (Honda). — *This is a one-to-one correspondence, i. e. for every Weil number there is an elementary abelian variety giving it.*

We note that the characteristic polynomial of an elementary abelian variety is not in general irreducible. It is so if and only if $e = 1$, if and only if End A is commutative, if and only if there are no real primes and, for all $\wp$ over p, $a \mid f_\wp \operatorname{ord}_\wp \pi$.

We consider briefly the structure of Weil numbers. Suppose first there is a real prime; then in that embedding $\pi^2 = q$, so $\pi = \pm\sqrt{q}$.

Case 1 *: a* even. — Here one of the conjugates of π is the rational number $\pm p^{\frac{a}{2}}$. Hence $P(T) = T \pm p^{\frac{a}{2}}$, and $\Phi = \mathbf{Q}$. At the unique real prime, $i_\infty = 1/2$; hence $i_p = 1/2$, as the sum of all invariants is $0 \pmod{\mathbf{Z}}$. Thus $e = 2$. Then $2 = ef = 2g$, so $g = 1$ and A is an elliptic curve. E is the quaternion algebra over $\mathbf{Q}$ ramified only at ∞ and p. (Such an A is called a " supersingular elliptic curve with all endomorphisms defined "; *cf.* Chapter 4.)

Case 2 *: a* odd. — Here Φ is the real quadratic extension $\mathbf{Q}(\sqrt{p})$, and $f = 2$. There are two infinite primes, with $i = 1/2$ at both; there is a single $\wp$ over p, and so $i_\wp = 0$ since the sum must be $0 \pmod{\mathbf{Z}}$. Then $e = 2$, so $2\,g = 2.2$ and dim A $= 2$. The algebra E is the quaternion algebra over $\mathbf{Q}(\sqrt{p})$ ramified only at the two infinite primes.

Thus real primes are uncommon. Suppose then that $\mathbf{Q}(\pi)$ is totally imaginary. Let $\beta = \pi + \frac{q}{\pi}$. In every embedding $|\pi| = q^{\frac{1}{2}}$, so $\pi\bar{\pi} = q$, and $\beta = \pi + \bar{\pi}$ is real. Thus $\mathbf{Q}(\beta)$ is totally real, and $\mathbf{Q}(\pi)$ is quadratic over it (π satisfies the equation $\pi^2 - \beta\pi + q = 0$). The fact that the solution of this equation is totally imaginary means that in every embedding of $\mathbf{Q}(\beta)$ in $\mathbf{R}$, $|\beta| < 2\sqrt{q}$. Conversely, if β is any totally real algebraic integer satisfying this condition, the solution of $\pi^2 - \beta\pi + q = 0$ will be a Weil number with $\mathbf{Q}(\pi)$ quadratic over $\mathbf{Q}(\beta)$.

Note finally that passing from k to an extension of degree s replaces π by π^s. If $\mathbf{Q}(\pi) = \mathbf{Q}(\pi^s)$, then E is unchanged. It follows that End A is unchanged. Indeed, suppose $\varphi \in E$ is an endomorphism defined over the extension. Then for some m, $m\varphi \in$ End A, since End A is a lattice in E. But $m\varphi$ vanishes on the subgroup A_m, so there is a $\psi : A \to A$ defined over k with $\psi . m = m\varphi$, whence $\varphi = \psi$.

If $\mathbf{Q}(\pi) \neq \mathbf{Q}(\pi^s)$, however, E can change. An elementary variety A may stay elementary but acquire more endomorphisms; an example with A an elliptic curve is given in Chapter 4. Or, A may cease to be elementary. For an example, take Case 2 of the real primes, with $\pi = \pm\sqrt{q}$; passing to a quadratic extension makes π rational, and the variety becomes isogenous to the product of two isomorphic supersingular elliptic curves.

CHAPTER 3.

Isogenies and Kernel Ideals.

3.1. Preliminary Results on Endomorphism Rings. — We now begin the study of isomorphism classes lying in a given isogeny class. We know the isogeny class is determined by a suitable semi-simple algebra E and an element π (generating its center) which represents the Frobenius. The object we consider will actually be a variety A in the isogeny class together with a specific map $i_A : E \xrightarrow{\sim} \operatorname{End} A \otimes \mathbf{Q}$ taking π to $\mathfrak{f}_A$. This eliminates the confusion which otherwise tends to arise in comparing endomorphism rings of different varieties, although it imposes the (perhaps salutary) requirement of making the dependence on i_A explicit.

Given an isogeny $\varphi : A \rightarrow B$, we have an i_B naturally induced by i_A as follows. If $\deg \varphi = n$, there is an isogeny $\psi : B \rightarrow A$ such that $\psi \circ \varphi = n.1_A$, $\varphi \circ \psi = n.1_B$ (obvious since $B = A/\ker\varphi$ and $\ker\varphi \subseteq \ker n.1_A$). We define $i_B(\alpha) = \frac{1}{n}\varphi \circ 1_A(\alpha) \circ \psi$. Clearly i_B is an isomorphism; $i_B(\pi)$ is $\mathfrak{f}_B$ because the Frobenius commutes with k-morphisms, giving us

$$i_B(\pi) = \frac{1}{n}\varphi \circ \mathfrak{f}_A \circ \psi = \frac{1}{n}\varphi \circ \psi \circ \mathfrak{f}_B = \mathfrak{f}_B.$$

In this situation we will always assume that B has this particular i_B unless otherwise specified.

Consider the case $A = B$, so φ is an isogeny in End A. Then $\varphi = i_A(\beta)$ for some invertible $\beta \in E$, and $\psi = i_A(n\beta^{-1})$. The new i'_A induced by φ is given by

$$i'_A(\alpha) = \frac{1}{n}\varphi\, i_A(\alpha)\, \psi = i_A(\beta\alpha\beta^{-1}),$$

and thus is i_A preceded by a conjugation in E.

Proposition 3.1. — *All possible i'_A arise from some isogeny in this way.*

Proof. — Let i'_A be given. Then $i_A^{-1}.i'_A$ is an automorphism of E which takes π to π and hence is identity on the center. By the Skolem-Noether theorem ([1], p. 110) it is an inner automorphism, so $i_A^{-1}.i'_A(\alpha) = \beta\alpha\beta^{-1}$ for some $\beta \in E$. Now End A is a lattice in $\operatorname{End} A \otimes \mathbf{Q}$, so multiplying β by a large integer we may assume $i_A\beta = \varphi \in \operatorname{End} A$. Then i'_A is induced by φ. ❙

Again let $\varphi : A \rightarrow B$ be an isogeny. For $l \neq p$ it induces $\varphi_l : T_l A \rightarrow T_l B$ and an isomorphism $\varphi_l : V_l A \rightarrow V_l B$. There are seemingly two natural ways for E to act on $V_l B$: we can compose i_B with the natural action of $\operatorname{End} B \otimes \mathbf{Q}$, or we can identify $V_l B$ with $V_l A$ via φ_l and take the action on $V_l A$ given by i_A. But as they should be, these two are the same. Indeed, the first takes α to $\left(\frac{1}{n}\varphi \circ i_A(\alpha) \circ \psi\right)_l$. Now $(n.1_A)_l = n$, so functoriality gives $\frac{1}{n}\psi_l = \varphi_l^{-1}$ on V_l, and we see that the second method takes α to $\frac{1}{n}\varphi_l \circ i_A(\alpha)_l \circ \psi_l$.

We know that $\operatorname{End} B \otimes \mathbf{Z}_l$ consists of those elements of $\operatorname{End} B \otimes \mathbf{Q}_l$ taking $T_l B$ to itself. Tracking back the identifications made then gives

Proposition 3.2.

$$\{\alpha \mid i_B(\alpha) \in \operatorname{End} B \otimes \mathbf{Z}_l\} = \{\alpha \mid i_A(\alpha)\ (\varphi_l^{-1} T_l B) \subseteq \varphi_l^{-1} T_l B\}. \ \blacksquare$$

This is a quite computational criterion : $\varphi_l^{-1} T_l B$ is the lattice in $V_l A$ whose quotient by $T_l A$ is the l-primary part of $\ker\varphi$.

Similar results hold at p : the map $\varphi_p : V_p B \to V_p A$ is an isomorphism, and the two possible actions of E on $V_p B$ are the same. We have

Proposition 3.3.

$$\{\alpha \mid i_B(\alpha) \in \operatorname{End} B \otimes \mathbf{Z}_p\} = \{\alpha \mid i_A(\alpha)\ \varphi_p T_p B \subseteq \varphi_p T_p B\}. \ \blacksquare$$

Here $T_p A / \varphi_p T_p B$ is the Dieudonné module corresponding to the p-primary part of $\ker\varphi$.

Example. — Let $i_A(\rho) \in \operatorname{End} A$ be an isogeny, and apply the construction to it. Set $R = i_A^{-1}(\operatorname{End} A)$, $R' = (i'_A)^{-1}(\operatorname{End} A)$. Then $R' = \rho^{-1} R \rho$.

Indeed, $i'_A(\alpha)$ is in $\operatorname{End} A \otimes \mathbf{Z}_l$ iff $i_A(\alpha)_l$ takes $i_A(\rho)_l^{-1} T_l A$ to itself, iff $i_A(\rho\alpha\rho^{-1})_l$ takes $T_l A$ to itself, iff $i_A(\rho\alpha\rho^{-1}) \in \operatorname{End} A \otimes \mathbf{Z}_l$. Up to change of variance, the same holds at p. Now $\operatorname{End} A$ is determined by its localizations, so $i'_A(\alpha) \in \operatorname{End} A$ iff $i_A(\rho\alpha\rho^{-1}) \in \operatorname{End} A$, iff $\rho\alpha\rho^{-1} \in R$, iff $\alpha \in \rho^{-1} R \rho$.

This example shows how the propositions will be used; they give us the localizations of End B, and like any lattice End B is determined by its localizations. To avoid misconceptions, it should be pointed out that the isomorphism type of End B is *not* determined by the isomorphism types of its localizations. For an explicit example, let B be a supersingular elliptic curve with all endomorphisms defined, so (*cf.* Chapter 4) End B is a maximal order in the quaternion algebra over $\mathbf{Q}$ ramified at ∞ and p. For $l \neq p$, $E \otimes \mathbf{Q}_l \simeq M_2(\mathbf{Q}_l)$; the localization of End B is a maximal order in this, and all such are isomorphic ([5], p. 100). Furthermore, $E \otimes \mathbf{Q}_p$ is a division algebra, and so has a unique maximal order. But for most p the quaternion algebra will have non-isomorphic maximal orders [7].

In summary, we have for each A an order $i_A^{-1}(\mathrm{End}\,A)$ in E; this order is determined up to conjugacy, which is the same thing as an isomorphism preserving π. For later calculations we will need to know that we can choose a single member of the conjugacy class for two varieties at once. More precisely, we have

PROPOSITION 3.4. — *Let* A *and* B *be abelian varieties over* k, *and suppose there is a ring isomorphism of* End B *onto* End A *taking* $\mathfrak{f}_B$ *to* $\mathfrak{f}_A$. *Let* i_A *be given. Then there is an isogeny* $\psi : A \rightarrow B$ *for which* $i_A^{-1}(\mathrm{End}\,A) = i_B^{-1}(\mathrm{End}\,B)$.

Proof. — From the results stated in Chapter 2 we know A and B are isogenous; let $\varphi : A \rightarrow B$ be an isogeny. Let

$$i_A^{-1}(\mathrm{End}\,A) = R, \qquad i_B^{-1}(\mathrm{End}\,B) = R'.$$

By the argument of Proposition 3.1, there is a $\rho \in R'$ with $\rho R \rho^{-1} = R'$. Then $i_B(\rho) : B \rightarrow B$ is an isogeny giving us a new i'_B for which $(i'_B)^{-1}(\mathrm{End}\,B) = R$. Hence $\psi = i_B(\rho).\varphi$ has the required property. ❙

Any attempt to describe isomorphism classes seems to be naturally two-fold : find the orders R in E which can be endomorphism rings; then, given an A with $i_A^{-1}(\mathrm{End}\,A) = R$, classify the isogenous B giving the same order. It is possible that the problem in this generality has a reasonable solution, but I am inclined to doubt it. The approach I will take, at least, relies on a study of the ideals of R, and disgracefully little is known about ideal structure of nonmaximal orders. But the method will reduce any specific case to pure computation, and also leads to some interesting general results.

We end this preliminary section with a simple necessary condition on endomorphism rings.

PROPOSITION 3.5. — *If* $R = i_A^{-1}(\mathrm{End}\,A)$, *then* π *and* $q\pi^{-1}$ *are in* R.

Proof. — Clearly $\pi \in R$, as $i_A(\pi) = \mathfrak{f}_A$. For the other, recall that the Frobenius F over $\mathbf{Z}/p\mathbf{Z}$ takes A to the conjugate variety $A^{(p)}$; doing this a times brings us back to A, and $F^a = \mathfrak{f}_A$. Now $\ker F \subseteq A_p$, and there is a functorial map $V : A^{(p)} \rightarrow A$ with $FV = VF = p$ (*cf.* [12]). Then V^a is an endomorphism of A with $F^a V^a = p^a = q$, so $V^a = i_A(q\pi^{-1})$. ❙

For elliptic curves, the only case studied before, the condition was just $\pi \in R$. This is true because there either $q\pi^{-1} = \pi$ (if π is rational) or (*cf.* Chapter 4) $q\pi^{-1}$ is the conjugate of π in a quadratic number field and so lies in the same orders as π. In the general case, however, $q\pi^{-1} \in R$ is definitely a further restriction.

3.2. KERNEL IDEALS. — We now describe a way of constructing finite subgroups of an abelian variety. We fix a variety A and an i_A; when possible we suppress i_A and write α for $i_A(\alpha)$, R for End A, and so on.

Let I be a left ideal of R; then I is a lattice in E if and only if I contains an isogeny. Indeed, if it is a lattice, it contains $n.1_A$ for large n; if it contains an isogeny ρ, it contains $(\deg\rho).\varphi'$ for all $\varphi \in R$. As no others will arise, " ideal " will from now on mean an ideal satisfying these equivalent conditions. If A is elementary, of course, they say simply $I \neq 0$.

DEFINITION. — H(I) *is the intersection of the kernels of all elements of* I.

Clearly H(I) is a finite subgroup, and so gives us an isogenous variety A/H(I) associated with I. To construct it explicitly, take ideal generators $\rho_1, \ldots, \rho_m$ for I; then A/H(I) is easily seen to be the image of A under the map $(\rho_1, \ldots, \rho_m) : A \rightarrow A \times \ldots \times A$. Hence it is the same as the variety constructed in ([17], § 7). A related construction is discussed in the appendix.

We now want to show that A/H(I) depends only on the R-module structure of I. For this we need a criterion for two varieties isogenous to A to be isomorphic; what we get is

PROPOSITION 3.6. — *Let* G_1 *and* G_2 *be two finite subgroups of* A, *not necessarily étale. Then* $A/G_1 \simeq A/G_2$ *if and only if for some isogeny* $\rho \in \operatorname{End} A$ *and some* $0 \neq N \in \mathbf{Z}$, $\rho^{-1}G_1 = (N)^{-1}G_2$.

Proof. — Suppose $A/G_1 \simeq A/G_2$. Then we have $\varphi_i : A \rightarrow B$ with $\ker\varphi_i = G_i$, $i = 1, 2$. For N_1 large (e. g., $N_1 = \operatorname{rank} G_1$), $(N_1)^{-1}G_2 \supseteq G_1$. Now $(N_1)^{-1}G_2 = \ker(N_1\varphi_2)$, so by the definition of quotient there is a $\sigma : B \rightarrow B$ such that $\sigma\varphi_1 = N_1\varphi_2$. For N_2 large enough there is a $\rho : A \rightarrow A$ with $\varphi_1\rho = N_2(\sigma\varphi_1)$ (choose an i_A and look at the two lattices in E). Thus $\varphi_1\rho = N_1N_2\varphi_2$. Set $N = N_1N_2$; then

$$\rho^{-1}G_1 = \ker\varphi_1\rho = \ker N\varphi_2 = N^{-1}G_2.$$

Conversely, $A \xrightarrow{\rho} A \rightarrow A/G_1$ shows that $A/G_1 \simeq A/\rho^{-1}G_1$; likewise $A/G_2 \simeq A/N^{-1}G_2$, so the condition is sufficient. ▎

PROPOSITION 3.7. — *If* I *and* J *are isomorphic* R-*modules, then* $A/H(I) \simeq A/H(J)$.

Proof. — The isomorphism of J to I extends (since both are lattices) to an E-isomorphism of E, and so is given by a scalar multiplication : $I = J\lambda$. For some N we have $N\lambda \in R$, and $NI = J(N\lambda)$. Clearly $H(NI) = N^{-1}H(I)$ and $H(J(N\lambda)) = (N\lambda)^{-1}H(J)$; thus the previous proposition applies. ▎

It is a fact of life that the converse of Proposition 3.7 is false. We do at least have the following criterion, which is clear from the correspondence between lattices and finite subgroups :

PROPOSITION 3.8. — *Let* φ *be the quotient map* $\varphi : A \to A/H(I)$. *Then*

$$\varphi_l^{-1} T_l(A/H(I)) = \bigcap \{ \rho_l^{-1} T_l A \mid \rho \in I \},$$

$$\varphi_p T_p(A/H(I)) = \sum \{ \rho_p T_p A \mid \rho \in I \}.$$

Hence $H(I) = H(J)$ *if and only if the right hand sides of these equalities are the same for* I *and* J. ❙

DEFINITION. — I *is a* kernel ideal *if* $I = \{ \rho \mid \rho H(I) = 0 \}$. (The terminology is derived from the analogous situation in Banach algebras.)

Every I is contained in a kernel ideal J with $H(J) = H(I)$, namely $J = \{ \rho \mid \rho H(I) = 0 \}$. Not all ideals need be kernel ideals. In addition, as examples in Chapter 6 show, the property of being a kernel ideal depends on A, not just on the ring R.

PROPOSITION 3.9. — *Let* $B = A/H(I)$. *Then* $i_B^{-1}(\mathrm{End}\, B)$ *contains the right order of* I, *and equals it if* I *is a kernel ideal.*

Proof. — The α we want are those such that

$$\alpha_l \cap \rho_l^{-1} T_l A \subseteq \cap \rho_l^{-1} T_l A \qquad \text{and} \qquad \alpha_p(\Sigma \rho_p T_p A) \subseteq \Sigma \rho_p T_p A.$$

That is, for all $\tau \in I$, we want

$$\alpha_l \cap \rho_l^{-1} T_l A \subseteq \tau_l^{-1} T_l A, \qquad \text{i. e.} \quad (\tau\alpha)_l \cap \rho_l^{-1} T_l A \subseteq T_l A;$$

and likewise $(\tau\alpha)_p T_p A \subseteq \Sigma \rho_p T_p A$. In particular the conditions imply

$$(\tau\alpha)_l T_l A \subseteq T_l A \qquad \text{and} \qquad (\tau\alpha)_p T_p A \subseteq T_p A,$$

so $\tau\alpha \in R = i_A^{-1}(\mathrm{End}\, A)$. Certainly if $\tau\alpha \in I$, i. e. α is in the right order of I, then the conditions are satisfied. Further, if the conditions hold and we set $J = I + I\alpha$, then J is an ideal of R with $H(J) = H(I)$. Thus if I is a kernel ideal, $I = J$ and α is in the right order of I. ❙

Example. — Let I be the principal ideal $R\rho$. If σ vanishes on $H(I) = \ker \rho$, then by the universal property there is a $\lambda : A \to A$ with $\lambda\rho = \sigma$. Thus $R\rho$ is a kernel ideal. We computed once before that the ring of $A/H(R\rho)$ is $\rho^{-1}R\rho$, the right order of $R\rho$. More generally, we have

LEMMA 3.10. — *If* I *is a kernel ideal, so is* $I\rho$ *for any isogeny* ρ.

Proof. — Let $\lambda \in R$, and suppose that for all x, $I\rho x = 0$ implies $\lambda x = 0$. Then in particular $\rho x = 0$ implies $\lambda x = 0$, so $\lambda H(R\rho) = 0$ and by the example $\lambda \in R\rho$.

Let $\lambda = \beta\rho$; thus for all x, $I\rho x = 0$ implies $\beta\rho x = 0$. Now being an isogeny ρ is surjective; so for all y, $Iy = 0$ implies $\beta y = 0$. As I is a kernel ideal, $\beta \in I$, so $\lambda = \beta\rho \in I\rho$. ❙

From this now we can prove the best converse possible for Proposition 3.7.

THEOREM 3.11. — *Let* I *and* J *be kernel ideals. Then* $A/H(I) \simeq A/H(J)$ *if and only if* I *and* J *are isomorphic* R-*modules, if and only if* $I = J\lambda$ *for some invertible* $\lambda \in E$.

Proof. — Most of this was proved before. Suppose $A/H(I) \simeq A/H(J)$. By Proposition 3.6, then, $\rho^{-1}H(I) = N^{-1}H(J)$. These equal $H(I\rho)$ and $H(JN)$. By the lemma, both $I\rho$ and JN are kernel ideals, so $I\rho = JN$. ❙

Finally we note that ideal multiplication corresponds to composition of isogenies. Specifically,

PROPOSITION 3.12. — *Let* I *be a left ideal of* R, $\varphi : A \to A/H(I) = B$ *the canonical map. Let* J *be a left ideal in* $i_B^{-1}(\mathrm{End}B)$, $\psi : B \to B/H_B(J)$. *Then* $\psi \circ \varphi$ *is the canonical map of* A *onto* $A/H_A(IJ)$.

Proof. — We have

$$\begin{aligned}
&(\psi \circ \varphi)_l^{-1}\, T_l B/H(J) \\
&\quad = \varphi_l^{-1}\, \psi_l^{-1}\, T_l B/H(J) \\
&\quad = \varphi_l^{-1} \cap \{\, i_B(\sigma)_l^{-1}\, T_l B \mid \sigma \in J \,\} \\
&\quad = \cap \{\, \varphi_l^{-1}\, i_B(\sigma)_l^{-1}\, T_l B \mid \sigma \in J \,\} \\
&\quad = \cap \{\, i_A(\sigma)_l^{-1}\, \varphi_l^{-1}\, T_l B \mid \sigma \in J \,\} \\
&\quad = \cap \{\, i_A(\sigma)_l^{-1} \cap i_A(\rho)_q^{-1}\, T_l A \mid \rho \in I,\ \sigma \in J \,\} \\
&\quad = \cap \{\, i_A(\rho\sigma)_l^{-1}\, T_l A \mid \rho \in I,\ \sigma \in J \,\} \\
&\quad = \cap \{\, i_A(\tau)_l^{-1}\, T_l A \mid \tau \in IJ \,\}.
\end{aligned}$$

A similar computation holds at *p*, and we simply compare with Proposition 3.8. ❙

3.3. MAXIMAL ORDERS. — We can draw two immediate consequences from the theory developed in 3.2.

THEOREM 3.13. — *Every maximal order in* E *occurs as an endomorphism ring.*

Proof. — Let S be a maximal order. As R is a lattice in E, we have $NS \subseteq R$ for some integer N. Let $I = R.NS$. This is a left ideal of R, and its right order contains S. Hence the endomorphism ring of $A/H(I)$ contains S; as S is maximal, the two are equal. ❙

THEOREM 3.14. — *If* End A *is a maximal order, so is* End $A/H(I)$ *for any* I.

Proof. — In this case it is known ([5], p. 75) that the right order of I is also maximal. ❙

By drawing much more on the theory of maximal orders [5], we can deduce a quite strong result.

THEOREM 3.15. — *Suppose* End A *is a maximal order. Then every* I *is a kernel ideal, and* rank H(I) *is the reduced norm* N(I).

Proof. — First of all, " reduced norm " must be explained. Since E is semi-simple, it is a direct sum of simple algebras, and the maximal order R = End A is necessarily just a direct sum of maximal orders in the components. In particular, projections on components are in R, so I is a direct sum of left ideals, one in each component. If now J is an ideal in a maximal order S of a simple algebra having dimension e^2 over its center, then the ordinary norm (= card S/J) is an e-th power, and we call its e-th root the reduced norm of J. This is multiplicative under proper multiplication. Finally we let N(I) be the product of the reduced norms of the components of I.

Next we observe that for I = Rλ, N(I) indeed equals rank H(I). For rank H(I) = degλ, the constant term in the characteristic polynomial of λ. Since the same polynomial is the characteristic polynomial of λ on V_lA, which is simply a direct sum of spaces acted on by their matrix algebras, the result is clear.

Now given any I, let R′ be its right order. Then there is an R′-ideal J such that IJ = Rλ and N(J) is prime to rank H(I). Indeed, for E simple this is a theorem of Nehrkorn ([5], p. 106), and we just choose J appropriately on each component. By Proposition 3.12, rank H(I). rank H(J) = rank H(Rλ), and this is N(Rλ) = N(I) N(J). By the choice of J, then, rank H(I) divides N(I). But the same reasoning shows that rank H (J) divides N (J), and so we must have equality.

Finally, if I were not a kernel ideal, its associated kernel ideal would be a larger ideal with the same norm; clearly this is impossible. ❙

Most of this proof is modeled on ([17], p. 56).

This theorem is a good example of the way in which facts about maximal orders can be transformed into facts about varieties, and shows why the absence of theory for non-maximal orders makes the general case much more complicated.

We can now make the simple (and classical) remark that, even for elliptic curves, not every variety isogenous to A need have the form A/H(I); i. e. not every finite subgroup of A has the form H(I). For (*cf.* Chapter 4) there is a curve B with End B non-maximal; the proof of Theorem 3.13 shows B is isogenous to an A with End A maximal, and then Theorem 3.14 shows that B is not of the form A/H(I).

If we restrict to those A with End A maximal, however, the situation is more interesting. Theorem 3.15 shows that we have an action of the

Brandt groupoid of E on the isomorphism classes of such A, but this action will *not* in general be transitive, even if E is commutative. This is a new phenomenon; as we will see in Chapter 5, it is closely related to questions of separability.

CHAPTER 4.

Elliptic Curves.

The goal of this chapter is to illustrate the theory by studying an important special case in which everything can be computed explicitly. Most of the results are from Deuring's classical paper [6], which has been a model for the whole theory.

4.1. Weil Numbers and Isogeny Classes.

Definition ([6], p. 246). — *An elliptic curve is* supersingular *if its endomorphism ring over* $\bar{k}$ *is non-commutative.*

Theorem 4.1. — *The isogeny classes of elliptic curves over k are in one-to-one correspondence with the rational integers β having $|\beta| \leqq 2\sqrt{q}$ and satisfying some one of the following conditions :*

(1) $(\beta, p) = 1$;

(2) *If a is even :* $\beta = \pm 2\sqrt{q}$;

(3) *If a is even and* $p \not\equiv 1 \bmod 3 : \beta = \pm\sqrt{q}$;

(4) *If a is odd and $p = 2$ or 3 :* $\beta = \pm p^{\frac{a+1}{2}}$;

(5) *If either* (i) *a is odd or* (ii) *a is even and* $p \not\equiv 1 \bmod 4 : \beta = 0$.

The first of these are not supersingular; the second are and have all their endomorphisms defined over k; the rest are but do not have all their endomorphisms defined over k.

Proof. — If we are to get an elliptic curve, then in the notation of Chapter 2 we must have $ef = 2g = 2$, so either $f = 1$, $e = 2$ or $e = 1$, $f = 2$. In the first case we have $h_A = P_A^2 = (X - b)^2$, and in the second case $h_A = P_A = X^2 - \beta X + q$.

The first case can occur only for a even, and gives us two isogeny classes corresponding to $h_A = X^2 - \beta X + q$ with $\beta = \pm 2\sqrt{q}$. As we saw before, E is the unique quaternion algebra ramified only at p and ∞; the curves are supersingular with all endomorphisms defined.

In the second case $e = 1$, so there are no real primes, and $|\beta| < 2\sqrt{q}$. A root π of $X^2 - \beta X + q = 0$ is then a Weil number, but it may not give an elliptic curve; for that it must satisfy the additional conditions $a \mid \operatorname{ord} P_\wp(0)$ for the factors $P_\wp$ of P_A over $\mathbf{Q}_p$. To check these we need to know the decomposition of p in $\Phi = \mathbf{Q}(\pi) = \mathbf{Q}(\sqrt{\beta^2 - 4q})$.

LEMMA. — *In* $\mathbf{Q}(\sqrt{\beta^2 - 4q})$:

(1) *p ramifies if*

(i) $\beta = 0$ *and a is odd;*

(ii) $\beta = 0$, *a is even, and* $p = 2$;

(iii) $\beta = \pm\sqrt{q}$, *a is even, and* $p = 3$;

(iv) $\beta = \pm p^{\frac{a+1}{2}}$, *$a$ is odd, and* $p = 2$ *or* 3.

(2) *p stays prime if*

(i) $\beta = 0$, *a is even, and* $p \equiv 3 \bmod 4$;

(ii) $\beta = \pm\sqrt{q}$, *a is even, and* $p \equiv 2 \bmod 3$.

(3) *p splits in all other cases.*

Proof. — Write $\beta = p^b\lambda$, with $\lambda = 0$ or $(\lambda, p) = 1$. If $\lambda = \beta = 0$ we have $\mathbf{Q}(\sqrt{-p^a})$. For a odd, p ramifies; for a even, $p = 2$ ramifies $p \equiv 1 \bmod 4$ splits, $p \equiv 3 \bmod 4$ stays prime.

If $\lambda \neq 0$ and $2b < a$, then

$$\beta^2 - 4q = (p^b)^2 (\lambda^2 - 4p^{a-2b}).$$

As $\lambda^2 - 4p^{a-2b} \equiv \lambda^2 \bmod 4p$, the prime p splits. Note that if $|\lambda| \geq 2$, then necessarily $2b < a$, since $\beta^2 < 4q$.

Say now $\lambda = \pm 1$, $2b \geq a$. As $\beta^2 - 4p^a < 0$, we have either $2b = a$ or $2b = a + 1$ with $p = 2$ or 3. The first gives $\mathbf{Q}(\sqrt{-3})$, where $p = 3$ ramifies, $p \equiv 2 \bmod 3$ stays prime, and $p \equiv 1 \bmod 3$ splits. The second gives either $\mathbf{Q}(\sqrt{-1})$ with $p = 2$ ramified or $\mathbf{Q}(\sqrt{-3})$ with $p = 3$ ramified. ||

Now if p ramifies or stays prime, P_A is irreducible over $\mathbf{Q}_p$ and we automatically have an elliptic curve. The Weil numbers we get, in the order listed in the lemma, are

$$\pm i\sqrt{q}, \quad \pm i, \quad \pm 3^{\frac{a}{2}} \frac{1 \pm i\sqrt{3}}{2}, \quad \pm 2^{\frac{a+1}{2}}(1 \pm i),$$

$$\pm 3^{\frac{a-1}{2}} \frac{3 \pm i\sqrt{3}}{2'}, \quad \pm i\sqrt{q} \quad \text{and} \quad \pm p^{\frac{a}{2}} \frac{1 \pm i\sqrt{3}}{2}.$$

The second, second, third, fourth, sixth, second, and third powers of these respectively are rational, so all the curves are supersingular, the rest of their endomorphisms becoming defined over the extension of the stated degree.

(One could deduce without computation that some power of such a π is rational. Indeed, since $\pi\bar{\pi} = q$ and there is a unique valuation over p in $\mathbf{Q}(\pi)$, we must have $\operatorname{ord}\pi = \frac{1}{2} \operatorname{ord} q$. Thus all absolute values of $\frac{\pi}{\sqrt{q}}$ are 1, whence it is a root of unity.)

Suppose now p splits as $\mathfrak{p}\mathfrak{p}'$. We have $N\pi = q$, so $(\pi) = \mathfrak{p}^m \mathfrak{p}'^n$ with $m + n = a$. The invariants at the two primes then are $\frac{m}{a}$ and $\frac{n}{a}$, so for $e = 1$ we need $m = 0$ or $n = 0$. As $\beta = \pi + \bar{\pi}$, the necessary and sufficient condition is that neither $\mathfrak{p}$ nor $\mathfrak{p}'$ divide β, i. e. $(\beta, p) = 1$. In this case π^s is never rational, since $(\pi^s) = \mathfrak{p}^{as}$ or $(\mathfrak{p}')^{as}$; hence the curves are not supersingular. |

Remark. — We seem to be committing an abuse of language by talking of elliptic curves instead of abelian varieties of dimension 1. This is, however, justified by a theorem of F. K. Schmidt ([3], p. 243) which says that every elliptic curve over a finite field has a rational point.

Example. — Over $k = \mathbf{F}_7 = \mathbf{Z}/7\mathbf{Z}$, we have 11 isogeny classes of elliptic curves $(5 < 2\sqrt{7} < 6)$, one of them supersingular. Not all its endomorphisms are defined over k; indeed, no supersingular curve can have all its endomorphisms defined over a prime field.

Over $\mathbf{F}_{49}$ there are 27 isogeny classes, all values $|\beta| \leqq 14$ being admissible except $\beta = \pm 7$. Those coming by extension from $\mathbf{F}_7$ are $\beta = -14$, -13, -10, -5, 2, 11; to see this just note that if $\pi^2 - \beta\pi + q = 0$, then

$$(\pi^2)^2 - (\beta^2 - 2q)\pi^2 + q^2 = 0.$$

Observe that β and $-\beta$ give the same isogeny class in this extension.

Consider the supersingular curves with all endomorphisms defined; as soon as a is even there are two isogeny classes of them, corresponding to $\beta = 2\sqrt{q}$ and $\beta = -2\sqrt{q}$. When we make a quadratic extension these two fall together : any two supersingular curves are isogenous over a quadratic extension of a field where all their endomorphisms are defined. But the extension which identified these two classes created also a new isogeny class; there are two classes at each stage, even though any two fixed curves eventually become isogenous. It is this sort of non-stable behavior which is overlooked in a treatment like Deuring's which considers only endomorphism rings over $\bar{k}$. Such a treatment also loses sight of the curves with not all endomorphisms defined, which can form as many as three more isogeny classes.

4.2. Endomorphism Rings.

Theorem 4.2. — *Let* E *be the endomorphism algebra of an isogeny class of elliptic curves. The orders in* E *which are endomorphism rings of curves in the class are as follows :*

(1) *If the curves are supersingular with all endomorphisms defined : the maximal orders;*

(2) *If the curves are not supersingular : all orders containing* π*;*

(3) *If the curves are supersingular with not all endomorphisms defined : the orders which contain* π *and are maximal at* p, *i. e. have conductors prime to* p.

Proof. — Take first case (1). It of course suffices to prove that End A is maximal everywhere locally. For $l \neq p$, $E \otimes \mathbf{Q}_l$ is $M_2(\mathbf{Q}_l)$ operating on the 2-dimensional $\mathbf{Q}_l$-space $V_l A$. In $V_l A$ is the lattice $T_l A$. The set of matrices taking $T_l A$ to itself is then conjugate to the set taking any other lattice to itself, thus conjugate to $M_2(\mathbf{Z}_l)$, and hence maximal.

For $l = p$, now, $V_p A$ is a $2a$-dimensional space over $\Phi_v = \mathbf{Q}_p$. Acting on it is the algebra

$$L[F, F^{-1}]/(F^a - \pi) = L[F]/(F^a - \pi),$$

which is central simple of invariant $\frac{1}{2}$ and dimension a^2 over $\mathbf{Q}_p$. It has a unique $2a$-dimensional representation, so we simply construct such a representation. Passing to a quadratic extension of k leaves E and hence End A unchanged, so we may assume $\pi = p^{\frac{a}{2}}$. Let V be a 2-dimensional L-space with basis x, y. Define

$$F(\alpha x + \beta y) = p\beta^\sigma x + \alpha^\sigma y, \qquad \text{where} \quad \alpha, \beta \in L$$

and σ is the Frobenius; this gives an action of L [F] with $F^a = p^{\frac{a}{2}}$.

Elements of the commutant in particular commute with the L-action and so are given by 2×2 matrices over L. Computing the action of F, we find that the commutant comprises the matrices of the form

$$\begin{pmatrix} \alpha & p\beta^\sigma \\ \beta & \alpha^\sigma \end{pmatrix}, \qquad \alpha^{\sigma^2} = \alpha, \quad \beta^{\sigma^2} = \beta.$$

This is the quaternion algebra, as it should be.

Suppose now T is any lattice in V invariant under W; it has then a basis of the form $p^n x$, $cx + p^m y$ with $c \in L$ and either $c = 0$ or ord $c < n$. If $FT \subseteq T$, we have

$$p^n y = \lambda p^n x + \mu c x + \mu p^m y,$$
$$p^{m+1} x + c_\sigma y = \alpha p^n x + \beta c x + \beta p^m y$$

for some λ, μ, α, β in W. The first equation gives ord $\mu = n - m$ and ord c + ord $\mu \geqq n$, i. e. $n \geqq m$ and ord $c \geqq m$. The second gives ord β = ord $c - m$ and then $m + 1 \geqq \min\{2 \operatorname{ord} c - m, n\}$ with equality if $2 \operatorname{ord} c - m < n$. The equality cannot hold, since 2 ord c is even while $2m + 1$ is odd. Thus $2 \operatorname{ord} c - m \geqq n$, $m + 1 \geqq n$, which implies ord $c \geqq n$ and so $c = 0$. Thus T has a basis $p^n x$, $p^n y$ or $p^n x$, $p^{n-1} y$, and so clearly is taken to itself by the maximal order in the commutant (the matrices with α and β integral).

Take now case (2). Here $P'(\pi) = 2\pi - \beta$ is divisible neither by $\mathfrak{p}$ nor by $\mathfrak{p}'$, so $\mathbf{Z}[\pi]$ is maximal at p; the same then is true of any endomorphism ring. At $l \neq p$, $V_l A$ is free of rank 1 over the algebra $E_l = \Phi_l$, and hence it contains a lattice with any prescribed order in Φ. For the lattice to be invariant under the Galois group it is necessary and sufficient that its order contain π.

Choose then a curve A_0 in the isogeny class, and let R be an order containing π. There are only finitely many primes $l_1, \ldots, l_n$ at which $R_l \neq (\operatorname{End} A_0)_l$ since both are lattices. Choose a lattice L_1 in $V_{l_1} A_0$ which contains $T_{l_1} A_0$ and has order R_{l_1}, and let A_1 be the quotient of A_0 by the finite l_1-power subgroup $L_1/T_{l_1} A_0$. Then at $l \neq l_1$, A_1 has the same T_l, and $T_{l_1} A_1 \simeq L_1$, so $\operatorname{End} A_1$ is now correct at l_1 and unchanged elsewhere. Repeat this for $l_2, \ldots, l_n$.

Take finally case (3). At $l \neq p$ the same argument as in case (2) shows that we can get any order containing π. At p however I claim the order must be maximal. Indeed, a base field extension gives a quaternion algebra where we know the order is maximal. Being a division algebra, the quaternion algebra at p has a unique maximal order comprising all integral elements, and the intersection of that with any subfield is the maximal order there. But the argument at the end of Chapter 2 shows that this intersection gives the endomorphism ring over k. ∎

PORISM 4.3. — The foregoing in fact proves a more general statement. Let E be the endomorphism algebra of an isogeny class of abelian varieties, and assume E is commutative. Let R be any order in E containing π. Then there is a variety A in the isogeny class with $(\operatorname{End} A)_l = R_l$ for all primes $l \neq p$.

Example. — The restriction of maximality at p in case (3) is not vacuous. Indeed, in the course of Theorem 4.1 we proved that $\pi = 3\,\frac{1-\sqrt{-3}}{2}$ corresponds to a supersingular elliptic curve over $\mathbf{F}_9$. Here $\mathbf{Z}[\pi]$ has conductor 3 in the maximal order and so is not a possible endomorphism ring.

COROLLARY 4.4. — *A supersingular elliptic curve has no point of order p in* $A(\bar{k})$, *while one not supersingular is ordinary and has p points killed by p.*

Proof. — If the curve is supersingular we may assume all its endomorphisms are defined, in which case our computation shows that $V_p A$ is an irreducible $L[F]$-module; hence $A(p)$ cannot have an étale summand. If now A is not supersingular, we know that π is a unit at one of the valuations $\wp$ over p. Hence F is invertible on $T_\wp \subset V_\wp$, since $F^a = \pi$. Thus one half of $A(p)$ is étale, giving p points killed by p in $A(\bar{k})$. ∎

4.3. Class Groups and Isomorphism Classes.

Theorem 4.5. — *Let* E *be the endomorphism algebra of an isogeny class of elliptic curves,* R *an order in it which is a possible endomorphism ring. Then every ideal of* R *is a kernel ideal for every* A *with* End A = R.

If E *is commutative, the isomorphism classes of curves with endomorphism ring* R *form a principal homogeneous space over the ideal class group of* R.

If E *is noncommutative, the number of isomorphism classes equals the class number of* R (the classes are a homogeneous space for the Brandt groupoid). *Each* R *has one or two isomorphism classes of curves with order* R, *according as the ideal* $\mathfrak{p}$ *in* R *with* $\mathfrak{p}^2 = p$ *is or is not principal.*

Proof. — First we show that every ideal is a kernel ideal. For E noncommutative this follows from Proposition 3.15, so we may assume E commutative. We must show then that an ideal I is determined by the sets $\cap\{\rho^{-1}T_l A \mid \rho \in I\}$ and $\Sigma\{\rho T_p A \mid \rho \in I\} = I.T_p A$. At p the order is maximal, so $T_p A$ is a sum of free modules and $I.T_p A$ determines the localization of I at p.

For $l \neq p$ it is perhaps easier to understand the situation if we dualize. Let $X_l(A)$ be the $\mathbf{Q}_l$-dual space of $V_l(A)$, and $S_l(A)$ the dual lattice of $T_l A$. Then the dual of $\varphi_l^{-1} T_l(A/H(I))$ is simply $I.S_l A$. Now R is an order in a quadratic number field, and $S_l A$ like $T_l A$ is a rank one module whose order is R_l. It therefore is invertible, i. e. free; this is a pleasant feature of orders in quadratic fields. Hence $I.S_l A$ does determine the localization of I at l.

Take E commutative. As already remarked, the ideals of R with order R are all invertible, and conversely all invertible ideals of R have order R. These ideals modulo scalar multiplication form the ideal class group of R. Theorems 3.9, 3.11 and 3.12 show that this ideal class group operates freely on the isomorphism classes of curves with order R. What we must do is show that there is only one orbit.

For this we let G be a finite subgroup of A with End A/G = R; we claim G = H(I) for some ideal I. At $l \neq p$, G corresponds to a lattice including $T_l A$, or to a sublattice of $S_l A$. Since $S_l A$ is free of rank one, this is indeed given by $I_l . S_l A$ for some local ideal I_l. At p, we know R_p is maximal, and the fact that we get all the lattices from ideals is a special case of a computation we will do in Chapter 5; we therefore omit it here. As G is finite, $I_l = R_l$ for all but finitely many l. Hence there is a lattice I whose localizations are the I_l; it is an ideal because it is one locally, and clearly then G = H(I).

Finally, suppose E noncommutative. As before the ideal classes operate on the isomorphism classes. Again we must show there is only one orbit, and again we simply look at lattices. At $l \neq p$ we have (as we saw) $M_2(\mathbf{Z}_l)$ acting on $\mathbf{Z}_l \oplus \mathbf{Z}_l$, and obviously every lattice here is given by some ideal. At p we computed all the invariant lattices in the course of proving Theorem 4.2, and they obviously are all given by powers of the maximal ideal generated by $\begin{pmatrix} 0 & p \\ 1 & 0 \end{pmatrix}$.

This proves all but the very last statement. To get it, take an A with $\operatorname{End} A = R$. By Proposition 3.4, all the other B we want can be gotten from ideals I having $i_B^{-1} \operatorname{End}(A/H(I)) = R$; by Proposition 3.9, these are the two-sided ideals. But every two-sided ideal in R has the form nR or $n\mathfrak{p}$ ([6], p. 263); these represent one ideal class if $\mathfrak{p}$ is principal, two otherwise. ▌

Remark. — The correspondence between ideal classes and isomorphism classes has one interesting consequence. As we saw earlier, a base field extension can leave endomorphism algebras unchanged and still make two isogeny classes fall together. But if two curves are isogenous and not isomorphic, no base field extension leaving their endomorphism rings unchanged can make them isomorphic.

Example : Elliptic curves over $\mathbf{F}_7$. — With isogeny classes indexed by β as before, we have the following orders :

$\beta = 0$, $\pi = \sqrt{-7}$. The order $\mathbf{Z}[\pi]$ has index 2; both it and the maximal order have class number $h = 1$;

$\beta = \pm 1$, $\pi = \frac{1 \pm 3\sqrt{-3}}{2}$. The order $\mathbf{Z}[\pi]$ has index 3; for it and the maximal order, $h = 1$;

$\beta = \pm 2$, $\pi = 1 \pm \sqrt{-6}$. Here $\mathbf{Z}[\pi]$ is maximal, $h = 2$;

$\beta = \pm 3$, $\pi = \frac{3 \pm \sqrt{-19}}{2}$. Again $\mathbf{Z}[\pi]$ is maximal, but $h = 1$;

$\beta = \pm 4$, $\pi = 2 \pm \sqrt{-3}$. The order $\mathbf{Z}[\pi]$ has index 2; for it and the maximal order, $h = 1$;

$\beta = \pm 5$, $\pi = \frac{5 \pm \sqrt{-3}}{2}$. Here $\mathbf{Z}[\pi]$ is maximal, $h = 1$.

All in all there are 18 isomorphism classes of elliptic curves over $\mathbf{F}_7$. Note that the case of $\mathbf{Z}[\pi]$ for $\beta = 0$ shows that the endomorphism ring of a supersingular curve with not all endomorphisms defined need not be the maximal order in E, even though it is the intersection with E of a maximal order in the quaternion algebra.

We owe it to the reader now to mention a fact which has thus far been suppressed. Elliptic curves are simple enough that, besides studying them via their endomorphism rings, one can put them in normal forms and study those. If $p \neq 2,3$ for example, any curve is isomorphic to one of the form $Y^2 = X^3 + AX + B$, two of these being isomorphic iff

$A' = AC^4$, $B' = BC^6$ for some $C \in k$ ([3], p. 211). (The condition that a curve of this form be nonsingular, and so give an elliptic curve, is the well-known $4A^3 + 27B^2 \neq 0$.) Using this we can check the number of isomorphism classes over $\mathbf{F}_7$. The normal form also yields the j-invariant and so lends itself to computing the number of classes which fall together over $\bar{k}$; for this use ([9], § 2).

The two approaches are complementary, not equivalent; comparing them gives interesting relations on class numbers ([6], § 10). Presumably more such relations could be found from moduli for other abelian varieties.

CHAPTER 5.

Principal Varieties.

Definition. — *An abelian variety* A *is* principal *if it is elementary,* E *is commutative, and* End A *is the maximal order in* E.

(Using the results of Chapter 2, it is easy to verify that this agrees with the definition in [17] where the algebra of complex multiplication is taken as all of E.)

Theorem 5.1. — *Let* A *be principal. Then the ideal class group of* $R = i_A^{-1}(\operatorname{End} A)$ *acts freely on the isomorphism classes of principal varieties isogenous to* A.

The number of orbits is $\prod_v N_v$, *where* v *ranges through the valuations of* E *over* p, *and* N_v *is defined as follows. Let* e_v *and* f_v *be the ramification index and residue degree of* E_v *over* $\mathbf{Q}_p$, *and set* $g_v = (f_v, a)$. *Then* N_v *is the number of ordered* g_v*-tuples* $(n_1, \ldots, n_{g_v})$ *satisfying*

$$0 \leq n_1, n_2, \ldots, n_{g_v} \leq e_v$$

and

$$\sum n_i = \frac{g_v \operatorname{ord}_v \pi}{a}.$$

Furthermore, two varieties are in the same orbit if and only if there is a separable isogeny between them.

Proof. — The idea of the proof is simply to construct the representation of E_p on V_pA in a manageable form and compute the lattices involved. We already know every ideal is a kernel ideal; and Theorem 3.11 shows that the class group acts, and that every orbit is a principal homogeneous space. Our basic concern then will be with the number of orbits. Note also that in any ideal class there is an ideal prime to p; Theorem 3.15

then shows that the corresponding isogeny has degree prime to p, and hence is separable. Thus two curves in the same orbit are connected by separable isogenies.

At $l \neq p$, $T_l A$ is rank one over R_l, and so is free since R_l is semi-local and integrally closed. Hence just as before every other lattice can be gotten from it by an ideal of R_l. Thus the question of counting orbits involves only $T_p A$. All ideals in R_p are principal, so we must count the number of admissible lattices in $V_p A$ modulo scalar multiplication.

We first must construct the representation. There is one $2g$-dimensional L-space naturally given to us, namely $L \otimes_{\mathbf{Q}_p} E_p$. Now $E_p = \bigoplus E_\wp$, and $L \otimes E_p \simeq \bigoplus (L \otimes E_\wp)$. On this we have L acting by left multiplication, E_p by right multiplication.

The field $L \cap E_\wp$ has degree $g_\wp = (f_\wp, a)$, and $LE_\wp$ over $E_\wp$ has degree $a/g_\wp$. Then $L \otimes E_\wp$ is a sum of $g_\wp$ copies of the composite extension :

$$L \otimes E_\wp \xrightarrow{\sim} LE_\wp \oplus \ldots \oplus LE_\wp .$$

If σ is the Frobenius of L over $\mathbf{Q}_p$, the map giving this identification is

$$\omega \otimes \beta \mapsto \langle \omega\beta, \sigma(\omega)\beta, \ldots, \sigma^{g_\wp - 1}(\omega)\beta \rangle .$$

An element λ in L acts on the direct sum then by the diagonal matrix

$$\operatorname{diag}(\lambda, \sigma(\lambda), \ldots, \sigma^{g_\wp - 1}(\lambda)).$$

Furthermore, σ acting on the L factor of the tensor product takes the $\omega \otimes \beta$ above to

$$\langle \sigma(\omega)\beta, \sigma^2(\omega)\beta, \ldots, \sigma^{g_\wp}(\omega)\beta \rangle .$$

Here $\sigma^{g_\wp}(\omega)\beta = \tau(\omega\beta)$, where τ is the Frobenius of $LE_\wp$ over $E_\wp$; thus σ acts by a cyclic permutation followed by τ in the last place.

Since E is commutative we have $a \mid f_\wp \operatorname{ord}_\wp \pi$, whence $a/g_\wp$ divides $\operatorname{ord}_\wp \pi$. This is precisely the condition for π to be a norm in the extension $LE_\wp/E_\wp$, which is unramified of degree $a/g_\wp$. Hence we can choose an $\alpha \in LE_\wp$ with

$$N\alpha = \alpha\alpha^\tau \ldots \alpha^{\tau^{-1+\frac{a}{g_\wp}}} = \pi .$$

Let $u = \langle 1, 1, \ldots, 1, \alpha \rangle \in \bigoplus LE_\wp$, and define

$$F = u\sigma .$$

Then $F\lambda = \lambda^\sigma F$ for all $\lambda \in L$, and

$$F^a = (u\sigma)^a = uu^\sigma \ldots u^{\sigma^{a-1}}\sigma^a = Nu = \langle N\alpha, \ldots, N\alpha \rangle = \pi .$$

Thus we have constructed the algebra $\mathcal{B}_\wp$ acting on $\bigoplus LE_\wp$. As this space has the right dimension, it is isomorphic to the $\wp$-component of $V_p A$.

Now we must find the lattices in V_pA invariant under $W[F, V]$ and also under R_p. But R_p is the direct sum $\bigoplus R_\wp$ of the maximal orders in $E_\wp$, and in particular it contains the projections onto components. Hence any invariant lattice is a sum of invariant components. We may therefore restrict to a single component, and later multiply together the number of classes in each.

Since L is unramified, $W \otimes R_\wp$ is the maximal order in $L \otimes E_\wp$, and so in $\bigoplus LE_\wp$ goes onto $\bigoplus \mathcal{O}_\wp$, the sum of the maximal orders. Thus any lattice in $\bigoplus LE_\wp$ invariant under W and $R_\wp$ is a $\bigoplus \mathcal{O}_\wp$-module, i. e. a fractional ideal in each summand. It thus has the form $(\bigoplus \mathcal{O}_\wp)$ $\langle t^{\varepsilon_1}, t^{\varepsilon_2}, \ldots, t^{\varepsilon_g} \rangle$, where t is a uniformizer of $LE_\wp$. We can choose t to lie in $E_\wp$ and so be invariant under τ.

It is easy to write out the condition that the lattice be invariant under F and V. We have

$$F \langle t^{\varepsilon_1} \ldots t^{\varepsilon_g} \rangle = \langle t^{\varepsilon_2} \ldots t^{\varepsilon_g}, \alpha t^{\varepsilon_1} \rangle.$$

This must lie in the lattice, giving the conditions

$$\varepsilon_1 \leqq \varepsilon_2 \leqq \varepsilon_3 \leqq \ldots \leqq \varepsilon_g \leqq \varepsilon_1 + \operatorname{ord} \alpha.$$

We note

$$\operatorname{ord} \alpha = \frac{\operatorname{ord} \pi}{|LE_\wp : E_\wp|} = \frac{g_\wp \operatorname{ord}_\wp \pi}{a}.$$

Similarly, since $V = pF^{-1}$, we get

$$V \langle t^{\varepsilon_1} \ldots t^{\varepsilon_g} \rangle = \left\langle \tau^{-1} \frac{1}{\alpha} p t^{\varepsilon_g}, p t^{\varepsilon_1}, \ldots, p t^{\varepsilon_{g-1}} \right\rangle,$$

giving the conditions

$$\varepsilon_\wp + \varepsilon_1 \geqq \varepsilon_2, \qquad e_\wp + \varepsilon_2 \geqq \varepsilon_3, \qquad \ldots, \qquad e_\wp + \varepsilon_{g-1} \geqq \varepsilon_g,$$
$$e_\wp + \varepsilon_g - \operatorname{ord} \alpha \geqq \varepsilon_1;$$

here we have used $\operatorname{ord} p = e_\wp$, $\operatorname{ord} \tau^{-1} \frac{1}{\alpha} = - \operatorname{ord} \alpha$.

The conditions become simpler if we introduce integers

$$n_1 = \varepsilon_2 - \varepsilon_1, \qquad n_2 = \varepsilon_3 - \varepsilon_2, \qquad \ldots, \qquad n_{g-1} = \varepsilon_g - \varepsilon_{g-1},$$
$$n_g = \frac{g_\wp \operatorname{ord}_\wp \pi}{a} - n_1 - n_2 - \ldots - n_{g-1}.$$

We then have simply

$$0 \leqq n_i \leqq e_\wp,$$
$$\sum n_i = \frac{g_\wp \operatorname{ord}_\wp \pi}{a}.$$

Two lattices can be taken to each other by scalars from $R_\wp$ if and only if the corresponding ε_i all differ by the same constant, since $R_\wp$ acts diagonally on $\bigoplus LE_\wp$. This difference is precisely what drops out when we pass to the n_i, so we have now computed the number of orbits.

Finally suppose we can get from A to another variety by separable isogeny. On the lattices this does something (it matters not what) at $l \neq p$ and replaces $T_p A$ by a lattice differing from it only in the étale components. Now on an étale component F is invertible, so $\pi = F^a$ is a unit and $\operatorname{ord}_\nu \pi = 0$. Hence $N_\nu = 1$ and all lattices in that component are in the same orbit. Thus A is changed only to a variety in the same orbit of the class group. ▌

Without exploring in any detail the behavior of the N_ν, we can at least make one observation. If $\operatorname{ord} \pi = 0$, $\operatorname{ord} \pi = ae_\nu = \operatorname{ord} q$, or $g_\nu = 1$, we have $N_\nu = 1$; and it is easy to see that these are the only cases for which $N_\nu = 1$. Now pass to the extension of k with degree s, assuming that E stays unchanged. Then f_ν and e_ν stay the same, but a is replaced by sa and hence g_ν may increase. If we assume that E is the endomorphism algebra over $\bar{k}$, then eventually $g_\nu = f_\nu$. Thus the number of orbits remains equal to 1 if and only if, for every ν, either π is a unit, $q\pi^{-1}$ is a unit, or E_ν is totally ramified over $\mathbf{Q}_p$.

At this point the reader clearly deserves an example of a case with more than one orbit. Here is one having 9 orbits; all of its endomorphisms are defined over k.

Example. — Consider $x^3 - 3x - 1$. Mod 2 this is $x^3 + x + 1$, which gives the cubic extension of $\mathbf{F}_2$. Hence it is irreducible over $\mathbf{Q}_2$, and a root of it gives the cubic unramified extension of $\mathbf{Q}_2$. It is *a fortiori* irreducible over $\mathbf{Q}$. Solving by the usual formula we find that it has the three real roots $2 \cos \frac{\pi}{18}$, $2 \cos \frac{7\pi}{18}$, $2 \cos \frac{13\pi}{18}$. All three are less than 2 in absolute value.

Let β be 2 times a root of this equation. As the extension at $\mathbf{Q}_2$ is unramified, there is a single valuation over 2 in $\mathbf{Q}(\beta)$, and $\operatorname{ord} 2 = \operatorname{ord} \beta = 1$. All absolute values of conjugates of β are $< 4 < 2\sqrt{8}$. Thus if we let π be a root of $\pi^2 - \beta\pi + 8 = 0$, π will be a Weil number corresponding to an isogeny class of abelian varieties over $\mathbf{F}_8$. We have $\beta^3 - 12\beta - 8 = 0$, so the minimal equation for π over $\mathbf{Q}$ is

$$P(X) = X^6 + 21X^4 - X^3 + 168X^2 + 8^3.$$

Over $\mathbf{Q}_2(\beta)$ the equation $\pi^2 - \beta\pi + 8$ must factor; for otherwise its two conjugate roots would have the same order, which is clearly impossible since their sum β has order 1. In fact, its roots π, $\bar{\pi}$ must satisfy $\operatorname{ord} \pi = 1$, $\operatorname{ord} \bar{\pi} = 2$. In other words, there are two valuations on $\mathbf{Q}(\pi)$ over 2, with $\operatorname{ord}_1 \pi = 1$, $\operatorname{ord}_2 \pi = 2$. Then $\mathbf{Q}(\pi) \otimes \mathbf{Q}_2$ splits into two copies of $\mathbf{Q}_2(\beta)$, each giving $e_\nu = 1$ and $f_\nu = 3$. There are no real primes, and at the two valuations over 2 we have $a = 3$ dividing $f_\nu \operatorname{ord}_\nu \pi = 3 \operatorname{ord}_\nu \pi$. Therefore E is commutative, $E = \mathbf{Q}(\pi)$.

We have $g_\wp = (a, f_\wp) = 3$ for both $\wp$. At $\wp_1$ we have $\frac{g_\wp \operatorname{ord}_\wp \pi}{a} = 1$, so $N_\wp$ is the number of solutions of $0 \leqq n_1, n_2, n_3 \leqq 1$, $\Sigma n_i = 1$; thus $N_\wp = 3$. For $\wp_2$ we have $\frac{g_\wp \operatorname{ord}_\wp \pi}{a} = 2$, and again $N_\wp = 3$. (It is easy to see in general that π and $\bar{\pi} = q/\pi$ will give the same N.) Thus there are 9 orbits for the class group.

Finally we must show that no base field extension can change E; equivalently, no power of π can fall into a proper subfield of $\mathbf{Q}(\pi)$. Now the subfields of $\mathbf{Q}(\pi)$ are $\mathbf{Q}$, the unique $\mathbf{Q}(\beta)$ of degree 3, and possibly a quadratic extension of $\mathbf{Q}$. The powers of π have different valuations at $\wp_1$ and $\wp_2$, so they can never lie in the field $\mathbf{Q}(\beta)$ which has a unique valuation over 2. We can finish things off then by proving simply that $\mathbf{Q}(\pi)$ does not have a quadratic subfield.

Suppose to the contrary $\mathbf{Q}(\sqrt{m}) \subseteq \mathbf{Q}(\pi)$. Then $\mathbf{Q}(\pi) = \mathbf{Q}(\beta, \sqrt{m})$, so $X^2 - \beta X + 8$ has a root

$$\alpha_0 + \alpha_1 \sqrt{m}, \qquad \alpha_i \in \mathbf{Q}(\beta), \qquad \alpha_1 \neq 0.$$

This means

$$2\alpha_0\alpha_1 - \beta\alpha_1 = 0,$$
$$\alpha_0^2 + m\alpha_1^2 - \beta\alpha_0 + 8 = 0,$$

which reduces to

$$\beta^2 - 32 = n\alpha_1^2$$

with $n = 4m$. Writing $\alpha_1 = b + c\beta + d\beta^2$ and recalling $\beta^3 = 12\beta + 8$, we get

$$n(b^2 + 16cd) = -32,$$
$$n(8d^2 + 2bc + 24cd) = 0,$$
$$n(c^2 + 12d^2 + 2bd) = 1,$$

which give us

$$4d^2 + bc + 12cd = 0,$$
$$0 \neq b^2 + 16cd = -32(c^2 + 12d^2 + 2bd).$$

The second of these is impossible if $d = 0$, so $d \neq 0$; by homogeneity we may set $d = 1$. Then $c(b + 12) = -4$, so $u = b + 12 \neq 0$. Solving for b and c in terms of u, we get

$$u^4 + 40u^3 - 240u^2 - 64u + 512 = 0.$$

Any root of this would be $\pm 2^r$, $r \leqq 9$; in fact $r \leqq 3$ because otherwise all terms but 512 are divisible by 2^{10}. The only solution mod 7 is $u \equiv 3$, so $u = -4$ is the only possibility, and it is not a root. Thus the supposition is untenable, and there is no quadratic subfield.

One consequence of Theorem 5.1 is that on principal varieties, separable isogeny is an equivalence relation. This, however, is true in general.

THEOREM 5.2. — *For abelian varieties over a finite field, separable isogeny is an equivalence relation.*

Proof. — Let $\varphi : A \to B$ be a separable isogeny, with $\ker\varphi$ the finite étale subgroup G. We must prove there is a separable isogeny $B \to A$. If $n = \operatorname{rank} G$ is prime to p, G is contained in $\ker(n.1_A)$, and there is a $\psi : B \to A$ with $\psi . \varphi = n$; since $n.1_A$ is separable, ψ is also. In general we can divide A by the direct factor of G of order prime to p, and the result will be a variety having a separable isogeny to A. Replacing A by this, we may assume G is an étale p-power group.

Since G has Dieudonné module T_pA/φ_pT_pB, φ_pT_pB contains all of $(T_pA)^0$. Let $p^r = \operatorname{rank} G$, and let G_1 be the kernel of p^r on $A(p)^{et}$, i. e. all points in $A(\bar{k})$ killed by p^r. Then $G \subseteq G_1$, so the map $\rho : A \to A/G_1$ factors as $\psi\varphi$, $\psi : B \to A/G_1$ separable.

We have now $\rho_pT_p(A/G_1) = p^rT_p(A)^{et} \oplus T_p(A)^0$. Clearly this is isomorphic as an $\mathfrak{A}$-module to $T_p(A)$. That is, $\operatorname{Hom}_{\mathfrak{A}}(T_pA/G_1, T_pA)$ contains an isomorphism. The set of isomorphisms then is open and so contains an element τ from $\operatorname{Hom}(A, A/G_1)$. Then $\tau : A \to A/G_1$ is an isogeny with τ_p an isomorphism, whence $\deg\tau$ is prime to p. By the earlier argument there is a separable isogeny $A/G_1 \to A$, and we compose it with ψ. ▎

I am told that Shimura has a counterexample to this statement when k is not finite.

The methods of Theorem 5.1 can be used in other situations, limited only by the reader's patience in calculating lattices. As an example, we prove a result recently derived by Shimura using other methods.

THEOREM 5.3. — *Let* A *be an elementary abelian variety with* E *commutative. Let* K *be the totally real subfield of index* 2 *in* E, *and assume that* p *splits completely in* K. *Assume also that* $R = i_A^{-1}(\operatorname{End} A)$ *contains the maximal order of* K. *Then :*

1. R_p *is maximal;*

2. *The class group of* R *operates freely on the isomorphism classes with order* R*; there are* 2^s *orbits, where* s *is the number of prime factors of* p *in* K *staying prime in* E*;*

3. *Two classes are in the same orbit if and only if there is a separable isogeny between them.*

Proof. — Here, as for elliptic curves, any rank 1 R-module with order R is invertible; this is easy to prove directly, and is also a special case of a theorem in [4]. Thus it makes sense to talk about the class group. Also, every ideal I has its localizations at $l \neq p$ determined, and every lattice away from p can be obtained from an ideal. What we will do is look closely at the invariant lattices at p and deduce that R_p is the maximal order. All the results will then follow from the argument of Theorem 5.1.

We group together the valuations ν over p having the same restriction νK to K. If νK ramifies or is undecomposed, so there is a unique ν over it, then $\pi\pi' = q = p^a$ gives $\mathrm{ord}_\nu \pi = \frac{a}{2} \mathrm{ord}_\nu p$. If νK ramifies this is a; if νK is undecomposed it is $\frac{a}{2}$ (and a is even). If νK splits into ν and ν', then $\mathrm{ord}_\nu \pi + \mathrm{ord}_{\nu'} \pi = a$. As E is commutative, $a \mid f_\nu \mathrm{ord}_\nu \pi$. This is automatic in the first two cases, but in the third (since $f_\nu = f_{\nu'} = 1$) it gives $\mathrm{ord}_\nu \pi = a$, $\mathrm{ord}_{\nu'} \pi = 0$.

Inside $L \otimes E_p = L \otimes (\oplus E_\nu)$ is the subalgebra $L \otimes (\oplus K_{\nu K})$. Group together $E_\nu \oplus E_{\nu'}$ if $\nu K = \nu' K$, so that there is the same number of summands in each. Since R contains the maximal order of K, R_p contains the projections on these summands, and an invariant lattice is a sum of invariant parts. Hence we can restrict ourselves to a single νK.

We have in all cases $K_{\nu K} = \mathbf{Q}_p$, and thus $L \otimes K_{\nu K} = L$. Suppose first E_ν is an unramified extension. Then $\mathrm{ord}_\nu \pi = \frac{a}{2}$, a is even, and $L \otimes E_\nu \simeq L \oplus L$. As before there is an $\alpha \in W$ with norm π in $E_\nu \subseteq L$, and $\mathrm{ord}_\nu \alpha = 1$. We set $u = \langle 1, \alpha \rangle$, $F = u\sigma$. Suppose now we have a W-lattice invariant under F and V. As a W-lattice it has a basis $(p^n, 0)$, (μ, p^m) with $\mu = 0$ or $\mathrm{ord}\,\mu < n$. If $F(p^n, 0)$ is in the lattice, then

$$(0, \alpha p^n) = (\gamma p^n; 0) + (\delta\mu, \delta^\sigma p^m) \qquad \text{for some} \quad \gamma, \delta \in W;$$

this gives us $m \leqq n + 1$ and $\mathrm{ord}\,\mu \geqq m - 1$. If

$$F(\mu, p^m) \equiv (p^m, \alpha\mu^\sigma) = (\gamma p^n, 0) + (\delta\mu, \delta^\sigma p^m),$$

we get

$$\mathrm{ord}\,\delta = 1 + \mathrm{ord}\,\mu - m \qquad \text{and then} \qquad m \geqq \min\{1 + 2\,\mathrm{ord}\,\mu - m, n\}$$

with equality if the first is smaller. If $\mathrm{ord}\,\mu < m$ the first is $\leqq m - 1$, impossible since $n \geqq m$. Thus $\mathrm{ord}\,\mu \geqq m$, so the first is $\geqq m$, whence $m \geqq n$. Hence $n = m \leqq \mathrm{ord}\,\mu$, $\mu = 0$, and the lattice basis is $(p^n, 0)$, $(0, p^n)$. This clearly is invariant under the full maximal order of E_ν.

Suppose next E_ν is ramified. Then $L \otimes E_\nu = LE_\nu$, a field. Choose α in it with $N\alpha = \pi$, whence $\mathrm{ord}_\nu \alpha = 1$. Choose c in E_ν Eisenstein, i. e.

$$c^2 = r_1 c + r_2, \qquad \text{with} \quad p \mid r_1, p \mid r_2, p^2 \mid r_2,$$

so $\mathrm{ord}\,c = 1$ and c generates the maximal order of E_ν over $\mathbf{Z}_p$. Let $\alpha = d + bc$, d, $b \in L$; then $\mathrm{ord}_L b = 0$, $\mathrm{ord}_L d > 0$. Any W-lattice in LE_ν has a basis of the form p^n, $\mu + p^m c$ with $\mu \in L$, $\mu = 0$ or $\mathrm{ord}_L \mu < n$. Suppose $Fp^n = \alpha p^n = dp^n + bp^n c$ is in the lattice; that gives $n \geqq m$ and $\mathrm{ord}_L \mu \geqq m$. We may divide by p^m and assume $m = 0$.

$$F(\mu + c) = (d\mu^\sigma + br_2) + (d + b\mu^\sigma + br_1)c;$$

suppose this is $\gamma p^n + \delta\mu + \delta c$. Then $\delta = d + b\mu^\sigma + br_1$, and the other terms must give $d\mu^\sigma + br_2$. If $\mathrm{ord}_L \mu = 0$, then $\mathrm{ord}_L \delta = 0$; but $\mathrm{ord}(d\mu^\sigma + br_2) > 0$, so $\mathrm{ord}(\gamma p^n) = 0$, $n = 0$, $\mu = 0$ and we have the basis $1, c$. If $\mathrm{ord}_L \mu > 0$, then $\mathrm{ord}_L(d\mu^\sigma + br_2) = 1$. Hence $\mathrm{ord}_L \delta\mu \geqq 2$, so $n \leqq 1$. Again $\mu = 0$. We have thus the lattices $1, c$ and p, c; these are taken to themselves by c, and so by the entire maximal order.

Suppose finally E splits over $K_{\nu K}$. We have

$$L \otimes (E_\nu \oplus E_{\nu'}) = L \oplus L, \qquad \text{with} \quad \alpha_1 \in E_\nu,\ \alpha_2 \in E_{\nu'}$$

satisfying $N\alpha_i = \pi$. Here $\mathrm{ord}\,\alpha_1 = 1$, $\mathrm{ord}\,\alpha_2 = 0$. $F = (\alpha, \alpha)(\sigma, \sigma)$. A W-lattice again has the form $(p^n, 0)$, (μ, p^m) with $\mu = 0$ or $\mathrm{ord}\,\mu < n$. Now

$$F(\mu, p^m) = (\alpha_1 \mu^\sigma, \alpha_2 p^m);$$

for this to be in the lattice we need $p^n \mid \alpha_1 \mu^\sigma - \alpha_2 \mu$. This implies $p^n \mid \mu$, and we are through. ❙

Remarks. — 1. With E as in the above theorem, any order R containing π and the maximal order of K actually occurs as an endomorphism ring : *cf.* Porism 4.3.

2. The theorem fails without the hypothesis on the splitting of p in K. Indeed, let E be the field of the Example (after 5.1). Carrying out the computation shows that

$$L \otimes E_p = L \otimes (L \oplus L) \simeq (L \oplus L) \oplus (L \oplus L) \oplus (L \oplus L)$$

contains a W-lattice with basis

$$(p, 0), (1, 1); \quad (p, 0), (0, p); \quad (p, 0), (0, p^2)$$

which is taken to itself by F and V and the maximal order of K_p but not by the maximal order of E_p.

CHAPTER 6.

Elementary Varieties over the Prime Field.

We assume throughout this chapter that our abelian varieties are elementary and are defined over the prime field $\mathbf{F}_p$.

Theorem 6.1. — *Assume* $\mathbf{Q}(\pi)$ *has no real prime. Then :*

1. E *is commutative;*

2. *All orders* R *in* E *containing* π *and* $p\pi^{-1}$ *are endomorphism rings;*

3. *For each such* R, *the isomorphism classes of isogenous varieties with endomorphism ring* R *correspond bijectively to the isomorphism classes of lattices in* E *with order* R.

Proof. — Since $a = 1$, $\frac{f_v \operatorname{ord}_v \pi}{a}$ is always an integer, and so $E = \Phi = \mathbf{Q}(\pi)$ is commutative. By Porism 4.3, we can get any order containing π at all $l \neq p$. But here $|\mathbf{Q}(\pi) : \mathbf{Q}| = 2g = \dim_{\mathbf{Q}_p} V_pA$, since $L = \mathbf{Q}_p$. Thus V_pA is free rank 1 over E_p, so at p we can again choose any lattice invariant under $F = \pi$ and $V = p\pi^{-1}$. Hence we get all the stated endomorphism rings.

Suppose now such an R is given. For all but finitely many l, R_l will be maximal, and so T_lA will be free rank 1 over it. At the other l, and at p, we can select a lattice free rank 1 over R_l; by an isogeny then we can get an A with T_pA and all T_lA free rank 1. For such an A clearly every ideal of R is a kernel ideal, and those giving varieties with endomorphism ring R are those whose order is precisely R. Once we note that every lattice with order R is isomorphic to an ideal of R, Theorem 3.11 completes the proof. ▎

Remarks. — 1. As in the similar situation in [21], it is necessary to pass to the special variety A in the proof. Lattices with order R need not be projective R-modules; in particular, one can find a lattice T and distinct ideals $I \subset J$ with $IT = JT$ (*cf.* [4]). This shows that for an appropriately chosen A, not all ideals are kernel ideals, and hence the property of being a kernel ideal depends on the variety chosen.

2. Inside the isogeny class and the class of varieties with order R there is a naturally defined subset : the varieties with T_pA and all T_lA free. From these and only these can we get all others as $A/H(I)$. They form a principal homogeneous space over the class group of R (isomorphism classes of invertible ideals). It would be interesting to know whether there are other special properties that they share.

For completeness we should discuss the case in which there is a real prime. As we know, $\Phi = \mathbf{Q}(\sqrt{p})$ and E is the quaternion algebra over Φ ramified only at the two real primes. Since $\sqrt{p}$ and $-\sqrt{p}$ are conjugate, there is only one isogeny class.

THEOREM 6.2. — *The class number of* E *equals the number of isomorphism classes with endomorphism ring a maximal order. If* $p \not\equiv 1 \bmod 4$, *these are all; if* $p \equiv 1 \bmod 4$ *there are others belonging to orders of index* 8 *and* 16.

Proof. — The prominence of 2 comes from the fact that the endomorphism ring must contain $\mathbf{Z}[\pi] = \mathbf{Z}[\sqrt{p}]$, which is the maximal order in Φ if $p \not\equiv 1 \bmod 4$ but has index 2 otherwise. For $p \equiv 1 \bmod 4$, then, we will have to look more carefully over $\mathbf{Q}_2$.

Suppose first we take an $l \neq p$ (and $l \neq 2$ if $p \equiv 1 \bmod 4$). If l stays prime or ramifies in Φ, then Φ_l is a field, and $\mathrm{E} \otimes \mathbf{Q}_l$ is $\mathrm{M}_2(\Phi_l)$ acting on a 2-dimensional Φ_l-space. The endomorphism ring contains $\sqrt{p}$ and so the whole maximal order of Φ_l, so the lattices we want are Φ_l-lattices. As with elliptic curves, the orders in $\mathrm{M}_2(\Phi_l)$ preserving them are maximal, and all the lattices are conjugate.

If l splits in Φ, then $\Phi_l = \mathbf{Q}_l \oplus \mathbf{Q}_l$ and E_l is $\mathrm{M}_2(\mathbf{Q}_l) \oplus \mathrm{M}_2(\mathbf{Q}_l)$ in its natural representation. Since we have the maximal order in Φ_l, we have projections on the summands, and any admissible lattice is a sum of admissible parts. Hence we get a maximal order in each $\mathrm{M}_2(\mathbf{Q}_l)$, i. e. a maximal order in E_l, and again we can pass from any lattice to any other.

At p we have a field Φ_p. Over $\mathrm{L} = \mathbf{Q}_p$, $\mathrm{V}_p\mathrm{A}$ is a 4-dimensional space, and $\mathcal{B}$ acts on it through an algebra central simple of degree 1; that is, $\mathcal{B}_p = \mathbf{Q}_p$. Thus $\mathrm{V}_p\mathrm{A}$ is a 2-dimensional Φ_p-space, and $\mathrm{E}_p = \mathrm{M}_2(\Phi_p)$. The argument then is just as for Φ_l.

This finishes the proof for $p \not\equiv 1 \bmod 4$. Suppose now $p \equiv 5 \bmod 8$, so 2 stays prime in Φ and $\mathrm{E}_2 = \mathrm{M}_2(\Phi_2)$. Let $t = \frac{1+\sqrt{p}}{2}$, so that $1, t$ are a $\mathbf{Z}_2$-basis of the maximal order in Φ_2. Let L be any $\mathbf{Z}_2$-lattice in $\mathrm{V}_2\mathrm{A}$, with basis v_1, v_2, v_3, v_4. It is easy to see that we can choose these with v_1, v_2 independent over Φ_2 and v_3, v_4 integral combinations over Φ_2. Subtracting multiples of v_1, v_2 we can then make v_3, v_4 into $\mathbf{Z}_2$-linear combinations of tv_1 and tv_2. Changing by unimodular $\mathbf{Z}_2$-matrices we may assume $v_3 = btv_1$, $v_4 = ctv_2$ with $b \mid c$. For this to be preserved by $\mathbf{Z}_2[\pi] = \mathbf{Z}_2 + 2t\mathbf{Z}_2$ we need $b \mid 2$, $c \mid 2$. Thus the possible lattices are

$$\{v_1, tv_1, v_2, tv_2\}, \quad \{v_1, tv_1, v_2, 2tv_2\} \quad \text{and} \quad \{v_1, 2tv_1, v_2, 2tv_2\}.$$

Writing the elements of E_2 as matrices in the basis v_1, v_2, we find that the first gives us a maximal order; the second, an order of index 8; and the third, an order of index 16.

Suppose finally $p \equiv 1 \bmod 8$, so $\Phi_2 = \mathbf{Q}_2 \oplus \mathbf{Q}_2$ and $\mathrm{E}_2 = \mathrm{M}_2(\mathbf{Q}_2) \oplus \mathrm{M}_2(\mathbf{Q}_2)$. If L is any $\mathbf{Z}_2$-lattice in $\mathbf{Q}_2^2 \oplus \mathbf{Q}_2^2$, we can choose a basis of four elements so that the first two lie in the first summand. Conjugating by an element of E_2 to change basis in each summand, we may assume the basis is of the form

$$(1, 0, 0, 0), \quad (0, 1, 0, 0), \quad (a, b, 1, 0), \quad (c, d, 0, 1).$$

This must be preserved by $(\sqrt{p}, -\sqrt{p})$ in $\mathbf{Q}_2 \oplus \mathbf{Q}_2$, or (equivalently) by $(2\sqrt{p}, 0)$, which means that $2a$, $2b$, $2c$, $2d \in \mathbf{Z}_2$. Since we can change a, b, c, d by elements of $\mathbf{Z}_2$ and can permute the basis elements in each summand, we see that every lattice is similar to one of the following :

$$\begin{array}{cccc}
(1, 0, 0, 0), & (0, 1, 0, 0), & (0, 0, 1, 0), & (0, 0, 0, 1), \\
\text{»}\quad , & \text{»}\quad , & \left(\frac{1}{2}, 0, 1, 0\right), & (0, 0, 0, 1), \\
\text{»}\quad , & \text{»}\quad , & \left(\frac{1}{2}, \frac{1}{2}, 1, 0\right), & (0, 0, 0, 1), \\
\text{»}\quad , & \text{»}\quad , & \left(\frac{1}{2}, 0, 1, 0\right), & \left(\frac{1}{2}, 0, 0, 1\right), \\
\text{»}\quad , & \text{»}\quad , & \left(\frac{1}{2}, \frac{1}{2}, 1, 0\right), & \left(\frac{1}{2}, 0, 0, 1\right), \\
\text{»}\quad , & \text{»}\quad , & \left(0, \frac{1}{2}, 1, 0\right), & \left(\frac{1}{2}, 0, 0, 1\right), \\
\text{»}\quad , & \text{»}\quad , & \left(\frac{1}{2}, \frac{1}{2}, 1, 0\right), & \left(\frac{1}{2}, \frac{1}{2}, 0, 1\right).
\end{array}$$

The first of these gives a maximal order; the others, orders of index 8 and 16. ▌

The class number of E is investigated in [7].

CHAPTER 7.

ORDINARY ELEMENTARY VARIETIES.

PROPOSITION 7.1. — *Let* π *be the Weil number of an isogeny class of elementary varieties. Then the varieties are ordinary if and only if there are no real primes and, in the notation of Chapter* 2, $(p, \beta) = 1$.

Proof. — There are no real primes, since they give either supersingular elliptic curves or twisted products thereof. If $(p, \beta) = 1$, then over any $\mathbf{Q}_p(\beta)$ the equation $X^2 - \beta X + q = 0$ must split with roots of orders 0 and $\operatorname{ord} q$. Hence half the places have $\operatorname{ord}_v \pi = 0$, so π and hence F are units on $V_v A$ and the summand is étale. Conversely, if $A(p)$ is half étale, this argument will show $\operatorname{ord}_v \beta = 0$ for all v and so $(p, \beta) = 1$. ▌

We assume from now on that, unless otherwise stated, our abelian varieties are elementary and ordinary.

THEOREM 7.2. — End A *is commutative, and is unchanged by base field extension. The principal varieties in an isogeny class are a principal homogeneous space for the ideal class group.*

Proof. — We have seen that there are no real primes, and that $\operatorname{ord}_v \pi$ is 0 or $\operatorname{ord} q$ at every v. Hence $\| \pi \|_v = q^{-i_v}$ for an integer i_v, and End A is commutative. The same is true after base field extension, so by dimension count E and hence End A are unchanged. The final statement follows from Theorem 5.1 and the comments following it. ❙

The major result of this chapter is that for ordinary elementary varieties, all conceivable endomorphism rings actually occur. We first need a result of some interest in itself :

PROPOSITION 7.3. — *Let* R *be a local ring which is a finitely generated free* $\mathbf{Z}_p$*-module. Let* W *be the ring of integers in the unramified extension* L *of* $\mathbf{Q}_p$ *with degree* a, *and set* $S = W \otimes R$. *Then if* α *is a unit in* R, *it is the norm of an element in* S.

Proof. — Let $e_1, \ldots, e_a$ be a basis of S over R giving a basis of $S/\mathfrak{p}S$ over $K = R/\mathfrak{p}R$, where $\mathfrak{p}$ is the maximal ideal of R. (For example, we can take $e_i = \zeta^{p^{i-1}}$, where $\zeta^{p^a} = 1$.) Consider the norm form

$$F(X_1, \ldots, X_a) = N(\Sigma X_i e_i) = \prod_{\sigma_j} (\Sigma X_i \sigma_j(e_i)),$$

which maps S into R. Since R is complete, we can apply Hensel's lemma if we show that $\overline{F}(X_1, \ldots, X_a) = \overline{\alpha}$ has a simple root in K^a.

Now $\overline{F}$ is the norm form from $S/\mathfrak{p}S$, which maps onto K because K is finite and $S/\mathfrak{p}S$ is separable over K. Thus it assumes the value $\overline{\alpha} \neq 0$; I claim now that all roots x of $NX = \overline{\alpha}$ are simple. Indeed, x is invertible since $Nx \neq 0$, and the derivative of $Nx = \prod \sigma_i x$ along $\overline{e}_i$ is

$$\Sigma \sigma_i(\overline{e}_i) \prod_{j \neq i} \sigma_j(x) = \mathrm{Tr}\frac{\overline{e}_i}{x} N(x).$$

Here for some i, $\mathrm{Tr}\frac{\overline{e}_i}{x} \neq 0$, since the extension is separable. Thus Hensel's lemma applies. ❙

THEOREM 7.4. — *The possible endomorphism rings are precisely those orders in* $E = \Phi$ *which contain* π *and* $q\pi^{-1}$.

Proof. — We know by Porism 4.3 that we only need to consider the situation at p. There we must study the orders in $E_p = \oplus E_v$. If R is one, let $m_v(R) = \{x \in R \mid \mathrm{ord}_v x > 0\}$; clearly these all are ideals of R. I claim they are maximal. Indeed, suppose $y \in R$, $y \notin m_1(R)$. Write $y = \langle y_1, \ldots \rangle$, so y_1 is a unit in E_1. Taking its characteristic polynomial and noting that its constant term is the unit Ny_1, we see that $\frac{1}{y_1}$ is a polynomial in y_1 with $\mathbf{Z}_p$-coefficients. Taking that same polynomial in y gives us an element of yR of the form $\left\langle \frac{1}{y_1}, \ldots \right\rangle$, and multiplying gives $\langle 1, \ldots \rangle \in yR$.

Now let $\mathcal{O}_v$ be the maximal order in E_v, so $\bigoplus \mathcal{O}_v$ is the maximal order in E_p. As R is an order, we have $p^n(\bigoplus \mathcal{O}_v) \subseteq R$ for n large enough. Take then the element $\langle 1, \ldots \rangle$ in $yR + m_1(R)$ and raise it to a high power; those entries which were units stay units, and the others increase steadily in ord. Eventually the others then are all in $m_1(R)$, so we can subtract them off and get an element whose entries are all units and zeros. The same argument as before with characteristic polynomials gives us then an element in $yR + m_1(R)$ of the form $\langle 1 \ldots 1, 0 \ldots 0 \rangle$. Since $1 \in R$, $\langle 0 \ldots 0, 1 \ldots 1 \rangle$ is in R and so in $m_1(R)$. Adding gives $1 \in yR + m_1(R)$, and thus $m_1(R)$ is maximal.

This argument shows also that an element not in any $m_v(R)$ is invertible, so they are the only maximal ideals. The topology defined by the radical $\bigcap m_v(R)$ is the p-adic topology, so R is semi-local and complete. Hence it is a composite of finitely many local rings, one for each maximal ideal. This does *not* mean that there is one summand for each E_v, since some of the $m_v(R)$ may coincide; but it does give enough structure to allow us to prove the theorem.

Assume that R contains π and $q\pi^{-1}$. We will define an action of F on $L \otimes E_p$ for which $W \otimes R$ is invariant under F and V. As $W \otimes R$ is a subring, those elements of $1 \otimes E_p$ taking it to itself are just those lying in it, i. e. R; this will complete the proof.

As we saw, R is a sum of certain local rings $\bigoplus R_j$. We know that in each E_v either π or $\frac{\pi}{q}$ is a unit, since the varieties are ordinary. The same is true in each R_j, since the maximal ideals of the R_j are given by the valuations. Then the image π_j of π in R_j is a norm from $W \otimes R_j$; this is clear from the proposition if π_j is a unit, and holds if $\frac{\pi_j}{q}$ is a unit because $q = p^a = Np$. Adding together the elements in the various $W \otimes R_j$ whose norms are π_j, we find an element $u \in W \otimes (\bigoplus R_j) = W \otimes R$ whose norm is π. Note that at every j the element we take is either a unit or p times a unit; the argument given before shows that if a unit is in an order so is its inverse, and therefore we have $pu^{-1} \in W \otimes R$.

Finally, we let F act on $L \otimes E$ by $F = u\sigma$. As in Theorem 5.1, this gives the correct algebra representation. Since σ operates only on the L factor, it preserves W and so also $W \otimes R$. The ring $W \otimes R$ contains u, so u preserves it, and $W \otimes R$ is invariant under F. The same argument shows it is invariant under $V = pF^{-1} = \sigma^{-1}pu^{-1}$, and we are done. ▎

Example. — The theorem may fail for non-ordinary varieties, even if E is commutative and stable under base field extension.

Indeed, let $\beta = 6 + \sqrt{29}$, in $\mathbf{Q}(\sqrt{29})$. Then $|\beta| < 2.7$, so $\pi^2 - \beta\pi + 49 = 0$ gives a Weil number π.

In $\mathbf{Q}(\sqrt{29})$, $7 = (6+\sqrt{29})(6-\sqrt{29})$; there are two valuations over 7, giving $\mathrm{ord}_1 \beta = 1$, $\mathrm{ord}_2 \beta = 0$. At ord_2 the equation $X^2 - \beta X + 49 = 0$ splits in $\mathbf{Q}_7$, giving $\mathrm{ord}_{21} \pi = 0$, $\mathrm{ord}_{22} \pi = 2$. Both of these are divisible by $a = 2$, so the condition for commutativity holds here.

At ord_1 we have $7 \mid \beta$ in $\mathbf{Q}_7$, so $\sqrt{29} \equiv 1 \bmod 7$. Then

$$\frac{7}{\beta} = 6 - \sqrt{29} \equiv 5 \bmod 7, \qquad \text{so} \quad \frac{\beta}{7} \equiv \frac{1}{5} \equiv 3 \bmod 7 \quad \text{in } \mathbf{Z}_7.$$

The equation $X^2 - \beta X + 49 = 0$ has solution $X = 7Y$, where

$$Y^2 - \frac{\beta}{7} Y + 1 = 0.$$

Mod 7 this is $Y^2 - 3Y + 1 = 0$, which has no solution mod 7. Thus Y generates the unramified quadratic extension of $\mathbf{Q}_7$, and $\pi = 7Y$ has $\mathrm{ord}_1 \pi = 1$ for the unique valuation over ord_1. Here the commutativity condition is also satisfied, so $E = \Phi$.

To show stability we must show that no power of π falls into a proper subfield. Now consideration of ord_2 shows that no power can lie in $\mathbf{Q}(\beta)$, and the only possibility is that some power is in a different quadratic subfield. But a direct computation like that after 5.1 shows that there are no other quadratic subfields.

Now Theorem 5.3 applies, and any endomorphism ring containing the maximal order $\mathbf{Z}\left(\frac{1+\sqrt{29}}{2}\right)$ of $\mathbf{Q}(\beta)$ must be maximal at 7. As 7 is not ramified in $\mathbf{Q}(\pi)$, this means the discriminant of any such endomorphism ring must be prime to 7. But the discriminant of $\mathbf{Z}\left(\pi, \frac{1+\sqrt{29}}{2}\right)$ over $\mathbf{Z}\left(\frac{1+\sqrt{29}}{2}\right)$ is $\beta^2 - 4.49$, which is not prime to 7; hence the discriminant over $\mathbf{Z}$ is not prime to 7. Thus $\mathbf{Z}\left(\pi, \frac{1+\sqrt{29}}{2}\right)$ is an order containing π and $\frac{49}{\pi} = \beta - \pi$ which is not an endomorphism ring.

We should mention an additional nice property of ordinary varieties, one which (in a sense) is already in the literature [11] : such varieties have canonical liftings to characteristic 0.

Finally, lest the reader in his enthusiasm overdraw the analogy with elliptic curves, it should be pointed out that End A need not be maximal at p. For an example, let $\beta = 1 + 2\sqrt{2}$, defining a Weil number π over $\mathbf{F}_8$. Here $(\beta, 2) = 1$, so the varieties are ordinary, but

$$\mathbf{Z}[\pi, 8/\pi] \cap \mathbf{Q}(\beta) = \mathbf{Z}[\beta] = \mathbf{Z}[2\sqrt{2}].$$

APPENDIX.

For elliptic curves, Serre [14], [15] has defined an action of ideals on varieties closely related to the definition of A/H (I) in Chapter 3. This appendix shows to what extent the two definitions can differ.

To be general for a moment, let R be a noetherian ring, G a commutative group scheme over a field k with R operating on G. Let M be a finitely generated left R-module. Then for every k-algebra B we have an abelian group $\mathrm{Hom}_R(M, G(B))$; clearly this gives a group functor. If $L \rightarrow M \rightarrow N \rightarrow 0$ is an exact sequence of R-modules, then for all B

$$0 \rightarrow \mathrm{Hom}_R(N, G(B)) \rightarrow \mathrm{Hom}_R(M, G(B)) \rightarrow \mathrm{Hom}_R(L, G(B))$$

is exact.

Proposition A.1. — $B \mapsto \mathrm{Hom}_R(M, G(B))$ *is a representable group functor.*

Proof. — An exact sequence $R^m \rightarrow R^n \rightarrow M \rightarrow 0$ gives for every B the exact sequence

$$0 \rightarrow \mathrm{Hom}_R(M, G(B)) \rightarrow G(B)^n \rightarrow G(B)^m.$$

Thus the functor in question is the functor kernel of $G^n \rightarrow G^m$, which is known to be representable by a commutative group scheme. |

We denote the group scheme so defined by $\mathrm{Hom}_R(M, G)$. Then clearly $M \mapsto \mathrm{Hom}_R(M, G)$ defines an additive functor from finitely generated left R-modules to commutative group schemes. It is left exact, its values are in an abelian category, and there are enough projective R-modules; hence by the usual process we may make the

Definition. — $\mathrm{Ext}_R^n(-, G)$ *are the derived functors of* $\mathrm{Hom}_R(-, G)$.

These again are additive functors from modules to group schemes, and a short exact sequence of modules gives a long exact sequence of group schemes. They have been introduced independently by Giraud [23].

This is not the place to study the behavior of these mixed (module, module scheme) Ext groups. We note only that a short exact sequence $0 \rightarrow F \rightarrow G \rightarrow H \rightarrow 0$ of commutative group schemes with R-operation gives a long exact sequence of Ext groups. Indeed, for that we need only the exactness of

$$0 \rightarrow \mathrm{Hom}_R(P, F) \rightarrow \mathrm{Hom}_R(P, G) \rightarrow \mathrm{Hom}_R(P, H) \rightarrow 0$$

for P a finitely generated projective, which follows by additivity from the trivial case $P = R$.

Returning now to our specific situation, let A be an abelian variety with $\operatorname{End} A = R$, and let I be a left ideal in R which is a lattice. Then

$$0 \to I \to R \to R/I \to 0$$

gives us

$$0 \to \operatorname{Hom}_R(R/I, A) \to A \to \operatorname{Hom}_R(I, A) \to \operatorname{Ext}^1_R(R/I, A) \to 0,$$

the last 0 coming because R is projective. If $\alpha_1, \ldots, \alpha_m$ span I as an R-module, then $R^m \to R \to R/I \to 0$ is the start of a resolution, and $\operatorname{Hom}_R(R/I, A)$ is by definition the kernel of $(\alpha_1, \ldots, \alpha_m) : A \to A^m$. Comparing with the definition in 3.2, we have

Proposition A.2. — $H(I) = \operatorname{Hom}_R(R/I, A)$. ▌

But $\operatorname{Hom}_R(I, A)$ need not equal $A/H(I)$; clearly it will if and only if $\operatorname{Ext}^1_R(R/I, A) = 0$. Having the Ext group, however, we can be a little more specific. Since R/I is finite and the functor is additive, $\operatorname{Ext}^1_R(R/I, A)$ is annihilated by some integer. By construction $\operatorname{Hom}_R(I, A)$ is a subgroup of an abelian variety, and so the only such quotients of it are finite. Noting finally that the image of A must be connected, we have

Proposition A.3. — $A/H(I)$ *is the connected component of* $\operatorname{Hom}_R(I, A)$; *the quotient of* $\operatorname{Hom}_R(I, A)$ *by its connected component is* $\operatorname{Ext}^1_R(R/I, A)$. ▌

Corollary A.4. — *If* I *is projective,* $A/H(I) = \operatorname{Hom}_R(I. A)$.

Proof. — In this case $\operatorname{Hom}_R(I, A)$ is a direct summand of some A^n, and hence is connected. ▌

In [14] and [15], Serre considered the case where A is an elliptic curve and I is an ideal whose order is R; there he used the $\operatorname{Hom}_R(I, A)$ definition. This, we now see, gave an abelian variety only because such an I is invertible and hence projective ([2], p. 148). The following example shows that in higher dimensions $\operatorname{Hom}_R(I, A)$ need not be connected, even in the classical case $k = \mathbf{C}$. (It therefore also shows, of course, the non-triviality of the Ext theory constructed above.)

Example. — Let α be $\left(-2 + \sqrt{2}\right)^{\frac{1}{2}}$, and let $F = \mathbf{Q}(\alpha)$. The field F is a totally complex quadratic extension of a totally real field; the equation for α is $\alpha^4 = -4\alpha^2 - 2$. Let R be the order spanned over $\mathbf{Z}$ by $\{1, 2\alpha, 2\alpha^2, 2\alpha^3\}$; then R is the order of the (non-invertible) module $M = \{1, \alpha, 2\alpha^2, 2\alpha^3\}$, and so also of the ideal $I = \{2, 2\alpha, 4\alpha^2, 4\alpha^3\}$.

As an R-module, I is spanned by 2 and 2α. The kernel of the map $(2, 2\alpha) : R \oplus R \to I$ is $\{(x, y) \mid x + \alpha y = 0\}$, which is isomorphic to the ideal $\{y \in R \mid \alpha y \in R\}$ spanned by $\{2, 2\alpha, 2\alpha^2, 2\alpha^3\}$. Thus we have an exact sequence $R^4 \to R^2 \to I \to 0$.

Define now $\varphi : \mathrm{F} \to \mathbf{C} \oplus \mathbf{C}$ by two non-conjugate embeddings. Since F has no imaginary subfields, $\mathrm{A} = \mathbf{C} \oplus \mathbf{C}/\varphi(\mathrm{M})$ is an abelian variety with endomorphism ring R, the R-operation being induced from multiplication by $\varphi(\mathrm{R})$ on $\mathbf{C} \oplus \mathbf{C}$ ([17], p. 45-46).

By definition $\mathrm{Hom}_{\mathrm{R}}(\mathrm{I}, \mathrm{A})$ is the kernel of the map $\mathrm{A}^2 \to \mathrm{A}^4$, i. e. the common kernel of the maps $\mathrm{A}^2 \to \mathrm{A}$ given by taking (x, y) to $2y - 2\alpha x$, $2\alpha y - 2\alpha^2 x$, $2\alpha^2 y - 2\alpha^3 x$, and $2\alpha^3 y - 2\alpha^4 x$. Suppose we write

$$x = u_0\,\varphi(1) + u_1\,\varphi(\alpha) + u_2\,\varphi(2\alpha^2) + u_3\,\varphi(2\alpha^3),$$
$$y = v_0\,\varphi(1) + v_1\,\varphi(\alpha) + v_2\,\varphi(2\alpha^2) + v_3\,\varphi(2\alpha^3),$$

so the u_i and v_i are reals mod 1. The condition that (x, y) go to 0 in A under all four maps is easily seen to be equivalent to a set of congruences mod 1, namely

$$2v_2 - u_1 + 8u_3 \equiv 0, \qquad 2v_3 - 2u_2 \equiv 0,$$
$$v_1 - u_0 \equiv 0, \qquad v_0 + 4u_3 \equiv 0.$$

The solution set of these has two components, corresponding to $v_3 \equiv u_2$ and $v_3 \equiv u_2 + \frac{1}{2}$.

REFERENCES.

[1] N. Bourbaki, *Algèbre*, chap. VIII, Hermann, Paris, 1958.

[2] N. Bourbaki, *Algèbre commutative*, chap. II, Hermann, Paris, 1961.

[3] J. W. S. Cassels, *Diophantine equations with special reference to elliptic curves* (*J. London Math. Soc.*, vol. 41, 1966, p. 193-291).

[4] E. C. Dade, O. Taussky and H. Zassenhaus, *On the theory of orders* (*Math. Ann.*, vol. 148, 1962, p. 31-64).

[5] M. Deuring, *Algebren* (*Ergeb. der Math.*, IV.1, Springer, Berlin, 1935).

[6] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper* (*Abh. Math. Sem. Hamburg*, Bd. 14, 1941, p. 197-272).

[7] M. Eichler, *Zur Zahlentheorie der Quaternionen-Algebren* (*J. Reine Angew. Math.*, Bd. 195, 1955, p. 127-151).

[8] T. Honda, *Isogeny classes of abelian varieties over finite fields* (*J. Math. Soc. Japan*, vol. 20, 1968, p. 83-95).

[9] Y. Ihara, *Hecke polynomials as congruence ζ functions in elliptic modular case* (*Ann. of Math.*, (2), vol. 85, 1967, p. 267-295).

[10] S. Lang, *Abelian Varieties*, Interscience, New York, 1959.

[11] J. Lubin, J.-P. Serre and J. Tate, *Elliptic curves and formal groups*; in *Lecture Notes*, Woods Hole Institute in Algebraic Geometry, privately printed, 1964.

[12] T. Oda, *The first de Rham cohomology group and Dieudonné modules* (*Ann. scient. Éc. Norm. Sup.*, (4), t. 2, 1969, p. 63-135).

[13] F. Oort, *Commutative Group Schemes* (*Lecture Notes in Math.*, 15, Springer, Berlin, 1966).

[14] J.-P. Serre, *Algèbre et géométrie*, Annuaire Coll. de France, Paris, 1965-1966, p. 45-49.

[15] J.-P. Serre, *Complex multiplication*; in J. W. S. Cassels and A. Fröhlich (eds.), *Algebraic Number Theory*, Academic Press, London, 1967.

[16] J.-P. Serre, *Groupes p-divisibles* (d'après J. Tate), Sém. Bourbaki, 318, 1966-1967.

[17] G. Shimura and Y. Taniyama, *Complex Multiplication of Abelian Varieties*, Publ. Math. Soc. Japan, 6, Tokyo, 1961.

[18] J. Tate, *Endomorphisms of abelian varieties over finite fields* (*Invent. Math.*, vol. 2, 1966, p. 134-144).

[19] J. Tate, *Endomorphisms of abelian varieties over finite fields.* II (*Invent. Math.*, to appear).

[20] J. Tate, *p-divisible groups*; in T. A. Springer (ed.), *Local Fields*, Springer, Berlin, 1967.

[21] W. Waterhouse, *A classification of almost full formal groups* (*Proc. Amer. Math. Soc.*, vol. 20, 1969, p. 426-428).

[22] A. Weil, *Variétés abéliennes et courbes algébriques*, Hermann, Paris, 1948.

[23] J. Giraud, *Remarque sur une formule de Shimura-Taniyama* (*Invent. Math.*, t. 5, 1968, p. 231-236).

[24] J. Tate, *Classes d'isogénie des variétés abéliennes sur un corps fini* (d'après T. Honda), Sém. Bourbaki, 358, 1968-1969.

(Manuscrit reçu le 24 mai 1969.)

W. C. Waterhouse,
Department of Mathematics,
Cornell University,
Ithaca (N. Y. 14850), U. S. A.