J. Math. Soc. Japan
Vol. 20, Nos. 1-2, 1968

Isogeny classes of abelian varieties over finite fields

Dedicated to Professor Shôkichi Iyanaga on his 60th birthday

By Taira HONDA

(Received July 24, 1967)
(Revised Sept. 25, 1967)

In the present paper we shall give a complete classification of isogeny classes of abelian varieties over finite fields in terms of Frobenius endomorphism and indicate some of its applications.

Let p be a fixed prime number and Ω the algebraic closure of the prime field of characteristic p. Let k_a denote the finite field with p^a elements. We consider $k_a \subset \Omega$. By an algebraic number field we mean a subfield of the complex number field $\boldsymbol{C}$ which is of finite degree over the rational number field $\boldsymbol{Q}$. We identify an ideal of an algebraic number field K with its extensions to over-fields of K as usual. We denote by $\boldsymbol{Z}$ the ring of rational integers and by $\boldsymbol{Z}_l$ its l-adic completion for a prime number l.

We shall say that an algebraic integer π (resp. an integral ideal $\mathfrak{a}$ of an algebraic number field) is *of type* (A_0), if we have

$$\pi^{\sigma}\pi^{\sigma\rho} = p^a \qquad (\text{resp. } \mathfrak{a}^{\sigma}\mathfrak{a}^{\sigma\rho} = (p^a))$$

with a positive integer a for any conjugate π^{σ} of π (resp. $\mathfrak{a}^{\sigma}$ of $\mathfrak{a}$), where ρ denotes the complex conjugacy of $\boldsymbol{C}$. The integer a is called the *order* of π (resp. $\mathfrak{a}$). It is well-known that to every k_a-simple abelian variety A over k_a corresponds a conjugacy class of numbers of type (A_0) with order a by considering the Frobenius endomorphism of A. Thus we obtain a map

Φ_a: {k_a-isogeny classes of k_a-simple abelian varieties over k_a}
$\rightarrow$ {conjugacy classes of numbers of type (A_0) with order a}.

Our main result is as follows:

MAIN THEOREM. *The map Φ_a is bijective for every $a \geqq 1$.*

In § 1 of this paper we shall study basic properties of numbers and ideals of type (A_0). It is shown that any ideal of type (A_0) can be represented as a principal ideal with a number of type (A_0) in a suitable extension field (Theorem 1). Our aim in § 1 is to prove Theorem 2, which asserts that some power of an ideal of type (A_0) has a prime ideal decomposition attached to a suitable CM-type. This implies that some power of a number of type (A_0) is in fact a value of a suitable "Grössencharakter" of type (A_0). (For the definition of

such a character, see Weil [20].)

In § 2 we shall prove the main theorem. First we consider Ω-simple abelian varieties over Ω. Let π_1 and π_2 be numbers of type (A_0). We shall say that π_1 is *equivalent* to π_2 and write $\pi_1 \sim \pi_2$, if ${\pi_1}^{\nu_1}$ is conjugate to ${\pi_2}^{\nu_2}$ for some positive integers ν_1 and ν_2. The same definition applies also to ideals of type (A_0). With this definition we have a map

Φ: {Ω-isogeny classes of Ω-simple abelian varieties over Ω}
$\rightarrow$ {equivalence classes of numbers of type (A_0)}.

By Theorem 1 of Tate [17] the map Φ_a, a fortiori Φ, is injective. Moreover the surjectivity of Φ_a follows from that of Φ by the standard method of descending the field of definition. Since we have a bijection

Ψ: {equivalence classes of numbers of type (A_0)}
$\rightarrow$ {equivalence classes of ideals of type (A_0)}

by Theorem 1, we have only to prove the surjectivity of $\Psi \circ \Phi$. Our idea to prove it consists in combining Theorem 2 with a basic theorem in the theory of complex multiplication which determines the prime ideal decomposition of the Frobenius endomorphism of the abelian variety obtained by reducing an abelian variety of a CM-type (cf. Shimura-Taniyama [13]). The criterion of Néron-Ogg-Šafarevič (Serre [7], Serre-Tate [9]) then guarantees a good reduction by a finite extension of the field of definition. In this way we see that *for a given ideal* $\mathfrak{a}$ *of type* (A_0) *there is a* CM*-type with the following property: let* A *be an abelian variety of this type defined over a sufficiently large algebraic number field and let* $\tilde{A}$ *be the reduction of* A *at a prime divisor of* p. *Then an* Ω*-simple component of* $\tilde{A}$ *is mapped to the class of* $\mathfrak{a}$ *by* $\Psi \circ \Phi$. In some cases we can find a CM-type such that $\tilde{A}$ itself is Ω-simple. In these cases we can also determine the endomorphism algebra $\mathrm{End}_{\Omega}(\tilde{A}) \otimes \boldsymbol{Q}$ explicitly as a certain cyclic algebra, proving the formula (7) of Tate [17].

In § 3 we shall indicate a few ideas to apply the main theorem to certain important problems. Firstly our main theorem is most directly applied to various types of existence problems. For example we can easily give an affirmative answer to the conjecture of Manin [5] that the formal group $G_{m,n} \times G_{n,m}$ is algebroid for any (m, n). Secondly our main theorem, combined with that of Tate [17], allows us an analytic construction of abelian varieties over finite fields by considering the representations of the Frobenius endomorphism in the Tate and Dieudonné modules. Thirdly the results of Tate and us will also make it possible to generalize Deuring's results [1] on endomorphism rings of elliptic curves over finite fields to those of abelian varieties of higher dimensions. These ideas will be developped in forthcoming papers.

The fact, that the surjectivity of Φ_a follows from that of Φ, was pointed out by Professor J. Tate to the author who had at first considered only Ω-

isogeny classes. The endomorphism μ in Proposition 9 is due to Professor G. Shimura. The author wishes to express his hearty thanks to them.

§ 1. Numbers and ideals of type (A_0).

Following Shimura [12], we mean by a CM-field a totally imaginary quadratic extension of a totally real algebraic number field. The following properties of CM-fields can be easily verified.

PROPOSITION 1. *An algebraic number field K is a* CM*-field if and only if the following two conditions are satisfied.*

(a) *The complex conjugacy ρ induces a non-trivial automorphism of K.*

(b) *$\rho\sigma=\sigma\rho$ for every isomorphism σ of K into $\boldsymbol{C}$.*

PROPOSITION 2. *The composite of a finite number of* CM*-fields is again a* CM*-field. In particular the normal closure of a* CM*-field over $\boldsymbol{Q}$ is a* CM*-field.*

For a number π of type (A_0) we denote by $[\pi]$ the conjugacy class of π and by $\langle\pi\rangle$ its equivalence class. The same notations are applied also to ideals.

PROPOSITION 3. *Let π_1 and π_2 be numbers of type (A_0). Then we have $(\pi_1)\sim(\pi_2)$, if and only if $\pi_1\sim\pi_2$.*

PROOF. "If" part is obvious. Assume that $(\pi_1)\sim(\pi_2)$. This implies $\pi_1^{\nu_1}=\varepsilon\pi_2^{\nu_2}$ with positive integers ν_1, ν_2 and a unit ε. Since every conjugate of ε has absolute value 1, ε must be a root of unity. Thus we have $\pi_1\sim\pi_2$.

PROPOSITION 4. *Let π be a number of type (A_0) and let a be its order. If π is real, $\pi=\pm p^{a/2}$. If π is imaginary, $\boldsymbol{Q}(\pi)$ is a* CM*-field.*

PROOF. The first assertion is clear. The second follows from the definition of type (A_0) and Proposition 1.

Let π be a number of type (A_0). We put $\boldsymbol{Q}(\pi^\infty)=\bigcap_{\nu=1}^{\infty}\boldsymbol{Q}(\pi^\nu)$. This is an algebraic number field determined by $\langle\pi\rangle$ up to conjugacy.

LEMMA 1. *Let $\mathfrak{a}$ be an ideal of type (A_0) of an algebraic number field L normal over $\boldsymbol{Q}$. Put $H=\{\tau\in\mathrm{Gal}(L/\boldsymbol{Q})\,|\,\mathfrak{a}^\tau=\mathfrak{a}\}$ and let K be the corresponding subfield of L. Then we can find an integer $\nu\geqq 1$ and a number π of type (A_0) in K such that $(\pi)=\mathfrak{a}^\nu$.*

PROOF. Let $\mathfrak{p}$ be a prime divisor of p in L and let Z (resp. D) be the decomposition group (resp. field) of $\mathfrak{p}$ for $L/\boldsymbol{Q}$. For a left coset decomposition $G=\mathrm{Gal}(L/\boldsymbol{Q})=Z\sigma_1+\cdots+Z\sigma_g$, we have a prime ideal decomposition of p in L: $(p)=\prod_{j=1}^{g}\mathfrak{p}^{e\sigma_j}$, where e denotes the ramification index of p in L. Let a be the order of $\mathfrak{a}$ and let $\mathfrak{a}=\prod_{j=1}^{g}\mathfrak{p}^{\nu_j\sigma_j}$ be the prime ideal decomposition of $\mathfrak{a}$. For $\tau\in G$, let $Z\sigma_{\tau(j)}$ be the coset containing $\sigma_j\tau$. We have

$$\nu_{\tau(j)}=\nu_j \quad \text{for} \quad \tau\in H \tag{1}$$

and

$$\nu_j+\nu_{\rho(j)}=ae\,. \tag{2}$$

Since $\mathfrak{p}^e$ is an ideal of D, we can find $h\geqq 1$ and $\xi\in D$ such that $\mathfrak{p}^{eh}=(\xi)$. Put $\pi=\prod_{j=1}^{g}\xi^{\nu_j\sigma_j}$. By (1) we see $\pi\in K$. Moreover we have by (2)

$$\pi\pi^{\rho}=\prod_{j=1}^{g}(\xi^{ae})^{\sigma_j}=N_{D/\boldsymbol{Q}}\ \xi^{ae}\in\boldsymbol{Q}$$

and the same holds for every conjugate of π. As $(\pi)=\mathfrak{a}^{eh}$, we have $\pi^{\sigma}\pi^{\sigma\rho}=p^{aeh}$ for every conjugate π^{σ} of π. Hence π is of type (A_0). This completes our proof.

For an ideal $\mathfrak{a}$ of type (A_0), we denote by $\boldsymbol{Q}(\mathfrak{a}^{\infty})$ the field K defined as above. It is easy to see that this is independent of the choice of L.

PROPOSITION 5. *For every ideal $\mathfrak{a}$ of type (A_0), there exists a positive integer ν_0 such that every $\mathfrak{a}^{\nu}$ with $\nu_0|\nu$ is an ideal of $\boldsymbol{Q}(\mathfrak{a}^{\infty})$, but an ideal of no proper subfield of it.*

PROOF. This follows immediately from the definition and Lemma 1.

THEOREM 1. *Let $\mathfrak{a}$ be an ideal of type (A_0). Then we can find a number π of type (A_0) such that $(\pi)=\mathfrak{a}$. For a given $\mathfrak{a}$ such a number π is determined uniquely up to roots of unity. Moreover we have $\mathbf{Q}(\mathfrak{a}^{\infty})=\mathbf{Q}(\pi^{\infty})$.*

PROOF. By Lemma 1 we can find $\pi'\in\mathbf{Q}(\mathfrak{a}^{\infty})$ of type (A_0) such that $(\pi')=\mathfrak{a}^{\nu}$ with $\nu\geqq 1$. Let π be a number such that $\pi^{\nu}=\pi'$. We have $\pi'\pi'^{\rho}=p^{a\nu}$, where a denotes the order of $\mathfrak{a}$. Therefore we have $\pi\pi^{\rho}=\zeta p^{a}$ with $\zeta^{\nu}=1$. Since $\zeta>0$, we must have $\zeta=1$. Applying the same reasoning to conjugates of π, we see in fact π is of type (A_0). Now the second assertion is obvious. The last is contained in Lemma 1.

COROLLARY. *Put $\Psi(\langle\pi\rangle)=\langle(\pi)\rangle$ for a number π of type (A_0). Then Ψ gives a bijection: {equivalence classes of numbers of type (A_0)}$\to${equivalence classes of ideals of type (A_0)}.*

PROOF. The injectivity of Ψ follows from Proposition 3 and the surjectivity from Theorem 1.

Now it is an easy excercise to determine all the ideals of type (A_0) in a given CM-field L normal over $\boldsymbol{Q}$, whenever we know the prime ideal decomposition of p in L.

PROPOSITION 6. *Let $\mathfrak{a}$ be an ideal of type (A_0) and L the normal closure of $\boldsymbol{Q}(\mathfrak{a}^{\infty})$ over $\mathbf{Q}$. If the decomposition field D of a prime divisor $\mathfrak{p}$ of p in L is normal over $\boldsymbol{Q}$, we must have $L=D$; in other words p decomposes completely in $\mathbf{Q}(\mathfrak{a}^{\infty})$.*

PROOF. We may assume $\mathfrak{a}$ is an ideal of $\boldsymbol{Q}(\mathfrak{a}^{\infty})$. Let $(p)=\prod_{j=1}^{g}\mathfrak{p}^{e\sigma_j}$ be the prime ideal decomposition of p in L and put $\mathfrak{a}=\prod_{j=1}^{g}\mathfrak{p}^{\nu_i\sigma_i}$. By our assumption

$\mathfrak{p}^{\sigma_i e}$ is an ideal of D for $1 \leqq j \leqq g$. Hence $\mathfrak{a}^e$ is an ideal of D, which implies $\boldsymbol{Q}(\mathfrak{a}^\infty) \subset D$. Therefore we have $L \subset D$ and hence $L = D$.

PROPOSITION 7. *Let $S(a, n)$ be the set of conjugacy classes of numbers π of type (A_0) with order a such that $[\boldsymbol{Q}(\pi) : \boldsymbol{Q}] = 2n$. Then $S(a, n)$ is a finite set for any $a, n \geqq 1$.*

PROOF. Let $[\pi] \in S(a, n)$ and let $f(X) = X^{2n} + c_1 X^{2n-1} + \cdots + c_j X^{2n-j} + \cdots + p^{an}$ be the minimal polynomial of π in $\mathbf{Q}$. Denoting by $\pi_1, \cdots, \pi_{2n}$ the complete set of conjugates of π, we have

$$|c_j| = \Big|\sum_{i_1 < \cdots < i_j} \pi_{i_1} \cdots \pi_{i_j}\Big| \leqq \sum_{i_1 < \cdots < i_j} |\pi_{i_1}| \cdots |\pi_{i_j}| = \binom{2n}{j} p^{aj/2}$$

for $1 \leqq j \leqq 2n-1$. Therefore the number of such polynomials $f(X)$ is bounded by a suitable constant depending only on a and n.

Now let F be a CM-field of degree $2n$ over $\boldsymbol{Q}$ and $\{\varphi_1, \cdots, \varphi_n\}$ be n isomorphisms of F into $\boldsymbol{C}$ such that no two of them are complex conjugate. Then $(F; \{\varphi_i\})$ is a CM-type, that is, there is an abelian variety A over an algebraic number field such that there is an injection $\iota : F \to \mathrm{End}_C(A) \otimes \boldsymbol{Q}$ and such that the representation of $\iota(F)$ in the space of invariant differential forms on A is equivalent to $\varphi_1 \oplus \cdots \oplus \varphi_n$ (cf. [**13**, Chap. II]). Now our aim in § 1 is to prove

THEOREM 2. *For any ideal $\mathfrak{a}$ of type (A_0) there is a* CM*-type $(F; \{\varphi_i\})$ with the following properties:*

(a) *F is a* CM*-field normal over $\boldsymbol{Q}$.*

(b) *For a prime divisor $\mathfrak{p}$ of p in F we have*

$$\mathfrak{a} \sim \prod_i \mathfrak{p}^{\psi_i}$$

with $\psi_i = \varphi_i^{-1}$.

PROOF. By Proposition 5 we may assume that $\mathfrak{a}$ is an ideal of $\boldsymbol{Q}(\mathfrak{a}^\infty)$. Moreover we may suppose that $\boldsymbol{Q}(\mathfrak{a}^\infty)$ is a CM-field by Proposition 4 and by Theorem 1 excluding the trivial case $\boldsymbol{Q}(\mathfrak{a}^\infty) = \boldsymbol{Q}$. Let a be the order of $\mathfrak{a}$ and let C be a cyclic extension of $\boldsymbol{Q}$ for which the degree of p is a multiple of a. Denoting by L the normal closure of $\boldsymbol{Q}(\mathfrak{a}^\infty)$ over $\boldsymbol{Q}$, we see that the composite field $F = L \circ C$ is a CM-field normal over $\boldsymbol{Q}$. Let $\mathfrak{p}$ be a prime divisor of p in F and denote by f, e and Z its degree, its ramification index and its decomposition group respectively. For $\mathrm{Gal}(F/\boldsymbol{Q}) = G = Z\sigma_1 + \cdots + Z\sigma_g$ we have $(p) = \prod_{j=1}^{g} \mathfrak{p}^{e\sigma_j}$. Put $\mathfrak{a} = \prod_{j=1}^{g} \mathfrak{p}^{\nu_j \sigma_j}$. Now $d = f/a$ is an integer. By taking $d\nu_j$ elements of $Z\sigma_j$ for all $1 \leqq j \leqq g$, we obtain $\sum_{j=1}^{g} d\nu_j = efg/2 = [F : \boldsymbol{Q}]/2$ elements of G. As is shown in the following, we can choose these so that no two of them are complex conjugate. First assume $\rho(1) \neq 1$, that is, $Z\sigma_1\rho \neq Z\sigma_1$. Take any subset S_1 of $Z\sigma_1$ with $d\nu_1$ elements and put $S_{\rho(1)} = Z\sigma_1\rho - S_1\rho$. Since $ef - d\nu_1 = d(ae - \nu_1) = d\nu_{\rho(1)}$ by (2), the subset $S_{\rho(1)}$ of $Z\sigma_{\rho(1)}$ has $d\nu_{\rho(1)}$ elements. If $\rho(1)$

$=1$, that is, $Z\sigma_1\rho=Z\sigma_1$, we choose a subset S_1 of $Z\sigma_1$ with $ef/2=d\nu_1$ elements so that no two of them are complex conjugate. By repeating the same procedure for the remaining cosets of G/Z, we derive the subset $S=\bigcup_{j=1}^{g} S_j$, which is the required one. Denote the elements of S by $\{\psi_i\}$ and put $\varphi_i=\psi_i^{-1}$. Then $(F:\{\varphi_i\})$ is a CM-type and we have

$$\prod_i \mathfrak{p}^{\psi_i}=(\prod_{j=1}^{g}\mathfrak{p}^{\nu_j\sigma_j})^d\sim\mathfrak{a}\,.$$

This completes the proof.

REMARK. In the same way we can prove that a generalized CM-type in the sense of Shimura [11], [12] can be obtained by "restricting" a suitable CM-type.

§ 2. The proof of the main theorem.

In order to prove the main theorem we have only to prove the surjectivity of $\Psi\circ\Phi$ and to deduce the surjectivity of Φ_a from that of Φ, as was mentioned in the introduction. The surjectivity of $\Psi\circ\Phi$ follows directly from Theorem 2 and the following two theorems:

THEOREM A. *Let $(F;\{\varphi_i\})$ be a* CM*-type and let (A,ι) be an abelian variety of that type, defined over an algebraic number field K. Suppose K is large enough so that $F^{\varphi_i}\subset K$ for all i. Suppose A has non-degenerate reduction at a prime $\mathfrak{P}$ of K, and let $\tilde{A}$ be the reduction of $A \bmod \mathfrak{P}$. Then there exists an element $\pi_0\in F$ such that $\tilde{\tau}(\pi_0)$ is the Frobenius endomorphism of $\tilde{A}$ relative to the residue field of $\mathfrak{P}$, and we have*

$$(\pi_0)=\prod_i (N_{K/F\varphi_i}\mathfrak{P})^{\psi_i}\qquad \textit{with}\quad \psi_i=\varphi_i^{-1}\,.$$

THEOREM B. (Serre-Tate [9].) *Let (A,ι) be an abelian variety of a* CM*-type, defined over an algebraic number field K. Then there exist a finite extension K' of K and an abelian variety (A',ι') defined and isomorphic to (A,ι) over K' such that A' has non-degenerate reduction at every prime of K'.*

For a given ideal $\mathfrak{a}$ of type (A_0), let $(F;\{\varphi_i\})$ be a CM-type satisfying the conditions of Theorem 2 and take (A,ι) and K as in Theorem A. By Theorem B we may suppose A has non-degenerate reduction at every prime of K. Let $\mathfrak{p}$ be a prime of F above p and $\mathfrak{P}$ a prime of K above $\mathfrak{p}$. By [13, II, Proposition 3] $\tilde{A}$ is Ω-isogenous to a power of an Ω-simple abelian variety B. Let ξ be the Frobenius endomorphism of B (relative to a finite field of definition). Then we have, with the notations of Theorem A,

$$(\xi)\sim(\pi_0)=\prod_i (N_{K/F}\mathfrak{P})^{\psi_i}\sim\prod_i\mathfrak{p}^{\psi_i}\sim\mathfrak{a}\,,$$

which completes our proof.

Now Theorem A was first mentioned in Taniyama [**14**], where he reduced the proof to the case $\mathfrak{P}$ was of absolute degree 1. In this case the proof is direct (Shimura [**10**], Taniyama [**14**]). But there was an error in this reduction of the proof and a complete proof was given by Shimura (cf. the footnote (2) of [**15**]). According to his letter to the author, it is as follows: let l be a prime number prime to $\mathfrak{P}$ and prime to $\zeta-1$ for all the roots of unity $\zeta \neq 1$ in F. We may suppose l-section points of A are rational over K. Now we can find $h \geqq 1$ and $\xi \in K$ such that $\mathfrak{P}^h=(\xi)$ and $\xi \equiv 1 \pmod{l}$. Let $\tilde{\tau}(\pi_1)$ be the $N(\mathfrak{P})^h$-power endomorphism of $\tilde{A}$ with $\pi_1 \in F$ and put $\mu=\prod_i (N_{K/F}\varphi_i\xi)^{\psi_i}$. It suffices to prove $\pi_1=\mu$. Suppose there were $\nu>0$ with $\pi_1 \not\equiv \mu \pmod{l^\nu}$. Let K'' be the extension of K obtained by adjoining the coordinates of l^ν-section points of A and the ray class field mod l^ν over K. K'' is an abelian extension of K in which $\mathfrak{P}$ is unramified. Put $\sigma=\left(\frac{K''/K}{\mathfrak{P}^h}\right)$. We can find a prime $\mathfrak{Q}$ of K with absolute degree 1 such that $\left(\frac{K''/K}{\mathfrak{Q}}\right)=\sigma$ and $\mathfrak{Q}=(\eta)$ with $\eta \in K$, $\eta \equiv \xi \pmod{l^\nu}$. Let $\tilde{\tau}(\lambda)$ be the $N(\mathfrak{Q})$-th power endomorphism of $A \bmod \mathfrak{Q}$ with $\lambda \in F$. Since Theorem A holds for $\mathfrak{Q}$, we have $(\lambda)=\prod_i (N_{K/F}\varphi_i\mathfrak{Q})^{\psi_i}$. More precisely we have $\lambda=\prod_i (N_{K/F}\varphi_i\eta)^{\psi_i}$, because the both members of the last equality $\equiv 1 \pmod{l}$ and their ratio is a root of unity in F. Since $\lambda \equiv \mu \pmod{l^\nu}$, we have $\pi_1 t=t^\sigma=\lambda t=\mu t$ for any l^ν-section point t of A. This implies $\pi_1 \equiv \mu \pmod{l^\nu}$, a contradiction. Theorem 1 in [**13**, Chap. III], proved in an alternative way, is somewhat weaker than Theorem A in that it assumes unramifiedness of p in F.

Now we have proved the surjectivity of Φ. Let us prove that of Φ_a. Let π be a number of type (A_0) of order a. Then there are $\nu \geqq 1$ and an abelian variety A defined and simple over $k_{a\nu}$ such that there is an imbedding of $\boldsymbol{Q}(\pi^\nu)$ into $\mathrm{End}_{k_{a\nu}}(A) \otimes \boldsymbol{Q}$ mapping π^ν to the Frobenius endomorphism of A. Denote by σ the Frobenius substitution of $k_{a\nu}/k_a$ and by ξ_V the p^a-th power morphism of V onto V^σ for an algebraic variety V over $k_{a\nu}$. Put $B=A \times A^\sigma \times \cdots \times A^{\sigma^{\nu-1}}$ and let g be an isomorphism of B^σ onto B obtained by the obvious permutation of the factors. We see easily $g \circ g^\sigma \circ \cdots \circ g^{\sigma^{\nu-1}}=1$. Put

$$f_{ij}=g^{\sigma^j} \circ \cdots \circ g^{\sigma^{i+1}} \quad \text{for} \quad 0 \leqq i \leqq j \leqq \nu-1$$

and

$$f_{ij}=f_{ji}^{-1} \quad \text{for } 0 \leqq j \leqq i \leqq \nu-1 .$$

We have easily

(i) $$f_{jk} \circ f_{ij}=f_{ik}$$

(ii) $$f_{i+j,i+k}=f_{j,k}^{\sigma^i},$$

which imply the consistence conditions of Weil [21] (see also Lang [4]), and by [21, Theorem 3] there exists an abelian variety A_0 over k_a and an isomorphism $f: B \to A_0$ over $k_{a\nu}$ such that $f^\sigma = f \circ g$. Now put $\alpha = g \circ \xi_B$ ($\in \mathrm{End}_{k_{a\nu}}(B)$). Since

$$f \circ \alpha = f \circ g \circ \xi_B = f^\sigma \circ \xi_B = \xi_{A_0} \circ f$$

ξ_{A_0} has the same eigenvalues as α. Let $\mathfrak{B}$ be a basis of the Tate module $T_l(A)$ of A with respect to a prime $l \neq p$. Then $(\mathfrak{B}, \mathfrak{B}^\sigma, \cdots, \mathfrak{B}^{\sigma^{\nu-1}})$ is a basis of $T_l(B)$. The matrix representation of α with respect to this basis has a form

$$\begin{pmatrix} 0 & X & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots\cdots & 0 & & X \\ X & 0 & \cdots\cdots & 0 & \end{pmatrix},$$

where X^ν is the representation matrix of the Frobenius endomorphism ξ_A^ν of A with respect to $\mathfrak{B}$ and has an eigenvalue π^ν. From this it is easily verified that every ν-th root of π^ν is an eigenvalue of α. In particular π is an eigenvalue of α and hence that of ξ_{A_0}. Therefore there exists a k_a-simple component of A_0 which is mapped to $[\pi]$ by Φ_a. This proves the surjectivity of Φ_a and completes the proof of our main theorem.

Now let us come back to consideration of Ω-isogeny classes. From now on until the end of § 2 we shall consider every homomorphism of an abelian variety a homomorphism over an algebraically closed field. Let $\mathfrak{a}$ be an ideal of type (A_0) of order a, let (A, ι) be an abelian variety of a CM-type $(F; \{\varphi_i\})$ satisfying the conditions of Theorem 2, and let $\tilde{A}$ be the reduction of A at a prime divisor of p. In general $\tilde{A}$ is not simple, but isogenous to some power of a simple abelian variety A_1 such that $\Psi \circ \Phi(\langle A_1 \rangle) = \langle \mathfrak{a} \rangle$, where $\langle A_1 \rangle$ denotes the (Ω-) isogeny class of A_1. But in certain cases we can find a CM-type such that $\tilde{A}$ itself is simple. We shall say that an ideal $\mathfrak{b}$ of an algebraic number field K is primitive, if there is no ideal $\mathfrak{b}'$ of K such that $\mathfrak{b} = \mathfrak{b}'^\nu$ with $\nu > 1$.

PROPOSITION 8. *Let $\mathfrak{a}$ be an ideal of type (A_0) of order a and suppose $\mathfrak{a}$ is a primitive ideal of $\boldsymbol{Q}(\mathfrak{a}^\infty)$. Suppose the following conditions are satisfied;*

(a) *$p \neq 2$ or $8 \nmid a$.*

(b) *$\boldsymbol{Q}(\mathfrak{a}^\infty)$ is normal over $\boldsymbol{Q}$.*

(c) *The degree of p in $\boldsymbol{Q}(\mathfrak{a}^\infty)$ is 1.*

Then we can find a CM-type $(F; \{\varphi_i\})$ such that $\tilde{A}$ is simple and $\Psi \circ \Phi(\langle \tilde{A} \rangle) = \langle \mathfrak{a} \rangle$ for an abelian variety A of this type.

By (a) there is a cyclic extension C of $\boldsymbol{Q}$ of degree a in which p remains prime (Hasse [2]). Put $F = \boldsymbol{Q}(\mathfrak{a}^\infty) \circ C$ and construct a CM-type $(F; \{\varphi_i\})$ as in

the proof of theorem 2. We have to prove the simplicity of $\tilde{A}$ for an abelian variety (A, ι) of this type. This follows immediately from a result of Tate [**17**, p. 142] taking the primitivity of $\mathfrak{a}$ into account. But we shall prove Proposition 8 by determining $\mathrm{End}_{\mathfrak{Q}}(\tilde{A})\otimes\boldsymbol{Q}$ explicitly as a cyclic algebra. In the following we shall use definitions and results of [**13**, Chap. II] freely without referring to them. Suppose (A, ι) is principal and defined over a sufficiently large algebraic number field K normal over $\boldsymbol{Q}$. Let $\mathfrak{P}$ be a prime divisor of p in K and let σ be a Frobenius substitution of $K/\boldsymbol{Q}$ at $\mathfrak{P}$. We can choose σ so that $\sigma|F\in\mathrm{Gal}(F/\boldsymbol{Q}(\mathfrak{a}^{\infty}))$. (We may assume $K\supset F$, because K is "sufficiently" large. We omit the same kinds of remarks in the following.) This σ induces the Frobenius substitution of the residue field k of $K \bmod \mathfrak{P}$. We shall denote it by the same letter σ.

LEMMA 2. *Let (A, ι) be as above and put $\iota_1(\alpha)=\iota^{\sigma}(\alpha^{\sigma^{-1}})$ for $\alpha\in F$. Then (A^{σ}, ι_1) is of type $(F; \{\varphi_i\})$.*

PROOF. Let $\{\omega_1, \cdots, \omega_n\}$ be a basis of invariant differential forms on A such that

$$\delta\iota(\alpha)\omega_i=\alpha^{\varphi_i}\omega_i \qquad \text{for} \quad \alpha\in F\,.$$

We have

$$\delta\iota^{\sigma}(\alpha)\omega_i{}^{\sigma}=\alpha^{\varphi_i\sigma}\omega_i{}^{\sigma}$$

and hence

$$\delta\iota_1(\alpha)\omega_i{}^{\sigma}=\alpha^{\sigma^{-1}\varphi_i\sigma}\omega_i{}^{\sigma}=\alpha^{\varphi_i}\omega_i{}^{\sigma}\,,$$

since $\sigma|F$ belongs to the center of $\mathrm{Gal}(F/\boldsymbol{Q})$. This completes the proof.

By Lemma 2 there are an integral ideal $\mathfrak{b}$ of F and a $\mathfrak{b}$-multiplication λ of (A^{σ}, ι_1) onto (A, ι). Denote by ξ the p-th power homomorphism of abelian varieties and put $\mu=\tilde{\lambda}\xi$ $(\in\mathrm{End}_{\mathfrak{Q}}(\tilde{A}))$. Since we have

$$\mu\tilde{\iota}(\alpha)=\tilde{\lambda}\xi\tilde{\iota}(\alpha)=\tilde{\lambda}\tilde{\iota}^{\sigma}(\alpha)\xi=\tilde{\lambda}\tilde{\iota}_1(\alpha^{\sigma})\xi$$
$$=\tilde{\iota}(\alpha^{\sigma})\tilde{\lambda}\xi=\tilde{\iota}(\alpha^{\sigma})\mu\,,$$

μ^a commutes with $\tilde{\iota}(F)$ and $\in\tilde{\iota}(F)$. Thus we obtain a cyclic subalgebra $(\mu^a, \tilde{\iota}(F), \sigma)$ of $E=\mathrm{End}_{\mathfrak{Q}}(\tilde{A})\otimes\boldsymbol{Q}$. Now the simplicity of $\tilde{A}$ is contained in

PROPOSITION 9. *With the notations and assumptions as above, $(\mu^a, \tilde{\iota}(F), \sigma)$ is a division algebra and coincides with E. Moreover, for the prime ideal decomposition $\mathfrak{a}=\prod_{j=1}^{g}\mathfrak{p}_j{}^{\nu_j}$ in $\boldsymbol{Q}(\mathfrak{a}^{\infty})$, we have*

$$\mathrm{inv}_{\mathfrak{p}_j}E\equiv\nu_j/a \pmod{\boldsymbol{Z}} \qquad \textit{for} \quad 1\leqq j\leqq g\,.$$

PROOF. By Theorem 1 and the proof of the main theorem there is an integer $\nu_0\geqq 1$ such that $\boldsymbol{Q}(\xi^{\nu})=\tilde{\iota}(\boldsymbol{Q}(\mathfrak{a}^{\infty}))$ for $\nu_0|\nu$. But ξ^{ν} belongs to the center of E, when k_{ν} is a field of definition for $\mathrm{End}_{\mathfrak{Q}}(\tilde{A})$. Hence $\tilde{\iota}(\boldsymbol{Q}(\mathfrak{a}^{\infty}))$, the center of $E'=(\mu^a, \tilde{\iota}(F), \sigma)$, is contained in the center of E. This implies $E=E'$ by

the well-known theorem on simple algebras, since both E and E' have the maximal subfield $\tilde{\tau}(F)$ in common. Let p^{ah} be the number of elements of k. Putting $\iota_i(\alpha)=\iota^{\sigma^i}(\alpha^{\sigma^{-i}})$, we have

$$\lambda\iota^{\sigma}(\alpha^{\sigma^{-1}})=\iota(\alpha)\lambda\,,$$

$$\lambda^{\sigma^i}\iota^{\sigma^{i+1}}(\alpha^{\sigma^{-1}})=\iota^{\sigma^i}(\alpha)\lambda^{\sigma^i}$$

and

$$\lambda^{\sigma^i}\iota_{i+1}(\alpha)=\iota_i(\alpha)\lambda^{\sigma^i}\,.$$

This shows that λ^{σ^i} is a $\mathfrak{b}^{\sigma^i}$-multiplication of $(A^{\sigma^{i+1}}, \iota_{i+1})$ onto (A^{σ^i}, ι_i). Thus we have

$$\begin{aligned}\mu^{ah}&=(\tilde{\lambda}\tilde{\xi})\cdots(\tilde{\lambda}\tilde{\xi})\\&=\tilde{\lambda}^{1+\sigma+\cdots+\sigma^{ah-1}}\xi^{ah}\end{aligned}$$

and hence

$$(\mu^{ah})=(N_{F/L}\mathfrak{b})^h(\xi^{ah})\,,$$

writing $\boldsymbol{Q}(\mathfrak{a}^{\infty})=L$. Let m_j be an integer such that $\mathfrak{p}_j^{m_j}|\mu^a$, but $\mathfrak{p}_j^{m_j+1}\nmid\mu^a$ for every $1\leqq j\leqq g$. Since $(\xi^{ah})=\mathfrak{a}^h$ and the degree of $\mathfrak{p}_j$ for F/L is a, we have

$$hm_j\equiv h\nu_j \pmod{ah}$$

and then

$$m_j\equiv\nu_j \pmod{a}\,.$$

As $\mathfrak{p}_j$ is unramified in F/L, this implies

$$\mathrm{inv}_{\mathfrak{p}_j}E\equiv m_j/a\equiv\nu_j/a \pmod{\boldsymbol{Z}}\,.$$

Since the primitivity of $\mathfrak{a}$ implies $(\nu_1,\cdots,\nu_g)=1$, E is a division algebra. Thus all the assertions of our proposition are proved.

This idea of the explicit determination of E already appeared in Honda [3], where we determined E for the jacobian of the curve $y^2=1-x^l$ with an odd prime l. I have not been able to construct a CM-type for an arbitrary ideal $\mathfrak{a}$ of type (A_0) so that $\tilde{A}$ is simple.

§ 3. Applications. (Sketches.)

3.1. Algebroid formal groups.

By the fundamental theorem 4.1 of Manin [5] the prime ideal decomposition of the Frobenius endomorphism of an abelian variety A over a finite field determines the formal structure of A over Ω up to isogeny. (The condition imposed on the roots of the characteristic polynomial in that theorem is superfluous. For this see Tate [18].) Thus all the existence problems of commutative algebroid formal groups over Ω have now been reduced to excercises on algebraic number theory, that is, problems of finding ideals of type (A_0) with

preappointed properties. For example we can easily give an affirmative answer to the conjecture of Manin [5].

THEOREM 3. *The formal group $G_{m,n}\times G_{n,m}$ is algebroid over Ω for any (m, n).*

PROOF. As a formal group isogenous to an algebroid group is also algebroid, we have only to prove $G_{m,n}\times G_{n,m}$ is algebroid up to isogeny. Moreover we may assume $(m, n)=1$. Let K be an imaginary quadratic field in which p decomposes: $(p)=\mathfrak{p}\mathfrak{p}'$. Then $(\Psi\circ\Phi)^{-1}(\langle\mathfrak{p}^m\mathfrak{p}'^n\rangle)$ answers to our requirement.

Problem (15.9) of Oort [6] is not less trivial. Examples of simple abelian varieties of mixed type in the sense of Oort are already found in the jacobians of the curves $y^2=1-x^l$ (Honda [3]). We can also give examples of Ω-simple abelian varieties of dimension 2 whose formal completions are isogenous to $G_{1,0}\times G_{1,1}$. Let K_0 be a real quadratic field in which p decomposes and let K be a totally imaginary quadratic extension of K_0 in which one of the prime divisors of p decomposes and the other is ramified: $(p)=\mathfrak{p}_1\mathfrak{p}_1'\mathfrak{p}_2^2$ in K. It is easy to see that $\mathfrak{a}=\mathfrak{p}_1\mathfrak{p}_2$ is of type (A_0) and that $A\sim G_{1,0}\times G_{1,1}$ for $A\in(\Psi\circ\Phi)^{-1}(\langle\mathfrak{a}\rangle)$ by Manin's theorem.

3.2. Analytic construction of abelian varieties over finite fields.

The most important consequence of our main theorem is that it allows us an analytic construction of abelian varieties over finite fields.

Let A be an abelian variety of dimension n over k_a. For a prime number $l\neq p$, denote by $T_l(A)$ the Tate module of A. This is a vector space of dimension $2n$ over $\boldsymbol{Z}_l$. Let $M_l(A)$ be the representation matrix of the p^a-th power endomorphism of A in $T_l(A)$ with respect to some basis of $T_l(A)$. This matrix determines the isogeny class of A by the main theorem of Tate [17]. More precisely $M_l(A_1)$ is conjugate to $M_l(A_2)$ over $\boldsymbol{Z}_l$, if and only if there is an isogeny $\lambda: A_1\to A_2$ over k_a such that $l\nmid$ the degree of λ. Moreover, for any semi-simple matrix M' of order $2n$ over $\boldsymbol{Z}_l$ which has the same eigenvalues as $M_l(A)$, there is an abelian variety A' such that $M_l(A')$ is conjugate to M' over $\boldsymbol{Z}_l$. Now our main theorem gives necessary and sufficient conditions in order that the conjugacy class of a matrix M of order $2n$ over $\boldsymbol{Z}_l$ corresponds to some abelian variety. These conditions are quite analogous to those of Riemann matrices in case of complex tori.

For $l=p$ we consider the Dieudonné module $T_p(A)$ of the p-divisible group $A(p)$ obtained from A (cf. Manin [5], Serre [8]). It is a vector space of dimension $2n$ over the Witt vector ring $W(k_a)$. The theorem of Tate [18], which gives a canonical bijection: $\mathrm{Hom}_k(A, B)\otimes\boldsymbol{Z}_p\to\mathrm{Hom}_k(A(p), B(p))$ for abelian varieties A, B over a finite field k, makes it possible to generalize the results for $l\neq p$ to those for p. It should be noted that there is an essential difference between two cases: the matrix $M_l(A)$ is an l-adic unimodular matrix for $l\neq p$,

whereas $M_p(A)$ is not unimodular over $W(k_a)$ and p-adic values of its eigenvalues (considered in some extension of $W(k_a)$) determines the class $\langle A\rangle$. Finally we can deal with the isomorphism class of A by working in the adèle space

$$\coprod_{l\neq p} \boldsymbol{Z}_l^{2n} \times W(k_a)^{2n}.$$

These considerations would be applicable to the construction of higher jacobian varieties over finite fields and perhaps to the conjecture of Weil.

3.3. Types of the endomorphism rings of abelian varieties over finite fields.

Our main theorem together with results of Tate [**17**], [**18**] will make it possible to study endomorphism rings of abelian varieties over finite fields. This was completely carried out in Deuring [**1**] for elliptic curves and some of his theorems extend almost trivially to higher dimensions. (In fact some results for any dimensions are already given in [**13**, Chap. II, 7].) Moreover his results on $\mathfrak{p}$-adic representations of endomorphism rings can be replaced by more complete ones by using Dieudonné modules. Of course the explicit determination of types of endomorphism rings would be complicated in case of higher dimensions and we should have to overcome ring-theoretical difficulties.

Osaka University

References

[1] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Math. Sem. Univ. Hamburg, **14** (1941), 197–272.
[2] H. Hasse, Zum Existenzsatz von Grunwald in Klassenkörpertheorie, J. Reine Angew. Math., **188** (1950), 40–64.
[3] T. Honda, On the jacobian variety of the algebraic curve $y^2=1-x^l$ over a field of characteristic $p>0$, Osaka J. Math., **3** (1966), 189–194.
[4] S. Lang, Abelian varieties, Interscience Tracts, New York, 1959.
[5] Y. Manin, The theory of commutative formal groups over fields of finite characteristic, Russian Math. Surveys, **18** (1963), 1–81.
[6] F. Oort, Commutative group schemes, Lecture Notes in Math., Springer, Berlin-Heidelberg-New York, 1966.
[7] J.-P. Serre, L'Annuaire du College de France, 1964/65.
[8] J.-P. Serre, Groupes p-divisible, Sem. Bourbaki, 318, 1966/67.
[9] J.-P. Serre and J. Tate, Good reduction of abelian varieties and applications, to appear.
[10] G. Shimura, On complex multiplications, Proceedings of the International Symposium on Algebraic Number Theory, Tokyo-Nikko, 1955, Science Council of Japan, 1956, 23–30.
[11] G. Shimura, On the field of definition for a field of automorphic functions, I, II, III, Ann. of Math., **80** (1964), 160–189, **81** (1965), 124–165, **83** (1966), 377–385.

[12] G. Shimura, Construction of class fields and zeta functions of algebraic curves, Ann. of Math., **85** (1967), 58–159.
[13] G. Shimura and Y. Taniyama, Complex multiplication of abelian varieties and its applications to number theory, Publ. Math. Soc. Japan, No. 6, Tokyo, 1961.
[14] Y. Taniyama, Jacobian varieties and number fields, Proceedings of the International Symposium on Algebraic Number Theory, Tokyo-Nikko, 1955, Science Council of Japan, 1956, 31–45.
[15] Y. Taniyama, L-functions of number fields and zeta functions of abelian varieties, J. Math. Soc. Japan, **9** (1957), 330–366.
[16] J. Tate, Algebraic cycles and poles of zeta functions, Arithmetical algebraic geometry, 93–110, Harper and Row, New York, 1965.
[17] J. Tate, Endomorphisms of abelian varieties over finite fields, Invent. Math., **2** (1966), 134–144.
[18] J. Tate, In preparation.
[19] A. Weil, Variétés abéliennes et courbes algébriques, Hermann, Paris, 1948.
[20] A. Weil, On a certain type of characters of the idèle-class group of an algebraic number-field, Proceedings of the International Symposium on Algebraic number Theory, Tokyo-Nikko, 1955, Science Council of Japan, 1956, 1–7.
[21] A. Weil, The field of definition of a variety, Amer. J. Math., **78** (1956), 509–524.