CHAPTER IV

Hom(X, X) AND THE l-ADIC REPRESENTATION

18. Etale coverings.

The main result is the following

THEOREM. (Serre-Lang.) *If X is an abelian variety, Y a variety and $f: Y \to X$ is an étale covering, then Y has a structure of abelian variety such that f becomes a separable isogeny.*

PROOF. Let Γ_m be the graph of the multiplication $m: X \times X \to X$ in $X \times X \times X$, and Γ' the inverse image in $Y \times Y \times Y$ of Γ_m by $f \times f \times f$. Since (1) $\Gamma' \to \Gamma_m$ is an étale covering, (2) $p_{12}: \Gamma_m \to X \times X$ is an isomorphism, (3) we have the commutative diagram

$$\begin{array}{ccc} \Gamma' & \longrightarrow & \Gamma_m \\ \downarrow{\scriptstyle p_{12}} & & \downarrow{\scriptstyle p_{12}} \\ Y \times Y & \xrightarrow[f \times f]{} & X \times X \end{array}$$

and (4) $f \times f$ is an étale covering, $p_{12}: \Gamma' \to Y \times Y$ is an étale covering too. Choose a point $y_0 \in Y$ such that $f(y_0) = 0$, and let Γ be the connected component of Γ' containing (y_0, y_0, y_0) (which belongs to Γ' since $f(y_0) = 0$ and $(0, 0, 0) \in \Gamma_m$). Then the restriction $p: \Gamma \to Y \times Y$ of p_{12} is again an étale covering, so that the degree of p equals the number of points of *any* fibre of p. We want to show that p is an isomorphism, or equivalently that there is one point of $Y \times Y$ whose inverse image in Γ is again a single point. Let $\sigma_1, \sigma_2: Y \to \Gamma$ be defined by $\sigma_1(y) = (y_0, y, y)$, $\sigma_2(y) = (y, y_0, y)$. (Since $\sigma_i(Y) \subset \Gamma'$ and $(y_0, y_0, y_0) \in \sigma_i(Y)$, it follows that $\sigma_i(Y) \subset \Gamma$.) Then the restriction of p to $\sigma_2(Y)$ is a bijection of $\sigma_2(Y)$ onto $Y \times \{y_0\}$. It therefore suffices to establish that $p^{-1}(Y \times \{y_0\}) = \sigma_2(Y)$, or equivalently that if $q: \Gamma \to Y$ is the restriction to Γ of $p_2: Y \times Y \times Y \to Y$, $q^{-1}(y_0) = \sigma_2(Y)$. Since $\sigma_2(Y)$ is an irreducible component of $q^{-1}(y_0)$, it suffices to show that $q^{-1}(y_0)$ is irreducible. Now, Γ is non-singular, being étale over $Y \times Y$ and hence $X \times X$,

and since it is also connected, it is irreducible. Further, the morphism $q\colon \Gamma \to Y$ is smooth, being the composite of the étale morphism $\Gamma \to Y \times Y$ and the projection $Y \times Y \xrightarrow{p_2} Y$. Finally $\sigma_1\colon Y \to \Gamma$ is a section for q. Now the assertion that $q^{-1}(y_0)$ is irreducible follows from the

LEMMA. *Let $f\colon X \to Y$ be a proper smooth morphism of irreducible varieties such that there is a section $\sigma\colon Y \to X$, $f \circ \sigma = 1_Y$. Then all fibres of f are irreducible.*

PROOF. We may assume $Y = \operatorname{Spec} A$ affine. Let $B = \Gamma(X, \mathcal{O}_X)$, so that B is an A-algebra which is a domain since X is irreducible and a finite A-module since f is proper. The morphism f factorises as $X \xrightarrow{g} \operatorname{Spec}(B) \xrightarrow{h} Y$ where $\operatorname{Spec}(B)$ is again an irreducible variety. But $g \circ \sigma$ is a section of h, and since $\dim(\operatorname{Spec} B) = \dim Y$, $g \circ \sigma$ is surjective, hence h is an isomorphism, and $A = B$.

Since f is smooth, its fibres are non-singular, and it suffices to show that they are connected. Let $0 \to K_0 \to K_1 \to \dots$ be a complex of free finitely generated A-modules giving the direct images of $\mathcal{O}_X$ universally, so that by the above, we have an exact sequence $0 \to A \to K_0 \to K_1$. Let y be any point of Y, $\mathfrak{M}$ its maximal ideal in A. Since completion with respect to the $\mathfrak{M}$-adic topology is an exact functor, we have an exact sequence $0 \to \hat{A} \to \hat{K}_0 \to \hat{K}_1$, so that $\hat{A} \simeq \varprojlim_n \operatorname{Ker}\left[\frac{K_0}{\mathfrak{M}^n K_0} \to \frac{K_1}{\mathfrak{M}^n K_1}\right]$. But now,

$$\operatorname{Ker}\left[\frac{K_0}{\mathfrak{M}^n K_0} \to \frac{K_1}{\mathfrak{M}^n K_1}\right] = H^0\left(f^{-1}(y), \mathcal{O}_X/\mathfrak{M}^n \mathcal{O}_X\right),$$

so the natural map $\hat{A} \xrightarrow{\sim} \varprojlim H^0(f^{-1}(y), \mathcal{O}_X/\mathfrak{M}^n\, \mathcal{O}_X)$ is a ring isomorphism. If $f^{-1}(y)$ were not connected, let $f^{-1}(y) = Z_1 \cup Z_2$, Z_i closed, $Z_1 \cap Z_2 = \emptyset$ and $Z_i \neq f^{-1}(y)$. We can find a unique $f_n \in H^0(f^{-1}(y), \mathcal{O}_X/\mathfrak{M}^n \mathcal{O}_X)$ which reduces to 1 on Z_1 and 0 on Z_2,

and $\{f_n\}$ defines an element $f \in \varprojlim H^0(\mathcal{O}_X/\mathfrak{M}^n\mathcal{O}_X) \simeq \hat{A}$ with $f^2 = f$, and $f \neq 0$ or 1. This is impossible since $\hat{A}$ is a local ring.

The lemma is proved.

Returning to the proof of the theorem, we have shown that $p_{12}\colon \Gamma \to Y \times Y$ is an isomorphism, so that $\nu = p_3 \circ p_{12}^{-1}\colon Y \times Y \to Y$ is a morphism. Since, as we saw, $\Gamma \supset \sigma_1(Y)$ and $\sigma_2(Y)$, it follows that $\nu(y, y_0) = y = \nu(y_0, y)$. Therefore, from the theorem proved in the Appendix to §4, Y is an abelian variety with composition law ν and zero element y_0. Since $f(y_0) = 0$, f is a homomorphism of abelian varieties.

REMARK. If X is an abelian variety and $f\colon Y \to X$ is an isogeny, then we can find an isogeny $g\colon X \to Y$ with $f \circ g = n_X$ for some $n > 0$. In fact, since $\ker f$ is a finite group scheme, it is killed by some integer $n > 0$, hence $\ker f \subseteq \ker(n_Y)$. Since $X \simeq Y/\ker f$, it follows that n_Y factorizes as $n_Y = g \circ f$ for a homomorphism $g\colon X \to Y$. But then $f \circ g = n_X$ too, since for all $x \in X$, $x = f(y)$ for some $y \in Y$, and therefore

$$f \circ g(x) = f(g(f(y))) = f(ny) = nf(y) = nx.$$

We can interpret our results in terms of the fundamental group $\pi_1(X)$. Recall, that if X is any non-singular variety, and $x_0 \in X$ is a base point, the group $\pi_1(X, x_0)$ is constructed as follows†: consider the set of all morphisms

$$\begin{array}{ccc} Y & \xrightarrow{\pi} & X \\ y_0 & \longmapsto & x_0 \end{array}$$

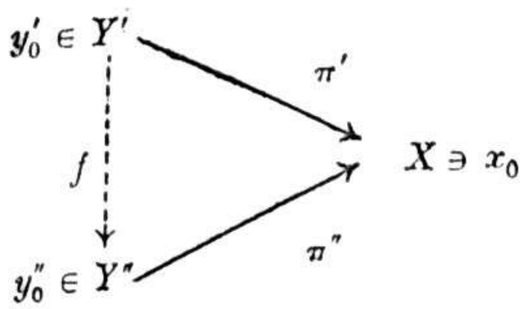
together with a base point $y_0 \in Y$ lying over x_0 such that

(1) a finite group G_Y acts freely on Y and $X \simeq Y/G_Y$ and

(2) Y is connected, hence Y is again a non-singular variety.

Given two such :

†For details, cf. [G2] pp. 60-61.



recall that there is at most one morphism $f\colon Y' \to Y''$ such that

(i) $\pi'' \circ f = \pi'$,

(ii) $f(y_0') = y_0''$.

When f exists, there is a unique surjective homomorphism

$$\rho\colon G_{Y'} \longrightarrow G_{Y''}$$

such that $f(\sigma \cdot y) = \rho(\sigma) \cdot f(y)$, all $\sigma \in G_{Y'}$, $y \in Y'$. We order the triples (Y, y_0, π) by saying $(Y', y_0', \pi') > (Y'', y_0'', \pi'')$ if such an f exists. Then the set of (Y, y_0, π)'s forms an inverse system, and we define

$$\pi_1(X, x_0) = \varprojlim_{(Y, y_0, \pi)} G_Y.$$

Now suppose X is an abelian variety and $x_0 = 0$. Then all such Y's are abelian varieties, and G_Y is just the kernel of π acting on Y by translations. In particular, we see that $\pi_1(X)$ is abelian. To describe it more explicitly, it is convenient to break it up into the product of its l-primary piece for different primes l. First suppose $l \neq p$. By the remark following the theorem, the set of étale coverings

$$X \xrightarrow{l_X^n} X$$

is cofinal in the set of all étale coverings

$$Y \xrightarrow{\pi} X, \#(\operatorname{Ker} \pi) = l^m, \text{ some } m.$$

Therefore, the l-adic component of $\pi_1(X)$ is the inverse limit of $\ker(l_X^n)$, or X_{l^n}. This is called the *l-adic Tate group* of X.

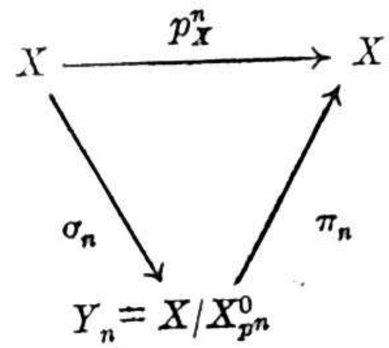
DEFINITION. $T_l(X) = \varprojlim_n X_{l^n}$, *where the inverse system is*

$$\cdots \longrightarrow X_{l^{n+1}} \xrightarrow{l_X} X_{l^n} \xrightarrow{l_X} \cdots \xrightarrow{l_X} X_l.$$

As an inverse limit of finite abelian l-torsion groups, $T_l(X)$ has the structure of a module over the l-adic integers $\mathbf{Z}_l$. Since $X_{l^n} \cong (\mathbf{Z}/l^n\mathbf{Z})^{2g}$, it is easy to see that $T_l(X) \cong \mathbf{Z}_l^{2g}$, as a $\mathbf{Z}_l$-module. Secondly suppose $l = p$. In this case, break up

$$\operatorname{Ker}(p_X^n) = X_{p^n}^0 \times X_{p^n}^r$$

where $X_{p^n}^0$ is local and $X_{p^n}^r$ is reduced. Then by the remark following the theorem, the set of étale coverings π_n in the diagrams



is cofinal in the set of all étale coverings of X whose degree is a power of p. But $\operatorname{Ker}(\pi_n) = \sigma_n(X_{p^n}^r) \cong X_{p^n}^r$, so the p-adic component of $\pi_1(X)$ is again the p-adic *discrete* Tate group.

DEFINITION. $T_p(X) = \varprojlim_n X_{p^n}^r$ (*the inverse system as before*).

$T_p(X)$ is a $\mathbf{Z}_p$-module and if $r = p$-rank of X, then clearly $T_p(X) \cong (\mathbf{Z}_p)^r$. The full fundamental group is then given by

$$\pi_1(X) \cong \prod_{\text{all primes } l} T_l(X).$$

Now suppose $k = \mathbf{C}$, and $X = V/U$ where, as usual, V is a complex vector space and U is a lattice. Then, in addition to the algebraic fundamental group as just defined, we have the usual topological fundamental group $\pi_1^{\text{top}}(X)$, which, as we saw in §1, is canonically isomorphic to U. On the other hand, since

$$X_{l^n} \cong \frac{1}{l^n} U/U \subset V/U = X,$$

it follows that

$$\begin{cases} T_l(X) \simeq \varprojlim_n \frac{1}{l^n} U/U \\ \text{with maps } \frac{1}{l^{n+1}} U/U \xrightarrow{\ l\ } \frac{1}{l^n} U/U, \end{cases}$$

i.e.

$$\begin{cases} T_l(X) \simeq \varprojlim U/l^n U \\ \text{with maps } U/l^{n+1}U \xrightarrow{\ 1\ } U/l^n U. \end{cases}$$

In other words, $T_l(X)$ is the l-adic completion of $U = \pi_1^{\text{top}}(X)$, and

$$\begin{aligned} \pi_1^{\text{alg}}(X) &= \prod_l T_l(X) \\ &= \varprojlim_n U/n!U \\ &= \text{full pro-finite completion of } U \\ &= \widehat{\pi_1^{\text{top}}}(X). \end{aligned}$$

19. Structure of $\mathrm{Hom}(X, X)$. For two abelian varieties X and Y, we denote by $\mathrm{Hom}(X, Y)$ the group of homomorphisms of X into Y, and by $\mathrm{End}\, X$ the ring $\mathrm{Hom}(X, X)$. Further we shall put $\mathrm{Hom}^0(X, Y) = \mathbf{Q} \otimes_{\mathbf{Z}} \mathrm{Hom}(X, Y)$ and $\mathrm{End}^0(X) = \mathbf{Q} \otimes_{\mathbf{Z}} \mathrm{End}\, X$ ($\mathrm{End}^0 X$ is classically called the algebra of complex multiplications of X).

Composition of homomorphisms extends to a unique $\mathbf{Q}$-bilinear map $\mathrm{Hom}^0(X, Y) \times \mathrm{Hom}^0(Y, Z) \to \mathrm{Hom}^0(X, Z)$, so that we can form a category whose objects are abelian varieties, and morphisms from X to Y are elements of $\mathrm{Hom}^0(X, Y)$, the so-called category of "abelian varieties up to isogeny". We have seen that given any isogeny $f: Y \to X$, there is another isogeny $g: X \to Y$ such that $f \circ g = n_X$, and this proves that in the new category, isogenies are isomorphisms. Thus in future, whenever we have an isogeny $f: Y \to X$, we shall denote by f^{-1} its inverse in

$\mathrm{Hom}^0(X, Y)$. It is also clear that we can give the following more fancy definition of $\mathrm{Hom}^0(X, Y)$:

$$\mathrm{Hom}^0(X, Y) = \varinjlim_{(\substack{\text{Isogenies} \\ X' \to X})} \mathrm{Hom}(X', Y).$$

THEOREM 1. (Poincaré's complete reducibility theorem.) *If X is an abelian variety and Y an abelian subvariety there is an abelian subvariety Z such that $Y \cap Z$ is finite and $Y + Z = X$. In other words, X is isogenous to $Y \times Z$.*

PROOF. Let $i: Y \to X$ be the inclusion, and $\hat{i}: \hat{X} \to \hat{Y}$ its dual homomorphism. Let L be ample on X, so that $\phi_L: X \to \hat{X}$ is an isogeny. We take Z to be the connected component of 0 of $\phi_L^{-1}(\ker \hat{i})$. We then have $\dim Z = \dim \ker \hat{i} \geqslant \dim \hat{X} - \dim \hat{Y} = \dim X - \dim Y$. Further, by definition of i and ϕ_L, if $z \in Y$, then

$$\begin{aligned} z \in \phi_L^{-1}(\ker \hat{i}) \cap Y &\iff T_z^* L \otimes L^{-1}|_Y \text{ is trivial} \\ &\iff z \in K(L|_Y). \end{aligned}$$

Since $L|_Y$ is ample, $K(L|_Y)$ and hence $Z \cap Y$ is finite. This means that the natural homomorphism $Z \times Y \to X$ has finite kernel, and since $\dim(Z \times Y) = \dim Z + \dim Y \geqslant \dim X$, it is also surjective.

REMARK. Over the complex field, the complete reducibility theorem is very simple to prove. In fact, let $X = V/U$ with V a complex vector space and U a lattice, and H a positive finite hermitian form on V which is non-degenerate with $E = \mathrm{Im}\, H$ integral on $U \times U$. Then any abelian subvariety Y of X is of the form $V_1/U \cap V_1$ where V_1 is a complex subspace of V with $V_1 \cap U$ a lattice in V_1. If V_2 is the orthogonal complement of V for H, then (a) V_2 is also the orthogonal complement of V for E, hence the lattice $U \cap V_2$ is of maximal rank in V_2; and (b) $V_1 \cap V_2 = (0)$ since H is positive definite. Thus, if $Z = V_2/V_2 \cap U$, Z is a complex subtorus of X such that $Y \cap Z$ is finite. The restriction of H to V_2 gives a Riemann form on V_2, which shows that Z is an abelian subvariety.

In fancy language, the theorem shows that the category of abelian varieties up to isogeny is a "semi-simple abelian category, all of whose objects have finite length". More concretely, we get the following corollaries by standard arguments.

DEFINITION. *An abelian variety is simple if it does not contain an abelian subvariety distinct from itself and zero.*

COROLLARY 1. *Any abelian variety X is isogenous to a product $X_1^{n_1} \times \ldots \times X_k^{n_k}$ where the X_i are simple and not isogenous to each other. The isogeny type of the X_i and the integers n_i are uniquely determined.*

(Proof standard.)

COROLLARY 2. *For X simple, the ring $\mathrm{End}^0 X$ is a division ring. For any abelian variety X, if $X = X_1^{n_1} \times \ldots \times X_k^{n_k}$, with X_i simple and not isogenous, and $D_i = \mathrm{End}^0 X_i$, then*

$$\mathrm{End}^0(X) = M_{n_1}(D_1) \oplus \ldots \oplus M_{n_k}(D_k).$$

[Here $M_k(R)$ = ring of $k \times k$ matrices over R.]

PROOF. For X simple, any non-zero endomorphism of X is an isogeny, hence an invertible element in $\mathrm{End}^0 X$, which proves the first assertion. As for the second, $\mathrm{Hom}(X_i^{n_i}, X_j^{n_j}) = (0)$ for $i \neq j$, so $\mathrm{End}^0 X = \bigoplus_{i=1}^{k} \mathrm{End}^0(X_i^{n_i})$. And $\mathrm{End}^0(X_i^{n_i})$ is clearly the algebra of matrices of order n_i on the division algebra D_i.

We shall say that a function ϕ defined on a vector space V is a polynomial function of degree n if restricted to any finite-dimensional subspace, it is a polynomial function of degree n or, equivalently, if for any $v_0, v_1 \in V$, $\phi(x_0 v_0 + x_1 v_1)$ is a polynomial in x_0 and x_1 of degree n. Thus for instance, we have seen that $\chi(L)$ extends to a homogeneous polynomial function of degree g on the vector space $NS(X) \otimes_{\mathbf{Z}} \mathbf{Q}$.

THEOREM 2. *The function $\phi \longmapsto \deg \phi$ on $\mathrm{End}\, X$ extends to a homogeneous polynomial function of degree $2g$ on $\mathrm{End}^0 X$.*

PROOF. Since for $\phi \in \mathrm{End}\, X$ and $n \in \mathbf{Z}$,

$$\deg n\phi = \deg n_X \cdot \deg \phi = n^{2g} \deg \phi,$$

it suffices to show that for $\phi, \psi \in \mathrm{End}\, X$, the function $P(n) = \deg(n\phi + \psi)$ is a polynomial function. If L is an ample line bundle, we have that

$$\deg(n\phi + \psi) = \frac{\chi((n\phi + \psi)^*(L))}{\chi(L)}.$$

Therefore it suffices to show that $\chi((n\phi + \psi)^*(L))$ is polynomial in n. Putting $L_{(n)} = (n\phi + \psi)^*(L)$ and applying Corollary 2 of the theorem of the cube to the three morphisms $n\phi + \psi$, ϕ, ϕ respectively we get that

$$L_{(n+2)} \otimes L_{(n+1)}^{-2} \otimes L_{(n)} \otimes (2\phi)^* L^{-1} \otimes \phi^* L \otimes \phi^* L = 1,$$

from which it follows by induction on n that for suitable line bundles L_1, L_2, and L_3 on X,

$$L_{(n)} = L_1^{n(n-1)/2} \otimes L_2^n \otimes L_3.$$

Since $\chi(L)$ is a polynomial function of L, $\chi(L_{(n)})$ is a polynomial in n.

To go further and prove, in particular, that $\dim_{\mathbf{Q}} \mathrm{Hom}^0(X, Y)$ is finite, it seems to be essential to use some entirely new method. If $k = \mathbf{C}$, we can compute $\mathrm{Hom}(X, Y)$ very quickly like this.

Let $X_1 = V_1/U_1$, $g_1 = \dim X_1$,

$X_2 = V_2/U_2$, $g_2 = \dim X_2$,

V_i complex vector spaces, U_i lattices.

Then every algebraic homomorphism $f : X_1 \to X_2$ lifts to a complex-analytic homomorphism $\tilde{f} : V_1 \to V_2$. As is well known, such $\tilde{f}$'s are simply the complex *linear* maps from V_1 to V_2. Conversely a complex linear map $L : V_1 \to V_2$ induces an analytic homomorphism $f : X_1 \to X_2$ if and only if $L(U_1) \subset U_2$, and by Chow's theorem (cf. §1) all analytic homomorphisms from X_1 to X_2 are algebraic.

This proves:

$$\mathrm{Hom}_{\substack{\text{abelian}\\ \text{varieties}}}(X_1,X_2) \simeq \left\{ L: V_1 \to V_2 \;\middle|\; L \text{ complex-linear},\ L(U_1) \subset U_2 \right\}.$$

In particular, L is determined by its restriction to U_1 so we get an injection

$$T\colon \mathrm{Hom}_{\substack{\text{abelian}\\ \text{varieties}}}(X_1, X_2) \longrightarrow \mathrm{Hom}_{\mathbf{Z}}(U_1, U_2).$$

Since U_i is the topological fundamental group $\pi_1^{\mathrm{top}}(X_i)$ (or the homology group $H_1(X_i)$), the map T is just the functorial representation of maps between spaces via maps between π_1's (or H_1's). If we introduce bases, we have a faithful representation of $\mathrm{Hom}(X_1, X_2)$ by $2g_1 \times 2g_2$-integral matrices. In particular, $\mathrm{Hom}(X_1, X_2)$ is a free abelian group on at most $4g_1g_2$ generators.

Even when the group field k is not $\mathbf{C}$, an analog of the above method works. This consists in using the free $\mathbf{Z}_l$-module $T_l(X)$ instead of the free $\mathbf{Z}$-module $U = \pi_1^{\mathrm{top}}(X)$. In fact $T_l(X)$ is just the l-primary component of the algebraic fundamental group $\pi_1(X)$, and when $k = \mathbf{C}$, $T_l(X)$ is nothing but the l-adic completion of U. If X_1 and X_2 are two abelian varieties, every homomorphism $f: X_1 \to X_2$ restricts to maps $f\colon (X_1)_{l^n} \to (X_2)_{l^n}$, and hence it induces a map

$$T_l(f)\colon T_l(X_1) \longrightarrow T_l(X_2).$$

The map $f \longmapsto T_l(f)$ itself is a canonical homomorphism:

$$T_l\colon \mathrm{Hom}_{\substack{\text{abelian}\\ \text{varieties}}}(X_1, X_2) \to \mathrm{Hom}_{\mathbf{Z}_l}(T_l(X_1), T_l(X_2)),$$

known as the *l-adic representation*. In fact, in terms of bases of $T_l(X_i)$ over $\mathbf{Z}_l$, this represents homomorphisms f by $2g_1 \times 2g_2$ matrices with coefficients in $\mathbf{Z}_l$. We now prove

THEOREM 3. *For any pair of abelian varieties X and Y, $\mathrm{Hom}(X, Y)$ is a finitely generated free abelian group, and the natural map*

$$\mathbf{Z}_l \otimes_{\mathbf{Z}} \mathrm{Hom}(X, Y) \longrightarrow \mathrm{Hom}_{\mathbf{Z}_l}(T_l(X), T_l(Y)) \qquad (*)$$

induced by T_l: $\mathrm{Hom}(X, Y) \to \mathrm{Hom}_{\mathbf{Z}_l}(T_l(X), T_l(Y))$ (l any prime $\neq$ char k) is injective.

PROOF. Note that since $\mathrm{Hom}(X, Y)$ is torsion free, we have an inclusion $\mathrm{Hom}(X, Y) \subset \mathrm{Hom}^0(X, Y)$.

Step I. For any finitely generated subgroup M of $\mathrm{Hom}(X, Y)$,

$$\mathbf{Q}M \cap \mathrm{Hom}(X, Y) = \{\phi \in \mathrm{Hom}(X, Y) \mid n\phi \in M, \text{ some } n \neq 0\}$$

is again finitely generated.

To prove this, choose isogenies $\prod X_i^{n_i} \to X$ and $Y \to \prod Y_j^{m_j}$ where X_i, Y_j are simple abelian varieties. Then $\mathrm{Hom}(X, Y)$ gets mapped injectively into $\prod_{i,j} \mathrm{Hom}(X_i, Y_j)$, so that it suffices to prove this result for X and Y simple. If X and Y are not isogenous, $\mathrm{Hom}(X, Y) = (0)$, so that we may assume that they are; in this case using the injection $\mathrm{Hom}(X, Y) \to \mathrm{End}\ X$ induced by an isogeny $Y \to X$, we are reduced to the case $X = Y$ and X simple. By the earlier theorem, there is a homogeneous polynomial function P on $\mathrm{End}^0 X$ such that for $\phi \in \mathrm{End}\, X$, $P(\phi) = \deg \phi \in \mathbf{Z}$. Since any $\phi \neq 0$ is an isogeny, $P(\phi) \geqslant 1$ if $\phi \in \mathrm{End}\, X$ and $\phi \neq 0$. Now $\mathbf{Q}.M$ is a finite-dimensional space, and $|P(\phi)| < 1$ is a neighborhood U of 0 in this space. Therefore $U \cap \mathrm{End}\,(X) = (0)$, so $\mathrm{End}\, X \cap \mathbf{Q}.M$ is discrete in $\mathbf{Q}.M$ and hence is finitely generated.

Step II. For any $l \neq p$, the map (*) is injective.

In fact, it suffices to show, in view of Step I, that for any finitely generated (hence free) submodule M of $\mathrm{Hom}(X, Y)$ such that $M = \mathbf{Q}.M \cap \mathrm{Hom}(X, Y)$,

$$\mathbf{Z}_l \otimes_{\mathbf{Z}} M \longrightarrow \mathrm{Hom}_{\mathbf{Z}_l}(T_l(X), T_l(Y))$$

is injective. Let $f_1, \ldots, f_p$ be a $\mathbf{Z}$-base of M. If this map is not injective, since the right side is $\mathbf{Z}_l$-free, we can find $\alpha_i \in \mathbf{Z}_l$ with at least one α_i a unit such that $\Sigma\, \alpha_i f_i \longmapsto 0$. Hence we can find integers n_i ($1 \leqslant i \leqslant p$) not all $\equiv 0 \pmod{l}$ such that $T_l(\sum_1^p n_i f_i)$ maps $T_l(X)$ into $lT_l(Y)$. By the very definition of $T_l(f)$, this

means that $\sum_1^p n_i f_i = f$ maps X_l into 0. But then, f factorizes as $X \xrightarrow{l} X \xrightarrow{g} Y$, and since $g \in \mathbf{Q}.M \cap \mathrm{Hom}(X, Y) = M$, $g = \sum_1^p m_i f_i$. Thus $\Sigma n_i f_i = l\Sigma m_i f_i$, and $f_1, \ldots, f_p$ being a basis of M, $l \mid n_i$ for all i, a contradiction.

The theorem now follows. In fact, because of the injectivity of (*), $\mathrm{Hom}^0(X, Y)$ is finite-dimensional over $\mathbf{Q}$, and because of Step I, $\mathrm{Hom}(X, Y)$ is finitely generated, and being torsion free, it is also free.

COROLLARY 1. $\mathrm{Hom}(X, Y) \simeq \mathbf{Z}^\rho$ *with* $\rho \leqslant 4\dim X.\dim Y$.

PROOF. In fact, the rank of $\mathrm{Hom}(X, Y)$ is at most that of $\mathrm{Hom}_{\mathbf{Z}_l}(T_l(X), T_l(Y))$ which is $4\dim X.\dim Y$.

COROLLARY 2. *For any abelian variety* X, *the group* $NS(X) = \mathrm{Pic}X/\mathrm{Pic}^0X$ *is free of finite rank* (*called the base number of* X).

PROOF. In fact, the homomorphism $L \longmapsto \phi_L$ induces an injection of $NS(X)$ into $\mathrm{Hom}(X, X)$.

COROLLARY 3. End^0X *is a finite-dimensional semisimple algebra over* $\mathbf{Q}$.

Let A be a finite-dimensional associative algebra over a field Γ, which, for simplicity, we assume to be infinite. By a *trace form* on A over Γ, we mean a Γ-linear form

$$S: A \longrightarrow \Gamma$$

such that $S(XY) = S(YX)$ for $X, Y \in A$. A *norm form* on A over Γ is a non-zero polynomial function

$$N: A \longrightarrow \Gamma$$

(i.e. in terms of a basis of A over Γ, $N(a)$ can be written as a polynomial over Γ in the components of a) such that $N(XY) = N(X).N(Y)$ for $X, Y \in A$. The following lemma is well known, but we include a proof for the sake of completeness.

LEMMA. *Let* A *be a finite-dimensional associative simple algebra over a field* Γ (*assumed infinite*) *with center* Λ, *separable over* Γ. *There is a canonical norm form* N^0 *and a canonical trace form* Tr^0 *of* A *over* Λ *such that any norm form* (*resp. trace form*) *of* A *over* Γ_0 *is of the type* $(\mathrm{Nm}_{\Lambda/\Gamma} \circ N^0)^k$ *with* k *an integer* $\geqslant 0$ (*resp.* $\phi \circ \mathrm{Tr}^0$ *where* $\phi: \Lambda \to \Gamma$ *is a* Γ-*linear form*). *If* $[A:\Lambda] = d^2$, N^0 *is homogeneous of degree* d.

PROOF. When $\Gamma = \Lambda$ is separably closed, A can be taken to be a matrix algebra $M_d(\Gamma)$. In this case, the elements $XY - YX$ span the vector subspace of matrices of zero trace, and any norm form gives rise to a rational homomorphism of algebraic groups $GL(d) \to \mathbf{G}_m$. This shows the validity of the lemma with Tr = matrix trace, N = matrix determinant.

In the general case, let $\overline{\Gamma}$ be the separable closure of Γ, $\sigma_i: \Lambda \to \overline{\Gamma}$ $(1 \leqslant i \leqslant [\Lambda:\Gamma])$ the various imbeddings of Λ in $\overline{\Gamma}$ over Γ, and $\overline{\Gamma}_{(i)}$ the field $\overline{\Gamma}$ considered as a Λ-algebra through σ_i. We have an isomorphism of $\overline{\Gamma}$-algebras

$$A \otimes_\Gamma \overline{\Gamma} \simeq A \otimes_\Lambda (\Lambda \otimes_\Gamma \Gamma) \simeq \prod_i A \otimes_\Lambda \overline{\Gamma}_{(i)}.$$

Denote the image of $\alpha \in A \otimes_\Gamma \overline{\Gamma}$ under this isomorphism by $\{\phi_i(\alpha)\}$. If N is any norm form on A over Γ, it extends to a norm form of $A \otimes_\Gamma \overline{\Gamma}$ over $\overline{\Gamma}$, and defines a norm form N_i on $A \otimes_\Gamma \overline{\Gamma}_{(i)}$ by the equation $N_i(\xi) = N(1, 1, \ldots, \xi, 1, \ldots, 1)$. By what we have seen, $N_i = (N_i^0)^{n_i}$, where N_i^0 is the reduced norm of $A \otimes_\Lambda \overline{\Gamma}_{(i)}$ over $\overline{\Gamma}_{(i)}$ so that we get

$$N(\alpha) = \prod_i N_i^0(\phi_i(\alpha))^{n_i}.$$

We shall show that the norm $\alpha \longmapsto \prod_i N_i^0(\phi_i(\alpha))^{n_i}$ of $A \otimes_\Gamma \overline{\Gamma}$ over $\overline{\Gamma}$ comes from a norm of A over Γ by base extension if and only if all the n_i are equal. Since $\overline{\Gamma}$ is the separable closure of Γ, N comes from Γ if and only if for any automorphism σ of $\overline{\Gamma}$ over Γ, we have $N((1 \otimes \sigma)\alpha) = \sigma(N\alpha)$, that is to say,

$$\prod_i N_i^0(\phi_i((1\otimes\sigma)\alpha))^{n_i} = \sigma\prod_i N_i^0(\phi_i(\alpha))^{n_i}.$$

Now, there is a permutation π of the integers from 1 to $[\Lambda:\Gamma]$ such that $\sigma\circ\sigma_i = \sigma_{\pi(i)}$, and we have the commutative diagram

$$\begin{array}{ccc} A\otimes_\Gamma\bar{\Gamma} & \xrightarrow{\phi_i} & A\otimes_\Lambda\bar{\Gamma}_{(i)} \\ \downarrow{\scriptstyle 1\otimes\sigma} & & \downarrow{\scriptstyle 1\otimes\sigma} \\ A\otimes_\Gamma\bar{\Gamma} & \xrightarrow{\phi_{\pi(i)}} & A\otimes_\Lambda\bar{\Gamma}_{\pi(i)} \end{array}$$

so that (since the second vertical arrow is an isomorphism of simple algebras over the isomorphism σ of separably closed base fields) we get $N^0_{\pi(i)}[\phi_{\pi(i)}((1\otimes\sigma)(\alpha))] = \sigma N_i^0(\phi_i(\alpha))$, and on substitution, we see that we must have $n_{\pi(i)} = n_i$ for all i. Now, the Galois group of $\bar{\Gamma}$ over Γ acts transitively on the imbeddings over Λ in $\bar{\Gamma}$, so that we must have all the n_i equal.

Thus we see that we may take $N^0(\alpha) = \prod_i N_i^0(\phi_i(\alpha))$ in the lemma, and then $N(\alpha) = \mathrm{Nm}_{\Lambda/\Gamma}(N^0_{A/\Lambda}(\alpha))^{n_i}$. The assertion about the trace is even simpler.

DEFINITION. *$\mathrm{Nm}_{\Lambda/\Gamma}\circ N^0$ will be called the reduced norm of A over Γ and $\mathrm{Tr}_{\Lambda/\Gamma}\circ\mathrm{Tr}^0$ will be called the reduced trace of A over Γ.*

We can now prove the following important

THEOREM 4. *Let f be an endomorphism of an abelian variety, and $T_l(f)$ the induced endomorphism of $T_l(X)$ ($l\neq$ characteristic). Then*

$$\deg f = \det T_l(f),$$

hence

$$\deg(n.1_X - f) = P(n),$$

where $P(t)$ is the characteristic polynomial, $\det(t - T_l(f))$, of $T_l(f)$. The polynomial P is monic of degree $2g$, has rational integral coefficients, and $P(f) = 0$.

PROOF. The functions $f\longmapsto \deg f$ and $f\longmapsto \det T_l(f)$ both extend uniquely to norm forms N_1 and N_2 respectively of degree $2g$ on the semi-simple $\mathbf{Q}_l$-algebra $\mathbf{Q}_l\otimes_{\mathbf{Z}}$ End X, where $\mathbf{Q}_l$ is the quotient field of $\mathbf{Z}_l$. If $|\ \ |$ denotes the l-adic absolute value, we assert that $|N_1\alpha| = |N_2\alpha|$ for all $\alpha\in\mathbf{Q}_l\otimes_{\mathbf{Z}}$ End X. In fact, it suffices to verify this by homogeneity for $\alpha\in\mathbf{Z}_l\otimes_{\mathbf{Z}}$ End X, and by continuity for $\alpha\in$ End X. Thus we have to show that the power of l dividing $\deg f$ equals the power of l dividing $\det T_l(f)$. Now, the power of l dividing $\deg f$ is the order of the kernel of $X_{l^n}\xrightarrow{f} X_{l^n}$ for n large, or what is the same the order of the cokernel of this map for n large. On passing to the limit, it is also the order of the cokernel of $T_l(f)$, which is l^ν, where ν is the power of l occurring in $\det T_l(f)$.

Now let $\mathbf{Q}_l\otimes_{\mathbf{Z}}\mathrm{End}\ X\simeq\prod_{j=1}^r A_j$ be the decomposition of $\mathbf{Q}_l\otimes_{\mathbf{Z}}$ End X into a product of simple algebras. The norms N_1 and N_2 go over into norms on $\prod_j A_j$, i.e. into power products

$$N_i(\alpha_1,\ldots,\alpha_p) = \prod_{j=1}^r N_j^0(\alpha_j)^{\nu_{ij}}\ (i=1,2),$$

where N_j^0 are the norm forms on A_j over $\mathbf{Q}_l$ of lowest degree, by the lemma. On taking $\alpha_j = 1$ for $j\neq j_0$, we deduce that $|N_{j_0}(\alpha_{j_0})|^{\nu_{1j_0}-\nu_{2j_0}} = 1$ for all $\alpha_{j_0}\in A_{j_0}$. Since N_{j_0} is homogeneous of positive degree, we see (by multiplying α_{j_0} by l) that $\nu_{1j_0} = \nu_{2j_0}$, and since this holds for all j_0, $N_1 = N_2$.

This proves the first statement of the theorem. The second follows on substituting $n.1_X - f$ for f and using $T_l(n.1_X - f) = n.1_{T_l(X)} - T_l(f)$. Now P has to be monic of degree $2g$ and, since $P(n)$ is an integer for all n, its coefficients are all rational. Further, since End X is a finite $\mathbf{Z}$-module, f is integral over $\mathbf{Z}$, so f and hence $T_l(f)$ satisfies a monic equation over $\mathbf{Z}$. Hence all the eigenvalues of the matrix $T_l(f)$ are algebraic integers, and its characteristic polynomial has coefficients which are algebraic integers. Since the coefficients are also

rational, they are rational integers. Hence $P(f)$ is a well-defined element of $\mathrm{End}\,X$, and we have finally $T_l(P(f)) = P(T_l f) = 0$, so that $P(f) = 0$.

DEFINITION. *The above polynomial $P(t)$ (which belongs to $\mathbf{Z}[t]$ and is independent of l) is called the characteristic polynomial of f. Its constant term and minus the coefficient of t^{g-1} are called the norm and trace respectively of f.*

By the lemma proved earlier, we see that if $\mathrm{End}^0X = A_1 \times \ldots \times A_k$ where A_i are simple algebras over $\mathbf{Q}$, and we denote the components of an $f \in \mathrm{End}^0X$ in A_i by f_i, and the reduced norm of A_i over $\mathbf{Q}$ and the reduced trace over $\mathbf{Q}$ by Nm^0 and Tr^0 respectively, we have

$$\mathrm{Nm}\, f = \prod_{i=1}^{k} (\mathrm{Nm}^0 f_i)^{n_i},$$

$$\mathrm{Tr}\, f = \sum_{i=1}^{k} n_i \mathrm{Tr}^0 f_i,$$

where n_i are integers > 0.

COROLLARY. *Let X be a simple abelian variety of dimension g, K the center of the algebra* End^0X, $[K:\mathbf{Q}] = e$, $[\mathrm{End}^0X : K] = d^2$. *Then de divides $2g$.*

PROOF. We have $\mathrm{Nm}\, f = (\mathrm{Nm}^0 f)^n$ for some n. But Nm is a polynomial function of degree $2g$, and Nm^0 is a polynomial function of degree de.

REMARK. When the characteristic of k is zero, with assumptions as in the above corollary, one can say even that d^2e divides $2g$. In fact, we may assume (by the Lefschetz principle) that k is the complex field. Let $X = V/U$ as usual. Then the division ring End^0X admits a faithful representation in the rational vector space $U \otimes \mathbf{Q}$, so $U \otimes \mathbf{Q}$ becomes a vector space over End^0X. Hence $\dim_{\mathbf{Q}} U \otimes \mathbf{Q} = 2g$ must be divisible by $\dim_{\mathbf{Q}} \mathrm{End}^0X = d^2e$.

This is definitely false in positive characteristic. In fact, for any characteristic $p > 0$, we shall see in §22 that there exists an

elliptic curve X with p-rank 0 and that for such a curve, End^0X is non-commutative of rank 4 with center $\mathbf{Q}$. Thus, in this case, $de = 2 = 2g$.

DEFINITION. *A simple abelian variety X is of (CM)-type if $de = 2g$ where d^2 is the rank of* End^0X *over its center K, e is the degree of K over $\mathbf{Q}$ and g the dimension of X.*

Now, in a division algebra A of rank d^2 over its center K it is well known that all maximal commutative subfields have degree d over K. Thus, a simple abelian variety X is of (CM)-type if and only if End^0X admits a subfield of degree $2g$ (since in any case, $de \leqslant 2g$).

20. Riemann forms. Let l be a prime different from the characteristic of k, and let μ_{l^n} be the group of l^n-th roots of unity in k^*. We have homomorphisms $\mu_{l^{n+1}} \to \mu_{l^n}$ given by $\xi \longmapsto \xi^l$, and this makes $\{\mu_{l^n}\}$ a projective system. Let us put $M_l = \varprojlim \mu_{l^n}$.

M_l has the structure of $\mathbf{Z}_l$-module. Since evidently we can choose isomorphisms $\mu_{l^n} \simeq \mathbf{Z}/l^n\mathbf{Z}$ such that the maps $\mu_{l^{n+1}} \to \mu_{l^n}$ go over into the natural maps $\mathbf{Z}/l^{n+1}\mathbf{Z} \to \mathbf{Z}/l^n\mathbf{Z}$ the projective limit is (non canonically) isomorphic to the $\mathbf{Z}_l$ itself.

Now, let n be any integer prime to the characteristic. We have set up a canonical isomorphism of $\ker n_{\hat{X}}$ with the dual of $\ker n_X$, that is to say, we have defined a pairing which we will call $\bar{e}_n$: $X_n \times (\hat{X})_n \to \mu_n$, where μ_n is the group of n-th roots of unity in k^*. Recall the definition:

Take $a \in X_n$ and $\lambda \in (\hat{X})_n$, and let λ correspond to the line bundle L. Then L^n is trivial, so $n_X^* L$ is trivial too and

$$L \simeq \mathbf{A}^1 \times X \Big/ \left\{ \begin{array}{l} \text{action of } X_n \\ \\ \phi_u(\alpha, x) = (\chi(u).\alpha,\ x + u) \end{array} \right\}$$

for a character $\chi\colon X_n \to k^*$. Then

$$\bar{e}_n(a, \lambda) = \chi(a).$$

In other words, we take the canonical action of X_n on $n_X^* L$ and carry it over to an action of X_n on the trivial bundle, where it is given by a character χ. It is useful to have an alternate definition of $\bar{e}_n$ using divisors instead of line bundles. Let D be a divisor such that

$$\mathcal{O}_X(D) \simeq \underline{L}.$$

Since L^n and $n_X^* L$ are trivial, there are rational functions f and g on X such that

$$(f) = nD,$$

$$(g) = n_X^{-1}(D).$$

Then

$$(n_X^* f) = n.n_X^{-1} D = (g^n),$$

so for some constant α,

$$g^n(x) = \alpha . f(n . x), \text{ all } x \in X.$$

It follows that $[g(x)/g(x+a)]^n = 1$ for all $x \in X$, i.e. $g(x)/g(x+a)$ is a constant n-th root of unity, and we can prove

LEMMA. $\bar{e}_n(a,\lambda) = \dfrac{g(x)}{g(x+a)}$.

PROOF. Let $\dfrac{g(x)}{g(x+a)} = \eta(a)$. Consider the diagram of maps of sheaves:

$$\mathcal{O}_X(D) \xrightarrow{n_X^*} \mathcal{O}_X(n_X^{-1}D) \xleftarrow[\text{mult. by } g]{\approx} \mathcal{O}_X.$$

It follows that for all affine open sets $U \subset X$, if $V = n_X^{-1}(U)$, then we get a diagram

$$\Gamma(U,\mathcal{O}_X(D)) \xrightarrow{n_X^*} \Gamma(V, \mathcal{O}_X(n_X^{-1}D)) \xleftarrow[\text{mult. by } g]{\approx} \Gamma(V,\mathcal{O}_X)$$

and this identifies $\Gamma(U,\mathcal{O}_X(D))$ with the subspace of $\Gamma(V,\mathcal{O}_X)$ of functions $f(x)$ such that

$$f(x+u) . g(x+u) = f(x) . g(x), \text{ all } u \in X_n.$$

On the other hand, if we let M be the quotient of $\mathbf{A}^1 \times X$ by the action of X_n

$$\phi_u(\alpha, x) = (\eta(u).\alpha, x+u),$$

then $\Gamma(U, \underline{M})$ is identified with the subspace of $\Gamma(V,\mathcal{O}_X)$ of functions $f(x)$ such that

$$\phi_u(f(x), x) = (f(x+u), x+u), \quad \text{all } u \in X_n,$$

i.e. $f(x+u) = \eta(u) . f(x)$, all $u \in X_n$. This is the same condition as before, so $\underline{M} \simeq \mathcal{O}_X(D)$, i.e., $M \simeq L$. Therefore η must equal χ.

We want to pass to the limit over n, by means of the

PROPOSITION. *Let m, n be two integers coprime to the characteristic, $x \in X_{mn}$, $y \in (\hat{X})_{mn}$. We then have*

$$\bar{e}_n(mx, my) = (\bar{e}_{mn}(x, y))^m.$$

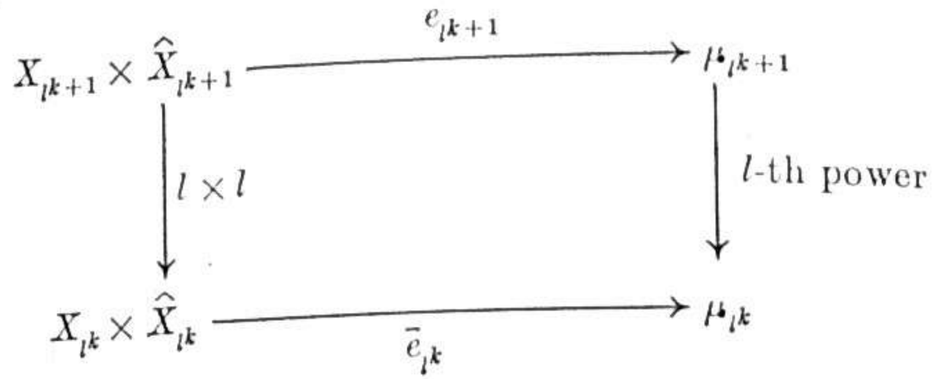
PROOF. Let V be a complete variety, G a finite group acting freely on V, H a normal subgroup of G, L a line bundle on V/G which becomes trivial when pulled back to V/H. Then we get an associated homomorphism χ of G/H into k^* as above. But now, L becomes trivial also when pulled back to V, and we thus get a homomorphism χ' of G into k^*. It is then clear that $\chi' = \chi \circ \eta$ where $\eta: G \to G/H$ is the natural homomorphism.

Let us now apply this remark with $V = X$, $G = X_{mn}$ and $H = X_m$. The quotients $X \to X/G$, $X \to X/H$ and $X/H \to X/G$ identify themselves to the maps $(mn)_X: X \to X$, $m_X: X \to X$ and $n_X: X \to X$ respectively, and the natural homomorphism $G \to G/H$ becomes $X_{mn} \xrightarrow{m_X} X_n$. Hence, for any line bundle L on X such that $n_X^*(L)$ is trivial, and any $x \in X_{mn}$, we have by the above that

$$\bar{e}_n(mx, \lambda) = \bar{e}_{mn}(x, \lambda),$$

where $\lambda \in \hat{X}_n$ corresponds to L. Writing $\lambda = my$ with $y \in (\hat{X})_{mn}$, the proposition follows.

In particular, taking $n = l^k$ and $m = l$, we get the commutative diagram



and hence by passage to the limit as $k \to \infty$, we get a natural pairing

$$e_l\colon T_l(X) \times T_l(\hat{X}) \longrightarrow M_l.$$

One checks trivially that this pairing is $\mathbf{Z}_l$-bilinear and non-degenerate. Further, if $f\colon X \to Y$ is a homomorphism of abelian varieties, $\hat{f}$ its dual and $T_l(f)$ and $T_l(\hat{f})$ are the homomorphisms induced on the Tate modules, we have for $\xi \in T_l(X)$ and $\eta \in T_l(\hat{Y})$,

$$e_l(T_l(f)(\xi), \eta) = e_l(\xi, T_l(\hat{f})(\eta)). \tag{I}$$

This follows from a corresponding equation for $\bar{e}_n$, which follows readily after writing out the definitions.

THE RIEMANN FORM OF A DIVISOR.

DEFINITION. *Let L be a line bundle on an abelian variety X, and l a prime distinct from the characteristic of k. We then define the Riemann form E^L of L to be the $\mathbf{Z}_l$-bilinear map $E^L\colon T_l(X) \times T_l(X) \to M_l$ given by $E^L(x, y) = e_l(x, T_l(\phi_L)(y))$.*

THEOREM 1. *The Riemann form E^L of any line bundle L is skew-symmetric.*

We will give a sheaf-theoretic proof of this in §23. Rather than chase through confusing diagrams, here is the proof in the language of divisors.

PROOF. It suffices to prove that $\bar{e}_n(a, \phi_L(a)) = 1$, all $a \in X_n$. Let the divisor D represent L. If $a \in X_n$, and g satisfies

$$(g) = n_X^{-1}(T_a^{-1}D - D),$$

then we must prove that $g(x + a) = g(x)$, all $x \in X$. Choose b such that $nb = a$, and let $E = n_X^{-1}D$, so

$$(g) = T_b^{-1}E - E.$$

Then

$$(T_{ib}^{*}g) = T_{(i+1)b}^{-1}E - T_{ib}^{-1}E,$$

and since E is invariant under T_a,

$$\left(\prod_{i=0}^{n-1} T_{ib}^{*}g\right) = \sum_{i=0}^{n-1} T_{(i+1)b}^{-1}E - T_{ib}^{-1}E = 0.$$

Therefore $h(x) = \prod_{i=0}^{n-1} g(x + ib)$ is a constant, hence

$$1 = \frac{h(x+b)}{h(x)} = \frac{\prod_{i=0}^{n-1} g(x + b + ib)}{\prod_{i=0}^{n-1} g(x + ib)} = \frac{g(x+a)}{g(x)}.$$

Thus $L \longmapsto E^L$ induces a map:

$$\begin{array}{c} NS(X) \\ \| \text{def} \\ \mathrm{Pic}(X)/\mathrm{Pic}^0(X) \end{array} \longrightarrow \left\{ \begin{array}{l} \text{Alternating 2-forms} \\ T_l(X) \times T_l(X) \to M_l \end{array} \right\}.$$

This is injective since $E^L = 0 \Rightarrow \phi_L = 0$ since e_l is non-degenerate. Now, if $f\colon X \to Y$ is a homomorphism of abelian varieties, and L is a line bundle on Y, then

$$E^{f^{*}L}(x, y) = E^L(T_l f(x), T_l f(y)),\ x, y \in T_l X. \tag{II}$$

PROOF.
$$\begin{aligned} E^{f^{*}L}(x, y) &= e_l(x, \phi_{f^{*}L}\, y) \\ &= e_l(x, T_l\hat{f} \circ \phi_L \circ T_l f(y)) \\ &= e_l(T_l f(x), \phi_L(T_l f(y))) \\ &= E^L(T_l f(x), T_l f(y)). \end{aligned}$$

Next, we can compute E^P, when P is the Poincaré bundle on $X \times \hat{X}$. Identifying $T_l(X \times \hat{X})$ with $T_l(X) \times T_l(\hat{X})$, then

$$E^P((x, \hat{x}), (y, \hat{y})) = e_l(x, \hat{y}) - e_l(y, \hat{x}). \tag{III}$$

PROOF. By skew-symmetry and linearity, it suffices to show that $E^P((x,0),(y,0)) = E^P((0,\hat{x}),(0,\hat{y})) = 0$ and $E^P((x,0),(0,\hat{y})) = e_l(x,\hat{y})$. Using the functoriality property of E for the inclusion of $X \times (0)$ in $X \times \hat{X}$ and the triviality of the restriction of P to $X \times (0)$, it follows that $E^P((x,0),(y,0)) = 0$; similarly $E^P((0,\hat{x}),(0,\hat{y})) = 0$. To prove the last assertion note that we have an isomorphism $(X \hat{\times} Y) \xrightarrow{\sim} \hat{X} \times \hat{Y}$ which is given by the map of line bundles $L \longmapsto (L|X \times (0), L|(0) \times Y)$ for $L \in \mathrm{Pic}^0(X \times Y)$. In particular, taking $Y = \hat{X}$, we have an identification of $(X \hat{\times} \hat{X})$ with $\hat{X} \times \hat{\hat{X}}$. Now, for any $(x, \hat{x}) \in X \times \hat{X}$, $\phi_P((x,\hat{x}))$ is given by the line bundle $T^*_{(x,\hat{x})} P \otimes P^{-1}$, and this is determined by the pair of bundles

$$(T^*_{(x,\hat{x})} P \otimes P^{-1}|_{X\times(0)},\ T^*_{(x,\hat{x})} P \otimes P^{-1}|_{(0)\times\hat{X}}) \cong (P|_{X\times(\hat{x})},\ P|_{(x)\times\hat{X}}).$$

Therefore $\phi_P((x,\hat{x})) = (\hat{x}, i(x))$, where $i: X \to \hat{\hat{X}}$ is the natural homomorphism. Thus, we obtain

$$E^P((x,0),\ (0,\hat{y})) = e_l((x,0),\ (\hat{y},0)) = e_l(x,\hat{y}).$$

Theorem 1 has the following partial converse.

THEOREM 2. *Let X be an abelian variety, and $\phi: X \to \hat{X}$ a homomorphism. Then the bilinear form $(x,y) \longmapsto e_l(x,\phi y)$ on $T_l(X)$ is skew-symmetric if and only if there is a line bundle L on X such that $2\phi = \phi_L$.*

PROOF. If $2\phi = \phi_L$, $2e_l(x,\phi(y)) = e_l(x,\phi_L(y))$ is skew-symmetric by Theorem 1, hence so is $e_l(x,\phi y)$. Conversely suppose this form is skew-symmetric, and let L be the pull back of the Poincaré bundle P by the homomorphism $(1,\phi): X \to X \times \hat{X}$. Then we claim that $2\phi = \phi_L$. It suffices, because of the non-degeneracy of e_l, to show that $2e_l(x,\phi y) = e_l(x,\phi_L y)$ for any $x, y \in T_l(X)$. Now, we have

$$\begin{aligned} e_l(x,\phi_L(y)) &= E^L(x,y) = E^P((1,\phi)(x),(1,\phi)(y)) \\ &= e_l(x,\phi y) - e_l(y,\phi x) = 2e_l(x,\phi y), \end{aligned}$$

by formulas (II) and (III) and the skew-symmetry of $e_l(x,\phi y)$.

REMARK. We shall see in §23 that if $2\phi = \phi_L$ for some line bundle L, we must have $\phi = \phi_{L'}$ for another line bundle L'. Thus, the above theorem would then give a necessary and sufficient condition for a homomorphism $\phi: X \to \hat{X}$ to be of the form ϕ_L.

THE ROSATI INVOLUTION.

We fix an ample line bundle L on the abelian variety X, so that $\phi_L: X \to \hat{X}$ is an isogeny.

DEFINITION. *The Rosati involution on the algebra* $\mathrm{End}^0 X$ *with respect to L is the involution $\phi' = \phi_L^{-1} \circ \hat{\phi} \circ \phi_L$, $\hat{\phi} \in \mathrm{End}^0 \hat{X}$.*

One has the following properties of this map.

(1) For $\phi, \psi \in \mathrm{End}^0 X$, $(a\phi)' = a\phi'$, $a \in \mathbf{Q}$

$$(\phi + \psi)' = \phi' + \psi'$$

$$(\phi\psi)' = \psi'\phi'.$$

These are clear.

(2) Extend the homomorphism of rings T_l: End $X \to \mathrm{End}_{\mathbf{Z}_l} T_l(X)$ to a homomorphism $\mathrm{End}^0 X \to \mathrm{End}_{\mathbf{Q}_l}(\mathbf{Q}^l \otimes_{\mathbf{Z}_l} T_l(X))$ and denote the extended map again by T_l. Then for any $\phi \in \mathrm{End}^0 X$, $T_l(\phi')$ is the adjoint of $T_l(\phi)$ for the non-degenerate bilinear form E^L, that is, we have

$$E^L(\phi x, y) = E^L(x, \phi' y).$$

In particular, $\phi'' = \phi$, i.e., $\phi \longmapsto \phi'$ is an involution.

PROOF. We have

$$\begin{aligned} E^L(x,\phi' y) &= e_l(x, \phi_L \circ \phi_L^{-1} \circ \hat{\phi} \circ \phi_L y) \\ &= e_l(x, \hat{\phi} \circ \phi_L y) \\ &= e_l(\phi x, \phi_L y) \\ &= E^L(\phi x, y) \end{aligned}$$

which proves the equation.

(3) Identify $\mathbf{Q}\otimes_{\mathbf{Z}} NS(X) = \mathbf{Q}\otimes_{\mathbf{Z}} \dfrac{\operatorname{Pic} X}{\operatorname{Pic}^0 X}$ with a subspace of $\operatorname{Hom}^0(X, \hat{X})$ by the map $M \longmapsto \phi_M$. Then, under the isomorphism $\operatorname{Hom}^0(X, \hat{X}) \xrightarrow{\sim} \operatorname{End}^0 X$ given by $\psi \to \phi_L^{-1}\circ\psi$, the above subspace goes over into the subspace $\{\psi \in \operatorname{End}^0 X \mid \psi' = \psi\}$ of symmetric elements of $\operatorname{End}^0 X$ for the Rosati involution.

PROOF. In fact, by the last theorem, an element $\psi \in \operatorname{End}^0 X$ belongs to this subspace if and only if for $\phi = \phi_L \circ \psi$, we have $e_l(x, \phi y) = -\, e_l(y, \phi x)$. But this means $E^L(x, \psi y) = -\, E^L(y, \psi x)$, that is, $E^L(x, \psi y) = E^L(\psi x, y) = E^L(x, \psi' y)$, for all $x, y \in T_l(X)$. The result follows since E^L is non-degenerate and $\psi \longmapsto T_l(\psi)$ is faithful.

THEOREM 3. *Let X be an abelian variety. Then there is a generator*

$$v \in \operatorname{Hom}_{\mathbf{Z}_l}(\Lambda^{2g} T_l(X), M^{\otimes g})$$

with the following property: for all divisors $D_1, \ldots, D_g$ on X, let L_i be the line bundles $L_X(D_i)$ and let $E_i = E^{L_i}$ be their Riemann forms. Then

$$E_1 \wedge \ldots \wedge E_g = (D_1 \cdot \ldots \cdot D_g)\cdot v.$$

PROOF. Since both the left and the right depend in a polynomial fashion on the images of the L_i in $NS(X)$, this formula results by polarization from the formula with $L_1 = \ldots = L_g$, $D_1 = \ldots = D_g$. Using the fact that $\chi(L) = (D^g)/g!$, we are reduced to proving

$$[E^L]^{\wedge g} = g!\chi(L)\cdot v.$$

Fix an isomorphism $M_l \simeq \mathbf{Z}_l$, and choose a basis for $T_l(X)$ over $\mathbf{Z}_l$. Then $\overset{2g}{\Lambda}\, T_l(X)$ becomes isomorphic to $\mathbf{Z}_l$ by using this basis, and so that $[E^L]^{\wedge g}$ becomes a scalar. Further, by using this basis, E^L becomes a matrix. We assert that

$$([E^L]^{\wedge g})^2 = (\det\ E^L).(g!)^2.$$

In fact, this equation remains invariant under change of basis for $\mathbf{Q}_l \otimes T_l(X)$, and it follows by a simple computation on choosing a basis so that E^L takes the standard form

$$\left[\begin{array}{c|c|c} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} & \mathbf{0} & \mathbf{0} \\ \hline \mathbf{0} & \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{0} & \ddots \end{array}\right]$$

Again since both sides of the equality of the theorem are polynomials in L, we are reduced to showing that $\chi(L)^2 = c.\det E^L$, where c is an l-adic unit. By the Riemann-Roch theorem this is equivalent to: $\deg \phi_L = c.\det E^L$, where c is an l-adic unit. Now, $E^L(x, y) = e_l(x, \phi_L(y))$, and since e_l is a non-degenerate pairing over $\mathbf{Z}_l$, we see that $\det E^L = \det T_l(\phi_L)$ if we define the matrix representation of $T_l(\phi_L)$ using a dual basis of $T_l(\hat{X})$.

Choose and fix an isogeny $\psi\colon \hat{X} \to X$. We then have that

$$\begin{aligned} \deg\psi \cdot \deg\phi_L &= \deg(\psi\circ\phi_L) \\ &= \det\,[T_l(\psi)\circ T_l(\phi_L)] \\ &= \det\,(T_l(\psi))\cdot\det\,(T_l(\phi_L)). \end{aligned}$$

Thus, to complete the proof of the theorem, we have only to observe that $\deg\psi/\det T_l(\psi)$ is an l-adic unit, and this follows from the fact that the largest power of l dividing $\deg\psi$ is the order of the kernel, or equivalently cokernel, of $\psi \mid X_{l^n}\colon X_{l^n} \to X_{l^n}$ for n large and this is the same as the largest power of l dividing $\det T_l(\psi)$.

COROLLARY. *Let X be a simple abelian variety of dimension g, and $K \subset \operatorname{End}^0 X$ a $\mathbf{Q}$-subalgebra such that $\phi = \phi'$ for all $\phi \in K$. Then $[K\colon \mathbf{Q}]$ divides g.*

PROOF. Since $\phi\psi = \phi'\psi' = (\psi\phi)' = \psi\phi$ for $\phi, \psi \in K$, K is a subfield of $\operatorname{End}^0 X$. Further, since K consists of symmetric elements, it is contained in the image of $\mathbf{Q}\otimes_{\mathbf{Z}} \operatorname{Pic} X/\operatorname{Pic}^0 X$ by the map $M \longmapsto \phi_L^{-1}\circ\phi_M$. Now $\chi(M)$ depends only on the endomorphism

$\phi_L^{-1} \circ \phi_M$, and it extends to a homogeneous polynomial function of degree g on the space of symmetric elements of $\mathrm{End}^0 X$. We assert that the restriction to K of the function $\frac{\chi(M)}{\chi(L)}$ is a norm function on K. Now, it is easy to check that (since it is already polynomial), if its square $\frac{\chi^2(M)}{\chi^2(L)}$ is multiplicative on K, then it is multiplicative too. But $\frac{\chi^2(M)}{\chi^2(L)} = \frac{\deg \phi_M}{\deg \phi_L} = \deg \phi_L^{-1} \circ \phi_M$, which is multiplicative in $\phi_L^{-1} \circ \phi_M$. Thus we get a norm function of degree g on K, and K being a field of degree $[K: \mathbf{Q}]$, the corollary follows.

21. Positivity of the Rosati involution.

THEOREM 1. *Let H be an ample divisor on an abelian variety, $L = L_X(H)$ the associated line bundle and $'$ the involution of* $\mathrm{End}^0 X$ *given by L. Then for any $\phi \in \mathrm{End}\ X$, we have*

$$\mathrm{Tr}(\phi\phi') = \frac{2g}{(H^g)} (H^{g-1} . \phi^*(H))$$

where $(\ ,\ )$ denotes intersection numbers. In particular, $\phi \longmapsto \mathrm{Tr}(\phi . \phi')$ is a positive definite quadratic form on $\mathrm{End}^0 X$.

PROOF. The first assertion clearly implies the second, since for any effective divisor D and an ample divisor H, $(H^{g-1}. D) > 0$. It suffices therefore to prove the first statement.

Choose and fix bases for $T_l(X)$ and M_l. Applying Theorem 3 §19, we get

$$[E^L]^{\wedge g} = c . (H^g),$$
$$[E^L]^{\wedge g-1} \wedge E^{\phi^*(L)} = c . (H^{n-1} . \phi^*(H)),$$

for some l-adic constant c. Therefore,

$$\frac{[E^L]^{\wedge g-1} \wedge E^{\phi^*(L)}}{[E^L]^{\wedge g}} = \frac{(H^{g-1} . \phi^*(H))}{(H^g)}.$$

Since we have $E^{\phi^*(L)} = E^L \circ (\phi \times \phi)$, we are reduced to proving the equation

$$\frac{[E^L]^{\wedge g-1} \wedge (E^L \circ (\phi \times \phi))}{[E^L]^{\wedge g}} = \frac{1}{2g} \mathrm{Tr}(\phi\phi'),$$

where ϕ' is the transpose of ϕ with respect to E^L. This is purely a problem on linear algebra. We may utilize a basis $e_1, e_2, \ldots, e_{2g}$ of $\mathbf{Q}_l \otimes T_l(X)$ such that $E^L(e_{2i-1}, e_{2i}) = 1$ and $E^L(e_{2i-1}, e_j) = E^L(e_{2i}, e_j) = 0$ if $j \neq 2i$ or $2i-1$. Then the left side becomes (by definition of exterior multiplication)

$$\sum_{i_1, i_2, \ldots, i_g \text{ odd}} E^L(\phi(e_{i_g}), \phi(e_{i_g+1})) \Big| \sum_{i_1, \ldots, i_g \text{ odd}} 1$$

$$= \left[\frac{(g-1)!}{g!} \cdot \sum_{i \text{ odd}} E^L(\phi(e_i), \phi(e_{i+1})) \right]$$

$$= \frac{1}{2g} \sum_{i \text{ odd}} \left[E^L(e_i, \phi\phi'(e_{i+1})) + E^L(\phi'\phi(e_i), e_{i+1}) \right]$$

$$= \frac{1}{2g} \mathrm{Tr}(\phi'\phi).$$

APPLICATION I. STRUCTURE OF $\mathrm{End}^0 X$ FOR SIMPLE X.

We have seen that for a simple abelian variety X, $D = \mathrm{End}^0 X$ is a division algebra of finite rank over $\mathbf{Q}$ with an involution $x \longmapsto x'$ such that if $x \neq 0$, $\mathrm{Tr}(xx') > 0$ where the trace is the reduced trace over $\mathbf{Q}$ (or any positive multiple of it).

We shall now give the classification, due to Albert, of all pairs $(D, ')$ where D is a division algebra of finite rank n over $\mathbf{Q}$ and $x \longmapsto x'$ is an involution such that $\mathrm{Tr}_{D/\mathbf{Q}}(xx') > 0$ for $x \in D$, $x \neq 0$. We shall consistently use the following notations. The center of D will be denoted by K, and $K_0 = \{x \in K \mid x' = x\}$ is the set of elements of K fixed by the involution. We put $[D: K] = d^2$, $[K: \mathbf{Q}] = e$ and $[K_0: \mathbf{Q}] = e_0$ (so that $n = e.d^2$ and $e = e_0$ or $e = 2e_0$ according as the involution is trivial on K or not). Without further mention, we make use of the fact that the restriction of $\mathrm{Tr}_{D/\mathbf{Q}}$ to any simple subalgebra of $\mathbf{R} \otimes_{\mathbf{Q}} D$ is a positive multiple of the reduced trace over $\mathbf{R}$ of this subalgebra.

STEP I. Now, let $\sigma_i : K_0 \to \mathbf{R} (1 \leqslant i \leqslant r_1)$ be the set of distinct real imbeddings of K_0, and $\sigma_{r_1+j} : K_0 \to \mathbf{C}\ (1 \leqslant j \leqslant r_2)$ a set of complex imbeddings such that any non-real complex imbedding of K_0 in $\mathbf{C}$ is either a certain σ_{r_1+j} or a complex conjugate of some σ_{r_1+j}. Thus, $r_1 + 2r_2 = e_0$. We then have an isomorphism of $\mathbf{R}$-algebras

$$\sigma : \mathbf{R} \otimes_{\mathbf{Q}} K_0 \xrightarrow{\sim} \mathbf{R}^{r_1} \times \mathbf{C}^{r_2},$$

$$\sigma(1 \otimes x) = (\sigma_1(x), \ldots, \sigma_{r_1}(x), \sigma_{r_1+1}(x), \ldots, \sigma_{r_1+r_2}(x)).$$

Since the involution is the identity on K_0, for $x \in K_0^*$, we must have $\operatorname{Tr} x^2 > 0$, and the same must hold in $\mathbf{R} \otimes_{\mathbf{Q}} K_0$ also (in fact, this quadratic form has to be positive semi-definite on $\mathbf{R} \otimes_{\mathbf{Q}} K_0$ by continuity, and its null space, being the orthogonal complement of the whole space for this quadratic form, must be a rational subspace. But then, $\operatorname{Tr}(x.x') > 0$ for $x \in K_0$, $x \neq 0$, so that it has no null space). But this implies that $r_2 = 0$, as is trivially seen, so that K_0 is totally real.

If now $K \neq K_0$, $K = K_0(\sqrt{\alpha})$ for some $\alpha \in K_0$, $\sqrt{\alpha} \notin K_0$, and $(\sqrt{\alpha})' = -\sqrt{\alpha}$. Now, $\mathbf{R} \otimes_{\mathbf{Q}} K \simeq (\mathbf{R} \otimes_{\mathbf{Q}} K_0) \otimes_{K_0} K \simeq \prod_{i=1}^{e_0} \mathbf{R}_{(i)} \otimes_{K_0} K$ where $\mathbf{R}_{(i)}$ is $\mathbf{R}$ considered as a K_0-algebra via σ_i. Now, $\mathbf{R}_{(i)} \otimes_{K_0} K$ is isomorphic as an $\mathbf{R}$-algebra to either $\mathbf{R} \times \mathbf{R}$ or to $\mathbf{C}$ according as $\sigma_i(\alpha) > 0$ or $\sigma_i(\alpha) < 0$, and the restriction of the involution interchanges the factors in the first case and is complex conjugation in the second case. Again from the positive definiteness of $\operatorname{Tr}(x.x')$ on $\mathbf{R} \otimes_{\mathbf{Q}} K$, one deduces easily that $\mathbf{R} \times \mathbf{R}$ cannot occur as a factor, i.e., K is totally imaginary, and $\sigma_i(\alpha) < 0$ for all i. We shall say that the involution is of the *first kind* if $K = K_0$, and otherwise we say it is of the *second kind*.

STEP II. If the involution is of the first kind, the involution defines an isomorphism of D and its opposite algebra over the center K, so that its class in the Brauer group $\operatorname{Br}(K)$ of K is of order 1 or 2. If this order is one, we must have $D = K$. Next assume that the order is 2. Since by a theorem of Hasse-Brauer-Noether, the rank of a central division algebra over a number field is the square of its order in the Brauer group, D must be of rank 4 over K (i.e. a

so-called quaternion division algebra over K). In this case, there is a canonical involution $x \longmapsto x^*$ of D over K given by $x^* = \operatorname{Tr}^0_{D/K} x - x$ where Tr^0 is the reduced trace. (To check this is an involution, extend D to the algebraic closure of K, so that we are reduced to the case of a 2-by-2 matrix algebra over a field, when this is trivial to check.) By the theorem of Skolem-Noether, there is an $a \in D - \{0\}$ such that $x' = ax^*a^{-1}$ and the condition that $x'' = x$ gives us that $a^* = \epsilon . a$ with $\epsilon \in K^*$. But now, $a = a^{**} = (\epsilon.a)^* = \epsilon^2 a$, so that $\epsilon = \pm 1$.

Now, if $\epsilon = 1$, $a^* = \operatorname{Tr}_{D/K} a - a = a$, so that $a \in K$ and $x' = x^*$. We have an isomorphism

$$\mathbf{R} \otimes_{\mathbf{Q}} D \simeq (\mathbf{R} \otimes_{\mathbf{Q}} K) \otimes_K D \xrightarrow{\sim} (\mathbf{R}_{(1)} \otimes_K D) \times \ldots \times (\mathbf{R}_{(e)} \otimes_K D) \qquad (*)$$

where $\mathbf{R}_{(i)}$ is, as before, $\mathbf{R}$ considered as a K-algebra through the i-th imbedding σ_i, and each $\mathbf{R}_{(i)} \otimes_K D$ is $\mathbf{R}$-isomorphic to either the matrix algebra $M_2(\mathbf{R})$ or to the standard quaternion algebra $\mathbf{K}$ over $\mathbf{R}$. If factors of the type $M_2(\mathbf{R})$ occur, we would have that for any $A \in M_2(\mathbf{R})$, $A \neq 0$, $\operatorname{Tr}((\operatorname{Tr} A - A).A) > 0$, that is, $(\operatorname{Tr} A)^2 > \operatorname{Tr} A^2$, and this is false for $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Hence all the factors in the above decomposition of $\mathbf{R} \otimes_{\mathbf{Q}} D$ are isomorphic to $\mathbf{K}$ and the involution restricts on each factor to the canonical involution. Since for the standard involution on $\mathbf{K}$, we have $\operatorname{Tr}(x.x^*) > 0$ if $x \neq 0$, the conditions derived (when $\epsilon = 1$) are necessary and sufficient.

Next consider the case when $\epsilon = -1$. In the decomposition (*), let a_i be the image of a in $\mathbf{R}_{(i)} \otimes_K D = D_i$, so that on this factor, the involution takes the form $x \longmapsto a_i(\operatorname{Tr}_{D_i/\mathbf{R}} x - x)a_i^{-1}$, and we have also $a_i^* = \operatorname{Tr}_{D_i/\mathbf{R}} a_i - a_i = -a_i$, so $\operatorname{Tr}_{D_i/\mathbf{R}} a_i = 0$. Suppose now that D_i is $\mathbf{R}$-isomorphic to $\mathbf{K}$. Since $a_i a_i^*$ is real and positive, a_i satisfies an equation $x^2 + \lambda^2 = 0$, $\lambda \in \mathbf{R}^*$, and hence by Skolem-Noether, we can choose an isomorphism of $D_{(i)}$ with $\mathbf{K}$ such that a_i goes to $\lambda i \in \mathbf{K} = \mathbf{R} + \mathbf{R}i + \mathbf{R}j + \mathbf{R}k$. But then, if $x = x_0 + x_1 i + x_2 j + x_3 k$, we have $\operatorname{Tr}(x.x') = 2(x_0^2 + x_1^2 - x_2^2 - x_3^2)$ which

is not positive definite. Hence, each D_i is isomorphic to $M_2(\mathbf{R})$. Further, $K[a]$ is a subfield of D stable for the involution such that $a' = -a$, which shows that $a^2 \in K$ and a^2 is negative in every real imbedding of K. Thus, each a_i satisfies a minimal equation $a_i^2 = \lambda_i \in \mathbf{R}$ in $M_2(\mathbf{R})$ with $\lambda_i < 0$. Again by Skolem-Noether (or trivial checking) we can choose an isomorphism $\mathbf{R}_{(i)} \otimes_K D \simeq M_2(\mathbf{R})$ such that a_i goes to $\mu_i \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ with $\mu_i > 0$, $\mu_i \in \mathbf{R}$. But one checks that in this case, the involution on this factor is nothing but the transpose (in the sense of matrices), and we certainly have $\mathrm{Tr}(A.{}^tA) > 0$ for $A \in M_2(\mathbf{R})$, $A \neq 0$. Thus the conditions derived are necessary and sufficient for the positive definiteness of $\mathrm{Tr}(x.x')$.

STEP III. We come now to the case of an involution of the second kind. We summarize the results of class field theory concerning the Brauer groups of an algebraic number field and p-adic fields in the following theorem.

THEOREM. (1) *The Brauer group of a p-adic field is canonically isomorphic to $\mathbf{Q}/\mathbf{Z}$. If $L \supset K$ are two p-adic fields with $[L:K] = n$, the induced map $\mathrm{Br}(K) \to \mathrm{Br}(L)$ goes over by means of the above isomorphisms into multiplication by n in $\mathbf{Q}/\mathbf{Z}$.*

The Brauer group of $\mathbf{R}$ is cyclic of order two, and we identify it with the unique cyclic subgroup of order 2 of $\mathbf{Q}/\mathbf{Z}$.

The Brauer group of $\mathbf{C}$ is trivial.

(2) *For any central simple algebra D over an algebraic number field K, and any finite or infinite place v of K, if K_v denotes the completion of K at v, let $\mathrm{Inv}_v(K)$ denote the element of $\mathbf{Q}/\mathbf{Z}$ corresponding to the class of $D \otimes_K K_v$ in $\mathrm{Br}(K_v)$. Then we have an exact sequence*

$$0 \longrightarrow \mathrm{Br}(K) \longrightarrow \prod_v \mathrm{Br}(K_v) \longrightarrow \mathbf{Q}/\mathbf{Z} \longrightarrow 0$$

where the second map is gotten by forming the sum of the elements in $\mathbf{Q}/\mathbf{Z}$.

Let us now look at the involutorial division algebras of the second kind over $\mathbf{Q}$. Let σ be the restriction of the involution to K, so that σ induces an automorphism of $\mathrm{Br}(K)$. The existence of an involution of the second kind implies that $\sigma(\mathrm{cl}(D)) = -\mathrm{cl}(D)$, or equivalently, using the above theorem, that for any place v of K,

$$\mathrm{Inv}_v(D) + \mathrm{Inv}_{\sigma v}(D) = 0. \tag{A}$$

Since we have shown that K is totally imaginary, this condition is always fulfilled for infinite v. Suppose then that (A) holds, so that D is isomorphic to the opposite algebra to the conjugate algebra $D_{(\sigma)}$. This means that we can find a map $D \to D$, $x \longmapsto x^*$ such that for $\lambda \in K$, $(\lambda x)^* = \sigma(\lambda)x^*$, $(x+y)^* = x^* + y^*$ and $(xy)^* = y^*x^*$. By Skolem-Noether, any involution inducing σ on K must be of the form $x' = ax^*a^{-1}$ for some $a \in D$, $a \neq 0$. Since $x \longmapsto x^{**}$ is a K-automorphism of D, we must have $x^{**} = \alpha x \alpha^{-1}$ for some $\alpha \in D$, and since

$$\alpha x^* \alpha^{-1} = (x^*)^{**} = (x^{**})^* = (\alpha x \alpha^{-1})^* = \alpha^{*-1} x^* \alpha^*, \; x \in D,$$

we deduce that $\alpha^*\alpha \in K$, and since $(\alpha^*\alpha)^* = \alpha^*\alpha$, $\alpha^*\alpha \in K_0$. In order that $x \longmapsto x' = ax^*a^{-1}$ be an involution, we must have that $aa^{*-1}\alpha x \alpha^{-1} a^* a^{-1} = x$ for all $x \in D$, i.e., $a.a^{*-1}\alpha \in K$, or equivalently, $\alpha^{-1}a^* = \mu a$ for some $\mu \in K$. If we put $\phi(x) = \alpha^{-1}x^*$ for $x \in D$, then ϕ is σ-linear, and the solvability of $\phi(a) = \mu a$ with $a \neq 0$ implies that

$$(\alpha^*\alpha)^{-1} a = a(\alpha^*\alpha)^{-1} = \alpha^{-1}\alpha a \alpha^{-1}\alpha^{*-1} = \alpha^{-1}(\alpha^{-1}a^*)^* = \phi^2(a)$$
$$= \mu.\sigma\mu.a = \mathrm{Nm}_{K/K_0}\mu.a,$$

so that $\alpha^*\alpha \in \mathrm{Nm}_{K/K_0}K^*$. Conversely, if this holds, let $(\alpha^*\alpha)^{-1} = \mathrm{Nm}_{K/K_0}\lambda$, so that for any $x \in D$, if $a = \lambda x + \phi(x)$, we have

$$\phi(a) = \sigma(\lambda)\,\phi(x) + (\alpha^*\alpha)^{-1} x = \sigma(\lambda)\,(\lambda x + \phi(x)) = \sigma(\lambda).a.$$

Thus, under assumption (A), with * and α defined as above, the necessary and sufficient condition for the existence of an involution is that $\alpha^*\alpha \in \mathrm{Nm}_{K/K_0}K^*$. Since K/K_0 is a quadratic (hence cyclic) extension, this holds if and only if $\alpha^*\alpha$ is a norm in each $(K_0)_{v_0}$ from K_{v_0}, v_0 being any place of K_0, and K_{v_0} being the direct product of the completions of K at all places of K lying over v_0. If v_0 is

infinite and $\sigma_i : K_0 \to \mathbf{R}$ is the corresponding imbedding, $D \otimes_{K_0} \mathbf{R} = D \otimes_K (K \otimes_{K_0} \mathbf{R}) \simeq D \otimes_K \mathbf{C} \simeq M_d(\mathbf{C})$ and * extends to a map of $M_d(\mathbf{C})$ onto itself of the form $X^* = A \bar{X}^t A^{-1}$, $A \in GL(d, \mathbf{C})$. Hence $X^{**} = A.\bar{A}^{t-1}.X.\bar{A}^t.A^{-1}$, so that the image of α in $D \otimes_{K_0} \mathbf{R}$ is $\lambda A.\bar{A}^{t-1}$ for some $\lambda \in \mathbf{C}^*$, and $\alpha^*\alpha$ has for image $|\lambda|^2$ which is a norm from $\mathbf{C}$. Thus, it suffices to look at the Archimedean v_0. Again, if there are two extensions of v_0 to K, K_{v_0} is the direct product of two copies of $(K_0)_{v_0}$ as a $(K_0)_{v_0}$-algebra, so that the norm condition is vacuous.

Thus, we are left with the case of a v of K such that $\sigma v = v$. In this case, $\mathrm{Inv}_v(D) = 0$ or $\frac{1}{2}$ by (A). If $\mathrm{Inv}_v(D) = 0$, $D \otimes_K K_v$ is a matrix algebra over K_v and $A \longmapsto \sigma(A)^t$ is an involution of $D \otimes_K K_v$ inducing σ on K_v, so that, by the previous reasoning applied in the local case, $\alpha^*\alpha$ is a norm. Suppose now that $\mathrm{Inv}_v(D) = \frac{1}{2}$, so that $D_v = D \otimes_K K_v$ is a matrix algebra over the quaternion division algebra Q on K_v. Since σ induces the identity on $\mathrm{Br}(K_v)$ (see the theorem above), condition (A) gives us a σ-linear map $Q \to Q$, $X \longmapsto \hat{X}$, such that $\widehat{(XY)} = \hat{Y}\hat{X}$. If we put $\hat{\hat{X}} = \beta X \beta^{-1}$ for some $\beta \in Q$ and $X^* = A \hat{X}^t A^{-1}$ for all $X \in D_v$ and some $A \in D_v$, we see that upto a factor which is an element of the center, α equals $A \hat{A}^{t-1}\beta$, and $\alpha^*\alpha$ differs from

$$A.(A\hat{A}^{t-1}\beta)^{\wedge t}.A^{-1}(A\hat{A}^{t-1}\beta) = A(\hat{\beta}\hat{\hat{A}}^{-1}\hat{A}^t)\hat{A}^{t-1}\beta$$

$$= A.\hat{\beta}\hat{\hat{A}}^{-1}.\beta = \hat{\beta}\beta$$

by a factor in $\mathrm{Nm}_{K_v/K_{0v}}(K_v^*)$. Hence $\alpha^*\alpha$ is a norm in K_{0v} if and only if $\hat{\beta}\beta$ is, hence if and only if Q admits an involution inducing σ on K_v. Suppose $'$ is such an involution. Then we have (by the functoriality of trace) that $\mathrm{Tr}\, x' = \sigma(\mathrm{Tr}\, x)$, so that if i: $Q \to Q$ is the canonical involution of Q, $i(x') = i(x)'$. Thus $x \xrightarrow{\phi} i(x')$ is an automorphism ϕ of order two of Q inducing σ on K. If we put $Q_0 = \{x \in Q \mid \phi(x) = x\}$, Q_0 is a K_0-subalgebra of Q and $K_v \otimes_{K_{0v}} Q_0 \to Q$ is an isomorphism. But now, Q_0 is of rank four over K_{0v}, hence a quaternion algebra, and since $\mathrm{Br}(K_{0v}) \to \mathrm{Br}(K_v)$ is, by

means of the canonical isomorphisms with $\mathbf{Q}/\mathbf{Z}$, nothing but multiplication by 2, $Q = Q_0 \otimes_{K_{0v}} K_v$ is a matrix algebra over K_v, which is a contradiction.

Thus, if K_0 is a totally real field, K a purely imaginary quadratic extension of K and D a central division algebra on K, the necessary and sufficient condition for the existence of an involution of D inducing the non-trivial automorphism σ of K over K_0 is that besides (A), we also have

$$\mathrm{Inv}_v(D) = 0 \text{ if } \sigma v = v. \tag{B}$$

Step IV. Suppose then that (A) and (B) hold and let $x \longmapsto x^*$ be an involution. We shall then show that there are positive involutions too and we will classify them. For this, choose an isomorphism

$$D \otimes_{\mathbf{Q}} \mathbf{R} \xrightarrow{\sim} \overbrace{M_d(\mathbf{C}) \times M_d(\mathbf{C}) \times \ldots \times M_d(\mathbf{C})}^{e_0 \times}.$$

Then the given involution has an extension to the right side given by $(X_1, X_2, \ldots, X_{e_0}) \longmapsto (A_1 \bar{X}_1^t A_1^{-1}, \ldots, A_{e_0} \bar{X}_{e_0}^t A_{e_0}^{-1})$ with $\bar{A}_i^t = \eta_i A_i$, $\eta_i \in \mathbf{C}^*$, $A_i \in GL(d, \mathbf{C})$. We must have $|\eta_i| = 1$, and on replacing A_i by a scalar multiple, we may assume $\eta_i = 1$, so that $\bar{A}_i^t = A_i$. Hence, if $A = (A_1, \ldots, A_{e_0})$, we have $A^* = A$. The set of $A \in D \otimes_{\mathbf{Q}} \mathbf{R}$ with $A^* = A$ is of the form $V \otimes_{\mathbf{Q}} \mathbf{R}$ where V is a $\mathbf{Q}$-subspace of D, so that we can find an $\alpha \in V$ such that $\alpha \otimes 1$ is arbitrarily close to $A \in D \otimes_{\mathbf{Q}} \mathbf{R}$. The map $x \longmapsto x' = \alpha^{-1}x^*\alpha$ is again an involution of D whose extension to $M_d(\mathbf{C}) \times \ldots \times M_d(\mathbf{C})$ is arbitrarily close to $(X_1, \ldots, X_{e_0}) \longmapsto (\bar{X}_1^t, \ldots, \bar{X}_{e_0}^t)$. Hence for α a good enough approximation to A, $\mathrm{Tr}_{D/\mathbf{Q}}(x.x') > 0$ if $x \neq 0$, $x \in D$. On $M_d(\mathbf{C}) \times \ldots \times M_d(\mathbf{C})$, this involution is of the form

$$(X_1, \ldots, X_{e_0}) \longmapsto (A_1 \bar{X}_1^t A_1^{-1}, \ldots, A_{e_0} \bar{X}_{e_0}^t A_{e_0}^{-1}),$$

with A_i hermitian and close to I, so that the A_i are positive definite. Let B_i be a positive definite square root of A_i. Modifying the chosen isomorphism $D \otimes_{\mathbf{Q}} \mathbf{R} \xrightarrow{\sim} M_d(\mathbf{C}) \times \ldots \times M_d(\mathbf{C})$ by the inner automorphism given by $B = (B_1, \ldots, B_{e_0})$, we see that we

may assume that the extension of the involution to $M_d(\mathbf{C}) \times \ldots \times M_d(\mathbf{C})$ is the standard one

$$(X_1, \ldots, X_{e_0}) \longmapsto (\overline{X}_1^t, \ldots, \overline{X}_{e_0}^t),$$

which is certainly positive.

Thus, when (A) and (B) hold, we have found one positive involution on D and an isomorphism $D \otimes_{\mathbf{Q}} \mathbf{R} \xrightarrow{\sim} M_d(\mathbf{C}) \times \ldots \times M_d(\mathbf{C})$ such that the involution goes over into the standard one written above. Suppose $*$ is any other positive involution, so that $x^* = \alpha x' \alpha^{-1}$, $\alpha' = \lambda\alpha$ for some $\lambda \in K$. Since $\lambda.\lambda' = \mathrm{Nm}_{K/K_0}\lambda = 1$, we can write $\lambda = \dfrac{\sigma\mu}{\mu}$ for some $\mu \in K$, and when α is replaced by $\mu\alpha$, the involution is unchanged whereas the new α satisfies $\alpha' = \alpha$. Hence α goes over into $(A_1, \ldots, A_{e_0}) \in M_d(\mathbf{C}) \times \ldots \times M_d(\mathbf{C})$ with A_i hermitian. Positivity of $\mathrm{Tr}(x\,x^*)$ gives us the condition that $\mathrm{Tr}(X\,A_i\,\overline{X}^t\,A_i^{-1}) > 0$ for $X \in M_d(\mathbf{C})$, or equivalently, for some unitary U and any $X \in M_d(\mathbf{C})$,

$$\mathrm{Tr}(UXU^{-1}A_iU\overline{X}^tU^{-1}A_i^{-1}) = \mathrm{Tr}(XU^{-1}A_iU\overline{X}^tU^{-1}A_i^{-1}U) > 0.$$

Choose U so that $U^{-1}A_iU$ is real diagonal:

$$U^{-1}A_iU = \begin{bmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_d \end{bmatrix} = D_i.$$

We must then have $\mathrm{Tr}(X\,D\,\overline{X}^t\,D^{-1}) > 0$ for all $X \in M_d(\mathbf{C})$. But if $X = (x_{ij})$,

$$\mathrm{Tr}(X\,D\overline{X}^tD^{-1}) = \sum_{j,k=1}^{d} |x_{jk}|^2 \frac{\lambda_j}{\lambda_k},$$

so the condition is that D is positive definite or negative definite. Since we may replace α by $-\alpha$, this proves that all positive involutions are of the form $x \longmapsto \alpha x' \alpha^{-1}$ where the hermitian matrices A_i are positive definite.

Summarizing, we have

THEOREM 2. *Let D be a division algebra of finite rank over $\mathbf{Q}$ with an involution $'$ such that $\mathrm{Tr}_{D/\mathbf{Q}}(xx') > 0$ for $x \in D$, $x \neq 0$. Let K be the center of D and K_0 the subfield of elements of K fixed by $'$. Then $(D, ')$ is one of the following types.*

TYPE I. $D = K = K_0$ is a totally real algebraic number field and the involution is the identity.

TYPE II. $K = K_0$ is a totally real algebraic number field and D a quaternion division algebra over K (i.e. a central division algebra of rank 4 on K) such that for any imbedding $\sigma: K \to \mathbf{R}$,

$$\mathbf{R}_{(\sigma)} \otimes_K D \simeq M_2(\mathbf{R}).$$

Let $x^* = \mathrm{Tr}\ x - x$ be the standard involution of D and $a \in D$ such that $a^2 \in K$ and a^2 is totally negative. Then the involution is of the form $x' = a\,x^*a^{-1}$, and conversely, any such map is a positive involution. For any such involution, we can choose an isomorphism

$$\mathbf{R} \otimes_{\mathbf{Q}} D \xrightarrow{\sim} M_2(\mathbf{R}) \times \ldots \times M_2(\mathbf{R}) \quad (e = [K: \mathbf{Q}] \text{ factors})$$

such that the involution extended to the right side by $\mathbf{R}$-linearity is given by $(X_1, \ldots, X_e) \to (X_1^t, \ldots, X_e^t)$.

TYPE III. $K = K_0$ is a totally real algebraic number field and D a quaternion division algebra over K such that for any imbedding $\sigma: K \to \mathbf{R}$,

$$\mathbf{R}_{(\sigma)} \otimes_K D \simeq \mathbf{K},$$

where $\mathbf{K}$ is the standard algebra of quaternions on $\mathbf{R}$. In this case the involution $'$ is the standard one, $x' = \mathrm{Tr}_{D/K}x - x$, and there is an isomorphism

$$\mathbf{R} \otimes_{\mathbf{Q}} D \xrightarrow{\sim} \mathbf{K} \times \ldots \times \mathbf{K},$$

carrying the involution into the product of the standard involutions in each factor $\mathbf{K}$.

TYPE IV. K_0 is a totally real algebraic number field, K a totally imaginary quadratic extension of K_0 with conjugation σ over K_0. Then D is a division algebra with center K such that (i) if v is a finite place fixed by σ, $\mathrm{Inv}_v(D) = 0$, and (ii) for any finite place v of K, $\mathrm{Inv}_v(D) + \mathrm{Inv}_{\sigma v}(D) = 0$.

In this case, there exist totally positive involutions $x \longmapsto x'$ and isomorphisms

$$\mathbf{R} \otimes_{\mathbf{Q}} D \xrightarrow{\sim} M_d(\mathbf{C}) \times \ldots \times M_d(\mathbf{C})$$

which carry the involution into the standard involution $(X_1, \ldots, X_{e_0}) \longmapsto (\overline{X}_1^t, \ldots, \overline{X}_{e_0}^t)$. Given one such $'$, any other positive involution $*$ of D is of the form $x^* = a\, x'\, a^{-1}$ with $a \in D$, $a' = a$ and such that the image of $1 \otimes a$ by the above isomorphism is of the form $(A_1, \ldots, A_{e_0})$ with A_i hermitian positive definite.

The following table gives the numerical invariants in all four types, and also indicates the restrictions on these invariants when $D = \mathrm{End}^0 X$ where X is a simple g-dimensional abelian variety. The symbols e, e_0, and d have the same significance as before, and $S = \{x \in D \mid x' = x\}$ and $\eta = \dfrac{\dim_{\mathbf{Q}} S}{\dim_{\mathbf{Q}} D}$.

Type	e	d	η	Restriction in char 0 when $D = \mathrm{End}^0 X$, $\dim X = g$	Restriction in char p > 0 when $D = \mathrm{End}^0 X$ $\dim X = g$
I	e_0	1	1	$e \mid g$	$e \mid g$
II	e_0	2	$\frac{3}{4}$	$2e \mid g$	$2e \mid g$
III	e_0	2	$\frac{1}{4}$	$2e \mid g$	$e \mid g$
IV	$2e_0$	d	$\frac{1}{2}$	$e_0 d^2 \mid g$	$e_0 d \mid g$

Excepting the indicated restrictions, all the assertions contained in the table have been proved. As for the restrictions, they are immediate consequences of the three divisibility results established earlier, viz. (i) in char 0, $\dim D \mid 2 \dim X$, (ii) in char $p > 0$, $ed \mid 2 \dim X$, and (iii) if L is a subfield of D whose elements are fixed by the involution, $[L\colon \mathbf{Q}] \mid g$.

One might ask to what extent the conditions derived above on the endomorphism rings of a simple abelian variety are complete, that is, given a division algebra of one of the four types and an integer g fulfilling the restrictions imposed

above, whether there exists a simple abelian variety of dimension g having the given algebra as endomorphism algebra. In characteristic zero at least, the answer is known and is due to Albert. The result is that there always exists such an X, excepting when D is of type III or IV *and* the quotient $g/2e$ in the first case and $g/e_0 d^2$ in the second case is 1 or 2. Even in these exceptional cases, it is known what further restrictions ensure the existence of an X (cf. Shimura, [Sh], esp. §4). On the other hand, not much seems to be known in positive characteristics.

APPLICATION II. THE RIEMANN HYPOTHESIS.

We first prove the

PROPOSITION. *Let X be an abelian variety, $'$ the Rosati involution on* $\mathrm{End}^0 X$ *defined by some ample line bundle and* $\alpha \in \mathrm{End}\, X$ *such that* $\alpha' \alpha = a \in \mathbf{Z}$. *Let* $\omega_1, \ldots, \omega_{2g}$ *be the roots (in* $\mathbf{C}$*) of the characteristic polynomial P of α. Then the subalgebra* $\mathbf{Q}[\alpha] \subset \mathrm{End}\, X$ *generated by α is semi-simple, and*

(i) $|\omega_i|^2 = a$ *for all* i;

(ii) *the map* $\omega_i \to \dfrac{a}{\omega_i}$ *is a permutation of the roots* ω_i.

PROOF. Note that (ii) is an immediate consequence of (i) since $\dfrac{a}{\omega_i} = \overline{\omega}_i$ and P is an integral polynomial. Next, let $Q(X)$ be the minimal polynomial over $\mathbf{Q}$ of α (as an element in $\mathrm{End}\, X$). I claim that P and Q have the same complex roots. In fact, since P has integral coefficients, and $P(\alpha) = 0$, $Q \mid P$. But also P is the characteristic polynomial of $T_l(\alpha)$ in the matrix representation

$$T_l\colon \mathrm{End}(X) \longrightarrow \mathrm{End}(T_l X).$$

If $\omega \in \overline{\mathbf{Q}}_l$ (algebraic closure of $\mathbf{Q}_l$) is a root of P, then ω is an eigenvalue of $T_l(\alpha)$, hence $Q(\omega)$ is an eigenvalue of $T_l(Q(\alpha))$. But $T_l(Q(\alpha)) = 0$, so $Q(\omega) = 0$, i.e. all roots of P in $\overline{\mathbf{Q}}_l$ are roots of Q. Therefore $P \mid Q^n$ for some n, and P and Q have the same complex roots too.

The restriction S of the trace on End^0X to $\mathbf{Q}[\alpha]$ is a trace form on $\mathbf{Q}[\alpha]$ satisfying $S(X.X') > 0$ if $X \in \mathbf{Q}[\alpha]$, $X \neq 0$. Further, since α is invertible in End^0X and $\mathbf{Q}[\alpha]$ is finite-dimensional, it follows that $\alpha^{-1} \in \mathbf{Q}[\alpha]$. Hence $\alpha' = a/\alpha \in \mathbf{Q}[\alpha]$, so $\mathbf{Q}[\alpha]$ is stable for the involution. If $\mathfrak{A} \subset \mathbf{Q}[\alpha]$ is any ideal in $\mathbf{Q}[\alpha]$, and $\mathfrak{b}$ is its orthogonal complement in $\mathbf{Q}[\alpha]$ for the quadratic form $S(X.X')$, $\mathfrak{b}$ is again an ideal and $\mathfrak{A} \cap \mathfrak{b} = (0)$, $\mathfrak{A} \oplus \mathfrak{b} = \mathbf{Q}[\alpha]$. Thus $\mathbf{Q}[\alpha]$ is semisimple, hence isomorphic to $K_1 \times K_2 \times \ldots \times K_p$ where K_i are algebraic number fields. The involution, being an automorphism of $\mathbf{Q}[\alpha]$, permutes the factors K_i. But since $S(X.X') > 0$ for every $X \neq 0$, the involution must take each K_i onto itself, and therefore S is a trace form on each K_i over $\mathbf{Q}$ with $S(X.X') > 0$ if $X \neq 0$. Hence each K_i is either totally real with identity involution or is a totally imaginary quadratic extension of a totally real subfield with complex conjugation for involution. Now, the roots ω of the minimal polynomial of α are precisely the images of α under the various imbeddings ϕ_j of the K_i in $\mathbf{C}$. Since $\phi_j(x') = \overline{\phi_j(x)}$ for all $x \in \mathbf{Q}[\alpha]$, it follows that

$$a = \phi_j(a) = \phi_j(\alpha'.\alpha) = |\phi_j(\alpha)|^2.$$

We shall apply this proposition to obtain a proof of the Riemann hypothesis on abelian varieties over finite fields. Let $\mathbf{F} = \mathbf{F}_q$ be a finite field with $q = p^f$ elements, and X_0 a scheme of finite type over $\mathbf{F}$. (We do not consider X_0 as a variety whose points are geometric points with values in an algebraically closed field, but as a scheme in Grothendieck's sense.) We define the *Frobenius morphism on* X_0, $\pi_0: X_0 \to X_0$, to be the identity on the underlying space together with the homomorphism $\mathcal{O}_{X_0} \to \mathcal{O}_{X_0}$ of structure sheaves given by $f \longmapsto f^q$. Note that this is a homomorphism of sheaves of $\mathbf{F}$-algebras since $\lambda^q = \lambda$ for $\lambda \in \mathbf{F}$, so π_0 is a morphism over Spec $\mathbf{F}$. Now let k be the algebraic closure of $\mathbf{F}_q$, and let X be the k-scheme $X = k \otimes_{\mathbf{F}} X_0$. The morphism $\pi: X \to X$ obtained from π_0 by base extension is called the *Frobenius morphism on* X, relative to $\mathbf{F}$ and to X_0. Let us see what this looks like on the geometric (or closed) points of X. Suppose that $X_0 = \mathrm{Spec}\ A$, where

$A = \mathbf{F}[X_1, \ldots, X_m]/\mathfrak{A}$, so that X_0 is embedded as a closed subscheme in $\mathbf{A}_{\mathbf{F}}^m$, and the closed points of X can be considered as elements of the set k^m. The morphism π_0 is defined by the homomorphism of $\mathbf{F}$-algebras $A \to A$ sending $\overline{X_i}$ into $\overline{X_i^q}$, so that if $(x_1, \ldots, x_m)$ is a geometric point of X, π maps it into the point $(x_1^q, \ldots, x_m^q)$. In particular, a point $(x_1, \ldots, x_m)$ is fixed by π^n if and only if $x_i^{q^n} = x_i$, i.e. if and only if x_i is a rational point over the field $\mathbf{F}_{q^n}$ with q^n elements. Further, the Frobenius morphism has the functorial property that if $f: X_0 \to Y_0$ is a morphism of $\mathbf{F}$-schemes and π_{0,X_0} and π_{0,Y_0} are the Frobenius maps of X_0 and Y_0, respectively, $\pi_{0,Y_0} \circ f = f \circ \pi_{0,X_0}$. Finally, it is clear that the map induced on tangent spaces by π at any point of X is 0, since $D(f^q) = 0$ for any derivation D of a ring A of characteristic p and $f \in A$.

THEOREM 3. (Lang.) *Let X_0 be a scheme over $\mathbf{F}_q$ such that $X = k \otimes_{\mathbf{F}} X_0$ is an abelian variety. Then X_0 has at least one point rational over $\mathbf{F}_q$.*

PROOF. If π is the Frobenius morphism, then π must have the form $\pi(x) = x_0 + f(x)$ for some closed point $x_0 \in X$ and some endomorphism f of X. Then $1 - f$ is an endomorphism of X. Since π and hence f induce the zero map on the tangent space at 0, $1 - f$ induces the identity on this tangent space. Therefore $\ker(1-f)$ is 0-dimensional and $1 - f$ is surjective. Then if $(1-f)(x_1) = x_0$, it follows that $x_1 = x_0 + f(x_1) = \pi(x_1)$, hence x_1 is rational over $\mathbf{F}_q$.

Therefore, if X is an abelian variety, by choosing an appropriate origin $0 \in X$, we can always assume that 0 is $\mathbf{F}$-rational. Then each π^n fixes 0 and is therefore an endomorphism of X. Moreover, $1 - \pi^n$ induces the identity on the tangent space at 0, so it is also a separable endomorphism. Hence we obtain:

$$N_n \underset{\text{def}}{=} \text{Number of } \mathbf{F}_{q^n}\text{-rational points of } X = \#(\mathrm{Ker}(1 - \pi^n)) = \deg(1 - \pi^n).$$

But if $\omega_1, \ldots, \omega_{2g}$ are the roots of the characteristic polynomial of π, then the characteristic polynomial $P_n(t)$ of π^n, for all n, is $\prod_{i=1}^{2g}(t - \omega_i^n)$. Since $\deg(1 - \pi^n) = P_n(1)$, it follows that

$$N_n = \prod_{i=1}^{2g} (1 - \omega_i^n).$$

We now wish to show $|\omega_i| = \sqrt{q}$: this is the Riemann hypothesis. Since it suffices to prove that $|\omega_i^m| = \sqrt{q^m}$ for some m, we may replace $\mathbf{F}_q$ by $\mathbf{F}_{q^m}$, X_0 by $\mathbf{F}_{q^m} \otimes_{\mathbf{F}} X_0$ and π by π^m if necessary. By doing this, we can assume that there is a line bundle L_0 on X_0 such that $L = k \otimes_{\mathbf{F}} L_0$ is ample on X (since any line bundle on X is of this form for suitably large m). Denoting by $'$ the Rosati involution with respect to L, we shall prove that

(i) $$\pi' \circ \pi = q,$$

so that the proposition applies. But by the definition of $'$ this means that

(ii) $$\hat{\pi}(\phi_L(\pi(x))) = q\phi_L(x), \quad \text{all } x \in X.$$

But π_0 acts on $\mathcal{O}_{X_0}$ by $f \longmapsto f^q$, so it follows that $\pi_0^* L_0 \simeq L_0^q$. Therefore $\pi^* L \simeq L^q$ and

(iii) $$\begin{aligned} \pi^*(T_{\pi x}^* L \otimes L^{-1}) &\simeq T_x^* \pi^* L \otimes (\pi^* L)^{-1} \\ &\simeq (T_x^* L \otimes L^{-1})^{\otimes q}. \end{aligned}$$

Since the line bundle on the left represents $\hat{\pi}(\phi_L(\pi(x)))$ and the line bundle on the right represents $q.\phi_L(x)$, (ii) and hence (i) are correct.

We summarize our conclusions in

THEOREM 4. (Weil.) *Let X_0 be a scheme over $\mathbf{F}_q$ such that $X = k \otimes_{\mathbf{F}} X_0$ is an abelian variety. Let N_n = the number of points of X rational over $\mathbf{F}_{q^n}$. Then*

$$N_n = \prod_{i=1}^{2g} (\omega_i^{2g^n} - 1)$$

where $\omega_i \in \mathbf{C}$ and they satisfy

(i) $|\omega_i| = \sqrt{q}$,

(ii) $\omega_{ni} = q/\omega_i$ *for some permutation* π.

COROLLARY. *For some constant C, $|N_n - q^{ng}| \leqslant C.\, q^{n(g-\frac{1}{2})}$ for all n.*

Another application of the proposition is

THEOREM 5. (Serre.) *For any $n \geqslant 3$, and any L ample on an abelian variety X, the restriction homomorphism*

$$\left\{ \alpha \in \operatorname{Aut} X \,\middle|\, \alpha^* L \simeq L \otimes \begin{pmatrix} \text{something} \\ \text{in } \operatorname{Pic}^0 X \end{pmatrix} \right\} \longrightarrow \operatorname{Aut}(X_n)$$

is injective (here X_n = scheme-theoretic kernel of n_X).

PROOF. If $\alpha^* L \simeq L \otimes \begin{pmatrix} \text{something} \\ \text{in } \operatorname{Pic}^0 X \end{pmatrix}$, then $\phi_{\alpha^* L} = \phi_L$, hence $\hat{\alpha} \circ \phi_L \circ \alpha = \phi_L$. This means that for the Rosati involution defined by L, $\alpha' \alpha = 1$. Hence by the proposition the roots of the characteristic polynomial of α are algebraic integers all of whose conjugates have absolute value 1, and hence are all roots of unity.

Suppose now that α restricts to the identity on some $X_n (n \geqslant 3)$. Then the restriction of $\alpha - 1$ to X_n is 0, so that $(\alpha - 1) = n\beta$ for some $\beta \in \operatorname{End} X$. We deduce that if ω is any characteristic root of α, $\omega - 1 = n\eta$ where η is an algebraic integer. We now have the

LEMMA. *If ω is a root of unity such that $\omega = 1 + n\eta$ where n is a rational integer $\geqslant 3$ and η an algebraic integer, then $\omega = 1$.*

PROOF. If not, by raising ω to a suitable power, we may assume that ω is a primitive p-th root of unity for a prime p. Taking norms over $\mathbf{Q}$ in the equation $\omega - 1 = n\eta$, we obtain

$$\prod_{i=1}^{p-1} (1 - \omega^i) = n^{p-1}.N,$$

where $N = (-1)^{p-1} \operatorname{Nm} \eta$ is a rational integer. But the left side is the derivative at $X = 1$ of $X^p - 1 = \prod_{i=0}^{p-1} (X - \omega^i)$, that is, p. Hence n^{p-1} divides p, which is impossible if $n \geqslant 3$.

Applying the lemma, we deduce that the characteristic roots of α are all 1, so that $1 - \alpha$ is nilpotent. But by the proposition, $\mathbf{Q}[\alpha]$ is semi-simple, so it has no nilpotent elements. Thus $\alpha = 1$.

APPLICATION III. STRUCTURE OF $NS^0(X)$.

Let X be an abelian variety and let $NS^0(X) = NS(X) \otimes \mathbf{Q}$. As in § 20, if we fix an ample L on X, then we can identify

$$NS^0(X) \xrightarrow[\rho]{\sim} \{\alpha \in \mathrm{End}^0 X \mid \alpha' = \alpha\}.$$

In particular, $NS^0(X)$ has a natural structure of Jordan algebra over $\mathbf{Q}$ if we define

$$\alpha \circ \beta = \tfrac{1}{2}\rho^{-1}(\rho(\alpha)\rho(\beta) + \rho(\beta)\rho(\alpha)),\ \alpha, \beta \in NS^0(X),$$

using composition in $\mathrm{End}^0 X$. What can we say about this Jordan algebra? First of all, the fact that $\mathrm{Tr}(\rho(\alpha)^2) > 0$, all $\alpha \in NS^0(X)$, $\alpha \neq 0$, implies immediately that $NS^0(X)$ is *formally real*, i.e.

$$\sum_{i=1}^{n} \alpha_i \circ \alpha_i = 0 \Rightarrow \alpha_1 = \ldots = \alpha_n = 0$$

(cf. Braun, Koecher, [B-K] Ch. 11, § 3). Now the formally real Jordan algebras over $\mathbf{R}$ have been classified: cf. Braun, Koecher, Ch. 11, § 5. In our case, we do not get all possible such algebras by forming $NS^0(X) \otimes \mathbf{R}$. In fact, we have

THEOREM 6. *$NS^0(X) \otimes \mathbf{R}$ is isomorphic to a product of Jordan algebras of the types:*

$\mathscr{H}_r(\mathbf{R})$ $= r \times r$ *symmetric real matrices*

$\mathscr{H}_r(\mathbf{C})$ $= r \times r$ *Hermitian complex matrices*

$\mathscr{H}_r(\mathbf{K})$ $= r \times r$ *Hermitian quaternionic matrices, i.e.* ${}^t\overline{X} = X$, *where* $x \to \bar{x}$ *is the standard involution on* $\mathbf{K}$.

PROOF. Decompose $\mathrm{End}^0(X) \otimes \mathbf{R}$ into a product of copies of $M_n(\mathbf{R})$, $M_n(\mathbf{C})$ and $M_n(\mathbf{K})$. Then $NS^0(X) \otimes \mathbf{R}$ is isomorphic to the set of fixed points here under a positive involution. But it is easy to check that every such involution (a) fixes each of the factors $M_n(K)$, $K = \mathbf{R}$, $\mathbf{C}$ or $\mathbf{K}$, and (b) by inner automorphism of each factor, can be put in the standard form $X \to {}^t\overline{X}$. [Cf. the proof of Theorem 2, Step IV, for the case $K = \mathbf{C}$; the other cases are analogous. One checks first that every positive involution of $M_n(K)$ is of the form $X \longmapsto A \cdot {}^t\overline{X} \cdot A^{-1}$ where ${}^t\bar{A} = A$. One then

checks that $A = U \cdot D \cdot U^{-1}$ where D is diagonal with real entries either all positive or all negative and ${}^t\overline{U} = U^{-1}$. Finally, solve $\pm D = E^2$ and use the inner automorphism defined by UEU^{-1} to put the involution in standard form.]

Fix isomorphisms ϕ and ψ:

$$\begin{array}{ccc} \text{(I)}\quad \mathrm{End}^0(X) \otimes \mathbf{R} & \xrightarrow[\phi]{\sim} & \prod M_{r_i}(\mathbf{R}) \times \prod M_{s_i}(\mathbf{C}) \times \prod M_{t_i}(\mathbf{K}) \\ \uparrow \rho & & \cup \\ NS^0(X) \otimes \mathbf{R} & \xrightarrow[\psi]{\sim} & \prod \mathscr{H}_{r_i}(\mathbf{R}) \times \prod \mathscr{H}_{s_i}(\mathbf{C}) \times \prod \mathscr{H}_{t_i}(\mathbf{K}). \end{array}$$

What happens to the polynomial function $\chi\colon NS^0(X) \otimes \mathbf{R} \to \mathbf{R}$? For any $x \in \mathrm{End}^0(X) \otimes \mathbf{R}$, let $\phi_{i,1}(x)$, $\phi_{i,2}(x)$, $\phi_{i,3}(x)$ denote the components of $\phi(x)$ in the above decomposition. Then we know that the function "degree" can be written

$$\text{(II)}\quad \deg(x) = \prod \det(\phi_{i,1}x)^{a_i} \cdot \prod |\det(\phi_{i,2}x)|^{2b_i} \cdot \prod \mathrm{Nm}(\phi_{i,3}x)^{c_i}$$

where $\mathrm{Nm}\colon M_t(\mathbf{K}) \to \mathbf{R}$ is the reduced norm (the multiplicative polynomial of degree $2t$). Now on $NS(X)$, $\deg(\rho x) = \alpha \cdot \chi(x)^2$ for some constant α. It follows that the a_i are even and that the function χ can be written

$$\text{(III)}\quad \chi(x) = \mathrm{const.} \prod \det(\psi_{i,1}x)^{a_i/2} \cdot \prod \det(\psi_{i,2}x)^{b_i} \cdot \prod \mathrm{HNm}(\psi_{i,3}x)^{c_i}$$

all $x \in NS^0(X) \otimes \mathbf{R}$. Note that $\psi_{i,2}(x)$ is Hermitian, so its complex determinant is real. Here "HNm" is the "Haupt norm" of Braun-Koecher (Ch. 2. §4), a polynomial function of degree t from $\mathscr{H}_t(\mathbf{K})$ to $\mathbf{R}$. If $\lambda_0 \in NS^0(X) \otimes \mathbf{R}$ is the point defined by the ample L on X used to set up ρ, then $\rho(\lambda_0) = 1$, so $\psi_{i,j}(\lambda_0) = I$, so the constant in the above formula is $\chi(\lambda_0)$. Using the results of §16, it follows finally that:

(IV) If $\chi(x) \neq 0$, then

$$i(x) = \sum \frac{a_i}{2} \begin{pmatrix} \#\text{ neg. eigenvalues} \\ \text{of } \psi_{i,1}\,x \end{pmatrix} + \sum b_i \begin{pmatrix} \#\text{ neg. eigenvalues} \\ \text{of } \psi_{i,2}\,x \end{pmatrix} + \sum c_i \begin{pmatrix} \#\text{ neg. eigenvalues} \\ \text{of } \psi_{i,3}\,x \end{pmatrix}.$$

(The eigenvalues of a quaternionic Hermitian matrix H are defined as the entries of a diagonal matrix D such that $H = U \cdot D \cdot U^{-1}$, and ${}^t\overline{U} = U^{-1}$.) Since ample line bundles L are characterized by $\chi(L) \neq 0$, $i(L) = 0$, it follows from (III) and (IV) that the images of the ample line bundles in $NS(X)$ are exactly the totally positive elements of the formally real Jordan algebra $NS^0(X) \otimes \mathbf{R}$.

22. Examples.

FIRST EXAMPLE: ABELIAN VARIETIES OF CM-TYPE OVER $\mathbf{C}$.

Let X be a simple g-dimensional abelian variety, $D = \mathrm{End}^0(X)$, $K =$ center of D, $d^2 = [D:K]$ and $e = [K:\mathbf{Q}]$. Recall that $ed \mid 2g$ and that we have called X of *CM*-type if $ed = 2g$. We wish to classify these when $k = \mathbf{C}$. A glance at the table in §20 giving the types of division algebras D tells us that we must have $K = D$, K a totally imaginary quadratic extension of a totally real field K_0 of degree g over $\mathbf{Q}$.

We pose the problem a little differently. Suppose we are given a totally real number field K_0 of degree g over $\mathbf{Q}$ and a totally imaginary quadratic extension K of K_0. We consider all pairs (i, X) where X is an abelian variety over $\mathbf{C}$ of dimension g and $i: K \to \mathrm{End}^0 X$ is an imbedding of the field K in the ring $\mathrm{End}^0 X$. We define two such pairs (i, X) and (j, Y) to be equivalent if there is an isogeny $\alpha: X \to Y$ such that if $\tilde{\alpha}: \mathrm{End}^0 X \xrightarrow{\sim} \mathrm{End}^0 Y$ is the induced isomorphism, we have $\tilde{\alpha} \circ i = j$. It is easily checked that this is an equivalence relation. Our object is to exhibit a complete set of representatives for the equivalence classes.

Let (i,X) be any such pair, V the tangent space of X at 0 and U the kernel of the exponential map from V to X, so that we have a natural isomorphism $V/U \xrightarrow{\sim} X$. Then $\mathrm{End}\, X$ acts faithfully as a ring of $\mathbf{C}$-endomorphisms of the vector space V, leaving U stable. Thus, if we put $i^{-1}(\mathrm{End}\, X) = A \subset K$, A is an order (i.e. a finitely generated subring of maximal rank) in K and U becomes an A-module. Thus, $\mathbf{Q}.U \subset V$ becomes a vector space over $\mathbf{Q} \otimes_{\mathbf{Z}} A = K$, and since both K and $\mathbf{Q}.U$ are of dimension $2g$ over $\mathbf{Q}$, $\mathbf{Q}.U$ is a one-dimensional K-vector space. Hence, if we choose a non-zero element $u_0 \in U$, the map $\phi: A \to U$ defined by $a \longmapsto a.u_0$ is an injection of A into U, such that the index $[U:\phi(A)] < +\infty$. Changing X by an isogeny, we can first shrink U so that $U = \phi(A)$, and then increase U so that $U = \phi(A_0)$, $A_0 =$ ring of integers in K. Next, the map ϕ extends to an $\mathbf{R}$-linear map which we still denote by ϕ:

$$\mathbf{R} \otimes_{\mathbf{Q}} K = \mathbf{R} \otimes_{\mathbf{Z}} A_0 \xrightarrow{\phi} \mathbf{R} \otimes_{\mathbf{Z}} U = V.$$

It follows that ϕ defines an isomorphism between the *real* tori:

$$(\mathbf{R} \otimes_{\mathbf{Q}} K)/A_0 \xrightarrow{\approx} V/U = X.$$

Note that if $a \in A_0$, then this isomorphism has been set up exactly so that the endomorphism $i(a): X \to X$ corresponds to multiplication by $1 \otimes a$ in $\mathbf{R} \otimes_{\mathbf{Q}} K$.

Next, let Φ denote the complex structure on the real vector space $\mathbf{R} \otimes_{\mathbf{Q}} K$ obtained by pulling back the complex structure on V via ϕ. Since multiplication by $1 \otimes a$ in $\mathbf{R} \otimes_{\mathbf{Q}} K (a \in A_0)$ goes over via ϕ to a complex-linear map from V to V, it follows that in the complex structure Φ, multiplication by $1 \otimes a$ is complex-linear too. In other words, Φ actually makes the $\mathbf{R}$-algebra $\mathbf{R} \otimes_{\mathbf{Q}} K$ into a $\mathbf{C}$-algebra as well as a $\mathbf{C}$-vector space. We now invert this whole construction.

DEFINITION. *If K is as above, $A_0 =$ integers in K, and Φ is a structure of $\mathbf{C}$-algebra on $\mathbf{R} \otimes_{\mathbf{Q}} K$, then let*

$$X(K, \Phi) = \text{the complex torus } \mathbf{R} \otimes_{\mathbf{Q}} K / A_0,$$

and let $i_\Phi : A_0 \to \mathrm{Hom}_{\substack{\text{complex} \\ \text{tori}}}(X(K,\Phi), X(K,\Phi))$ be given by $i_\Phi(a) =$ map induced by mult. by $1 \otimes a$.

We have shown that for given K as above, and any pair (i, X), there is a structure Φ of complex algebra on the real algebra $\mathbf{R} \otimes_{\mathbf{Q}} K$ such that (i, X) is equivalent to $(i_\Phi, X(K, \Phi))$. Our next aim is to show that (i) for any structure Φ of complex algebra on $\mathbf{R} \otimes_{\mathbf{Q}} K$, $X(K, \Phi) = \mathbf{R} \otimes_{\mathbf{Q}} K / 1 \otimes A_0$ is an abelian variety, and (ii) for

different complex structures Φ_1 and Φ_2 on $\mathbf{R}\otimes_{\mathbf{Q}}K$, $(i_{\Phi_1}, X(K,\Phi_1))$ and $(i_{\Phi_2}, X(K,\Phi_2))$ are not equivalent.

To prove (i), let us look more closely at a structure Φ of complex algebra on $\mathbf{R}\otimes_{\mathbf{Q}}K$. Giving such a Φ is equivalent to giving a homomorphism $\tilde{\Phi}$ of $\mathbf{R}$-algebras, $\tilde{\Phi}\colon \mathbf{C} \to \mathbf{R}\otimes_{\mathbf{Q}}K$. Now, if $\sigma_i (1 \leqslant i \leqslant g)$ are the distinct embeddings of K_0 in $\mathbf{R}$, we have an isomorphism of $\mathbf{R}$-algebras

$$\mathbf{R}\otimes_{\mathbf{Q}}K \xrightarrow{\sim} (\mathbf{R}_{(1)}\otimes_{K_0}K) \times (\mathbf{R}_{(2)}\otimes_{K_0}K) \times \ldots \times (\mathbf{R}_{(g)}\otimes_{K_0}K),$$

$$\lambda\otimes\alpha \longmapsto (\lambda\otimes\alpha,\ \lambda\otimes\alpha,\ \ldots,\ \lambda\otimes\alpha),$$

where $\mathbf{R}_{(i)}$ is $\mathbf{R}$ considered as a K_0-algebra through σ_i. Thus, giving an $\mathbf{R}$-algebra homomorphism $\tilde{\Phi}\colon \mathbf{C}\to\mathbf{R}\otimes_{\mathbf{Q}}K$ is in turn equivalent to giving $\mathbf{R}$-algebra *isomorphisms* $\Phi_i\colon \mathbf{C}\xrightarrow{\sim}\mathbf{R}_{(i)}\otimes_{K_0}K$ for $1\leqslant i\leqslant g$. For each i, there are clearly two such possible $\mathbf{R}$-isomorphisms $\mathbf{C}\to\mathbf{R}_{(i)}\otimes_{K_0}K$. Thus, we see that there are exactly 2^g possible Φ on $\mathbf{R}\otimes_{\mathbf{Q}}K$, and each Φ is uniquely determined by giving the corresponding $\mathbf{R}$-isomorphisms $\Phi_i\colon \mathbf{C}\to\mathbf{R}_{(i)}\otimes_{K_0}K$ $(1\leqslant i\leqslant g)$. Let $\tau_i\colon \mathbf{R}_{(i)}\otimes_{K_0}K\to\mathbf{C}$ be the inverse of Φ_i, so that τ_i restricted to $K\simeq 1\otimes K\subset\mathbf{R}_{(i)}\otimes_{K_0}K$ is an imbedding of K in $\mathbf{C}$ extending the imbedding σ_i of K_0 in $\mathbf{R}$. We can choose an element $\alpha\in K$ such that $\alpha^2\in K_0$ and $\tau_i(\alpha)=i\beta_i$, $\beta_i\in\mathbf{R}$, $\beta_i>0$. In fact, if $K=K_0(\sqrt{\delta})$ then $\tau_i(\sqrt{\delta})=i\gamma_i$ with $\gamma_i\in\mathbf{R}^*$, and we can find $\eta\in K_0$ such that $\sigma_i(\eta)$ has the same sign as γ_i, and we can take $\alpha=\eta\sqrt{\delta}$. We may further assume α to be an algebraic integer. If $\tau_i(\alpha)=i\beta_i$ $(1\leqslant i\leqslant g)$, we define a Hermitian form H on $(\mathbf{R}\otimes_{\mathbf{Q}}K,\Phi)$ by putting

$$H(x,y)=2\sum_{i=1}^{g}\beta_i\,\tau_i(x)\,\overline{\tau_i(y)},\quad x,y\in\mathbf{R}\otimes_{\mathbf{Q}}K.$$

This form is clearly positive definite, and we shall show that $\operatorname{Im} H$ is integral on the lattice A_0. In fact, for $x, y\in A_0$, we have

$$\operatorname{Im} H(x,y)=-2\operatorname{Re}\sum_{i=1}^{g}i\beta_i\,\tau_i(x)\overline{\tau_i(y)}$$

$$=-2\sum_{i=1}^{g}\operatorname{Re}\,\tau_i(\alpha xy)$$

$$=-\sum_{i=1}^{g}(\tau_i(\alpha x\bar{y})+\bar{\tau}_i(\alpha x\bar{y}))$$

$$=-\operatorname{Tr}_{K/\mathbf{Q}}(\alpha x\bar{y})\in\mathbf{Z},$$

where for any $y\in K$, $\bar{y}$ denotes its conjugate over K_0. Thus, for any complex algebra structure Φ on $\mathbf{R}\otimes_{\mathbf{Q}}K$, and the lattice A_0 in it, H defined above is a Riemann form and $X(K,\Phi)$ is an abelian variety, proving assertion (i).

To prove (ii) suppose there is an equivalence of $(i_{\Phi_1}, X(K,\Phi_1))$ and $(i_{\Phi_2}, X(K,\Phi_2))$. Then we deduce an isomorphism of $\mathbf{C}$-vector spaces $\lambda\colon(\mathbf{R}\otimes_{\mathbf{Q}}K,\ \Phi_1)\xrightarrow{\sim}(\mathbf{R}\otimes_{\mathbf{Q}}K,\ \Phi_2)$ such that $\lambda(1\otimes K)=1\otimes K$ and λ is an isomorphism of K-modules. If $\lambda(1\otimes 1)=1\otimes x$, $x\in K^*$, by replacing λ by $(1\otimes x^{-1}).\lambda$ we may suppose further that $\lambda(1\otimes 1)=1\otimes 1$. Since λ is both K and $\mathbf{R}$-linear, we deduce that $\lambda(a\otimes x)=a\otimes x$, $a\in\mathbf{R}$, $x\in K$, so that λ is the identity. Since λ is $\mathbf{C}$-linear, we must have $\Phi_1=\Phi_2$, which establishes (ii).

We have therefore proved the

THEOREM. *Let K_0 be a totally real number field of degree g over $\mathbf{Q}$, and K a totally imaginary quadratic extension of K_0. Consider all pairs (X,i) where X is an abelian variety over $\mathbf{C}$ and $i\colon K\to \operatorname{End}^0 X$ an embedding, with the equivalence relation defined above.*

Then there are exactly 2^g equivalence classes, and as Φ runs through complex structures on $\mathbf{R}\otimes_{\mathbf{Q}}K$ which make $\mathbf{R}\otimes_{\mathbf{Q}}K$ a $\mathbf{C}$-algebra, the pairs $(X(K,\Phi), i_\Phi)$ give a complete system of representatives in the distinct equivalence classes.

REMARKS. (1) It is not true that $X(K,\Phi)$ is always simple. It can be shown that in order for $X(K,\Phi)$ to be simple, it is necessary and sufficient that there does not exist a proper subfield L of K satisfying the following conditions:

(i) L is a quadratic extension of $L\cap K_0$,

(ii) if Φ is given by the set of imbeddings $\tau_1, \ldots, \tau_g$ of K in $\mathbf{C}$, and if $\tau_i \mid L \cap K_0 = \tau_j \mid L \cap K_0$, then $\tau_i \mid L = \tau_j \mid L$.

If such an L exists, $X(K, \Phi)$ is isogenous to a power of $X(L, \Psi)$, where Ψ is given by $\{\tau_i \mid_{L \cap K_0}\}$.

(2) Let us specialize to the case of dimension one, that is, the case of elliptic curves over $\mathbf{C}$. If X is an elliptic curve over $\mathbf{C}$, either $\mathrm{End}^0 X = \mathbf{Q}$ or $\mathrm{End}^0 X = \mathbf{Q}(\sqrt{-d})$ for some square free $d \in \mathbf{Z}, d > 0$. Moreover, given any imaginary quadratic field $\mathbf{Q}(\sqrt{-d})$, there is an elliptic curve X with $\mathrm{End}^0 X \simeq \mathbf{Q}(\sqrt{-d})$, and upto an isogeny, $X \simeq \mathbf{C}/\{n + m\sqrt{-d} \mid n, m \in \mathbf{Z}\}$.

SECOND EXAMPLE: ELLIPTIC CURVES IN CHARACTERISTIC $p > 0$.

We begin with recalling some basic facts concerning abelian varieties of dimension one (or elliptic curves). These facts are immediate consequences of our general theory, as the reader may verify for himself.

Let X be an abelian variety of dimension one. We shall denote the divisor corresponding to a point P by $[P]$. Then, for any divisor D on X, we have $\chi(\mathcal{O}_X(D)) = \deg D$, and if further $\deg D > 0$, $\chi(\mathcal{O}_X(D)) = \dim H^0(\mathcal{O}_X(D))$ and $H^1(\mathcal{O}_X(D)) = (0)$. A divisor D belongs to $\mathrm{Pic}^0 X$ if and only if $\deg D = 0$. A divisor $D = \Sigma n_i [P_i]$ of degree 0 is linearly equivalent to zero if and only if $\Sigma n_i P_i = 0$ on X. Any divisor D of degree $\geqslant 3$ is very ample.

Suppose now that the characteristic is either 0 or greater than 2. Let 0 be the identity element of the group X and let P_1, P_2, and P_3 be the points of order two on X. Since $\dim H^0(\mathcal{O}_X(2[0])) = 2$, we can choose a non-constant function x having a double pole at 0 and regular elsewhere. Subtracting a constant from x, we may assume $x(P_1) = 0$, and since the sum of the zeros with multiplicity is 0 and there are exactly two zeros, we deduce that P_1 is a double zero of x and there are no other zeros. Thus, by dividing by a constant, we may assume that $x(P_2) = 1$ and $x(P_3) = \lambda \in k^*$. By applying the above argument to $x - 1$, we deduce that $\lambda \neq 0, 1$. Since $H^0(\mathcal{O}_X(3[0]))$ is of dimension 3, we can find a function y having a triple pole at 0 and regular elsewhere. By subtracting a suitable linear combination

$ax+b$ from y, we may assume that $y(P_1) = y(P_2) = 0$, and since the number of zeros is 3 (taking multiplicity into account) and the sum of the zeros is 0, we deduce that y has simple zeros at P_1, P_2 and $P_3 = -P_1 - P_2$. Both the functions y^2 and $x(x-1)(x-\lambda)$ have poles of order 6 at 0 and double zeros at P_1, P_2, and P_3 and no other zeros or poles anywhere, so that they differ by a non-zero scalar factor. Replacing y by a non-zero scalar multiple, we arrive at an equation

$$X_\lambda : y^2 = x(x-1)(x-\lambda) \qquad (N_p)$$

for $X - \{0\}$ in $\mathbf{A}^2(k)$. Conversely, the projective curve $y^2 t = x(x-t).(x-\lambda t)$ has no singularities and is of genus 1 for $\lambda \neq 0$ or 1, and hence defines an elliptic curve X_λ in $\mathbf{P}^2(k)$.

We wish to find all possible values of λ for which X_λ is of p-rank 0, for characteristics $p > 2$. We know that the p-rank is 0 if and only if the Frobenius map in $H^1(X, \mathcal{O})$ is trivial. The meromorphic form dx on X is regular in $X - \{0\}$ and vanishes at $P_1 = (0, 0)$, $P_2 = (1, 0)$ and $P_3 = (\lambda, 0)$ to the first order, and nowhere else, since $dx(P) = 0$ and $x(P) = \alpha$ implies that $x - \alpha$ vanishes to the second order at P, hence $2P$ must be 0. Thus, the form $\omega = dx/y$ is regular and nowhere vanishing in $X - \{0\}$. It follows that ω must be regular and non-vanishing at 0 also. If we put $U_0 = X - \{0\}$, $U_1 = X - \{P_1\}$, $\mathfrak{A} = (U_0, U_1)$ is an affine covering of X. A 1-cocycle for this covering is a regular function f in $U_0 \cap U_1 = X - \{0\} - \{P_1\}$, and this is a coboundary if and only if $f = g - h$ with g regular on U_0 and h regular on U_1. Consider the linear form on $C^1(\mathfrak{A}, \mathcal{O}) = \Gamma(U_0 \cap U_1, \mathcal{O})$ defined by $f \longmapsto \mathrm{Res}_{P_1}(f\omega)$. Since the residue at any point of a meromorphic form with a pole (of any order) at a single point of X and no other poles is zero by the residue theorem, we see that $\mathrm{Res}_{P_1}(f\omega) = 0$ if f is a coboundary. On the other hand, the function y/x is regular on $U_0 \cap U_1$ and has a simple pole at P_1, so that $\mathrm{Res}_{P_1}(y/x.\omega) \neq 0$. Since $\dim H^1(X, \mathcal{O}) = 1$, we deduce that the above linear form induces an isomorphism $H^1(X, \mathcal{O}) \xrightarrow{\sim} k$, and also that $y/x \in \Gamma(U_0 \cap U_1, \mathcal{O})$ defines a non-zero cohomology class in $H^1(X, \mathcal{O})$. Hence, the Frobenius map on $H^1(X, \mathcal{O})$ is trivial if and only if

$y^p/x^p \in \Gamma(U_0 \cap U_1, \mathcal{O})$ is a coboundary, hence if and only if $\mathrm{Res}_{P_1}\left(\frac{y^p}{x^p}\cdot\frac{dx}{y}\right) = 0$. Now,

$$\mathrm{Res}_{P_1}\left(\frac{y^p}{x^p}\cdot\frac{dx}{y}\right) = \mathrm{Res}_{P_1}\left(\frac{(y^2)^{\frac{(p-1)}{2}}}{x^{p-1}}\frac{dx}{x}\right)$$

$$= 2.\left\{\begin{array}{l}\text{coefficient of } x^{p-1} \text{ in}\\ (y^2)^{\frac{(p-1)}{2}} = x^{\frac{(p-1)}{2}}(x-1)^{\frac{(p-1)}{2}}(x-\lambda)^{\frac{(p-1)}{2}}\end{array}\right\}$$

$$= 2.\left\{\begin{array}{l}\text{coefficient of } x^{\frac{(p-1)}{2}} \text{ in}\\ (x-1)^{\frac{(p-1)}{2}}(x-\lambda)^{\frac{(p-1)}{2}}\end{array}\right\}$$

$$= \pm 2.\left\{\sum_{\nu=0}^{\frac{(p-1)}{2}}\binom{\frac{p-1}{2}}{\nu}^2.\ \lambda_\nu\right\} = \pm\, 2\,\Phi(\lambda),$$

where

$$\Phi(\lambda) = \sum_{\nu=0}^{\frac{p-1}{2}}\binom{\frac{p-1}{2}}{\nu}^2.\ \lambda^\nu.$$

Now, $\Phi(0) =$ coeff. of $x^{(p-1)/2}$ in $x^{(p-1)/2}(x-1)^{(p-1)/2}$, and $\Phi(1) =$ coeff. of $x^{(p-1)/2}$ in $(x-1)^{p-1} = \dfrac{x^p-1}{x-1} = 1 + x + \ldots + x^{p-1}$, so that $\Phi(0) \neq 0$, $\Phi(1) \neq 0$. Thus, every root of Φ defines an elliptic curve X_λ of p-rank 0, and these are the only elliptic curves of p-rank 0 upto isomorphism.

Let us call an elliptic curve in characteristic $p > 0$ *supersingular* if its p-rank is 0. We have then shown that *in characteristic $p > 2$, any supersingular curve is isomorphic to one of the X_λ where λ is a root of $\Phi(\lambda)$.* If $p = 2$, it is not hard to see that there is exactly one supersingular elliptic curve, namely $y^2 + y = x^3$. We omit this. Therefore, in any positive characteristic, there is one and there are only finitely many supersingular curves upto isomorphism.

We now study the algebra $\mathrm{End}^0 X$ of an elliptic curve over a field of characteristic $p > 0$. Let k be the algebraically closed field over which we work. We shall say that an abelian variety X over k is defined over a subfield k_0 of k if there is a scheme X_0 over k_0 such that $X \simeq k \otimes_{k_0} X$. We can then easily establish that there is a finite algebraic extension k_1 of k_0, a rational point 0 in $k_1 \otimes_{k_0} X_0 = X_1$ and a morphism $m_1: X_1 \times_{k_1} X_1 \to X_1$ over k_1 such that on base extension, we get (upto an isomorphism) the triplet $(X, 0, m)$. In future, when we speak of abelian varieties defined over various fields, we will assume that 0 is rational and m defined over this field. Another remark in this connection is that if $f: X \to Y$ is a *separable* isogeny and if either X or Y is defined over an algebraically closed subfield k_0 of k then f, X and Y are all defined over k_0. This is clear if we assume X defined over k_0, since Y is the quotient of X by its kernel which is a reduced finite subgroup of X, and all points of finite order in X are k_0-rational. Suppose on the other hand that Y is defined over k_0. By induction, we may assume f of prime degree l. If $l \neq p$, then there is a separable isogeny $g: Y \to X$, defined over k, such that $f \circ g: Y \to Y$ is l_Y, so that we are reduced to the first case. Suppose then that $l = p$, and let G be the infinitesimal part of p_Y, and $Y' = Y/G$. Then, G and Y' are defined over k_0. Then there is a separable isogeny $g: Y' \to X$, defined over k, such that the composite $Y \to Y' \to X \to Y$ is p_Y, so that we are reduced to the first case again.

THEOREM. (Deuring.) *Let X be an elliptic curve in characteristic $p > 0$. We have the following equivalences.*

(a) *X cannot be defined over a finite field* $\iff \mathrm{End}^0 X = \mathbf{Q}$.

(b) *Suppose X is defined over a finite field k_0. Then,*

(i) *$\mathrm{End}^0 X$ is imaginary quadratic over $\mathbf{Q}$* $\iff$ *p-rank of X is 1* $\iff$ *$\pi^n \neq p_X^m$ for suitable integers n, m, where π is the Frobenius morphism over k_0.*

(ii) *If, however, the p-rank is 0, then $\mathrm{End}^0 X$ is the (upto isomorphism, unique) quaternion division algebra $\mathbf{K}_{(p)}$ over $\mathbf{Q}$ which satisfies $\mathrm{Inv}_l \mathbf{K}_{(p)} = 0$ if l is finite and $\neq p$ and $\mathrm{Inv}_p \mathbf{K}_{(p)} = \mathrm{Inv}_\infty \mathbf{K}_{(p)} = \frac{1}{2}$.*

Finally, there exists at least one and upto isomorphisms, at most finitely many X in each characteristic for which (ii) *holds.*

PROOF. First consider the following three statements.

(A) X is of p-rank 0.

(B) End^0X is non-commutative.

(C) X is defined over a finite field, and if π is the Frobenius morphism over this field, $\pi^n = p_X^m$ for some n and $m > 0$.

We shall establish that (A) $\Longleftrightarrow$ (B) and (A) $\Longleftrightarrow$ (C) in that order.

Suppose then that (B) holds. A look at the table of §21 tells us that $\mathrm{End}^0(X)$ is a central simple quaternion algebra over $\mathbf{Q}$, hence $\mathbf{Q}_p \otimes_{\mathbf{Q}} \mathrm{End}^0(X)$ is also a central simple algebra over $\mathbf{Q}_p$. If the p-rank of X were one, $\mathbf{Q}_p \otimes_{\mathbf{Z}_p} T_p(X)$ would be a one-dimensional $\mathbf{Q}_p$-vector space in which $\mathbf{Q}_p \otimes_{\mathbf{Q}} \mathrm{End}^0X$ admits a representation, which is impossible. Hence X has p-rank 0, proving (A).

Next, suppose (A) holds and suppose End X were commutative, so that $\mathrm{End}^0X = K$ is an algebraic number field. Since every elliptic curve isogenous with X is again of p-rank zero, and there are only finitely many isomorphism classes of curves of p-rank 0, if R is the ring of integers of K, we can find an integer $N > 0$ such that for every X' isogenous to X, we have $N.R \subset \mathrm{End}\ X'$. Choose a prime l not dividing pN such that Rl is a prime ideal in R. (It is known that such l exist.) Let α be a non-zero element of $T_l(X)$ not divisible by l and let K_n be the cyclic subgroup generated by the image of α under the natural homomorphism $T_l(X) \to X_{l^n}$. Then $K_n \subsetneq K_{n+1}$. Again by the finiteness of the number of isomorphism classes of curves of p-rank 0, we can find integers $m > n$ such that $K_n \subsetneq K_m$ and there is an isomorphism $\xi: X/K_m \xrightarrow{\sim} X/K_n$. Thus, if $\eta: X/K_n \to X/K_m$ is the natural homomorphism induced by the inclusion $K_n \subset K_m$, we get an endomorphism $\alpha = \eta \circ \xi \in \mathrm{End}\ X'$, where $X' = X/K_m$, such that α has cyclic kernel of order l^k, $k > 0$. Since degree α and hence $\mathrm{Nm}_{K/\mathbf{Q}}\alpha$ is a power of l and Rl is a prime ideal in R, we must have $\alpha = l^r.u$ where u is a unit in R

and $r > 0$. So $N\alpha = l^r.Nu$, and $Nu \in \mathrm{End}\ X'$. Now, the degree of Nu is N^2 since u is a unit in R, so that the l-primary part of $\ker(l^r.Nu)$ is $(\mathbf{Z}/l^r\mathbf{Z})^2$. On the other hand, the l-primary part of $\ker(N\alpha)$ is isomorphic to $\ker\alpha$, which is cyclic. This contradiction proves (B).

We now prove that (A) $\Longleftrightarrow$ (C). We have already shown that (A) implies that X is defined over a finite field. Let π be the Frobenius morphism over this field. Since End X is finitely generated, we can find a finite extension of degree n, say, such that every element of End X is defined over this extension. Hence π^n commutes with End X, so π^n belongs to the center of End X. Since (A) holds, so does (B), so that End^0X is a quaternion algebra with center $\mathbf{Q}$. Hence, π^n is an integer, and by consideration of degree, $\pi^n = \pm p^m$ for some $m > 0$, so $\pi^{2n} = p^{2m}$. Conversely, if $\pi^n = p_X^m$ for some n and $m > 0$, then since π is bijective, p_X is also bijective and X has p-rank 0.

We have thus shown that (A) $\Longleftrightarrow$ (B) $\Longleftrightarrow$ (C). Next if End^0X is non-commutative, it is a quaternion division algebra over $\mathbf{Q}$, and since for $l \neq p$, $\mathbf{Q}_l \otimes_{\mathbf{Q}} \mathrm{End}^0X \to \mathrm{End}_{\mathbf{Q}_l}(\mathbf{Q}_l \otimes_{\mathbf{Z}_l} T_l(X))$ is injective and both sides have dimension 4 it is an isomorphism. Therefore $\mathrm{Inv}_l(\mathrm{End}^0X) = 0$ if l is finite and $l \neq p$. Since $\sum_v \mathrm{Inv}_v(\mathrm{End}^0X) = 0$, the sum being over the finite and infinite places of $\mathbf{Q}$, and $\mathrm{Inv}_\infty(\mathrm{End}^0X) = 0$ or $\frac{1}{2}$, we deduce that $\mathrm{Inv}_p(\mathrm{End}^0X) = \mathrm{Inv}_\infty(\mathrm{End}^0X) = \frac{1}{2}$. This establishes (b)(ii).

Next, we show that if X is defined over a finite field, $\mathrm{End}^0X \neq \mathbf{Q}$. We have proved this for X of p-rank 0. Suppose then that p-rank of X is 1. As before, π is an endomorphism of X which is bijective and of degree a power of p, so that it cannot equal m_X for any integer m. Thus, $\pi \in \mathrm{End}\ X$, $\pi \notin \mathbf{Z}$. It follows from the table of possibilities of §21 that then End^0X is an imaginary quadratic extension of $\mathbf{Q}$. This proves (b)(i).

We have also established therefore that if $\mathrm{End}^0X = \mathbf{Q}$, X cannot be defined over a finite field. Suppose finally that X is not defined over a finite field. We may assume X is the normal form

(N_p) in characteristic $p > 2$, with λ transcendental. (If $p = 2$, the argument still works if a somewhat different normal form is used.) Let us call this curve X_λ. Since any two transcendental elements λ and λ' over the prime field are conjugate over the prime field, we see that if $\mathrm{End}\, X_\lambda = A$, then $\mathrm{End}\, X_\mu \simeq A$ for any other transcendental μ over the prime field. Now, $\mathrm{End}^0 X$ must be either $\mathbf{Q}$ or an imaginary quadratic extension of $\mathbf{Q}$, since the only other possibility is that of a non-commutative division algebra, in which case, by the implication (B) $\Rightarrow$ (A) above, X_λ has p-rank 0 and λ must be algebraic. Suppose then that $\mathrm{End}^0 X$ is an imaginary quadratic extension of $\mathbf{Q}$. Then we can find an element α in A such that $\alpha^2 = N \in \mathbf{Z}$, $N < 0$. Hence for any transcendental μ over the prime field, there is an $\alpha_\mu \in \mathrm{End}\, X_\mu$ with $\alpha_\mu^2 = N$. Suppose l is a prime not dividing pN and $\xi \in T_l(X_\lambda)$. Let K_n be the cyclic group generated by the image of ξ under the map $T_l(X_\lambda) \to X_{l^n}$, and let $p: X_\lambda \to X_\lambda/K_n$ be the natural map. By our remarks preceding the theorem, X_λ/K_n is also not defined over a finite field, and is therefore of the form X_μ for some μ transcendental over the prime field. With α_μ as above, since the map $\mathrm{End}^0 X_\mu \to \mathrm{End}^0 X_\lambda$ given by $\alpha \longmapsto p^{-1} \circ \alpha \circ p$ is an isomorphism, we deduce that $(p^{-1} \circ \alpha_\mu \circ p)^2 = N_X$, and since $\alpha_\lambda^2 = N_X$ and $\mathrm{End}^0 X_\lambda$ is a commutative field, $p^{-1} \circ \alpha_\mu \circ p = \pm\, \alpha_\lambda$ and $\alpha_\mu \circ p = \pm\, p \circ \alpha_\lambda$. Thus, $\alpha_\lambda(\ker p) \subset \ker p$, that is, $\alpha_\lambda(K_n) \subset K_n$. Since this holds for every n, we deduce that $\alpha_\lambda(\xi) = a\xi$ for some $a \in \mathbf{Z}_l$. Thus, for α_λ acting as an endomorphism of $T_l(X_\lambda)$, every vector is an eigenvector, so that α_λ acts as a scalar on $T_l(X_\lambda)$. Since the characteristic polynomial of α_λ has integer coefficients, this scalar must be rational, and its square cannot be negative. This contradiction shows that if X is not defined over a finite field, $\mathrm{End}^0 X = \mathbf{Q}$, thereby proving (a).

A far-reaching generalization of part of this theorem to higher dimensions has been proven by Tate and Grothendieck. Suppose k has char p, and X is a simple abelian variety defined over k.

THEOREM. *X is isogenous to an X' defined over a finite field if and only if X is of CM-type.*

($\Rightarrow$ was proven by Tate: [T2]; $\Leftarrow$ was proven by Grothendieck: [G1]). Tate shows further:

THEOREM. *If X is defined over a finite field k_0, π is the Frobenius morphism over k_0, and $\mathrm{End}\,(X, k_0)$ is the ring of k_0-rational endomorphisms, then*

$$\mathrm{End}(X, k_0) \otimes \mathbf{Q}_l = \text{centralizer of } T_l(\pi) \text{ in } \mathrm{Hom}_{\mathbf{Q}_l}(T_l(X), T_l(X)).$$

23. **The group $\mathscr{G}(L)$.** There is a second approach to the Riemann form of a line bundle, via a technique which is important in other contexts such as the theory of moduli, and the closer study of linear systems on an abelian variety. We first make a group-theoretic digression to explain the class of group schemes that we will need.

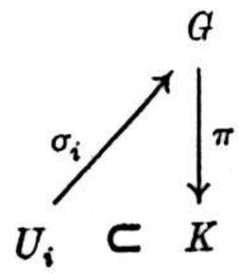
DEFINITION. *A theta-group will be a system of group schemes and homomorphisms*

$$1 \longrightarrow \mathbf{G}_m \xrightarrow{\ i\ } G \xrightarrow{\ \pi\ } K \longrightarrow 1$$

such that

(a) *K is commutative (but G need not be);*

(b) *$\exists$ an open covering $\{U_i\}$ of K and sections σ_i of π:*



(c) *i is a closed immersion, making $\mathbf{G}_m$ into the kernel of π;*

(d) *$\mathbf{G}_m \subset$ center of G.*

When K is a finite group scheme, there is a global section $\sigma: K \to G$ for π, and then *as a scheme*, $G \simeq \mathbf{G}_m \times K$ (i.e. define $\phi: \mathbf{G}_m \times K \to G$ by $\phi(\alpha, k) = i(\alpha).\sigma(k)$). Having made this splitting, the group law on G can be carried over to a "twisted" group law on $\mathbf{G}_m \times K$. There will be a morphism

$$f : K \times K \longrightarrow \mathbf{G}_m$$

such that the twisted group law is

$$(\alpha, k).(\alpha', k') = (\alpha.\,\alpha'.\,f(k, k'),\ k + k'), \tag{*}$$

where α, α' are S-valued points of $\mathbf{G}_m$, k, k' are S-valued points of K, and K is written additively. f must be a 2-co-cycle :

$$f(k + k', k'').\,f(k, k') = f(k, k' + k'').\,f(k', k'')$$

and changing the section σ has the effect of altering f by a coboundary :

$$f^*(k, k') = f(k, k').\,g(k + k').\,g(k)^{-1}.\,g(k')^{-1}.$$

Conversely, given any such f, (*) makes $\mathbf{G}_m \times K$ into a theta-group. In other words, the set of all theta-groups over a fixed finite K is isomorphic to the cohomology group $H^2(K, \mathbf{G}_m)$, computed via morphism cochains.

The deviation of G from commutativity is easily measured by taking the commutator. For any two S-valued points x, y of G, (1) $xyx^{-1}y^{-1}$ is an S-valued point of $\mathbf{G}_m$ and (2) it depends only on $\pi(x)$, $\pi(y)$ and not on x, y. Therefore there is a morphism

$$e : K \times K \longrightarrow \mathbf{G}_m$$

such that

$$xyx^{-1}y^{-1} = e(\pi x,\ \pi y), \quad \text{all } x, y \in G(S), \text{ all } S.$$

It is easily checked that e is a skew-symmetric bihomomorphism :

(a) $e(k + k', k'') = e(k, k'').\,e(k', k'')$

(b) $e(k, k' + k'') = e(k, k').e(k, k'')$

(c) $e(k, k) = 1.$

If G admits a global section of K and so is described by a 2-co-cycle f, normalised by the condition $f(0, 0) = 1$, then

(d) $e(k, k') = f(k, k')/f(k', k).$

In case K is finite, the bi-homomorphism e also can be expressed asymmetrically as a homomorphism :

$$\gamma : K \longrightarrow \hat{K}.$$

In fact, if we regard $K \times K$ and $\mathbf{G}_m \times K$ as group-schemes over K via p_2 then (e, p_2): $K \times K \to \mathbf{G}_m \times K$ is a K-homomorphism, i.e. a K-valued character of K, or a morphism $\gamma : K \to \hat{K}$. If $\langle\ ,\ \rangle : K \times \hat{K} \to \mathbf{G}_m$ is the universal pairing, then in terms of S-valued points k, k' of K, γ is given by

$$e(k, k') = \langle k, \gamma(k') \rangle .$$

PROPOSITION. *If K is finite, $\gamma : K \to \hat{K}$ as above, then for every S-valued point x of G, $[\pi(x) \in \ker \gamma] \iff$ [x is in the center of G] i.e. for all schemes S' over S, and all S'-valued points y of G, $xy = yxy$.*

PROOF. In fact, $\gamma(\pi(x)) \neq 0 \iff$ the character $\gamma(\pi(x)) : K \times S \to \mathbf{G}_m \times S$ is non-trivial $\iff$ for some S'-valued point k of K, $\gamma(\pi(x))(k) \neq 1 \iff$ for some k, $\langle k, \gamma(\pi(x)) \rangle \neq 1 \iff$ for some k, $e(k, \pi(x)) \neq 1 \iff$ for some S'-valued point y of G, $xy \neq yx$.

COROLLARY. *The following are equivalent.*

(i) *γ is an isomorphism.*

(ii) *$i(\mathbf{G}_m)$ is exactly the center of G, i.e. every S-valued point x of G commuting with all S'-valued points, all S'/S, is in $i(\mathbf{G}_m)$.*

Such theta-groups will be called *non-degenerate.*

At the other extreme, we need two facts about when such G's are trivial.

LEMMA 1. (i) *If K is finite and G is commutative, then $G \simeq \mathbf{G}_m \times K$ as a group, i.e. in the category of commutative group schemes, K finite $\Rightarrow \mathrm{Ext}^1(K, \mathbf{G}_m) = (0)$.*

(ii) *If K is finite of prime order, then G is commutative.*

PROOF. (i) is a standard fact for commutative algebraic group schemes. For instance, once one sets up the long exact sequence for Ext's in this category, one takes a maximal chain of subgroups of K and reduces (i) to the special cases $K = \mathbf{Z}/l\mathbf{Z}$, $\mathbf{Z}/p\mathbf{Z}$, μ_p, or α_p. In the first two cases, one lifts a generator of K to a point of G of the same order (using the fact that k^* is divisible); in the second two cases, one checks by a direct computation that the

p-Lie algebra of G must split. For details, cf. Oort [O], or Séminaire Heidelberg-Strasbourg. To prove (ii), if $K = \mathbf{Z}/l\mathbf{Z}$ or $\mathbf{Z}/p\mathbf{Z}$, lift a generator of K to any point of G and note that if a reduced group scheme is generated by a central subgroup and one element, then it is commutative. If $K = \mu_p$ or α_p, let $\mathfrak{g}$ be the Lie algebra of G: then $\mathfrak{g} = k.x + k.y$ where x generates $\mathrm{Lie}\,\mathbf{G}_m$ and y lifts a generator of $\mathrm{Lie}\,K$. Since $\mathbf{G}_m$ is central in G, $[x, z] = 0$, all $z \in \mathfrak{g}$. Therefore $\mathfrak{g}$ is an abelian Lie algebra, which implies that $G^{(p)}$ is commutative (cf. Séminaire Heidelberg-Strasbourg or [G 3]. Since, as a scheme $G \simeq \mathbf{G}_m \times K$, any S-valued point of G is the product of S-valued points of $\mathbf{G}_m$ and of K, hence of S-valued points of $\mathbf{G}_m$ and of $G^{(p)}$. Since $\mathbf{G}_m$ is central and $G^{(p)}$ is commutative, this shows that G is commutative too.

The natural idea for proving (ii) would be to show that when K has prime order there are no non-trivial skew-symmetric bi-homomorphisms

$$e : K \times K \longrightarrow \mathbf{G}_m.$$

But this is false in char 2, if $K = \alpha_2$! This has fascinating consequences: cf. [Br].

We now return to abelian varieties. First of all, to eliminate any possible confusion, let me state clearly that if L is a line bundle over X, with projection $p : L \to X$, and $\sigma : X \to X$ is an automorphism of X, then by an automorphism $\tau : L \to L$ covering σ we always mean a *linear* automorphism fitting into a diagram :

$$\begin{array}{ccc} L & \xrightarrow{\tau} & L \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle p} \\ X & \xrightarrow[\sigma]{} & X. \end{array}$$

Moreover, such a τ induces an isomorphism $\tau' : L \xrightarrow{\sim} \sigma^* L$ and any such isomorphism τ' induces an automorphism τ of L covering σ.

Secondly, recall that if X is an abelian variety, S any scheme and $f : S \to X$ is an S-valued point of X, then T_f, translation by f, denotes the S-isomorphism of schemes $(p_1, m \circ (f \times 1_X)) : S \times X \to S \times X$, where m is the multiplication on X.

Now here is how theta groups arise.

THEOREM 1. *Let L be a line bundle on an abelian variety X. For any scheme S, let* $\underline{\mathrm{Aut}}\,(L/X)(S)$ *be the group of automorphisms of $S \times L$ covering a translation map of $S \times X$.* $\underline{\mathrm{Aut}}\,(L/X)$ *is a contravariant group-valued functor on* $\underline{\mathrm{Sch}}$. *Then there is a group scheme $\mathscr{G}(L)$ and an isomorphism of group functors*

$$\underline{\mathrm{Aut}}(L/X) \simeq \mathscr{G}(L).$$

For any scheme S, the natural homomorphisms of groups

$$1 \to H^0(S, \mathcal{O}_S^*) \to \underline{\mathrm{Aut}}\,(L/X)(S) \to \left\{ \begin{array}{l} S\text{-valued points } f : S \to X \\ \text{such that} \\ T_f^*(S \times L) \simeq S \times L \end{array} \right\} \to 1$$

induce homomorphisms of group schemes

$$1 \longrightarrow \mathbf{G}_m \xrightarrow{i} \mathscr{G}(L) \xrightarrow{j} K(L) \longrightarrow 1$$

making $\mathscr{G}(L)$ into a theta-group.

PROOF. Let L^* be the complement of the 0-section in L; this is a principal fibre bundle over X with structure group $\mathbf{G}_m$. Fix a base point $P_0 \in p^{-1}(0) \cap L^*$, and put $\mathscr{G}(L) = p^{-1}(K(L)) \cap L^*$. For any automorphism α of $S \times L$ covering a translation T_f of $S \times X$, where $f \in X(S)$, we get a morphism $\tilde{\alpha} : S \to L^*$ defined by $\tilde{\alpha} = p_2 \circ \alpha \circ s_0$, where s_0 is the map $S \simeq S \times \{P_0\} \hookrightarrow S \times L$ and $p_2 : S \times L \to L$ is the projection. Since $p \circ \tilde{\alpha}$ is just the morphism f, and $f \in K(L)\,(S)$, we deduce that $\tilde{\alpha}$ factors through $\mathscr{G}(L)$:

$$S \xrightarrow{\bar{\alpha}} \mathscr{G}(L) \hookrightarrow L^*.$$

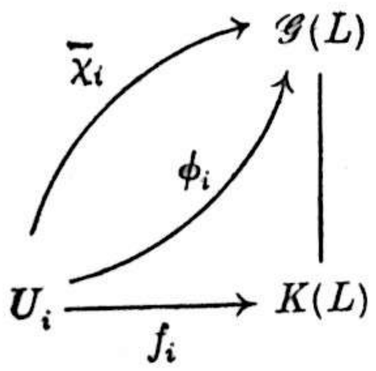
Then $\alpha \longmapsto \alpha$ defines a map

$$\underline{\mathrm{Aut}}\,(L/X)(S) \to \mathscr{G}(L)(S),$$

which is functorial in S. I claim that it is an isomorphism. Suppose $\alpha, \beta \in \underline{\mathrm{Aut}}\ (L/X)(S)$ covering T_f and T_g respectively, are such that $\bar{\alpha} = \bar{\beta}$. We then have $f = p \circ \bar{\alpha} = p \circ \bar{\beta} = g$, and $\gamma = \beta \circ \alpha^{-1}$ is an automorphism of $S \times L$ over the base $S \times X$ such that the composite $S \xrightarrow{s_0} S \times L \xrightarrow{\gamma} S \times L$ equals s_0. Now, γ is given by multiplication by an element γ_1 of $H^0(S \times X, \mathcal{O}^*_{S \times X})$ and since $s_0 = \gamma \circ s_0$, $\gamma_1 | S \times \{P_0\} = 1$. But $H^0(S \times X, \mathcal{O}^*_{S \times X}) \simeq H^0(S, \mathcal{O}^*_S)$, so $\gamma_1 = 1$ and $\gamma = 1_{S \times L}$. This proves that the map $\alpha \longmapsto \bar{\alpha}$ is injective. To prove that it is surjective, let $\phi \in \mathcal{G}(L)(S)$, and let $f = p \circ \phi$ so that $f \in K(L)(S)$. Then by definition of $K(L)$,

$$T_f^*(S \times L) \simeq (S \times L) \otimes p_1^* M$$

for some line bundle M on S. We can cover S by open sets $\{U_i\}$ such that $M|_{U_i}$ is trivial. Then over $U_i \times X$, $T_f^*(S \times L)$ and $S \times L$ are isomorphic, so there exist automorphisms χ_i of $U_i \times L$ covering T_{f_i}, f_i = restriction of f to U_i. If ϕ_i is the restriction of ϕ to U_i, we now have two liftings of the morphism f_i to $\mathcal{G}(L)$:



Since $\mathcal{G}(L)$ is a principal fibre bundle over $K(L)$ with group $\mathbf{G}_m$, there is a unit $\epsilon_i \in \Gamma(U_i, \mathcal{O}^*_S)$ such that $\phi_i = \epsilon_i(\bar{\chi}_i)$. But if λ_i is the automorphism, mult. by ϵ_i, of $U_i \times L$, then $\overline{\lambda_i \chi_i} = \epsilon_i(\bar{\chi}_i) = \phi_i$. Finally, since ϕ_i agrees with ϕ_j on $U_i \cap U_j$, the two automorphisms $\lambda_i \chi_i$ and $\lambda_j \chi_j$ agree on $(U_i \cap U_j) \times L$ (using injectivity of $\alpha \longmapsto \bar{\alpha}$), so there is an automorphism χ of $S \times L$ extending $\lambda_i \chi_i$. Then $\bar{\chi} = \phi$ so $\alpha \longmapsto \bar{\alpha}$ is a surjective map.

This establishes an isomorphism of functors $\underline{\mathrm{Aut}}\ (L/X) \simeq \underline{\mathcal{G}(L)}$, and since the left side is a group functor, $\mathcal{G}(L)$ becomes a

group scheme. Define homomorphisms $i: \mathbf{G}_m \to \mathcal{G}(L)$ and $j: \mathcal{G}(L) \to K(L)$ by the homomorphisms of functors:

$$\mathbf{G}_m(S) = \Gamma(S, \mathcal{O}^*_S) \longrightarrow \underline{\mathrm{Aut}}(L/X)(S) \simeq \mathcal{G}(L)(S)$$
$$\epsilon \longmapsto \text{mult. by } \epsilon$$
$$\mathcal{G}(L)(S) \simeq \underline{\mathrm{Aut}}\ (L/X)(S) \longrightarrow K(L)(S)$$
$$\alpha \longmapsto \left\{ \begin{array}{l} \text{the } S\text{-valued point } f \text{ of } X \\ \text{such that } \alpha \text{ covers } T_f \end{array} \right\}.$$

Then i is clearly injective, j is just the projection p, and $\mathrm{Im}(i) = \mathrm{Ker}(j)$. Since there are sections locally to p: $L \to X$, there are also sections locally to $j: \mathcal{G}(L) \to K(L)$. Finally, if $\epsilon \in \Gamma(S, \mathcal{O}^*_S)$, then the automorphism, mult. by ϵ, clearly commutes with all other automorphisms $\alpha \in \underline{\mathrm{Aut}}\ (L/X)(S)$, so $i(\mathbf{G}_m)$ is in the center of $\mathcal{G}(L)$. This proves that $\mathcal{G}(L)$ with i and j is a theta-group.

DEFINITION. *$e^L: K(L) \times K(L) \to \mathbf{G}_m$ is the skew-symmetric bihomomorphism associated to the commutator in the theta-group $\mathcal{G}(L)$.*

Look at the case $L \in \mathrm{Pic}^0 X$. Then $K(L) = X$ and the morphism e^L takes the complete variety $X \times X$ to the affine variety $\mathbf{G}_m$. Therefore $e^L \equiv 1$ and $\mathcal{G}(L)$ is a commutative group scheme, which is an extension of X by $\mathbf{G}_m$. It can in fact be shown that this map:

$$\mathrm{Pic}^0(X) \longrightarrow \underset{\substack{\text{comm.group} \\ \text{schemes}}}{\mathrm{Ext}^1}(X, \mathbf{G}_m)$$
$$L \longmapsto \mathcal{G}(L)$$

is an isomorphism (Theorem of Serre and Rosenlicht).

Suppose next that the line bundle L arises from a divisor D: $L \simeq \mathcal{O}_K(D)$. We leave it to the reader to check that the discrete group $\mathcal{G}(L)_k$ can be described as follows.

$$\mathcal{G}(L)_k = \{(x, f) \mid x \in X, f \in k(X), T_x^{-1} D = D + (f)\}$$
$$(x, f) \cdot (y, g) = (x + y, T_x^* g \cdot f).$$

This works since

$$T_{x+y}^{-1}D - D - (T_x^* g + f) = T_x^{-1}(T_y^{-1}D - D) + (T_x^{-1}D - D) - T_x^{-1}(g) - (f)$$
$$= T_x^{-1}(T_y^{-1}D - D - (g)) + (T_x^{-1}D - D - (f)) = 0.$$

The subgroup $k^* = (\mathbf{G}_m)_k \subset \mathscr{G}(L)_k$ corresponds to the pairs $x = 0$, $f = \alpha \in k^*$; the projection $\mathscr{G}(L)_k \to K(L)_k$ corresponds to the map $(x, f) \longmapsto x$.

FUNCTORIAL PROPERTIES OF e^L.

In the following formulas, the symbols x, y etc. are to be understood as R-valued points for any k-algebra R. One could equivalently interpret the formulas as commutativity of certain diagrams of morphisms. With this specific understanding, we shall often omit R from the statements and proofs and speak as though we were just dealing with ordinary points, but all the assertions are to be understood in the stronger sense mentioned.

(1) If $f: X \to Y$ is a homomorphism of abelian varieties and L a line bundle on Y, we have

$$e^{f^*(L)}(x, y) = e^L(f(x), f(y)),\ x, y \in f^{-1}(K(L)).$$

(2) For any line bundles L_1, L_2 on X,

$$e^{L_1 \otimes L_2}(x, y) = e^{L_1}(x, y) \cdot e^{L_2}(x, y),\ x, y \in K(L_1) \cap K(L_2).$$

(3) For algebraically equivalent line bundles L_1, L_2 on X, $e^{L_1} = e^{L_2}$.

(4) For $x \in K(L)$ and $y \in n_X^{-1}(K(L))$,

$$e^{L^n}(x, y) = e^L(x, ny).$$

(5) For $x \in X_n$, $y \in n_X^{-1}(K(L)) = \phi_L^{-1}(X_n)$, ($n$ any integer with $p \nmid n$)

$$\bar{e}_n(x, \phi_L(y)) = e^{L^n}(x, y).$$

PROOFS. (1) We may assume $f(x) = j(\xi)$, $f(y) = j(\eta)$, where $j: \mathscr{G}(L) \to K(L)$ is the natural homomorphism. (When x, y are R-valued points, we can find ξ, η after localizing on Spec R.) We

can then lift ξ and η to automorphisms ϕ, ψ of $f^*(L)$ covering T_x and T_y respectively, and then $\phi\psi\phi^{-1}\psi^{-1}$ lifts $\xi\eta\xi^{-1}\eta^{-1}$, which means precisely (1).

(2) Again we may assume that there are automorphisms ϕ_i, ψ_i respectively of L_i, $i = 1, 2$, covering T_x and T_y. Then $\phi_1 \otimes \phi_2$ and $\psi_1 \otimes \psi_2$ are automorphisms of $L_1 \otimes L_2$ covering T_x, T_y respectively, and the commutator of these two automorphisms is the tensor product of the commutators of ϕ_i and ψ_i ($i = 1, 2$), which proves (2).

(3) Write $L_3 = L_1 \otimes L_2^{-1}$, so that $L_3 \in \mathrm{Pic}^0 X$ and $L_1 = L_2 \otimes L_3$, $K(L_3) = X$. Apply (2) to the line bundles L_2 and L_3.

(4) By replacing the ring R by a ring $R' \supset R$ if necessary, we may assume $x = nz$ for some $z \in n_X^{-1}(K(L))$. (In fact, we have only to take Spec $R' =$ Spec $R \times_{K(L)} n_X^{-1}(K(L))$ which is finite and flat over Spec R, so that it is affine and $R' \supset R$.) We then have $z, y \in n_X^{-1}(K(L)) = K(L^n)$, so that by (1) applied to $n_X^*(L)$ and (2) applied repeatedly, and making use of the algebraic equivalence of $n_X^*(L)$ and L^{n^2}, we obtain

$$e^L(nz, ny) = e^{n_X^*(L)}(z, y)$$
$$= e^{L^{n^2}}(z, y)$$
$$= (e^{L^n}(z, y))^n$$
$$= e^{L^n}(nz, y),$$

which is formula (4).

(5) As in (4), we may assume that $y = nz$ for some z, and the equation to be proved assumes the form

$$\bar{e}_n(x, \phi_L(y)) \stackrel{?}{=} e^{L^n}(x, nz) = e^{L^{n^2}}(x, z) = e^{n_X^*(L)}(x, z)$$

since L^{n^2} is algebraically equivalent to $n_X^*(L)$ and $z \in K(L^{n^2}) = K(n_X^*(L))$. The fact that $z \in K(n_X^*(L))$ means that we have an automorphism σ of $n_X^*(L)$ covering the translation T_z (localize Spec R if need be).

Let us agree to denote (temporarily), for line bundles M, N on X, the line bundle associated to the locally free sheaf of germs of homomorphisms of M into N by $\mathrm{Hom}(M, N)$, so that we have a natural isomorphism $\mathrm{Hom}(M, N) \xleftarrow{\sim} M^{-1}\otimes N$. Note that there is a natural action of X_n on any pull back $n_X^*(M)$ covering translations, hence also natural actions on tensor products, Homs and translates of pull-backs (this last, since any translation commutes with any other). With this understanding, we have *natural* isomorphisms of the following line bundles on X commuting with this X_n action:

$$n_X^*(T_y^*L\otimes L^{-1}) \approx n_X^*(T_y^*(L))\otimes n_X^*(L^{-1}) \approx T_z^*(n_X^*(L))\otimes n_X^*(L)^{-1}$$
$$\approx \mathrm{Hom}\,[n_X^*(L), T_z^*(n_X^*(L))].$$

But what is $\bar{e}_n(\cdot, \phi_L(y))$? $n_X^*(T_y^*L\otimes L^{-1})$ is isomorphic to the trivial bundle, and $\bar{e}_n(\cdot, \phi_L(y))$ is given in the usual way by the natural action of X_n carried over to the trivial bundle. Equivalently, $n_X^*(T_y^*L\otimes L^{-1})$ has a nowhere vanishing section, unique up to scalars, and $e_n(\cdot, \phi_L(y))$ is given by the action on X_n on this section. Now make this computation on the bundle on the right instead of the one on the left. A nowhere vanishing section of the line bundle on the right is just an isomorphism $n_X^*(L) \xrightarrow{\phi} n_X^*(L)$ covering T_z, and the natural action of $x \in X_n$ on the right maps this section into the section ϕ': $n_X^*(L) \to n_X^*(L)$ defined by $\phi' = \eta_x \circ \phi \circ \eta_x^{-1}$, where η_x: $n_X^*(L) \to n_X^*(L)$ is the natural isomorphism covering T_x. We must therefore have $\eta_x \circ \phi \circ \eta_x^{-1} = e_n(x, \phi_L(y)).\phi$. Applying this in particular to the automorphism σ covering T_z chosen earlier, we get that $\eta_x \circ \sigma \circ \eta_x^{-1} \circ \sigma^{-1} = \bar{e}_n(x, \phi_L(y))$. But this means by definition that $e^{n_X^*(L)}(x, z) = e_n(x, \phi_L(y))$.

As a corollary, we get a second proof of the skew-symmetry of the Riemann form of L:

$$\bar{e}_n(x, \phi_L(y)) = e^{L^n}(x, y) = e^{L^n}(y, x)^{-1} = e_n(y, \phi_L(x))^{-1},$$

if $x, y \in X_n$. The formula (5), coupled with (4), shows how the Riemann forms can be computed from the e^L's and conversely,

how all the e^L's, on points of order l^n, can be computed from the Riemann forms.

THEOREM 2. *Suppose $\pi: X \to Y$ is an isogeny of abelian varieties, and L is a line bundle on X. Then there is a natural one-one correspondence between*

(a) *isomorphism classes of line bundles M on Y such that $\pi^*M \simeq L$,*

(b) *homomorphisms α: $\ker \pi \to \mathcal{G}(L)$ lifting the inclusion* $\ker \pi \hookrightarrow X$.

PROOF. This is just a restatement, in a special case of the general descent theorem in §12 for coherent sheaves with respect to quotients by finite group schemes. Use the fact that

$$\mathrm{Hom}_X(\ker \pi, \mathcal{G}(L)) \simeq \left\{\begin{array}{l}\text{actions of } \ker \pi \text{ on } L \text{ covering}\\ \text{its translation action on } X\end{array}\right\}.$$

COROLLARY. *Given $\pi: X \to Y$ and L as above. Then a line bundle M on Y such that $\pi^*M \simeq L$ exists if and only if* $\ker(\pi) \subset K(L)$ *and* $e^L|_{\ker \pi \times \ker \pi} \equiv 1$.

PROOF. Let $p: \mathcal{G}(L) \to K(L)$ be the projection and let $G = p^{-1}(\ker \pi)$. Then G is a theta-group over $\ker \pi$, and by part (i) of the lemma at the beginning of this §, $e^L|_{\ker \pi \times \ker \pi} \equiv 1 \iff G$ is commutative $\iff G \simeq \mathbf{G}_m \times \ker \pi$ as group-scheme $\iff \exists$ a homomorphism α: $\ker \pi \to G$ such that $p\circ\alpha = 1 \iff M$ exists.

We now prove the following theorem, promised in §20.

THEOREM 3. *If L is a line bundle on an abelian variety X and $n \in \mathbf{Z}$, $L \simeq M^n$ for some line bundle M if and only if $K(L) \supset X_n$.*

PROOF. The 'only if' part follows from the equation $\phi_L = n\phi_M$. Assume conversely that $K(L) \supset X_n$. To show that $L \simeq M^n$ for some line bundle M, it suffices to show that $L^n \simeq n_X^*(N)$ for some N. Indeed, we would then have that $(L\otimes N^{-n})^n \in \mathrm{Pic}^0X$, hence also $L\otimes N^{-n} \in \mathrm{Pic}^0X$, and if we choose $P \in \mathrm{Pic}^0X$ such that $L\otimes N^{-n} \simeq P^n$, we would obtain $L \simeq (N\otimes P)^n$.

To show that $L^n \simeq n_X^*(N)$, we merely compute, for any R-valued points x, y of X_n,

$$e^{L^n}(x,y) = e^L(x,ny) = 1.$$

The desired conclusion then follows from the corollary to Theorem 2.

Our last result concerns the non-degeneracy of $\mathcal{G}(L)$. We need some preliminary results.

Suppose $e\colon K \times K \to \mathbf{G}_m$ is a skew-symmetric bi-homomorphism on a finite group K. Let $\gamma\colon K \to \hat{K}$ be the associated homomorphism. Then if $H \subset K$ is a subgroup, I claim that there is a second subgroup $H^\perp$ characterized by the property:

$$\text{if } k \text{ is an } S\text{-valued point of } K,$$

$$k \in H^\perp(S) \iff \{\text{for all } S'/S, \text{ all } S'\text{-valued points } k' \text{ of } H,\ e(k,k') = 1\}.$$

In fact, restricting characters of K to H defines a morphism $q\colon \hat{K} \to \hat{H}$, and $H^\perp$ is clearly the kernel of $q \circ \gamma\colon K \to \hat{H}$. Now suppose $\pi\colon X \to Y$ is an isogeny of abelian varieties, M is a line bundle on Y and $L = \pi^*M$. Let $H = \ker(\pi)$: then as we have seen H is a subgroup of $K(L)$ such that $e^L|_{H\times H} \equiv 1$. In other words, $H \subset H^\perp$. The result we require is

LEMMA 2. $K(M) \simeq H^\perp/H$.

PROOF. Let $x\colon S \to X$ be an S-valued point of X. We must show that x is a point of $H^\perp$ if and only if πx is a point of $K(M)$. It will suffice to prove this when $S = \mathrm{Spec}(R)$, R a local ring, in which case S carries only trivial line bundles. Then, using the descent theorem of §12,

$$\pi x \in K(M)(S) \iff T_{\pi x}^*(S \times M) \simeq S \times M$$

$$\iff \left\{ \begin{array}{l} \exists \text{ an isomorphism } T_x^*(S \times L) \simeq S \times L \\ \text{commuting with the action of } \ker \pi \text{ on} \\ \text{these two line bundles} \end{array} \right\}.$$

Now suppose $\alpha : H \to \mathcal{G}(L)$ is the homomorphism giving the action of H on L for which M is the quotient. Then we continue our equivalences:

$$\iff \left\{ \begin{array}{l} \exists \text{ an } S\text{-valued point } w \text{ of } \mathcal{G}(L) \text{ such that} \\ p(w) = x \text{ and } w \text{ commutes with } \alpha(H) \end{array} \right\}$$

$$\iff \{e^L(x, h) = 1, \text{ all } S'\text{-valued points } h \text{ of } H\}$$

$$\iff x \in H^\perp(S).$$

The same argument shows in fact that

$$\mathcal{G}(M) \simeq \left\{ \begin{array}{c} \text{centralizer of } \alpha(H) \\ \text{in } \mathcal{G}(L) \end{array} \right\} \Big/ \alpha(H)$$

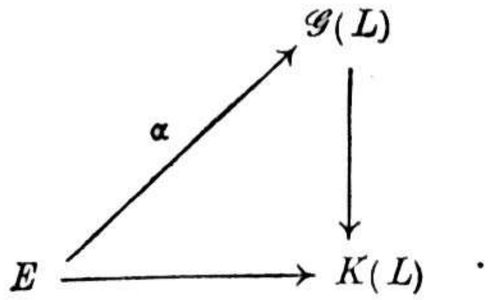
but we do not need this fact. We now apply the lemma to

THEOREM 4. *Let L be a non-degenerate line bundle on an abelian variety X. If $H \subset K(L)$ is a maximal subgroup such that $e^L|_{H\times H} \equiv 1$, then $H = H^\perp$ and* order $(H)^2 =$ order $(K(L))$.

PROOF. Let H be a maximal subgroup scheme of $K(L)$ such that $e^L|_{H\times H} \equiv 1$. Let $Y = X/H$, and let $\pi\colon X \to Y$ be the natural homomorphism. By the Cor. to Th. 2 there exists a line bundle M on Y such that $\pi^*M \simeq L$. The fact that H is maximal means that there are no further isogenies $\pi'\colon Y \to Y'$ for which $M \simeq \pi'^*(M')$ except the identity.

LEMMA 3. *Let L be a non-degenerate line bundle on an abelian variety X. If there are no isogenies $\pi\colon X \to Y$ of degree > 1 such that $L \simeq \pi^*M$, some line bundle M on Y, then $|\chi(L)| = 1$.*

PROOF. If $|\chi(L)| > 1$, then $K(L)$ is non-trivial. Then there exists a subgroup $E \subset K(L)$ of prime order, i.e., $E \simeq \mathbf{Z}/l\mathbf{Z}$, $\mathbf{Z}/p\mathbf{Z}$, μ_p or α_p. Look at the inverse image E in $\mathcal{G}(L)$: this is a theta-group scheme G over E. By the lemma at the beginning of this section, G is commutative, hence $G \simeq \mathbf{G}_m \times E$, hence there exists a homomorphism:



Therefore by Theorem 2, L descends to X/E, contradicting the assumption. So $|\chi(L)| = 1$.

Returning to the proof of the theorem, we deduce that $K(M) = (0)$ and $|\chi(M)| = 1$. Therefore by Lemma 2, $H = H^{\perp}$, and by the results of §16,

$$|\chi(L)| = \deg(\pi) = \text{order } (H),$$
$$\chi(L)^2 = \deg(\phi_L) = \text{order } (K(L));$$

so order $(H)^2 =$ order $K(L)$.

COROLLARY 1. *Every abelian variety X is isogenous to a principally polarized abelian variety Y, i.e. one which carries an ample line bundle L with $\chi(L) = 1$.*

PROOF. Apply the theorem to any ample L on X, and let $Y = X/H$, H maximal in $K(L)$ with $e^L|_{H\times H} \equiv 1$. Then $L \simeq \pi^*(M)$ and M is ample with $\chi(M) = 1$.

COROLLARY 2. *If L is a non-degenerate line bundle on X, then $\mathscr{G}(L)$ is a non-degenerate theta-group.*

PROOF. Let $\gamma\colon K(L) \to \widehat{K(L)}$ be the homomorphism associated to e^L and suppose D is its kernel. Choose an $H \subset K(L)$ with $H = H^{\perp}$ and order $(H)^2 =$ order $K(L)$, as in the theorem. Now since $\gamma(D) = (0)$, we find

$$e^L|_{D\times K(L)} \equiv 1 \text{ and } e^L|_{K(L)\times D} \equiv 1.$$

Therefore $D \subset H^{\perp}$, so $D \subset H$ and also all characters $e(x)$ annihilate D, all $x \in K(L)(S)$. Now by definition, $H^{\perp}$ is the kernel of the homomorphism $K(L) \xrightarrow{\gamma} \widehat{K(L)} \xrightarrow{q} \hat{H}$. It follows that $\text{Im}(q\circ\gamma) \subset (\widehat{H/D})$ and that we have an exact sequence

$$0 \longrightarrow H \longrightarrow K(L) \xrightarrow{q\circ\gamma} \widehat{H/D}.$$

Therefore

$$\text{order } K(L) \leqslant \text{order } H.\ \text{order } \widehat{H/D}$$
$$= (\text{order } H)^2/\text{order } D.$$

This proves that order $D = 1$.

The next step in the development of the theory of theta-groups is to show that (1) all representations of non-degenerate theta-groups which restrict to the identity character on the center G_m are completely reducible, (2) that there is only one irreducible representation with this property, and (3) that when L is non-degenerate, $i = i(L)$, then $\mathscr{G}(L)$ acts naturally on $H^i(X, L)$ and that this is the irreducible representation in (2). For these facts and their application, cf. [M2].

24. **The case $k = \mathbf{C}$.** The purpose of this last section is to tie together the algebraic approach of this chapter with the analytic methods of Chapter I. In particular, I want to relate the analytic and algebraic Riemann forms of a line bundle L, and I want to show how the positivity of the Rosati involution follows immediately from the positivity of the analytic Riemann form in its guise as a Hermitian form when L is ample.

As always, let $X = V/U$, V a complex vector space and U a lattice. Let $L = L(H,\alpha)$ be a line bundle on X, where H is a Hermitian form on V such that $E = \text{Im } H$ is integral on U, and $\alpha\colon U \to \mathbf{C}_1^*$ is a function such that

$$\alpha(u_1 + u_2) = \alpha(u_1).\alpha(u_2).e^{\pi i E(u_1,u_2)}.$$

Consider the group $\tilde{\mathscr{G}}$ of analytic automorphisms $\psi_{\sigma,u}$ of $\mathbf{C}\times V$ given by

$$\psi_{\sigma,w}(\lambda, z) = (\lambda.\sigma.e^{\pi H(z,w)},\ z + w)$$
$$\sigma \in \mathbf{C}^*,\ w \in V.$$

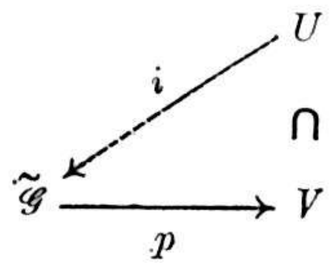
Then

$$\psi_{\sigma,w} \circ \psi_{\tau,v} = \psi_{\rho,w+v}$$
$$\rho = \sigma.\ \tau.\ e^{\pi H(v,w)},$$

so $\widetilde{\mathcal{G}}$ is an extension analogous to the theta-groups of §23:

$$1 \longrightarrow \mathbf{C}^* \xrightarrow{j} \widetilde{\mathcal{G}} \xrightarrow{p} V \longrightarrow 1$$
$$\psi_{\sigma,w} \xmapsto{p} w$$
$$\sigma \xmapsto{j} \psi_{\sigma,0}.$$

The data α defines a lifting i of U into $\widetilde{\mathcal{G}}$:

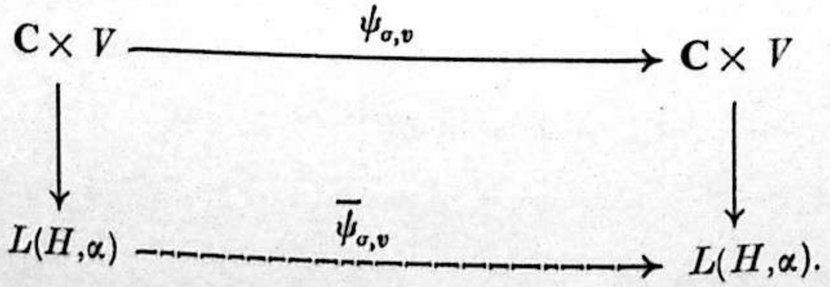


$$i(u) = \psi_{\sigma,u},\ \sigma = \alpha(u) \cdot e^{\frac{\pi}{2} H(u,u)},$$

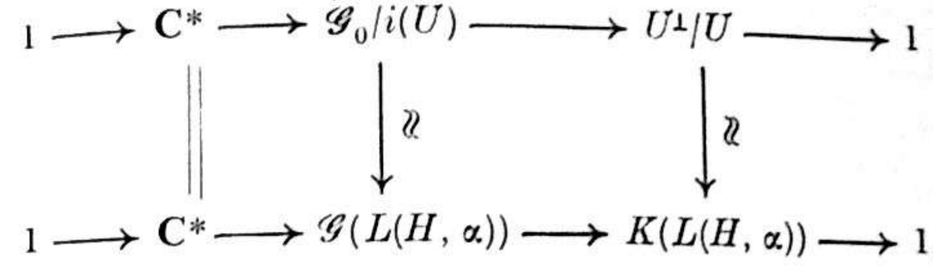
so that $L(H,\alpha)$ is, by definition, the quotient $\mathbf{C} \times V / i(U)$. The commutator in $\widetilde{\mathcal{G}}$, as in the theta-groups of §23, is given by a bi-homomorphism $\widetilde{e}: V \times V \to \mathbf{C}_1^*$ as follows:

$$\psi_{\sigma,w} \circ \psi_{\tau,v} \circ \psi_{\sigma,w}^{-1} \circ \psi_{\tau,v}^{-1} = \psi_{\widetilde{e}(v,w),0},$$
$$\widetilde{e}(v,w) = e^{2\pi i E(v,w)}.$$

Therefore, if $U^\perp = \{u \in V \mid E(u,u') \in \mathbf{Z},\ \text{all } u' \in U\}$ as before, it follows that the group $\widetilde{\mathcal{G}}_0 \underset{\text{def}}{=} p^{-1}(U^\perp) = \{\psi_{\sigma,v} \mid v \in U^\perp\}$ is the centralizer of $i(U)$ in $\widetilde{\mathcal{G}}$. Therefore, all the automorphisms $\psi_{\sigma,v}$, $v \in U^\perp$, descend to automorphisms $\bar{\psi}_{\sigma,v}$ of $L(H,\alpha)$:



This gives us a natural homomorphism $\mathcal{G}_0 \to \mathcal{G}(L(H,\alpha))$. But we saw in §9 that $K(L(H,\alpha)) \simeq U^\perp/U$, so we get in fact isomorphic extensions:



It follows that the commutators in these two groups are equal, hence we have proven

THEOREM 1. *If $L = L(H,\alpha)$ is a line bundle on $X = V/U$, $E = \operatorname{Im} H$, and $\pi : V \to X$ is the natural map, then for all $x, y \in U^\perp$:*

$$e^{-2\pi i E(x,y)} = e^L(\pi x, \pi y).$$

Since our ground field is $\mathbf{C}$, there is a canonical primitive n^{th} root of 1 for all n, namely $\zeta_n = e^{2\pi i/n}$. Therefore the module

$$M_l = \lim_{\leftarrow} \mu_{l^n}$$

has a canonical basis element ζ too, given by the sequence $e^{2\pi i/l^n} \in \mu_{l^n}$. We can now relate the Riemann forms

$$E: U \times U \to \mathbf{Z}, \text{ where } E = \operatorname{Im} H,$$
$$E^L: T_l X \times T_l X \to M_l, \text{ defined in § 20.}$$

Let π_l denote the natural map from U to $T_l X$, i.e. $\pi_l(u)$ is given by the sequence $u_n = \pi(u/l^n) \in X_{l^n}$, with $l u_{n+1} = u_n$. Then if $u, v \in U$,

$$E^L(\pi_l u, \pi_l v) = \text{the sequence } \bar{e}_{l^n}(u_n, \phi_L v_n)$$
$$= \text{the sequence } e^{L l^n}(u_n, v_n) \text{ (§ 23, property (5))}$$
$$= \text{the sequence } e^{-2\pi i l^n E(u/l^n,\, v/l^n)} \quad \text{(Theorem 1)}$$
$$= \text{the sequence } (\zeta_n)^{-E(u,v)}$$
$$= -E(u, v).\zeta.$$

Thus, except for sign, E^L is the $\mathbf{Z}_l$-linear extension of E from U to $T_l X$.

Applying this to the case where X is $Y \times \hat{Y}$ and L is the Poincaré bundle P, we see that the canonical non-degenerate integral pairing of the lattices U and $\hat{U}$ corresponding to Y and $\hat{Y}$, of the analytic theory (cf. §9, part (B)) is, up to sign, the same as the canonical non-degenerate l-adic pairing e_l of $T_l Y$ and $T_l \hat{Y}$ (cf. §20).

Next, consider the Rosati involution of $\mathrm{End}^0(X)$. Analytically, we use the interpretation:

$$\mathrm{End}^0(X) = \left\{ \begin{array}{l} \text{set of complex-linear endomorphisms } T\colon V \to V \\ \text{such that } T(\mathbf{Q}.U) \subset \mathbf{Q}.U \end{array} \right\}.$$

Then the natural involution is the adjoint with respect to H:

$$H(T^*x, y) = H(x, Ty), \quad \text{all } x, y \in V.$$

Since if $x \in \mathbf{Q}.U$, then for all $y \in \mathbf{Q}.U$, $E(T^*x, y) = E(x, Ty) \in \mathbf{Q}$, it follows that T^*x must be in $\mathbf{Q}.U$ too, i.e. $T^* \in \mathrm{End}^0(X)$. If T' is the image of T under the algebraic Rosati involution, then for all $x, y \in U$,

$$\begin{aligned} E((T^* - T')x, y) &= \mathrm{Im}\, H(T^*x, y) + E^L(T'\pi_l x, \pi_l y) \\ &= \mathrm{Im}\, H(x, Ty) + E^L(\pi_l x, T\pi_l y) \\ &= E(x, Ty) - E(x, Ty) = 0\ . \end{aligned}$$

Thus $T^* = T'$.

Now for any complex-linear operator $T\colon V \to V$, if T^* is its adjoint, then T^*T is a positive self-adjoint operator on the Hermitian vector space V, hence all its eigenvalues are positive, hence the complex trace, $\mathrm{Tr}(T^*T)$, is positive. If $T \in \mathrm{End}^0(X)$, so that T^*T maps the rational vector space $\mathbf{Q}.U$ into itself, its trace here is just twice its complex trace; and its l-adic trace in $T_l X \cong U \otimes \mathbf{Z}_l$ is equal to its rational trace. Therefore for any of these traces,

$$\mathrm{Tr}(T^* \circ T) > 0, \text{ all } T \in \mathrm{End}^0(X),\ T \neq 0.$$

Thus the positivity of the Rosati involution is obvious from the existence of the positive definite H with $\mathrm{Im}\, H = E$. In a sense, we have shown that over any ground field one can reverse this argument: namely, using the positivity of the Rosati involution, we have realised $NS^0(X)$ as a formally real Jordan algebra in which the ample L's are the positive elements.

BIBLIOGRAPHY

[A-G] A. Andreotti and H. Grauert : Théorèmes de finitude pour la cohomologie des espaces complexes, *Bull. Soc. Math. France*, 90 (1962), 193.

[B] Walter Baily : On the theory of θ-functions, the moduli of abelian varieties, and the moduli of curves, *Annals of Math.* 75 (1962), 342.

[B-K] H. Braun and M. Koecher : *Jordan Algebren*, Springer-Verlag, 1966.

[B-M] Armand Borel and George Mostow : editors, *Algebraic groups and discontinuous subgroups*, American Math. Soc. Providence, 1966.

[Br] L. Breen : On a non-trivial higher extension of representable abelian sheaves, *Bull. American Math. Soc.* 75 (1969), 1249.

[Bt] Iacopo Barsotti : Metodi analitici per varietà abeliane in caratteristica positiva, *Annali della Sc. Norm. Pisa*, appearing in several parts, 1964-1966.

[C] J. W. S. Cassels : Diophantine equations with special reference to elliptic curves, *J. London Math. Soc.* 41 (1966), 193.

[Co] Fabio Conforto : *Abelsche Functionen und algebraische Geometrie*, Springer, Berlin, 1956.

[D-G] Michel Demazure and Pierre Gabriel : *Séminaire Heidelberg-Strasbourg.*

[G1] Alexandre Grothendieck : *Séminaire de géométrie algébrique*, 1968.

[G2] A. Grothendieck : *Séminaire de géométrie algébrique*, 1960-61.

[G3] A. Grothendieck : *Séminaire de géométrie algébrique*, 1963-64 (Schémas en groupes).

[Go] Roger Godement : *Topologie algébrique et théorie des faisceaux*, Hermann, Paris, 1964.

[G-R] Robert Gunning and Hugo Rossi : *Analytic functions of several complex variables*, Prentice-Hall, 1965.

[H] G. Hochschild : *The structure of Lie groups*, Holden-Day, San Francisco, 1965.

[J] N. JACOBSON : *Lie algebras*, Wiley-Interscience, New York, 1962.

[K] KUNIHIKO KODAIRA : On compact analytic surfaces, *Analytic functions*, Princeton Univ. Press, 1960.

[L] SERGE LANG : *Abelian varieties*, Interscience-Wiley, New York, 1959.

[L-N] SERGE LANG and ANDRÉ NÉRON : Rational points of abelian varieties over function fields, *American J. Math.* 81 (1959), 95.

[M1] DAVID MUMFORD : *Geometric invariant theory*, Springer, Berlin, 1965.

[M2] D. MUMFORD : On the equations defining abelian varieties, *Inv. Math.* 1 (1966), 287.

[M3] D. MUMFORD : *Introduction to algebraic geometry*, forthcoming.

[Ma] YURI MANIN : The theory of commutative formal groups over fields of finite characteristic, *Uspekhi Mat. Nauk.* 18 (1963), No. 6, p. 1; transl. in *Russian Math. Surveys*, Macmillan.

[N] ANDRÉ NÉRON : Modèles minimaux des variétés abeliennes sur les corps locaux et globaux, *Publ. I.H.E.S.* No. 21, 1964.

[O] FRANS OORT : *Commutative group schemes*, Springer Lecture Notes, Vol. 15, 1966.

[S1] J.-P. SERRE : *Groupes algébrique et corps de classes*, Hermann et cie., Paris, 1959.

[Sh] GORO SHIMURA: On analytic families of polarized abelian varieties and automorphic functions, *Annals of Math.* 78 (1963), 149.

[T1] JOHN TATE : p-divisible groups in local fields, *Proc. NUFFIC summer school at Driebergen*, Springer, 1967.

[T2] J. TATE : Endomorphisms of abelian varieties over finite fields, *Inv. Math.* 2 (1966), 134.

[W1] ANDRÉ WEIL : *Variétés abéliennes et courbes algébrique*, Hermann, Paris, 1948.

[W2] A. WEIL : Théorèmes fondamentaux de la théorie des fonctions thêta, *Séminaire Bourbaki*, Exp. 16, 1949.

PRINTED IN INDIA

BY R. SUBBU

AT THE

TATA PRESS LIMITED

BOMBAY

AND

PUBLISHED BY

JOHN BROWN

OXFORD UNIVERSITY PRESS

BOMBAY